GLOBAL THREAT INTELLIGENCE REPORT

NTT Security

With visibility into 40% of the world's internet traffic, NTT Security combines analysis of over 6.1 trillion logs and 150 million attacks for the Global Threat Intelligence Report.

The report highlights the evolving global threat landscape, with this year's most notable findings being the increased number of attacks on the finance sector and a dramatic increase in ransomware detection.

VERTICAL MARKETS IN THE FIRING LINE

In the UK, Manufacturing has been cybercrime's biggest victim:

46% vs 18%

Manufacturing was the most attacked sector in the UK with 46% of all attacks – more than double the percentage of attacks on Manufacturing in EMEA (18%).

23% vs 19%

Technology was the second most attacked sector in the UK with 23% of all attacks – above the global percentage of 19%.

TOP FIVE ATTACKED INDUSTRIES

- Manufacturing – **46%**
- Technology – **23%**
- NEW Business and Professional Services – **10%**
- Finance – **8%**
- Government – **5%**

Business and Professional Services is a new member of the top five attacked industry sectors in the UK, ranking third with 10% of attacks, above Finance (8%) and Government (5%).

RANSOMWARE INCREASES AND TURNS DESTRUCTIVE

£350% INCREASE

Ransomware attacks jumped in malware detections, up from 1% in 2016 to 7% in 2017 at a global level.

#1 29%

In EMEA, ransomware was the leading type of malware – 29% of all attacks.

Gaming was the most targeted sector, with 36% of all ransomware attacks in EMEA.

3% vs 26%

Spyware and key loggers made up 3% of malware in EMEA, in contrast to 26% globally.

ATTACKERS CONTINUE TO USE REGIONAL SOURCES TO ATTACK THE UK

#1 89%

China was the top source country for attacks against Manufacturing in the UK with 89% of attacks.

#1 19%

China was also the top source of attacks against Government (19%).

The US was the top country source of attacks against the UK for the Technology sector (27%), Business and Professional Services (24%) and Finance (36%).

BUSINESSES FACE AN UPHILL BATTLE

NTT Security recommends the following steps:

Key Processes

Make security a part of key processes for business enablement and risk assessment.

Layered Defences

Implement layered defences, including multi-factor authentication, to make it more difficult for attackers to breach an organisation.

Endpoint Hygiene

Enforce good endpoint hygiene, including responsible computing usage and end-user training to help reduce the chances of users executing hostile environments.

Current Attack Techniques

Make the best use of data feeds and intelligence sources to keep up with current attack techniques, exploits, and campaigns.

Use Intelligence Services

Use threat intelligence services to help prioritise security resources in an effective manner, and potentially mitigate threats *before* they impact the organisation.

Develop Incident Response Plan

Develop and regularly review plans for incident response and disaster recovery.

The report and details of the research methodology can be downloaded at:
www.nttsecurity.com/gtir-uk