# WannaCry helps put EMEA as number one ransomware target – NTT Security 2018 Global Threat Intelligence Report

Submitted by: Origin Comms Ltd
Thursday, 26 April 2018

Ransomware attacks jumped in malware detections last year, up 350 per cent from just 1 per cent in 2016 to 7 per cent in 2017 at a global level. In EMEA, however, ransomware was the leading type of malware representing nearly one third (29 per cent) of all attacks in the region. This is according to the 2018 Global Threat Intelligence Report (GTIR) (http://www.nttsecurity.com/gtir-uk) launched by NTT Security (http://www.nttsecurity.com/), the specialised security company and center of excellence in security for NTT Group. At the other end of the scale, spyware and key loggers made up just 3 per cent of malware in EMEA, in contrast to 26 per cent globally.

One of the worst ransomware attacks to date, WannaCry infected more than 400,000 machines across 150 countries in May last year, with many healthcare organisations becoming the worst affected in the UK.

According the GTIR, while healthcare was identified as a major industry target for ransomware, the gaming sector, made up mostly of gambling companies (poker, casinos and sports betting), was the most targeted in 2017, with 36 per cent of all ransomware attacks in the region. NTT Security analysts put this down to the sector having high uptime requirements, with operations that are time sensitive and where outages could lead directly to major losses, making them more attractive to attackers.

NTT Security analysed data from over 6.1 trillion logs and 150 million attacks for the GTIR, highlighting global and regional threat and attack trends based on log, event, attack, incident and vulnerability data from NTT Group operating companies. While NTT Security detected ransomware attacks in every industry sector, the top five targeted sectors (gaming, business & professional services, health care, manufacturing and technology) accounted for more than 80 per cent of all ransomware detections in EMEA (and 72 per cent globally).

Jon Heimerl, senior manager of the Threat Intelligence Communication Team, Global Threat intelligence Center at NTT Security, says: “Ransomware became the weapon of choice last year and shows no sign of losing its popularity. The high detection rates in EMEA have certainly been buoyed by headline-grabbing incidents like WannaCry and Petya, which affected entire industries and effectively brought down some companies, and were designed to deliver maximum impact and cause huge disruption.

“It’s interesting, however, that we are seeing big differences in the more traditional tools of spyware and key loggers, accounting for just 3 per cent in EMEA but over a quarter of all attacks globally. This suggests that attack campaigns in EMEA have been focusing more on quick wins which ransomware can deliver, rather than long-term access other attack vectors can provide.”

According to the GTIR, while the volume of ransomware is rising, ransomware incident response engagement fell from over 22 per cent of incidents in 2016 to just over 5 per cent in 2017; the result of better detection, more effective policies and procedures, improved awareness and better incident response plans.

“It’s clear that organisations are prioritising incident response much more than they have done in

the past, at least when it comes to ransomware," adds NTT Security's Jon Heimerl. "Our 2017 Risk:Value Report showed that nearly half (48 per cent) of all respondents indicated they have an incident response plan in place, with another third working on their plans. However, just because organisations are getting better at managing some incidents, they cannot afford to be lulled into a false sense of security."

The 2018 Global Threat Intelligence Report (GTIR) gathers data from NTT Security monitoring, management, and incident response operations. It also includes details from NTT Security research sources including global honeypots and sandboxes in over 100 countries in environments independent from institutional infrastructures.

To learn more about the trends identified, follow the link to download the NTT Security 2018 GTIR: www.nttsecurity.com/gtir-uk

Ends

Notes for editors:

About NTT Security
NTT Security is the specialized security company and the center of excellence in security for NTT Group. With embedded security we enable NTT Group companies (Dimension Data, NTT Communications and NTT DATA) to deliver resilient business solutions for clients' digital transformation needs. NTT Security has multiple SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group (Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit nttsecurity.com to learn more about NTT Security or visit www.ntt.co.jp/index_e.html to learn more about NTT Group.

For sales enquiries, please visit dimensiondata.com, www.ntt.com/en/index.html, www.nttdata.com/global/en/ or speak to your NTT account representative for more information.

For more information, please contact:
Origin Communications
t. +44 (0)20 3814 2940
e. nttsecurity@origincomms.com



Distributed via Press Release Wire (https://pressreleases.responsesource.com/)on behalf of Origin Comms Ltd

Copyright © 1999-2019 ResponseSource, Melrose House, 42 Dingwall Road, Croydon, London, CR9 2DX UK

e: info@responsesource.com t: 0345 370 7777 f: 0345 370 7776 w: https://www.responsesource.com

ResponseSource
Press Release Wire