UK manufacturing is top target for cyber attackers – NTT Security 2018 Global Threat Intelligence Report

Submitted by: Origin Comms Ltd
Thursday, 3 May 2018

Manufacturing has become the most attacked industry sector in the UK, representing almost half (46 per cent) of all cyber attacks in 2017 – more than double that of attacks on manufacturing across EMEA.

This is according to the 2018 Global Threat Intelligence Report (GTIR) (https://www.nttsecurity.com/en-uk/landing-pages/2018-gtir) from NTT Security, the specialised security company and centre of excellence in security for NTT Group. The majority of attacks on UK manufacturers came from China, representing 89 per cent of attacks on this sector.

Technology organisations, in second place, were the target of 23 per cent of attacks in the UK, with business and professional services in third place with 10 per cent of attacks. While the finance industry was the most attacked sector worldwide with almost a quarter (23 percent) of all attacks, up from 14 per cent in 2016, it was fourth in the UK with 8 per cent, followed by government at 5 per cent.

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.

“We’ve seen manufacturing becoming an increasingly attractive target to attackers in recent years and we believe this is for a number of reasons,” explains Jon Heimerl, senior manager of the Threat Intelligence Communication Team, Global Threat intelligence Center at NTT Security.

“As manufacturers experience the benefits of automation and the emergence of interconnected and intelligent production systems, they are realigning their operational models to take advantage of these technologies. More than 50 per cent of manufacturers have now adopted Industry 4.0 and Smart Manufacturing, the latest phase in the evolution of manufacturing technology. The lines between traditional and digital manufacturing are blurring, where high value manufacturing and advanced technologies are key for global competitiveness. As a result, they have become more attractive to attackers who see them as a prime target for the theft of IP, for the disruption of operations, and for hijacking networks to launch an attack into other organisations. There’s no one thing driving this trend, but a whole host of interconnected reasons.”

China the number one attack source

China was the number one source of attacks against all sectors in EMEA during 2017. EMEA was the only region in which attacks from U.S. sources fell behind Chinese sources, whereas in 2016 China was the ninth most prominent attack source, accounting for less than 3 per cent of all attacks against EMEA.

Attacks from Chinese sources have escalated to the point that China was a top five attack source in each of the top five most attacked industries in EMEA, and accounted for 67 per cent of all attacks against manufacturing targets across EMEA.

According to the GTIR, the majority of these attacks on UK manufacturers were from a known bad source

(meaning the activity originated from IP addresses within China previously identified as hostile).

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: https://www.nttsecurity.com/en-uk/landing-pages/2018-gtir

Notes for editors:

Summary of findings – UK:

• Manufacturing was the most attacked sector in the UK, with 46% of all attacks, more than double the percentage of manufacturing attacks against EMEA.
• In EMEA the top 5 industry sectors were the same, but in different orders. The biggest difference was manufacturing at 20% in EMEA and 46% in UK.
• In each of the top five attack sources targeting manufacturing, at least 96% of all detections were due to "known bad source" or "reconnaissance".
• China alone was responsible for 89% of all attacks against manufacturing in the UK. After China and the US, many of the top attack sources against manufacturing were from other EMEA countries.
• Between the UK and EMEA, the overall attack patterns were comparable - reconnaissance, known bad sources, web application attacks, application specific attacks.
• In the UK, finance was the target in 8% of attacks, while in EMEA it was 20% - less than half of the attacks.
• UK sources also saw a lower percent of DoS/DDoS attacks than in EMEA in general.

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.

Media contact:

Amanda Hassall, Consultant
Origin Comms
amanda@origincomms.com
+441628 822741/+44 7855 359889