UK manufacturing drops to second place in league table of most attacked industry sectors – 2019 Global Threat Intelligence Report reveals

Submitted by: Origin Comms Ltd
Monday, 29 April 2019

UK Manufacturing and Technology sectors continue to battle it out for first and second place in the table of most targeted industry sectors by cyber attackers, according to the 2019 Global Threat Intelligence Report (GTIR) (https://www.nttsecurity.com/landing-pages/2019-gtir) from NTT Security (https://www.nttsecurity.com/en-uk), the is the specialised security company and the center of excellence in security for NTT Group. While Manufacturing took top billing in the 2018 GTIR, with almost half (46 per cent) of all cyber attacks in the UK, this year's report shows a significant fall to second place with a fifth (20 per cent) of attacks. However, the Tech sector, which attracted less than a quarter (23 per cent) last year, jumps to top spot with 47 per cent of attacks in the UK.

Finance, which earlier this month was revealed to be the most attacked sector in EMEA, accounting for 30% of all attacks, takes third place for the UK, with 13 per cent of attacks, falling some way short of the global figure of 17 per cent. Business & Professional Services and Healthcare take fourth and fifth place with 4 per cent and 3 per cent respectively.

The annual GTIR is the result of NTT Security summarising data from trillions of logs and millions of attacks, and analysing threat trends based on log, event, attack, incident and vulnerability data from NTT Group operating companies. In the latest report, NTT Security analyses of attacks against 18 industry sectors.

David Gray, Senior Manager – Cyber Security Consulting, NTT Security, says: "While manufacturing may have dropped down a position, the fact that it is still attracting a fifth of all attacks against UK organisations is a major concern. The critical national infrastructure sectors tend to grab the headlines, such as the attacks on the Ukrainian national grid in 2016, or the Wannacry attack on the NHS in 2017. However, the recent attacks on Norsk Hydro demonstrate the impact that cyber attacks can have on other sectors, such as manufacturing, and highlight the importance of effective incident response."

David Gray adds: "The lines between traditional and digital manufacturing are blurring, where high value manufacturing and advanced technologies are key for global competitiveness and there is greater convergence of IT with Operational Technology (OT), which brings with it greater complexity and risk. The problem is that OT has traditionally been something of a 'dark art' for IT and security teams who lack the knowledge and skills to effectively map their OT risk landscape and implement practical plans and processes."

NTT Security advises manufacturing organisations to focus on four key areas when it comes to cybersecurity:

1. Get the basics right: without the right fundamentals in place, attacks do not need to be advanced to succeed. People are often a manufacturer's greatest threat, so invest in staff awareness and training, and highlight the importance of collective responsibility.
2. Take an intelligence-driven approach to security. IT and security should avoid working in silos and

having a 'not in my backyard' mentality by developing robust holistic processes and procedures.
3. Develop threat intelligence capabilities. There is no such thing as an isolated incident and there is a need to manage the whole incident by developing threat intelligence – pervasive visibility is essential.
4. Manufacturers are still failing to prepare. There is still an element of 'head in the sand', where they do not think it is going to happen to them. Having effective incident response capabilities that are tested regularly is key and enables organisations to respond quickly in order to mitigate the threat and identify the cause.

China tops source of attacks table

Once again China is the number one source of attacks by country against UK organisations (20 per cent) followed by the US (16 per cent) and France (10 per cent). Apart from Sweden, the UK is the only country to see most attacks coming from China. Across EMEA, China is second (13 per cent) just behind the US (16 per cent) while at a global level again the US is top attack source on 22 per cent followed by China on 13 per cent.

To download the NTT Security 2019 GTIR: https://www.nttsecurity.com/2019GTIR

NTT Security is running a webinar called 'How to shine a light on operational technology risk' at 2.00pm BST on 22nd May 2019. To register go to: https://www.nttsecurity.com/en-uk/landing-pages/operational-technology-services

About NTT Security (https://www.nttsecurity.com/en-uk)

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

Methodology for the GTIR

The NTT Security 2019 Global Threat Intelligence Report contains global attack data gathered from NTT Security and supported operating companies from October 1, 2017, to September 31, 2018. The analysis is based on log, event, attack, incident and vulnerability data from clients. It also includes details from NTT Security research sources, including global honeypots and sandboxes located in over 100 countries in environments independent from institutional infrastructures. Leveraging the indicator, campaign and adversary analysis from our Global Threat Intelligence Platform has played a significant role in tying activities to actors and campaigns.

NTT Security summarizes data from trillions of logs and billions of attacks for the 2019 GTIR. NTT Security gathers security log, alert, event and attack information, enriches it to provide context, and analyzes the contextualized data. This process enables real-time global threat intelligence and alerting. The size and diversity of our client base, with over 10,000 security clients on six continents, provides NTT Security with security information which is representative of the threats encountered by most organizations.

The data is derived from worldwide log events identifying attacks based on types or quantities of events. The use of validated attack events, as opposed to the raw volume of log data or network traffic, more accurately represents actual attack counts. Without proper categorization of attack events, the disproportionately large volume of network reconnaissance traffic, false positives, authorized security scanning and large floods of DDoS monitored by Security Operations Centers (SOCs), would obscure the actual incidence of attacks.

The inclusion of data from the 10 SOCs and seven research and development centers of NTT Security provides a highly accurate representation of the ever-evolving global threat landscape.

Media contact:
Amanda Hassall, Consultant
M: +44 (0)7855 359889
T: +44 (0)1628 822741
amanda@origincomms.com