NTT Ltd. Global Threat Intelligence Report: UK Manufacturing most attacked industry as cyber criminals innovate and automate attacks

Submitted by: Origin Comms Ltd
Tuesday, 19 May 2020

Cyber criminals are evolving their tradecraft with new innovations and increasingly automating their attacks, according to the 2020 Global Threat Intelligence Report (GTIR) (https://hello.global.ntt/en-us/insights/2020-global-threat-intelligence-report?utm_source=PR&utm_medium=Referral&utm_car launched today by NTT Ltd. (https://hello.global.ntt/en-us), a world-leading global technology services provider. In the UK and Ireland, Manufacturing became the most attacked sector representing almost a third of all attacks, while Technology was the most attacked sector globally. The GTIR also highlights the importance of cyber-resilience and security-by-design as cyber criminals look to gain from the COVID-19 pandemic.

A comprehensive view of the threats impacting businesses in EMEA, the Americas and Asia Pacific, as well as emerging trends across different industries, the GTIR reveals that threat actors are innovating faster than ever before. Developing multi-function attack tools and using artificial intelligence (AI) and machine learning capabilities, attackers are investing in automation techniques; 21% of attacks globally were in the form of a vulnerability scanner. Despite efforts to layer up their defences, many organisations are unable to stay ahead of attackers, while others are struggling to do the basics like patching old vulnerabilities.

UK manufacturing under attack
Manufacturing regularly appears as one of the most attacked industries globally. Most commonly linked to intellectual property (IP) theft, it increasingly faces financially motivated data breaches, global supply chain risks and risks from unpatched vulnerabilities. The UK was the only country (apart from Hong Kong) this year where Manufacturing topped the list of most attacked sectors, representing 29% of all attacks, with Technology (19%) second and Business and Professional Services (17%) third. Government and Finance made up the other two sectors in the top five.

Reconnaissance attacks accounted for half of all hostile activity in the UK and Ireland, with web application the next most common form of attack (22%). Reconnaissance activity (60%) was also the most common attack type against manufacturers followed by web application attacks (36%).

Rory Duncan, Security Go-to-Market Leader, NTT Ltd. (https://hello.global.ntt/en-us), comments: “UK manufacturing has become a major target for attackers in recent years as a result of the increased risks brought about from the convergence of IT and Operational Technology (OT). The biggest worry is that security has lagged behind in this sector, potentially exposing systems and processes to attack. Poor OT security is a legacy issue; many systems were designed with efficiency, throughput and regulatory compliance in mind rather than security. In the past, OT also relied on a form of ‘security through obscurity’. The protocols, formats and interfaces in these systems were often complex and proprietary and different from those in IT systems, so it was difficult for attackers to mount a successful attack. As more and more systems come online, hackers are innovating and see these systems as ripe for attack.”

Duncan adds: “Now more than ever, it’s critical for all organisations, regardless of sector or region, to pay attention to the security that enables their business; making sure they are cyber-resilient and secure-by-design, which means embedding privacy and security into the fabric of their enterprise architecture and organisational culture. The current global pandemic and the flow of trusted and untrusted information used to mask the activities of cyber criminals has shown us that they will take advantage of any situation. Organisations must be ready to respond to these and other threats in a constantly evolving landscape.”

The ‘year of enforcement’
The 2020 Global Threat Intelligence Report calls last year the ‘year of enforcement’ with the number of Governance, Risk and Compliance (GRC) initiatives growing, creating a challenging global regulatory landscape. Several acts and laws now influence how organisations handle data and privacy, including the General Data Protection Regulation (GDPR), which has set a high standard for the rest of the world. The report provides organisations with recommendations to help navigate compliance complexity, including identifying acceptable risk levels, building cyber-resilience capabilities and implementing solutions that are secure-by-design.

The 2020 GTIR – the 8th annual report – analyses and summarises trends based on log, event, attack, incident and vulnerability data from trillions of logs and billions of attacks. To learn more about how this year’s GTIR offers organisations a robust framework to address today’s cyber threat landscape, and to learn more about the emerging trends across different industries and regions, including the Americas, APAC and EMEA, follow the link (https://hello.global.ntt/en-us/insights/2020-global-threat-intelligence-report?utm_source=PR&utm_medium=Referral&utm_car to download the NTT Ltd. 2020 GTIR:

Global Highlights: 2020 Global Threat Intelligence Report:
- Most common attack types accounted for 88% of attacks: Application-specific (33%), web application (22%), reconnaissance (14%), DoS/DDoS (14%) and network manipulation (5%) attacks.
- Weaponisation of IoT: Botnets like Mirai, IoTroop and Echobot have advanced in automation, improving propagation capabilities. Mirai and IoTroop are also known for spreading through IoT attacks, then propagating through scanning and subsequent infection from identified hosts.
- Old vulnerabilities remain an active target: Attackers leveraged those that are several years old, but have not been patched by organisations, such as HeartBleed, which helped make OpenSSL the second most targeted software with 19% of attacks globally. A total of 258 new vulnerabilities were identified in Apache frameworks and software over the past two years, making Apache the third most targeted in 2019, accounting for over 15% of all attacks observed.
- Attacks on Content Management Systems (CMS) accounted for about 20% of all attacks: Targeting popular CMS platforms like WordPress, Joomla!, Drupal, and noneCMS, cyber criminals used them as a route into businesses to steal valuable data and launch additional attacks. Additionally, more than 28% targeted technologies (like ColdFusion and Apache Struts) support websites.

About NTT Ltd.
NTT Ltd. is a leading global technology services company. We partner with organisations around the world to shape and achieve outcomes through intelligent technology solutions. For us, intelligent means data driven, connected, digital and secure. As a global ICT provider, we employ more than 40,000 people in a

diverse and dynamic workplace that spans 57 countries, trading in 73 countries and delivering services in over 200 countries and regions. Together we enable the connected future. Visit us at hello.global.ntt

Methodology for the Global Threat Intelligence Report (GTIR)
The NTT Ltd. 2020 Global Threat Intelligence Report contains global attack data gathered from NTT Ltd. and supported operating companies from October 1, 2018 to September 31, 2019. The analysis is based on log, event, attack, incident, and vulnerability data from clients. 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 Ltd. gathers security log, alert, event, and attack information from which it enriches and analyses contextualised 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 Ltd. with security information which is representative of the threats encountered by most organisations.

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 categorisation of attack events, the disproportionately large volume of network reconnaissance traffic, false positives, authorised 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 Ltd. provides a highly accurate representation of the ever-evolving global threat landscape.

Media information:

For access to the GTIR 2020 technical report, Exec Guide, infographics, video and threat insights, visit the NTT Insights page (https://hello.global.ntt/en-us/insights/2020-global-threat-intelligence-report?utm_source=PR&utm_medium=Referral&utm_car and for a global press release, visit the NTT Newsroom (https://hello.global.ntt/en-us/newsroom/ntt-ltds-global-threat-intelligence-report-attack-volumes-up-as-cyber-criminals-innovat

For more information, please contact:
Amanda Hassall, Consultant
Origin Communications
E: amanda@origincomms.com or nttsecurity@origincomms.com
T: +44 (0)1628 822741
M: +44 (0)7855 359889