2019 Global Threat Intelligence Report: Finance returns to top spot as most attacked sector in EMEA

Submitted by: Origin Comms Ltd
Tuesday, 9 April 2019

NTT Security (https://www.nttsecurity.com/en-uk), the specialised security company, has launched its 2019 Global Threat Intelligence Report (GTIR) (https://www.nttsecurity.com/en-uk/landing-pages/2019-gtir), which reveals finance as the most attacked sector in EMEA, accounting for 30% of all attacks – compared to 17% globally. It knocks business and professional services off the top spot, which was last year's most attacked sector at 20%.

NTT Security summarises data from trillions of logs and billions of attacks for the 2019 GTIR, which analyses threat trends based on log, event, attack, incident and vulnerability data from NTT Group operating companies. In the new report, NTT Security continues its analysis of attacks against 18 industry sectors and shares its observations of the challenges faced by organisations globally.

The GTIR also reveals that the finance sector is joined by business and professional services (24%), technology (17%) and manufacturing (9%) in the list of top four attacked industries in EMEA. Web application attacks are largely to blame, accounting for over 43% of hostile activity against these sectors, which is well above the global average of 32%.

The finance industry in EMEA experienced a sizeable increase in web attacks, almost doubling from 22% to 43% over the last year, reinforcing its vulnerability to cybersecurity attacks. Similarly, manufacturing experienced a massive surge in web attacks (rising from 9% to 42%), although the overall attack volume across EMEA decreased.

Kai Grunwitz, SVP NTT Security EMEA, says: "Finance is yet again on the top spot when it comes to targeted attacks, which surely is enough evidence to convince the board that cybersecurity is a must-have investment. Sadly, many financial organisations are moving forward with digital transformation but without security built-in. While legacy methods and tools are still quite effective at providing a solid foundation for mitigation, new attack methods are constantly being developed by malicious actors. Security leaders should ensure basic controls remain effective, but they must also embrace innovative solutions if they provide a good fit and true value.

"Some of the most prevalent activity in EMEA during the past year was related to web-application attacks – and it's not surprising. These attacks most often rely on leveraging an exposed unpatched vulnerability or misconfigured system, targeting organisations with high volumes of sensitive data. The consequences could be devastating as it could be used for financial gain, industry superiority or corporate espionage. Our GTIR once again highlights the fact that critical vulnerabilities – both old and new – need to be patched as quickly as possible in client environments, especially given the convergence of IT with Operational Technology."

Elsewhere in the GTIR, attacks from sources within China against all targets in EMEA dropped nearly 40% to 13% – following closely behind the United States at 16%. Although this does not imply the actual attacker has changed; rather the source of the attacks has changed. Interestingly, the top five attacked sectors in EMEA experienced more attacks from within EMEA than from any other region (75%). This supports

the common notion that attackers tend to leverage attack sources near their targets, an observation which was demonstrated stronger in EMEA than other regions.

Other quotes on the GTIR:

Mr. Fumitaka Takeuchi, Security Evangelist, Vice President, Managed Security Service Taskforce, Corporate Planning at NTT Communications, says: “Many organisations are caught up in simply buying solutions to problems that either don‘t really exist, or a solution that costs more than the potential loss being prevented. Our advice for organisations, regardless of the industry they operate in, is to leverage existing relationships with trusted experts and to keep an eye on professional and managed service maturity in the cybersecurity space. First and foremost, it is essential to know where the real risks lie and then develop solutions accordingly.”

Stefaan Hinderyckx, Senior Director Security Europe at Dimension Data, says: “This year’s GTIR clearly demonstrates that cybersecurity attacks are constantly evolving. While attack volumes don’t always increase, new threats are certainly being introduced. In fact, 2018 set a record for the number of new vulnerabilities identified and reported in a single year. NTT Group has spent the last 15 years working with our clients to help them defend against the evolving threat landscape, which is increasingly complex. Understanding the threat environment helps our clients predict and mitigate potential threats in the digital world.”

“The threat report indicates the variety of attacks is not as broad as it would seem, while the United States and China are also often identified as the most common attack sources,” said Neil Trussler SVP & CTO, NTT DATA UK. “As frequently attacked industries, such as financial services, safeguard their businesses from these sophisticated cybercriminals, leaders must ensure a completely secure infrastructure, from endpoint to core, that allows them to focus on daily operations.”

To learn more about the how this year’s GTIR offers organisations a robust framework to address today’s cyber threat landscape, follow the link to download the NTT Security 2019 GTIR (https://www.nttsecurity.com/en-uk/landing-pages/2019-gtir)

More information

About NTT Security

NTT Security is the specialised 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

Metholodogy for the Global Threat Intelligence Report (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 30, 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
M: +44 (0) 78 5535 9889
T: +44 (0) 16 2882 2741
amanda@origincomms.com