NTT Global Threat Intelligence Report: Up to 300% Increase in Attacks from Opportunistic Targeting

Tuesday 11 May, 2021

- Healthcare, finance and manufacturing industries hit hard as attackers take advantage of global destabilization

- Application attacks spike, accounting for 67% of all attacks as remote-access becomes a common vulnerability

- Cryptocurrency miners reach new heights, accounting for 41% of all detected malware

LONDON, UK: 11 May 2021 – NTT Ltd., a world-leading global technology services provider, today launched its 2021 Global Threat Intelligence Report (GTIR), which reveals how hackers are taking advantage of the global destabilization by targeting essential industries and common vulnerabilities from the shift to remote working. Healthcare, manufacturing, and finance industries all saw an increase in attacks (200%, 300%, and 53% respectively), with these top three sectors accounting for a combined total of 62% of all attacks in 2020, up 11% from 2019.

As organizations race to offer more virtual, remote access through the use of client portals, application-specific and web-application attacks spiked, accounting for 67% of all attacks, which has more than doubled in the past two years. Healthcare bore the brunt of these attacks from its shift to telehealth and remote care, with 97% of all hostile activity targeted at the industry being web-application or application-specific attacks.

The GTIR provides insights from NTT's Cybersecurity Advisory that applies a maturity score of an industry's security program, with a higher number indicating a more mature plan of action. Concerningly, healthcare and manufacturing have relatively low maturity scores of only 1.02 and 1.21, respectively. These have decreased from 2019's baseline of 1.12 and 1.32, while attack rates have significantly risen. Manufacturing has experienced a three-year decline in scores, most likely due to changes in the operating environment and the evolution of attacks. On the other hand, finance continued to demonstrate the highest maturity benchmark score for the third consecutive year, of 1.84, a 0.02 decrease on last year, however.

Kazu Yozawa, CEO of NTT's Security division, says: "Last year we predicted a surge in targeted, opportunistic attacks and unfortunately, this has proven all-too-true. While these industries have done their best to maintain essential services throughout disruptive times, the fall in security standards when companies need them most is alarming. As services continue to move online and become increasingly digital to account for the new normal, organizations must be extra vigilant in upholding and maintaining best practices in their security."

Malware sees a metamorphosis: Crypto malware surges while Trojans become more common

While malware is becoming more commoditized in features and functionality, it also became more diverse over the last year with the growth of multi-function malware. Cryptominers have replaced spyware as the most common malware in the world, but the use of certain variants of malware against specific industries continues to evolve. Worms appeared most frequently in the finance and manufacturing sectors. Healthcare was impacted by remote access trojans, while the technology industry was targetted by ransomware. The education sector was hit by cryptominers due to the popularization of mining among students who exploit unprotected infrastructures.

The crypto-currency market is a prime example, with cryptominers accounting for a staggering 41% of all detected malware in 2020. XMRig coinminer was the most common variant, representing nearly 82% of all coinminer activity and nearly 99% in EMEA specifically.

Mark Thomas, who leads NTT's Global Threat Intelligence Center comments: "On one hand you have threat actors taking advantage of a global disaster, and on the other, cybercriminals capitalizing on unprecedented market booms. The common thread throughout both of these situations is unpredictability and risk. Changes in operating models or adoption of new technologies present opportunities for malicious actors and with a surging crypto-currency market popular among inexperienced students; attacks were bound to happen. Now, as we enter a more stable phase of the pandemic, organizations and individuals alike must prioritize cybersecurity hygiene across all industries, including the supply

Related Sectors:

Computing & Telecoms ::

Related Keywords:

Cyber Attack :: Cyber Threat :: Cybersecurity :: Tech For Good :: Data Center :: Ransomware :: Malware :: Intelligent Cybersecurity :: Cryptominer ::

Scan Me:

chain."

Further 2021 GTIR highlights:

- Attacks against manufacturing increased from 7% last year to 22%; healthcare increased from 7% to 17%; and finance is up from 15% to 23%.
- Organizations in multiple industries saw attacks related to the COVID-19 vaccine and associated supply chains.
- COVID-19 cybercriminal opportunism intensified, with groups such as the Ozie Team, Agent Tesla and TA505, along with nation-state actors like Vicious Panda, Mustang Panda and Cozy Bear very active in 2020.
- The most commonly occurring forms of malware in 2020 were Miners: 41%; Trojans: 26%; Worms: 10%, Ransomware 6%.
- Cryptominers dominated activity in Europe, the Middle East and Africa (EMEA) and the Americas but were relatively rare in Asia Pacific (APAC).
- OpenSSL was the most targeted technology in the Americas but was not even on the top 10 list in APAC.
- Ongoing fallout following the Schrems II decision invalidated the EU-US Privacy Shield and placed additional obligations on organizations transferring personal data from the EU to third countries.
- NTT's research shows that 50% of organizations globally are prioritizing securing their cloud services - making it the top cybersecurity focus over the next 18 months.

To learn more about how this year's report offers organizations a robust framework to address today's cyber threat landscape, follow the link to download the NTT Ltd. 2021 GTIR.

ENDS

Regional breakdown

***The Americas*:**

- OpenSSL was the most targeted technology in the Americas but was not even on the top 10 list in APAC.
- Business and professional services was the most attacked industry in the Americas, accounting for 26% of all attacks.
- The US accounted for two of the highest rates of reconnaissance activity of any country analysed:
- Some 64% of all hostile activity targeting the technology industry was some form of reconnaissance.
- In the education industry, 58% of all hostile activity was reconnaissance.
- The Americas observed 8% of all attacks as DoS/DDoS attacks, while these attacks accounted for under 4% in APAC and 1% in EMEA.
- With 34% of all malware detections, XMRig was the most detected malware in the Americas and in the US.

EMEA:

- EMEA experienced 79% of all attacks as combined application-specific (42%) and web-application (37%) attacks.
- At 91% of all such attacks, the UK had the highest rate of combined web attacks of any country analysed.
- Healthcare was the most attacked industry in EMEA.
- The combined attacks from web-application (62%) and application-specific (36%) attacks targeting healthcare in EMEA accounted for 98% of all hostile activity in this sector. This is well above the global average of 67%.
- XMRig accounted for nearly 99% of all miner activity in EMEA and for over 87% of all malware detections.
- Trojans were the second most common form of malware within EMEA.
- In the UK&I, six of the 10 most observed malware were some form of Trojan.

APAC + ANZ:

- Malware varied greatly throughout APAC, but webshells, botnets, and all forms of Trojans combined to account for 72% of all malware. While XMRig was the most commonly detected malware globally, no country in APAC showed XMRig in their top 10 most common malware.

- In APAC, finance (24%) was the most attacked industry, followed by manufacturing (22%).
- In ANZ, finance (42%) accounted for almost half of all attacks, followed by education (24%).
- Healthcare industry maturity severely lacking in APAC and AU at 0.60 and 0.96, below global average of 1.02. Largest gap is APAC with 2.53 to target state.
- Technology sector (2.02) was more mature than the global average (1.64).

About NTT Ltd.

NTT Ltd. is a leading global technology services company. Working with organizations around the world, we achieve business outcomes through intelligent technology solutions. For us, intelligent means data driven, connected, digital and secure. Our global assets and integrated ICT stack capabilities provide unique offerings in cloud-enabling networking, hybrid cloud, data centers, digital transformation, client experience, workplace and cybersecurity. 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 2021 Global Threat Intelligence Report contains global attack data gathered from January 1, 2020 to December 31, 2020. The analysis is based on log, event, attack, incident, and vulnerability data from clients as well as from NTT's global honeypot network. The Report includes data from supported operating organizations including NTT’s Cybersecurity Advisory and WhiteHat Security, along with global primary research.

Company Contact:

NTT Ltd.

E. ntt@hotwireglobal.com
W. https://hello.global.ntt/

Additional Contact(s):
Hotwire for NTT Ltd.
Hannah Lock
hannah.lock@hotwireglobal.com

View Online

Newsroom: Visit our Newsroom for all the latest stories:
https://www.nttltd.pressat.co.uk