NTT LTD. GLOBAL THREAT INTELLIGENCE CENTER

Monthly Threat Report

June 2020

Contents

A quick look at the

2020 NTT Ltd. Global Threat Intelligence Report

Lead Analyst: Jon Heimerl — Sr. Manager,
Threat Intelligence Communication Team

The 2020 NTT Ltd. Global Threat Intelligence Report (GTIR) was published on 19 May 2020. In its eighth edition, it is the culmination of the data the Global Threat Intelligence Center gathered and analyzed throughout the year.

We produce this report by collecting a broad set of global data (log, event, attack, incident and vulnerability) to identify key cybersecurity trends of which businesses need to be aware.

The Report includes global analysis, as well as specific analysis for the Americas, Europe, Middle East and Africa, and Asia Pacific.

This year's GTIR also includes a more detailed look into five industries:

1. Technology
2. Finance
3. Manufacturing
4. Retail
5. Healthcare

Combining data from across all the aforementioned regions and industries created a significant number of statistics about attacks, which can be found in the full Report.

Below are the six key findings we've identified following our data analysis.

1. **Adversaries continue to innovate.** Attack volumes increased and attacks became more complex. Malware has evolved from having specialized purposes to being truly multifunctional. Advancements in automation continue to make attackers more successful.
2. **Old vulnerabilities are still a prime target.** We regularly detect exploit attempts against vulnerabilities over 15 and even 20 years old. Only two of the top 15 most commonly exploited vulnerabilities globally were originally defined since 2017, and none of them since November 2018. Unpatched vulnerabilities continue to be a problem.
3. **IoT Weaponization.** The re-emergence of Mirai and enhanced scanning and propagation techniques in variants like IoTroop has helped widen the spread of IoT attacks.
4. **Technology leads the top attacked industries.** Technology was the most attacked industry in 2019, accounting for 25% of all attacks observed. Significant increases in application-specific and denial-of-service attacks helped push the technology industry up from the number two spot in 2018.
5. **Content management systems are heavily targeted.** Almost 20% of all attacks detected targeted a Content Management System (CMS). These are suites like Joomla!, WordPress, Drupal, and noneCMS, which together account for about a 70% market share. The vulnerability with the single highest volume of exploit attempts in 2019 targeted Joomla!.
6. **GRC continues to become more complex.** The Global Data Protection Regulation (GDPR) led the way, while industries and countries continue to make strides in privacy and security regulations. GRC continues to be a challenge as organizations struggle to integrate their security and compliance initiatives.

For more information on the key findings, or for a detailed regional or industry-view, download the full Global Threat Intelligence Report.

> Our Global Threat Intelligence Report identifies **key cybersecurity trends** of which businesses need to be aware.

Current threat impacts on healthcare providers

Lead Analyst: Vijay Chakravarthy — National Solution Architect, Australia

As discussed in the March, April and May Threat Reports, attackers continue to target both individuals and organizations.

In the healthcare industry, changes in operations due to COVID-19 have forced healthcare organizations to embrace digital transformation to deliver patient services in a timely manner. As the industry embraces this change, they must also be prepared to manage the accompanying risks.

While some attackers (like the DoppelPaymer and Maze ransomware-related groups) have promised not to attack the healthcare industry, a number of attacks have surfaced suggesting the threat landscape for the healthcare industry is far from ideal. This has led to Interpol and the FBI issuing warnings to these vulnerable organizations.

Here are some attack types of which the healthcare industry should be aware.

Attacks on healthcare

Infostealers

Attacks against the World Health Organization (WHO) have more than doubled since the COVID-19 pandemic started. One unsuccessful attack is thought to have been carried out by a group called DarkHotel, who have been active for more than a decade. The attacker impersonated the internal email system used by the WHO to steal passwords of WHO staff members.

Another example was a group of Malspam actors taking advantage of the ongoing COVID-19 pandemic crisis. In this attack, AgentTesla malware variants (active since 2014) were distributed to victim organizations within the healthcare, pharmaceutical, and supporting industries (among others) via phishing emails.

Researchers uncovered a data dump containing 25,000 email credentials allegedly belonging to the National Institutes of Health, the WHO, the Gates Foundation and other organizations.

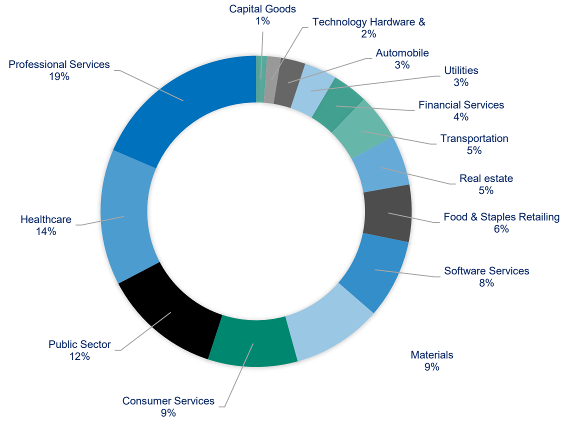
Ransomware attacks

In another case related to the WHO, a group of researchers from Unit42 observed[1] several malicious emails sent (between March 24 to March 26) from the spoofed address noreply@who[.]int (actual sender IP address at the time of the attack was 176.223.133[.]91). The emails were delivered to several individuals associated with a Canadian government health organization actively engaged in COVID-19 response efforts, as well as a Canadian university conducting COVID-19 research. The .RTF attachment was designed to deliver EDA2, an open-source ransomware variant associated with a larger parent ransomware family called HiddenTear.

Similarly, a medical facility which was on standby to help test coronavirus vaccines was hit by a Maze ransomware attack[2]. Attackers stole data from the victim and published it online to help incentivize them to pay the ransom demanded.

One survey showed the healthcare industry was the second most common industry targeted by ransomware in Q1 2020[3].

Common industries targeted by ransomware in Q1 2020



COVEWARE

[1] https://unit42.paloaltonetworks.com/covid19-cyber-threats/
[2] https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html
[3] https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report

Infrastructure attacks

Brute-force attacks targeting the Desktop Protocol (RDP) rose sharply in March and April[4]. COVID-19 isolation rules encouraged organizations to implement remote and distributed working environments, which often forced organizations to deploy more systems accessible through RDP connections. With organizations (healthcare included) facing the need to support more remote workers, the increasing number of systems being brought online has increased risk exposure overall, but in particular for the delivery of critical services and the confidentiality of patient data.

Critical systems

With the healthcare industry relying on IoT devices, botnets such as Mirai and IoTroop contributed to an increase in IoT attack activity and has drawn attention to the need to safeguard critical systems. The 2020 NTT Global Threat Intelligence Report specifically identifies elevated IoT activity as a trend and highlights the IoTroop IoT botnet as the single most commonly observed malware variant throughout 2019.

Additional considerations

Skill shortage

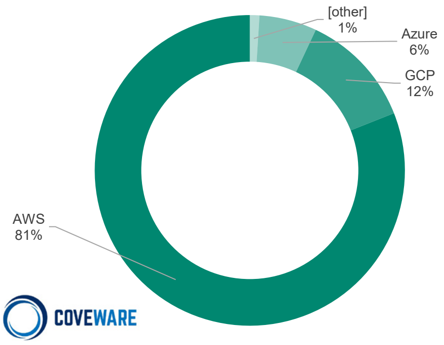
Many industries are grappling with a shortage in cybersecurity skills, and healthcare is no exception. At the same time, healthcare organizations are faced with supporting increased demand of services in a new, more distributed operating environment. These factors help increase the impact of the shortage in healthcare, compromising the ability of organizations to conduct timely response to cyberattacks. As a response, healthcare organizations may look for third parties to support their cybersecurity posture and ability to respond to attacks in a timely fashion (For example: NTT Ltd.'s Digital Forensics and Incident Response service), including the undertaking of cyber-resilience programs.

Attackers are creative – Low effort and high impact

Attackers have made great use of innovation and their ability to maximize their return. Increased use of multi-function malware, multi-vector attacks, and rapid pivots to attack collaboration tools and RDP are a few examples of how threat actors are changing their methods to deploy faster, more agile, larger and stealthier attacks.

Researchers identified a case[5] in which attackers used the corporate Mobile Device Management (MDM) solution as an attack vector to spread infections. There are also indications that attackers are using popular cloud providers (pictured below) to host malicious Newly Observed Hostnames (NOH). Furthermore, the Content Delivery Networks (CDN) in front of the cloud providers make it harder for detections based on malicious destinations.

High-risk or malicious NOHs in public clouds



COVEWARE

In cloud environments, attackers have made use of containers as their attack entry point before moving laterally (such as through unsecured Docker Engine API port) to other resources linked to the cloud account[6]. This is particularly relevant when organizations use containers as part of their standard application development process.

Summary

Attackers have become more sophisticated. Their attacks are modern, pervasive, and adaptive to the conditions we currently face.

As soon as COVID-19 emerged, attackers shifted focus, and in the few months since the pandemic began, healthcare began bearing the brunt of ransomware, application attacks, social engineering, and more.

With operational environments more complex, and health care services in higher demand than ever, the risk to the healthcare industry will be amplified throughout this crisis. It's worth noting the risk isn't just to hospitals - the threat extends to the entire industry and its entire supply chain of supporting organizations, research facilities, suppliers, and vendors. Hence, further attacks on these bodies could have a disruptive effect on the on-going treatment and prevention efforts and a holistic security effort is required.

A full strategy on how to combat these advanced threats for healthcare can be complicated. To start relevant security initiatives, we recommend considering the following safeguard measures:

- Identity protection
  - Use Multi-factor Authentication (MFA) for high-risk transactions, privileged users and self-service functions
  - Leverage SAML, OAuth 2.0, and OpenID Connect for assurance as applications are on-boarded
  - Automate the provisioning/de-provisioning of tasks
- Vigilance around cloud services
  - Audit cloud services periodically
  - Automate cloud services monitoring and management
  - Validate responsibility for system and application security to ensure there is no gap in controls between the business and the cloud service's responsibility
- Secure application development
  - Application security review workflow
  - Application security baseline
  - Bringing Security and DevOps together

For hospitals specifically handling COVID-19 patients and experiencing cyberattacks, NTT Ltd. has been offering security incident response services since April 7th at no charge to institutions in selected countries around the world. For more information, please view our offer overview here.

[4] https://www.zdnet.com/article/kaspersky-rdp-brute-force-attacks-have-gone-up-since-start-of-covid-19/
[5] https://research.checkpoint.com/2020/mobile-as-attack-vector-using-mdm/
[6] https://blog.aquasec.com/threat-alert-cloud-computing-security

#Spotlight

COVID-19 related cyberattacks focus on home users

Lead analyst: Vijay Chakravarthy — National Solution Architect, Australia

With large portions of the workforce working from home, the end user's security posture has become more critical than before. Attacks with varying degrees of sophistication have emerged which threaten this new way of working. Some of these attacks, along with related potential safeguard measures, are discussed below.

Home user attacks

As an example of identity-based attacks, researchers found a malicious website luring users to download an Android application under the guise of a COVID-19 heat map. Other researchers have found a similar example in which attackers used a Trojan hidden in a fake COVID-19 tracking map. The Trojan, related to the AZORult family, exfiltrated a range of credentials, including those for social media accounts and cryptocurrency wallets. Attackers are also taking advantage of the attention paid to COVID-19 to lure victims into opening attachments or clicking on phishing links spread via malicious emails. These attachments and links spread Remote Access Trojans (RATs) like NetWire, NanoCore, LokiBot and others.

We have also seen phishing messages in other communication channels. A prime example is the recent flood of fake SMS messages targeting users, as seen on the right.

An assessment by the Australian Cyber Security Centre (ACSC)[7] regarding the highlighted SMS campaign found the destination website was hosting the Cerberus banking Trojan. This Trojan targets Android devices to steal financial information.

With most remote workers using collaboration and communication tools, weaknesses in these tools have become a target for attackers for credential stuffing attacks. The 2020 Global Threat Intelligence Report found that application-specific and web-application attacks accounted for 55% of all attacks in 2019. Therefore, the risk to the remote worker is compounded by the fact that attackers have already prioritized the theft of logon credentials and attacks on some of these collaboration tools for much of the past year, even before COVID-19 increased risk exposure.

> Attacks with **varying degrees of sophistication have emerged** which threaten this new way of working.

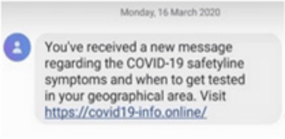
Other indicators

Domain name registrations (with COVID-19 themes) increased during the pandemic period from 9 March 2020 to 26 April 2020 (7 weeks). RiskIQ researchers[8] found over 86,600 (out of 1.2 million) fully qualified domain names, classified as 'high-risk' or 'malicious' (C2, malware, or phishing), spread across various regions. The United States has the highest number of malicious domain names (29,007), followed by Italy (2,877), Germany (2,564), and Russia (2,456). Proofpoint researchers reported that a specific domain – 'covid-19-gov[.]com' – exhibits similar behaviour as previously reported RedLine Stealer activity, which uses a ZIP file to drop Covid-Locator.exe[9].

We have also seen an increase in content-rich coronavirus-related websites including suspicious scripts. An example of such scripts is the 'coronavirus-game[.]ru' IP logger, in which an obfuscated script drops an invisible iframe which in turn sends user's IP addresses to the legitimate IP logging service 'iplogger[.]org'.

Examples of fake SMS messages

Australia

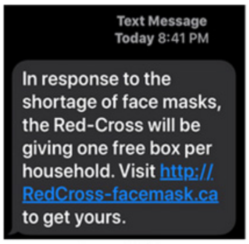


Monday, 16 March 2020

You've received a new message regarding the COVID-19 safetyline symptoms and when to get tested in your geographical area. Visit https://covid19-info.online/

Source: Scamwatch

Canada

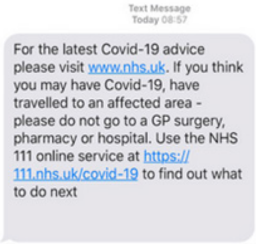


Text Message
Today 8:41 PM

In response to the shortage of face masks, the Red-Cross will be giving one free box per household. Visit http://RedCross-facemask.ca to get yours.

Source: Twitter

UK



Text Message
Today 08:57

For the latest Covid-19 advice please visit www.nhs.uk. If you think you may have Covid-19, have travelled to an affected area - please do not go to a GP surgery, pharmacy or hospital. Use the NHS 111 online service at https://111.nhs.uk/covid-19 to find out what to do next

Source: Twitter

[7] https://www.cyber.gov.au/threats/threat-update-covid-19-malicious-cyber-activity
[8] https://covid-public-domains.s3-us-west-1.amazonaws.com/index.html
[9] https://www.proofpoint.com/us/threat-insight/post/new-redline-stealer-distributed-using-coronavirus-themed-email-campaign

Summary

We can expect threats against home users to continue to evolve but practicing basic security hygiene can help mitigate concerns:

- If you're a user, make sure you understand the security policies and recommendations from your own organization. If you're responsible for security, ensure you communicate (and sometimes overcommunicate) the security guidelines you expect your teams to follow.
- Be cautious with emails and files received from unknown senders, especially if they prompt for a certain action you would not usually do.
- Ensure you are ordering goods from an authentic source. Navigate directly to the retailer's website, instead of searching for them or following links. Beware of 'special' offers.
- Be wary of visiting websites with COVID-19 themes unless they are from a reliable source.
- If your identity has been stolen, guidelines vary based on jurisdiction. Users are encouraged to look for a localized version of the appropriate guidelines, but typical steps are as follows:
  - Report the incident to appropriate authorities for ID theft and law enforcement.
  - Contact credit reporting agencies and banks to freeze accounts and credit applications.
  - Change your login and password information for online accounts.
  - Virus scan all PCs and electronic devices and change any log-on passwords.

> If you're responsible for security, **make sure you communicate your expectations and security guidelines** to your team.

NTT Ltd.'s Global Threat Intelligence Center

The NTT Ltd. Global Threat Intelligence Center (GTIC) protects, informs and educates NTT Group clients through the following activities:

- threat research
- vulnerability research
- intelligence fusion and analytics
- communication to NTT Group clients

The GTIC goes above and beyond the traditional pure research organization, by taking their threat and vulnerability research and combining it with their detective technologies development to produce applied threat intelligence. The GTIC's mission is to protect clients by providing advanced threat research and security intelligence to enable NTT Ltd. to prevent, detect and respond to cyberthreats.

Leveraging intelligence capabilities and resources from around the world, NTT Ltd.'s threat research is focused on gaining understanding and insight into the various threat actors, exploit tools and malware – and the techniques, tactics and procedures (TTP) used by attackers.

Vulnerability research pre-emptively uncovers zero-day vulnerabilities that are likely to become the newest attack vector, while maintaining a deep understanding of published vulnerabilities.

With this knowledge, NTT Ltd.'s security monitoring services can more accurately identify malicious activity that is 'on-target' to NTT Group clients' infrastructure.

Intelligence fusion and analytics is where it all comes together. The GTIC continually monitors the global threat landscape for new and emerging threats using our global internet infrastructure, clouds and data centers along with third-party intelligence feeds; and works to understand, analyse, curate and enrich those threats using advanced analysis techniques and proprietary tools; and publishes and curates them using the Global Threat Intelligence Platform (GTIP) for the benefit of NTT Group clients.

Our **Global Threat Intelligence Center** goes beyond a traditional research-only approach by combining focused research with detective technologies. This results in **true applied threat intelligence** to protect our clients with effective tools and services which reduce security risks and threats.

Recent assets

2020 Global Threat Intelligence Report

The 2020 NTT Ltd. Global Threat Intelligence Report (GTIR) is the culmination of the data the Global Threat Intelligence Center gathered and analyzed throughout the year. We produce this report by collecting a broad set of global data (log, event, attack, incident and vulnerability) to identify key cybersecurity trends of which businesses need to be aware.

Download report

If you haven't already, **register to receive the Monthly Threat Reports** directly to your inbox each month.

NTT