NTT LTD. GLOBAL THREAT INTELLIGENCE CENTER

Monthly Threat Report

May 2020

Contents

COVID-19 Timeline:
Escalation of the disease and cyberattacks

Lead Analyst: Danika Blessman — Sr. Threat Intelligence Analyst,
Global Threat Intelligence Center

As the world enters its fifth month of the COVID-19 pandemic, phishing campaigns and ransomware attacks (amongst others), as well as disinformation operations, continue to affect businesses around the globe.

Criminals continue to capitalize on the fear and uncertainty of the situation for profit, threaten to disrupt and/or to evoke a certain mindset in a given population. While different industries are having different experiences, one thing is well known: attacks have shifted to using COVID-19 as a lure in lieu of other themes – and they've done so with agility and speed.

By looking closer at what has happened to date, we can begin to make inferences about what threat actors might do next, helping businesses to be more prepared for another modified 'wave' of tactics and campaigns from threat actors.

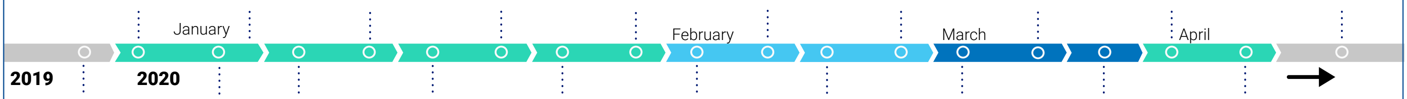
The timeline below gives a glimpse into both the global spread of the virus and the associated cybersecurity risks during the last four months, from the end of December 2019, when the disease first appeared and was reported in China, through the beginning of April 2020.

A brief summary of events:

- On 31 December 2019, cases of pneumonia began to appear in Wuhan and were reported to the World Health Organization's (WHO) office in China.
- In January 2020, almost immediately after China reported its first deaths due to COVID-19, phishing attacks using the disease as a lure began to emerge. At the time, there were so many unknowns about the disease – which wasn't even named during this timeframe – and attackers used these unknowns to prey on the curious. Attacks were not initially aimed at any particular group but sent out *en masse*.
- In February, the WHO issued warnings as phishing campaigns became more targeted. Attackers identified and focused on vulnerable users and organizations in specific geographic regions and/or affected industries.
- Towards the ends of February, new tactics began to emerge. Criminals began to register COVID-19-related domains – at one point up to 2000 a day – to use as malware hosting sites. Malware was even hosted on what appeared to trusted sites, as attackers mimicked the widely used Johns Hopkins Coronavirus tracking map.
- In March, as those potentially targeted changed basic day to day operations like working remotely, as business and individuals became financially strained, and people searched out constantly changing information on COVID-19, attacks becoming more diversified. Attackers increasingly used ransomware and information stealers like Trickbot in phishing campaigns. Another infostealer, Oski, was observed in attacks to hijack DNS settings in various routers.
- By the end of March, much larger numbers of people were working remotely, many schools moved online and telehealth was on the rise. This significantly increased the overall attack surface and the number of vulnerabilities available for exploitation. Cybercriminals targeted unsecured home networks, VPNs and communication applications (often non-corporate applications).
- Throughout April, COVID-19 continued to spread around the world, even as some countries began to feel like they were getting things back under control. Meanwhile, April saw continued targeted cyberattacks, including the use of the CLOP ransomware targeting hospitals and pharmaceutical firms, along with a surge in activity from the Maze ransomware. Phishing campaigns continued, targeting medical research facilities and critical infrastructure.

COVID-19 presents opportunities for exploitation at all levels.

COVID-19 Cybersecurity threat and attack timeline



31 Dec 2019: Chinese authorities inform WHO's China office of pneumonia cases in Wuhan City, Hubei Province.

7 Jan 2020: China identifies new coronavirus as cause of the outbreak.

Early to mid-Jan: First observations of COVID-19 related phishing emails observed.

9 Jan 2020: China reports first death linked to COVID-19.

Mid-Jan: Suspected Chinese nation state actors conduct attacks against multiple industries, as Wuhan sees its first wave of infections.

Phishing campaigns leveraging COVID-19 intensify. Tactics become more sophisticated.

20 Jan 2020: The CDC confirms that a US patient tested positive for COVID-19.

Domain registrations using COVID-19 themed domain names peak at close to 2,000 per day.

30 Jan 2029: WHO Director-General declares the COVID-19 outbreak a public health emergency of international concern.

Phishing campaigns increase, become more targeted.

WHO issues public warning about phishing scams.

11 Feb 2020: WHO assigns the novel coronavirus its official name: COVID-19.

The John Hopkins COVID-19 map is leveraged to distribute malware.

Threat actors employ ransomware under the guise of security software.

11 Mar 2020: WHO Director-General Tedros Adhanom Ghebreyesus declares the global COVID-19 outbreak a pandemic.

Information stealers like Trickbot are being leveraged in phishing and campaigns.

Attackers leverage Oski information-stealing malware to hijack a router's DNS settings.

2 Apr 2020: Global infections pass the one million mark.

Cybercriminals target remote communications applications like Zoom.

Zeus Sphinx Trojan reemerges after three years, with several instances beginning in Dec 2019, continually intensifying through April 2020.

Figure 1: Timeline of COVID-19 related threats and attacks

Which brings us to today

By the end of April, the official count of COVID-19 cases worldwide has passed 3 million, and researchers have observed a 30,000% increase in COVID-19 theme attacks since January. It does not seem like there will be any reduction in attacks for the time being and that the default attack will leverage the COVID-19 theme in some way.

Many industries like manufacturing, technology and communications, retail, and finance, are experiencing added stress on their organizations. Day-to-day operations have been affected by supply chain inadequacies, and there's been a surge in remote working which, some industries are more familiar with than other. Some are forced to, hopefully only temporarily, close their doors.

The healthcare industry in particular is in a fragile state. Resources are already stretched to the limit but unfortunately, Interpol has also issued a warning that healthcare organizations are experiencing an increase in incidents related to ransomware and other malware. Most experts expect such attacks to continue and potentially escalate even further.

It would appear that all industries which play supporting roles, such as those in various supply chains, the food and hospitality industry, law enforcement, medical – anyone critical to keeping society moving – are vulnerable and being targeted. Attackers have identified and concentrated their efforts on these industries, where there is the most at stake and where there is the most desperation. A hospital experiencing a successful ransomware attack in the middle of this health crisis may be more likely to consider paying the ransom, for instance, with hopes of returning to business as usual, faster. These are also often industries which are in danger of overlooking security risks, while they look to keep operations afloat.

What to watch for

We certainly won't be seeing a decrease in criminal activity soon.

COVID-19, particularly from a geopolitical standpoint, is a primary driver for nation-state and cybercriminal operations. Expect to continue to see everything from low-level criminal attacks and phishing campaigns to potential attacks by nation-state actors to gain intellectual property or conduct perception management campaigns.

Attacks could also target countries first exiting massive COVID-19 outbreaks lockdowns and societal restrictions as they'll be at an economic advantage as their economies come back online – and are also more vulnerable during yet another shift in how day to day activities are conducted. On the other hand, during an economic downturn, attacks may increase and be more successful as people become more desperate.

We may even see a shift in the actual infrastructure of communications networks. There's been an incredible increase in internet and telecommunications usage during this crisis. The overload on telecommunications providers may prompt a significant overhaul. This potentially introduces additional vulnerabilities with new systems and evolving architectures, providing further attack vectors, starting with increasing levels of attacks.

> **Good, basic security practices** have rarely been as important as they are right now.

Staying safe and secure

Given the predicament we find ourselves in, there are a few things organizations can keep in mind to keep itself safer from COVID-19 related cyberattacks:

- One of the most important steps an organization can take is to set security priorities based on their own business needs and risk tolerance. Secure those critical items, then, ignore the noise.
- Users are being inundated by phishing attacks and news from fake sites. Neither the CDC nor the WHO are going to send emails directly to people advising them of COVID-19 updates. Businesses should visit official websites and trusted providers to get official information to avoid subjecting themselves to increased threats or disinformation.
- Apply security best practices. COVID-19, and whatever comes in the post-crisis world, will present opportunities for attacks and exploitation at all levels: nation-state, organizational, and the individual user. Basic security practices have rarely been as important as they are right now and can prevent businesses from being an easy target.
- And lastly, work with trusted third parties. For those businesses in needs of help with their business continuity plans, NTT Ltd. is offering:
  - Complementary **Workplace Exploration Workshop** to assist qualifying enterprises in securing the remote work environment. Read more **here**.
  - Emergency cybersecurity incident response and remediation services at no cost to help frontline hospitals. Read more **here**.

COVID-19, and whatever comes in the post-crisis world, will present opportunities for attacks and exploitation at all levels: nation-state, organizational, and the individual user. As it all unfolds, we just have to stay healthy, adjust to change and continue to use good practices, because good, basic security practices have rarely been as important as they are right now.

5 things remote users need to know

Lead analyst: Jon-Louis Heimerl — Sr. Manager,
Global Threat Intelligence Center

The April Monthly Threat Report discussed things organizations should consider to support remote users adapting to a secure environment. Users, especially ones who are new to remote working, cannot be placed in a position where they are responsible for their own security. Organizations must take time and care to help ensure that their staff can be successful.

At the same time, it is unlikely the organization can control every single thing the user does, especially when remote working is new to both the organization and the user. To maximize the effectiveness of a remote working situation, both the organization and the user must work together. To that end, here are five important recommendations for the user to consider when working from home or in another telecommuting environment.

> **Attackers** know that people new to working from home may be out of their comfort zones, and **use a wide variety of attacks to target remote workers** with the intent to steal information or take over their systems.

Understand and use what the organization gives you

The organization has made some decisions about how much help to give you. If they provided a laptop, use that one, not your home system. Use access to file shares given to you; do not adapt some public file-sharing tool. Use the collaboration tools, like presentation tools and meeting applications, supported by the organization, not some other app you just happen to like. And if you don't understand what tools you have or how to use them, tell the organization that. The organization wants and needs you to succeed, and they may not realize they have not properly equipped you with the necessary tools and training.

Be aware of your surroundings

During World War 2, the government in the United States of America started using the slogan 'loose lips sink ships'. The concept was that someone could accidentally reveal sensitive information by saying the wrong thing in the wrong place. The same principle applies in your work-at-home setting. If you work alone, this is not a big deal. But if you share workspace with a roommate, it's another matter. If you have private organizational information on your laptop screen, or are having a conversation about sensitive information, you should be taking action to protect that information from any third party. Discussions about trade secrets, financial details, or personal healthcare information are meant to be shared, on screen or over the phone, with only authorized people. Position your laptop appropriately and lock the screen when you step away. If you have a sensitive phone conversation, figure out a way to have that conversation in a private environment.

> **Lock your laptop screen** when you step away.

Save your data

The saying 'no man is an island' has been around for a long time. You probably have organizational information on your laptop. You likely spend your time producing valuable work content for your organization. What happens if your laptop is damaged? It doesn't take much of a fall to break a laptop if it lands wrong. It only takes a couple ounces of well-placed coffee or water to ruin a laptop. What happens to the work product stored on your computer if that computer is destroyed, or stolen? Find out if your laptop is doing automatic backups to an organizational server. If it is not, take action to find a logical repository on an organizationally-approved internal system to store the things you are working on in the event your computer is no longer available. Hopefully you have some kind of organizationally-approved file-share or your incremental work is already stored through some organizational application, but worst case, email your work product to your work email account. That way there will always be a copy in your corporate email inbox.

Know your key policies, especially how to ask for help and how to report an incident

In a perfect world, everyone knows all organizational policies and procedures by heart. But if working remote is a new situation, you may not know all the rules which apply to you. Find (or ask for) the security policies which are the most pertinent to your work. For instance, data handling guidelines which would provide direction for what you can share with whom. If you do nothing else, make sure you understand how to ask for help, if that means opening a trouble ticket because something is broken, or you just don't know how to use that conferencing software you never had to use before because you worked in the office. And, make sure you know exactly how to report a security incident. The COVID-19 crisis has created a huge population of remote workers who have never been in this situation before. Attackers know this and are focusing on these new remote workers more than ever before.

Remember that you are, unfortunately, under attack

Attackers know that people new to working from home may be out of their comfort zones. As a result, they are attacking remote workers with a wide variety of attacks designed to steal information or take over their systems. A perfect list of how to minimize your risk would go on for pages, but ultimately, the best guidance is to be a little paranoid. Be ready for fraudsters to call to try to talk you into revealing information. Assume most unsolicited email you receive about COVID-19 is fake – the CDC is not emailing you an update. Don't click any links in anything from users you do not know. If you get an unexpected attachment in an email from a coworker don't be afraid to reach out and ask them if they sent you a document.

If you are using your own computer to access work, these recommendations still mostly apply, but that is a more complicated situation. Ultimately, you can maximize the effectiveness of your own security by making sure you get the support you need from your organization – and by exercising just a little paranoia.

Recap:

1. Understand and use what the organization gives you.
2. Be aware of your surroundings.
3. Save your data.
4. Know your key policies, especially how to ask for help and how to report an incident.
5. Remember that you are, unfortunately, under attack.

Know your key policies, especially **how to ask for help** and **how to report an incident.**

Cybersecurity risk evolves fast amid changing workplace dynamics

Lead analyst: Richard Thurston — Market Insights Manager, Strategy & Alliances

The absence of technology risk from the Top Five global risks published by the World Economic Forum (WEF) earlier this year is a misleading headline.

For the first time since 2016, and from research undertaken prior to the pandemic, neither of WEF's two leading technology risks – large-scale cyberattacks and 'massive incidents of data fraud or theft'– were considered by its global research of private and public sector organizations and influencers to be in the top 5 most likely risks – replaced entirely by environmental factors (they remain in the top 10 at #7 and #6 respectively).

The surge in concern about climate change was unmistakeable, but what is happening with technology risk is more nuanced, and these issues are changing fast as organizational dynamics fundamentally alter.

Analysing the data, WEF's work shows that the perceived impact of technology risk is far from diminished: over the last three years, this has remained static for cyberattacks (while they have become more sophisticated) and increased slightly for data fraud/theft. Indeed, there was already a heightened sense of concern about infrastructure susceptibility before the pandemic.

The concerning aspect is a sense of user complacency around technology risk that appears to be partly a result of the familiarity of always-available technology systems. There is some evidence that technology risk is struggling for mindshare – given all that is going on in the world – among younger generations who have grown up accustomed to a ubiquitous always-on, increasingly high performing internet.

The false sense of always-on and always-secure was highlighted in stark fashion by qualitative research of under 30s that NTT Ltd. carried out last year in London. As an example, one of the research respondents – an educated 28 year-old working in the finance industry – said on the subject of data privacy: 'I don't think I care anymore … I accept that at some point someone might try to defraud me and impersonate me and I will deal with it when it happens, I suppose.'

Our research showed that the younger generation was easily able to articulate knowledge about the existence of cybersecurity issues (and were more concerned than older demographics about a lack of cybersecurity skills in their organization - 46% of under 30s said that they thought their organizations lacked adequate resources/skills to address cybersecurity threats), but sometimes distanced themselves from responsibility and action.

Most organizations expect cybersecurity to become more challenging over the coming months. According to WEF, the ratio of those who expect the risk from cyberattacks to increase versus those who do not is 76:24, according to WEF. For data fraud/theft the balance was similar, at 75:25.

The situation has evolved rapidly since WEF published its work, as we discussed in our April Monthly Threat Report.

Many cybercriminals have unfortunately been quick to use the pandemic as a platform for exploitation, often through the use of industry and country-specific phishing attacks and a range of new malware campaigns. This can create additional risk for organizations as their employees work remotely – in some cases outside of the VPN or using personal devices - or with the distraction of switching between work and personal tasks.

Other heightened areas of concern brought about by the increase in home working include policy, patching, helpdesk support, user education and awareness, potentially any smart speakers that are turned on, and the security of the connection itself.

With around 2,000 coronavirus-themed websites being created every day (of which many contain disinformation and/or are designed with malicious intent), the threat landscape has rapidly complexified to exploit a pandemic that is already top-of-mind.

While headlines have shifted, the pace of change of technology risks is evolving faster. It is timely that WEF has expanded its Global Risks Initiative to understand and help mitigate the complex web of environmental, technological, economic, geopolitical and societal risks. Behind the news headlines lie interrelated, conflicting and often unexpected changes. An agile focus on mitigating cybersecurity risks is crucial and its interrelationship with driving positive business outcomes must be renewed.

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

2019 Global Threat Intelligence Report

This year's report focuses on several security challenges we have observed in organizations over the past year. Our analysis shows an escalation in coin mining, web-based attacks, and credential theft, along with changes in the sectors most targeted.

Download report

NTT