NTT LTD. GLOBAL THREAT INTELLIGENCE CENTER

Monthly Threat Report

Special edition: April 2020

Contents

Protecting the Remote Worker

Lead Analyst: Jon Heimerl — CISSP, Sr. Manager,
Global Threat Intelligence Center

Telecommuting. Virtual workplace. Teleworking. Working remotely. E-working.

Regardless of what we call it, the purpose is to enable employees to function effectively from remote locations. In the current climate of the coronavirus pandemic, many organizations have already implemented a remote workforce, and it is something others are considering for business continuity planning.

To start the process of shifting to a remote workforce, the organization must establish whether the role in question can be performed from outside a traditional work environment. It's worth noting that the current crisis has proven that many roles can in fact be performed remotely when it was previously thought they could not. Even if not the preference of the organization, it's becoming a critical consideration of business resiliency.

That said, there are a wide variety of issues to consider, including whether the employee has an internet connection capable of supporting access and how to manage, engage and properly enable employees who haven't previously worked from home. Efficiency concerns include the effectiveness of the employee's workspace.

To that end, the following list includes security-relevant issues an organization should consider when establishing and maintaining a virtual workplace. Some of these items should be obvious, and some are things organizations have struggled with as they attempt to migrate to a more virtual environment.

Does the employee have a remote workstation provided by the organization?

If the organization has already provided the employee with a laptop they can take home, this is significantly easier. But, if the employee normally works on a desktop system in the office, this is more difficult. It may be necessary for organizations to procure laptops or other portable systems (and supporting equipment like printers).

Allowing employees to work remotely from employee-owned equipment does not typically meet minimally acceptable security practices.

> Simply put: can an organization trust that an **employee's home computer, personal devices and Wi-Fi network are secure?**

Organizations must be aware that allowing users to use personal devices for work purposes does expose the business to potentially unmanaged risk.

Does the organization support the remote workstation?

If the organization does provide a remote workstation, helping to make sure it remains secure presents another challenge.

It's important to have answers to whether the organization provides all necessary updates or patches for the operating system and any applications or tools, or does it rely on the user to do so? Does the organization have a remote access capability with which they can readily provide remote support? Without remote access, there is little the organization can do to make sure users are performing proper patches and updates. If the organization wants to make sure that organizational systems remain in a controlled, known state, the organization needs to provide remote support for all users.

This also includes the installation and management of appropriate security software like anti-malware or endpoint security solutions. Good security practice calls for security software to be managed by the organization in a planned and defined manner which is designed to meet the organization's common security goals.

In general, organizational risk increases with the number of users who have administrative accounts – even if that access is for an individual workstation.

A significant number of vulnerabilities result in allowing the attacker 'remote access at the privilege level of the currently logged in user' after successful exploitation. Ultimately, if the organization can actively support remote workstations, there is little need for the end-user to operate with an administrative account.

Is the organization prepared for additional 'help-desk' support?

If you take a group of people who are used to working in an office setting, then put them in a foreign setting with a new operating environment, even if in the comfort of their own home, there is a good probability that there will be an increased need for IT support. Users are likely to need help using remote access capabilities like a new VPN, navigating a shared file system, or performing other remote functions that they had not had to do previously.

Additionally, migrating a new class of workers to the home environment is likely to increase break/fix demands. Systems which are more mobile are more likely to be dropped, have coffee or other liquids spilled on them, or in some other way be damaged to the point they need to be replaced. This will increase demand on processes and resources for ordering, provisioning, and delivering replacement systems.

Are remote systems encrypted?

Systems sitting in an organizational environment – in an owned or leased building – are generally more secure than mobile systems. The more mobile a device is, the more likely it is to be stolen or lost. Loss of an unencrypted device is much more likely to result in the compromise of sensitive information than the loss of an encrypted device.

A quick look at the healthcare breaches posted on ocportal.hhs.gov reveals that about 10% of reported health care breaches in the United States were related to the loss or theft of laptops or portable devices. That included about 43 breaches which resulted in the compromise of nearly 900,000 records. Reviewing the entire privacyrights.org database shows that number to be at least 15% of all reported breaches (some are classified poorly) – that's a total of more than 185,000,000 records compromised due to laptops or portable devices reported stolen or lost.

If the data on those systems was properly encrypted with industry leading technology, most, if not all, of those records would still be safe, even after the loss or theft of the hardware. Encrypting the laptop protects the organization and the user, as well as any third-party whose data is on that system.

Are remote systems connected via VPN?

Workers will connect to organizational systems via the internet. That means via a wired or wireless connection within their residence, to the router for their internet provider, then across the internet to a designated organizational system. By default, that connection is not encrypted – and not protected from eavesdropping or interception.

Conducting all electronic communications through a VPN is standard business practice. The VPN helps protect all communications as well as the end point systems, enabling employees to communicate effectively in a secure manner.

Are USB and other drives disabled?

The importance of this issue may vary greatly depending on the industry of the organization; some organizations should consider disabling the ability to write to USB drives and optical disks. Organizations with highly sensitive data, such as those in the financial or health care industries, will want to minimize the chances that users can make organizational data more 'mobile'. Any data on portable media such as a USB token also exposes the organization to potential compromise if that portable media is lost or stolen.

> Employees need to know **when and how to protect private discussions** from unauthorized eavesdropping.

Do users have the private space required to do business?

If your users are required to have private conversations about sensitive information, are they able to conduct those conversations from their residences in a private location where they cannot be easily overheard by unauthorized people? Exposing private conversations could violate non-disclosure agreements, and violate a variety of compliance regulations, including requirements to keep health care or financial information private. This may not be difficult in many home situations, but imagine an environment in which three roommates share a three bedroom apartment, and all three are working at home – employees need to know when and how to protect any private discussions from unauthorized eavesdropping, and organizations need to appreciate that this may not be easy for all employees.

Beyond that, the potential loss of control in an 'at home' situation (or perhaps, 'increase in chaos due to interruptions from children, pets, significant others, roommates, or just the new situation') can help decrease the amount of care and deliberation with which workers are able to conduct their jobs. Some of this should be expected in moments of crisis like with the coronavirus, but this potential reduction in focus can also increase the chances that an employee could have a lapse in judgement about how they protect organizational systems and data. Previous analysis of global breach data suggests that accidents or mistakes were contributing factors in as many as a third of all breaches. More than anything else, this is a call for both the employee and the organization to be more vigilant about minimizing the impact of any potential 'oops'.

Did you advise users to disable their smart devices?

Smart devices like Google Home and Amazon Echo have widespread popularity. The devices are constantly listening for users to ask them for help. There have been reports that some of these devices have captured conversations and sent them to Google or Amazon for analysis, allegedly to verify the accuracy of their voice recognition. Some smart TVs have a similar interface, as do electronic devices which listen for voice activation.

While people can argue about their risk-tolerance and whether or not this listening for and potential gathering of voice data is a violation of privacy, organizations should consider the types of conversations their home employees are likely to have, and what the potential is for exposure of sensitive information. If employees are likely to discuss highly sensitive information, it is worth considering a ban on work-related conversations within range of such smart devices, whether than means disabling the device or moving them (or the user) to another room.

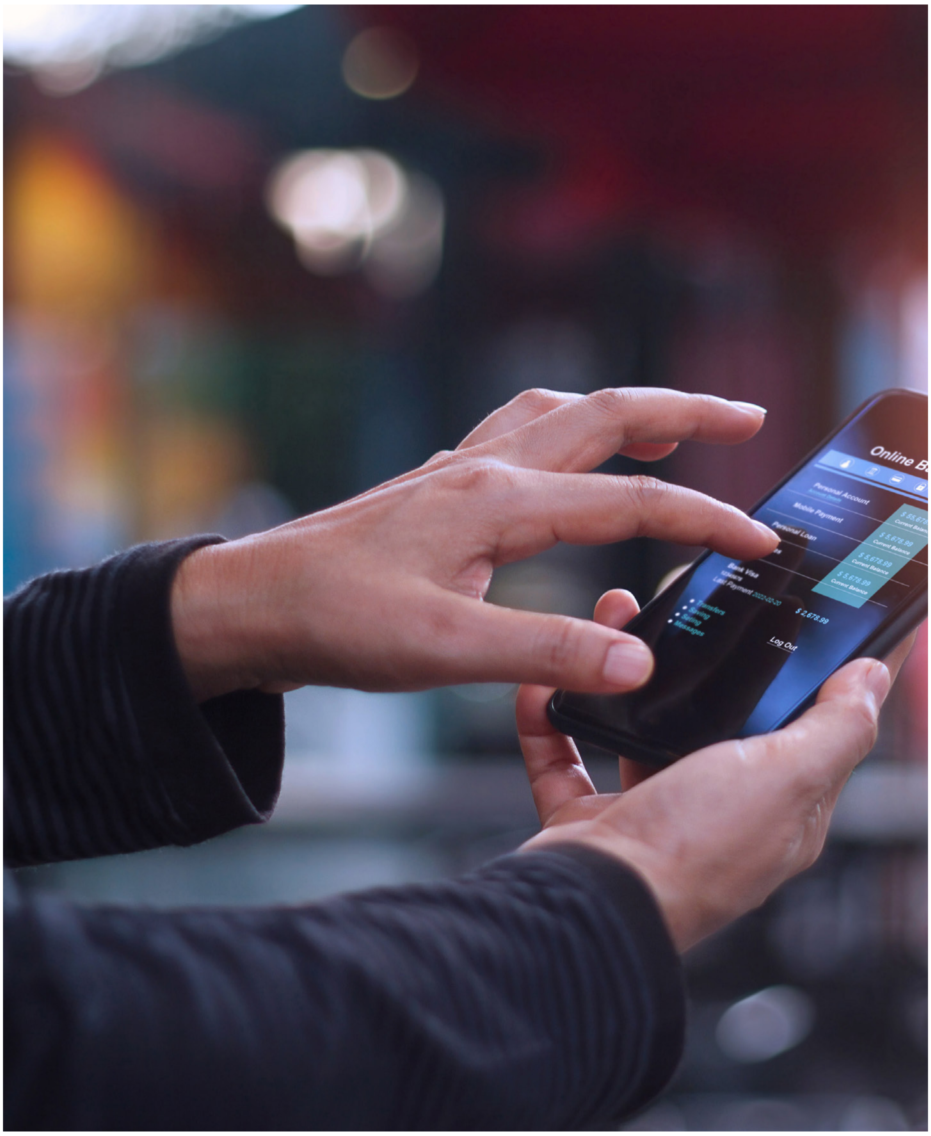
Did you remind remote users of security policies and their responsibility to protect organizational information?

Especially for workers who may be new to the situation, working from home can make users more relaxed about their work habits. Even in the office, it can be difficult to control and monitor work habits. As workers move to a more autonomous setting, it is good practice to provide a refresher on organizational security policies and practice, especially as they relate to management of organizational information. This would include proper classification, marking, and handling, as well as guidance on good security hygiene and internet habits. It should also include reminders not to allow non-employees access to organizational information or systems. Along with everything else, make sure users know how to report outages, system problems, and security issues or incidents.

Conclusion

In the end, compliance with controls for end-users in a distributed telecommuting environment does not need to be vastly more complex than working within a normal organizational environment. This list includes some of the issues an organization should consider when establishing and maintaining a virtual workplace, but it is not exhaustive. The actual implementation and management require some planning, as well as coordination and communications with the end-user. If organizational and employee objects are made clear, everything else can follow.

> Organizations should consider the types of conversations their home employees are likely to have, and **what the potential is for exposure of sensitive information.**



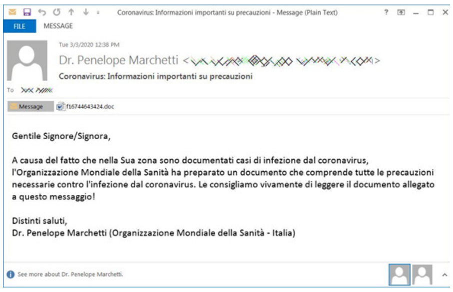
Threat Actors continuing to leverage COVID-19

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

As NTT Ltd. analysts described in the March 2020 GTIC Threat Report, there have been a multitude of phishing campaigns, leveraging a slew of newly-registered (likely illegitimate) domains to host malware or information stealers – using the subject of COVID-19 as a lure.

This month, we continued to see an increase in phishing campaigns which are currently the most observed threat employing the COVID-19 theme. Although we're seeing similar tactics to those we reported last month, it appears that the tactics and strategies of threat actors are becoming more sophisticated and more focused on aspects such as industry, geography (including country-specific phishing lures as the virus becomes more prevalent in that country), as well as considering the shopping and deliveries of the potential victim.

An extensive number of threat actors are leveraging techniques from phishing campaigns to malware infrastructures like Trickbot and Lokibot to deliver malware globally.



Coronavirus: Informazioni importanti su precauzioni - Message (Plain Text)

Tue 3/3/2020 12:38 PM

Dr. Penelope Marchetti <[redacted]>

Coronavirus: Informazioni importanti su precauzioni

To [redacted]

f16744643424.doc

Gentile Signore/Signora,

A causa del fatto che nella Sua zona sono documentati casi di infezione dal coronavirus, l'Organizzazione Mondiale della Sanità ha preparato un documento che comprende tutte le precauzioni necessarie contro l'infezione dal coronavirus. Le consigliamo vivamente di leggere il documento allegato a questo messaggio!

Distinti saluti,
Dr. Penelope Marchetti (Organizzazione Mondiale della Sanità - Italia)

Figure 1: Sample spam campaign

New spam campaigns

One new spam campaign using the COVID-19 theme has been discovered targeting Italians with Trickbot information-stealing malware.These emails have a subject of 'Coronavirus: Informazioni importanti su precauzioni' and contain a malicious Microsoft Word document. This email is meant to appear as information regarding necessary protective measures people in Italy should implement against the coronavirus. Research suggests that, when opened, the malicious Word document prompts the victim to click on the 'Enable Content' button to properly view the message.

Once a recipient clicks on 'Enable Content', malicious macros will be executed which extracts various files to install and launch the Trickbot malware. If successfully installed, Trickbot gleans information from the compromised system and attempts to move laterally through the connected network to gather more information. Any information acquired is then sent back to the attackers.

An example of this email is shown in Figure 1:

New malware campaigns

Threat actors are also employing ransomware under the guise of security software. One new ransomware, called CoronaVirus, is being distributed via a site claiming to encourage the use of system optimization software from WiseCleaner. The active downloads on this site are distributing a file called WSHSetup.exe, acting as a downloader not only for the CoronaVirus ransomware, but for a password-stealing Trojan called Kpot as well.

If Kpot is successfully executed, it attempts to steal login credentials and cookies from internet browsers, VPNs, email accounts, messaging programs, cryptocurrency wallets and other services.

Another tactic recently observed is leveraging Oski information-stealing malware to hijack a router's DNS settings. In this attack, internet browsers display alerts for a fake COVID-19 information app from the World Health Organization (WHO). Some users have reported browser windows opening on their own, subsequently displaying a message prompting them to download the 'COVID-19 Inform App,' allegedly from the WHO.

Additional research showed that these alerts were being caused by attackers changing the DNS settings on home D-Link or Linksys routers to use DNS servers operated by the attackers. It is unknown at this time as to how attackers are gaining initial access to these routers in order to change the DNS configuration, but it is thought that the router was likely enabled for remote access with a weak or default admin password.

Another campaign is using an open redirect (a web addresses which automatically redirects users between a source website and a target site) for the HHS.gov website. This redirect is being leveraged by attackers to push malware onto targeted systems, again, using coronavirus-themed phishing emails.

This campaign is using a malware called Raccoon which is yet another information-stealing malware. The Racoon malware, discovered about a year ago in cybercriminal forums, is capable of infiltrating about 60 different applications, including browsers, cryptocurrency wallets, email and FTP clients, to steal credentials and other data, then delivering this sensitive information to the attackers.

The open redirect, discovered and shared on Twitter by infosec analyst @SecSome (https[:]//dcis.hhs.gov/cas/login?service=MALICIOUSURL &gateway=true) is present on the subdomain of the HHS Departmental Contracts Information System. A sample phishing email is shown in Figure 2 below.

Nation-state actors

This month also saw reporting indicating that suspected nation-state actors are taking advantage of the crisis. This doesn't mean they haven't been active – likely quite the opposite. Researchers have observed that APT41, an advanced persistent threat group has ramped up its activities since February. Targeted organizations come from multiple industries, including healthcare, telecommunications, government/ defense and finance, and are in countries like Japan, India, the U.S., France, Australia and Canada. While only a handful of attacks have been successful, this campaign was APT41's most widely-cast in recent years.

Many of the attacks attempted to exploit a previously known remote code execution (RCE) vulnerability (CVE-2019-19781) in Citrix Application Delivery Controller (ADC) and Citrix Gateway devices.

And, while the impetus for these attacks remains unknown, Chinese APTs have historically sought a broad range of knowledge and sensitive information from a wide range of targets, sometimes provoked by – or leveraging – significant geopolitical or global events.

Phishing attacks continue to be the most-widely employed tactic across the board

Cybercriminals continue to use the branding of trusted organizations in these campaigns, especially the World Health Organization (WHO) and U.S. Centers for Disease Control and Prevention (CDC), in order to build credibility and get users to open attachments or click on the link.

This month saw a hack attempt on the WHO, which will likely elicit further phishing/domain hijacking.

With the announcement of the U.S. Federal Government's (U.S.G.) stimulus package, it is also not unreasonable to expect to see cybercriminals soliciting information about the stimulus checks coming from the U.S.G., asking users to 'click here' and provide personal information in order to deposit your check.

Fake checks are arriving in the mail already as well (see Figure 3).

Government-issued checks are not set to be issued until the second week of April and will be issued by an individual's (or organization's) tax filing method, typically direct deposit or a mailed check.

As with any disaster, attempted phishing campaigns include requests for donations to help those in need. Users should be cautious when donating; as always, go directly to a known legitimate website rather than clicking on links in emails soliciting donations. Phishing emails have commonly offered selling in-demand items like face masks and hand sanitizer, as well as COVID-19 tests.

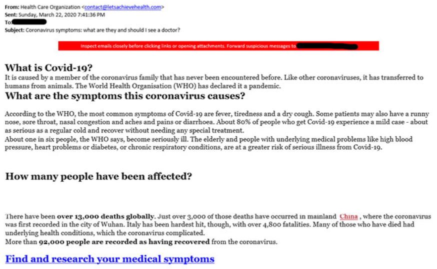
Conclusion

COVID-19 will continue to be used as a lure – especially since around 2,000 coronavirus-themed websites are created every day – and likely will be for the duration of the pandemic. In addition, new versions of these lures, targeting new countries will emerge – even as the world goes into recovery mode – using subjects such as 'COVID Cure' or 'COVID Resurgence'.

COVID-19 has generated a sprawling web of cybersecurity risks. But this story, of course, is not just a news story that criminals are using as fodder for phishing emails. The world is reaching into unknown territory – like new telecommuters, financial market uncertainty, not knowing exactly how to react to new social and physical restrictions… these are all things that most have never had to think about, let alone adjust to, in organizational environments.

And, as the number of COVID-19 cases and publicity rises globally, we expect to see that both cybercriminals and possible nation-state actors will increasingly exploit this global crisis.

Continue to use common sense and implement best practices in all aspects of your network – and day-to-day – environment.



From: Health Care Organization <contact@letsachievehealth.com>
Sent: Sunday, March 22, 2020 7:41:36 PM
To: [redacted]
Subject: Coronavirus symptoms: what are they and should I see a doctor?

Inspect emails closely before clicking links or opening attachments. Forward suspicious messages to [redacted]

What is Covid-19?
It is caused by a member of the coronavirus family that has never been encountered before. Like other coronaviruses, it has transferred to humans from animals. The World Health Organisation (WHO) has declared it a pandemic.
What are the symptoms this coronavirus causes?

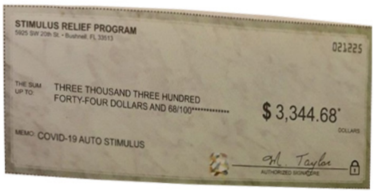
According to the WHO, the most common symptoms of Covid-19 are fever, tiredness and a dry cough. Some patients may also have a runny nose, sore throat, nasal congestion and aches and pains or diarrhoea. About 80% of people who get Covid-19 experience a mild case - about as serious as a regular cold and recover without needing any special treatment.
About one in six people, the WHO says, become seriously ill. The elderly and people with underlying medical problems like high blood pressure, heart problems or diabetes, or chronic respiratory conditions, are at a greater risk of serious illness from Covid-19.

How many people have been affected?

There have been **over 13,000 deaths globally**. Just over 3,000 of those deaths have occurred in mainland China , where the coronavirus was first recorded in the city of Wuhan. Italy has been hardest hit, though, with over 4,800 fatalities. Many of those who have died had underlying health conditions, which the coronavirus complicated.
More than **92,000 people are recorded as having recovered** from the coronavirus.

Find and research your medical symptoms

Figure 2: Sample phishing email



STIMULUS RELIEF PROGRAM
5925 SW 20th St. • Bushnell, FL 33513

021225

THE SUM UP TO: THREE THOUSAND THREE HUNDRED FORTY-FOUR DOLLARS AND 68/100************** $ 3,344.68* DOLLARS

MEMO: COVID-19 AUTO STIMULUS

M. Taylor
AUTHORIZED SIGNATURE

Figure 3: Sample fake check

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.

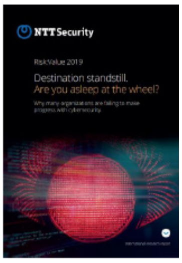
Our **Global Threat Intelligence Center** goes beyond a traditional research-only approach by combining focused research with detective technologies. This results in **true applied threat intelligence** to protect our clients with effective tools and services which reduce security risks and threats.

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



Risk:Value 2019

In 2019, 33% of organizations around the world would consider paying a ransom to a hacker rather than investing more in cybersecurity, because paying the ransom is cheaper. Read more about this and other trends in the 2019 Risk:Value report.

Download report

NTT