THALES

REMOTE WORKING IN TIMES OF CRISIS

CYBER THREAT ASSESSMENT

04/03/2020

Version – 01

CYBER THREAT INTELLIGENCE ASSESSMENT

REMOTE WORKING IN TIMES OF CRISIS

A STRONG AMPLIFYING FACTOR

SUMMARY

The modus operandi based on the COVID-19 or Coronavirus theme now dominates the cyberthreat ecosystem. This theme is used not only in the subject or body of malicious messages but also in attachments, URLs and decoys.

In this exceptional situation, the sudden change in the lifestyle of most of the employees in confinement has led to the introduction of telework on a very large scale.

According to a study by the Deskeo company, the proportion of the French population subject to the telework regime is now 70%, or nearly 20.8 million people. This trend seems to be similar to other tertiarized countries.

The global situation of containment is therefore at stake to introduce indirectly, through its exceptional nature in all fields of daily life, great feverishness into the cybersecurity world. Telework had never been envisaged in such a volume by most companies and institutions, which today poses a real security problem.

The increase in the number of threats related to COVID-19 and vulnerabilities related to the telework situation has led us to propose a set of operational recommendations as well as immediately available technical solutions in order to reduce the risk of a cyber crisis.

TYPES OF THREAT ACTORS IDENTIFIED

- ✓ SUSPECTED STATE-SPONSORED GROUPS
- ✓ CYBERCRIMINALS

MOTIVATION

- ✓ FINANCIAL GAINS
- ✓ ESPIONAGE

TABLE OF CONTENT

1 CONTEXTUALIZATION 4

1.1 COVID-19: A DISRUPTED WORK CULTURE 4

1.2 COVID-19: A THREAT ECOSYSTEM ON THE LOOKOUT 5

2 IDENTIFIED THREATS 9

2.1 TELEWORK-RELATED THREATS 9

2.1.1 Vulnerabilities in applications used for remote working 9

2.1.2 Ransomwares and teleworking 9

2.1.3 Spyware and backdoors 10

2.1.4 Malicious imitations of communication software 11

2.1.5 Structural vulnerabilities 11

2.2 THREATS IN URGENCY FEELING CONTEXT 12

3 RECOMMENDATIONS 14

3.1 TELEWORKING RECOMMENDATIONS 14

3.2 ADDITIONAL RECOMMENDATIONS 16

4 KNOWLEDGE RESOURCES 17

4.1 TO GO FURTHER 17

4.2 REFERENCES 18

1 CONTEXTUALIZATION

1.1 COVID-19: A DISRUPTED WORK CULTURE

The COVID-19 health crisis is now forcing half of the world's population to make a radical change in lifestyle; that of confinement.

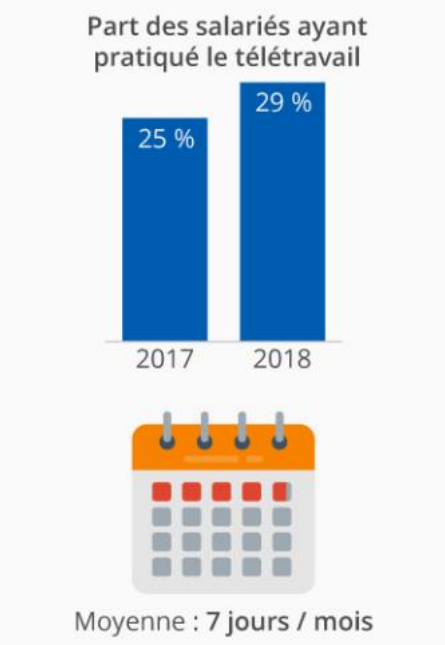
This upheaval has brought about several other changes; social, cultural, economic, political and so on. Such disruptions inevitably lead to an increased risk of adding other systemic crises to the health crisis.

One of these crisogenic fractures, which we all experiment, takes the form of a change in the way we work, produce and interact professionally.

In February 2019, the IFOP research institute and the Malakoff Médicis Humanis group estimated that, in 2018, 29% of French workers have experienced telework based on an average of 7 days per month.[1].

With containment measures, the French population share subject to the telework regime would be 70%, according to Deskeo's study[2], or nearly 20.8 million people, based on INSEE figures[3].

This situation is *de facto* crisogenic from a cybersecurity point of view.



Share of employees having practiced teleworking (average 7 days/month)

Precautionary usage measures to be respected during telework periods are more rarely implemented for several reasons:

- ✓ Illusion of security,
  The feeling of control over one's personal and intimate environment leads us, by extension, to consider that this control is real and applicable to the remote work situation,
- ✓ Reduced vigilance,
  Difficulty in considering the changing nature of the threat related to the change in the work environment,
- ✓ Poor mastery of tools,
  Unfamiliarity with the tools to be used to ensure one's safety when working remotely,
- ✓ Difficulty in positioning,
  Tendency to confuse and amalgamate personal and professional environments,
- ✓ Blurred limits,
  Decreasing caution in the use of professional tools,
- ✓ Weakening of security means,
  Lack of secure communication and workspace tools.

In addition to these classic factors that may imply a stretching of the vulnerability fabric, the magnitude of the phenomenon linked to the COVID-19 crisis has a multiplier effect.

Two information is important:

- ✓ Out of the 20.8 million French people teleworking, nearly 18.5 million were not used to working in this way until now,
- ✓ Almost 2.3 million French people teleworking from their second home (usually used for vacation periods).

Both of these factors increase cyber risk. They strongly incline almost all workers to fall into the pitfalls identified above.

1.2 COVID-19: A THREAT ECOSYSTEM ON THE LOOKOUT

The global situation of containment is therefore at stake to introduce indirectly, through its exceptional nature in all fields of daily life, great feverishness into the cybersecurity world.

This feverishness has been identified by the cyber threat ecosystem. Suddenly and massively, teleworking has become the new soft underbelly of cybersecurity for all businesses.

As shown in the analysis « COVID-19: CYBER THREAT ASSESSMENT[4]», that we are reusing and reinforcing here, cyber attackers around the world have taken up the topic of COVID-19 extensively to better defeat their targets.

Cybercriminals and certain groups that we suspect are sponsored by nation-states use decoys, spam and phishing campaigns, create dedicated web pages and corrupt several phone applications to trap their targets.

As a reminder, among the groups suspected of being sponsored by nation-states and having used the COVID-19 theme to reach their targets, Thales sources identify the following **ATK175** (Vicious Panda)[5] and **Mustang panda**[6], **ATK72** (Kimsuky)[7], **ATK64** (APT36)[8] and the **Hades** group linked to **ATK5** (APT28, Fancy Bear)[9].

Given the history of these groups, it is highly likely that their attacks, focused on classic geopolitical adversaries, will follow the same motivations as in their former campaigns: espionage.

It must be clearly understood that it is the entire threat ecosystem that uses the COVID-19 theme and the current situation to carry out its attacks. Nevertheless, groups suspected of being sponsored by nation-states remain a minimal typology in terms of attack volume linked to COVID-19.

Cybercriminals have also taken up the theme of COVID-19. We can mention the groups behind the following malwares:

✓ **LokiBot**: Loki, or "LokiBot" (not to be confused with Loki RAT), is an information stealer sold on secret forums. This malicious software collects information from the machine, such as:

o References from:
- Browsers
- Game platforms
- File transfer tools
- Mailboxes
- Password Managers

o Encrypted Currency Wallets
o Screenshots
o Key shots
o Cookies and other browser information

This data is then exfiltered via HTTP POST requests.

✓ **Emotet:** Emotet, which was first seen around May 2014, was originally designed as a modular banking Trojan. It shared its code with another banking Trojan, Feodo. However, the group has added functionality and improved the existing code. Today, it is one of the most powerful malwares in the cybercriminal ecosystem. Its main prerogative is to download other malware on the machines of infected victims.

✓ **Trickbot**: TrickBot is a Trojan-like spyware program that has been used primarily to target banking sites in the United States, Canada, the United Kingdom, Germany, Australia, Austria, Ireland, Switzerland and Scotland. TrickBot appeared in the wild in September 2016 and appears to be Dyre's successor. It is developed in the C++ programming language. Trickbot has often been dropped by Emotet.

In 2020, the author continues to improve the Trickbot malware, adding, for example, new techniques to bypass the UAC of Windows 10. In the context of attacks using the COVID-19 theme with Trickbot, Italy is particularly targeted.

✓ **Azorult**: Today Azorult is using a fake corrupted geographical map to track the evolution of the pandemic to infect its victims (imitation of the John Hopkins University map).

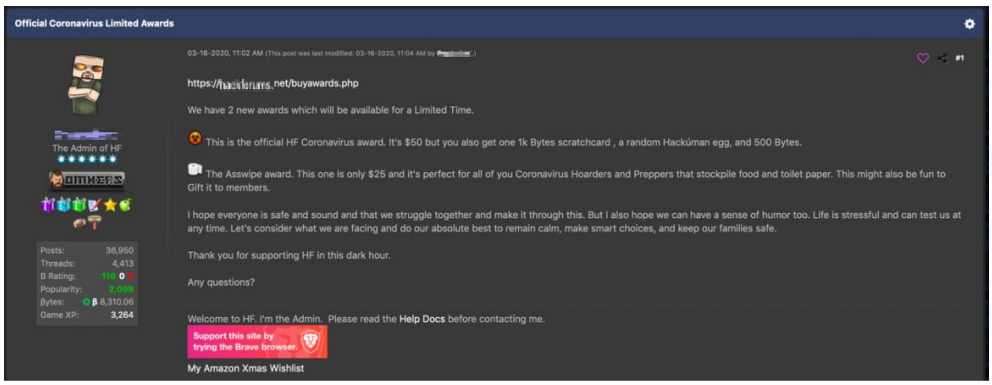
✓ **SpyNot RAT**: SpyNote RAT (Remote Access Trojan) is a family of malicious Android applications. The SpyNote RAT builder tool can be used to develop malicious applications with malware functionality.

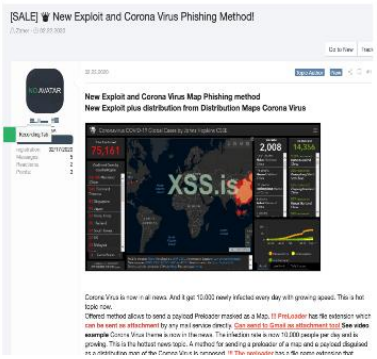
✓ **Formbook**: Formbook is an information stealer who first appeared in February 2016. It is sold online by "ng-Coder", for about $30 a week, alongside its panel. The author also provides hosting for his malware.

- ✓ **BlackWater**: BlackWater is a remote access Trojan that uses CloudFlare users for its C&C communications. For decoy purposes, this malware opens a Word document when launched. This malware is probably still under development and may continue to evolve.
- ✓ **Cerberus**: Cerberus is an Android banking Trojan first reported by ThreatFabric in June 2019 and could be active since at least 2017. The malware activates when victims move, triggering the accelerometer inside the device. Cerberus remains dormant until the phone's pedometer reaches a certain number of steps. It also modifies the decoy according to the name of the Android package, by entering bank details or postal references[10].

According to a U.S. source[11], the modus operandi based on the use of the COVID-19 or Coronavirus theme now dominates the threat ecosystem. This theme is used not only in the subject or body of malicious messages but also in attachments, URLs and decoys.

On Dark Web forums, we have noticed that some hackers are selling ready-to-use phishing kits on the COVID-19 theme[12]. In the image on the right, for example, new exploits related to COVID-19 with an explanation of the phishing method using a corrupted imitation of the map from Johns Hopkins University (USA)[13] are sold on a Russian forum.



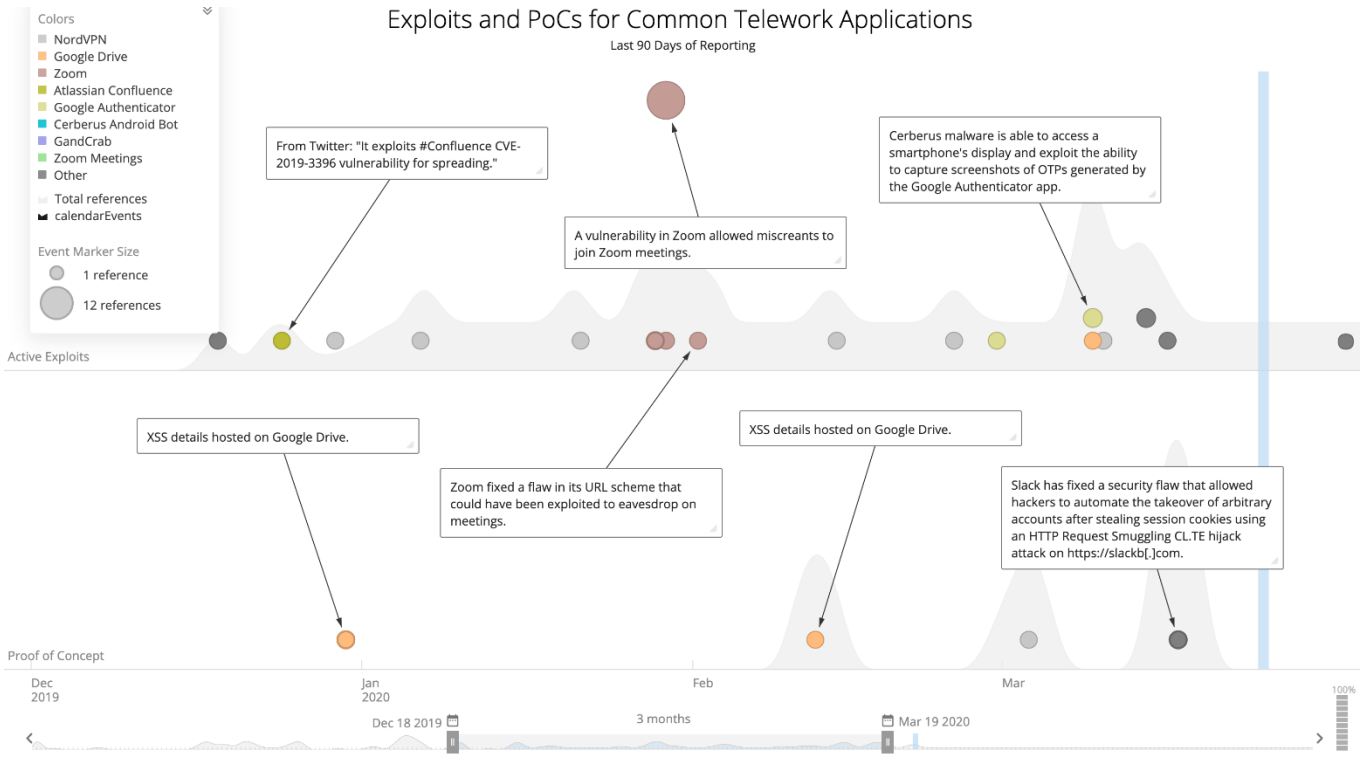


In a few figures, the use of the COVID-19 theme by the attackers has so far (March 27, 2020) been done by means of more than:

- ✓ **500 000** messages,
- ✓ **300 000** URL,
- ✓ **200 000** attachments,
- ✓ **140** attack campaigns.

Within the Cyber Threat Coalition focused on COVID-19 there are also approximately **79 343** suspect domains (April 1st, 2020), related to this topic that can download malware[14].

It should be noted that these attack campaigns affect the entire world and are carried out by all types of threat actors[15]. They also concern the tools that enable the pursuit of remote working as shown in this Recorded Future analysis [16].



Attacks on common teleworking applications in the last 90 days.

2 IDENTIFIED THREATS

2.1 TELEWORK-RELATED THREATS

Thus, several attack vectors, some new and others already used in previous attacks, become more interesting for attacker groups in this period of massive teleworking.

2.1.1 Vulnerabilities in applications used for remote working

Several applications used to work remotely have already, in the past, been victims of vulnerabilities and then targeted by attackers. In particular, a vulnerability was discovered in 2016 by Checkpoint that allowed an attacker to listen in on calls made through Zoom application[17]. Not all these flaws are theoretical and unused. Two main types of malware would be able to use this kind of vulnerability and represent the most important threats today: ransomware and spyware.

2.1.2 Ransomwares and teleworking

Ransomware is malware that encrypts files and requires a ransom to decrypt them. To make victims pay, who increasingly use high-performance backup systems, many ransomware families steal certain files and threaten to make them public if the victim refuses to pay.

Thus, a vulnerability in Citrix products, for example, has allowed several families of ransomwares to propagate.

The German company Gedia, which manufactures car parts, has been infected with **Sodinokibi** ransomware, that penetrated the corporate network using this vulnerability. This ransomware had already used a vulnerability in the Pulse Secure VPNs to infect other victims. Among the ransomwares using this vulnerability, we can find:

- ✓ **Sodinokibi** (Revil): Sodinokibi is a ransomware that appears in April 2019, a few months before the "retirement" of the GandCrab ransomware (June 2019). It infects machines by exploiting the CVE-2019-2725 of Oracle WebLogic Server. There are strong presumptions that Sodinokibi is exploited or at least created by the author of GandCrab:
  - We observed that Sodinokibi was dropped by variants of MalPack that had previously been used to drop GandCrab,
  - The decoding functions and other aspects of the code used by Sodinokibi and GandCrab are almost identical.
- ✓ **Ragnarok**: Ragnarok is a ransomware, which initially spread through unpatched Citrix systems vulnerable to CVE-2019-19781.

  This software, which uses AES and RSA to encrypt files, deliberately avoids encrypting machines with Chinese- and Russian-language keyboards.

It acts like most ransomware and disables Windows Defender and various other recovery methods.

Although it is currently only available for Windows, some strings refer to Unix paths. This could mean that this ransomware may become available on Linux in the future.

- ✓ **Maze**: Maze is a ransomware that appeared in 2019. It is distributed through spearphishing, as well as through exploitation kits such as FalloutEK and Spelevo. This ransomware is associated with a single threat actor and does not appear to be shared or part of a malware-as-a-service operation. It was one of the first to threaten to publish stolen information on its website, mazenews[.]top. Many victims of this ransomware is to be deplored.

  Once the ransomware has finished encrypting all the files, it drops a file named "DECRYPT-FILES.txt" in every folder it can find[18].

There is a strong competition between the actors of the threat deploying ransomwares for two reasons:

- ✓ First, there are many different ransomware families,
- ✓ Second, the RaaS (Ransomware-As-A-Service) model, where ransomware developers do not deploy their malware themselves but use "affiliates", creating broad competition among affiliates.

Thus, in an effort to distinguish themselves and infect the most important victims, ransomwares look for new ways to spread, and regularly look for new vulnerabilities.

Systems used for remote working, such as Citrix, Zoom, Pulse Secure VPN, Fortigate SSL VPN, etc. have already been vulnerable and have been used to deploy ransomwares.

2.1.3 Spyware and backdoors

Remote working tools, which often allow direct access to the company's network, also become prime targets for attackers who practice industrial espionage.

Thus, the group **ATK107** (APT5)[19] who specializes in industrial espionage and data theft, used vulnerabilities in VPN systems to steal credentials.

These attackers mainly target large industrial groups, particularly in Defense and Telecoms sector.

Another actor also used the vulnerability to deploy a backdoor, named **NOTROBIN**. This malware provides long-term access to VPN platforms, often located in the corporate network itself.

Attackers looking for trade secrets are often state-sponsored. They usually have the expertise to search for vulnerabilities and develop exploits for them, as well as the financial resources to purchase those same vulnerabilities.

2.1.4 Malicious imitations of communication software

Remote working tools, and in particular digital communication tools can be used by less-skilled attackers to target potential victims.

This is done in two main ways:

- ✓ First by creating fake sites that strongly resemble official sites. Since the beginning of the year, for instance, more than 1700 Zoom-like domains have been created, of which a quarter was created last week (March 23-29, 2020). This is the case for other online platforms, such as Google Classroom. False installers, named in the same way as those of Zoom and Microsoft Teams have also been discovered, deploying malware on the user's machine.
- ✓ The second way is to send e-mails masquerading as official communications from the software manufacturer, in order to either deploy malware or collect user IDs. These identifiers can then be used in later campaigns or sold to other groups.

2.1.5 Structural vulnerabilities

The very fact of opening up to telework can weaken the protections put in place by the company to protect itself from cyber-threats.

Several elements can provide attackers with opportunities for attacks:

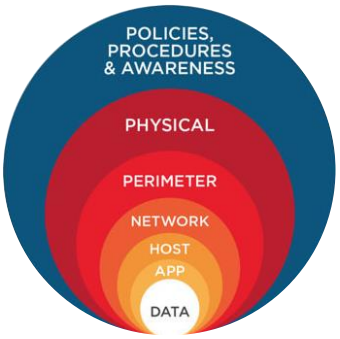
- ✓ First, increased access to information systems places an additional workload on helpdesk services. Malicious messages masquerading as these support services will therefore be very popular among attackers.
- ✓ In addition, the overload on VPN and remote access servers make distributed denial of service (DDoS) attacks even easier. These attacks, by opening a large number of connections on the servers could greatly disrupt access to these services, preventing employees from working.

The fact that employees work from home changes habits, resulting in two issues:

- ✓ First, behavioral detection tools are less effective, and may become less able to detect threats,
- ✓ Then, employees are more likely to use services that are not adapted to company security constraints.

2.2 THREATS IN URGENCY FEELING CONTEXT

The threat to telework activities under containment related to the COVID-19 crisis repeats the elements seen above with the addition of an ingredient: « Urgency feeling ».



In-depth defense

Urgency feeling crisis-driven will negatively affect the ability of users and technical teams to manage cyber risk. At the same time, that feeling will greatly help the attackers since it is the lever on which the human error rests.

Since the beginning of the crisis, we have seen a large number of companies offering their products for free to do telework. This is a good initiative, but it can lead to problems, for which some precautions must be taken:

- ✓ Beware of the multiplication of business solutions. It can make it more difficult to update and secure the solution,
- ✓ Be careful not to overload the IT teams. Completely overwhelmed by the demands, they might not be able to respond to a crisis situation.

As we have seen, setting up a telework system considerably increases the company's surface of attack. In addition, this system must be installed in a relatively short period of time, which leaves little time for the technical teams to adapt to the situation. This lack of adaptation time gives rise to several difficulties that will have to be taken into account during the crisis.

The main difficulty lies in the number of organizations will probably have to rapidly deploy technologies that neither its teams nor future users are used to working with (Cloud, secure file sharing, VPN connection, etc.). This lack of preparation time will result in configuration errors that can make these tools vulnerable (let the default password, administrator access, etc.). Configuration errors are one of the main threats to Cloud services[20], leaving each year thousands of companies vulnerable to sensitive data breaches.

With VPN vulnerabilities being widely used, the teams setting up these systems must keep each other informed in order to avoid a possible Supply Chain attack (attacking the VPN service to reach all its users).

For the users of these services, there will also be an abrupt change in habits: connections at different times (employees are less constrained by office hours), connections from unfamiliar locations, use of new services, etc.

As mentioned above, these changes may make it difficult to use detection tools based on behavioral analysis. Security teams need to be aware of these changes in order to adapt their detection.

Employees without mobile workstations may be required to use their own devices resulting in a wave of new device connections on the company's network. These devices may introduce

malware into the network that will not be detected by peripheral security systems. Security systems based on defense-in-depth are effective in such cases.

The final problem remains the users of telework services. The vast majority of employees are not accustomed to teleworking as we explained. These employees do not know what tools to use or how to use them.

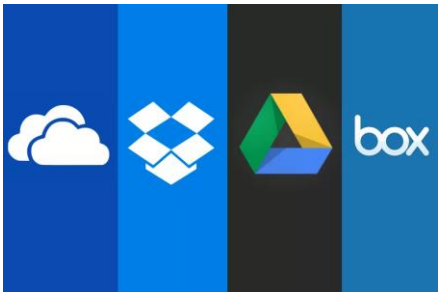
One possible consequence is overloading of HelpDesk support services who will then themselves be in a situation where their treatment capacity will not be optimal. These sudden inflows may cause stress to support teams, resulting in technical errors and increased cyber risk.

Technical staff should expect an overload of the various means of teleworking, overloading of VPNs, conferencing services, messaging, file storage systems, etc.

If the end user is left without a functional means to perform the requested task; he can choose to use other non-secure work tools.

If he is unable to use his video conferencing tool properly, either because it is overloaded or because it doesn't know/can't use a VPN, he may knowingly decide to use an accessible but unauthorized video conferencing service in corporate policy.

The use of these services may result in data leaks as demonstrated to us by Check Point's discovery of a vulnerability in the Zoom video conferencing tool allowing an attacker to identify and join a conference[21].



The same problem applies to file-sharing systems, which can quickly be replaced by simpler solutions such as Google Drive or DropBox.

3 RECOMMENDATIONS

3.1 TELEWORKING RECOMMENDATIONS

✓ **Virtual Private Network (VPN) Management**

Update VPNs and prepare for their massive use, which may require limiting the bandwidth of some users to prioritize critical activities.

✓ **Raising team awareness**

We strongly recommend conducting an awareness campaign aimed at users AND technical teams for everyone to be aware of the technical and human cyber risks generated by the current situation. It is necessary to recall the need to use the secure tools made available by the company and to refrain from using external tools. Moreover, attackers use the situation and the stress it generates to create phishing emails and effective water holing sites. Mistrust of emails received about COVID-19 should be maximized.

✓ **Password management**

Verify and enforce the password policy. An attacker could penetrate the company's local network by forcing an employee's account.

✓ **Use the tools recommended by your company**

As far as possible, personal equipment should not be used for work. If personal devices are to be connected to the company network, it is important to define a minimum-security profile that each device connecting to the network must respect (up-to-date system, presence of anti-virus software).

✓ **Use multiple identification levers**

The use of MFA (Multi-Factor Authentication) in addition to a robust password policy provides the best possible protection against password theft, especially when teleworking.

✓ **Keeping up to date on the vulnerability trends**

Continued priority needs to be given to monitoring the emergence of vulnerabilities in teleworking applications and the application of patches.

✓ **Connection monitoring**

It is interesting to monitor VPN connections from abroad as well, especially during the period when borders are closed.

✓ **Infrastructure security audits**

It is important to have the security of the telecommuting infrastructure tested and to conduct a test to ensure that the incident response teams are capable of providing security remotely.

✓ **Given the major attackers' campaigns, give priority to cyber-intelligence**

Some of the attackers mentioned earlier are extremely successful. Monitoring their movements in the light of ongoing campaigns is essential for institutions and organizations. Cyber Threat Intelligence teams are familiar with these groups, know how they operate and what motivates them. Regularly acquiring analysis allows a proactive stance to be taken against these attackers.

✓ **Combining detection tools with Cyber Threat Intelligence to protect its systems**

The use of tools such as IDS (Intrusion Detection Systems) enriched with the information provided by cyber intelligence allows the detection from the outset of the attacks carried out by those presented in this analysis at the time of their attacks and thus significantly reduce the potential damage.

✓ **It is imperative to take into account ANSSI's recommendations.**

We recommend following the recommendations of the ANSSI and more particularly the guide on Digital Nomadism freely available at the following address: https://www.ssi.gouv.fr/uploads/2018/10/guide_nomadisme_anssi_pa_054_v1.pdf

✓ **Take into account Positive Technologies' recommendations**

The article “Work from home: digital distancing to keep your network safe” offers a set of relevant recommendations in its “Work-from-home security checklist” section: https://www.ptsecurity.com/ww-en/analytics/knowledge-base/work-from-home-digital-distancing-to-keep-your-network-safe/

3.2 ADDITIONAL RECOMMENDATIONS

✓ Follow **ANSSI**'s recommendations in its Bulletin d'actualité CERTFR-2020-ACT-002 on the current state of containment and telework[22]:

1. It is important not to expose under any circumstances on the Internet the web interfaces of Microsoft Exchange servers that are not at the latest patch level,
2. Do not give access to your file sharing servers via the SMB protocol,
3. If you expose or need to expose new services on the Internet, update them as soon as possible with the latest security patches and activate the logging mechanisms. If possible, enable multi-factor authentication,
4. Apply security patches quickly, especially on equipment and software exposed to the Internet (VPN solution, remote desktop solution, messaging solution, etc.),
5. Perform offline backups for your critical systems,
6. Use a VPN (Virtual Private Network) type access solution specific to the company, ideally IPsec or TLS by default, so as not to expose applications directly to the Internet,
7. Implement multi-factor authentication mechanisms to limit the risk of identity theft (VPN and accessible applications),
8. Regularly check access logs of solutions exposed on the Internet to detect suspicious behavior.

4 KNOWLEDGE RESOURCES

4.1 TO GO FURTHER

- ✓ Trend Micro: https://blog.trendmicro.com/this-week-in-security-news-hong-kong-users-targeted-with-mobile-malware-via-local-news-links-and-hackers-hijack-routers-to-spread-malware-via-coronavirus-apps/
- ✓ F-Secure: https://blog.f-secure.com/coronavirus-spam-update-watch-out-for-these-emails/
- ✓ Talos Intelligence: https://blog.talosintelligence.com/2020/03/covid-19-relief-package.html
- ✓ Carbon Black: https://www.carbonblack.com/2020/03/31/threat-analysis-unit-tau-threat-intelligence-notification-coronavirus-ransomware/
- ✓ Fortinet: https://www.fortinet.com/blog/business-and-technology/secure-remote-access-for-the-teleworker-accessing-the-cloud.html
- ✓ Secureworks: https://www.secureworks.com/blog/securing-remote-work-adoption-growth
- ✓ Bitdefender: https://labs.bitdefender.com/2020/03/android-apps-and-malware-capitalize-on-coronavirus/
- ✓ Recorded Future: https://www.recordedfuture.com/remote-attack-surface/
- ✓ Carbon Black: https://www.carbonblack.com/2020/03/31/covid-19-cybersecurity-community-resources/
- ✓ Proof Point: https://www.proofpoint.com/us/threat-insight/post/threat-snapshot-coronavirus-related-lures-comprise-more-80-percent-threat
- ✓ Talos Intelligence: https://blog.talosintelligence.com/2020/03/covid-19-pandemic-threats.html
- ✓ Fortinet: https://www.fortinet.com/blog/industry-trends/maintaining-business-continuity-amid-changing-workplace-operations.html
- ✓ Anomali: https://www.anomali.com/blog/leverage-threatstream-and-domaintools-covid-19-threat-list
- ✓ Fire Eye: https://www.fireeye.com/blog/threat-research/2020/03/stimulus-bill-social-engineering-covid-19-financial-compensation-schemes.html
- ✓ Security Intelligence: https://securityintelligence.com/posts/zeus-sphinx-trojan-awakens-amidst-coronavirus-spam-frenzy/
- ✓ Bitdefender: https://labs.bitdefender.com/2020/03/infected-zoom-apps-for-android-target-work-from-home-users/
- ✓ Check Point: https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/
- ✓ ESET: https://www.welivesecurity.com/2020/03/13/beware-scams-exploiting-coronavirus-fears/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+eset%2Fblog+%28ESET+Blog%3A+We+Live+Security%29
- ✓ Security Affairs: https://securityaffairs.co/wordpress/99682/cyber-warfare-2/coronavirus-themed-attacks.html
- ✓ Malware Bytes: https://blog.malwarebytes.com/threat-analysis/2020/03/apt36-jumps-on-the-coronavirus-bandwagon-delivers-crimson-rat/
- ✓ Recorded Future: https://www.recordedfuture.com/coronavirus-panic-exploit/
- ✓ Korii: https://korii.slate.fr/tech/hackers-covid-19-coronavirus-cartes-emails-diffusion-virus-malwares-cheval-de-troie
- ✓ CERT-FR: https://www.cert.ssi.gouv.fr/actualite/CERTFR-2020-ACT-002/
- ✓ CERT-FR: https://www.cert.ssi.gouv.fr/actualite/CERTFR-2020-ACT-001/
- ✓ ANSSI: https://www.ssi.gouv.fr/uploads/2018/10/guide_nomadisme_anssi_pa_054_v1.pdf
- ✓ LCI: https://www.lci.fr/police/coronavirus-les-hopitaux-de-paris-aphp-victimes-d-une-cyberattaque-deni-de-service-de-hackers-2148857.html
- ✓ The Verge: https://www.theverge.com/2020/1/28/21082331/zoom-vulnerability-hacker-eavesdrop-security-google-hangouts-skype-checkpoint
- ✓ Check Point: https://research.checkpoint.com/2020/zoom-zoom-we-are-watching-you/

- ✓ Trend Micro: https://www.trendmicro.com/vinfo/pl/security/news/virtualization-and-cloud/-misconfigured-cloud-services-pose-high-security-risks-for-organizations
- ✓ Positive Technologies: https://www.ptsecurity.com/ww-en/analytics/knowledge-base/work-from-home-digital-distancing-to-keep-your-network-safe/
- ✓ Trend Micro: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains
- ✓ Center for Systems Science and Engineering (CSSE) at Johns Hopkins University (JHU): https://gisanddata.maps.arcgis.com/apps/opsdashboard/index.html#/bda7594740fd40299423467b48e9ecf6
- ✓ McAfee: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze/

4.2 REFERENCES

[1] https://fr.statista.com/infographie/17111/chiffres-cles-teletravail-en-france/
[2] https://www.deskeo.fr/blog/sondage-coronavirus-teletravail/
[3] INSEE, Tableaux de l'économie française, Édition 2019, Population active: https://www.insee.fr/fr/statistiques/3676623?sommaire=3696937
[4] https://www.thalesgroup.com/sites/default/files/database/document/2020-03/2020-03-24_COVID-19_CYBER_THREAT_ASSESSMENT_(FR).pdf?_ga=2.141375990.557932588.1585639566-673659253.1554283181
[5] Presumed Chinese origin. Targeting of Chinese and Mongolian victims.
[6] Presumed Chinese origin. Targeting of Taiwanese victims.
[7] Presumed North Korean origin. South Korean victims targeted.
[8] Presumed Pakistani origin. Targeting of Indian victims.
[9] Presumed Russian origin. Targeting of Ukrainian victims.
[10] These malwares are more broadly described in the report: « COVID-19: CYBER THREAT ASSESSMENT »: https://www.thalesgroup.com/sites/default/files/database/document/2020-03/2020-03-24_COVID-19_CYBER_THREAT_ASSESSMENT_(FR).pdf?_ga=2.141375990.557932588.1585639566-673659253.1554283181
[11] https://www.proofpoint.com/us/threat-insight/post/threat-snapshot-coronavirus-related-lures-comprise-more-80-percent-threat
[12] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains
[13] https://gisanddata.maps.arcgis.com/apps/opsdashboard/index.html#/bda7594740fd40299423467b48e9ecf6
[14] https://www.cyberthreatcoalition.org/
[15] https://www.proofpoint.com/us/threat-insight/post/threat-snapshot-coronavirus-related-lures-comprise-more-80-percent-threat
[16] https://www.recordedfuture.com/remote-attack-surface/
[17] https://www.theverge.com/2020/1/28/21082331/zoom-vulnerability-hacker-eavesdrop-security-google-hangouts-skype-checkpoint
[18] https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze/
[19] Presumed Chinese origin.
[20] https://www.trendmicro.com/vinfo/pl/security/news/virtualization-and-cloud/-misconfigured-cloud-services-pose-high-security-risks-for-organizations
[21] https://research.checkpoint.com/2020/zoom-zoom-we-are-watching-you/
[22] https://www.cert.ssi.gouv.fr/actualite/CERTFR-2020-ACT-002/