THALES

COVID-19

CYBER THREAT ASSESSMENT

24/03/2020

Version – 01

CYBER THREAT INTELLIGENCE ASSESSMENT

COVID-19
A POWERFUL CRISOGENIC FACTOR

SUMMARY

The aggravation of the COVID-19 crisis in Europe, which has become the new epicenter of the epidemic, implies an increase in the number of threat actors using decoys linked to this news to compromise their victims.

A change in this dynamic must in particular be taken into account by critical institutions and organizations. While the actors taking advantage of the news to carry out their attacks were initially cybercriminals, more and more state-sponsored groups (Advanced Persistent Threat) are now using this theme as part of their espionage campaigns.

Another phenomenon to watch out for is the growing number of Android mobile applications being used to largely compromise the populations.

Globally it appears today, according to several sources, that 50% of the domain names created since December and linked to the theme of COVID-19 or Coronavirus can lead to the injection of malicious software (infographics presented in 1.6).

TYPE OF THREAT ACTOR IDENTIFIED

- ✓ SUSPECTED STATE-SPONSORED GROUPS
- ✓ CYBERCRIMINALS

MOTIVATION

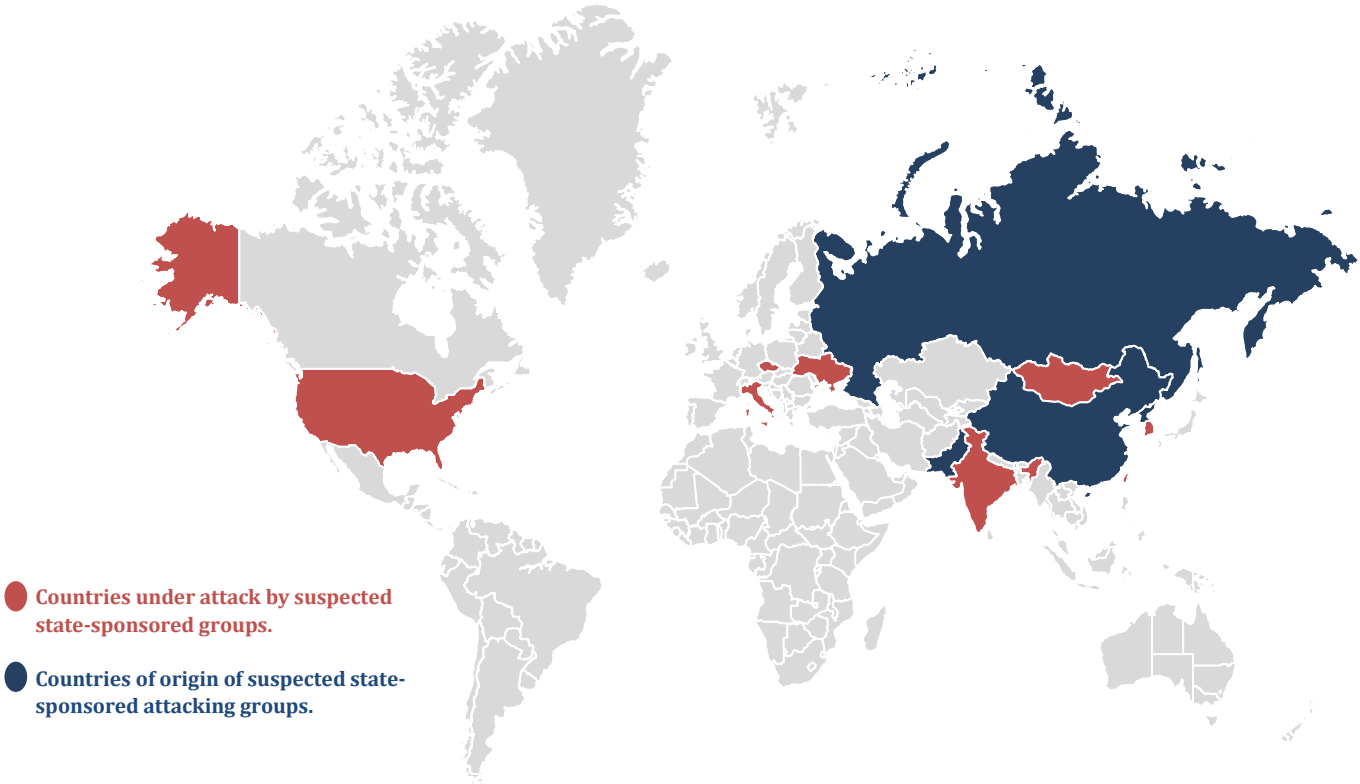
- ✓ FINANCIAL GAINS
- ✓ ESPIONAGE

TABLE OF CONTENT

1.1 CTI NOTICE

As the number of threat actors using decoys and corrupted applications related to COVID-19 increases rapidly, particular caution must be observed. These attack campaigns take advantage of a collective stupefaction phenomenon that has the effect of putting blinkers on the eyes of the greatest number of people.

It appears that the cyber threat ecosystem is following the geographic spread of COVID-19 with attacks first in Asia, then in Eastern Europe and now in Western Europe. French territory therefore presents an increased risk of attacks.



Countries targeted by attackers with modus operandi centered on the CORONAVIRUS theme.

Our attention, overstretched by the COVID-19 crisis, may lead us to act without consideration for our immediate security, especially cyber.

Fear pushes us to seek as much information as possible to build a sensation of individual control over a phenomenon that escapes us. This impulse makes us much more vulnerable to fake news.

This vulnerability must be addressed, integrated and accepted by institutions, organizations and individuals. Only in this first step is it possible to modulate behavior as recommended below.

According to some attacker groups' statements, hospitals should be spared. Groups of major cybercriminals, including those operating the MAZE and DOPPELPAYMER ransomwares, have declared that no hospital will be targeted in this global campaign. Nevertheless, these statements must not under any circumstances lead to a reduction in vigilance, since attacks have been noted, in particular against the Paris Hospitals.

1.2 ACTIVE THREAT ACTORS

The threat actors identified to date as using the COVID-19 crisis as part of their attack campaigns are as follows:

✓ **Vicious Panda (suspected Chinese origin)**: Check Point Research has uncovered a new campaign against the Mongolian public sector, which is taking advantage of the current coronavirus alert to deliver a previously unknown malware implant to the target.

Original

МОНГОЛ УЛСААС БНХАУ-Д СУУГАА ЭРЧИМ САЙДЫН ЯАМ

ШУУРХАЙ МЭДЭЭ

Шинэ коронавирусын халдварын тархалтын тухай

БНХАУ-ын Төрийн зөвлөлийн Хэвлэл мэдээллийн албанаас өнөөдрийн 10:00 цагт хийсэн хэлэлцүүлэгт баяа хурлын үеэр Хятад улсад шинэ коронавирусын халдварт хамгалагдаагүй өвчилсөн 440 хүн байгаа бөгөөд 9 нас барсан тохиолдол байгаад мэдээлсэн.

Хятадын Үндэсний эрүүл мэндийн хороонооос гаргасан статистик мэдээллээр өнөөдрийн байдлаар Хятад улсын өнөөд болсон эрүү өнөөд хэлэйн 14 муж, хот мөн АНУ, Япон, Өмнөд Солонгос, Австрали (тус бүр 1), Сингапур (7), Тайланд (2) зэрэг улсад тархсан байна. Вирусын тархалтын хэд хурдан байгаа бөгөөд дорох 440 өвчтөний сүүлчи хүрсний нийт 2197 хүнд тандалт хийж, 765 хүний халдварүйг тогтоож, 1394 хүнийг үргэлжлүүлэн хянаж байна.

Шинэ коронавирусын халдварын талаарх шуурхай мэдээллийг үргэлжлүүлэн хүргэх болно.

БОЛОВСРУУЛСАН: [redacted]

[redacted]

Translated (Automatically)

MONGOLIA FROM MONGOLIA TO CHINA
Ministry of Foreign Affairs

FAST NEWS

About the spread of new coronavirus infections

[redacted]

Original

[redacted]

Translated (Automatically)

[redacted]

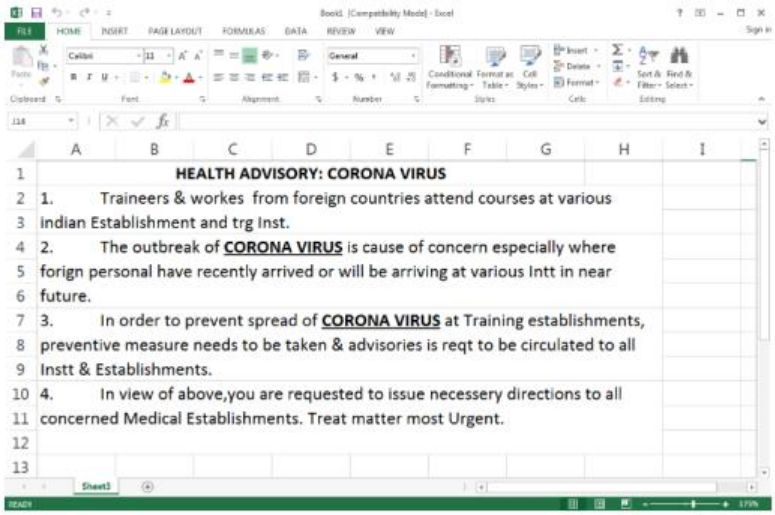
A deeper examination of this campaign allows us to link it to other operations that were conducted by the same anonymous group, dating back to at least 2016. Over the years, these operations have targeted different sectors in many countries, such as Ukraine, Russia and Belarus.

✓ **Mustang panda (suspected Chinese origin):** Mustang Panda is a China-based adversary that has demonstrated its ability to quickly assimilate new tools and tactics into its operations. In the COVID-19 crisis, it was able to use new decoys to target Taiwan.

✓ **Kimsuky (suspected origin: North Korea:** ATK72 (Kimsuky) was first identified in 2013 by Kaspersky. Since 2013, the Kimsuky Group has been pursuing a cyber-attack campaign against government organizations and defense-related agencies in South Korea as well as institutions and companies related to South Korea's engagement with North Korea. This threatening actor targets South Korean think tanks, industry, nuclear power operators and the Ministry of Unification for espionage. This actor appears to be part of the unit responsible for espionage in South Korea.

According to a tweet shared by the South Korean cybersecurity company IssueMakersLab, a group of North Korean hackers also hid malware inside documents detailing South Korea's response to the COVID-19 virus epidemic.

The documents, which were allegedly sent to South Korean officials, were tricked with BabyShark, a strain of malware previously used by Kimsuky.



	A	B	C	D	E	F	G	H	I
1	HEALTH ADVISORY: CORONA VIRUS								
2	1.	Traineers & workes from foreign countries attend courses at various							
3	indian Establishment and trg Inst.								
4	2.	The outbreak of CORONA VIRUS is cause of concern especially where							
5	forign personal have recently arrived or will be arriving at various Intt in near								
6	future.								
7	3.	In order to prevent spread of CORONA VIRUS at Training establishments,							
8	preventive measure needs to be taken & advisories is reqt to be circulated to all								
9	Instt & Establishments.								
10	4.	In view of above,you are requested to issue necessery directions to all							
11	concerned Medical Establishments. Treat matter most Urgent.								
12									
13									

- ✓ **APT36 (suspected Pakistani origin):** APT36 relies primarily on spearphishing and watering hole attacks to infect its victims. The phishing email is either a malicious macro document or an rtf file exploiting vulnerability, such as CVE-2017-0199. In the coronavirus-themed attack, APT36 used a phishing email with a link to a malicious document posing as the Indian government. (email.gov.in.maildrive[.]email/?att=1579160420).

- ✓ **Hades group (linked to APT28 and of presumed Russian origin)**: The first state-sponsored hacking group to use a coronavirus lure was the Hades group, believed to operate from Russia, and linked to APT28 (Fancy Bear), one of the groups that also hacked the DNC in 2016.

  According to cyber security firm QiAnXin, Hades hackers conducted a campaign in mid-February by hiding a C# Trojan horse in bait documents containing the latest news about COVID-19.

  The documents were sent to targets in Ukraine, disguised as emails from the Ukrainian Ministry of Health's Public Health Centre.

  The targeted emails appear to have been part of a larger misinformation campaign that has affected the entire country on various fronts.

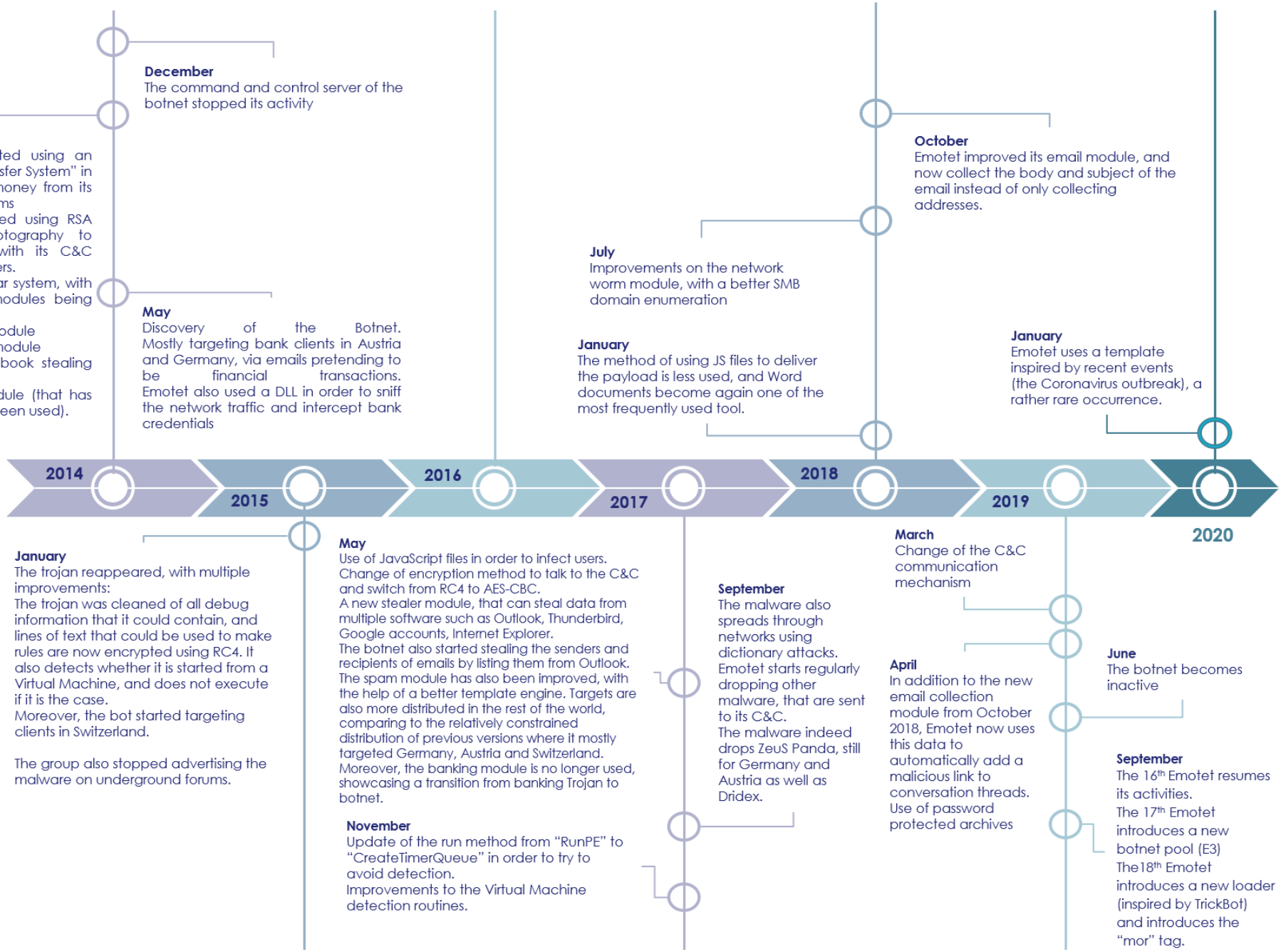
  First, at the same time that Hades was targeting its targets, a wave of unsolicited emails on the subject of coronaviruses hit the country. Second, the e-mail campaign was followed by an avalanche of social media messages claiming that COVID-19 had arrived in the country.

  According to a BuzzFeed News report, one of these emails went viral, and supported by the wave of social media alarmism, caused widespread panic and violent riots in parts of the country.

BuzzFeed News reported that in some Ukrainian cities, residents have blocked hospitals for fear that their children will be infected by evacuees infected with coronavirus from the war-torn eastern region of Ukraine.

In this general panic, a few e-mails containing malicious software were much more likely to go unnoticed and reach their targets, most of whom were most likely interested in current events in the country.

- ✓ **TA542 or Emotet:** Emotet is a very efficient downloader operated since 2014 by ATK104 (alias TA542), an actor of the financial threat. This malware has been noticed by the excellent OPSEC capabilities of its authors. It relies on a resilient command and control infrastructure and is designed to be difficult to detect with static detection rules. It has been observed spreading malware from other threat actors, which implies that being infected by Emotet means being potentially infected by any other actor using its services.



Timeline presenting the different evolutions of Emotet.

- ✓ **Actors using LokiBot malware:** Loki, or "LokiBot" (not to be confused with Loki RAT), is an information thief sold on underground forums. This malicious software collects information from the machine, such as:
  - References from:
    - Browsers
    - Game platforms
    - File transfer tools
    - Mailboxes
    - Password Managers
  - Encrypted Currency Wallets
  - Screenshots
  - Keystrokes
  - Cookies and other browser information

  This data is then exfiltered via HTTP POST requests.

- ✓ **Actors using Trickbot malware:** 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, London, Switzerland and Scotland. TrickBot appeared in the wild in September 2016 and appears to be Dyre's successor. TrickBot is developed in the C++ programming language. Trickbot has often been abandoned by Emotet.

  Trickbot appeared in the fall of 2016 and was initially described as the successor to Dyreza, a credential thief. Trickbot is modular malware with additional features such as an email spammer. Its most notable function is lateral movement. In July 2017, Trickbot added a worm propagation module based on SMB, but had not yet included an exploit.

  Since 2018 we have observed that Emotet has abandoned the Trickbot malware. We are convinced that this malware comes from different authors, but they seem to be linked and collaborate.

  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 COVID-19-themed attacks with Trickbot, Italy is particularly targeted.

- ✓ **Brno University Hospital (the largest Czech laboratory for COVID-19 testing) was also targeted by an unknown attacker.**

- ✓ **The U.S. Department of Health and Human Services was also the victim of a cyber-attack related to the COVID-19 context.**

1.3 ANDROID APPLICATIONS

Some attackers have noticed that people, in addition to following traditional media, are using mobile applications to track the spread of the virus around the world. As a result, they have created corrupted applications to reach new victims:

- ✓ **CovidLock**: Mobile coronavirus tracking application containing ransom software,
- ✓ Reconditioned version of the Banking Trojan Horse **Cerberus Android**,
- ✓ **Covid Android Ransomware**, (which can be unlocked with the code "4865083501")

1.4 RAMSOMWARES USING COVID-19 AS LURE

- ✓ **Azorult**: Azorult is a Trojan horse that is used to steal information from compromised hosts. It has been sold online on Russian-speaking cybercrime forums for about $100.

  Azorult was observed in the wild as early as 2016. Its author officially stopped developing it in December 2018, but the malware is still widely used today in various campaigns due to the various copies that have leaked.

  As Azorult was marketable, it is not surprising that it was released using a wide variety of droppers and exploit kits.

  Today Azorult is using a fake map to track the progress of the corrupt pandemic to infect its victims.

- ✓ **SpyNote RAT**: SpyNote RAT (Remote Access Trojan) is a family of malicious Android applications. The SpyNote RAT builder can be used to develop malicious applications with the following malware features.

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

  It has keystroke logging capabilities, can retrieve identifying information from multiple sources, but one of its features is the theft of form data directly from the browser, hence the name "Formbook". To do so, it uses the "WININET.DLL" method and especially the "HttpSendRequest" method.

  It is possible for the operator to download and run additional malware on the victim's computer.

- ✓ **BlackWater**: BlackWater is a remote access Trojan that uses CloudFlare users for its C&C communications. It is probably used so that the infrastructure is not easily blocked.

  It uses JSON to get commands that need to be executed.

  As a lure, this malware opens a Word document when it is 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 is for sale on a Russian hacking forum called xss [...] where the players behind its development sell licenses for the service between 4,000 and 12,000 dollars. This new malware-as-a-service may have filled the void for players who need Android malware rental services like Anubis and Red Alert which have ceased to exist.

  ThreatFabric analysts point out that the malware activates when victims move, triggering the accelerometer inside the device. Cerberus remains dormant until the pedometer (which measures the number of steps) 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.

1.5 RECOMMANDATIONS

Agence Nationale de Sécurité des Systèmes d'Information

✓ **Follow the recommendations of the ANSSI in its Bulletin d'actualité CERTFR-2020-ACT-002 on the current state of containment and telework [1] :**

1. 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 are exposing or need to expose new services on the Internet, update them as soon as possible with the latest security patches and enable logging mechanisms. If possible, enable two-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 otherwise, to avoid exposing applications directly to the Internet,
7. Implementing two-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.
9. It is essential to consult the ANSSI's nomadism guide (available here: https://www.ssi.gouv.fr/uploads/2018/10/guide_nomadisme_anssi_pa_054_v1.pdf)

[1] https://www.cert.ssi.gouv.fr/actualite/CERTFR-2020-ACT-002/

Thales
Additional Recommendations

✓ **Favoring trusted channels for getting information.**

As regards the obligation to monitor information on such a sensitive topic, we advise you to inform yourself only through trusted channels (.gouv.fr, national media, etc.).

If you want to follow the evolution of the epidemic use only the map of Johns Hopkins University (USA)[2].

✓ **Restricting the number of channels and guarding against sensationalism.**

Do not multiply information channels and distance yourself from the sensationalism of certain media.

✓ **Fact-checking information deemed unlikely.**

In addition to the increase in the number of attacks, this type of topic is conducive to the multiplication of false news campaigns. To avoid this, the advice given above is also valid. Cross-referencing information that is considered unlikely between several trusted channels reduces uncertainty.

✓ **Alert its teleworkers on the basis of ANSSI's recommendations.**

In times of containment, the vast majority of institutions and organizations have opted for remote working in order to avoid contamination. Nevertheless, the change in working methods should not lead employees to change their habits. On the contrary, in the light of the events detailed here, it is advisable to recall the good practices to be widely observed in your organization.

✓ **Against the campaigns of the major attackers, give priority to cyber threat intelligence.**

Some of the attackers mentioned earlier such as the APT are extremely successful. Monitoring their movements against the backdrop of ongoing campaigns is essential at the level of 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 threat intelligence allows the detection of the attacks of all the groups presented in this analysis at the time they occur, thus significantly reducing the potential damage.

[2] https://gisanddata.maps.arcgis.com/apps/opsdashboard/index.html#/bda7594740fd40299423467b48e9ecf6

1.6 INFOGRAPHICS

Timeline of attacks using COVID-19 as a decoy to reach their victims.

February 1, 2020 – Crooks begins exploiting Coronavirus as bait to spread malware

Security researchers warn against malware campaigns that exploit media attention on COVID-19.

February 25, 2020 - South Korea from the spread of people infected with the Corona virus 19

Eset Security found a malicious code disguised as an investigative program "Corona 19 real time status" and demanded public attention.

February 26 – New cyber campaign leverages the COVID-19 Infodemic

Researchers at Cybaze Yoroi have spotted a new campaign exploiting the interest of COVID-19's evolution to spread malicious software.

March 6 - TrickBot targets Italy using fake WHO emails on coronavirus as bait

Crooks continue to exploit the attention on the COVID-19 outbreak, TrickBot operators are targeting Italian users.

March 8 - New Coronavirus-themed Anti-Spam Campaign Releases FromBook Malware

Experts have discovered a new campaign on the theme of COVID-19 that distributes a malware downloader that provides the infostealer FormBook Trojan.

March 12 - Azorult Used through Compromised Coronavirus Map to Spread Malware

While the WHO declares the COVID-19 epidemic to be a pandemic, the crooks are trying to exploit the situation to make their efforts profitable.

March 13 – State-sponsored hackers are launching Coronavirus-themed attacks

State-sponsored hackers are now using coronavirus lures to infect their targets.

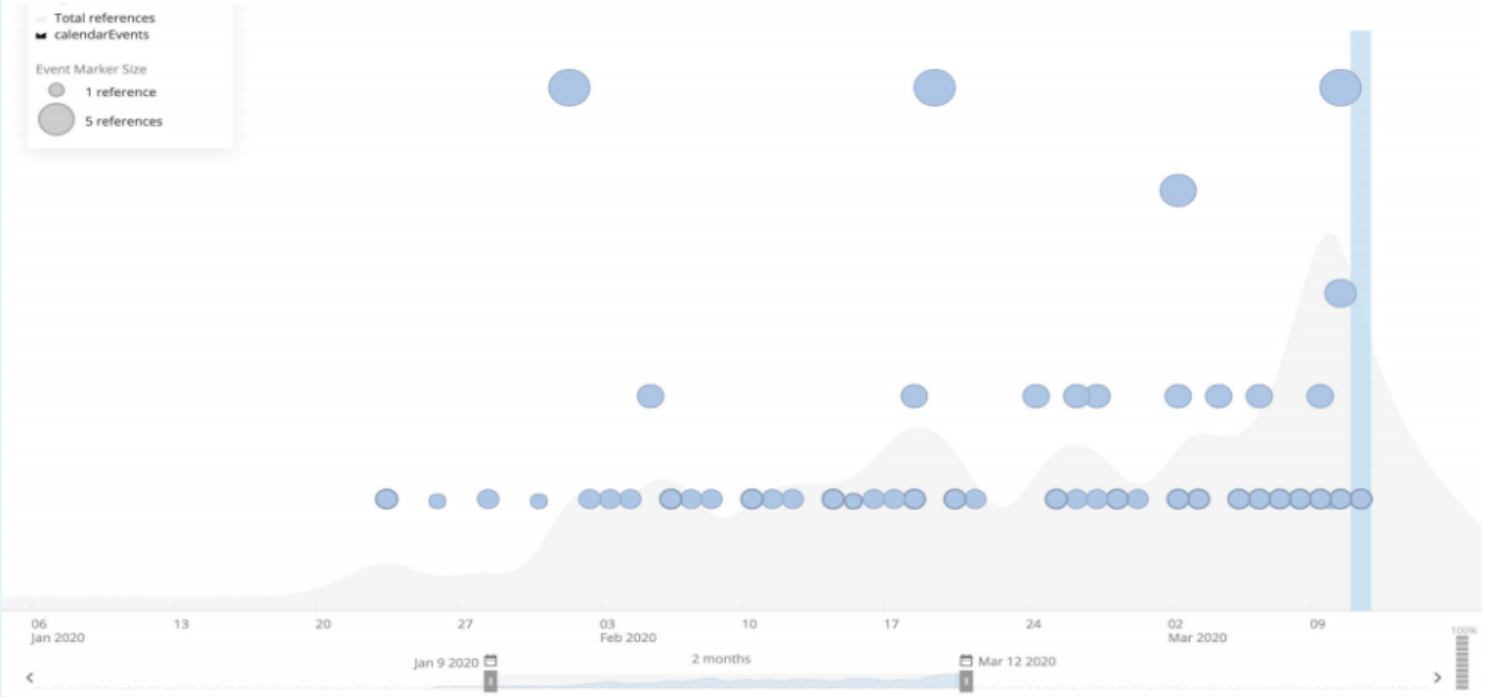
March 15 – BlackWater, a malware that uses Cloudflare Workers for C2 Communication

Crooks continue to abuse the interest in Coronavirus outbreak, now experts found a new backdoor called BlackWater that pretends to provide information about COVID-19.

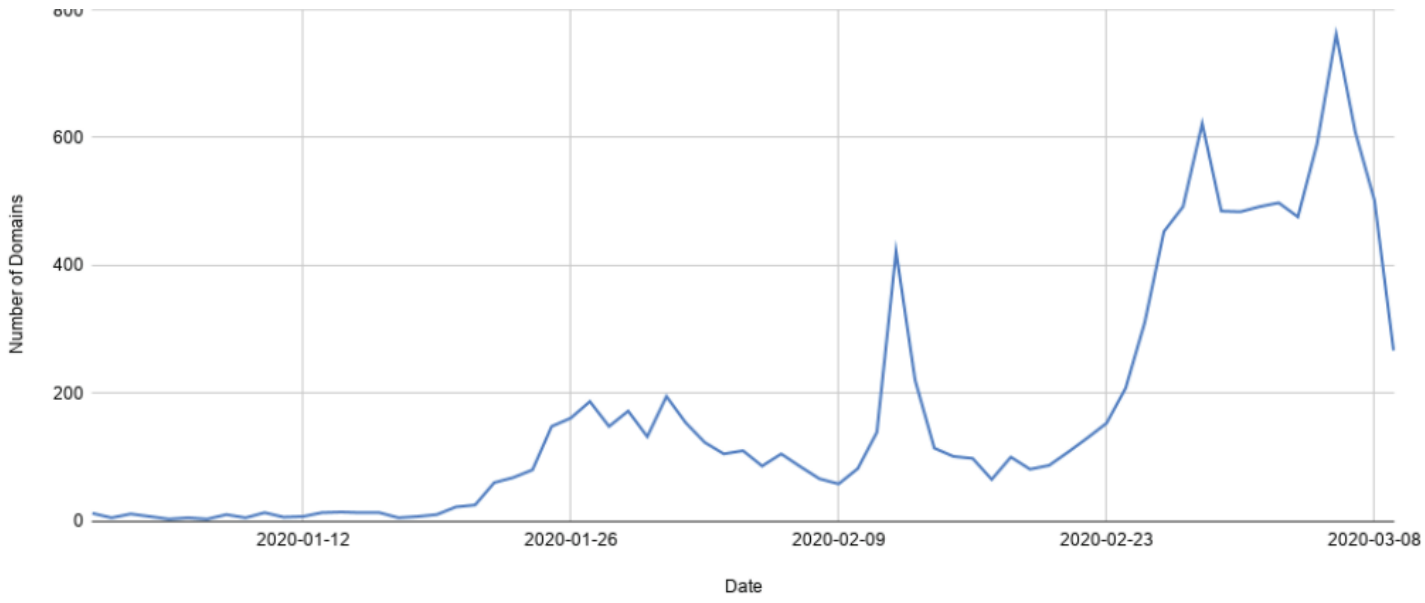
March 15 – Noooo, now Ancient Tortoise BEC scammers are launching Coronavirus-themed attacks

A cybercrime gang focused on Business Email Compromise (BEC) has started using COVID-19-themed scam emails in its attacks.

Evolution of the Cyber Attacks Related to the Exploitation of COVID-19 News.



Evolution of the number of domain names linked to COVID-19 created since December. Check Point points out that 50% of the domain names linked to the term coronavirus are likely to cause the intrusion of malicious software.



[3] https://www.recordedfuture.com/coronavirus-panic-exploit/

1.7 REFERENCES

- ✓ https://securityaffairs.co/wordpress/99744/hacking/us-health-and-human-services.html
- ✓ https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/
- ✓ http://feedproxy.google.com/~r/eset/blog/~3/D-6mwELGotQ/
- ✓ https://securityaffairs.co/wordpress/99682/cyber-warfare-2/coronavirus-themed-attacks.html
- ✓ https://blog.malwarebytes.com/threat-analysis/2020/03/apt36-jumps-on-the-coronavirus-bandwagon-delivers-crimson-rat/
- ✓ https://www.recordedfuture.com/coronavirus-panic-exploit/
- ✓ https://twitter.com/WebSecurityIT/status/1238877553642831872
- ✓ https://twitter.com/1ZRR4H/status/1239751485312970753
- ✓ https://twitter.com/LukasStefanko/status/1239826056103825408
- ✓ https://korii.slate.fr/tech/hackers-covid-19-coronavirus-cartes-emails-diffusion-virus-malwares-cheval-de-troie
- ✓ https://www.cert.ssi.gouv.fr/actualite/CERTFR-2020-ACT-002/
- ✓ https://www.cert.ssi.gouv.fr/actualite/CERTFR-2020-ACT-001/
- ✓ https://www.ssi.gouv.fr/uploads/2018/10/guide_nomadisme_anssi_pa_054_v1.pdf
- ✓ https://www.lci.fr/police/coronavirus-les-hopitaux-de-paris-aphp-victimes-d-une-cyberattaque-deni-de-service-de-hackers-2148857.html