Business as usual: Criminal Activities in Times of a Global Pandemic

gdatasoftware.com/blog/global-pandemic-remcos-tesla-netwire

The beginning of 2020 has been appalling for most parts of the world being affected by Coronavirus disease 2019 (COVID-19). This brought about a change in the everyday life of every individual in every country striving to sustain their daily tasks while simultaneously preventing further infection. Given this situation, businesses and schools have opted to transition to a ‘virtual setting’ wherein a job can be done remotely and school discussion as well as office meetings can be held via conference calls using applications like Zoom, Skype or Microsoft Teams. There has been a surge in demand for platforms for video and audio conferencing, chat and webinar solutions.

2018 FIFA World Cup Spam Email Sample

This upheaval created opportunities for cybercriminals, as they exploit these situations in executing their malicious intents. This is not the first time that cybercriminals have taken advantage of the current and significant events to lure more victims, as there were instances from the past years that shows how they utilize these happenings to spread malware. An example of which was the 2018 FIFA World Cup wherein cybercriminals created a fake FIFA partner website to gain access to victim's bank accounts and drop a malicious file into the victim's machine.

COVID-19 Related Phishing Emails

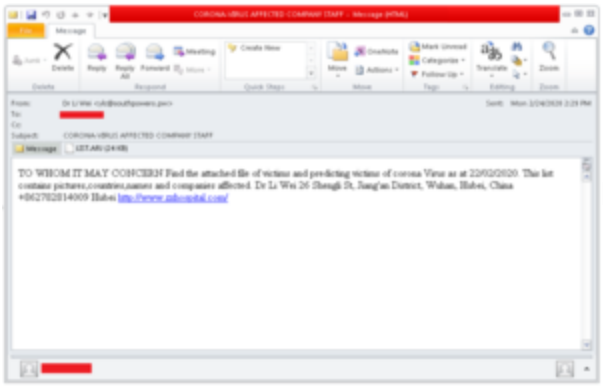
Copy of a legitimate infection heatmap, used by cybercriminals in their fake websites (July,2020)

With the rise in numbers of people infected by COVID-19 all over the world, cybercriminals work their way to increase the number of spam emails and phishing links related to COVID-19 proliferating in the cyberworld as well. They even made their cyberattacks more diverse in a way that they not only send spam emails with malicious attachments, but also created fake websites with fake COVID-19 related contents for victims to freely access like coronavirus-map[.]com(website is already unreachable at the time of writing). Some of these fake websites contain fake information regarding the current world statistics of COVID-19 cases. These fake websites often contain malicious cryptomining related contents known as cryptojacking which can harm the user's system by utilizing the system's resources to earn digital money such as Bitcoin for the malicious actor's gain without the user's consent.

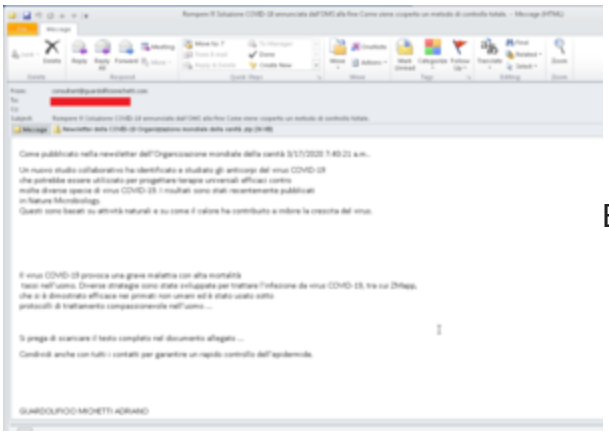
While some cybercriminals choose to explore new ways with their approach in pursuing their cybercrimes, some opt to carry on with the old ways like spam emails but with improved contents to make their attacks more successful.

Like the spam emails from 2018 FIFA World Cup, cybercriminals use and abuse COVID-19 as the subject for the spam emails that they were sending out. It is noticeable on the following two sample emails below with different contents and language used. It is one of the innovations that cybercriminals do to make their spam emails more tailored to their targets which increases the chance of a successful attack.

The first email is geared towards English-speaking individuals while the second email is aimed in targeting anyone who can understand Italian. At first look, it may seem that these two emails are different considering the language used, the subjects of the email, and the content of its message. But we can notice that both emails contain an attachment - *List.arj (24 KB)* and *Newsletter della COVID-19 Organizzazione mondialle della sanita.zip(36 KB)*.

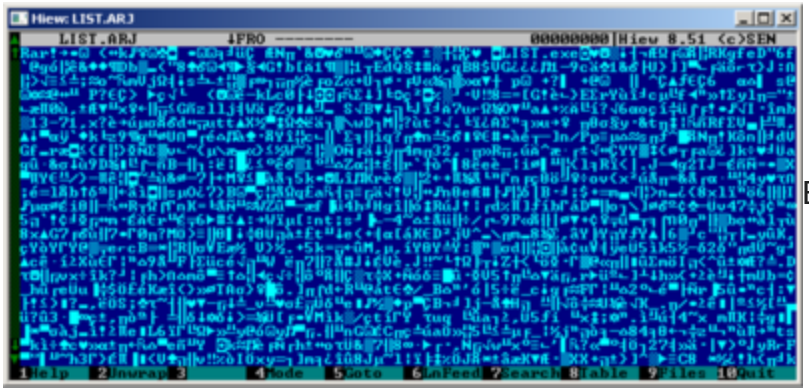


Example of a COVID19-related email campaign in English



Example of a COVID19-related email campaign in Italian

File attachments

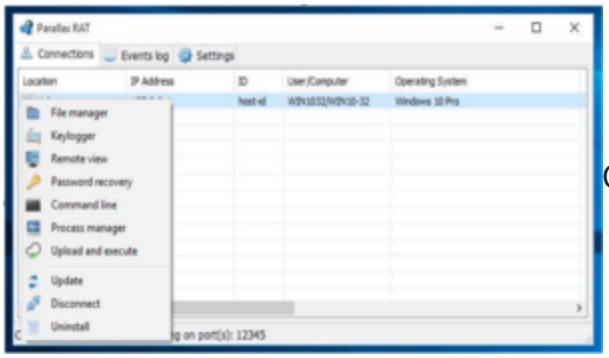


Email Attachment – RAR Archive

The attachment to the first email is said to be a list of the victims of COVID-19. However, upon analyzing the file, it can be easily identified as an archive that contains an executable file – LIST.exe. This is a red flag already as a file that claims to be a text file, is an archive that contains an executable file. The attachment from the second email looks like a usual archive, but also contains an executable file.

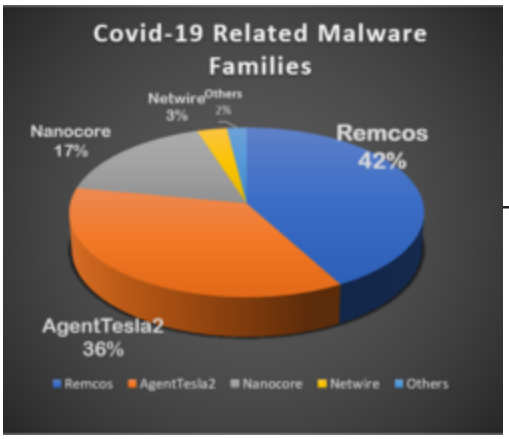
Further analysis shows that the malicious executable files from the extracted archives are files associated with a well-known malware family called GuLoader, that has been existing since way before COVID19. GuLoader is a known malware that downloads its payload from cloud services such as Google Drive and Microsoft Drives. It is then used to download a remote access trojan (RAT), a malicious program that includes a backdoor for administrative control over the target computer. In this case, considering that the files we analyzed came from two different emails with two distinct targets, the attachment files were identical, which both end up downloading a Parallax RAT.

Further analysis shows that the malicious executable files from the extracted archives are files associated with a well-known malware family that has been existing since way before COVID19: GuLoader is a known malware that downloads its payload from cloud services such as Google Drive and Microsoft Drives. It is then used to download a remote access trojan (RAT), a malicious program that includes a backdoor for administrative control over the target computer. In this case, considering that the files we analyzed came from two different emails with two distinct targets, the attachment files were identical, which both end up downloading a Parallax RAT.



Control Backend of the Parallax RAT

Parallax RAT is being considered as the “new RAT on the block” which had its first appearance in December 2019. It is a type of RAT that can work across all versions of Windows OS, capable of bypassing detections, stealing credentials, and executing remote commands like grabbing keystrokes and screenshots. This is a new RAT being offered as a MaaS (Malware-as-a-Service) and it has become a favorite amongst malware criminals as it is being sold in the black market for as low as $65 with a promise of 99% reliability for the service it provides.

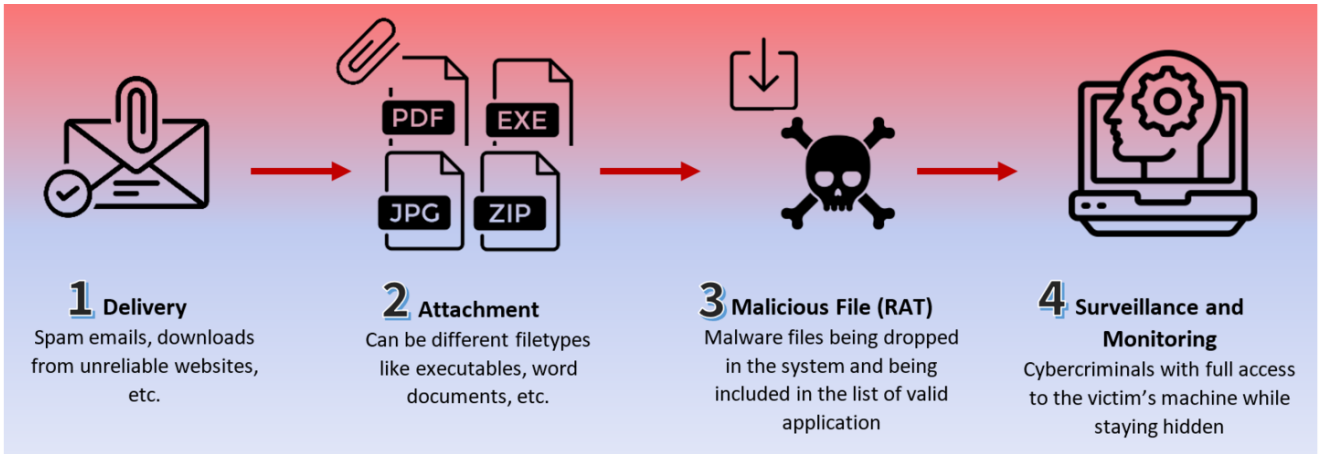


Telemetry Statistics of RATs utilizing Covid-19 related news to propagate

While checking our telemetry statistics for the past 6 months with 58,524 malware samples, aside from Parallax, there are several other malware families that leverages COVID-19 related news to entice a large number of potential victims to open attachments from unknown source. These malware families, most of which are RATs like Remcos, Nanocore, Netwire, Agent Tesla and other trojans, ranging from least destructive to most destructive, are unceasingly being distributed through various means like spam emails or as a downloadable file from deceitful websites.

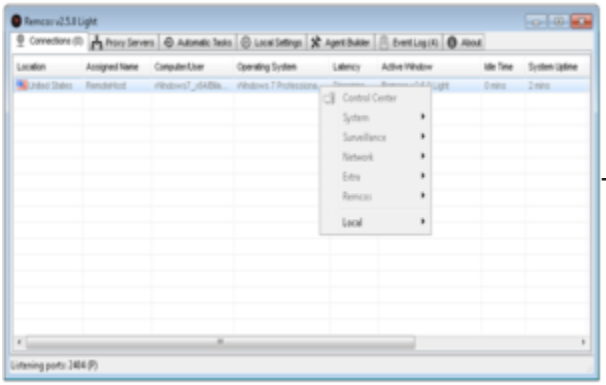
Typical malware during the pandemic

During the time of a global health crisis, RATs are the most commonly used tools found in malicious emails. Those RATs follow a distict pattern. We have taken a closer look at some of the proponents.



General Propagation Routine of RAT

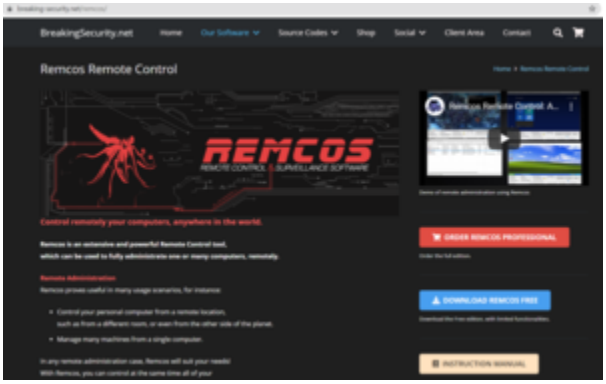
Remcos



The GUI of the Remcos RAT

Remcos was first seen in the wild at the 2nd half of 2016 being promoted as a commercialized RAT at the price of $58 to $389. It was first used in spear phishing campaigns targeting Turkish organizations. Currently, it is being sold by a German company called *'Breaking Security'*[2] and their website advertised it as a legitimate powerful remote control and surveillance software that can be used to access computers anywhere around the world.

The current trend for Remcos malware campaigns involved malware authors leveraging new and trending news worldwide for its phishing emails. Those mails usually have a pdf attachment. Once opened, this PDF contains a Remcos RAT dropper which runs a VB Script which in turn will execute the malware. To ensure persistence, a startup key is added to the registry.



Aliases:

- RemcosRAT
- Remvio

Other reference lines used in previous campaigns:

- "Re: nCoV: Coronavirus outbreak and safety measures in your city (Urgent)".
- Small Business Grant/Testing Centre Vouchers
- SBA Grant/Testing Centre Vouchers
- SBA Payroll Protection Program Status

AGENT TESLA


Agent Tesla Monitoring GUI

AgentTesla was first seen in 2014 and during the pandemic has been used in attacks that target energy companies. This may have been one of the effects of the pandemic where there is a low demand for oil. Before the pandemic, Agent Tesla the preferred toold for attacks against the oil industry.. Since Agent Tesla is also a commercial malware that can be bought on the Dark Web, it has a feature that allows you to monitor or customize the payload and monitor its targeted victims.

AgentTesla has been modified to be an advanced RAT that can also function as a keylogger and information stealer that can steal the victim's Microsoft outlook credentials and other saved passwords in web browsers such as Google Chrome, Internet Explorer and Mozilla Firefox.

What sets AgentTesla apart from other RATs is its added feature of stealing Wifi profiles. Malware actors uses this functionality in using WiFi as a mechanism to spread infection across different endpoints as well as using it as a gateway for future attacks on the victim's machine

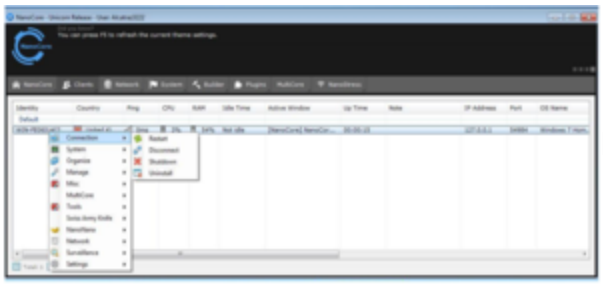
Aliases:

- AgenTesla
- AgentTesla

Other Email Subjects Used by AgentTesla RAT when sending Phishing Emails:

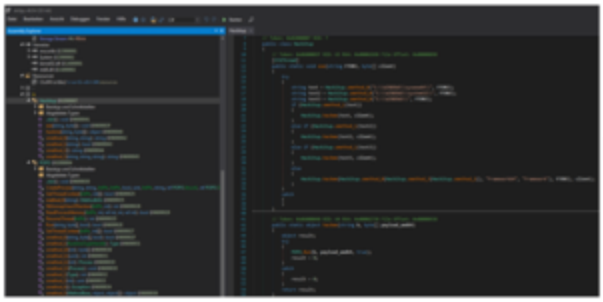
- URGENT INFORMATION LETTER: FIRST HUMAN COVID-19 VACCINE TEST/RESULT
- UPDATE Covid19″ Latest Tips to stay Immune to Virus!!
- "World Health Organization/Let's fight Corona Virus together"
- "Attention: List of Companies Affected With Coronavirus March 02, 2020".

NANOCORE



Nanocore RAT GUI

Nanocore was first seen in the wild in 2013. Its author Thoms Huddleston aka *AeonHacks*, admitted to developing and marketing NanoCore on the DarkWeb betweeen 2012 to 2016. He was arrested, but this does not stop the spread of his creation. It was kept alive and was updated since then. The new version of NanoCore was being sold on unterground markets for as low as $25. Some features included remote surveillance, reverse proxy connection, plugins and even customer support.



Netwire RAT Source Code

Nanocore is a sophisticated RAT that enables the attackers to gain access to details of victim's machine such as hostname and operating system. This in turn will let the cyber criminals carry out more malicious activities in the victim's machine like hijacking the web camera and microphone, steal confidential information and more.

What sets this RAT apart from other RATs is how difficult it is to detect. Unlike other RAT designed to run in a specific way, most of its behavior were similar with that of legitimate applications. Nanocore allows malware actors to just do anything they want to, once they gain access to a victim machine

Netwire

Screenshot of the cybercriminal's message to the victim

The NetWire RAT is a malicious tool that emerged in the wild during the first half of 2012. Netwire became famous as a RAT hidden in an IMG file (a file extension used by disk imaging software). Since then it has undergone various modifications that makes it remain stealthy as the years passes by. Like other RATs, NetWire RAT is offered commercially and can be easily purchased on Dark Web markets, which makes it accessible to malware authors. More information about Netwire here:

Aliases:

- Nancrat
- NanoCore

Other Email Subjects Used by Nanocore RAT when sending Phishing Emails:

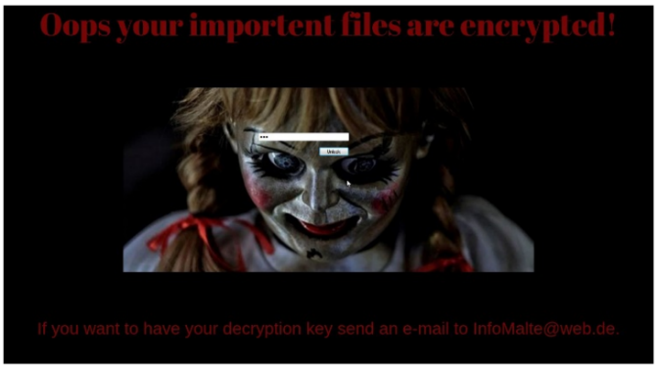
- “Covid-19 Urgent Precaution Measures”
- "Coronavirus Update: China Operations"
- "Fwd: Re: CoronaVirus Express Information"

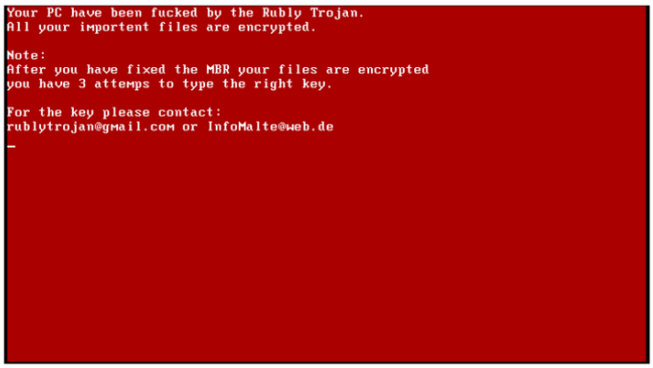
Various wipers / MBR-modifying malware

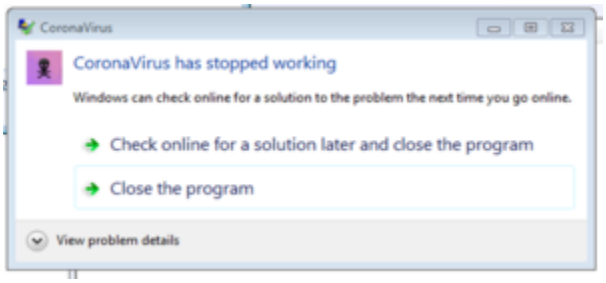
Wipers made their first appearance way back in 2008 when Narilam, a wiper malware, was used in targeting business and financial software in Iran. Wipers are malicious programs that cause data destruction on its victim machine. Unlike other malware whose aim is to achieve some sort of financial gain, wipers’ main motivation is to destroy all its targeted files/directory on a system or to replace the content of its target with a malicious content. As wipers evolved, malware authors decided to tweak the functionality of wipers and make these kinds of malwares to rewrite into master boot records (MBR).

Currently, a “Coronavirus.exe”[3] is spreading amongst Windows users. This malware’s name is very much connected to the COVID-19 pandemic. At first, this malware will drop several hidden helper files and batch files in a temporary folder in the computer system. Then, while still remaining unnoticed, it will disable Windows Task Manager and User Access Control and place itself inside the Startup registry. Lastly, upon reboot of the victim’s machine, a pop-up message box that tells victims to “not wast [sic] your time” because “you can’t terminate this process!” will be executed and won’t be terminated because the task manager was disabled. Meanwhile, the original MBR is being overwritten with a new malicious code.

Another variant of this MBR-modifying malware was discovered by one of our analysts[4] which at first may seem to be a simple screenlocker, but unknown to the user, is also a malware infecting the MBR.







This type of malware may not be as destructive as the previous malwares we have cited, but this can mislead the user into thinking that something is wrong with their system. One COVID-19 themed jokeware will prompt a message box that says “CoronaVirus has stopped working” when executed. This is very likely to cause alarm in many users and lead them into thinking that something is wrong with their computers, when in reality, all is well and the system was never in any danger to begin with. Jokewares may be the least of our worries involving COVID-19 malwares circulating the cyber world right now, but it is better to be safe than to be sorry. It may be mildly annoying to some, but has the potential to launch an organization into full “damage control mode” and cause some level of disruption.

Looking at the mode of delivery for malware, , there is one thing that stick out:
Even though malware authors take advantage of the current events around the world, most malicious files they commonly attach to spam emails are part of long-established and well-known malware families which have a high infection rate and enjoy broad support and a large user base within the underground community.

Aliases:

- NetWeird
- NetWire
- Recam

Other Email Subjects Used by Netwire RAT when sending Phishing Emails:

Malspam claiming to be from Dr Stella Chungong at the WHO

Conclusion

Just like in the real world, with proper hand washing, using mask and social distancing, we can prevent becoming a victim of these kind of attacks in cyberworld, through practicing and sharing appropriate cyber-hygiene too such as:

1. Avoid opening emails, downloading attached files, and clicking on links from unsolicited sender.
2. Disabling macro editing in your Microsoft office setting. You may refer to the instructions here.
3. Always have an updated AV for your protection.

While we are still in search for a vaccine that can cure COVID-19 in the real world, cyberworld on the other hand has its 'vaccine' against these malicious files which is the creation of advanced detections to identify possible threats and prevent further infection. Just like G Data's latest DeepRay Technology that uses artificial intelligence and machine learning in countering sophisticated attacks from cybercriminals. This 'vaccine' in the cyberworld is what will help every individual and organizations to thrive with their work and studies despite the change in their daily norms.

Indicators of Compromise

GuLoader

11a834cda4a55c8adb663fbcdd4b1f1018715dd737d3089a731b9840b77e5e76:

Detected as Win32.Trojan.Agent.YIZBCK

Remcos

73c07d1b17e8224996866c53ac95c9c327a1b88f78bef72852ca250016d06c33:

Detected as Trojan.GenericKD.30581682

DeepRay detection: RemcosRAT

Parallax

0a689281e5c807412fd9fca5f4a2d02f90e149da1ecc16179a09d88fa88eed74

Detected as Win32.Packed.Kryptik.WP03OZ

DeepRay detection: ParallaxRAT

NanoCore

2add0397fccd1c5cfe522530d20e672c47e6259ea625a3338845b1383272c23e:

Detected as Gen:Variant.MSIL.Lynx.52,

DeepRay detection: Nanocore

Netwire

cdd2e26792bd7ee81a6297d13dd514836778620c9bd96e79ae6ee26239c546b1:

Detected as Win32.Trojan.Netwire.C

AgentTesla

484aa9b06abff6b8b07695522b81fc70a8163f466b2aee2076481fab3e57840e:

Detected as Trojan.GenericKD.41932285

DeepRay detection: AgentTesla

Wiper/MBR-Rewriting Malware

fba31181ed1957e81c452fa1e860414d3a2bd2da470074a32f196f873a37d9ad

Detected as Trojan.GenericKD.33570587

Jokeware

6b61c223d618ead7ca78f4731a0128e30bf602bdfe8d940e442041486cb2fe76

Detected as Gen:Heur.Bodegun.1