EUROPOL
EC3 | European Cybercrime Centre

The Hague, March 2020

Intelligence Notification No 6/2020

CYBER BITS
Series: Trend

COVID-19 Cyber

What happened?

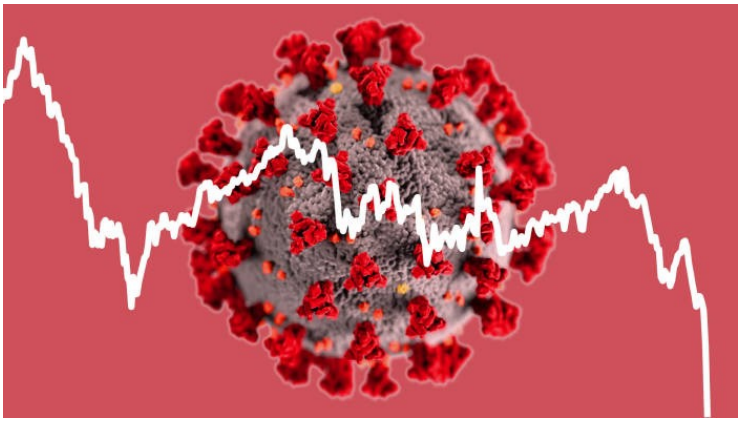

Image Source: https://www.ft.com/content/cbe2b35a-66d2-11ea-a3c9-1fe6fedcca75

As already reported in our latest Cyber Bit, criminals have been proficient in taking advantage of the tragedy the world is facing with the new COVID-19 pandemic.

As the coronavirus started spreading throughout the world, knowing no borders, so did the appropriation of cybercriminals of the phenomenon. The last months have witnessed an increase in phishing, fraud and a multitude of COVID-19 malicious domain registrations.

The cases mentioned below are not exhaustive by any means. At the time of writing, the type of cybercrime, from scams to malware dropped, related to COVID-19 is already too vast to be contained in the usual two pages of our Cyber Bits.

How does it work?

Phishing and malware distribution – Already as early as January, Emotet was being distributed via word documents allegedly containing health information related to COVID-19. These installed a PowerShell script that downloaded Emotet Trojan and infected users' machines. Other spam campaigns exploiting the fear of the virus have been seen delivering Trickbot information stealing malware. The email, supposedly from a World Health Organization doctor, pretends to be a list of precautions to prevent infections by the novel Coronavirus. Lokibot has also been distributed in a phishing campaign through a RAR file attachment using the extension .arj. The emails apparently originate from the Ministry of Health in China and uses Coronavirus as a bait. Once the machine is infected, it contacts a malicious IP address and extracts user credentials.

Another instance of AZORult, besides the one making use of the Coronavirus infections map, has also been distributed via emails containing Microsoft Office documents attachments built to exploit CVE-2017-11882 vulnerability. This particular threat seems to distribute the malware via an email claiming to advice on the impact of the virus in the shipping industry. One of the most recent cases analysed by researchers is a phishing campaign which distributes the Netwalker Ransomware. This ransomware usually targets enterprise and government agencies and has been recently disseminated via phishing emails with an attachment named "CORONAVIRUS_COVID-19.vbs".

EC3 Cyber Intelligence Team O31@europol.europa.eu PGP Fingerprint: C91D 6329 B144 4F38 E038 288E 2FF8 3886 021D 47DF

CYBER BITS

Series: Trend

Mobile Threats - Cybercrime appropriating the Coronavirus phenomenon has gone mobile with some instances of malware targeting Android devices. Researchers have found that an Android Ransomware called CovidLock, which claims to be Coronavirus information tracker, is being used to lock the victims' phones until they pay a ransom. Other types of scams and malicious apps targeting mobiles and making use of the topic have also been detected.

Advanced Persistent Threat Groups – APTs are also trying to benefit from the pandemic. An example of this are the Word documents making use of the WHO branding that contain C# backdoors and have been linked to Hades APT.

Other examples include Mustang Panda, a group that seems to be behind a campaign disseminating malicious executables via a file purportedly containing statements of the Vietnamese prime minister in relation to the virus. Amongst some of the most sophisticated, is what researchers' dubbed the Vicious Panda. An allegedly APT that by using information from the Mongolian Health Minister lured victims into sharing sensitive information. The RTF documents used to deploy the threat, were loaded with RoyalRoad exploit builder and aimed at gaining access to victims' computers and smartphones.

Another APT seems to have distributed spyware disguised in an app which claims to monitor eventual COVID-19 symptoms. However, it instead gathers sensitive information such as individuals' location or physical activity, being nothing more than a spyware in disguise.

A malicious Android application was noticed to masquerade as the most popular Coronavirus map. A software named SpyMax is being used in a long running campaign to spy people in Libya and which has now utilizing the pandemic to prey on Libyans. The aggressive spyware allows exfiltration of call and text logs as well as remotely activation of the mobile's camera and microphone.

Money mules - There have been reports in Canada and the US – but similar instances are certain to be replicated all over the globe – of money mules recruited for a supposed Foundation/NGO related to the Coronavirus. After being asked to complete a non-suspicious work related task, the individuals recruited are requested to process donations related to fighting the virus. They receive a specific amount into their bank accounts, from which they can keep a part, while the remainder should be taken to a Bitcoin ATM. Such schemes help criminals to launder money from fraudulent activities and hacked accounts.

Teleworking - Currently a vast majority of employees is working from home due to the outbreak of the pandemic. This situation has not passed unnoticed to cyber crooks who were fast in creating criminal occurrences to take advantage from it. Amongst the examples are the deployment of fake VPNs or getting access to mobile devices and personal devices which now might also contain company data.

Scams - Criminals are also taking advantage of the situation by resorting to the so-called non-delivery fraud. As the world faces an increasing demand for medical items in shortage, such as surgical masks or hand-sanitizer, so does the fraudulent advertisement of these products increase. Criminals request upfront payment for such items, with customers paying and not receiving the items. Other type of scams, such as home-test kits or investments and donations related COVID-19, have also been detected. An upsurge in products related to coronavirus has also been observed in Darknet markets. Products which claim to treat or cure infection by Coronavirus have been increasing swiftly since the beginning of the pandemic.

Extortion - While some news articles have announced that cybercriminals were willing to stop targeting healthcare services during the pandemic, there's already been a cyber-attack targeting a Czech Republic hospital, one of the major facilities testing for the virus, and causing computer shutdowns during the virus outbreak. Even though the reason of the attack has not been exposed, it is supposedly a case of ransom. In addition, only a day after promising not to target medical and health related facilities, the Maze ransomware group leaked sensitive data from a UK medical facility, that does research on medication and vaccines, after they denied to pay them ransom.

Additionally, in other extortion cases, cybercriminals are claiming that they know every detail and secret of their victims' lives by having infected their computers, and not only are they demanding a financial compensation in order not to disseminate sensitive information but are also threatening to infect the victim's family with Coronavirus.

Fake news - In the age of information overload, panic mixed with endless need for information is an explosive combination. From social media groups, email chains or APTs, there is an abundance of fake information dissemination. Recent reports have stated that some APTs are attempting to use fake news, "online trolls" and fake social media accounts to undermine other countries by spreading distrust and panic.

Privacy and Data Protection - Another worrisome aspect of the pandemic is related to Data Protection and privacy. Amongst some of the worrying reports are those of countries tracking their citizens in order to assess their health and possible development of infection. Other aspect of privacy to take into account is the amount of data big companies such as Facebook, Apple, Twitter, Amazon and Google hold. Not only do they know individuals' whereabouts, but also with whom they are spending time, as well as eating, exercising and sleeping habits. While some of this information could prove beneficial to understand where early outbreaks of the disease could happen and deploy eventual vaccines – and apparently some governments have already sent big tech companies requests for this type of data – loosening privacy boundaries in times of crises might proof difficult to retract when everything returns to normality.

Why do you need to know?

- There is need to develop awareness campaigns raising attention to the appropriation of the COVID-19 by cybercriminals. The fear this pandemic is causing, might make even usually cautious individuals to overlook dangers and be an easy prey of fraudsters and cybercriminals;
- Awareness needs to be raised on the fact that because an email is supposedly coming from a legitimate organisation is not necessarily trustworthy. In the course of the current pandemic the branding of legitimate health organizations have been heavily abused. Recipients of these communications should be cautious about opening attachments in these type of emails;
- The LE community and Internet Security companies should try to raise awareness to the vast array of malicious appropriation of the COVID-19 phenomenon;
- In times like this, where teleworking is becoming the norm, it is important for companies to ensure the operational security of every employee is sound and follows the recommended standards on remote connection security measures, such as company-approved VPN connections, OS and software up-to-date and a strong password policy;
- Concerning fake news, individuals should only follow and trust press statements of their national official representatives;
- Law enforcement and wider cyber security community should proactively exchange IoCs and malware samples related to the COVID-19 cyber malicious activities.

For more detailed information see the links below:

https://www.proofpoint.com/us/threat-insight/post/coronavirus-threat-landscape-update
https://www.politico.com/news/2020/03/18/big-tech-coronavirus-134523
https://securityaffairs.co/wordpress/99977/apt/apt27-abusing-covid-19.html
https://www.domaintools.com/resources/blog/covidlock-update-coronavirus-ransomware

EC3 would welcome feedback on this note. Please fill in the form through the link below making reference to the Intelligence notification No. on top of this CyberBit: https://ec.europa.eu/eusurvey/runner/o31_report_feedback

EC3 Cyber Intelligence Team O31@europol.europa.eu PGP Fingerprint: C91D 6329 B144 4F38 E038 288E 2FF8 3886 021D 47DF