How Coronavirus Helps Hackers Get Rich

COVID-19, SARS-CoV-2, the 2019 novel coronavirus (2019-nCoV) – these terms have suddenly supplemented everyone's vocabulary because they all denote the terrifying respiratory illness that's quickly accelerating around the world. With the total number of confirmed disease cases exceeding 1,450,000 at the time of writing, mankind is confronted with a global pandemic whose further impact is difficult to foresee.

What is cybercrime's response to this unprecedented outbreak? You guessed it – malefactors are busy perpetrating scams and malware distribution campaigns that take advantage of the panic around the crisis. The incidents below demonstrate how the real-world and cyber infections can be mixed up in a toxic surreal cocktail.

Phishing hoaxes with coronavirus fears at their core

People's desire to stay up to date with the infection statistics can fuel effective social engineering scams. Sounds wicked, but this is the way criminals are wheedling out users' personal information on a large scale. Phishing emails masqueraded as official alerts from healthcare organizations are used as bait to dupe recipients into clicking on booby-trapped links and giving away their sensitive credentials. In some cases, perpetrators leverage the 'infodemic' to defraud users of money without a second thought.

- **Fraudulent wire transfer requests from BEC scammers**

A cybercrime group codenamed Ancient Tortoise, which specializes in orchestrating business email compromise (BEC) attacks has been exploiting the disease outbreak to rip off businesses. This scam is a two-stage process. First, the crooks impersonating an organization's senior management contact employees from the finance department over email. They request what's called "aging reports" that contain details about unpaying customers, including their contact information and overdue invoices.

Once the felons obtain this database, they reach out to the people who owe money to the company. The email states that the COVID-19 calamity has caused the business to change banks and asks the recipients to wire funds to a different bank account. As a result, the payments go to a mule account instead of the correct one. Researchers from the Agari Cyber Intelligence Division who unveiled this BEC scam have traced this rogue account back to Hong Kong. The fraudsters then use it to complete the cash-out process.

- **Fake "Safety measures" emails**

A massive scam campaign doing the rounds amidst the COVID-19 pandemic uses deceptive messages camouflaged as an advisory from the World Health Organization (WHO). This wave has been up and running since early February 2020.

Users are instructed to click on the "Safety measures" link to download a document that supposedly includes the latest updates on disease prevention. However, it actually opens a spoofed email verification form requesting the would-be victim's password.

To feign legitimacy, this pop-up appears to be shown within the genuine WHO web page. The truth is that the scammers simply equipped their phishing page with a frame that displays the authentic website in the background. If the trick plays out and the user enters their credentials, the browsing session is automatically forwarded to www.who.int, the real site of the Geneva-based United Nations agency.

Upon closer inspection, a watchful person can identify a few giveaways in this hoax. First of all, the punctuation is poor and there are typos such as missing or extra spaces. Secondly, the landing page is HTTP rather than HTTPS – that's something a vigilant user will easily notice.

- **Pseudo alerts about new cases nearby**

One more social engineering stratagem in the wild revolves around bogus emails pretending to come from the U.S. Centers for Disease Control and Prevention (CDC). These messages mimic alerts generated by the organization's incident management system and claim to report the latest infection cases in the recipient's area. While thinking that they are about to view updated statistics for their city, users who fall for the scam and click on the embedded link end up on a phishing site that harvests their personally identifiable information (PII).

In contrast to the phony WHO notice described above, this ruse looks more trustworthy. The email appears to be based on actual CDC press release materials and doesn't have any spelling mistakes. Furthermore, the subject itself is more likely to pressure users into clicking the phishing link.

Malware distribution relying on COVID-19 panic

Not only are cyber crooks using the coronavirus scare to manipulate users into disclosing their personal info, but they are also spreading malware via malicious email attachments and links. The sections below will give you the lowdown on recent campaigns of that kind.

- **Spoofed health advisories pushing Crimson RAT**

To seize the moment in their very own shady way, the operators of the Crimson remote access tool (RAT) have recently unleashed a spear-phishing campaign with a flavor of state-sponsored espionage. Security analysts attribute this wave to a Pakistani hacking group known as APT36, or Transparent Tribe, which has reportedly performed a series of cyber-attacks against the Indian government and military facilities in the past.

In this scenario, the black hats impersonate Indian government officials, sending emails disguised as health advisories regarding the coronavirus. These messages contain malware-riddled attachments that may come in two different formats. Most of them are Excel documents that lure recipients into enabling malicious macros. Some of these items are Rich Text Format (RTF) files laced with the CVE-2017-0199 remote code execution vulnerability.

Either way, the payload is the Crimson RAT that starts collecting the victim's sensitive information surreptitiously. It captures screenshots, steals credentials as they are entered in a web browser, and retrieves different types of system information such as the list of running processes and antivirus software installed on the machine. The pest uses a custom TCP protocol to safely interact with its Command and Control server.

- **Ransomware authors follow suit**

Some unscrupulous distributors of file-encrypting ransom Trojans are aligning their campaigns with the new circumstances as well. The CoronaVirus ransomware is an example of this revolting cybercrime trend. This threat is doing the rounds via a web page mimicking the official site of a Windows optimization tool called WiseCleaner. Interestingly, the payload downloadable from this fake website additionally deposits the Kpot password-stealer onto the victim's computer.

Although the ransomware encrypts dozens of different file types, drops a ransom note with recovery instructions, and temporarily locks the screen with a warning message, it might not be the pivot of this attack. It uses a static Bitcoin address for payments, demands an unusually low ransom (0.008 BTC, worth about $50), and includes a political message in the lock screen. According to researchers, these oddities may be a clue that the ransomware only serves as a smokescreen distracting the user from the activity of the accompanying information-stealing Trojan.

A more shocking example of the ransomware foul play is the ongoing propagation of a strain called NetWalker. Its operators have recently started a coronavirus-themed phishing campaign to spread the malicious payload. The contagious emails contain an attachment named Coronavirus_COVID-19.vbs along with auxiliary code used to deploy the ransomware on recipients' computers.

- **AZORult threat spreading through a fake COVID-19 map**

Threat actors behind the AZORult info-stealing Trojan are distributing their infection by means of a bogus map that reflects the global coronavirus cases. The payload is a binary named Corona-Virus-Map.com.exe. When launched, it displays a replica of the official John Hopkins Coronavirus Resource Center, except that the data is rendered within an application GUI rather than a web browser. The dashboard looks convincing and pulls all the information from the genuine source in real time.

The catch is that while the user is viewing the stats, the malicious app spawns a number of additional EXE and DLL files and launches them in the background. This multi-pronged routine results in executing the AZORult Trojan that takes screenshots, amasses the victim's passwords, looks for cryptocurrency wallet details, and retrieves system information such as the OS version and hostname.

- **FormBook infection is quick to jump on the hype train**

In early March 2020, security researchers came across fake emails disseminating another info-stealing threat dubbed FormBook. These messages impersonate the World Health Organization and pretend to provide coronavirus updates. The attached ZIP archive cloaks an executable named MyHealth.exe. This file launches GuLoader, a dodgy application whose primary goal is to download other malware behind the scenes. When executed, it connects to a cloud-hosted resource and pulls in the FormBook malware.

The resulting payload easily circumvents traditional AV mechanisms because GuLoader incorporates the harmful process into the Windows application launcher (wininit.exe). In the aftermath of this complex attack chain, the info-stealer is all set to record the user's keystrokes, pilfer information saved to the clipboard, and gather data related to the victim's web browsing activities.

- **Remcos RAT gearing up for a rise**

Discovered in August 2019, a RAT codenamed Remcos was nowhere near the top cyber-threats for months. This changed in February 2020 when analysts stumbled upon its payload masqueraded as a binary called CoronaVirusSafetyMeasures_pdf.exe. The file was caught in the malware sandbox set up by the Yoroi threat intelligence company. Whereas it's difficult to say for sure how this toxic item is doing the rounds, the researchers think email is the most likely delivery channel.

The file drops a combo of the Remcos executable and a specially crafted VBScript object. The latter is tasked with triggering the RAT in the host environment. To maintain persistence on the contaminated computer, the malicious code creates a registry key that instructs the OS to launch the dubious process during startup.

When up and running, Remcos monitors the user's keystrokes and saves the harvested data to a file named logs.dat. The infection goes with a module that establishes a connection with its C2 server and thereby exfiltrates the stolen information at predefined intervals.

- **Emotet malware targeting Japanese users**

Emotet is a long-standing information stealer whose distributors took the opportunity and launched a Coronavirus-themed spam wave in late January 2020. The massive attack is geographically isolated to Japan. The fake messages pretend to come from local authorities and claim to report new infection instances in several areas, including the Tottori, Gifu, and Osaka prefectures.

The emails written in Japanese urge recipients into opening a Microsoft Word file to explore the alleged scope of the disaster in their region. Then, a notorious malware execution trick comes into play: the document doesn't display any intelligible content unless the unsuspecting user enables macros. This, in turn, invokes a PowerShell command that inconspicuously downloads the Emotet info-stealing Trojan onto the system.

- **Lokibot malware spreading like wildfire**

One more info-stealer called Lokibot is seeing a massive spike in distribution. In a recent campaign, its authors piggyback on COVID-19 fears by sending phishing emails camouflaged as an emergency regulation notice from China's Ministry of Health. The aspect that makes this hoax stand out from the rest is that it may be zeroing in on the enterprise. This can be deduced from the phrase in the email body saying, "for the safety of your industry."

The email arrives with a RAR attachment containing a batch file named "Emergency Regulation." Once opened, this item instantly triggers Lokibot and the culprit gets busy amassing user credentials. Finally, it reaches out to the Command and Control server and transmits the collected information to its operators.

A comeback of pharma spam

The current crisis entails favorable conditions for the growth of fake online drug stores. These sketchy services have literally risen from the ashes after a long-term hiatus. To promote shady pharmacies, malicious actors chose not to reinvent the wheel as they are primarily cashing in on the "good old" comment spamming.

To set these quandaries in motion, crooks leverage bots or scripts that inundate user comments on popular sites with hyperlinks leading to faux drug marketplaces. In addition to the "spray and pray" effect making people click on these links out of curiosity, this tactic is part of a smart SEO strategy. A plethora of keywords and phrases associated with the pandemic can boost website rankings in search results, which generates a greater number of leads and helps malefactors rake in more profits.

How to steer clear of coronavirus-related frauds

It's disgusting that cybercriminals are taking advantage of the COVID-19 threat to reach their moneymaking goals. Unfortunately, the black hats don't seem to care less, so users should watch out for these scams and treat various email-borne alerts with a certain degree of paranoia. The U.S. Federal Trade Commission (FTC) provides several recommendations in this context – here's a summary of these precautions:

- Abstain from clicking on links sent by unfamiliar individuals or organizations that claim to provide advice or stats regarding the disease.
- Use reputable resources such as the official WHO or CDC website to keep abreast of updates about the pandemic.
- Stay away from ads that offer vaccinations, keeping in mind that a cure has yet to be created.
- Don't donate in cash, by gift cards, or through wire transfers, especially if such a request comes over email. These "charities" are most likely scams in disguise.
- Ignore online offers to make a quick buck by investing in drugs that prevent or cure the infection.

Furthermore, to avoid malware such as adware, info-stealers, ransomware, or remote access tools camouflaged as benign email attachments or applications, use effective security software that identifies and proactively blocks suspicious executables.