# Cybersecurity Threats and How To Stay Safe During the COVID-19 Pandemic

## March 17, 2020

LCG-GLOBAL.COM
(832) 730-2850

RICHMOND, TX

Cyber Risk Management

| | | | |
|---|---|---|---|
| Govt. & Law Enforcement Trained | Veteran Owned | Unmatched Expertise | In business 10+ years |

# Table of Contents

**Dear Reader,**

In this modern age of the "Internet-of-Everything," the world has never experienced a pandemic like COVID-19. As we are collectively distracted by the global health crisis, cybercriminals are exploiting the situation in many ways. They prey on fear and urgency. They thrive in the chaos created by disruption to our work force.

LCG consumes an enormous amount of threat intelligence from dozens of sources each day as we help secure our Clients and protect our own infrastructure. Threat Intelligence is based on real-world observations, informs our decisions and is meant to be shared. This report contains highlights from some of the intelligence feeds of the last few days.

Our mission to protect LCG's Clients during times of uncertainty is uncompromising, especially in challenging times. We hope you find the information and safety tips here useful and that you will call on us to help without hesitation.

Respectfully,

**Andrew J. Frisbie**
Chief Information Security Officer

## HOW IS COVID-19 INCREASING CYBER-RISK?

- **Fear and Urgency** – Cybercriminals are preying on your fear and urgent need for news and supplies related to COVID-19. Attacks are frequently initiated through social engineering (phishing/spear phishing) and could lead to credential theft, financial fraud, ransomware and more.

- **Increased Attack Surface** – Government and employers are pushing employees to temporarily work remotely – outside of the fortress walls so to speak – creating opportunities to exploit people and resources like never before.

## A SUMMARY OF THE LATEST COVID-19 RELATED THREAT INTELLIGENCE

- **Fake Domains** – A significant spike in newly registered COVID-19-related domains has been observed. These domains are used to lure visitors to malware-infected sites or to further perpetrate social engineering tactics. While there are hundreds of new fake domain registrations here are just a few examples to illustrate the tactic:

coronavirusoutbreakmap[.]com, www.coronavirusoutbreakmap[.]com, corona-virus[.]healthcare, coronavirusprotectionmasks[.]org.[1]

- **Phishing Attacks** – A significant spike in COVID-19-themed phishing attacks has been observed and these attacks exploits the fearful mindset of recipients. Supply shortages (e.g. hand sanitizer, masks, etc.) foster a sense of urgency and create opportunities for threat actors to "meet the demand" by selling supplies. In reality, they take your money and don't deliver.

- **Use of Familiar Brands/Trademarks** - Social engineering tactics focused on gaining trust by leveraging brands such as the US Centers for Disease Control (CD) and the World Health Organization (WHO), as well as country-specific agencies and businesses such as FedEx and major airlines are being used to similarly trick unsuspecting and fearful recipients.

- **Sophisticated Attackers** - Nation-state attackers – Advanced Persistent Threats from China, North Korea, Russia and elsewhere - have been associated with a handful of cases that reference COVID-19. Such attackers have better skills and resources and their goal is often to silently infiltrate an organization, where they meticulously gather information, move laterally through the network in search of privileged accounts and sensitive information prior to executing a variety of attacks.

- **Malware** – The use of fake domains, social engineering and familiar brands is ultimately designed to get something valuable from you. Often, these techniques are also used to deliver malicious software, or malware, that facilitate the theft of information or fraud.

## CHALLENGES FOR COMPANIES AS WORKFORCE GOES HOME

Social distancing recommendations to combat the spread of COVID-19 are sending America's workforce home in droves. Below is a summary of the potential issues that companies will have to consider:

- **Sensitive Information** – Inside the corporation there are typically more controls in place to protect and monitor sensitive information such as intellectual property and trade secrets. While executives, managers and certain team members may have remote access privileges, it is likely that not everyone does. With the rapid expansion of the remote workforce companies will grapple with how to keep their critical information secure while expanding their footprint beyond the traditional perimeter defenses.

[1] Recorded Future, Capitalizing on Coronavirus Panic, Threat Actors Target Victims Worldwide (FR-2020-0312), Retrieved on March 16, 2020.

- **Strain on IT Staff** – IT teams are already short staffed and overburdened and now the prospect of having to send the workforce home – with connectivity to the office – may be overwhelming. Mistakes or oversights, particularly with respect to security, will increase.

- **VPN Security** – VPNs are devices or software that encrypts your computer's connection to the corporate office and they are essential to data security. Unfortunately, the patch window for VPNs (the time between discovery of a vulnerability and the time it is fixed by the company) is historically long, leaving the vulnerability exposed to exploitation. Further, employees typically access other corporate resources, such as email (e.g. Office 365) and other online portals without utilizing a VPN from home and insecure public networks.

- **Unmanaged Devices** – The remote employee may utilize a company-issued computer on a home network with dozens of other Internet-connected devices, including vulnerable Smart TVs. Unless the employee is technically savvy and cyber-aware, the patch window on personal computers is probably longer than desired. These unmanaged systems may be running outdated antivirus or none at all.

- **Lack of Monitoring** – Companies typically have no visibility into an employee's home network and may have no process in place for monitoring VPN connections or what the employee is doing while connected remotely to the company network. Further, most companies have little to no visibility into what the employee does with sensitive information that has been removed from the company's internal network.

- **Insecure Wi-Fi** – Home Wi-Fi if is often a "set-and-forget" service. Typically, home wi-fi broadcasts the network name (SSID) with descriptive information about the router and may be secured with a weak or default password – which are available online.

- **Skeleton Office Crews** – Vacant homes with unlocked doors are invitations to burglars. An empty office without monitoring of critical systems and data is no different.

## TIPS TO PROTECT YOUR COMPANY

The advice below is not novel in the cybersecurity space, but it deserves renewed focus as we all brace for the impact of increased cyber-attacks related to COVID-19:

### Avoid Being A Victim of Social Engineering In the Office Or At Home[2]

- **ALWAYS** check the email 'From' field to validate the sender. This 'From' address may be spoofed.
- **ALWAYS** check for so-called 'double-extended' scam attachments. A text file named 'safe.txt' is safe, but a file called 'safe.txt.exe' is not.
- **ALWAYS** report all suspicious emails to your Information Technology help desk.
- **ALWAYS** note that verify the domain name of the websites you visit or that are revealed in embedded links. For example, *www.microsoft.com* and *www.support.microsoft.software.com* are two different domains. (and only the first is real).
- **NEVER** open any email attachments that end with: .exe, .scr, .bat, .com or other executable files you do not recognize.
- **NEVER** "unsubscribe" - it is easier to delete the e-mail than to deal with the security risks.
- **NEVER** click embedded links in messages without hovering your mouse over them first to check the URL and verify the domain is safe/secure.
- **NEVER** respond or reply to spam in any way. Use the delete button.

[2] Tips from KnowBe4; LCG provides KnowBe4 security awareness training as a managed service for Clients.

## Prepare for Reduced Personnel In the Office

- If you do not have a **Business Continuity Plan**, make one and ensure everyone understands their role.
- **Test remote access** to ensure it works in the event your building closes or is completely vacated.
- Review the safeguards in place to ensure the **security of your sensitive data**.
- If possible, **monitor access** to the network, VPN usage and to systems that store your critical data.
- To the extent possible, restrict remote access connections to the resources needed and avoid network-wide access.
- Have a backup plan in the event your **IT team gets sick or incapacitated** (ensure that more than one person has the ability to perform all IT functions).
- Ensure that systems used to process **payroll and accounts receivables** are secure and accessible to the right people remotely.

## Bolster Your Home Office Defenses

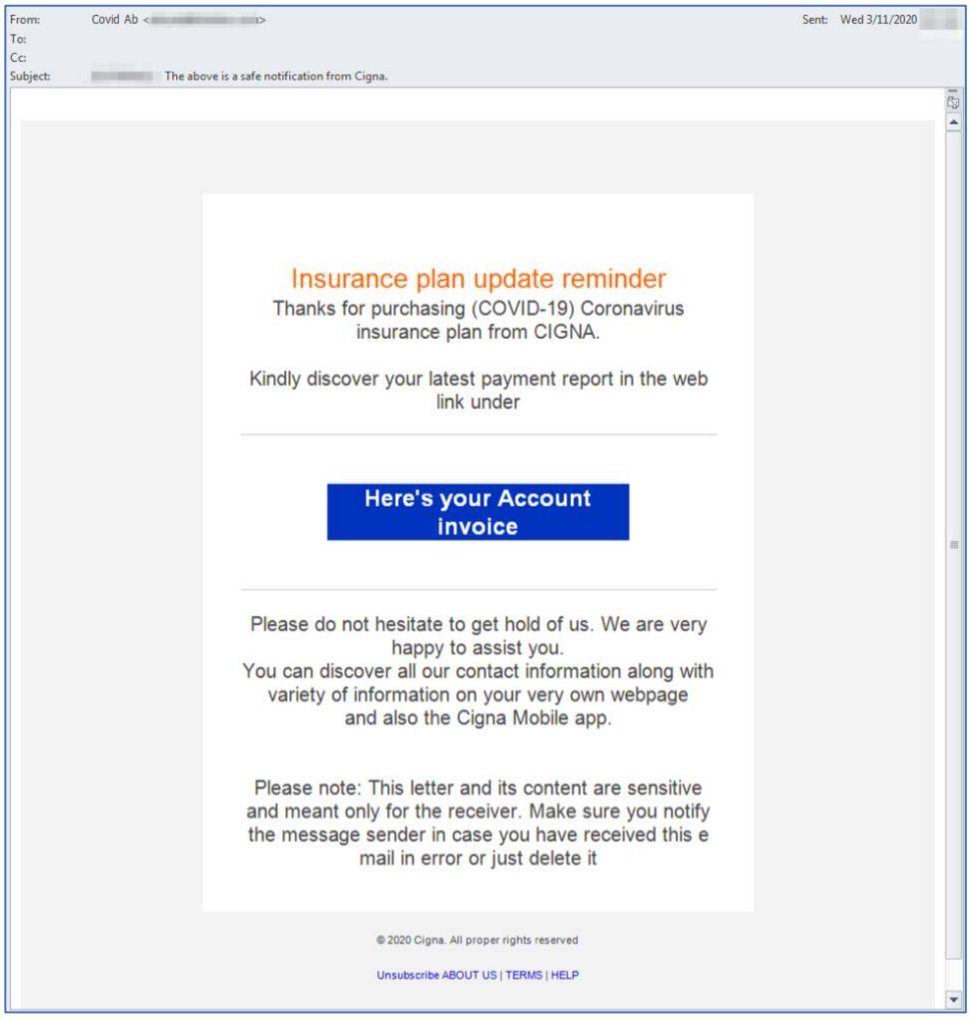
- **RESET** your modem or router password to a custom, strong password.
- **BE AWARE** that the default password or password-bypass PIN code might be affixed to the back or bottom of your router.
- **USE** a password manager (e.g. LastPass, Password1, Dashlane) to securely create and store your passwords.
- **HIDE or CHANGE** your Wi-Fi network name (SSID) to something non-descriptive. While you're at it change the name of your iPhone to something non-descriptive so you are not broadcasting your name and device type to everyone in the coffee shop or airport.
- **ENABLE** WPA2 encryption on your Wi-Fi network.
- **ENABLE** a Guest network at home so you can keep your home network isolated.
- **PATCH** your home devices regularly by setting the operating system and applications to automatic updates.

- **USE** multi-factor authentication to access all online portals and corporate resources.
- **USE** next generation anti-virus software that is smart enough to detect/block advanced attacks, ransomware and polymorphic malware.
- **USE** a VPN whenever you are connecting to work resources or personal financial websites.
- **USE** a VPN whenever you are in the coffee shop (public Wi-Fi), including on your Smart phone.
- **SEPARATE** your IoT devices (such as Smart TVs, appliances, etc.) onto a different network if your router allows it - or buy one that does.
- **ENABLE** Windows Defender on computers running the Windows 10 operating system.
- **INSTALL** a firewall appliance between your home network and your modem/router.
- **USE** an app (e.g. Fing) on your Smart phone to quickly scan and identify all of the devices on your home network. Track down anything suspicious.

# SEE IT FOR YOURSELF – A FEW EXAMPLES OF COVID-19 RELATED MALWARE

## March 12, 2020 – Healthcare Insurance Theme Delivers Malware

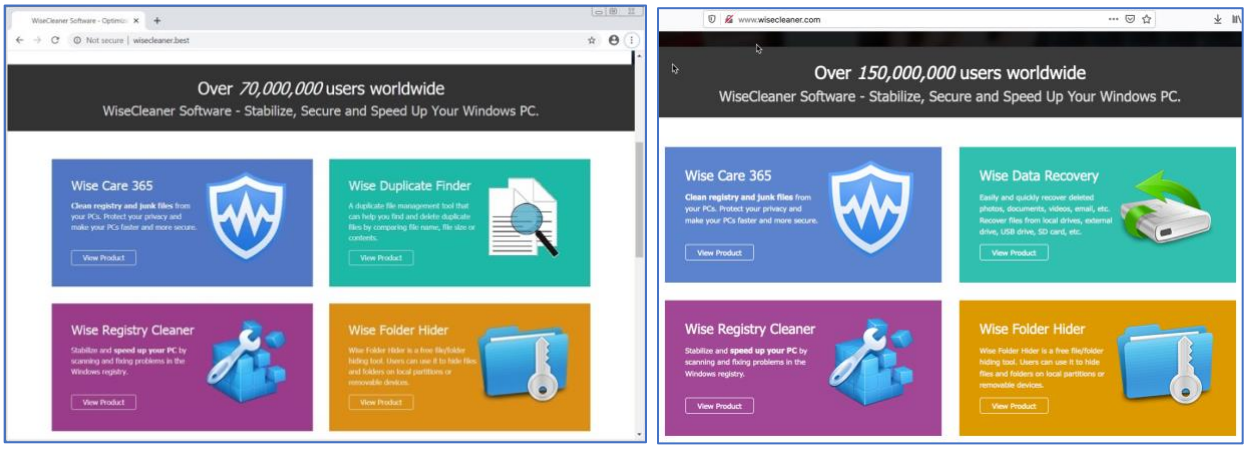
Known malware known as *Hancitor* has been observed using a coronavirus Insurance healthcare provider theme. The attack follows this sequence: 1) Recipient clicks on a click from a malicious email, 2) Link leads to another URL that returns a zip file, 3) malware is extracted from the zip file and installs on the victim system.[3] While the example below utilizes a CIGNA-branded insurance healthcare theme, as you can imagine, it could be modified to represent any provider.




[3] https://isc.sans.edu/forums/diary/Hancitor+distributed+through+coronavirusthemed+malspam/25892/

## March 13, 2020 – Impersonated Website Delivers Coronavirus Ransomware

A new ransomware called CoronaVirus is has been distributed through a fake web site pretending to promote the legitimate system optimization software and data recovery software called *WiseCleaner*.[4] The fake website was found to be almost an exact replica of the real thing. The fake website is used to distribute the *CoronaVirus* Ransomware and the *KPOT* information-stealing Trojan. While KPOT has been around for years, the new ransomware was discovered by MalwareHunterTeam.[5] *KPOT* aims to steal your banking passwords that it harvests from browsers, gaming apps and cryptocurrency wallets. The ransomware encrypts your data.

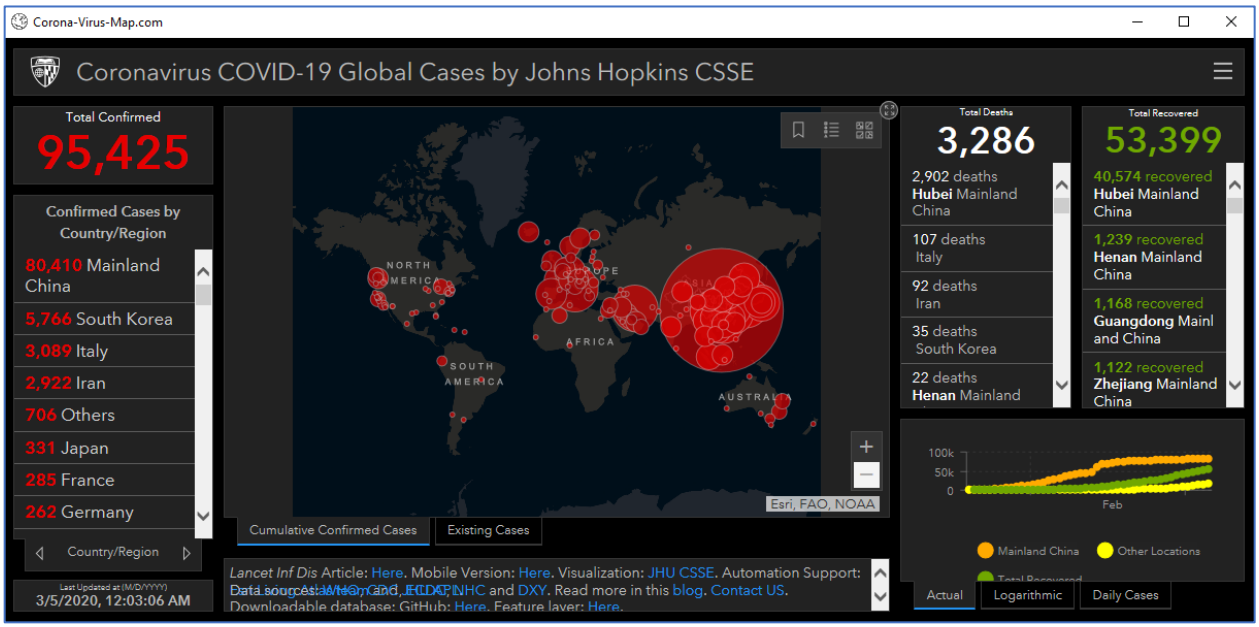



**LEFT**: Fake site, wisecleaner[.]best[6]; **RIGHT**: Real site, wisecleaner[.]com

[4] https://www.wisecleaner.com/
[5] https://twitter.com/malwrhunterteam
[6] Photo retrieved from https://www.bleepingcomputer.com/news/security/new-coronavirus-ransomware-acts-as-cover-for-kpot-infostealer/

## March 16, 2020 – Weaponized Virus Mapping Software Delivers Malware

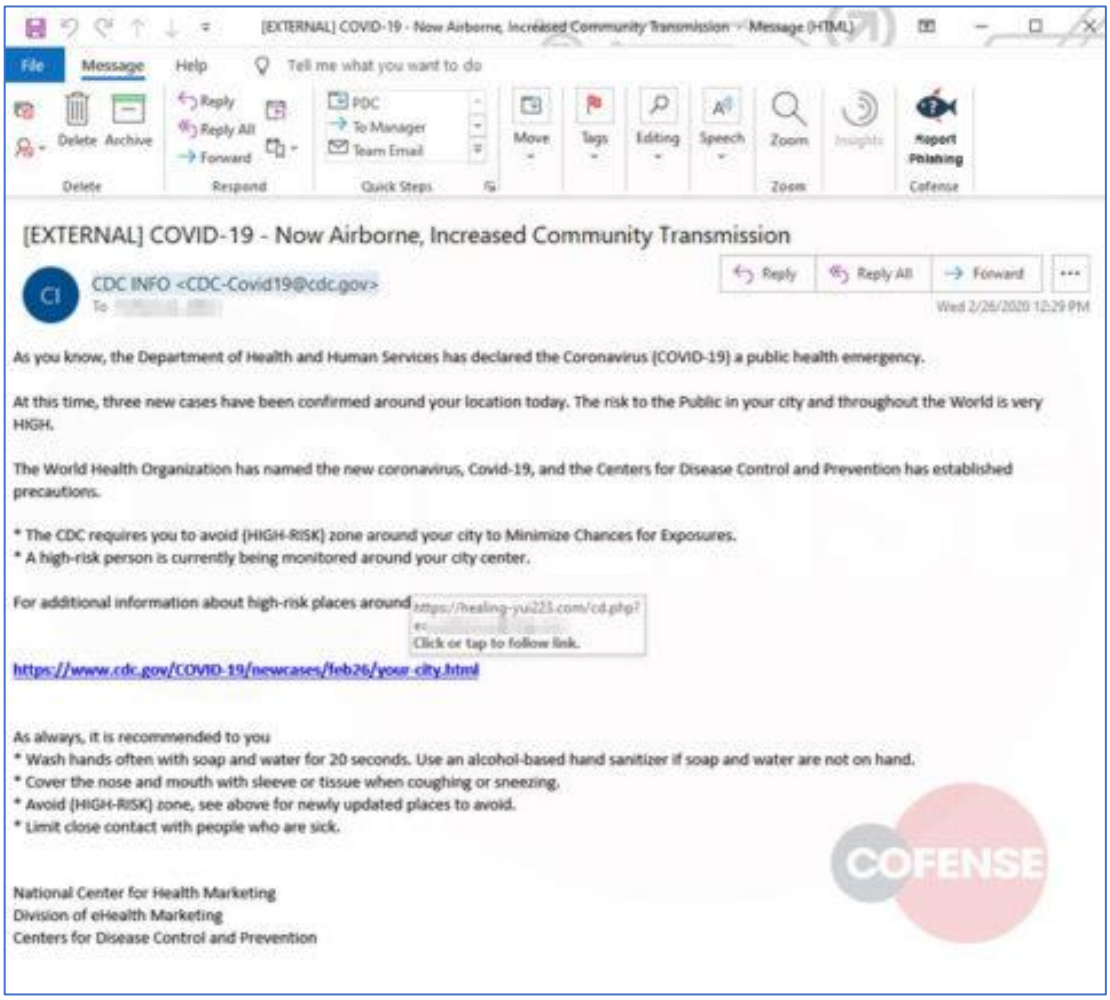
Malware called *AZORult* was used to weaponize a coronavirus mapping software in order to steal credentials such as usernames, passwords, credit card numbers and other sensitive information that is stored in the users' browser.[7] Attackers can use this information for many other operations as well, such as selling it on the deep web or for gaining access to bank accounts or social media. While *AZORult* has been around for a while, there is also a variant of the *AZORult* that creates a new, hidden administrator account on the infected machine in order to allow Remote Desktop Protocol (RDP) connections.




[7] https://blog.reasonsecurity.com/2020/03/09/covid-19-info-stealer-the-map-of-threats-threat-analysis-report/

## March 3, 2020 – CDC and Microsoft Emulated in Phishing Campaign To Steal Credentials

CoFense Phishing Defense Center (PDC)[8] discovered a new phishing campaign that preys on Coronavirus fears to get recipients to click on a malicious link from the Centers for Disease Control (CDC) in a Microsoft® branded email. In fact, the email did not originate from the CDC and the link, which purports to contain safe havens from airborne COVID-19, is unsafe. An examination of the email header (not shown) revealed that the domain name was manipulated to show "cdc.gov) despite having originated in the UK. The attack redirects the victim to a credential phishing site of Japanese origin.




[8] https://cofense.com/threat-actors-capitalize-global-concern-coronavirus-new-phishing-campaigns/

## HOW LCG CONTINUES TO DELIVER CYBERSECURITY

LCG is a nimble company and most of our services are delivered remotely, including:

- Risk Assessments
- Policy review
- Cybersecurity program design
- Vulnerability Assessments
- Penetration Tests
- Security Awareness Training
- Endpoint Detection and Response (EDR) deployment and monitoring
- SIEM deployment and monitoring
- Intelligent Data Loss Prevention.
- Virtual CISO services
- Forensic analysis (insider data theft, misconduct, malware analysis, etc.)

Incident response typically requires an onsite presence to triage the crisis and ensure continuity of operations for our Clients. Our commitment to Clients who need incident response services during this period of heightened awareness is:

- Conduct an internal evaluation of our responders, using guidelines published by the CDC and other leading health agencies, to determine if they are healthy to travel and to ensure the safety our Clients.
- Discuss the health status of the affected location to ensure the safety of our responders.
- Follow recommended guidelines for social distancing and hygiene while onsite.
- Minimize the time onsite by setting up remote access services for use after the cybersecurity crisis is abated.
- Always respond with essential staff only (we do this on every response to manage cost and efficiency).

**Whether you need proactive cybersecurity services or incident response, we are ready to go.**

**Call (832) 730-2850 Today.**
**https://lcg-global.com**