CYBER DEFENSE INTELLIGENCE CENTER

April 20, 2020

COVID-19 related Cyber risks are significantly increased as a result of the pandemic

SCOPE: This intelligence briefing affects all Industry Segments and Organizations.

Prepared by the Cyber Defense Intelligence Center Analysis Team.

Cyber Defense Intelligence Analysts have identified several areas where COVID-19 has been leveraged by Cyber Actors to target individuals and organizations. The attacks have been increasing significantly since the onset of the pandemic.

Key Cyber Actors

Our analysts have determined that there has not been a substantial change in the active threat actors during the pandemic. The table below represents the various categories of Cyber Threat Actors and high-level details about the different actors. (While some of these actors have been identified as running specific COVID-19 Ops, such as APT41 from China, not all of these have been attributed to attacks)

Cyber Threat Actor	Description	Motivation	Techniques	Targets	Uses of Stolen Data	Key Players
Cyberterrorists	Extremist groups or nonstate actors using cyber techniques to intimidate, coerce, or influence an audience; force a political change; cause fear or physical harm	Gain support for and deter opposition to a cause; carry out dictates of an ideology	Cause kinetic damage: destroy or disrupt critical infrastructure or systems; loss of life	Determined by actors' ideology	Disrupt critical infrastructure via cyberattack; Change prescription or allergy information, switch or delete medical record; further a campaign on a particular target	Hamas al-Qaeda Algeria's Armed Islamic Group Hezbollah Egyptian Islamic Group Sri Lankan Internet Black Tigers White supremecist Groups
Hacktivists	Bring awareness to a cause (political, economic, social); exercise free speech (e.g., "lulz")	Ideological activism; disruption of services or access	Steal and leak sensitive, proprietary, or classified information; conduct DDoS on websites or services	No one type of target	Gather personal information of a specific target; publicize a breach to highlight how vulnerable a particular organization is	DkD[ ] [ ] Anonymous WikiLeaks AnonCoders DCLeaks Decocidio#Θ
State-sponsored actors	Receive direction, funding, or technical assistance from nationstates; highly sophisticated and often use the mostsophisticated methods (e.g., zero-day vulnerabilities); targeted and persistent	Advance interests of their nation-state; further political agenda	Conduct intelligence, surveillance, reconnaissance, espionage; employ watering-hole attacks; exfiltrate data (e.g., intellectual property); degrade or destroy technical components; conduct targeted attacks	Other nation-states, defense contractors, technology sector, and critical infrastructure; (rare) banks or cryptocurrency wallets	Build profiles of possible targets for follow-on targeting, exploitation, or espionage campaigns; use personal, financial, or medical information as leverage to gain other types of intelligence	**China** • APT14 (Anchor Panda) • APT19 (Deep Panda) • APT27 (Goblin Panda) • Mustang Panda • APT4 (Samurai Panda) • APT41 **Iran** • Clever Kitten • Helix Kitten (APT34) • Refined Kitten (APT33) **North Korea** • Stardust Chollima (APT38) **Pakistan** • Mythic Leopard (APT36) **Russia** • Cozy Bear (APT29) • Fancy Bear (APT28) • Venomous Bear • Voodoo Bear
Cybercriminals	Access personal, financial, or health data to monetize it	Financial gain; power	Use crimeware (e.g., exploit kits, "script-kiddy" tools); rely on already known vulnerabilities, phishing, and spearphishing; smashand-grab	Data repositories (e.g., banks, retail companies, health care) that can be monetized; cryptocurrency wallets	Use credentials (username/password combinations) and harvest contact lists for phishing attacks; exploit password reuse; conduct identity theft, tax, or medical fraud	• Cobalt Spider • Dungeon Spider • Mummy Spider • Salty Spider (Sality) • Wicked Spider • Organized Crime Groups • Individual Criminals

Types of Attacks

Threat actors have been leveraging key attack vectors related to the COVID-19 pandemic.

Phishing Attacks

Phishing is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers. Attackers are using fear and uncertainty to entice users into clicking on emails and false links. They are counting on users being distracted and not thinking clearly. This requires all users to keep phishing top of mind. It is important for Information Security teams to continually communicate and educate.

Threat actors have continued using Phishing as a primary attack vector. OSINT sources have identified ~136k newly created COVID-19 related domains since December 1, 2019. The attacks have been used to deliver malware, ransomware and misinformation. Our analysts have seen an increase in the use of different Phishing mediums. Attackers are also using Social and SMS(Texting) as delivery mechanisms in addition to traditional email.

Misinformation / Disinformation Campaigns

Our analysts have seen a very large increase of social media campaigns specifically crafted to spread misinformation and increase paranoia around the Coronavirus pandemic. Threat actors are currently running multiple, ongoing misinformation campaigns across all social media platforms (ex: Twitter, Facebook, Instagram).

These campaigns are intended to create fear and confusion in society. This can lead to users conducting searches that lead to an attack or making misinformed decisions that put the users themselves at risk. Actors are using social platforms to:

- *Increase fear*
- *Sow discord*
- *Create confusion*
- *Divide citizens*
- *Slow community response*

Social Engineering

Cyber actors have increased Social Engineering activities over the past few weeks. There has been an increase in attempts to lure unsuspecting victims into going to malicious sites, clicking on malicious links, or providing personal information over the phone under the auspices of COVID-19. Many of these scams attempt to impersonate legitimate organizations, such as the Center for Disease Control, the World Health Organization, COVID relief organizations and Government agencies. The actors are offering fake informational updates and even promises of access to vaccines or economic relief in exchange for a fee or information.

The attacks have been very diverse and have included the following attack vectors:

Digital Attacks

- *Phishing/Spear-phishing*
- *Social Media Deception*
- *Pretexting*
- *WaterHoling*

Phone Based Attacks

- *Smishing*
- *Vishing*

Network vulnerability exploits

The change in work paradigm during COVID-19 has led to most organizations moving their workforces to a remote work model involving access from users home networks over some type of secured channel such as VPN. This change has dramatically increased the attack surface of these organizations. It has also increased the risks. Work devices that staff use at home could become more vulnerable if the systems are not properly updated to fix vendor vulnerabilities. The users are also connecting over their home WiFi networks which may or may not be configured using proper security controls.

There has also been an increased use of Cloud and SaaS based tools by end-users. These tools can be video conferencing tools such as Zoom or WebEx, File storage tools such as Dropbox or OneDrive, or various other collaboration tools. While these tools are very helpful in improving the user's productivity, if they are not properly configured they could result in a breach of confidential data.

Cyber actors have also been targeting end-user personal accounts such as Netflix, Apple, Bank Accounts and Home automation accounts (i.e. Ring, Nest, etc) to compromise account credentials. Many users have the habit of re-using account credentials for sake of convenience. Compromising these credentials can allow the attackers to access other accounts and potential compromise corporate networks.

Societal disruption

Domestic Violent Extremists (DVE) and radical political groups have been leveraging the COVID-19 pandemic to spread their propaganda and hate. These groups have been using social media platforms such as Facebook, Twitter and Instagram to conduct misinformation campaigns. These campaigns have been sowing social discord, spreading dangerous conspiracy theories and encouraging dissident behavior related to "Stay-at-home" orders and government programs.

Financial Scams and Fraud

Financial scams (invoicing and payroll scams) are always a threat, but during this pandemic, criminals are using fear and distraction to make users fall for their pandemic specific schemes.

It is vital that users not trust any offers or requests tendered via email or phone without verifying the person, organization and offer. All corporate transactions should be validated by an alternate means and not through an email.

Criminals are running different scams:

- *Charitable contributions scams*
- *COVID-19 financial relief scams*
- *Airline carrier refunds*
- *Fake cures and vaccines*
- *Fake testing kits*
- *Government agency scams*

Economic disruption

Denial of Service Attacks are where an attacker leverages a bot network to direct traffic at a specific target to overload the device or network. The U.S. Health and Human Services Department suffered a cyber-attack on its computer system. People familiar with the incident called a campaign of disruption and disinformation, aimed at undermining the response to the coronavirus pandemic. This may have been the

work of a foreign actor. These types of attacks can take a corporate network offline leading to a complete loss of productivity.

Cyber actors DoS attacks against networks and VPN's to:

- *Impact economic productivity*
- *Slow pandemic response*
- *Create chaos in society*
- *Distract Security teams as part of larger attacks*

Mitigations

The challenges created by the COVID-19 pandemic require Organizations, Security Practitioners and End-users to exercise additional caution to minimize the new risks and not become a victim. Cyber Defense Intelligence Analysts have recommended the follow actions to protect your assets and users from attack.

Use MFA Everywhere
All personal accounts that support MFA should be using it, including personal accounts like Netflix, ITunes, Ring, Etc., and passwords should not be reused on any accounts.

Secure Home Wifi networks
Home wifi routers should be configured to use WPA2 encryption and a strong password should be used for setup and complex passwords should be used for accessing the configuration. Guidance should be provided to end-users on how to accomplish this successfully.

Limit Access to Work Devices
Work computers and devices should be restricted to only work activities and not used by other family members. Educating users and establishing proper policies is very important.

Ensure End User Security Awareness
The prevalence of Phishing scams and campaigns means that users need to exercise additional diligence. It is important that Security training continues to reinforce good security behaviors.

Coordinate with Users on new Tools
It is very important that users not just "find" new tools to perform work activities without checking with IT to understand the risks that may be created. IT and InfoSec teams should assess tools and ensure that the configurations are secure before users begin to utilize the new technology.

Continue Proper Security Hygiene
InfoSec and IT teams must review all security hygiene practices (Patch management, Vulnerability Management, Identity and Access Management) and ensure that they will continue to work in the remote model.

Increase monitoring of new attack surface
InfoSec teams should assess their current tools and ensure that they are capable of identifying threats and attacks originating on the remote devices.

Inform users of threats
InfoSec teams should be communicating new threats with end-users as they identify them. The InfoSec teams should closely monitor OSINT (OpenSource Intelligence) sites such as CERT, FBI, SANS, RiskIQ and others and a daily basis to stay information of new threats.