National Cyber Awareness System:

AA20-099A: COVID-19 Exploited by Malicious Cyber Actors

04/08/2020 08:00 AM EDT

Original release date: April 8, 2020

Summary

This is a joint alert from the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC).

This alert provides information on exploitation by cybercriminal and advanced persistent threat (APT) groups of the current coronavirus disease 2019 (COVID-19) global pandemic. It includes a non-exhaustive list of indicators of compromise (IOCs) for detection as well as mitigation advice.

Both CISA and NCSC are seeing a growing use of COVID-19-related themes by malicious cyber actors. At the same time, the surge in teleworking has increased the use of potentially vulnerable services, such as virtual private networks (VPNs), amplifying the threat to individuals and organizations.

APT groups and cybercriminals are targeting individuals, small and medium enterprises, and large organizations with COVID-19-related scams and phishing emails. This alert provides an overview of COVID-19-related malicious cyber activity and offers practical advice that individuals and organizations can follow to reduce the risk of being impacted. The IOCs provided within the accompanying .csv and .stix files of this alert are based on analysis from CISA, NCSC, and industry.

Note: this is a fast-moving situation and this alert does not seek to catalogue all COVID-19-related malicious cyber activity. Individuals and organizations should remain alert to increased activity relating to COVID-19 and take proactive steps to protect themselves.

Technical Details

Summary of Attacks

APT groups are using the COVID-19 pandemic as part of their cyber operations. These cyber threat actors will often masquerade as trusted entities. Their activity includes using coronavirus-themed phishing messages or malicious applications, often masquerading as trusted entities that may have been previously compromised. Their goals and targets are consistent with long-standing priorities such as espionage and “hack-and-leak” operations.

Cybercriminals are using the pandemic for commercial gain, deploying a variety of ransomware and other malware.

Both APT groups and cybercriminals are likely to continue to exploit the COVID-19 pandemic over the coming weeks and months. Threats observed include:

- Phishing, using the subject of coronavirus or COVID-19 as a lure,
- Malware distribution, using coronavirus- or COVID-19- themed lures,
- Registration of new domain names containing wording related to coronavirus or COVID-19, and
- Attacks against newly—and often rapidly—deployed remote access and teleworking infrastructure.

Malicious cyber actors rely on basic social engineering methods to entice a user to carry out a specific action. These actors are taking advantage of human traits such as curiosity and concern around the coronavirus pandemic in order to persuade potential victims to:

- Click on a link or download an app that may lead to a phishing website, or the downloading of malware, including ransomware.
    - For example, a malicious Android app purports to provide a real-time coronavirus outbreak tracker but instead attempts to trick the user into providing administrative access to install "CovidLock" ransomware on their device.[1]
- Open a file (such as an email attachment) that contains malware.
    - For example, email subject lines contain COVID-19-related phrases such as “Coronavirus Update” or “2019-nCov: Coronavirus outbreak in your city (Emergency)”

To create the impression of authenticity, malicious cyber actors may spoof sender information in an email to make it appear to come from a trustworthy source, such as the World Health Organization (WHO) or an individual with “Dr.” in their title. In several examples, actors send phishing emails that contain links to a fake email login page. Other emails purport to be from an organization’s human resources (HR) department and advise the employee to open the attachment.

Malicious file attachments containing malware payloads may be named with coronavirus- or COVID-19-related themes, such as “President discusses budget savings due to coronavirus with Cabinet.rtf.”

Note: a non-exhaustive list of IOCs related to this activity is provided within the accompanying .csv and .stix files of this alert.

Phishing

CISA and NCSC have both observed a large volume of phishing campaigns that use the social engineering techniques described above.

Examples of phishing email subject lines include:

- 2020 Coronavirus Updates,
- Coronavirus Updates,
- 2019-nCov: New confirmed cases in your City, and
- 2019-nCov: Coronavirus outbreak in your city (Emergency).

These emails contain a call to action, encouraging the victim to visit a website that malicious cyber actors use for stealing valuable data, such as usernames and passwords, credit card information, and other personal information.

SMS Phishing

Most phishing attempts come by email but NCSC has observed some attempts to carry out phishing by other means, including text messages (SMS).

Historically, SMS phishing has often used financial incentives—including government payments and rebates (such as a tax rebate)—as part of the lure. Coronavirus-related phishing continues this financial theme, particularly in light of the economic impact of the epidemic and governments' employment and financial support packages. For example, a series of SMS messages uses a UK government-themed lure to harvest email, address, name, and banking information. These SMS messages—purporting to be from "COVID" and "UKGOV" (see figure 1)—include a link directly to the phishing site (see figure 2).

Figure 1: UK government-themed SMS phishing

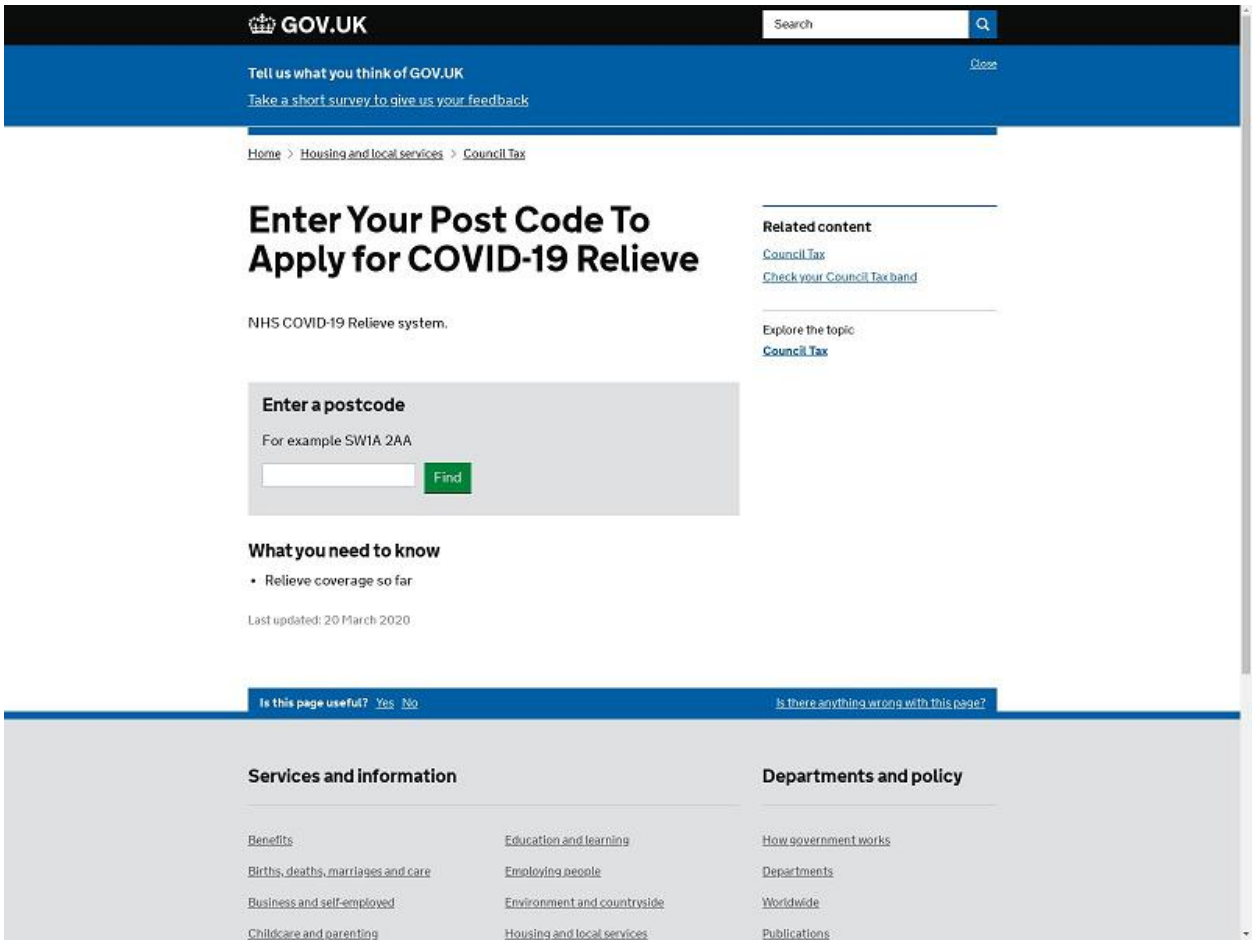

Figure 2: UK government-themed phishing page

As this example demonstrates, malicious messages can arrive by methods other than email. In addition to SMS, possible channels include WhatsApp and other messaging services. Malicious cyber actors are likely to continue using financial themes in their phishing campaigns. Specifically, it is likely that they will use new government aid packages responding to COVID-19 as themes in phishing campaigns.

Phishing for credential theft

A number of actors have used COVID-19-related phishing to steal user credentials. These emails include previously mentioned COVID-19 social engineering techniques, sometimes complemented with urgent language to enhance the lure.

If the user clicks on the hyperlink, a spoofed login webpage appears that includes a password entry form. These spoofed login pages may relate to a wide array of online services including—but not limited to—email services provided by Google or Microsoft, or services accessed via government websites.

To further entice the recipient, the websites will often contain COVID-19-related wording within the URL (e.g., “corona-virus-business-update,” “covid19-advisory,” or “cov19esupport”). These spoofed pages are designed to look legitimate or accurately impersonate well-known websites. Often the only way to notice malicious intent is through

examining the website URL. In some circumstances, malicious cyber actors specifically customize these spoofed login webpages for the intended victim.

If the victim enters their password on the spoofed page, the attackers will be able to access the victim's online accounts, such as their email inbox. This access can then be used to acquire personal or sensitive information, or to further disseminate phishing emails, using the victim's address book.

Phishing for malware deployment

A number of threat actors have used COVID-19-related lures to deploy malware. In most cases, actors craft an email that persuades the victim to open an attachment or download a malicious file from a linked website. When the victim opens the attachment, the malware is executed, compromising the victim's device.

For example, NCSC has observed various email messages that deploy the "Agent Tesla" keylogger malware. The email appears to be sent from Dr. Tedros Adhanom Ghebreyesus, Director-General of WHO. This email campaign began on Thursday, March 19, 2020. Another similar campaign offers thermometers and face masks to fight the epidemic. The email purports to attach images of these medical products but instead contains a loader for Agent Tesla.

In other campaigns, emails include a Microsoft Excel attachment (e.g., "8651 8-14-18.xls") or contain URLs linking to a landing page that contains a button that—if clicked—redirects to download an Excel spreadsheet, such as "EMR Letter.xls". In both cases, the Excel file contains macros that, if enabled, execute an embedded dynamic-link library (DLL) to install the "Get2 loader" malware. Get2 loader has been observed loading the "GraceWire" Trojan.

The "TrickBot" malware has been used in a variety of COVID-19-related campaigns. In one example, emails target Italian users with a document purporting to be information related to COVID-19 (see figure 3). The document contains a malicious macro that downloads a batch file (BAT), which launches JavaScript, which—in turn—pulls down the TrickBot binary, executing it on the system.

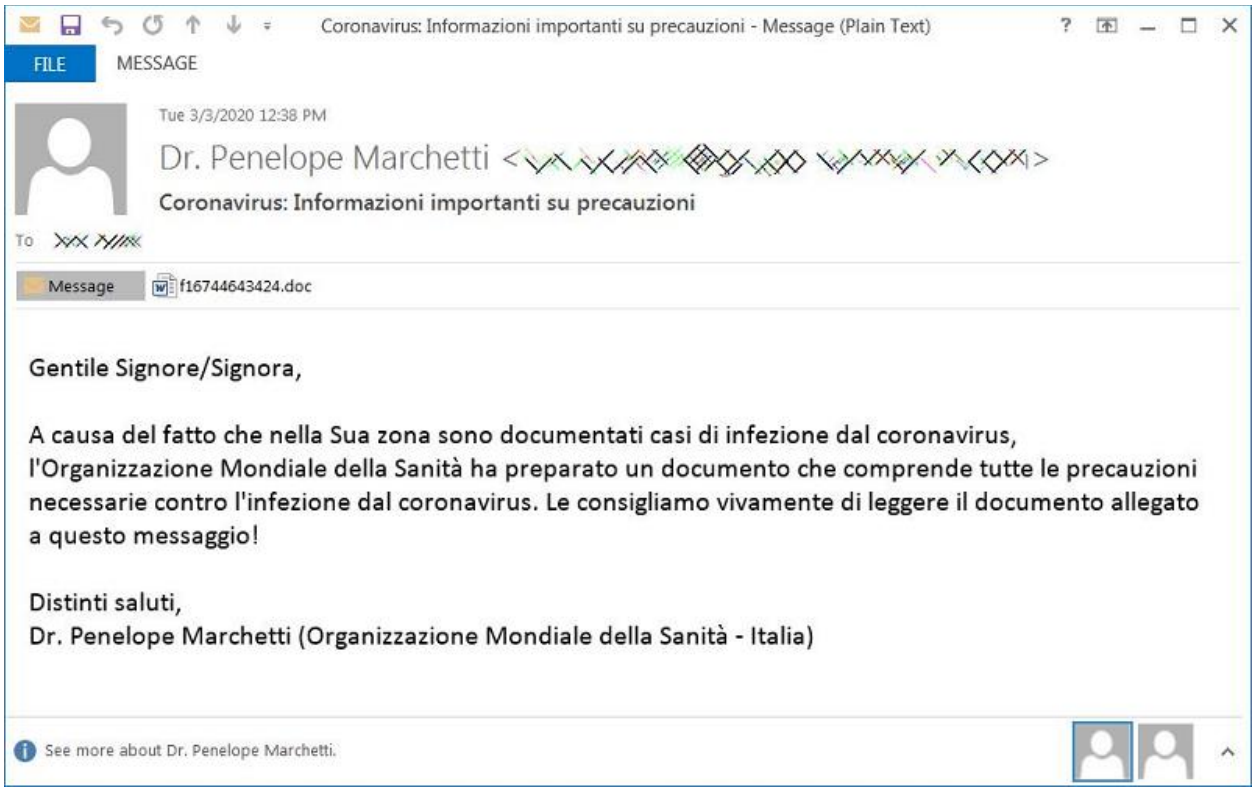

Figure 3: Email containing malicious macro targeting Italian users[2]

In many cases, Trojans—such as Trickbot or GraceWire—will download further malicious files, such as Remote Access Trojans (RATs), desktop-sharing clients, and ransomware. In order to maximize the likelihood of payment, cybercriminals will often deploy ransomware at a time when organizations are under increased pressure. Hospitals and health organizations in the United States,[3] Spain,[4] and across Europe[5] have all been recently affected by ransomware incidents.

As always, individuals and organizations should be on the lookout for new and evolving lures. Both CISA[6],[7] and NCSC[8] provide guidance on mitigating malware and ransomware attacks.

Exploitation of new teleworking infrastructure

Many organizations have rapidly deployed new networks, including VPNs and related IT infrastructure, to shift their entire workforce to teleworking.

Malicious cyber actors are taking advantage of this mass move to telework by exploiting a variety of publicly known vulnerabilities in VPNs and other remote working tools and software. In several examples, CISA and NCSC have observed actors scanning for publicly known vulnerabilities in Citrix. Citrix vulnerability, CVE-2019-19781, and its exploitation have been widely reported since early January 2020. Both CISA[9] and NCSC[10] provide guidance on CVE-2019-19781 and continue to investigate multiple instances of this vulnerability's exploitation.

Similarly, known vulnerabilities affecting VPN products from Pulse Secure, Fortinet, and Palo Alto continue to be exploited. CISA provides guidance on the Pulse Secure vulnerability[11] and NCSC provides guidance on the vulnerabilities in Pulse Secure, Fortinet, and Palo Alto.[12]

Malicious cyber actors are also seeking to exploit the increased use of popular communications platforms—such as Zoom or Microsoft Teams—by sending phishing emails that include malicious files with names such as "zoom-us-zoom_##########.exe" and "microsoft-teams_V#mu#D_##########.exe" (# representing various digits that have been reported online).[13] CISA and NCSC have also observed phishing websites for popular communications platforms. In addition, attackers have been able to hijack teleconferences and online classrooms that have been set up without security controls (e.g., passwords) or with unpatched versions of the communications platform software.[14]

The surge in teleworking has also led to an increase in the use of Microsoft's Remote Desktop Protocol (RDP). Attacks on unsecured RDP endpoints (i.e., exposed to the internet) are widely reported online,[15] and recent analysis[16] has identified a 127% increase in exposed RDP endpoints. The increase in RDP use could potentially make IT systems—without the right security measures in place—more vulnerable to attack.[17]

Indicators of compromise

CISA and NCSC are working with law enforcement and industry partners to disrupt or prevent these malicious cyber activities and have published a non-exhaustive list of COVID-19-related IOCs via the following links:

- AA20-099A_WHITE.csv
- A20-099A_WHITE.stix

In addition, there are a number of useful publicly available resources that provide details of COVID-19-related malicious cyber activity:

- Recorded Futures' report, *Capitalizing on Coronavirus Panic, Threat Actors Target Victims Worldwide*
- DomainTools' *Free COVID-19 Threat List - Domain Risk Assessments for Coronavirus Threats*
- GitHub list of IOCs used COVID-19-related cyberattack campaigns gathered by GitHub user Parth D. Maniar
- GitHub list of Malware, spam, and phishing IOCs that involve the use of COVID-19 or coronavirus gathered by SophosLabs
- Reddit master thread to collect intelligence relevant to COVID-19 malicious cyber threat actor campaigns
- Tweet regarding the MISP project's dedicated #COVID2019 MISP instance to share COVID-related cyber threat information

Mitigations

Malicious cyber actors are continually adjusting their tactics to take advantage of new situations, and the COVID-19 pandemic is no exception. Malicious cyber actors are using the high appetite for COVID-19-related information as an opportunity to deliver malware and ransomware, and to steal user credentials. Individuals and organizations should

remain vigilant. For information regarding the COVID-19 pandemic, use trusted resources, such as the Centers for Disease Control and Prevention (CDC)'s COVID-19 Situation Summary.

Following the CISA and NCSC advice set out below will help mitigate the risk to individuals and organizations from malicious cyber activity related to both COVID-19 and other themes:

- CISA guidance for defending against COVID-19 cyber scams
- CISA Insights: Risk Management for Novel Coronavirus (COVID-19), which provides guidance for executives regarding physical, supply chain, and cybersecurity issues related to COVID-19
- CISA Alert: Enterprise VPN Security
- CISA webpage providing a repository of the agency's COVID-19 guidance
- NCSC guidance to help spot, understand, and deal with suspicious messages and emails
- NCSC phishing guidance for organizations and cyber security professionals
- NCSC guidance on mitigating malware and ransomware attacks
- NCSC guidance on home working
- NCSC guidance on end user device security

Phishing guidance for individuals

The NCSC's suspicious email guidance explains what to do if you've already clicked on a potentially malicious email, attachment, or link. It provides advice on who to contact if your account or device has been compromised and some of the mitigation steps you can take, such as changing your passwords. It also offers NCSC's top tips for spotting a phishing email:

- **Authority** – Is the sender claiming to be from someone official (e.g., your bank or doctor, a lawyer, a government agency)? Criminals often pretend to be important people or organizations to trick you into doing what they want.
- **Urgency** – Are you told you have a limited time to respond (e.g., in 24 hours or immediately)? Criminals often threaten you with fines or other negative consequences.
- **Emotion** – Does the message make you panic, fearful, hopeful, or curious? Criminals often use threatening language, make false claims of support, or attempt to tease you into wanting to find out more.
- **Scarcity** – Is the message offering something in short supply (e.g., concert tickets, money, or a cure for medical conditions)? Fear of missing out on a good deal or opportunity can make you respond quickly.

Phishing guidance for organizations and cybersecurity professionals

Organizational defenses against phishing often rely exclusively on users being able to spot phishing emails. However, organizations that widen their defenses to include more technical measures can improve resilience against phishing attacks.

In addition to educating users on defending against these attacks, organizations should consider NCSC's guidance that splits mitigations into four layers, on which to build defenses:

1. Make it difficult for attackers to reach your users.
2. Help users identify and report suspected phishing emails (see CISA Tips, Using Caution with Email Attachments and Avoiding Social Engineering and Phishing Scams).

3. Protect your organization from the effects of undetected phishing emails.
4. Respond quickly to incidents.

CISA and NCSC also recommend organizations plan for a percentage of phishing attacks to be successful. Planning for these incidents will help minimize the damage caused.

Communications platforms guidance for individuals and organizations

Due to COVID-19, an increasing number of individuals and organizations are turning to communications platforms—such as Zoom and Microsoft Teams— for online meetings. In turn, malicious cyber actors are hijacking online meetings that are not secured with passwords or that use unpatched software.

Tips for defending against online meeting hijacking (Source: FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic, FBI press release, March 30, 2020):

- Do not make meetings public. Instead, require a meeting password or use the waiting room feature and control the admittance of guests.
- Do not share a link to a meeting on an unrestricted publicly available social media post. Provide the link directly to specific people.
- Manage screensharing options. Change screensharing to "Host Only."
- Ensure users are using the updated version of remote access/meeting applications.
- Ensure telework policies address requirements for physical and information security.

Disclaimers

This report draws on information derived from CISA, NCSC, and industry sources. Any findings and recommendations made have not been provided with the intention of avoiding all risks and following the recommendations will not remove all such risk. Ownership of information risks remains with the relevant system owner at all times.

CISA does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by CISA.

References

- [1] CovidLock ransomware exploits coronavirus with malicious Android app. TechRepublic.com. March 17, 2020.
- [2] TrickBot Malware Targets Italy in Fake WHO Coronavirus Emails. Bleeping Computer. March 6, 2020.
- [3] Maze Ransomware Continues to Hit Healthcare Units amid Coronavirus (COVID-19) Outbreak. Security Boulevard. March 19, 2020.
- [4] Spanish hospitals targeted with coronavirus-themed phishing lures in Netwalker ransomware attacks. Computing.co.uk. March 24, 2020.
- [5] COVID-19 Testing Center Hit By Cyberattack. Bleeping Computer. March 14, 2020.
- [6] CISA Tip: Protecting Against Malicious Code
- [7] CISA Ransomware webpage
- [8] NCSC Guidance: Mitigating malware and ransomware attacks

- [9] CISA Alert: Detecting Citrix CVE-2019-19781
- [10] NCSC Alert: Actors exploiting Citrix products vulnerability
- [11] CISA Alert: Continued Exploitation of Pulse Secure VPN Vulnerability
- [12] NCSC Alert: Vulnerabilities exploited in VPN products used worldwide
- [13] COVID-19 Impact: Cyber Criminals Target Zoom Domains. Check Point blog. March 30, 2020.
- [14] FBI Press Release: FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic
- [15] Microsoft Security blog: Human-operated ransomware attacks: A preventable disaster. March 5, 2020.
- [16] Reposify blog: 127% increase in exposed RDPs due to surge in remote work. March 30. 2020.
- [17] CISA Tip: Securing Network Infrastructure Devices

Revisions

- April 8, 2020: Initial Version
