Forum-SLDS Collaborative Webinar: Cybersecurity and Remote Learning/Working

Steven Hernandez, U.S. Department of Education

National Forum on Education Statistics

Cyber Security: A Federal Perspective during COVID-19

Office of the Chief Information Officer

U.S. Department of Education

Agenda

Introduction

Overview of the present threatscape

Best practices

Federal resources that can help

Questions

3

Introduction

Steven Hernandez

MBA, CISSP, CISA, CNSS, CSSLP, SSCP, CAP, ITIL

Chief Information Security Officer (CISO)

US Department of Education

Prior Roles:

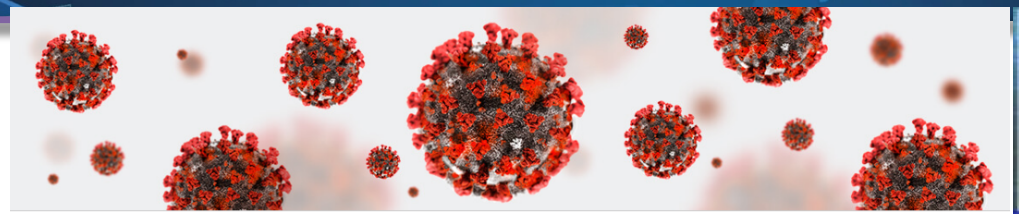
Vice Chairman Board of Directors $(ISC)^2$

CISO HHS OIG

Senior Official for Privacy, HHS OIG

4

COVID-19 Cyber Vigilance Update



- OCIO has been increasing outreach and alerts to the Department of the evolving security threats and attacks due to the current COVID-19 situation

- There has been a significant increase in phishing and other cybercriminal scams targeting a largely at-home workforce. Experts are warning that cybercriminals are targeting those who use Zoom, Houseparty, Zoho Meeting and many other commercially free offerings for teleconferencing. Thousands of phishing sites have been created to target these providers.

- Phishing, malicious websites, malware, ransomware, and shadow IT solutions were cited as current top threats

- Department users are urged to stay vigilant and continue to report suspected phishing attempts and suspicious emails through the ***ED Report Phishing*** button

Alert (AA20-099A)
COVID-19 Exploited by Malicious Cyber Actors

- **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).**
- 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.

Alert (AA20-099A)
COVID-19 Exploited by Malicious Cyber Actors

- 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.

Alert (AA20-099A)

COVID-19 Exploited by Malicious Cyber Actors

- 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)”

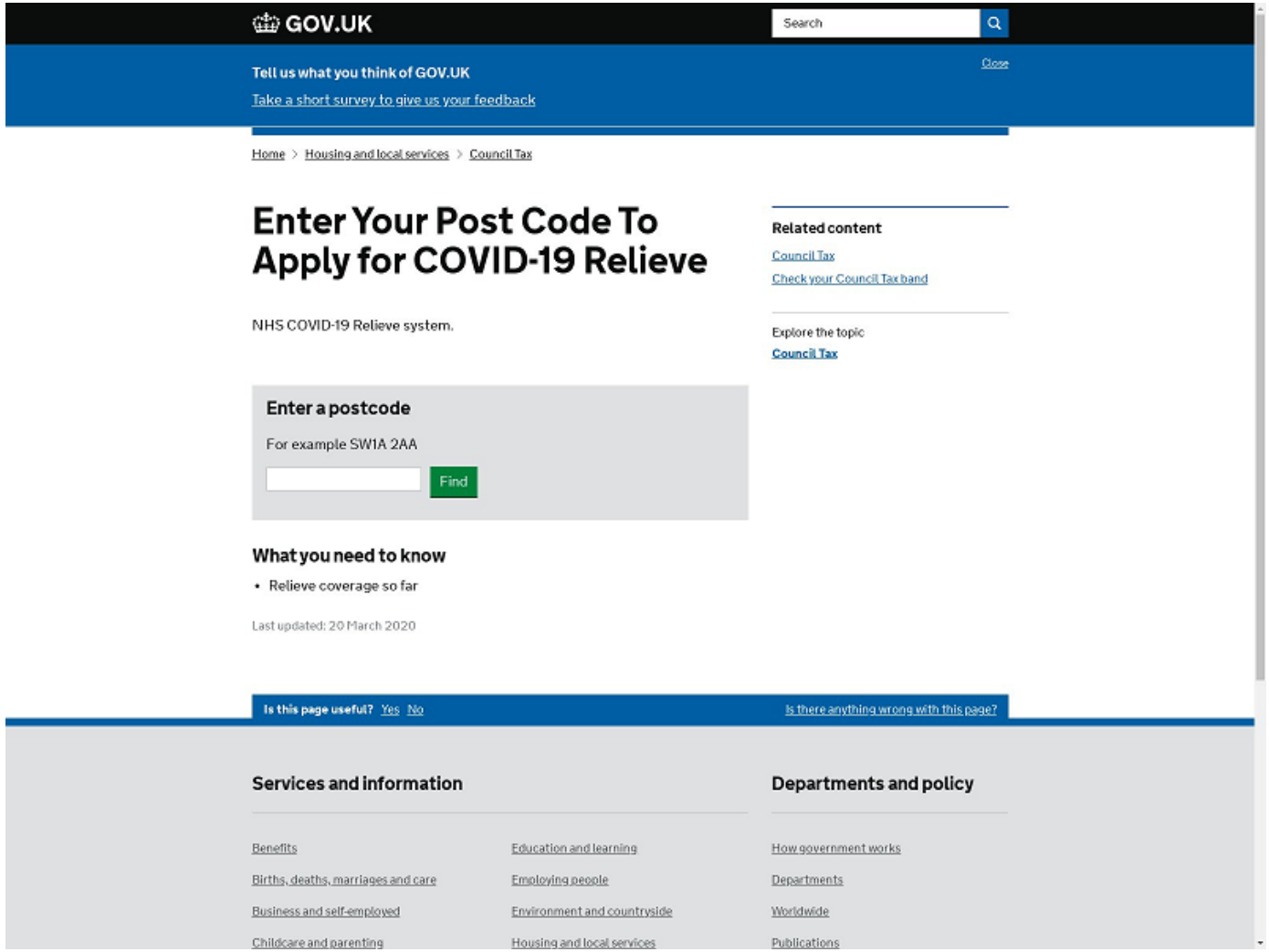
Alert (AA20-099A)
COVID-19 Exploited by Malicious Cyber Actors

- 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.”

SMS Phishing

SMS Phishing



COVID-19 Cyber Vigilance Update

1. Phishing for credential theft

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.

2. Phishing for malware deployment

Several 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.

3. **Exploitation of new teleworking infrastructure and Services**

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.

COVID-19 Cyber Vigilance Update

1. Phishing for credential theft

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.

2. Phishing for malware deployment

Several 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.

3. **Exploitation of new teleworking infrastructure and Services**

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.

Teleconferencing Vulnerabilities

Beware of watering hole attacks!

Teleconferencing Vulnerabilities

1. Leverage your organization's approved teleconferencing services
    1. For Organizers:
        1. Require a password for entry or use a lobby to only allow known attendees
        2. For sensitive information consider a list of passwords sent via sms or another channel to the recipients. Remove those who will not confirm their identity
        3. If the solution supports "closing" or "locking" your conference do so after the start
        4. Understand how to remove participants if needed
        5. Ensure you limit your screenshare. Share in this order when possible:
            1. File
            2. Application
            3. Desktop
        6. If on webcam blur/replace or be aware of your background
        7. You may want to inform folks if taking screenshots is ok.

Teleconferencing Vulnerabilities

1. Leverage your organization's approved teleconferencing services whenever possible
    1. For Attendees:
        1. Double check the URL of the meeting you think you are attending
        2. Make sure your client software is up to date
        3. Assume everything you share will be recorded and potentially made public. This is exceptionally true when joining free/no cost solutions.

Best Practices for Data Focused Missions

- Identify Your “Crown Jewels”
  - Least Function
  - Least Privilege
  - De-Identification
  - Retention
- Have an Actionable Plan in Place Before an Intrusion Occurs
- Have Appropriate Technology and Services in Place Before An Intrusion Occurs
- Have Appropriate Authorization in Place to Permit Network Monitoring
- Ensure Your Legal Counsel is Familiar with Technology and Cyber Incident Management to Reduce Response Time During an Incident
- Ensure Organization Policies Align with Your Cyber Incident Response Plan
- Engage with Law Enforcement Before an Incident
- Establish Relationships with Cyber Information Sharing Organizations

17

Best Practices for Data Focused Missions

- Building the Security in from the start
  - Consider leveraging cloud SaaS as much as possible
    - Review terms and SLA
    - Data Portability
  - Leverage FedRAMP systems
    - May not always be able to use GSA contracts
    - Federal Government Level of Security
    - You are still accountable for control configuration
    - State and local government representatives are encouraged to contact any FedRAMP Authorized CSP directly to determine their security package specifications.
  - EDUCAUSE Higher Education Cloud Assessment Tool
    - https://library.educause.edu/resources/2016/10/higher-education-cloud-vendor-assessment-tool

18

Helpful Federal Resources

- US Department of Education
  - https://studentprivacy.ed.gov/
  - https://nces.ed.gov/programs/ptac/

- FBI
  - Internet Crime Compliant Center (https://www.ic3.gov/default.aspx)
  - Local Field Offices (Establish a relationship sooner than later!)
    - https://www.fbi.gov/contact-us/field-offices
  - Infraguard (https://www.infragard.org/)

- MS-ISAC (https://www.cisecurity.org/ms-isac/)
  - Connects back to the US Department of Homeland Security

- Secret Service Field Offices (http://www.secretservice.gov/field_offices.shtml)
  - Electronic Crimes Task Forces (ECTFs) (http://www.secretservice.gov/ectf.shtml)

19

Helpful Federal Resources

- DOJ Best Practices for Victim Response and Reporting of Cyber Incidents -
  - https://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents.pdf

- NSA's Top Ten Cybersecurity Mitigation Strategies
  - https://www.iad.gov/iad/library/ia-guidance/security-tips/nsas-top-ten-cybersecurity-mitigation-strategies.cfm

- United States General Services Administration FedRAMP Program
  - https://www.fedramp.gov/training/

20

Helpful Federal Resources

Cyber Infrastructure and Security Agency

Request information about the service(s) you are interested in by emailing ncats_info@hq.dhs.gov.

All services are available at no cost to federal agencies, state and local governments, critical infrastructure, and private organizations generally.

Cyber Hygiene: Vulnerability Scanning helps secure your internet-facing systems from weak configuration and known vulnerabilities, and encourages the adoption of modern security best practices. DHS performs regular network and vulnerability scans and delivers a weekly report for your action. Once initiated, this service is mostly automated and requires little direct interaction. After we receive the required paperwork for Cyber Hygiene, our scans will start within 72 hours and you'll begin receiving reports within two weeks.
Cyber Hygiene Sample Report

A **Phishing Campaign Assessment** (PCA) measures your team's propensity to click on email phishing lures. Phishing is commonly used as a means to breach an organization's network. The assessment occurs over a 6 week period, and the results can be used to provide guidance for anti-phishing training and awareness.
Phishing Campaign Assessment (PCA) Sample Report

21

THANKS!!!!

Questions??

Contact me:

Steven G Hernandez

Steven.Hernandez@ed.gov

Thank You Steven!

The forthcoming *Forum Guide to Cybersecurity* will be published on the Forum website at https://nces.ed.gov/forum/.