SITUATION REPORT | CYBER

Federal Aviation Administration

February 26, 2020

Prepared by the Office of Security & Hazardous Material Safety (ASH)

Spearphishing Using Coronavirus Disease (COVID-19) Theme Poses Potential Risk to Aviation Personnel

Threat from Recent Phishing Trend: Malicious cyber actors are using the Coronavirus Disease (COVID-19) as a theme to disguise phishing emails and entice users to click on malicious links or attachments. The malicious links direct users to websites requesting they input their credentials, allowing malicious cyber actors to use the stolen credentials to obtain unauthorized access. The malicious attachments either contain a link to similar credential harvesting websites or deploy malware on the user's system.

- In February 2020, an information security company observed COVID-19 themed spearphishing emails targeting industries reliant on global shipping. The emails contained a malicious Word document attachment with AZORult[a] malware.[1]
- In February 2020, an information security company observed phishing emails masquerading as information from the Centers for Disease Control and Prevention (CDC). These emails included a link appearing to be to a cdc.gov page on COVID-19 cases in the recipient's city but redirected recipients who clicked on the link to a credential harvesting site. Phishing emails were also observed with an attachment labeled as preventative measures for COVID-19, but the attachment instead contained a link to a credential harvesting site.[2]
- In late January 2020, a threat intelligence company observed phishing emails targeting multiple Japanese prefectures with a malicious Word document attachment containing the Emotet[b] Trojan. The emails masqueraded as a disability welfare service notifying recipients of local COVID-19 cases and added legitimate contact information to increase the message's credibility.[3]

***Background:** Spearphishing emails are used to gain unauthorized access to a network through a malicious attachment or link. Unlike traditional phishing emails, spearphishing is tailored with key pieces of information to target a specific individual or organization. These emails may be spoofed to appear legitimate or originate from legitimate accounts that have been compromised.*

Potential Impact to Aviation Networks: Aviation personnel working on COVID-19-related matters are likely more susceptible to these themed emails, since they may resemble legitimate emails that these personnel expect to receive as part of their normal duties. A successful spearphishing attack on aviation entities could result in the compromise of networks or devices. A malicious actor with access to a network could manipulate or steal data, maintain persistence or move laterally across the network, escalate privileges, or deploy malware. Cybersecurity best practices, such as implementing appropriate network defenses, may reduce the risk of a compromise.

[a] Azorult is a commercial Trojan that is used to steal information from compromised hosts. https://attack.mitre.org/software/S0344/

[b] Emotet is an advanced, modular banking Trojan that primarily functions as a downloader or dropper of other banking Trojans. https://www.us-cert.gov/ncas/alerts/TA18-201A

Mitigation Strategies: Aviation personnel working on COVID-19-related matters should be careful to verify the authenticity of email attachments or links regarding COVID-19. All aviation personnel should remain aware of the potential risk to their networks from spearphishing emails containing malicious attachments or links, including the possibility that their networks, if compromised, may be used by malicious cyber actors as a staging point to target other organizations. Please see Table 1 and the resources section below for additional information, including mitigation strategies.

Techniques	Targets	Vulnerabilities	Consequences	Mitigation
Spearphishing Attachment	▪ Business systems ▪ Personal devices	▪ Lack of cyber hygiene and user training ▪ Outdated antivirus signatures ▪ Improperly establishing heuristic scanners	▪ Theft of sensitive data, including personally identifiable information, financial information, research, and intellectual property ▪ Unauthorized access to systems and credential harvesting ▪ Operational disruption ▪ Remediation costs	▪ User training to identify social engineering techniques and spearphishing emails with attachments. ▪ Implement and update antivirus, antimalware, network intrusion prevention systems, and email gateways to scan, quarantine, and remove suspicious or malicious email attachments. ▪ Block unknown or unused attachments
Spearphishing Link	▪ Business systems ▪ Personal devices	▪ Lack of cyber hygiene and user training ▪ Outdated antivirus signatures ▪ Improperly establishing heuristic scanners ▪ Unrestricted or unfiltered website access	▪ Theft of sensitive data, including personally identifiable information, financial information, research, and intellectual property ▪ Unauthorized access to systems and credential harvesting ▪ Operational disruption ▪ Remediation costs	▪ User training to identify social engineering techniques and spearphishing emails with links. ▪ Implement website content filtering ▪ Remove hyperlinks from email traffic ▪ Implement virtual browsers.

(U) Table 1: Potential techniques, targets, vulnerabilities, consequences, and mitigation strategies

Resources: The following links provide additional information:

- CISA Security Tip (ST04-014) provides background information and mitigation strategies on social engineering and phishing attacks: https://www.us-cert.gov/ncas/tips/ST04-014
- CISA Tips page provides advice about common security issues for non-technical computer users: https://www.us-cert.gov/ncas/tips

If there are any questions, please contact the CITE Watch at 202-267-3203.

Coordinated with: Department of Transportation/S-60 and Department of Homeland Security/TSA

Shared with: Department of Homeland Security/CISA

[1] Proofpoint, "Coronavirus-themed Attacks Target Global Shipping Concerns," 10 February 2020, https://www.proofpoint.com/us/corporate-blog/post/coronavirus-themed-attacks-target-global-shipping-concerns, accessed 14 February 2020.
[2] Trustwave, "Multiple Phishing Attacks Discovered Using the Coronavirus Theme," 13 February 2020, https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/multiple-phishing-attacks-discovered-using-the-coronavirus-theme, accessed 14 February 2020.
[3] IBM X-Force Exchange, "Coronavirus Goes Cyber With Emotet," 30 January 2020, https://exchange.xforce.ibmcloud.com/collection/18f373debc38779065a26f1958dc260b, accessed 14 February 2020.