Office of Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

HC3: Sector Alert

July 23, 2024 TLP:CLEAR Report: 202407231200

Phishing Attacks Following Global Technology Outage

Summary

A global technology outage caused by a faulty software update grounded flights, knocked banks and media outlets offline, and disrupted hospitals, small businesses and other services on July 19, 2024. While the cybersecurity firm that issued the update stated that the outage was not due to a hacking incident or cyber attack, it has nonetheless emboldened threat actors to seize upon the chaos. Phishing and other social engineering attacks targeting customers and contacts have since been observed, with attackers pretending to be from the support branch of the cybersecurity firm and offering unsolicited help. These malicious messages could lead to data exfiltration, ransomware deployment, and extortion. This Sector Alert provides sample fake domains already annotated, an impact of the outage to the Healthcare and Public Health (HPH) sector, and defense and mitigations from social engineering attacks.

Malicious Domains

As of July 20, 2024, the following domains have been noted as registered in relation to this incident by the e-mail security community:

crowdstrike-helpdesk[.]com	microsoftcrowdstrike[.]com
crowdstrikebluescreen[.]com	crowdfalcon-immed-update[.]com
crowdstrike-bsod[.]com	crowdstuck[.]org
crowdstrikedown[.]site	failstrike[.]com
crowdstrike0day[.]com	winsstrike[.]com
crowdstrikedoomsday[.]com	crowdpass[.]live
crowdstrikefix[.]com	crowdstrokeme[.]me
crashstrike[.]com	crowdstrikerecovery1.blob.core[.]windows[.]net
crowdstriketoken[.]com	crowdstrikeupdate[.]com
fix-crowdstrike-bsod[.]com	crowdstrike.phpartners[.]org
bsodsm8r[.]xamzgjedu[.]com	crowdstrikeodayl[.]com
crowdstrikebsodfix[.]blob[.]core[.]windows[.]net	crowdstrikedown[.]com
crowdstrikecommuication[.]app	crowdstrikeblueteam[.]com
fix-crowdstrike-apocalypse[.]com	crowdstrikefix[.]zip
supportportal-crowdstrike-com[.]translate[.]goog	crowdstrikereport[.]com
crowdstrike-cloudtrail-storage-bb-126d5e[.]s3[.]us-west-1[.]amazonaws[.]com	crowdstrike.phpartners[.]org
crowdstrikeoutage[.]info	crowdstrikeodayl[.]com
clownstrike[.]co[.]uk	crowdstrikedown[.]com
crowdstrikebsod[.]com	crowdstrikeblueteam[.]com
whatiscrowdstrike[.]com	crowdstrikefix[.]zip
clownstrike[.]co	crowdstrikereport[.]com

Defense and Mitigations

In addition to doing your best to identify a potential phishing or social engineering attempt, there are precautions you can take to protect yourself.

CISA

The Cybersecurity & Infrastructure Security Agency (CISA) recommends the following steps to avoid falling victim to social engineering scams:

- Be suspicious of unsolicited phone calls, visits, or e-mail messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.

- Avoid clicking on links, and instead type the web address into an internet browser.
- Keep web browsers up to date, because older versions have fewer protections in place.
- Hover over links before clicking on them to see the true destination. If the web address that the link directs to is unfamiliar, it might be an attempt to deceive you.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in an e-mail, and do not respond to e-mail solicitations for this information. This includes following links sent in an e-mail.
- Install and maintain anti-virus software, firewalls, and e-mail filters to reduce some of this traffic.
- Take advantage of any anti-phishing features offered by your e-mail client and web browser.
- Enforce multi-factor authentication (MFA).

Mitigations

If you think you have been a victim of a phishing or social engineering attack, you can file a complaint with the FCC's Consumer Complaint Center. You can also report fraud to the Federal Trade Commission. You can also file a report with the FBI's Internet Crime Complaint Center (IC3) and the Cybersecurity & Infrastructure Security Agency. Be sure to have detailed knowledge of what transpired for the reporting.

MITRE ATT&CK Techniques

The MITRE ATT&CK framework is a globally accessible knowledge base of adversary tactics and techniques designed for threat hunters, defenders, and red teams to help classify attacks, identify attack attribution and objectives, and assess an organization's risk. While not exclusive, below are some sample MITRE ATT&CK techniques that have been used by threat actors relevant to this problem set:

Phishing	
ID: T1566	
Sub-Techniques	
T1566.001	Spear phishing Attachment
T1566.002	Spear phishing Link
T1566.002	Spear phishing via Service
T1566.004	Spear phishing Voice
Description	
Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spear phishing. In spear phishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims e-mails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques, such as removing or manipulating e-mails or metadata/headers from compromised accounts being abused to send messages (e.g., E-mail Hiding Rules). Another way to accomplish this is by forging or spoofing the identity of the sender, which can be used to fool both the human	

recipient as well as automated security tools.

Victims may also receive phishing messages that instruct them to call a phone number, and then are directed to visit a malicious URL, download malware, or install adversary-accessible remote management tools onto their computer (i.e., User Execution).

The Way Forward

The success of phishing and other social engineering attacks depends on the human interaction between threat actor and victim. It remains a popular tactic among attackers because it is often easier to exploit people than it is to find a network or software vulnerability. The recent global outage will only fuel more threat actors to exploit the situation. Organizations and individuals should remain vigilant to suspicious offers to assist them, especially those with the name of the cybersecurity firm in question.

In addition to a HC3 Analyst Note on Healthcare Sector DDoS Guide on how to safeguard against ransomware/extortion attacks, some cybersecurity professionals advise that the healthcare industry acknowledge the ubiquitous threat of cyberwar against them, and recommend that their cybersecurity teams implement the following steps:

- Educate and train staff to reduce the risk of social engineering attacks via email and network access.
- Assess enterprise risk against all potential vulnerabilities, and prioritize implementing the security plan with the necessary budget, staff, and tools.
- Develop a cybersecurity roadmap that everyone in the healthcare organization understands.

At no cost, the Cybersecurity & Infrastructure Security Agency (CISA) also offers Cyber Hygiene Vulnerability Scanning Services to federal, state, local, tribal and territorial governments, as well as public and private sector critical infrastructure organizations. This service helps organizations monitor and evaluate their external network posture.

The probability of cyber threat actors targeting the healthcare industry remains high. Prioritizing security by maintaining awareness of the threat landscape, assessing the situation, and providing staff with the tools and resources necessary to prevent a cyberattack remain the best ways forward for healthcare organizations.

Relevant HHS Reports

HC3: Analyst Note – Healthcare Sector DDoS Guide (February 13, 2023)

HC3: Threat Briefing – Business E-mail Compromise (BEC) & Healthcare (May 16, 2024)

HC3: Threat Briefing – Cybersecurity Incident Response Plans (October 12, 2023)

HC3: Threat Briefing – Data Exfiltration Trends in Healthcare (March 9, 2023)

HC3: Threat Briefing – The Impact of Social Engineering on Healthcare (August 18, 2022)

HC3: Threat Briefing – Multi-Factor Authentication & Smishing (August 10, 2023)

HC3: Threat Briefing – Social Engineering Attacks Targeting the HPH Sector (April 11, 2024)

HC3: Threat Briefing – Strengthening Cyber Posture in the Health Sector (June 16, 2022)

HC3: White Paper – AI-Augmented Phishing and the Threat to the Health Sector (October 26, 2023)

HC3: White Paper – QR Code-Based Phishing (Quishing) as a Threat to the Health Sector (October 23, 2023)

References

"2024 Data Breach Investigations Report." Verizon. Accessed July 8, 2024. https://www.verizon.com/business/resources/T3e1/reports/2024-dbir-data-breach-investigations-report.pdf

Alder, Steve. "Healthcare Data Breaches Due to Phishing." The HIPAA Journal. January 6, 2024. https://www.hipaajournal.com/healthcare-data-breaches-due-to-phishing/

Graham-McLay, Charlotte and Elaine Kurtenbach, David McHugh. "Widespread global tech outage disrupts flights, banks, hospitals and media outlets." AP News. July 19, 2024. https://apnews.com/article/microsoft-crowdstrike-outage-australia-internet-banks-media-0a5f792b6571b37a35181d64028fefc4

"IBM X-Force Threat Intelligence Index 2024." IBM. Accessed July 8, 2024. https://www.ibm.com/reports/threat-intelligence

Kerkhofs, Piet. "CrowdStrike Falcon blue screen issue updates." Eye Security. July 19, 2024. https://www.eye.security/blog/crowdstrike-falcon-blue-screen-issue-updates#:~:text=Important%20update%3A%20CrowdStrike%20has%20observed,reach%20out%20without%20prior%20contact.

Pilkington, Ed. "US transportation, police and hospital systems stricken by global CrowdStrike IT outage." The Guardian. July 19, 2024. https://www.theguardian.com/technology/article/2024/jul/19/crowdstrike-microsoft-outage

Rosencrance, Linda and Madelyn Bacon. "Social Engineering." TechTarget. Accessed July 19, 2024. https://www.techtarget.com/searchsecurity/definition/social-engineering?_gl=1*1b5rgkr*_ga*MTIyOTkyNTk4Mi4xNzIxNDAxNDgw*_ga_TQKE4GS5P9*MTcyMTQwMTQ3OS4xLjAuMTcyMTQwMTQ4MC4wLjAuMA..

Scroxton, Alex. "CrowdStrike update chaos explained: What you need to know." Computer Weekly. July 19, 2024. https://www.computerweekly.com/feature/CrowdStrike-update-chaos-explained-What-you-need-to-know

"Statement on Falcon Content Update for Windows Hosts." CrowdStrike. July 19, 2024. https://www.crowdstrike.com/blog/statement-on-falcon-content-update-for-windows-hosts/

"Threat Actors Posing As CrowdStrike Employees Using Phishing Tactics." The Mississippi Cyber Unit. July 20, 2024.

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback