Vishing and Phishing Campaigns Targeting the HPH Sector

Executive Summary

In late March 2021, security researchers revealed details of a malicious campaign targeting the healthcare and public health (HPH) sector by leveraging call centers to distribute malware to its targets. Numerous campaigns in the past year have successfully leveraged voice-changing software, Voice over IP (VoIP) software, caller ID spoofing, and social engineering techniques to obtain sensitive information or install malware on targeted systems. HC3 assesses that these trends will continue due to previous successful exploitation.

Report

HC3 has observed numerous phishing and vishing campaigns in the last year, with an uptick of recent activity targeting the HPH sector. Voice phishing, also known as vishing, is the practice of eliciting information or attempting to influence action via the telephone. Threat actors often leverage VoIP services to conduct social engineering attacks. These attacks enable hackers to appear to be originating from a trusted telephone number by spoofing the caller ID. Attackers may even leverage voice-changing software to further convince victims and obscure their identity. The objectives of these attacks are to obtain sensitive information or distribute malware. Some relevant threat activity observed by the HC3 over the past year includes the following:

- In April 2021, the Molerats cyberespionage group was discovered using voice-changing software to pose as women when social engineering its targets to install malware. This group is also believed to hack VoIP systems which could allow them to appear to be coming from a trusted phone number. While this group mainly targets entities in the Middle East they have also targeted entities in Europe and the United States.
- In late March 2021, individuals operating fake call centers were arrested in India for vishing campaigns that targeted U.S citizens and impersonated tech support of various major U.S. tech companies—such as Apple, McAfee, and Amazon—with VoIP calling and caller ID spoofing. Government entities were also impersonated.
- Also in March 2021, suspected Iranian hackers impersonated a well-known Israeli physicist as part of a broader campaign to break into the email accounts of medical researchers in Israel and the U.S.
- In late January 2021, the BazarLoader malware was observed being distributed by call centers in a malware distribution campaign dubbed 'BazarCall' targeting medical professionals and healthcare entities. TrickBot, IcedID, Gozi IFSB, and other malware were also observed being distributed as part of this campaign. Some of these malware families are known to result in the deployment of additional malware such as ransomware.
- In November 2020, Check Point revealed a large-scale campaign targeting VoIP Session Initiation Protocol (SIP) servers across the globe. Successful exploitation of VoIP servers could enable attackers to make outgoing phone calls impersonating the victim to carry out their objectives.
- In September 2020, a Michigan healthcare provider warned patients of a vishing scam impersonating a local health system in attempts to steal protected health information (PHI).

How to Identify Vishing / Phishing

- Suspicious emails claiming a free trial has ended for a service for which the recipient never signed.
- Unexpected emails containing only the name, address, and phone number of an unrecognized organization.
- Individuals asking callers to navigate to a website to cancel a subscription for which they did not sign.
- Emails from a Gmail account with the name of a high-level individual in medical research.
- Phone calls or emails pretending to be from a government entity, such as a Department of Health or major technology company.

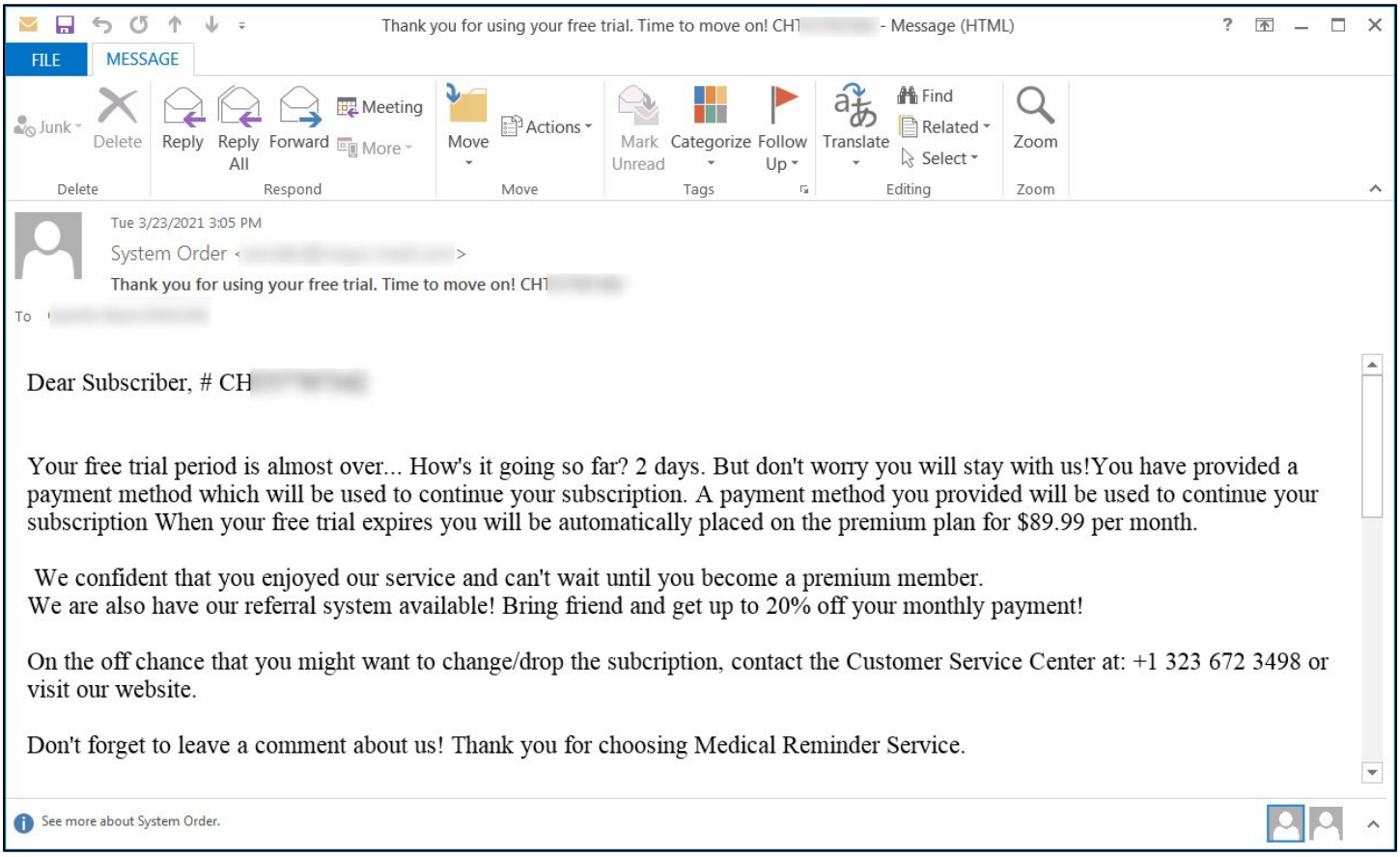

Figure 1. Example of a phishing email pretending to be a medical service instructing recipients to contact customer service to cancel a subscription they did not sign up for and then convincing callers to download malware such as BazarLoader.

Mitigations

- User training and awareness of new phishing campaigns targeting the HPH sector.
- Confirm receipt of an email from a known sender via a trusted communication method or contact.
- Secure VoIP servers and look for evidence of existing compromise (such as web shells for persistence).
- Block malicious domains and other indicators associated with campaigns, such as those mentioned above.
- Stay up-to-date with the latest COVID-19 scams and fraud schemes.

References

Abrams, Lawrence. "BazarCall malware uses malicious call centers to infect victims," Bleeping Computer. 31 March 2021. https://www.bleepingcomputer.com/news/security/bazarcall-malware-uses-malicious-call-centers-to-infect-victims/.

Arghire, Ionut. "APT Group Using Voice Changing Software in Spear-Phishing Campaign," Security Week. 2021 April 6. https://www.securityweek.com/apt-group-using-voice-changing-software-spear-phishing-campaign.

Barth, Bradley. "Array of recent phishing schemes use personalized job lures, voice manipulation," SC Magazine. 2021 April 06. https://www.scmagazine.com/home/security-news/phishing/array-of-recent-phishing-schemes-use-personalized-job-lures-voice-manipulation/

Davis, Jessica. "FBI, CISA Alert of Surge in Vishing Cyberattacks on Remote Workers," 2020 August 25.

https://healthitsecurity.com/news/fbi-cisa-alert-of-surge-in-vishing-cyberattacks-on-remote-workers.
Drees, Jackie. "Scammers posing as Spectrum Health employees are calling patients to steal their PHI, health system warns. 2020 September 15. https://www.beckershospitalreview.com/cybersecurity/scammers-posing-as-spectrum-health-employees-are-calling-patients-to-steal-their-phi-health-system-warns.html.
Health IT Security. "FBI: Spike in Vishing Attacks Seeking Escalated Access, Credential Theft." Health IT Security. 2021 January 21. https://healthitsecurity.com/news/fbi-spike-in-vishing-attacks-seeking-escalated-access-credential-theft.
Lyngaas, Sean. "How alleged Iranian hackers are posing as an Israeli scientist to spy on US medical professionals," 2021 March 31. https://www.cyberscoop.com/iran-charming-kitten-medical-proofpoint/.
Miller, Joshua. "BadBlood: TA453 Targets US and Israeli Medical Research Personnel in Credential Phishing Campaigns," 2021 March 30. https://www.proofpoint.com/us/blog/threat-insight/badblood-ta453-targets-us-and- israeli-medical-research-personnel-credential.
Security Boulevard. "The Impact of COVID-19 on Security," Security Boulevard. 2021 April 07. https://securityboulevard.com/2021/04/the-impact-of-covid-19-on-security/.
The New Indian Express. "Fake call centre duping US citizens busted in Delhi; 16 arrested," 2021 March 31. https://www.newindianexpress.com/cities/delhi/2021/mar/31/fake-call-centre-duping-us-citizens-busted-in-delhi-16-arrested-2284056.html.
World Health. "What Clinicians Need to Know About Mounting Healthcare Cyberattacks," World Health. 2021 April 07. https://www.worldhealth.net/news/what-clinicians-need-know-about-mounting-healthcare