LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF INFORMATION SECURITY

HC3: Analyst Note

September 2, 2021 TLP: White Report: 202109021400

Phishing Campaigns Demonstrate Importance of User Training and Awareness

Executive Summary

Most threat actors today continue to rely on phishing to compromise their targets. Using the various types of phishing threat actors continue to evolve their tactics, techniques, and procedures (TTPs) to increase chances of successful exploitation. HC3 has observed numerous high-profile attacks in the HPH sector in the past year and HC3 assesses that these trends will continue due to previous successful exploitation. Organizations need to be aware of new trends and lures to ensure staff are properly vigilant against this threat.

Report

There are various types of phishing attacks that may be leveraged by threat actors. These include:

1) Spear phishing: Spear phishing targets a specific group or type of individuals such as a company's system administrators or human resources department, for example.
2) Whaling: Whaling is an even more targeted type of phishing as it goes after the "whales," or a company's CEO, CFO, CIO, or other high-level employee within a target industry or business.
3) Smishing: Smishing is an attack that uses text messaging or short message service (SMS) to get your attention and lure individuals to click a link or unwittingly contact the threat actor.
4) Vishing: Vishing carries the same theme as all the other phishing attacks but is carried out over the phone through a voice call. Hence the "v" rather than the "ph" in the name. Vishing may even leverage voice changing software to sound more convincing and obscure the caller's identity, often with a female voice.
5) Email phishing: Email phishing is the most common type of phishing, and it has been in use since the 1990s. Hackers may send these emails to any and all email addresses they can obtain and may leverage personal information about the target individual to increase chances of successful exploitation.

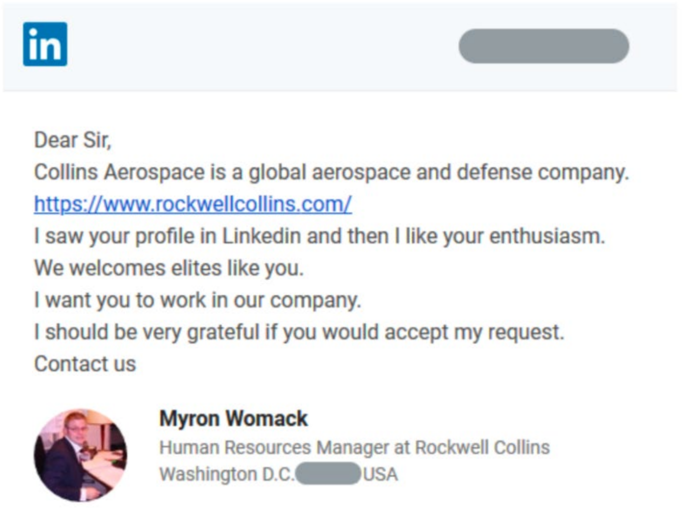
HC3 has observed numerous high-profile phishing campaigns and successful attacks in the past year, with an uptick of activity targeting the HPH sector. Some relevant threat activity observed by the HC3 includes the following:

- In late June 2021, an infectious disease practice in the U.S. fell victim to an email security incident in which a threat actor gained access to employee email accounts containing protected health information (PHI).
- In May 2021, researchers identified a LinkedIn spearphishing campaign targeting individuals in the health care sector to distribute malware and exfiltrate sensitive information.
- In April 2021, a children's hospital in Virginia fell victim to business email compromise (BEC) after a small number of employees were compromised in a phishing attack, leading to a breach of patient information.
- 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.
- In August 2020, Idaho nurses were targeted with a scam over the phone from a fake member of the state's nursing board telling her that her license had been suspended and then tried to extort $17,500 from her.

How to Identify Phishing Attempts

- Suspicious emails claiming a free trial has ended for a service for which the recipient never signed up for.
- 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 up for.
- Emails from an email account with the name of a high-level individual in a known company, for example Tim Cook at Apple.
- Phone calls or emails pretending to be from a government entity, such as a Department of Health.
- Phishing attempts also come through social media platforms such as LinkedIn, Facebook and twitter. On LinkedIn or other job hunting sites be weary of suspicious LinkedIn messages offering fake job offers or illegitimate contact requests. Suspicious requests on personal social media sites such as requesting to collaborate on research.

Figure 1 below is an example of a spear phishing message on LinkedIn from someone claiming to be a recruiter with a fake job offer. Users should ask themselves whether a job offer is too good to be true and many fake jobs for healthcare professionals offer the chance to work from home, which may not be realistic given the nature of the work. You should check whether the company or recruiter is legitimate and never divulge personal information. Additionally users should navigate to the company's public website and use contact information provided there to confirm the validity of the messages.



[redacted]

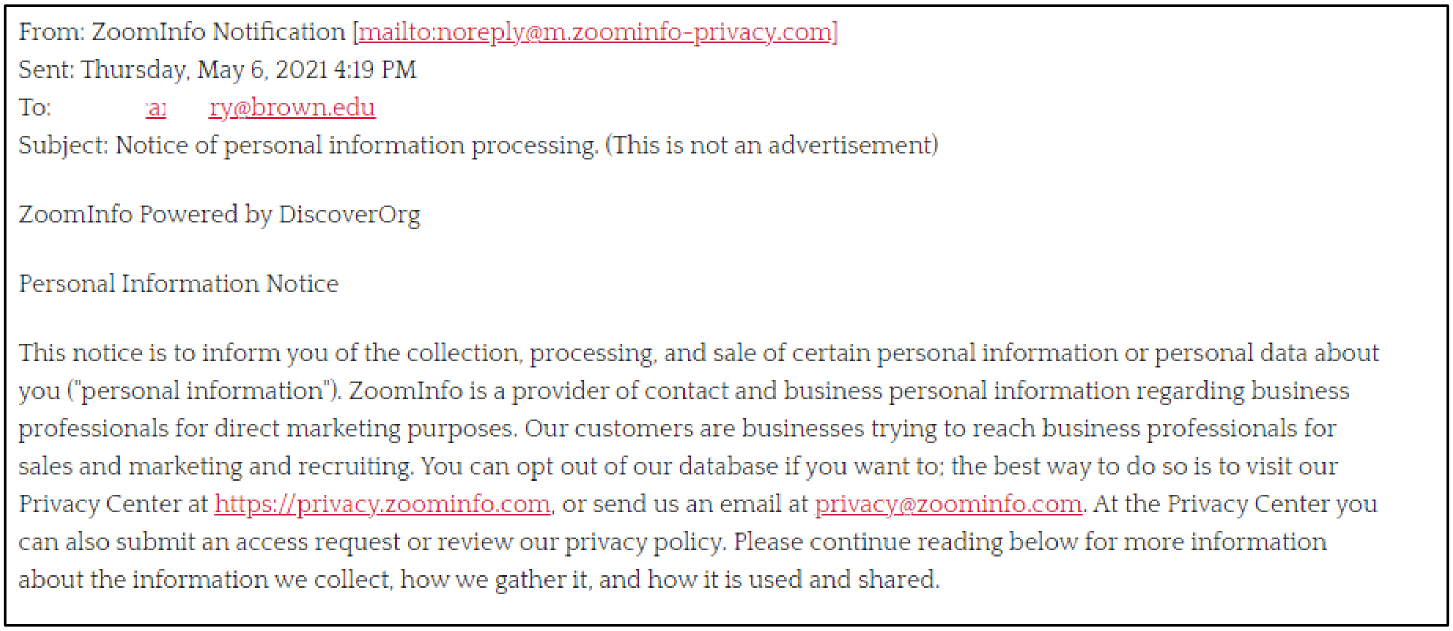
Dear Sir,
Collins Aerospace is a global aerospace and defense company.
https://www.rockwellcollins.com/
I saw your profile in Linkedin and then I like your enthusiasm.
We welcomes elites like you.
I want you to work in our company.
I should be very grateful if you would accept my request.
Contact us

Myron Womack
Human Resources Manager at Rockwell Collins
Washington D.C.[redacted]USA

Figure 1 // A fake job offer sent via LinkedIn to employees at one of the targeted companies

Figure 1. Sample spear message on LinkedIn

Additionally, be wary of messages claiming to be from social networking sites which are looking to confirm information via email. The figure below shows a phishing attempt which looks to be from a company trying to confirm information.



From: ZoomInfo Notification [mailto:noreply@m.zoominfo-privacy.com]
Sent: Thursday, May 6, 2021 4:19 PM
To: [redacted]ry@brown.edu
Subject: Notice of personal information processing. (This is not an advertisement)

ZoomInfo Powered by DiscoverOrg

Personal Information Notice

This notice is to inform you of the collection, processing, and sale of certain personal information or personal data about you ("personal information"). ZoomInfo is a provider of contact and business personal information regarding business professionals for direct marketing purposes. Our customers are businesses trying to reach business professionals for sales and marketing and recruiting. You can opt out of our database if you want to; the best way to do so is to visit our Privacy Center at https://privacy.zoominfo.com, or send us an email at privacy@zoominfo.com. At the Privacy Center you can also submit an access request or review our privacy policy. Please continue reading below for more information about the information we collect, how we gather it, and how it is used and shared.

Figure 2. Phishing email from ZoomInfo stating Privacy Policy and notifying users of personal data that is collected.

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.
- Opt-out to remove your company data from data brokers such as Zoominfo as threat actors often leverage this information when carrying out attacks and performing reconnaissance.
- Employee training on Operational Security (OPSEC) best practices to reduce personal information on public personal and professional social media accounts such as LinkedIn that could be leveraged in social engineering and spearphishing or whaling attacks.

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/

BrandYourself. “ZoomInfo Opt Out: Remove Your Private Info,” 9 September 2020. https://brandyourself.com/blog/privacy/zoominfo-opt-out/

Brown University. “Notice of personal information processing. (This is not an advertisement) [ZoomInfo],” 6 May 2021. https://it.brown.edu/alerts/read/notice-personal-information-processing-not-advertisement-zoominfo

CareerStaff. “SCAM ALERT: HOW TO SPOT FAKE JOBS FOR HEALTHCARE PROFESSIONALS,” 5 October 2020. https://www.careerstaff.com/blog/allied/alert-scams-fake-jobs-for-healthcare-professionals/

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

Lucas, Emmy. “FBI warns healthcare systems of Hive ransomware following Memorial Health System attack,” 1 September 2021. https://www.fiercehealthcare.com/tech/fbi-warns-healthcare-systems-hive-ransomware-following-memorial-health-system-attack

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.

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

Trend Micro. “What are the different types of phishing?,” https://www.trendmicro.com/en_us/what-is/phishing/types-of-phishing.html.

Tripwire. “Why OPSEC Is for Everyone, Not Just for People with Something to Hide,” 18 October 2017. https://www.tripwire.com/state-of-security/security-data-protection/opsec-everyone-not-just-people-something-hide/

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

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