Cyber Criminals Take Advantage of Increased Telework Through Vishing Campaign

SUMMARY

The Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) are issuing this advisory in response to a voice phishing (vishing)[1] campaign.

The COVID-19 pandemic has resulted in a mass shift to working from home, resulting in increased use of corporate virtual private networks (VPNs) and elimination of in-person verification. In mid-July 2020, cybercriminals started a vishing campaign—gaining access to employee tools at multiple companies with indiscriminate targeting—with the end goal of monetizing the access. Using vished credentials, cybercriminals mined the victim company databases for their customers' personal information to leverage in other attacks. The monetizing method varied depending on the company but was highly aggressive with a tight timeline between the initial breach and the disruptive cash-out scheme.

TECHNICAL DETAILS

The initial steps of this vishing campaign followed a common thread. Actors registered domains and created phishing pages duplicating a company's internal VPN login page, also capturing two-factor authentication (2FA) or one-time passwords (OTP). Actors also obtained Secure Sockets Layer (SSL) certificates for the domains they registered and used a variety of domain naming schemes, including the following examples:

- support-[company]
- ticket-[company]
- employee-[company]
- [company]-support
- [company]-okta

Actors then compiled dossiers on the employees at the specific companies using mass scraping of public profiles on social media platforms, recruiter and marketing tools, publicly available background

[1] Vishing is a form of criminal phone fraud, using social engineering over the telephone system to gain access to private personal and financial information for the purpose of financial reward.

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by email at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at CISAServiceDesk@cisa.dhs.gov.

This document is marked TLP AMBER: The information in this product may be shared with members of your organization and with clients and customers who need to know the information to protect themselves or prevent future harm.

For more information on the Traffic Light Protocol, see https://us-cert.cisa.gov/tlp.

check services, and open-source research. Information collected included: name, home address, personal cell/phone number, position at company, and duration at company.

Actors first began using unattributed Voice over Internet Protocol (VoIP) numbers to call targeted employees on their personal cellphones, and later began incorporating spoofed numbers of other offices and employees in the victim company. The actors used social engineering techniques and, in some cases, posed as members of the victim company's IT help desk, using their knowledge of the employee's personally identifiable information—including name, position, duration at company, and home address—to gain the trust of the targeted employee. The actors then convinced the targeted employee that a new VPN link would be sent and required their login, including any 2FA or OTP. The actor logged the information provided by the employee and used it in real-time to gain access to corporate tools using the employee's account.

In some cases, unsuspecting employees approved the 2FA or OTP prompt, either accidentally or believing it was the result of the earlier access granted to the help desk impersonator. In other cases, attackers have used a SIM-Swap attack[2] on the employees to bypass 2FA and OTP authentication. The actors then used the employee access to conduct further research on victims, and/or to fraudulently obtain funds using varying methods dependent on the platform being accessed.

The COVID-19 pandemic has resulted in a mass shift to working from home, resulting in increased use of corporate VPN and elimination of in-person verification, which can partially explain the success of this campaign. Prior to the pandemic, similar campaigns exclusively targeted telecommunications providers and internet service providers with these attacks but the focus has recently broadened to more indiscriminate targeting.

MITIGATIONS

Organizational Tips

- Restrict VPN connections to managed devices only, using mechanisms like hardware checks or installed certificates, so user input alone is not enough to access the corporate VPN.
- Restrict VPN access hours, where applicable, to mitigate access outside of allowed times.
- Employ domain monitoring to track the creation of, or changes to, corporate, brand-name domains.
- Actively scan and monitor web applications for unauthorized access, modification, and anomalous activities.
- Employ the principle of least privilege and implement software restriction policies or other controls; monitor authorized user accesses and usage.
- Consider using a formalized authentication process for employee-to-employee communications made over the public telephone network where a second factor is used to authenticate the phone call before sensitive information can be discussed.
- Improve 2FA and OTP messaging to reduce confusion about employee authentication attempts.

[2] https://attack.mitre.org/techniques/T1451/

End-User Tips

- Verify web links do not have misspellings or contain the wrong domain.
- Bookmark the correct corporate VPN URL and do not visit alternative URLs on the sole basis of an inbound phone call.
- Be suspicious of unsolicited phone calls, visits, or email messages from unknown individuals claiming to be from a legitimate organization. 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. If possible, try to verify the caller's identity directly with the company.
- If you receive a vishing call, document the phone number of the caller as well as the domain that the actor tried to send you to and relay this information to law enforcement.
- Limit the amount of personal information you post on social networking sites. The internet is a public resource; only post information you are comfortable with anyone seeing.
- Evaluate your settings: sites may change their options periodically, so review your security and privacy settings regularly to make sure that your choices are still appropriate.
- For more information on how to stay safe on social networking sites and avoid social engineering and phishing attacks, visit the CISA Security Tips below.
    - Avoiding Social Engineering and Phishing Attacks
      https://us-cert.cisa.gov/ncas/tips/ST04-014
    - Staying Safe on Social Networking Sites
      https://us-cert.cisa.gov/ncas/tips/ST06-003