'Vishing' Attacks on Remote Workers on the Rise

By Roy Maurer
September 3, 2020

The FBI and the Cybersecurity and Infrastructure Security Agency (CISA) is warning employers about an ongoing voice-phishing ("vishing") campaign targeting remote workers.

According to the alert (http://www.documentcloud.org/documents/7041919-Cyber-Criminals-Take-Advantage-of-Increased.html), the campaign began in mid-July and involves criminals creating fake websites that duplicate the virtual private network (VPN) login pages for targeted companies. They then pose as the information technology (IT) help desk of those companies when calling employees, to gain their trust and get them to log in to the mock VPN.

Vishing is a form of social engineering done over the telephone to trick victims into giving up their account credentials to gain access to private information. In this case, most of the calls were made using Voice over Internet Protocol numbers to call victims on their personal cellphones. In other cases, legitimate phone numbers from the employer were spoofed.

Information was collected about individually targeted employees, usually by "mass scraping of public profiles on social media platforms, recruiter and marketing tools, publicly available background-check services, and open-source research," according to the FBI and CISA. Collected information included names, home addresses, personal cellphone numbers, job titles and the length of time employees had been with the company.

"With the mass shift to large-scale work-from-home environments, cybercriminals and hacker groups are employing increasingly creative tactics to take advantage of weakened security protocols and overly trusting employees," said Kevin Cloutier, a partner in the Chicago office of Sheppard Mullin. "Before the pandemic and the sudden increase in remote workforces, vishing scams were not uncommon. However, since July 2020, vishing scams have evolved into coordinated and sophisticated campaigns aimed at obtaining a company's confidential, proprietary and trade-secret information through the company's VPN with the help of the company's own employees."

According to Brian Krebs, a cybersecurity expert and journalist based in Arlington, Va., the attacks have had "a remarkably high success rate," and some of the world's biggest corporations have been targeted, primarily in the financial, telecommunications and social media industries.

SHRM RESOURCE SPOTLIGHT

Remote Work (www.shrm.org/ResourcesAndTools/Pages/Remote-Work.aspx)

Allison Nixon, chief research officer at Unit 221B, a cyberthreat intelligence firm in New York City, explained what makes schemes like this particularly effective. Due to the coronavirus pandemic and the shift to working from home, she said, employees are more likely to use personal devices without the controls and access restrictions of their corporate computer systems, or they are using hastily set up VPN services.

"Most importantly, though, employees working from home are more vulnerable to certain kinds of social engineering attacks," she said.

That's because remote workers are more isolated and distracted, said Linn Freedman, a partner in the Providence, R.I., office of Robinson & Cole. "They do not have onsite support and are, in general, more casual about cybersecurity than when they are working in the office," she said. "It is human nature to not be as vigilant when working in one's kitchen than when working in a formal office environment. Attackers know this and are banking on the fact that workers are distracted. It is just harder to focus. As a result, they may not be as vigilant and may be more susceptible to these attacks."

Nixon said that, for example, "when in the office, employees can see each other face to face, and authenticating each other isn't a problem. But as they migrated to working remotely, they were more willing to trust telephone calls they received on their cellphones, which appear to be coming from someone within their employer's domain."

The FBI and CISA advised companies to consider instituting a formal process for validating the identity of employees who call each other. In addition, the agencies recommend companies restrict VPN connections to managed devices only, restrict VPN access hours, and employ domain monitoring to track the creation of or changes to corporate brand-name domains.

Remote workers should be more vigilant in checking Internet addresses, more suspicious of unsolicited phone calls and more assertive in verifying the caller's identity with the company.

"Companies should continue to engage and train employees on proper network usage, security concerns and when to call a secure IT number," Cloutier at Sheppard Mullin said. "Companies should regularly remind employees to be suspicious of any request for their logins and credentials or other personal information, and remind employees where to go and whom to contact if they have any security concerns."

Freedman said employers must continue to educate employees on these types of attacks; give tips on how to prevent them; and stay connected with their remote workforce by providing frequent, meaningful educational materials to build awareness and vigilance.

CISA has routinely advised employers to patch their VPNs, strengthen existing security and implement multifactor authentication, as many employees continue to log in to corporate networks from their homes during the pandemic.

"COVID-19 isn't going away anytime soon, and we won't be returning to in-person authentication for a long time," Unit 221B's Nixon said. "To prevent against future hacks, it's important for companies to be aware of the shifting techniques used in the hacker communities. This means being involved in threat intelligence, gathering information about what threat actors are doing, sharing information back with other targeted companies and staying up-to-date on what everyone else is seeing."