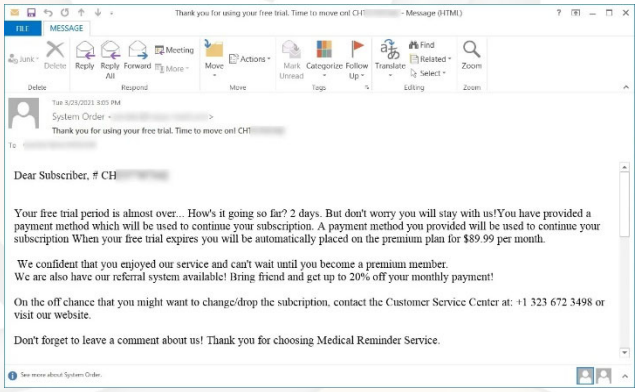
Callback Phishing Scams Evolve Via Social Engineering



Callback phishing operations have evolved their social engineering methods, keeping old fake subscriptions lure for the first phase of the attack but switching to pretending to help victims deal with an infection or hack. Successful attacks infect victims with a malware loader that drops additional payloads such as remote access trojans, spyware, and ransomware. Callback phishing attacks are email campaigns pretending to be high-priced subscriptions designed to lead to confusion by the recipient as they never subscribed to these services.

Enclosed in the email is a phone number the recipient can call to learn more about this "subscription" and cancel it. However, this leads to a social engineering attack that deploys malware on victims' devices and, potentially, full-blown ransomware attacks. According to a new report by Trellix, the latest campaigns target users in the United States, Canada, the UK, India, China, and Japan.

It all started with BazarCall

Callback phishing attacks first appeared in March 2021 under the name "BazarCall," where threat actors began sending emails pretending to be a subscription to a streaming service, software product, or medical services company, giving a phone number to call if they want to cancel the purchase. When a recipient called the number, the threat actors walked them through a series of steps that led to downloading a malicious Excel file that would install the BazarLoader malware. BazarLoader would provide remote access to an infected device, providing initial access to corporate networks and eventually leading to Ryuk or Conti ransomware attacks. Over time callback phishing attacks have emerged as a significant threat as they are now used by numerous hacking groups, including the Silent Ransom Group, Quantum, and the Royal ransomware /extortion operations.

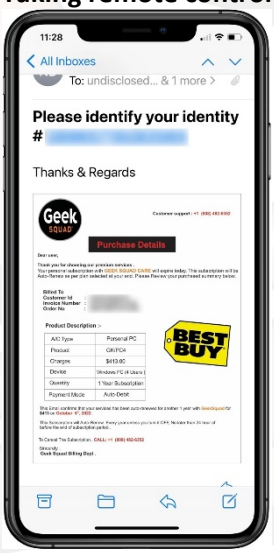
New social engineering tricks

The social engineering process has changed in recent callback phishing campaigns, although the bait in the phishing email remains the same, an invoice for a payment made to Geek Squad, Norton, McAfee, PayPal, or Microsoft. Once the recipient calls the scammer on the provided number, they are requested to give the invoicing details for “verification.” Next, the scammer declares that there are no matching entries in the system and that the email the victim received was spam.

Then, the supposed customer service agent warns the victim that the spam email may have resulted in a malware infection on their machine, offering to connect them with a technical specialist. After a while, a different scammer calls the victim to help them with the infection and directs them to a website where they download malware masqueraded as anti-virus software. Another variant used in the PayPal-themed phishing attacks is to ask the victim if they use PayPal and then allegedly check their email for compromise, claiming that their account was accessed by eight devices spread across various locations worldwide. In the security software subscription renewal campaigns, the scammers claim that the security product pre-installed with the victim’s laptop expired and was automatically renewed to extend protection.

Eventually, the scammer directs the victim to a cancelation and refund portal, which is, again, the malware-dropping site. The result of all of these campaigns is convincing the victim to download malware, which could be BazarLoader, remote access trojans, Cobalt Strike, or some other remote access software, depending on the threat actor.

Taking remote control of devices



Trellix says the majority of these recent campaigns are pushing a ClickOnce executable named 'support.Client.exe,' that, when launched, installs the ScreenConnect remote access tool. "The attacker can also show a fake lock screen and make the system inaccessible to the victim, where the attacker is able to perform tasks without the victim being aware of them," explains Trellix. In some cases seen by the security analysts, the scammers opened fake cancellation forms and asked the victims to fill them out with their personal details.

Finally, to receive the refund, the victim is urged to log in to their bank account, where they are tricked into sending money to the scammer instead. "This is achieved by locking the victim's screen and initiating a transfer-out request and then unlocking the screen when the transaction requires an OTP (One Time Password) or a secondary password," explains the Trellix report.

"The victim is also presented with a fake refund successful page to convince him into believing that they have received the refund. The scammer may also send an SMS to the victim with a fake money received message as an additional tactic to prevent the victim from suspecting any fraud."

Of course, losing money is only one of the problems that infected users can face, as the threat actors can drop additional, nastier malware at any time, spying on them long-term and stealing highly sensitive information.

Prevention

Because traditional anti-phishing software does not detect callback phishing emails, it is important for organizations to train their staff on how to spot one. As stated previously, callback phishing attempts start off as an email and will encourage the target to call a number to speak with a customer service representative about a subscription or bill. Here are a few ways you can help keep your organization safe and secure from callback phishing attempts:

- **Review** – Organizations and individuals should ensure that they know when there is a legitimate company trying to reach them. One can do this by clicking on the email sender's email address and verifying if the sender is from the expected organization's domain. If there are any misspellings or suspicious characters in an email address, then the sender is likely trying to spoof a company.

- **Ask yourself some questions** – If language in an email keeps trying to convince you to do something with urgency, that is a red flag. Cybercriminals are always very persistent in their phishing emails and just like traditional phishing emails, they will try to be convincing in getting you to call a phone number. Be diligent in verifying telephone numbers before calling, just as you would for traditional phishing emails with suspicious links. Always look up contact numbers from the organization's official website.

- **Ask for help** – If you follow the above steps and are still skeptical about the email, reach out to someone for help. Your IT team will more than likely help you and do further digging. A false alarm is better than setting off a real one.