Cybercrime Group Uses G Suite, Physical Checks in BEC Scam

(CSB20-03)

An African cybercrime group named Exaggerated Lion uses G Suite and physical checks as new tools for Business Email Compromise (BEC) attacks, as disclosed in a research paper by Agari. Like other BEC scams, the targets belong to company departments that handle finance.

The threat actors behind this particular scam sent emails requesting their targets to mail a check to a vendor. Later on, they added fake invoices and other forms to make the email more believable. When entertained with a positive response, the group replied with addresses where the check can be sent. These addresses belong to likely unwitting check mules who will then forward the money to the threat group.

Sending emails through G Suite

The threat group used G Suite, a collection of Google productivity apps such as Domains, Gmail, Drive, Docs and Sheets, to send emails. The researchers noted the benefits of using G Suite for the group: it has 30-day free trial for each domain, and doesn't require the threat actors to set up other infrastructure (such as SMTP server) for sending emails. The group can also maximize the emails sent in a day, as the suite allows users to send 500 during the trial period and 2,000 beyond it.

The group used domains that are very long, with the words separated with hyphen. Some of the words they used were "secure", "ssl", "portal", "server", "apps", "office", "mail", and "executive", making it appear like the domains are secure and associated with a company executive.

Transferring money through checks

The threat group took advantage of check mules to serve as an intermediary between them and their victims. These check mules were victims of romance scams, lured through fake personas curated by the group. The threat actors establish a "romantic relationship" with the victims over time; it wasn't made clear whether these connections were cultivated offline, online, or both.

The fake personas then ask help from the romance scam victims to recover a massive inheritance. They claim that the money had to be distributed gradually over time as the money is still tied up with lawyers. The victims who agree became unwitting check mules who were asked to encash checks and mail the money, open new bank accounts, and perform other bank transactions.

The group also groomed newer check mules (who they entrusted with less money) and wire transfer mules. The researchers believe that the use of physical checks can be traced to the cybercriminal group's forays as check fraud scammers

Defending against BEC Attacks

Personnel should pay attention to emails that request fund transfers and verify the identity of the sender through other known means, such as in-person verification or through via a phone call, before pushing through with the transaction.

Personnel should also watch out for a change in the email address and writing style of the sender of the email. If the email has grammatical errors, misspellings, or generally a style that is different from what is usually received from the supposed sender, these can be signs of a scam.

For more information on how to check an email you can download a learning material in this link **bit.ly/2SWASgt**

REFERENCE

- https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/powerghost-spreads-beyond-windows-devices-haunts-linux-machines