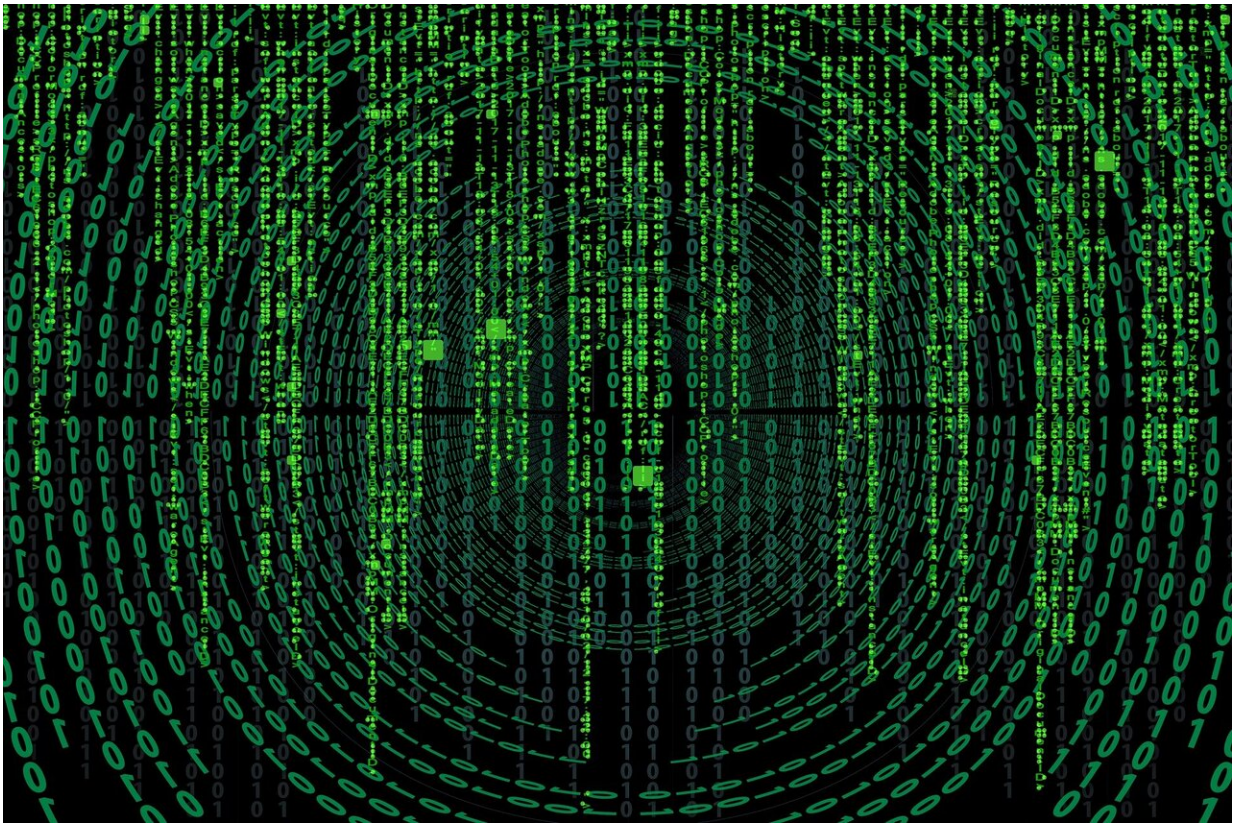
Microsoft issues warning about a malware campaign involving a call center

June 24 2021, by Bob Yirka



Credit: CC0 Public Domain

Microsoft, via its Security Intelligence account on Twitter, has issued a warning to Windows users of a new type of phishing scam that involves emails requesting users to dial a call center. They warn users to not dial

the call center because following the instructions given by a human operator can lead to malware infections. The malware scam only works with Windows computers that have Microsoft Excel.

The new threat involves BazarLoader, a type of malware that allows backdoor access to infected computers. BazarLoader works by allowing criminals to sneak in through a hidden backdoor on a user's computer, which allows them to install viruses or other types of malware. Over the past several years, criminals have used different methods to trick users into carrying out instructions that allow BazarLoader to infect their computer. In this new campaign, Microsoft reports that such criminals are using an email/call center approach.

The new approach involves an email sent to users. The email claims that a trial subscription is about to expire and that the user's credit card is going to be used to automatically charge them unless they dial a specified number. If a user falls for the message and calls the center, a human being answers and claims that all they need to do is download a certain Excel spreadsheet.

After they do so, the victim is instructed to enable macros on the file, which paves the way for an infection by BazarLoader. The criminal operator at the fake call center then tells the victim that the subscription has been revoked and that their credit card will not be charged. But those infected are then at risk of private data theft from the criminals running the new BazarLoader campaign. as they have given themselves direct access. Users also run the risk of a ransomware attack. A group called malware-traffic-analysis.net has posted a video of the process on YouTube. Users can avoid being scammed by simply ignoring the initial email.

As part of its tweet, Microsoft reports that they are tracking the campaign.

More information: unit42.paloaltonetworks.com/bazarloader-malware/

github.com/microsoft/Microsoft … r/Campaigns/Bazacall