Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

November 13, 2014

Alert Number
I-111314-PSA

NEW TWIST TO THE TELEPHONE TECH SUPPORT SCAM

The IC3 has produced Scam Alerts in the past advising the public of an ongoing telephone scam in which callers purport to be an employee of a major software company. The callers have strong foreign accents. The callers report the user's computer is sending error messages and numerous viruses have been detected. The caller convinces the user to give them permission to run a program allowing the caller to gain remote access. The caller advises the virus can be removed for a fee.

Intimidation tactics used in this scam have influenced victims to pay fees associated with the removal of alleged viruses. It has been reported to the IC3 an individual who paid the required fees, later received a call advising the victim the funds paid for the services went to India and were used to purchase weapons for ISIS. The call came with an additional request for money to remove the victim's name from a black list.

In a new twist to the tech support scam, cyber criminals attempt to defraud using another avenue. The scam is executed while a user is browsing the Internet. In this scenario, a website being viewed provided a link to articles related to popular topics. The user clicked the link and was redirected to a website which produced a window that advised the user's computer had been hacked. Another window was displayed that contained a telephone number to obtain assistance. The user reported all attempts to close the windows were ineffective. Upon calling the number for assistance the user was connected with an individual who spoke with a heavy foreign accent claiming to be an Apple representative. During the process the user's web browser was hijacked. Restarting the computer in an attempt to regain access to the Web produced another message with a different telephone number to obtain assistance.

The execution of this fraud is similar to what was reported in a Public Service Announcement (PSA) dated 07/18/2013. The PSA reports on a version of ransomware that targets OS X Mac users. This version is not a malware; it appears as a webpage that uses JavaScript to load numerous iframes (browser windows) and requires victims to close each iframe. The cyber criminals anticipate victims will pay the requested ransom before realizing all iframes need to be closed. The full PSA can be found at https://www.ic3.gov/media/2013/130718-2.aspx

If you are a victim of this scam or a similar scheme it is suggested:

- To file a complaint at www.IC3.GOV
- Resist the pressure to act quickly
- Be cautious of clicking on unknown links