(U) VFC Highlight #17-04: Tech Support Scams

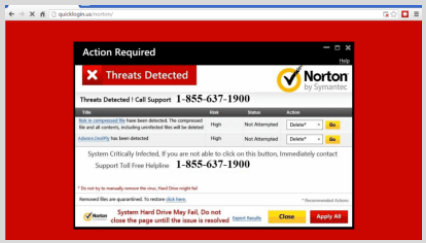
Date 04/04/2017; Tracked by: HSEC-1

According to the Internet Crime Complaint Center, "from January 1, 2016, through April 30, 2016, the IC3 received 3,668 complaints with adjusted losses of $2,268,982."

(U) *Key Points*

- (U) A tech support scam is an attempt to either gain remote access to an individual's electronic device, commit fraud, or both by claiming that the individual has viruses on their device that need *immediate* attention.
- (U) Any electronic device, no matter the operating system, with Internet capabilities can be vulnerable to a tech support scam.
- (U) The most common methods criminals use to initiate tech support scams include:
  - **Vishing (Voice Phishing)**: social engineering that occurs over the telephone in order to gain remote access to an individual's electronic devices or personal identifying information
  - **Adware**: unwelcome advertisements typically in the form of pop-ups
    - Adware may also present as an **Advanced Persistent Threat (APT)** which make the appearance of pop-ups *persistent* and difficult to exit.
- (U) Vishing tech support scammers will often call back at a later date offering a refund for services rendered previously and initiate a whole new scam.

(U) *Examples of Adware Pop-Ups*



(U) *Prevention*

- (U) Do not allow unverified remote access to your accounts, computers, or other devices.
- (U) Do not give credit card information, passwords, or personal identifying information over the phone to unknown individuals.
- (U) Do not send or wire transfer money to unverified individuals or businesses.
- (U) If you suspect a vishing attempt in the workplace, tell the individual that you will have your supervisor contact him/her if they will provide their name, employee code or ID number and a phone number. Politely terminate the call and report the incident to your IT security department.
- (U) If you suspect a vishing attempt at home, terminate the call and contact your affiliated tech support or account support directly. File a complaint with the Internet Crime Complaint Center (IC3).
- (U) If a tech support pop-up appears in your browser, exit out of the pop-up and the entire browser. Do not follow the instructions in the pop-up.
- In the event of an APT, locate your operating system's task manager and end the application.
- (U) Adjust your browser settings to block pop-ups and enable access to trusted sites as necessary.
- (U) Adjust your browser settings to enable temporary storage removal each time you exit the browser.
- (U) Do not save your credentials/passwords in your browser.

(U) Please report any information pertaining to tech support scams to the VFC at VFC@vsp.virginia.gov.