Cyber Intel Advisory
November 3, 2014, IA2014-0847

Tech Support Call Scam Leads to Malware & Financial Loss

Integrated Intelligence Center
Multi-State Information Sharing and Analysis Center
William F. Pelgrin, President and CEO

Risk: ***medium*** *probability of occurrence – Impact:* ***potential high*** *impact event*

The Risk: Malicious actors use call centers to cold call victims in an attempt to gain access to the victim's computer, install malware, steal personally identifiable information (PII), and receive monetary gain.

This is a reissue of the October 2013 Cyber Intel Advisory and includes new variants of the Tech Support Call Scam.

The Threat: A malicious actor, claiming to work for a well-known software or technology company cold calls victims in an attempt to convince them that their computer is at risk of attack, attacking another computer, or is infected with viruses, and that only the caller can remediate the problem. Victims who comply with the caller's requests are highly likely to have their computer systems compromised, as well as potentially experience monetary loss. Victims may receive the calls at work or home, and on cell phones or landlines.

The Event: While there are variations of the scam, most follow a similar script:

- Introduction: The caller informs the victim that their computer is sending out error messages, attacking another computer, or exhibiting behaviors indicative of viruses. The caller claims that only they can repair the problem for the victim or that the problem can be fixed with a software upgrade.
- Gaining Trust: The caller may attempt to gain the victim's trust by instructing the victim to access the Windows Event Viewer, which displays standard messages about the computer's operations, including general warning and error messages that are normal for the computer. The caller states these warnings and error messages are proof of malicious activity. Additionally, the caller may use technical terms to confuse the victim or gain credibility, or be forceful and attempt to create a sense of fear or urgency.
- "Fixing" the Problem: The caller will offer to fix the problem by installing an update, or requesting remote access to the victim's computer; however, the "updates" and remote access programs are actually malware.
- Charging for Service: The caller may request the victim's credit card information, or direct the victim to a website to enter their credit card number and personal information, in order to charge the victim for services rendered or for the software package provided. In a new variant, the caller may delete files from the victim's computer and demand the victim pay $200 to restore the files. Another variant has the caller requesting the victim to log in to an account and then turn off the computer monitor, thereby allowing the caller to make changes to the victim's account without their knowledge.

- Further Victimization: In November 2013, the Internet Crime Complaint Center[U.S. entity] (IC3) alerted previous victims that the same malicious actors may call and offer a refund, allegedly for dissatisfaction or the company going out of business. The caller uses the refund offer as an opportunity to gain remote access to the victim's computer or collect financial information, resulting in additional monetary loss.

The Implications: In most cases, the main motive for conducting this scam is monetary gain, which could be achieved through two possible means:

- Financial Fraud: The caller may request monetary reimbursement for services rendered or for the software installation. If the victim provides credit card or financial information, the caller can charge the incorrect amount or make additional unauthorized charges.
- Malware: It is highly likely malware will be installed if the victim provides the caller with remote access to the computer or installs unknown programs. Malware can be used to install additional malware or collect sensitive information such as usernames and passwords, which could lead to compromised financial institution accounts.

The Action:

If you receive a call:

- If you receive an unsolicited telephone call from a technology company, hang up and report the incident to either your local police department, Information Technology (IT) department, or IC3 (www.ic3.gov). Most legitimate technology companies will not directly call a computer owner, unless the owner requested assistance.
- Do not rely on caller identification (Caller ID) to authenticate a caller. Callers can spoof telephone numbers so they appear to be coming from another location or entity.
- Never provide sensitive information such as passwords and financial information over the telephone.
- Do not turn computer monitors off at the request of callers; legitimate organizations will never request the computer monitor be turned off and will not cold call users.

If you previously received a call:

- If you provided password information, change the password for that account. Never use the same password for multiple accounts.
- Use a credible anti-virus program, and enable automatic installation of software patches. If malware may have been downloaded, run an anti-virus scan on the computer.
- If the caller charged a credit card account, call the credit card provider and request to reverse those charges. Check financial statements for other unauthorized charges.
- Register your telephone number on the National Do Not Call Registry (www.donotcall.gov) and report any further solicitation calls.

Organizations have permission and are encouraged to co-brand and redistribute this advisory in whole for educational, non-commercial purposes. The information in this document is current as of November 3, 2014. Citations and more information regarding potential cyber threats are available by contacting:

IT Security Group(ITSG)
DoIT-Security@doit.nh.gov

Center for Internet Security
518-266-3460 · IIC@cisecurity.org
www.cisecurity.org