PRODUCT & SERVICE GUIDE

Tax season scams that tax preparers need to worry about

The last thing you need in the middle of tax season is to be hit by scammers trying to plant malware on your computer and force you to make payments to them.

Dave McClure • Jan. 31, 2014

From Dave McClure's Bleeding Edge blog.

The last thing you need in the middle of tax season is to be hit by scammers trying to plant malware on your computer and force you to make payments to them.

The Internet Crime Complaint Center (http://www.ic3.gov), a joint effort of the National White Collar Crime Center and the Federal Bureau of Investigation, is currently warning about two scams, the Citadel Malware Extortion Scam and the Tech Support Scam.

Here are the reports, taken from the IC3 web site:

Citadel Malware Extortion

A new extortion technique is being deployed by cyber-criminals using the Citadel malware platform to deliver Reveton ransomware. The latest version of the ransomware uses the name of the Internet Crime Complaint Center to frighten victims into sending money to the perpetrators. In addition to instilling a fear of prosecution, this version of the malware also claims that the user's computer activity is being recorded using audio, video, and other devices.

As described in prior alerts on this malware, it lures the victim to a drive-by download website, at which time the ransomware is installed on the user's computer. Once installed, the computer freezes and a screen is displayed warning the user they have violated United States Federal Law. The message further declares that a law enforcement agency has determined that a computer using the victim's IP address has accessed child pornography and other illegal content.

To unlock the computer, the user is instructed to pay a fine using prepaid money card services. The geographic location of the user's PC determines what payment services are offered. In addition to the ransomware, the Citadel malware continues to operate on the compromised computer and can be used to commit online banking and credit card fraud. Below is a screenshot of the new variation.

This is not a legitimate communication from the IC3, but rather is an attempt to extort money from the victim. If you have received this or something similar do not follow payment instruction.

It is suggested that you:

- File a complaint at www.IC3.gov.
- Keep operating systems and legitimate antivirus and antispyware software updated.
- Contact a reputable computer expert to assist with removing the malware.

Online Tech Support Scam

The IC3 continues to receive complaints reporting telephone calls from individuals claiming to be with Tech Support from a well-known software company. The callers have very strong accents and use common American names such as “Adam” or “Bill.” Callers report the user's computer is sending error messages, and a virus has been detected. In order to gain access to the user's computer, the caller claims that only their company can resolve the issue.

The caller convinces the user to grant them the authority to run a program to scan their operating system. Users witness the caller going through their files as the caller claims they are showing how the virus has infected their computer.

Users are told the virus could be removed for a fee and are asked for their credit card details. Those who provide the caller remote access to their computers, whether they paid for the virus to be removed or not, report difficulties with their computer

afterwards; either their computers would not turn on or certain programs/files were inaccessible.

Some report taking their computers to local technicians for repair and the technicians confirmed software had been installed. However, no other details were provided.

In a new twist to this scam, it was reported that a user's computer screen turned blue, and eventually black, prior to receiving the call from Tech Support offering to fix their computer. At this time, it has not been determined if this is related to the telephone call or if the user had been experiencing prior computer problems.

These scams are just as likely to hit small businesses as they are home computers, and accounting firms should consider passing this information along to their clients.

Product & Service Guide • Tax • Blog • Blogs • IC3 • Income Tax Refunds • Internet Crime • Tax Preparation • Tax Scams