ESJ Enterprise Systems Journal
High-End Datacenter and Server Solutions

Ramsomware Poses New Threat to Users

A new exploit poses as law enforcement to trap users into paying to unlock their system What you need to know about the exploit and how to keep your users safe.

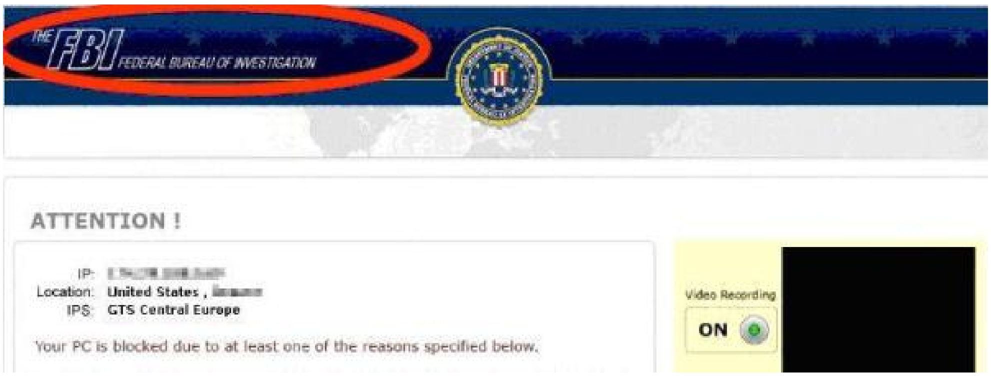
12/12/2012

By Alvin Estevez

In the last two months, there has been a dramatic spike in a relatively new kind of malware. It's called ransomware and it's the next evolution in the efforts of Internet thieves to separate unsuspecting victims from their money. This time, they're pretending to be law enforcement agencies collecting fines for illegal computer activity. Perhaps even more disturbing is the way these crooks are collecting their "fines."

Here's how the police ransomware scam works: Internet crooks create a malware infection that gets onto a computer any number of ways: phishing e-mails, ads on adult Web sites, downloadable executable files posing as video player codecs, etc.

Some time later, the victim's screen freezes and a message pops up with an official looking law enforcement logo telling them their computer has been frozen because of suspected illegal activity. Note the FBI header (see figure below) from an infection called FBI Moneypak.



ATTENTION !

IP: [redacted]
Location: United States , [redacted]
IPS: GTS Central Europe

Your PC is blocked due to at least one of the reasons specified below.

This particular message tells the victim someone using their computer is suspected of everything from "illegally using or distributing copyrighted content" to viewing and distributing child pornography. The only way to "unlock" your computer is to pay a "fine. Note the "Video Recording" icon in the lower right hand part of the screen. This infection even turns on your computer's web camera to make it seems as though your image is being recorded and sent to authorities.

Although these police ransomware infections have been around for a while, in the last few months, they have spiked dramatically. At SpyWareRemove.com, a site that tracks malware infections, we've seen a jump in traffic of 460 percent for the **FBI Moneypak** infection in early October alone.

The **UKash virus** is a similar ransomware infection, this one purports to be from a European law enforcement agency.

UKash and the FBI Moneypak infection currently account for more than 25 percent of the people coming to SpyWareRemove.com looking for help to remove infections.

These ransomware infections are particularly effective because many times they are planted in somewhat seedy corners of the Internet: porn sites and movie download sites. The victims may have actually been doing some of the activities these fake police messages allege, which may make folks think the warning is legit.

How do these fake infections collect their “fines”? That’s a new wrinkle as well. Most scareware or ransomware requires you to actually make a credit card payment of some sort. The hackers can only collect money if they can find a way to process those payments. Many times they will find a shady processor overseas in Russia or Eastern Europe.

1 2 NEXT »

Most Popular Articles

Free Webcasts

Simplifying Hyper-V Backups with the Public Cloud

Finding the Right Backup Model for Your Business

> More Webcasts

Application Development Trends

AWSInsider.net

MCPmag.com

Redmond

Redmond Channel Partner

Virtualization Review

Visual Studio Magazine

1105 MEDIA INC.
YOUR GROWTH. OUR BUSINESS.