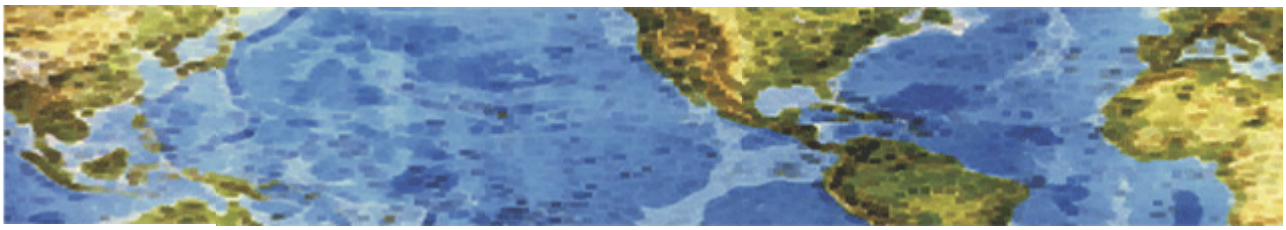
HALL ASSOCIATES



Risk-Based Decision Making Commentary

5 January 2014 Newsletter

Prison Locker Ransomware, an upcoming malware threat in 2014

Ransomware is a type of malware that tries to extort money from you. One of the nastiest examples we have noted before is CryptoLocker, which takes your files hostage and holds them for ransom, forcing you to pay hundreds of dollars to regain access. Most of this type of malware is no longer created by bored teenagers looking to cause some chaos. Much of the current malware is now produced by organized crime for profit and is becoming increasingly sophisticated. Ransomware is one of the most blatant and obvious criminal's money-making schemes out there. And many money motivated cyber criminals have started developing their own Cryptolocker versions. Two hackers are advertising a new ransomware malware tool-kit called "Prison Locker" on various hacking forums with tutorials. They have developed the Prison Locker (or Power Locker) ransomware toolkit in C/C++ programming language, proving a GUI version with customizable features for customers.

The Ransomware is using BlowFish encryption to encrypt all available files on the victim's hard disk and shared drives except .exe, .dll, .sys, other system files. During encryption it will generate a unique BlowFish key for each file and then encrypts the keys further with RSA-2048 encryption and will send the victim's system information back to the command-and-control center of the attacker.

As the developer mentions in a Pastebin post, the command-and-control center allows an attacker to set the ransomware warning time duration, ransom amount, payment mode and also allow decrypting the files on the victim system after payment is received. The additional features added to Prison Locker are:

- The malware is able to detect Virtual Machine, Sandbox mode, and debugging environments.
- It will disable Windows key & Escape key to prevent unwanted user actions.
- Can kill taskmgr.exe, regedit.exe, cmd.exe, explorer.exe, and msconfig.exe processes to prevent unwanted user actions.
- Malware can startup in both regular boot mode and safe boot under HKCU.

As discussed before in this newsletter, the only way to avoid this is be careful what links or web sites you click on and make sure you back up your files to a location where they cannot be written to or erased.

http://thehackernews.com/2014/01/power-locker-ransomware-upcoming_3.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog%29&_m=3n.009a.449.wb0ao05fi9.9ka#

HALL ASSOCIATES

Hackers steal from ATMs using Malware-loaded USB Device

Hacking ATM Machines is nothing new, but it seems that instead of relying on ATM skimmers some smart hackers in Europe are targeting ATM Machines using malware-loaded USB drives to steal money. This has been reported only in Europe so far, but as most of the world's ATMs are running on Windows XP operating system, which is highly vulnerable to Malware attacks, it is simply a matter of time (and not much of that) before we start seeing this in the US.

Not many people know this, but most of the world's ATMs run some flavor of Windows. In the olden days, it wasn't too unusual to find an ATM that had crashed with a blue screen of death and to this day it's still fairly common to hear the standard Windows "ding" when interacting with an ATM. A conventional ATM might consist of a standard Windows XP PC (or perhaps XP Embedded), connected to a display, a secure keypad, cryptoprocessor, various other bits of hardware, and of course the vault (where the money is stored). The ATM boots up normally, then launches into a full-screen program that manages all of the tasks that a customer might want to carry out.

Unfortunately, just like your Windows PC, some ATMs also have USB sockets — and just like your PC, some ATMs will automatically boot whatever's plugged into the USB socket. The USB socket is hidden behind the ATM's fascia, but it can be revealed if you know where to cut — and once you've loaded the malware on, you can easily cover up the hole. If you have knowledge of the ATM's software, it's possible to use malware to inject new features, or disable existing ones. In a word, once you've infected the ATM, it's fairly easy to steal its money with complete impunity

This malware creates a backdoor that can be accessed on the front panel. The malware allowed the thieves to create a unique interface on the ATMs by typing in a 12-digit code. This interface allowed for withdrawal and also showed the criminals the amount of money and each bill denomination inside the machines. This meant the thieves could save time by only taking the highest value bills. Once the thieves finished their theft at a cash machine, they would patch up the hole to allow the same exploit to be used on other machines. This indicates that the criminal crew is highly familiar with the ATMs' mechanism. The malware does not appear to harvest customer PINs or other sensitive data and now some European banks have upgraded their ATMs to prevent them from booting from external USB drives. This exploit should be of interest to US financial institutions and other organizations that use ATMs.

http://thehackernews.com/2014/01/hacking-ATM-machine-Malware-USB-Drive.html
http://www.extremetech.com/extreme/173701-atms-running-windows-xp-robbed-with-infected-usb-sticks-yes-most-atms-still-run-windows