Windows XP ATM's Under Hacker Attacks in Europe - US Could Be Next!

June 4 2009, by John Messina

(PhysOrg.com) -- There have been approximately 20 ATM's in Eastern Europe that have been compromised. These attacks are in the early stages of development and would probably gain momentum and even spread to US ATM machines.

A security outfit, TrustWave's SpiderLabs performed the analysis of malware found installed on compromised ATMs in the Eastern European region. The ATM's that were compromised ran Microsoft Windows XP. The malware captures magnetic stripe data and PIN codes from the private memory space of transaction-processing applications installed on infected ATM.

The attacker can gain full control of the infected ATM through a customized user interface built into the malware. This is accomplished

by inserting a controller card into the ATM's reader.

TrustWave's analyses don't believe the malware has networking functionality that would send data to other, remote locations over the Internet. The malware would output the harvested data through the ATM's receipt printer or write the data to a storage device inserted into the ATM's card reader.

TrustWave stated; "this malware is unlike any we have ever had experience with. It allows the attacker to gain complete control over the ATM to obtain track data, Pins and cash from each infected machine."

"We believe the current attack vector is an early version of the malware sample, and future attacks will add functionality such as propagation via the ATM network. If an attacker can gain access to one machine, the malware will evolve and propagate automatically to other systems."

A dropper file named isadmin.exe, is installed into the ATM and executed within the C:\WINDOWS directory of the compromised machine. The malware then proceeds to control the Protected Storage service that would handle the original lsass.exe executable file, located in the C:\WINDOWS\system32 directory, to point to the infected file.

The malware is designed to remain active in the event the ATM crashes and has to restart.