Automated Teller Machine (ATM) Malware Analysis Briefing

Date: May 28, 2009

Author	Trustwave SpiderLabs
Subject	Malware Analysis Briefing Report
Project	Automated Teller Machine Malware Analysis

Malware Snapshot

Malware Sample Properties	
Malware Sample Name	lsass.exe
Compressed	☐ Yes ☒ No
Obfuscated	☐ Yes ☒ No
Armored	☐ Yes ☒ No
Rootkit	☐ Yes ☒ No
Target Platform	☒ Windows ☐ Unix
Target application	ATM card Track and PIN data processing software
File size of sample malware per this report	50176 bytes
File type / Compiler	PE32 Executable / Borland Delphi 6.0 - 7.0
File creation / installation date	July 25th 2007
MD5 Checksum	695551C68C06591C3074377D4B27682E
SHA1 Checksum	982F62C76EBDD71E31A9F61CE86FAAD7814B2568
Sizes of other known versions of this malware	41984 bytes 49664 bytes
MD5 Checksums of other known versions	113DC62206EFF20111C8CEBCDDD397FB 26A5A6E9F85656B28E2698676AEE114B D222B730441ABA903EF3F5517D071C58

Malware Sample Properties

Description:

Trustwave's SpiderLabs performed the analysis of malicious software (malware) found installed on compromised ATMs (Automated Teller Machines) in the Eastern European region. This malware captures magnetic stripe data and PIN codes from the private memory space of transaction-processing applications installed on a compromised ATM. The compromised ATMs discussed in this briefing ran Microsoft's Windows XP operating system.

The malware contains advanced management functionality allowing the attacker to fully control the compromised ATM through a customized user interface built into the malware. This interface is accessible by inserting controller cards into the ATM's card reader. SpiderLabs analysts do not believe the malware includes networking functionality that would allow it to send harvested data to other, remote locations via the Internet. The malware does, however, allow for the output of harvested card data via the ATM's receipt printer or by writing the data to an electronic storage device (possibly using the ATM's card reader). Analysts also discovered code indicating that the malware could eject the cash-dispensing cassette.

What follows is a high-level summary of the key features identified during Trustwave's in-depth analysis of the malware sample. It is, however, believed that this is a relatively early version of the malware and that subsequent versions have seen significant additions to its functionality.

Card Data Harvesting Malware - lsass.exe

Method of Infection of the ATM

The malware is installed and activated through a dropper file (a file that an attacker can use to deploy tools onto a compromised system) by the name of `isadmin.exe`. It is a Borland Delphi Rapid Application Development (RAD) executable and is essentially a replacement for the original `isadmin.exe` utility written by Bill Stewart (www.westmesatech.com/wast.html).

The dropper binary contains a Data Resource (RCDATA) named `PACKAGEINFO` which in turn contains the actual malware.

Executing the dropper file produces the malware file `lsass.exe` within the `C:\WINDOWS` directory of the compromised system and does so via functionality provided by a Windows API (Application Programming Interface).

Once the malware is extracted, the dropper proceeds to manipulate the 'Protected Storage' service—this normally handles the legitimate `lsass.exe` executable, located in the `C:\WINDOWS\system32` directory—to point towards the newly created malware. The service is also configured to automatically restart in the event that it crashes, ensuring that the malware remains active.

Targeting Track Data

The malware itself is also a Borland Delphi Graphic User Interface (GUI)-compiled executable, launched as a Microsoft Windows service. It contains the ability to enumerate the available printing devices. Once active, the malware intercepts ATM transactions by injecting code into targeted processes through the binary modification of these processes in memory.

The first process targeted by the malware appears to be a system-messaging utility, while the other is a form of ATM software service.

Once it resides in the memory, the malware polls the transaction message queue looking for track 2 data from the current transaction. It then performs a level of validation and manipulation against this track data to determine whether the transaction is the attacker's trigger or controller card or a valid transaction involving track data that the malware collects by recording it in a file. The trigger cards (either a master function card or a single function card) allow an attacker to interact with and control both the malware and the ATM.

When the parsing routine fails to identify a trigger card, the malware stores the transaction information in a temporary file named `tr12` in the `C:\WINDOWS` directory. The malware harvests transactions as well as balance enquiries provided the currency indicated is American Dollar (USD), Russian Rouble (RUR) or the Ukrainian Hryvnia (UAH).

Additionally, the malware harvests what is believed to be key or `PIN` data, saving the information in a file `C:\WINDOWS\kl`.

Primary Command Options and Functionality

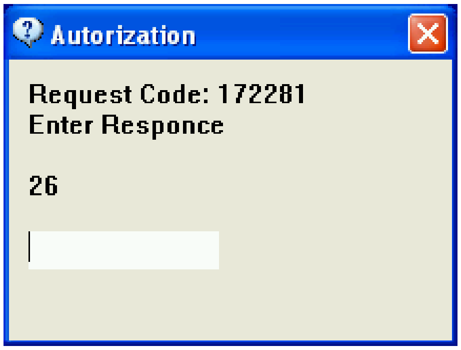
When a trigger card is detected, a small window appears giving the user 10 seconds to select one of 10 command options using the ATM's keypad.

Trustwave®

Option	Function	Possible Description
0	Restore Logs	Restore the log files to the condition prior to the malware's operation.
1	Uninstall	To uninstall itself, the malware will: - Delete the `trl2` and `kl` log files - Remove the malicious service - Restore the original `lsass.exe` executable - Finally, delete the malicious `lsass.exe` file
2	Display Stats	Creates and displays a window presenting statistics (numbers of transactions, cards, keys) and version numbers of components ("Agilis" and "Agent").
3	Delete Logs	Deletes the harvesting log files `C:\WINDOWS\trl2` and `C:\WINDOWS\kl`
4	Reboot ATM	Adjusts the privileges of the malware and then forces a full system reboot.
5	Test Printer	This command seems to be for testing the ATM's receipt printer by printing `Hello` and `123456789`.
6	Print Collected Data	Print the harvested data, in an encrypted format, via the ATM receipt printer. The malware uses the DES algorithm for encryption.
7	Secondary Menu	This option will present the user with a window displaying a challenge and wait for the corresponding response to be entered. Further details of this secondary menu are provided below.
8	Supply Manager Information	The malware tries to access the ATM-vendor-software's user interface, authenticate using a default-password and then waits for another pop-up window that can be used to retrieve information about bills/cash present in the ATM at the time of access.
9	Unclear/Possibly writing to a smart card	Appears to be associated with memory card reader/writer functionality that may be used to transfer the harvested data directly to a card injected into a compromised ATM.

Secondary Command Menu Options

Command option 7 presents the user with a challenge window and allows the user 30 seconds to input a corresponding valid response using the ATM's keypad.

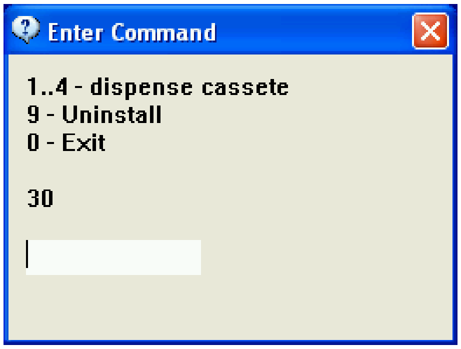


Autorization

Request Code: 172281
Enter Responce

26

If the response provided by the ATM user agrees with the malware's expectation, the following command menu is displayed.



Enter Command

1..4 - dispense cassete
9 - Uninstall
0 - Exit

30

There is evidence that the malware is executing the ATM API call which is probably related to cassette dispensing when the 'dispense cassette' options are selected.

Conclusion

Given the impact this malware can have on an infected ATM environment, Trustwave highly recommends ALL financial institutions with ATMs under management perform analysis of their environment to identify if this malware or similar malware is present.

Trustwave collected multiple version of this malware and therefore, feels that over time it will evolve. It will also begin to propagate to a more wide-spread population of ATMs, thus a proactive approach in prevention and identification will be necessary to prevent future attacks.

Contacts

The following individuals are the lead contacts for Trustwave's SpiderLabs Incident Response Team:

USA Contact Information	
Contact Name:	Colin Sheppard
Contact Phone:	312.873.7474
Contact Fax:	312.443.1620
Contact E-Mail Address:	csheppard@trustwave.com
Address:	70 W Madison St Suite 1050 Chicago, IL 60602

EMEA Contact Information	
Contact Name:	Stephen Venter
Contact Phone:	+44 207 070 5982
Contact Fax:	+44 845 456 9612
Contact E-Mail Address:	sventer@trustwave.com
Address:	8th floor, Westminster Tower 3 Albert Embankment London, UK SE1 7SP