ATM infector

By GReAT

Published: 2016-05-17 · Archived: 2026-04-02 11:20:04 UTC

Seven years ago, in 2009, we saw a completely new type of attack on banks. Instead of infecting the computers of thousands of users worldwide, criminals went directly after the ATM itself – infecting it with malware called Skimer. Seven years later, our Global Research and Analysis Team together with Penetration Testing Team have been called on for an incident response. They discovered a new, improved, version of Skimer.

Virus style infections

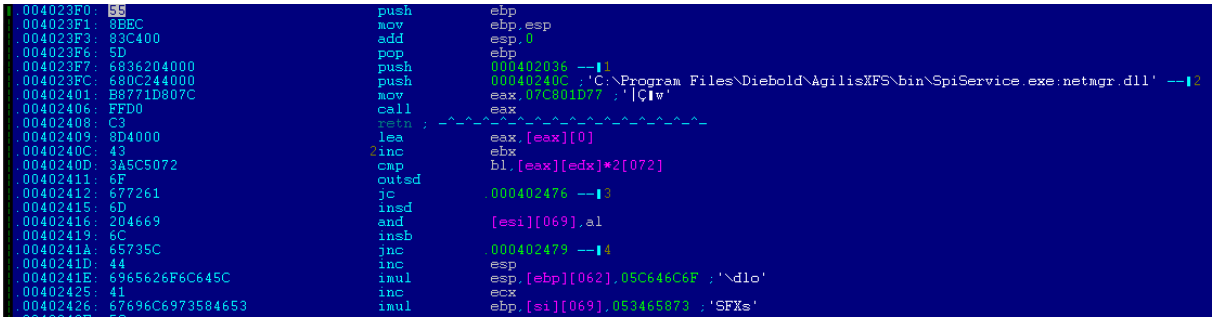
Criminals often obscured their malware with packers to make analysis more difficult for researchers. The criminals behind Skimer also did this, using the commercially available packer Themida, which packs both the infector and the dropper.

Once the malware is executed it checks if the file system is FAT32. If it is, it drops the file netmgr.dll in the folder C:\Windows\System32. If it is an NTFS file system, the same file will be placed in the NTFS data stream corresponding to the XFS service´s executable file. Placing the file in an NTFS data stream is most likely done to make forensic analysis more difficult.

After successful installation, the sample patches the XFS executable (SpiService.exe) entry point, in order to add a LoadLibrary call to the dropped netmgr.dll file. This file is also protected by Themida.

```
.00402036: 6A28                  push        028 ;'('
.00402038: 68A0384000            push        0040038A0 --▌1
.0040203D: E8FA010000            call        .00040223C --▌2
.00402042: 33FF                  xor         edi,edi
.00402044: 57                    push        edi
.00402045: FF1588304000          call        GetModuleHandleA
.0040204B: 6681384D5A            cmp         w,[eax],05A4D ;'ZM'
.00402050: 751F                  jnz         .000402071 --▌3
.00402052: 8B483C                mov         ecx,[eax][03C]
.00402055: 03C8                  add         ecx,eax
.00402057: 813950450000          cmp         d,[ecx],000004550 ;'  EP'
.0040205D: 7512                  jnz         .000402071 --▌3
.0040205F: 0FB74118              movzx       eax,w,[ecx][018]
.00402063: 3D0B010000            cmp         eax,00000010B
.00402068: 741F                  jz          .000402089 --▌4
.0040206A: 3D0B020000            cmp         eax,00000020B
.0040206F: 7405                  jz          .000402076 --▌5
.00402071: 897DE4              3mov          [ebp][-01C],edi
.00402074: EB27                  jmps        .00040209D --▌6
.00402076: 83B9840000000E      5cmp          d,[ecx][000000084],00E
```

Entry point in SpiService.exe before infection



Entry point in SpiService.exe after infection

After a successful installation the ATM is rebooted. The malicious library will be loaded into the SpiService.exe thanks to the new LoadLibrary call, providing it with full access to XFS.

Functionality

Unlike Tyupkin, where there was a magic code and a specific time frame where the malware was active, Skimer only wakes up when a magic card (specific Track 2 data, see IOCs at the bottom of this blogpost) is inserted. It is a smart way to implement access control to the malware's functionality.

Once the magic card is inserted, the malware is ready to interact with two different types of cards, each with different functions:

1. 1 Card type 1 – request commands through the interface
2. 2 Card type 2 – execute the command hardcoded in the Track2

After the card is ejected, the user will be presented with a form, asking them to insert the session key in less than 60 seconds. Now the user is authenticated, and the malware will accept 21 different codes for setting its activity. These codes should be entered from the pin pad.

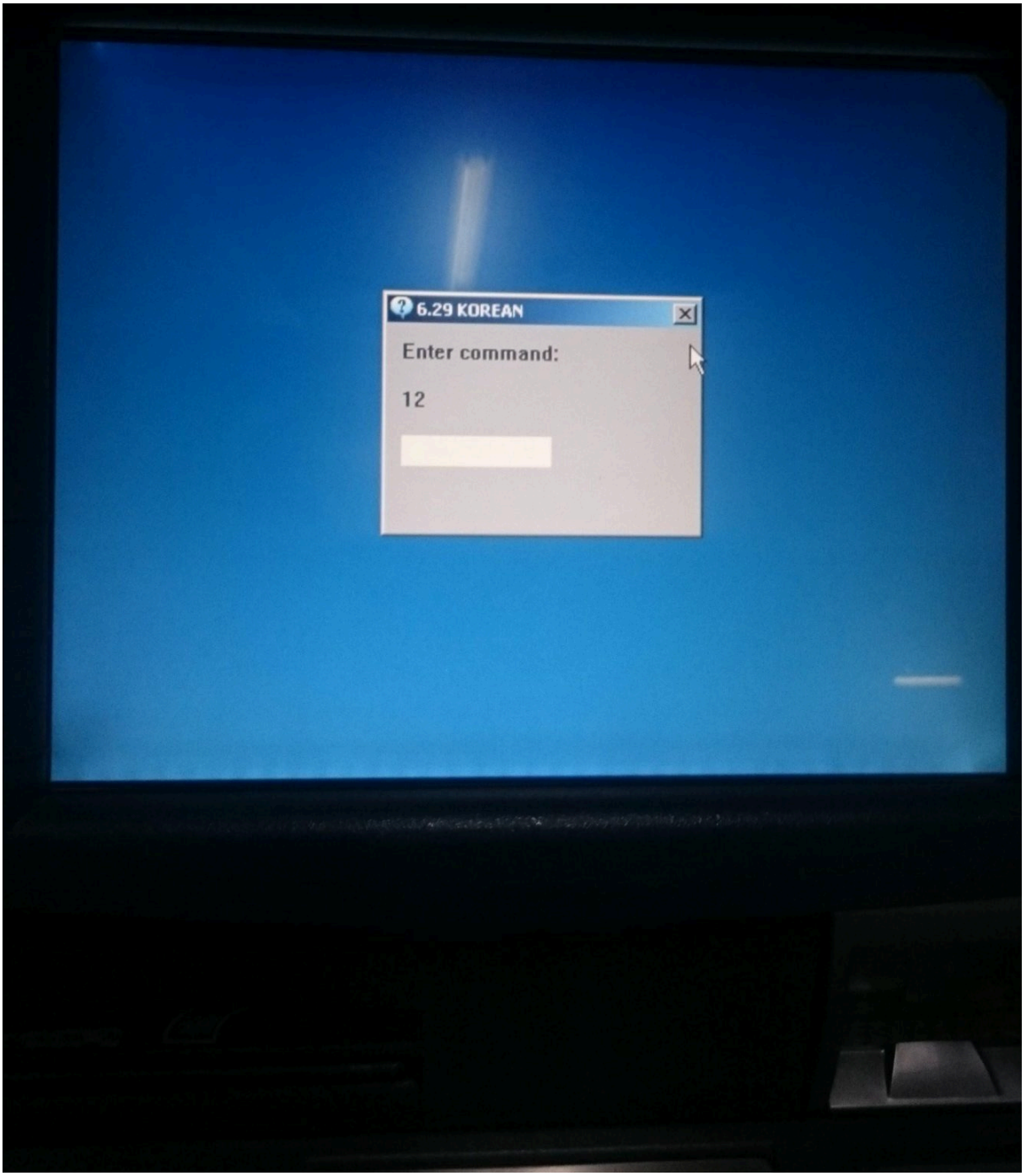
Below is a list of the most important features:

1. 1 Show installation details;
2. 2 Dispense money – 40 notes from the specified cassette;
3. 3 Start collecting the details of inserted cards;
4. 4 Print collected card details;
5. 5 Self delete;
6. 6 Debug mode;
7. 7 Update (the updated malware code is embedded on the card).

During its activity, the malware also creates the following files or NTFS streams (depending on the file system type). These files are used by the malware at different stages of its activity, such as storing the configuration, storing skimmed card data and logging its activity:

C:\Windows\Temp\attrib1	card data collected from network traffic or from the card reader;

C:\Windows\Temp\attrib4	logs data from different APIs responsible for the communication with the keyboard (effectively logging data such as the pin);
C:\Windows\Temp\mk32	
C:\Windows\Temp:attrib1	same as the homologue file;
C:\Windows\Temp:attrib4	same as the homologue file;
C:\Windows\Temp:mk32	same as the homologue file;
C:\Windows\Temp:opt	logs mule´s activity.



Main window

The following video details the scenario on how money mules interact with an infected ATM as described above.

Conclusions

During our recent Incident Response cases related to the abuse of ATMs, we have identified Tyupkin, Carbanak and black box attacks. The evolution of Backdoor.Win32.Skimer demonstrates the attacker interest in these malware families as ATMs are a very convenient cash-out mechanism for criminals.

One important detail to note about this case is the hardcoded information in the Track2 – the malware waits for this to be inserted into the ATM in order to activate. Banks may be able to proactively look for these card numbers inside their processing systems, and detect potentially infected ATMs, money mules, or block attempts to activate the malware.

We also recommend regular AV scans, the use of allowlisting technologies, a good device management policy, full disk encryption, the protection of ATM BIOS with a password, only allowing HDD booting, and isolating the ATM network from any other internal bank networks.

Kaspersky Lab has now identified 49 modifications of this malware, with 37 of these modifications targeting ATMs made by just one manufacturer. The most recent version was discovered at the beginning of May 2016.

All samples described are detected by Kaspersky Lab as Backdoor.Win32.Skimer. Patched SpiService.exe files are detected as Trojan.Win32.Patched.rb

As this is still an ongoing investigation, we have already shared the full report with different LEAs, CERTs, financial institutions and Kaspersky Lab Threat Intelligence-Service customers. For more information please contact intelreports@kaspersky.com

Appendix I. Indicators of Compromise

Hashes

F19B2E94DDFCC7BCEE9C2065EBEAA66C
3c434d7b73be228dfa4fb3f9367910d3
a67d3a0974f0941f1860cb81ebc4c37c
D0431E71EBE8A09F02BB858A0B9B80380
35484d750f13e763eae758a5f243133
e563e3113918a59745e98e2a425b4e81
a7441033925c390ddfc360b545750ff4

Filenames

C:\Windows\Temp\attrib1
C:\Windows\Temp\attrib4
C:\Windows\Temp\mk32
C:\Windows\Temp:attrib1
C:\Windows\Temp:attrib4
C:\Windows\Temp:mk32
C:\Windows\Temp:opt
C:\Windows\System32\netmgr.dll

Track 2 data

******446987512*=**********
******548965875*=**********
******487470138*=**********
******487470139*=**********
******000000000*=**********
******602207482*=**********
******518134828*=**********
******650680551*=**********
******466513969*=**********

Source: https://securelist.com/atm-infector/74772/