Pulling back the covers on credit card fraud
A detailed look at financial fraudware

Chester Wisniewski
Senior Security Advisor
@chetwisniewski
nakedsecurity
Award-winning news, opinion, advice and research from SOPHOS
How did we get here?
The greedy '80s
'90s introduces another go at the idea
I suppose I didn't have to use my card
PCI DSS is driving innovation

- Encryption in transit
- Encryption at rest
- Secure remote access
First custom, now common

A study conducted by the Verizon Business RISK Team

2009 Data Breach Investigations Supplemental Report
Anatomy of a Data Breach

14. RAM scraper

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

Targeted attacks steal credit cards from hospitality and educational institutions
What's in/on a card?

<table>
<thead>
<tr>
<th>Track</th>
<th>Recording Density (bits per inch)</th>
<th>Character Configuration (including parity bit)</th>
<th>Information Content (including control characters)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.110&quot;</td>
<td>Track 1 IATA</td>
<td>210 BPI</td>
<td>7 Bits per Character</td>
</tr>
<tr>
<td>0.110&quot;</td>
<td>Track 2 ABA</td>
<td>75 BPI</td>
<td>5 Bits per Character</td>
</tr>
<tr>
<td>0.110&quot;</td>
<td>Track 3 THRIFT</td>
<td>210 BPI</td>
<td>5 Bits per Character</td>
</tr>
</tbody>
</table>

Source: http://www.q-card.com/support/magnetic-stripe-card-standards.asp
Many cards, similar form
Let's take a look
The third generation, security and stupidity
Bad, not terrible

Track Data - Visa Contactless

%B4510155020973316^ / ^1608201101;/4510155020973 316=16082011890253010001?

Track Data - Visa Contactless

%B4510155020973316^ / ^1608201401;/4510155020973 316=16082014940254010001?
Criminals respond – RAM scraping malware

Alina
Chewbacca
VSkimmer

Troy/Trackr
Kaptoxa
Dexter
Where to begin?
Begin by scraping the RAM
Don't waste time
Trip up & hide from researchers

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

    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) = "*EXCELSOR_TECHNOLOGY_*" 'CWSandbox mwanalysis.org

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

    ZZ = SetErrorMode(1024)
    If ZZ = 0 Then bFound = True
Grab the cards
Trust, but verify

```plaintext
sListaNeagra(34) = "4555555555555555"
sListaNeagra(35) = "4999999999999999"
sListaNeagra(36) = "4026444444444444"
sListaNeagra(37) = "4026777777777777"

For i = LBound(sListaNeagra) To UBound(sListaNeagra)
If sNR = sListaNeagra(i) Then: Luhn = False: Exit Function
Next i

If Len(sNR) < 12 Then Luhn = False: Exit Function
If Len(sNR) > 19 Then Luhn = False: Exit Function

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
```
Collect data for research

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
PCI says to encrypt before exfiltration, right?
Anatomy of an attack
Characteristics
Using admin tools for evil

Dumping private memory for pid %s to %s.dmp...", 0Ah, 0

char aDone[]

0A+1 0A+aDone! db 'Done!', 0Ah, 0; DATA XREF: dump_memory+12410

char aDone_0[]

06 73 65 20+5aUseAsMemdump_exeOptionsPid db 9, 9, 'Use as: memdump.exe -<options> [PID]', 0Ah, 0

4F 70 74 69+aOptions db 9, 9, 'Options:', 0Ah, 0

02 0D 3F 20+5aShowThisHelp db 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, 9, ? = Show this help', 0Ah, 0

09 0D 6C 20+5aListAllRunningProcesses db 9, 9, 9, 9, 9, 9, 9, -l = List all running processes', 0Ah, 0

09 0D 73 20+5aShowInfoOnProcessLikePath db 9, 9, 9, 9, s = show info on process like path', 0Ah, 0

09 0D 66 20+aFDumpPrivateProcessMemoryByPid db 9, 9, 9, -f = Dump private process memory by PID', 0Ah, 0

09 0D 66 20+aFALlDumpsPrivateDumpOfAllRunningProcesses db 9, 9, 9, -f = Full private dump of all running processes', 0Ah, 0

char format[]

02 28 50 49+5aFormat db '%s', 9, (PID: %u), 9, 'Hex: %xh', 0Ah, 0

20 25 75 29+; DATA XREF: open_process+6810
A glimpse into the dark side
DIY carding

Screenshot courtesy of Xylibox.com

Beast

Join Date: Jan 2011
Funds: $0
Posts: 7
Reputation: 0

vSkimmer - Track2 grabber / POS trojan

Hello dear fraudsters,

I’m offering a POS malware, specially designed to grab every track2 swiped into a POS Terminal running Windows.

vSkimmer - Virtual Skimmer

Botnet Functions:
- Track 2 grabber
- HTTP Loader (Download & Execute)
- Update bot itself

Working Modes:
- Online: If internet is reachable it will try to bypass firewalls and communicate to the web panel.
- Offline: If internet is not reachable it wait for a specific pendrive/flashdrive plugged in and copy logs to it.

(possibility to swap to bluetooth for physical access, you say and we make)
Cost of License:
Full license: 6k one time // Limited time offer including a cool dumps shop.
Package includes:
- vSkimmer bot bin FUD* (exe) *1 file fud only, crypting service not offered.
- vSkimmer control panel (php+sql+ajax)
- With dumps shop (unique design) (php+sql+ajax)

Q: What operative systems are supported?
A: All Windows Versions should work fine. 32bits mode only.

Q: What payment methods do you accept?
A: All payments through escrow, any payment method they accept I accept too.
(I decide or refuse who will be the guarantor, you pay the fee)

Q: Is your niceware called Dexter?
A: No, software is coded by me with similar functionalities but much better =)
Selling on WordPress.com

- More reasons to distrust Yahoo!?
- Selling one-offs – high profit
- 101 – No PIN
  201 – PIN preferred
- Corp cards more resistant to fraud algos
CVV/DOB/Zip Code affect price

- Us with bin = $7/1cvv
- Uk with bin = $10/1cvv
- Uk with dob = $20/1cvv
- Uk with bin + dob = $25/1cvv
- Us fullz = $30/1cvv
- Uk fullz = $35/1cvv
- Eu fullz = $40/1cvv
- other country = ask me for price

=> when you buy bulk, i will sell for you good price

- Usa = 1$/1con (cc not cvv2 code)
- Usa visa.mc = $3/1cvv
- Usa amex.dis = $5/1cvv
- Uk visa.mc = $5/1cvv
- Uk amex.dis = $7/1cvv
- Au visa.mc = $12/1cvv
- Au amex.dis = $15/1cvv
- Ca visa.mc = $7/1cvv
- Ca amex.dis = $10/1cvv
- Eu visa.mc = $15-20/1cvv
- Eu amex.dis = $20-25/1cvv
- Asia = $15/1cvv
Cashing out near Georgia
Got gear?
Cashing out
BBQ anyone?
Chillin at the дача
Now for the stats
Who is a target

Troj/Trackr-* infections by Industry in 2013

- Service 17%
- Education 14%
- Healthcare 9%
- Food Services 7%
- IT 5%
- Manufacturing 10%
- Recreation 4%
- Government 4%
- Financial 3%
- Religious 2%
- Hotel & Tourism 10%
- Retail 12%
- Entertainment 1%
- Transport 1%
What can we do?

- Network separation is critical
- Privilege separation
- Modern OS helps
- Firewalls must be used correctly
- Provide alternate means for employees to communicate