Today's Threat Landscape

How to stay safe

Ken Swain
Sr. SE - SC TN GA
@kenotic
PenTester
Built ShadowL
Mobile Security
Agenda
Opportunistic Threat
Digital smash and grab
Methods of infection – Drive-by downloads
Typical Drive By Download
Methods of infection - Video codecs

This video cannot be played due to old version of your codecs

Update codec  Close
Phishing getting more sophisticated

Dear Facebook user,

In an effort to make your online experience safer and more enjoyable, Facebook will be implementing a new login system that will affect all Facebook users. These changes will offer new features and increased account security. Before you are able to use the new login system, you will be required to update your account.

Click here to update your account online now.

If you have any questions, reference our New User Guide.

Thanks,
The Facebook Team

This message was intended for [redacted].

Facebook's offices are located at 1601 S. California Ave., Palo Alto, CA 94304.
Phishing getting more sophisticated
Phishing getting more sophisticated

In an effort to make your online experience safer and more enjoyable, Facebook will be implementing a new login system that will affect all Facebook users. These changes will offer new features and increased account security. Before you are able to use the new login system, you will be required to update your account.

A new Facebook Update Tool has been released for your account. Please download and install the tool using the link below:

**Facebook Update Tool**

necessary to install  

`updatetool.exe`

Email

your email address
Facebook, we don't need any help
Pavel Vrublevsky
$$\$$ help recruit new affiliates
Methods of infection - Exploit kits
Affiliate marketing, Russian style
Email Protection
Whitelisting/Blacklisting and AV
HIPS
Ransomware
Out with the old

Interest over time

Ransomware

FakeAV

Average

AIDS trojan

Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don’t use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A6978294-2695577-

The price of 365 user applications is US$189. The price of a lease for the lifetime of your hard disk is US$378. You must enclose a bankers draft, cashier’s check or international money order payable to PC CYBORG CORPORATION for the full amount of $189 or $378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue
AIDS trojan
Modern ransomware

ATTENTION!

Your PC is blocked due to at least one of the reasons specified below.

You have been violating Copyright and Related Rights Law (Title 17, United States Code) by distributing copyrighted content. Pursuant to article 305 of the Criminal Code of the United States of America, article 305 of the Criminal Code provides for a fine of up to $250,000 in addition to a maximum of 3 years in prison.

Illegal access has been obtained from your PC without your knowledge or consent, your PC may be infected by malware, you are visiting a website on your behalf (such as your Personal Computer); article 305 of the Criminal Code provides for a fine of up to $250,000 and a maximum of 3 years in prison.

Pursuant to the amendment to the Criminal Code of the United States of America of March 29, 2011, this law enforcement if it is not repeated - first time you may be considered as conditional in cases you pay the fine to the State.

Illegal access has been obtained from your PC without your knowledge or consent, your PC may be infected by malware, you are visiting a website on your behalf (such as your Personal Computer); article 305 of the Criminal Code provides for a fine of up to $250,000 in addition to a maximum of 3 years in prison.

Pursuant to the amendment to the Criminal Code of the United States of America of March 29, 2011, this law enforcement if it is not repeated - first time you may be considered as conditional in cases you pay the fine to the State.

Illegal access has been obtained from your PC without your knowledge or consent, your PC may be infected by malware, you are visiting a website on your behalf (such as your Personal Computer); article 305 of the Criminal Code provides for a fine of up to $250,000 in addition to a maximum of 3 years in prison.

To unblock the computer, you must pay the fine through MoneyPak of $188.

How do I unblock computer using the MoneyPak?
1. Find a retail location near you.
2. Look for a MoneyPak in the prepaid section. Take it to the cashier and load it with cash. A service fee of 2.99 will apply.
3. To pay fine, you should enter the digits MoneyPak resulting code in the payment form and press the button.

Where you can buy MoneyPak?

FBI.gov is an official site of the U.S. Federal Government, U.S. Department of Justice.
Modern ransomware
Cryptolocker
GameOver botnet
Methods of infection – Zeus/Zbot
Methods of infection - SPAM

Notification,

E-TICKET NUMBER / EH036256364
SEAT / 71F/ZONE 3
DATE / TIME 10 AUGUST, 2012, 12:35 PM
ARRIVING / Tucson
FORM OF PAYMENT / CC
TOTAL PRICE / 257.50 USD
REF / EF 2982 ST / OK
BAG / 4PC

Your bought ticket is attached.
You can print your ticket.

Thank you for your attention.
Delta Air Lines.
Real life consequences

Romanian Man Commits Suicide After Police Ransomware Tells Him He Must Pay Fine

Timpul rămas: 47:56:17

Codul PIN
Suma
1 2 3 4 5 6 7 8 9 0

Achită PaySafeCard
Achită Ukash

Roşul acceptă PaySafeCard de la numeroase supermarketuri, benzinării, tabăraşturi şi clişături. PaySafeCard-ul poate utiliza în mai de 100 de țări din lume.
Defense
Web filtering
Mobile
Devices everywhere
Cloudy with a chance of breaches
Android malware
ATTENTION!
Your phone has been blocked up for safety reasons listed below.
All the actions performed on this phone are fixed.
All your files are encrypted.
CONDUCTED AUDIO AND VIDEO.
Andr/Slocker-A AKA Simplelocker

```
public static final List<String> EXTENSIONS_TO_ENCRYPT =
    Arrays.asList(new String[] {
```
Oleg Pliss

Screenshot sent in by a reader
Defense
Mobile AV

Scanner
- Last scan less than one hour ago.

Privacy Advisor
- Privacy Information for 38 Apps available.

Loss & Theft
- Feature configured.

Security Advisor
- 3 insecure system settings

Spam Protection
- Calls and messages: ON
Data everywhere? Encrypt it!
Advanced Persistent Threat
**Another Popular Term?**

<table>
<thead>
<tr>
<th>Specific individuals</th>
<th>Espionage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specific well-defined goals</td>
<td>Watering hole</td>
</tr>
<tr>
<td>Nation-state sponsored</td>
<td>Dragnet by vertical</td>
</tr>
</tbody>
</table>
Research
Exploit
Gain Persistence

where脸色 db 0 ; DATA XREF: sub_4013E+727F
76 63+aNetSvc_0 db 'NetSvc',0 ; DATA XREF: sub_4013E+9710
 ; sub_40162D+610 ...
60 6C+aInstall db 'install',0 ; DATA XREF: _main+3D10
76 65+aRemove db 'remove',0 ; DATA XREF: _main+5A10
70 00 aDebug db 'debug',0 ; DATA XREF: _main+7710
 ; char format[]
72 74+format db 0Ah ; DATA XREF: main:loc 40128410
69 63+ db 'StartServiceCtrlDispatcher being called.',0Ah,0
 ; char ThisMayTakeSeveralSeconds_PleaseWait[]
20 6D+aThisMayTakeSeveralSeconds_PleaseWait db 'This may take several seconds. Please wait.',0Ah,0
61 6B+ ; DATA XREF: _main+AF10
74 53+aStartServiceCtrlDispatcher db 'StartServiceCtrlDispatcher',0
63 65+ ; DATA XREF: _main+D710
 ; char ServiceName[]
76 63+ServiceName db 'NetSvc',0 ; DATA XREF: sub_4012E2+810
65 72+aSetServiceStatus db 'SetServiceStatus',0
53 74+ ; DATA XREF: sub_40138A+8910
 ; char SourceName[]
6F 72+SourceName db 'Network Location',0
63 61+ ; DATA XREF: sub_40143F:loc_4014B110
6C 65+aUnableToInstall%$%$ db 'Unable to install $s - $s',0Ah,0
Gain persistence

```
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
```
Gain persistence

```assembly
push    offset aSoftwareMicrosoftWindowsCurrentVersionP ; "Software\Microsoft\Windows\CurrentVersion"...
push    80000001h ; hkey
call   ds:RegCreateKeyEXA
push    offset Data  ";.exe;.bat;.reg;.vbs;"
call   ds:strlenA
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
```
Explore

hasdump

procmon

nc
tcpdump

memdump

psexec

nessuspskull

nmap
Explore

```
5C 20 6D 65+ad1Memdump_dmpNu2Nu1 db 'del memdump\*.dmp >NUL 2>NUL',0
75 6D 70 5C+
      ; DATA \REF: \_main:\loc_4011F710
74 byte _40F3E6
56 byte _40F3E6 db 0
      ; DATA \REF: dump\_memory:\loc_4012CA10
73 char aPid\_s\_dmp[]
55 2D 25 73+aPid\_s\_dmp db 'pid-%s.dmp',0 ; DATA \REF: dump\_memory+BF10
72 6D 70 69 6E+_asc\_40F3F2 db 'Dumping private memory for pid %s to %s.dmp...',0Ah,0
54 70 69 76+
      ; DATA \REF: dump\_memory+BF10
52 char aDone[]
6E 65 21 0A+aDone! db 'Done!',0Ah,0 ; DATA \REF: dump\_memory+12410
70 6D 70 69 76+
      ; DATA \REF: dump\_memory+12410
50 char aDone[0]
5E 65 21 0A+aDone!_0 db 'Done!',0Ah,0 ; DATA \REF: dump\_memory+14310
72 6F 63 65+aProcess\_Memory\_Dumper db 9,'\Process Memory Dumper',0Ah,0
61 64 65 20+aMadeBy01ab0 loophorn\(proud\_Member\_Of\_KdTeam\) db 9,'Made By:
65 73 65 20+aUse\_as\_Memdump\_exe\_Options\_Pid db 9,9,
55 'Use as: memdump.exe \-options> [PID]',0Ah,0
4F 70 70 69+aeOptions db 9,9,'Options:',0Ah,0
39 2D 3F 20+aShowThisHelp db 9,9,9,'-? = Show this help',0Ah,0
39 2D 6C 20+aList\_all\_Running\_Processes db 9,9,9,'-1 = List all running processes',0Ah,0
39 2D 73 20+aShow\_In\_Running\_Processes\_Like\_Path db 9,9,9,'-s = Show info on Process like Path',0Ah,0
39 2D 66 20+aDump\_Private\_Process\_Memory\_by\_PId db 9,9,9,'-f = Dump private process memory by PID',0Ah,0
39 2D 66 20+aFull\_Private\_Dump\_of\_All\_Running\_Processes db 9,9,9,'-f = Full private dump of all running processes',0Ah,0
39 2D 73 20+char \_format[]
39 2B 50 49+Format db '\%s',9,'(PID: \%u)',9,'\Hex: \%xh',0Ah,0
39 2D 75 29+
      ; DATA \REF: open\_process+6810
74 65 72 20+aEnter\_Process\_Id db 'Enter Process Id:',0
39 \x4d_0 db '\x4d',0
39 75 6C 65+aModule\_Snapshot\_Failed db 'Module Snapshot Failed',0Ah,0
39 74 6C 65+aModule\_Snapshots\_Succeeded db 'Module Snapshot succeeded',0Ah,0
74 68 65 72+agathering\_Module\_Information\_Failed db 'Gathering Module information failed',0Ah,0
39 75 6C 65+aModule\_Snapshot\_Failed db 'Module Snapshot Failed',0Ah,0
53
```
Act on objective
Cleanup

delete from xxxxLogs where xxxxLogID>2400000 and xxxxPAN in
('xxxxxxxxxxxxxxxx4809', 'xxxxxxxxxxxxxxxx3926', 'xxxxxxxxxxxxxxx1041', 'xxxxxxxxxxxxxxxx5815', 'xxxxxxxxxxxxxxxx4912', 'xxxxxxxxxxxxxxx9488', 'xxxxxxxxxxxxxxxx2840', 'xxxxxxxxxxxxxxxx3890')
APT vs Opportunistic threat

- Well funded
- Targeted
- Specialized
- Diverse goals
- Maintained

- Well funded
- Broad
- Generalized
- Financially motivated
- Abandoned
Global specialization

Global Reach

Law Enforcement Response To Date:

Total FBI cases: 390
Attempted loss: $220 million
Actual loss: $70 million

United States: 92 charged and 39 arrested
United Kingdom: 20 arrested and eight search warrants
Ukraine: Five detained and eight search warrants

Image courtesy of krebsonsecurity.com
What about the NSA?

A CRYPTO NERD’S IMAGINATION:

HIS LAPTOP’S ENCRYPTED. LET’S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.

NO GOOD! IT’S 4096-BIT RSA!

BLAST! OUR EVIL PLAN IS FOILED!

WHAT WOULD ACTUALLY HAPPEN:

HIS LAPTOP’S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.

GOT IT.
Point of Sale
MY IDENTITY'S BEEN STOLEN, SO NOW I CAN'T USE MY CREDIT CARD...
In the news
The greedy '80s
'90s introduces another go at the idea
The third generation, security and stupidity
I suppose I didn't have to use my card
Many cards, similar form
What's on a card?

Source: http://www.q-card.com/support/magnetic-stripe-card-standards.asp
What's on a stripe?

Track 1:

%4349120384822282^SHIER/JOHN
^170320190100005490000000?

Track 2:

:4349120384822282=170320190100549?
ATM Skimmer
Pocket Skimmer
Bad, not terrible
Where to begin?
Begin by scraping the RAM

C7 05 C0 95 40 00+ mov pe.dwSize, 128h
6A 00 push 0 ; th32ProcessID
6A 02 push 2 ; dwFlags
88 76 23 00 00 call CreateToolhelp32Snapshot
89 45 D4 mov eax, [ebp+hSnapshot], eax

88 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+nNumberOfBytesRead]
56 push edx ; lpNumberOfBytesRead
88 45 C0 mov eax, [ebp+nSize]
50 push eax ; nSize
88 4D DC mov ecx, [ebp+lpBuffer]
51 push ecx ; lpBuffer
88 55 FC mov edx, [ebp+lpBaseAddress]
52 push edx ; lpBaseAddress
88 4D D8 mov eax, [ebp+hObject]
50 push eax ; hProcess
FF 15 F8 10 40 00 call ds:ReadProcessMemory

88 4D D4 mov ecx, [ebp+hSnapshot]; hSnapshot
51 push ecx
E8 AF 21 00 00 call Process32Next
85 C0 test eax, eax
DF 85 4C FE FF jnz start_check
Don't waste time
Trip up & hide from researchers

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

    aDlls(0) = "SbieD11.dll" 'sandboxie
    aDlls(1) = "dbghelp.dll"
    aDlls(2) = "LOG_API12.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
```
Grab the cards
Trust, but verify

```vbnet
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
    End If
  Next i
```

SOPHOS
Command & Control (C2)

```plaintext
; char a_var[8]
26 76 61 6C 3D 00 a&val_0 db '"&val=',0 ; DATA XREF: commands_received+7810
  ; commands_received+2310
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+bDetectshutdownclass_2 db 'DetectShutdownClass',0
; char aDownload[]
64 6F 77 6E 6C 6F+aDownload db 'download-',0 ; DATA XREF: commands_received:loc_405E7D10
61 64 2D 00
00 00
align 4
75 70 64 61 74 65+aUpdate db '"update=',0 ; DATA XREF: commands_received+3310
2D 00
; char aCheckin[]
63 68 65 63 68 6E+aCheckin db 'checkin:',0
6E 3A 00
00 00 00
; char aScanin[]
73 63 61 6E 69 6E+aScanin db '"scanin=',0 ; DATA XREF: commands_received:loc_405D5010
3A 00
; char aUninstall[]
75 6E 69 6E 73 74+aUninstall db '"uninstall=',0 ; DATA XREF: commands_received:loc_405E5410
6C 00
00 00
align 10h
```

SOPHOS
PCI says to encrypt before exfiltration, right?
Cashing out
What can you do?
PCI DSS is driving innovation

- Encryption in transit
- Encryption at rest
- Secure remote access
Firewall
Old and busted
New hotness
Active protection

SophosLabs
Active Protection

Correlated Intelligence
Reputation Data
Content Classification

Network
- Web
- Email
- Next Gen FW
- Web App FW
- Wifi

Servers
- Email
- Web
- File

Devices
- Smartphone/Tablet
- Workstation/Laptop
- Data
SophosLabs

SOPHOSLABS

SAMPLES
TELEMETRY
HONEY POTS

HUMAN DECISION MAKING

AUTOMATED LEARNING & AUTOMATION

BIG DATA

ANALYTICS
Dynamic & Static

AT HOME
ON THE MOVE
REMOTE OFFICE
HEADQUARTERS
Complete Security
Latest news: http://nakedsecurity.sophos.com
Podcasts: http://podcasts.sophos.com
Videos: http://youtube.com/SophosLabs
See us again: http://nakedsecurity.sophos.com/events

Contact me: ken.swain@sophos.com
@kenotic
Email
Twitter

Newsletter