HUNTING WEBSHELLS

TRACKING TWOFACE
THE HUNTERS

Josh M. Bryant
Director of Technical Account Management
Tanium

Master Sergeant
183 Air Communications Flight
Illinois Air National Guard

Robert Falcone
Threat Researcher
Palo Alto Networks

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

@r0bf4lc
“Consistent use of web shells by Advanced Persistent Threat (APT) and criminal groups has led to significant cyber incidents.”
TWOFACE

64-byte Key → Key Salt → Embedded Webshell → Redirected To Decrypted Webshell
Embedded webshell

```csharp
byte[] brjCSBCsoKt = System.Convert.FromBase64String("O+Hp1vX181ykFZOp62sq rwxa6qfk2F8nWVuQkPUJotEG/pTGaUD124npIWvuuB8rmhT5iNRtWq 70KzEX4MwFePIU8mo6inH/0xxKRQuCr9ZcrSBZao1+/Nj4S5KCcYby VD3jTS1/QvHQLx6OCPGAcL ..snip..
```

Key salt

```csharp
byte[] CPccVznRld = System.Convert.FromBase64String("6nxL+zKa3nBOxtI8EWOQ KA1Sxngz861Sio1/Ei3dPv2Zyd4VtPSskJIG8XPX7xn8niGep9lWak yUqppyNZg/dXdzPDxkbqNTLwzgOY69jkJVdv71b15+CsV0OwSnSU1B HfYbirkwa5rQ0/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
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];
for x in range(0, 255):
    if chr(((ord(ciphertext_webshell[r]) -
             ord(key_salt[r%len(key_salt)])) &
             0xff) - x) & 0xff) in printable:
        ...
        curSet = curSet.intersection(set(possible_keys[c+(r*64)]))
        ...

Ciphertext Output

\x05/\x86/\xa5/\xda/\x89/\x8a/\xc8/\x85/\xec/\x84/\xa6/\xd9/\x17/\xa4/\xf3/\xb5/\xc5/\x82/\xa5/\x9f/\xe6/\xc4/\xd3/\x86/\x8c/\xd2/\x83/\xb1/\x81/\x96/\x0b/\xa8/\x0f/\x0b/\x7f/\x0a/\x03/\x0e/\x0f/\x0c/\x0d/\x02/\x01/\x00/\x01/\x02/\x03/\x04/\x05/\x06/\x07/\x08/\x09/\x0a/\x0b/\x0c/\x0d/\x0e/\x0f/\x10/\x11/\x12/\x13/\x14/\x15/\x16/\x17/\x18/\x19/\x1a/\x1b/\x1c/\x1d/\x1e/\x1f/\x20/\x21/\x22/\x23/\x24/\x25/\x26/\x27/\x28/\x29/\x2a/\x2b/\x2c/\x2d/\x2e/\x2f/\x30/\x31/\x32/\x33/\x34/\x35/\x36/\x37/\x38/\x39/\x3a/\x3b/\x3c/\x3d/\x3e/\x3f/\x40/\x41/\x42/\x43/\x44/\x45/\x46/\x47/\x48/\x49/\x4a/\x4b/\x4c/\x4d/\x4e/\x4f/\x50/\x51/\x52/\x53/\x54/\x55/\x56/\x57/\x58/\x59/\x5a/\x5b/\x5c/\x5d/\x5e/\x5f/\x60/\x61/\x62/\x63/\x64/\x65/\x66/\x67/\x68/\x69/\x6a/\x6b/\x6c/\x6d/\x6e/\x6f/\x70/\x71/\x72/\x73/\x74/\x75/\x76/\x77/\x78/\x79/\x7a/\x7b/\x7c/\x7d/\x7e/\x7f/\x80/\x81/\x82/\x83/\x84/\x85/\x86/\x87/\x88/\x89/\x8a/\x8b/\x8c/\x8d/\x8e/\x8f/\x90/\x91/\x92/\x93/\x94/\x95/\x96/\x97/\x98/\x99/\x9a/\x9b/\x9c/\x9d/\x9e/\x9f/\xa0/\xa1/\xa2/\xa3/\xa4/\xa5/\xa6/\xa7/\xa8/\xa9/\xaa/\xab/\xac/\xad/\xae/\xaf/\xb0/\xb1/\xb2/\xb3/\xb4/\xb5/\xb6/\xb7/\xb8/\xb9/\xba/\xbb/\xbc/\xbd/\xbe/\xbe/\xbf/\xc0/\xc1/\xc2/\xc3/\xc4/\xc5/\xc6/\xc7/\xc8/\xc9/\xca/\xcb/\xcc/\xcd/\xce/\xcf/\xd0/\xd1/\xd2/\xd3/\xd4/\xd5/\xd6/\xd7/\xd8/\xd9/\xda/\xdb/\xdc/\xdd/\xde/\xdf/\xe0/\xe1/\xe2/\xe3/\xe4/\xe5/\xe6/\xe7/\xe8/\xe9/\xea/\xeb/\xec/\xed/\xee/\xef/\xf0/\xf1/\xf2/\xf3/\xf4/\xf5/\xf6/\xf7/\xf8/\xf9/\xfa/\xfb/\xfc/\xfd/\xfe/\xff

Key

\x05/\x86/\xa5/\xda/\x89/\x8a/\xc8/\x85/\xec/\x84/\xa6/\xd9/\x17/\xa4/\xf3/\xb5/\xc5/\x82/\xa5/\x9f/\xe6/\xc4/\xd3/\x86/\x8c/\xd2/\x80/\xfa/\x96/\x85/\xf6/\x03/\xe7/\xcd/\xf3/\x0b/\xa7/\xcd/\x0f/\xd1/\xbd

Cleartext Output

<%@ Page Language="C#" ValidateRequest="false" EnableViewState="false"
%>

r
r
r

<html>
</head>
<%
    NameValueCollection t=HttpContext.Current.Request.Form;
r
    npwd=t["pwd"]; ..snip..
LET’S GO HUNTING!
"Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win."

#SANSHackFest

John Lambert
GM, Microsoft Threat Intelligence Center

John Rodriguez
@johnroMSFT

Graph theory and attack graphs in #eko12.
"Six degrees of domain admin"
Episode IV: An Attacker's Hope

- SQL Injection?
- Remote File Inclusion?
- Cross-Site Scripting?
- Local File Inclusion?
- Remote Code Execution?

---

- Phishing
- Password Theft
- Web Application Hijacking
- FTP File Transfer

---

-OWNED!

- Plant Webshell...

---

- I use Domain Admin

---

- All your base are belong to us!
Episode VI: Return of the Attacker

Oops I PWNED you again...
ACTOR ACTIVITIES
June 16, 2016

15 Distribution Lists

81 User Accounts
Downloads
Offline Address Book (OAB)
for offline processing
whoami

---

June 18, 2016

/owa/auth/error2.aspx
/owa/auth/error3.aspx
** 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
> 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$\Program
... Files\Microsoft\Exchange Server\V14\ClientAccess\exchweb\ews"
copy c:\windows\temp\Exchange.aspx "\\<server name 2>\d$\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"
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"
> 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\ **
> 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
May 3, 2017

```plaintext
> 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
```

/owa/auth/errorn.aspx
Where my logs at?

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

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Site</th>
<th>ServerRole</th>
<th>Edition</th>
<th>AdminDisplayVersion</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX2016</td>
<td>contoso.com/Conf...</td>
<td>Mailbox,...</td>
<td>Standard...</td>
<td>Version 15.1</td>
</tr>
</tbody>
</table>

**Step 2** – Find where the IIS Logs are stored.

```powershell
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
### Searching IIS Logs with Log Parser Studio

#### Note UserAgent

<table>
<thead>
<tr>
<th>Time</th>
<th>ServerIP</th>
<th>User</th>
<th>Method</th>
<th>URI</th>
<th>Query</th>
<th>UserAgent</th>
<th>HTTPStatus</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/2000 12:50</td>
<td>10.10.10.10</td>
<td></td>
<td>POST</td>
<td>/owa/auth/owaauth.dll</td>
<td>&amp;Correlation...</td>
<td>Mozilla/5.0+(Android;+Mobile;+rv:24.0)+Gecko/24.0+Firefox/24.0</td>
<td>302</td>
</tr>
<tr>
<td>1/1/2000 1:01</td>
<td>10.10.10.10</td>
<td></td>
<td>POST</td>
<td>/owa/auth/owaauth.dll</td>
<td>&amp;Correlation...</td>
<td>Mozilla/5.0+(Android;+Mobile;+rv:24.0)+Gecko/24.0+Firefox/24.0</td>
<td>302</td>
</tr>
<tr>
<td>1/1/2000 2:16</td>
<td>10.10.10.10</td>
<td></td>
<td>POST</td>
<td>/owa/auth/owaauth.dll</td>
<td>&amp;Correlation...</td>
<td>Mozilla/5.0+(Android;+Mobile;+rv:24.0)+Gecko/24.0+Firefox/24.0</td>
<td>302</td>
</tr>
<tr>
<td>1/1/2000 2:21</td>
<td>10.10.10.10</td>
<td></td>
<td>POST</td>
<td>/owa/auth/owaauth.dll</td>
<td>&amp;Correlation...</td>
<td>Mozilla/5.0+(Android;+Mobile;+rv:24.0)+Gecko/24.0+Firefox/24.0</td>
<td>302</td>
</tr>
<tr>
<td>1/1/2000 9:16:52</td>
<td>10.10.10.10</td>
<td></td>
<td>POST</td>
<td>/owa/auth/owaauth.dll</td>
<td>&amp;Correlation...</td>
<td>Mozilla/5.0+(Android;+Mobile;+rv:24.0)+Gecko/24.0+Firefox/24.0</td>
<td>302</td>
</tr>
<tr>
<td>1/1/2000 9:24:49</td>
<td>10.10.10.10</td>
<td></td>
<td>POST</td>
<td>/owa/auth/owaauth.dll</td>
<td>&amp;Correlation...</td>
<td>Mozilla/5.0+(Android;+Mobile;+rv:24.0)+Gecko/24.0+Firefox/24.0</td>
<td>302</td>
</tr>
</tbody>
</table>

```sql
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,
s-c-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

<table>
<thead>
<tr>
<th>Time</th>
<th>ServerIP</th>
<th>User</th>
<th>Method</th>
<th>URI</th>
<th>Query</th>
<th>UserAgent</th>
<th>HTTPStatus</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/4/2015 12:00</td>
<td>10.10.10.10</td>
<td>GET /owa/</td>
<td>GET</td>
<td>owa/</td>
<td>ae=Folder&amp;l=IPF... Mozilla/5.0+(Android;Mobile;+... 302</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2/4/2015 12:00</td>
<td>10.10.10.10</td>
<td>GET /owa/auth/logon.aspx</td>
<td>GET</td>
<td>owa/auth/logon.aspx</td>
<td>url=https%3a%2f%2f... Mozilla/5.0+(Android;Mobile;+... 200</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2/4/2015 12:00</td>
<td>10.10.10.10</td>
<td>GET /owa/</td>
<td>GET</td>
<td>owa/</td>
<td>&amp;CorrelationID=&lt;... Mozilla/5.0+(Android;Mobile;+... 302</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2/4/2015 12:00</td>
<td>10.10.10.10</td>
<td>GET /owa/auth/logon.aspx</td>
<td>GET</td>
<td>owa/auth/logon.aspx</td>
<td>url=https%3a%2f%2f... Mozilla/5.0+(Android;Mobile;+... 200</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2/4/2015 12:00</td>
<td>10.10.10.10</td>
<td>POST /owa/auth/owauth.dll</td>
<td>POST</td>
<td>/owa/auth/owauth.dll</td>
<td>&amp;CorrelationID=&lt;... Mozilla/5.0+(Android;Mobile;+... 302</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2/4/2015 12:00</td>
<td>10.10.10.10</td>
<td>GET /owa/</td>
<td>GET</td>
<td>owa/</td>
<td>ae=Folder&amp;l=IPF... Mozilla/5.0+(Android;Mobile;+... 200</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2/4/2015 12:00</td>
<td>10.10.10.10</td>
<td>GET /owa/</td>
<td>GET</td>
<td>owa/</td>
<td>wa=wsignin1.0&amp;l=... Mozilla/5.0+(Android;Mobile;+... 200</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Identify Compromised Accounts

```sql
/* UserAgent Search */
SELECT
date,
time,
s-username as ServerIP,
cs-method as Method,
sc-uri-stem as URI,
sc-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
```
<table>
<thead>
<tr>
<th>ClientId</th>
<th>Server-side Cookie Reference</th>
</tr>
</thead>
</table>

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
Unusual POST operations? Looks like a webshell!

Save us #DFIR, you’re our only hope!
QUESTIONS?

Josh M. Bryant  
Director of Technical Account Management  
Tanium

Master Sergeant  
183 Air Communications Flight  
Illinois Air National Guard

Robert Falcone  
Threat Researcher  
Palo Alto Networks