Pi$$$ing off an APT

Edward Williams
Name: Ed Williams
Position: SpiderLabs Director, EMEA
Previously: Principal Security Consultant
Other: Crest Fellow
Interesting facts: Welsh
Father of twins
Have taken part in a bollywood film
My Film Career


**Reception** [edit]

It was screened at the 2005 Global Indian Film Awards held in Dubai. Rediff.com's film critic called the picture "an insult to cinema".[1]

**References** [edit]

The enemy

Red Teams Blog @redtea... · 3h
Act, don’t react.

Sun Tzu @SunTzuCyber
"The enemy does not check your risk register prior to attacking." - Sun Tzu, The Art of Cyber War
Red Teaming / Attack Simulation

Red team != Pen Test

Red Team different mindset
Don’t do mass scanning…the bad guys don’t
Slow and Steady to achieve goal
When to red team?
Cyber Kill Chain

1. Reconnaissance
   - Harvesting email addresses, conference information, etc.

2. Weaponization
   - Coupling exploit with backdoor into deliverable payload

3. Delivery
   - Delivering weaponized bundle to the victim via email, web, USB, etc.

4. Exploitation
   - Exploiting a vulnerability to execute code on victim's system

5. Installation
   - Installing malware on the asset

6. Command & Control (C2)
   - Command channel for remote manipulation of victim

7. Actions On Objectives
   - With 'Hands on Keyboard' access, intruders accomplish their original goals

Observation 1

“A big, expensive shiny box isn't going to make you more secure.”

You need more...
You need the basics..
...and you need layers!
Observation 2

“it’s not 0-days that cause APTs to succeed, it’s poor Operational Security (OpSec) and technical debt.”

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Status</th>
<th>Startup Type</th>
<th>Log On As</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Server (SPIDE</td>
<td>Provides st...</td>
<td>Started</td>
<td>Automatic</td>
<td>THOR\Administrator</td>
</tr>
</tbody>
</table>
How do we ‘actually’ pi$$ off an APT?

http://detect-respond.blogspot.co.uk/2013/03/the-pyramid-of-pain.html
Credential Dumping

Credential dumping is the process of obtaining account login and password information, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform Lateral Movement and access restricted information.

Several of the tools mentioned in this technique may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

SAM (Security Accounts Manager)

The SAM is a database file that contains local accounts for the host, typically those found with the ‘net user’ command. To enumerate the SAM database, system level access is required. A number of tools can be used to retrieve the SAM file through in-memory techniques:

- `pwdumpx.exe`
- `gsecdump`
- `Mimikatz`
- `secretsdump.py`

Alternatively, the SAM can be extracted from the Registry with Reg:

- `reg save HKEY\local\sam`
- `reg save HKEY\system\system`

Creddump7 can then be used to process the SAM database locally to retrieve hashes.[1]

Notes: RId 500 account is the local, in-built administrator. RId 501 is the guest account. User accounts start with a RID of 1,000+.

Cached Credentials
Reduce External Visibility

KEEP CALM AND LOCK IT DOWN!
To begin at the beginning… OSINT Everything
To begin at the beginning... OSINT Everything

E-Mail harvesting / format

Social Media all the things

trustwave.com

Find email addresses

Most common pattern: {f}{last}@trustwave.com

105 email addresses

Subdomain Discovery... uat/test... vpn... lync etc etc
To begin at the beginning... OSINT Everything

Shodan

Iranian & Russian Networks Attacked Using Cisco’s CVE-2018-0171 Vulnerability

By Lawrence Abrams

April 7, 2018

Last night, a hacker group going under the name "JHT" attacked foreign network infrastructure, including Russian and Iranian networks, using the Cisco CVE-2018-0171 Smart Install vulnerability. Using this vulnerability the hackers were able to reset the routers back to their default configuration and display a message to the victims.

After vulnerable Cisco routers were attacked using the CVE-2018-0171, the router’s configuration file called startup-config was overwritten and the router rebooted. Not only did this cause outages for the affected networks, but admins also discovered that the router’s startup-config file was changed to a message stating “Don’t mess with our elections.... -JHT usafreedom_jht@tutanota.com” as shown below.
To begin at the beginning... OSINT Everything

Shodan

TOTAL RESULTS
2,412,450

TOP COUNTRIES
United Arab Emirates 628,602
United States 409,399
Russian Federation 192,208
Taiwan 134,124
Japan 122,635

TOTAL RESULTS
3,132,116

TOP COUNTRIES
United States 887,521
China 530,384
Hong Kong 307,804
Germany 118,226
Brasil 112,105

TOP ORGANIZATIONS
Google Cloud 163,604
Amazon.com 157,844
Tencent cloud computing 148,827
Microsoft Azure 119,896
Incapsula 97,817
Determine Cloud Services

DNS (MX & TXT records)

*.mail.protection.outlook.com

ms=ms* O365 domain tenant in TXT record

google-site-verification=*

Gsuite TXT record
To begin at the beginning... OSINT Everything

Anti-Spoofing

Sender Policy Framework (SPF)

DomainKeys Identified Mail (DKIM)

Domain-based Message Authentication, Reporting and Conformance (DMARC)

| SPF: | PASS with IP 209.85.220.41 Learn more |
| DKIM: | 'PASS' with domain gmail.com Learn more |
| DMARC: | 'PASS' Learn more |
To begin at the beginning... OSINT Everything
Getting in...

Phishing

Macros – still very popular and successful!

Weekly Threat Report 21st September 2018

This report is drawn from recent open source reporting.

Microsoft Office Macros, most popular method of malware delivery

Cyber criminals continue to utilise weaponised macros in Microsoft Office documents to deliver malware. In a recent report from Cofense, it was noted that the exploitation of Microsoft Office macros comprised 45% of all deliveries. A separate report showed that a further 37% exploited the Microsoft Office Memory Corruption Vulnerability (CVE-2017-11882).
Getting in...

Phishing

**HTA via HTML** (*html files that contain an encrypted HTA file. the key is fetched and the HTA is decrypted dynamically within the browser and pushed directly to the user.)*

**OLE (Object Linking & Embedding)**

**DDE (Dynamic Data Exchange)**
Getting in...cont’d

Smishing (very popular)
Social Media Phishing (also, very popular)
Watering hole / Phishing
  Third Party Exploits (N-day - CVE-2018-4877 - Flash)
Browsers (user agent - CVE-2018-8174)
Login Portal Clone (e.g. O365)
Getting in…password spraying

https://www.us-cert.gov/ncas/alerts/TA18-086A?t=1&cn=ZmxleGlhbGFcmVjcw%3D%3D&refsrc=email&iid=53f6697a57384c138ec81a1c59db5f2a&uid=729139915951218688&nid=244+272699400
Stopping - Getting in…

Microsoft et al offers:

• Anti-Phishing
• Mailbox Intelligence (safe-links etc)
• Smart / IP Lockout
• Banned passwords – Checks passwords against a known list

The reality, these aren’t enabled in most cases and can’t stop 100% of threats!
These technologies aren’t perfect though…

Sending from a high reputation domain

```html
<!DOCTYPE html>
<html lang="en">
<head>
</head>
<body>

Normally, a malicious <a href="https://bit.do/ee9mr">link</a> is blocked.

</body>
</html>

<!DOCTYPE html>
<html>
<head>
    <base href="https://bit.do/"
</head>
<body>

But by splitting the URL, the <a href="ee9mr">link</a> gets through.

</body>
</html>
```

What really starts to pi$$ them off...


- 8 character min* (>64 max)
- Dictionary to disallow common passwords
- Allow all printing characters (inc. space)
- Throttling (100 attempts in 30-day period)
- No requirement for password expiration

*doesn’t differentiate between admin and non-admin user
Frustrating++

2FA
SMS Hell!

SMS two-factor authentication can be a hassle. In the Money Box article, "TSB customers hit by 'SIM swappers'" discusses how customers can avoid SIM swap fraud. The fraud involves identity theft, where criminals impersonate their victim in financial transactions. Available now, the article offers details and prevention tips.
Exchange Web Services (EWS)

The O365 portal may require ~2FA
EWS doesn’t always

The default URL for EWS is:
https://<mail.server>/ews/exchange.asmx
Proper 2FA

None of Google's 85,000 employees have had their work accounts taken over in a year — and it's because of a simple $20 product anyone can buy.
Remove technical debt

Sun Tzu @SunTzuCyber

"The enemy does not check your risk register prior to attacking." - Sun Tzu, The Art of Cyber War

This can be difficult in large, complex environments.
Assume breach

“Defenders think in lists and attackers think in graphs”  
John Lambert (MSTIC)

Take a domain controller for example. Bob admins the DC from a workstation. If that workstation is not protected as much as the domain controller, the DC can be compromised.
The EUD is the battleground
The EUD is the battleground

Once a foothold is gained, one of two things is likely to happen:

- Situational Awareness / Enumerate creds (Password Spray etc.)
- Enumerate local host & network
The EUD is the battleground…Windows version

Harden the EUD & reduce situational awareness:
LAPS
White listing / App locker
Host based firewall
Logging (PS v5) / SYSMON
I wrote a thing...post exploitation
Authenticated Users

SPN Hunting / kerberoasting

“any domain user that has an arbitrary service principal name set can have a TGS for that SPN requested by ”any” user in the domain, allowing for the offline cracking of the service account plaintext password!”

https://www.harmj0y.net/blog/powershell/kerberoasting-without-mimikatz/

https://www.youtube.com/watch?v=jJgPTBgD52U
Authenticated Users

SPN Hunting / kerberoasting

https://www.youtube.com/watch?v=jJgPTBgD52U
Living off the land
Living off the land

Red Teams are less likely to upload tools / malware; use in-built tools
Living off the land

Alternatively, the SAM can be extracted from the Registry with Reg:

- `reg save HKLM\sam sam`
- `reg save HKLM\system system`

Credump7 can then be used to process the SAM database locally to retrieve hashes.¹

Notes: Rid 500 account is the local, in-built administrator. Rid 501 is the guest account. User accounts start with a RID of 1,000+.
EVENT IDs FTW!

Red Teaming isn’t only about protection, to catch the red team, you’ll need to detect and respond.
EVENT IDs FTW (Targeted Monitoring)!

Cleanup and Cover Tracks

In multiple instances, the threat actors created new accounts on the staging targets to perform cleanup operations. The accounts created were used to clear the following Windows event logs: System, Security, Terminal Services, Remote Services, and Audit. The threat actors also removed applications they installed while they were in the network along with any logs produced. For example, the Fortinet client installed at one commercial facility was deleted along with the logs that were produced from its use. Finally, data generated by other accounts used on the systems accessed were deleted.

Threat actors cleaned up intended target networks through deleting created screenshots and specific registry keys. Through forensic analysis, DHS determined that the threat actors deleted the registry key associated with terminal server client that tracks connections made to remote systems. The threat actors also deleted all batch scripts, output text documents and any tools they brought into the environment such as "scr.exe".

Security logs being cleared (1102)
EVENT IDs FTW (Targeted Monitoring)!

Establishing Local Accounts

The threat actors used scripts to create local administrator accounts disguised as legitimate backup accounts. The initial script "symantec_help.jsp" contained a one-line reference to a malicious script designed to create the local administrator account and manipulate the firewall for remote access. The script was located in "C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\tomcat\webapps\ROOT\".

Local group changes (4732 & 4733)
lLocal account creation (4720 & 4726)
In at least two instances, the threat actors used batch scripts labeled “pss.bat” and “psc.bat” to run the PsExec tool. Additionally, the threat actors would rename the tool PsExec to “ps.exe”.

1. The batch script (“pss.bat” or “psc.bat”) is executed with domain administrator credentials.
2. The directory “out” is created in the user’s %AppData% folder.
3. PsExec is used to execute “scr.exe” across the network and to collect screenshots of systems in “ip.txt”.
4. The screenshot’s filename is labeled based on the computer name of the host and stored in the target’s C:\Windows\Temp directory with a “.jpg” extension.
5. The screenshot is then copied over to the newly created “out” directory of the system where the batch script was executed.
6. In one instance, DHS observed an “out.zip” file created.
EVENT IDs FTW (Targeted Monitoring)!

Password spraying against SMB on a Domain Controller results in event ID 4625 "logon failure" being logged on the DC.

What if we don’t use SMB?

EVENT IDs FTW (Targeted Monitoring)!

When using LDAP, no 4625 events are logged.
Kerberos logging needs to be enabled to log event ID 4771 (Failure code - 0x18, bad password)

Blue Teamers – high level

Understand your network
Understand how data flows around your network
Concentrate on TTPs & Behaviors
Blue Teamers – detailed

Raise your domain functional level

*Domain name:*
*ad.contoso.com*

*Current domain functional level:*
*Windows 2000 mixed*

*Select an available domain functional level:*
*Windows Server 2003*

⚠️ After you raise the domain functional level, it cannot be reversed. For more information on domain functional levels, click Help.
Blue Teamers – detailed

**Windows 2008R2:**
- Fine grained password polices
- Last Interactive Logon Information

**Windows 2012R2:**
- DC-side protections for Protected Users
- Authentication Policies
Blue Teamers – detailed

Privileged Access workstations (PAWs) – “provide a dedicated operating system for sensitive tasks that is protected from Internet attacks and threat vectors.”

Or

Stop doing domain admin / subscription admin / root on standard workstations
“Red Forest - Enhanced Security Administrative Environment”

How do we ‘actually’ pi$$ off an APT...again!?

http://detect-respond.blogspot.co.uk/2013/03/the-pyramid-of-pain.html
Conclusion

Get the basics done…even though they are really hard to do across everything

Layers, make sure one thing doesn’t blow everything up

Visibility and reaction are key
Questions?

https://uk.linkedin.com/in/edwilliamscymro

@dynllandeilo