Trustwave®
Smart security on demand

From Battlefield to Bunker

Matt Lorentzen

4th December 2018

Matt Lorentzen

Principal Security Consultant
Trustwave SpiderLabs

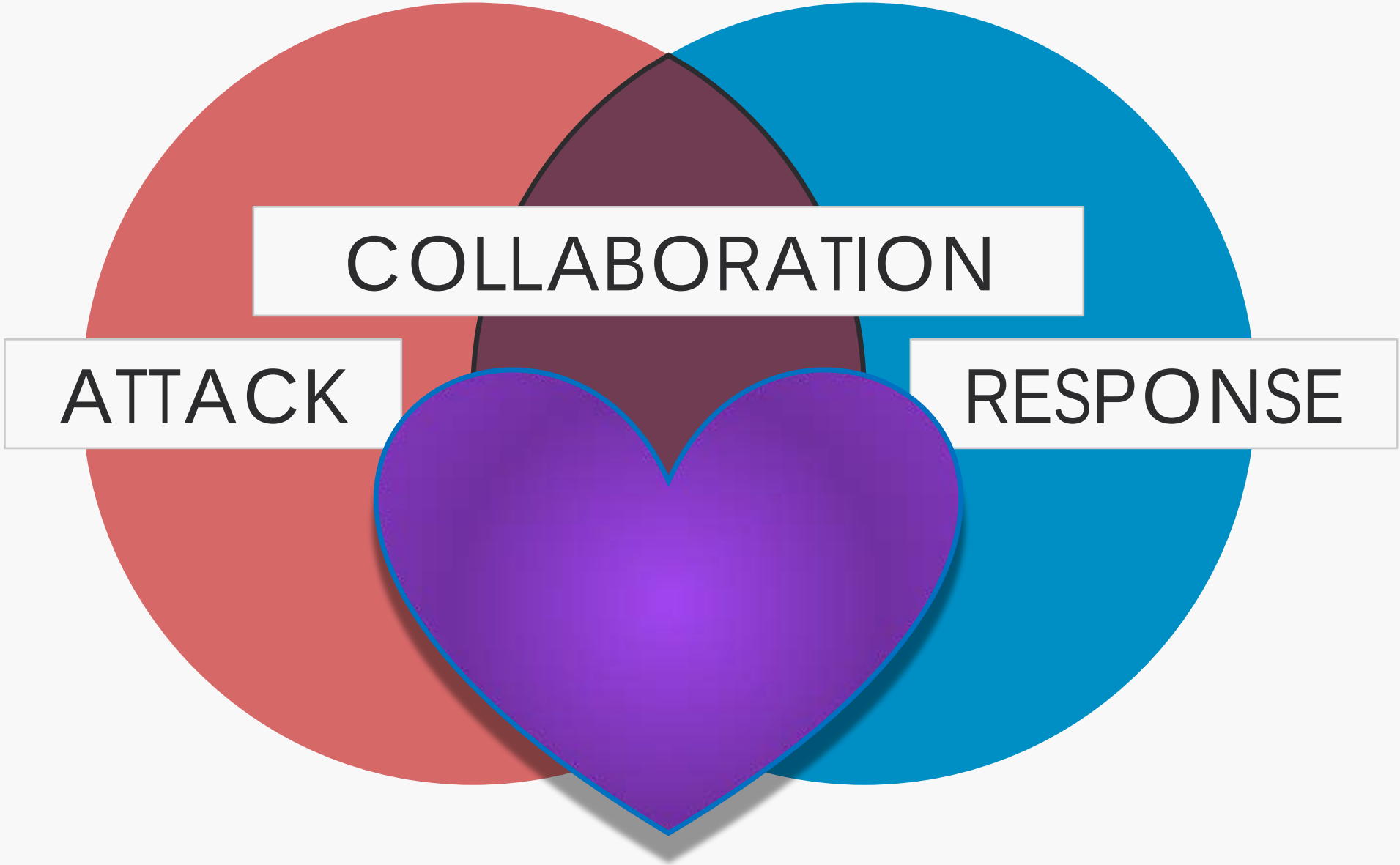
CCSAS, CCT

Focus on Red Teaming
Delivered testing for Government, Military, Commercial and Education establishments

Former CHECK Team Leader

Experience of business implementation after running a small consultancy for 7 years

Presented at CrestCon ASIA, 44Con London and various regional and national meetings


COLLABORATION
ATTACK
RESPONSE

Attacking Mindset

“A red team or the red team is an independent group that challenges an organization to improve its effectiveness by assuming an adversarial role or point of view.”

https://en.wikipedia.org/wiki/Red_team

"A red team or the red team is an independent group that challenges an organization to improve its effectiveness by assuming an adversarial role or point of view."

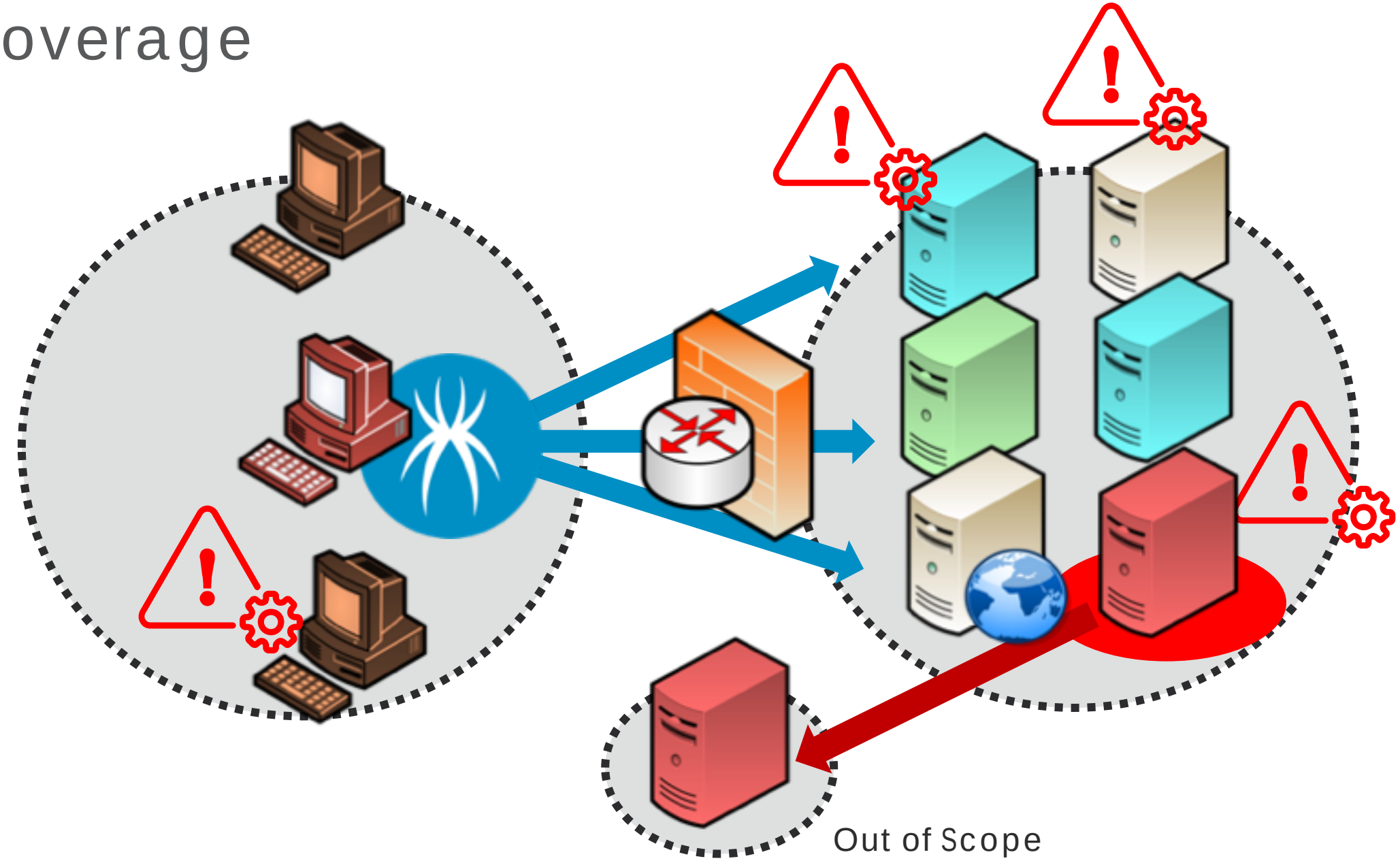
https://en.wikipedia.org/wiki/Red_team

Red Teaming versus Pentesting

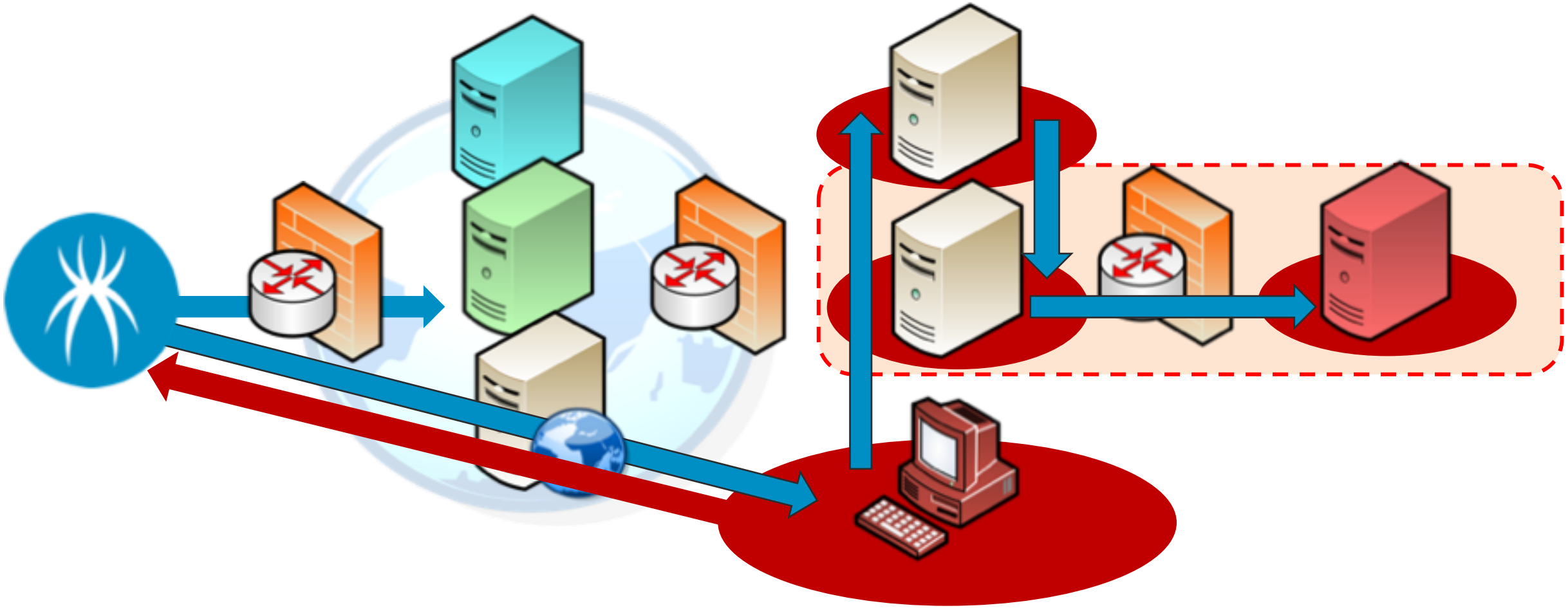
What are the differences in approach?

Isn't this just another buzzword?

Coverage

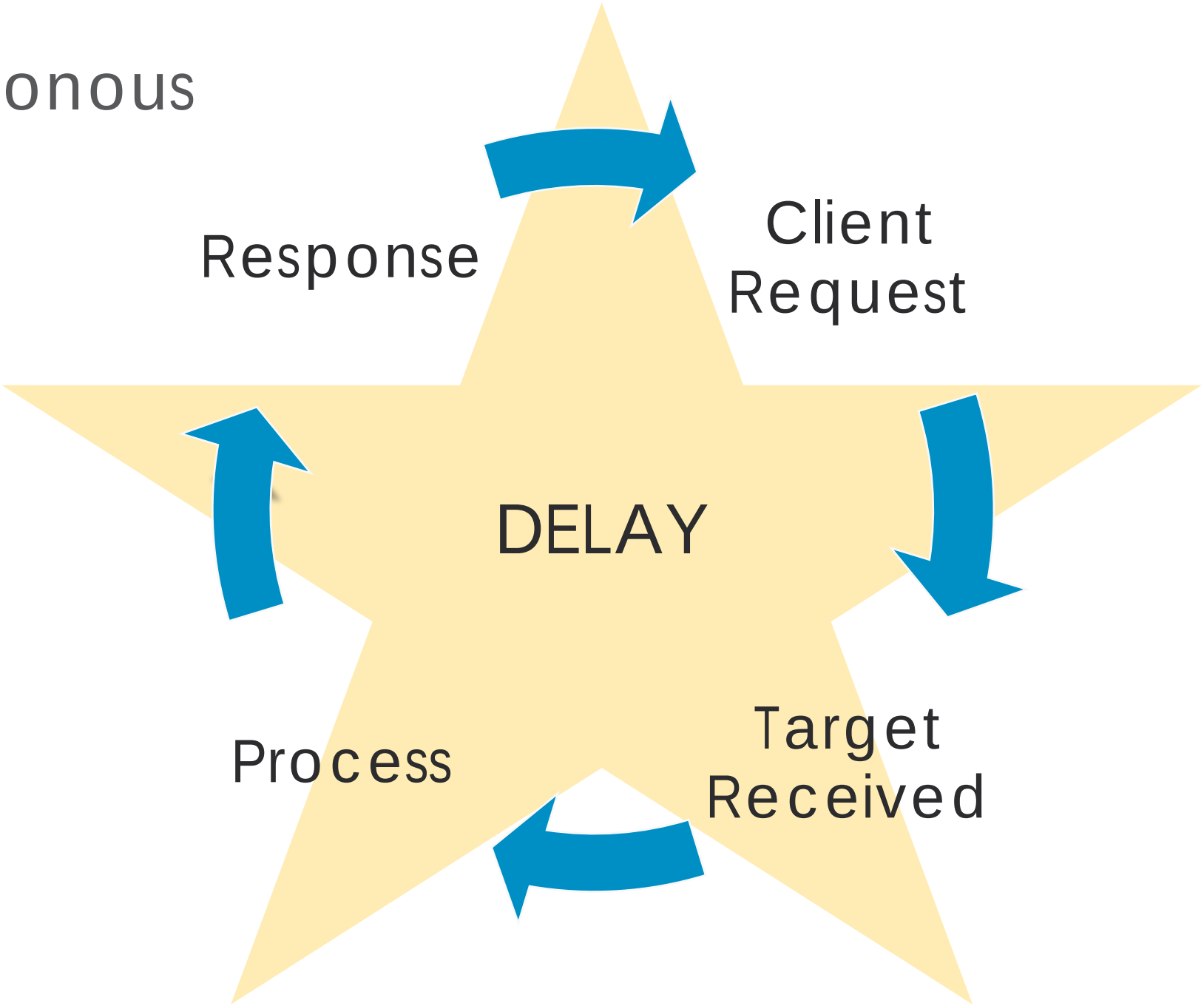


Goals




O.V.L
Made in Korea

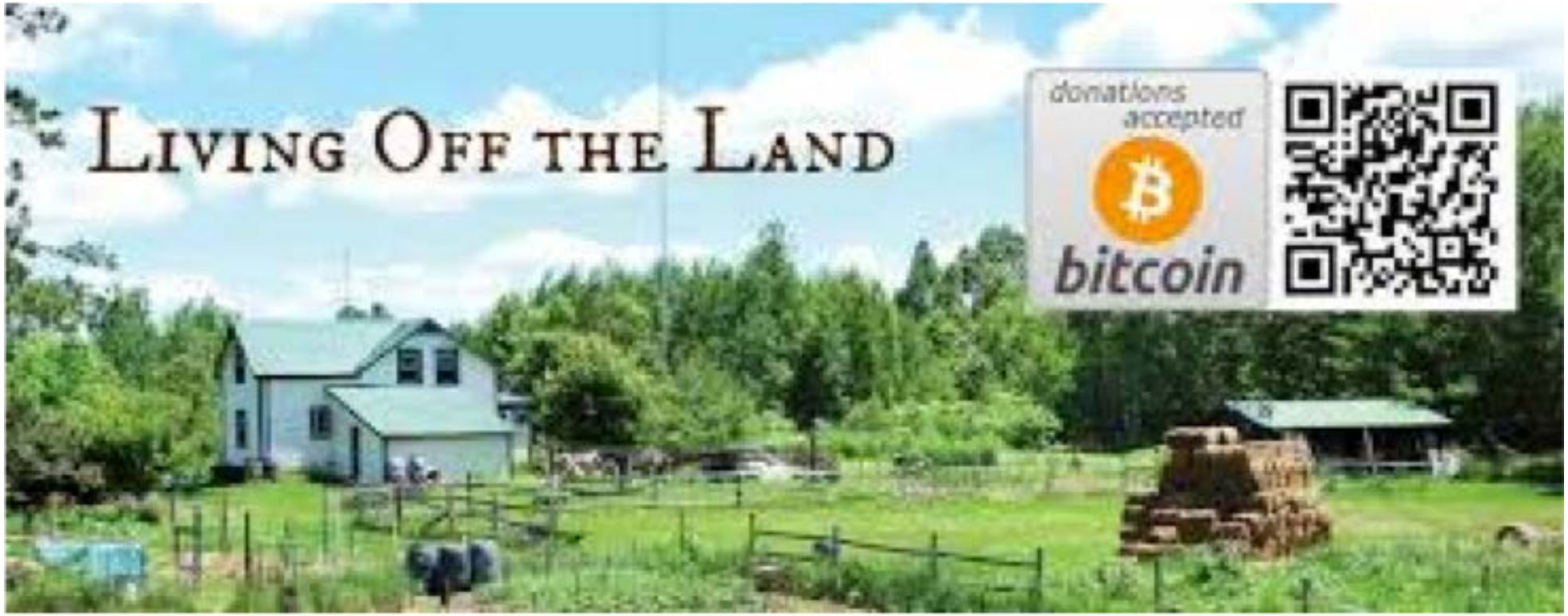
Asynchronous



redteam

Source : http://www.unitedliberty.org/files/images/ParadignShift.jpg

Ironic



Movement has started around using native windows tools to bypass protections via Microsoft signed executables

https://lolbas-project.github.io

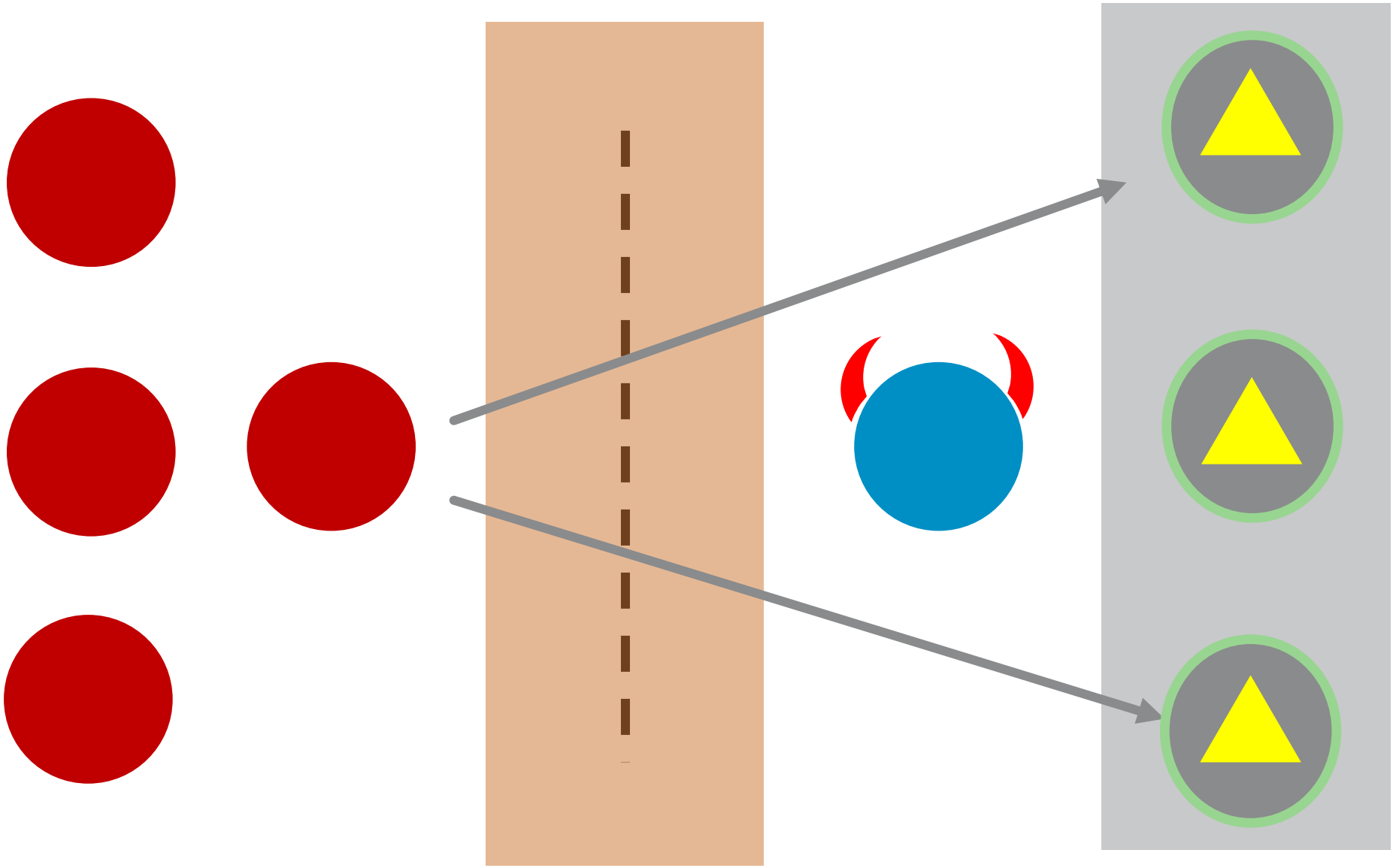
Binary	Functions	Type
Atbroker.exe	Execute	Binaries
Bash.exe	Execute, AWL bypass	Binaries
Bitsadmin.exe	Execute, Download, Copy, Alternate data streams	Binaries
Certutil.exe	Download, Encode, Decode, Alternate data streams	Binaries
Cmdkey.exe	Credentials	Binaries
Cmstp.exe	Execute, AWL bypass	Binaries
Control.exe	Alternate data streams	Binaries
Csc.exe	Compile	Binaries
Cscript.exe	Alternate data streams	Binaries
Dfsvc.exe	AWL bypass	Binaries
Diskshadow.exe	Execute, Dump	Binaries
Dnscmd.exe	Execute	Binaries

Attack

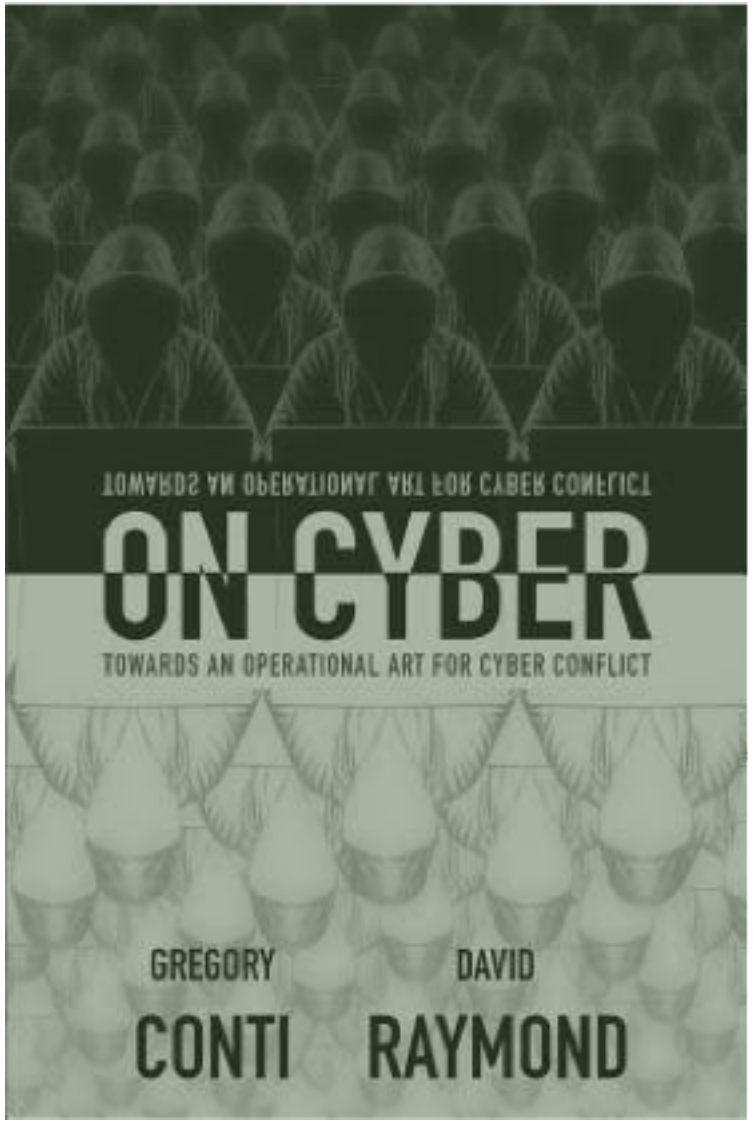
A campaign has a goal in mind :

- either to defend an attack from an enemy
- demonstrate ability to claim territory and/or resources
- protect those unable to defend themselves

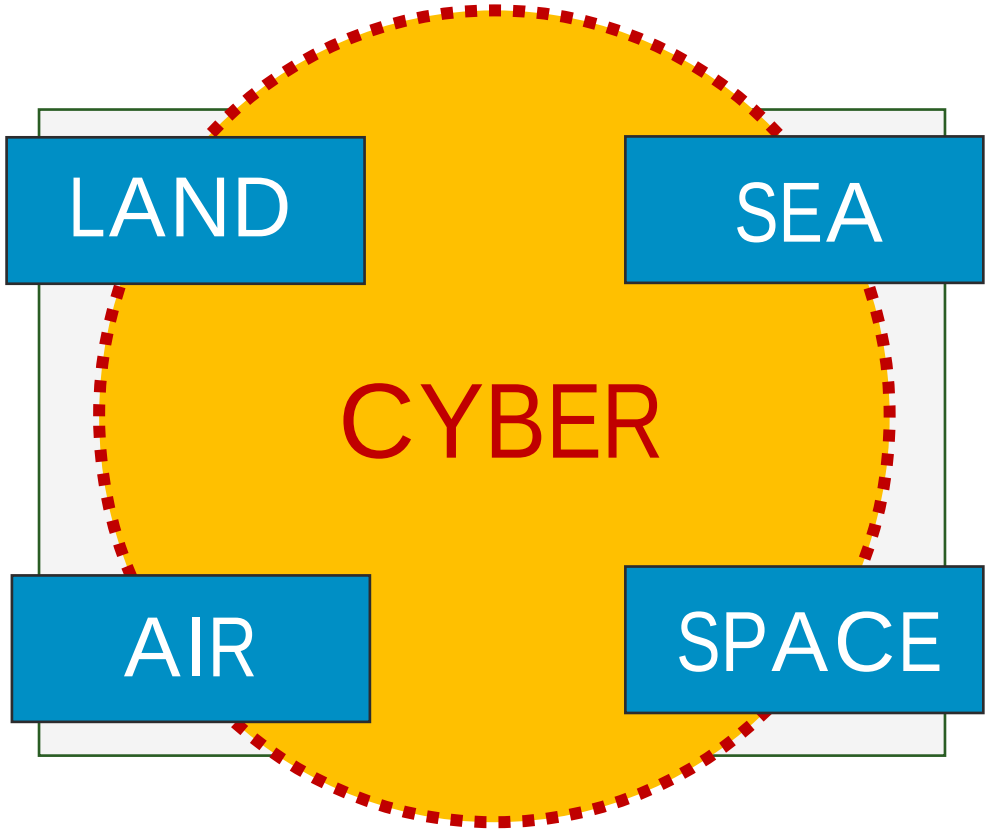
Attack



Nothing new



Domains of Battle



Operational Delivery

Protect the core

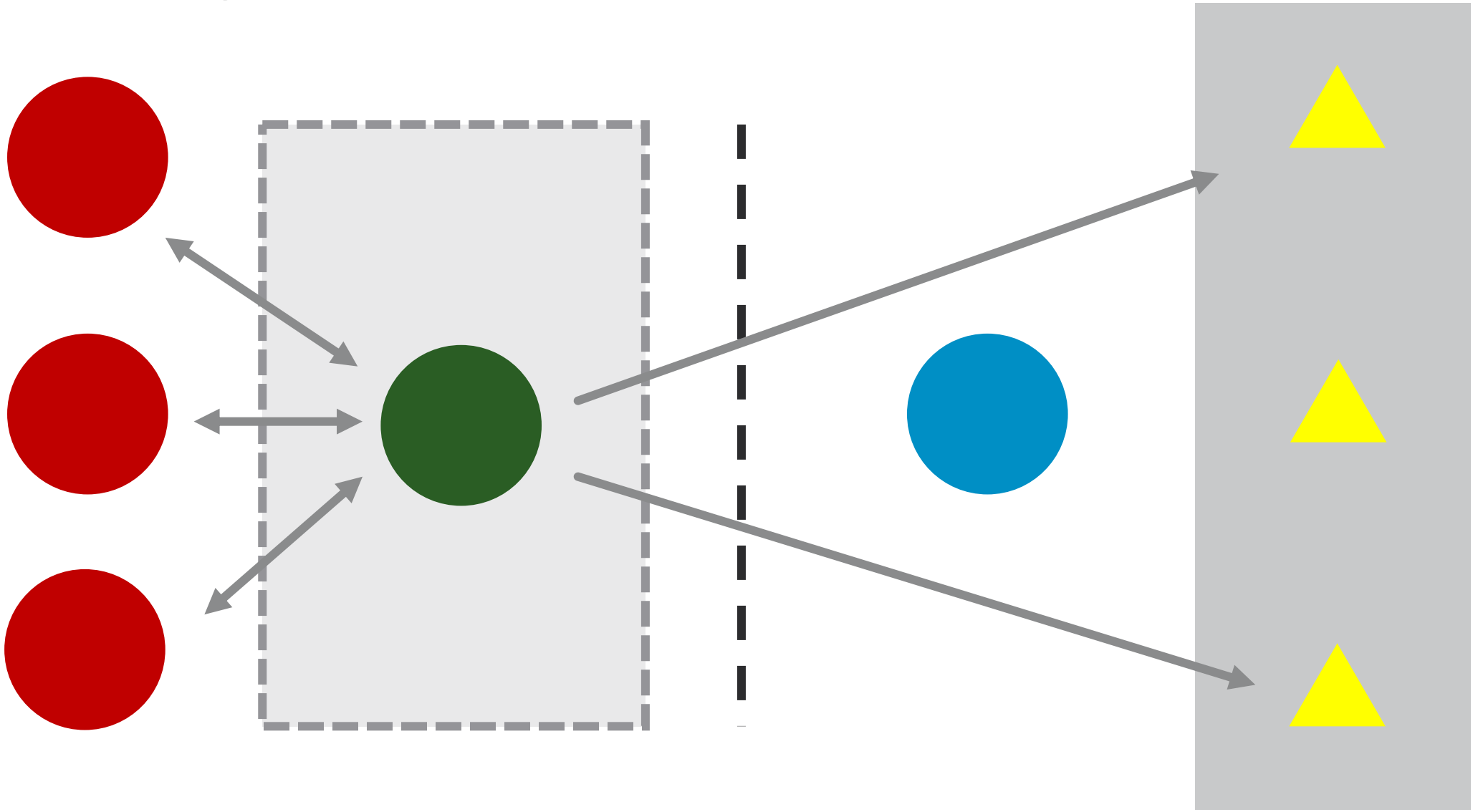
Protect C2 Infrastructure

Protect C2 Infrastructure

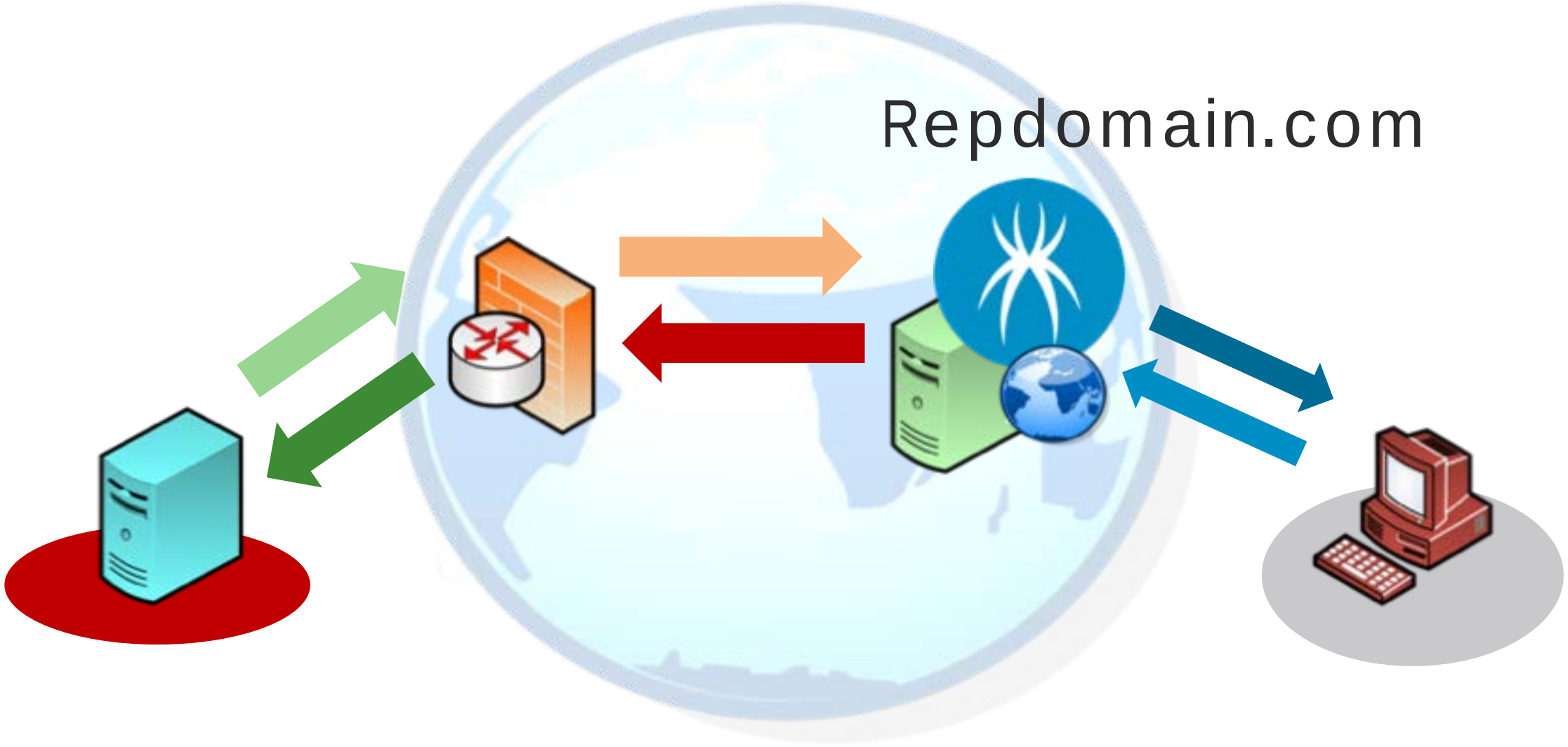
Redirectors

https://livingdeadrose.wordpress.com/tag/hiding/

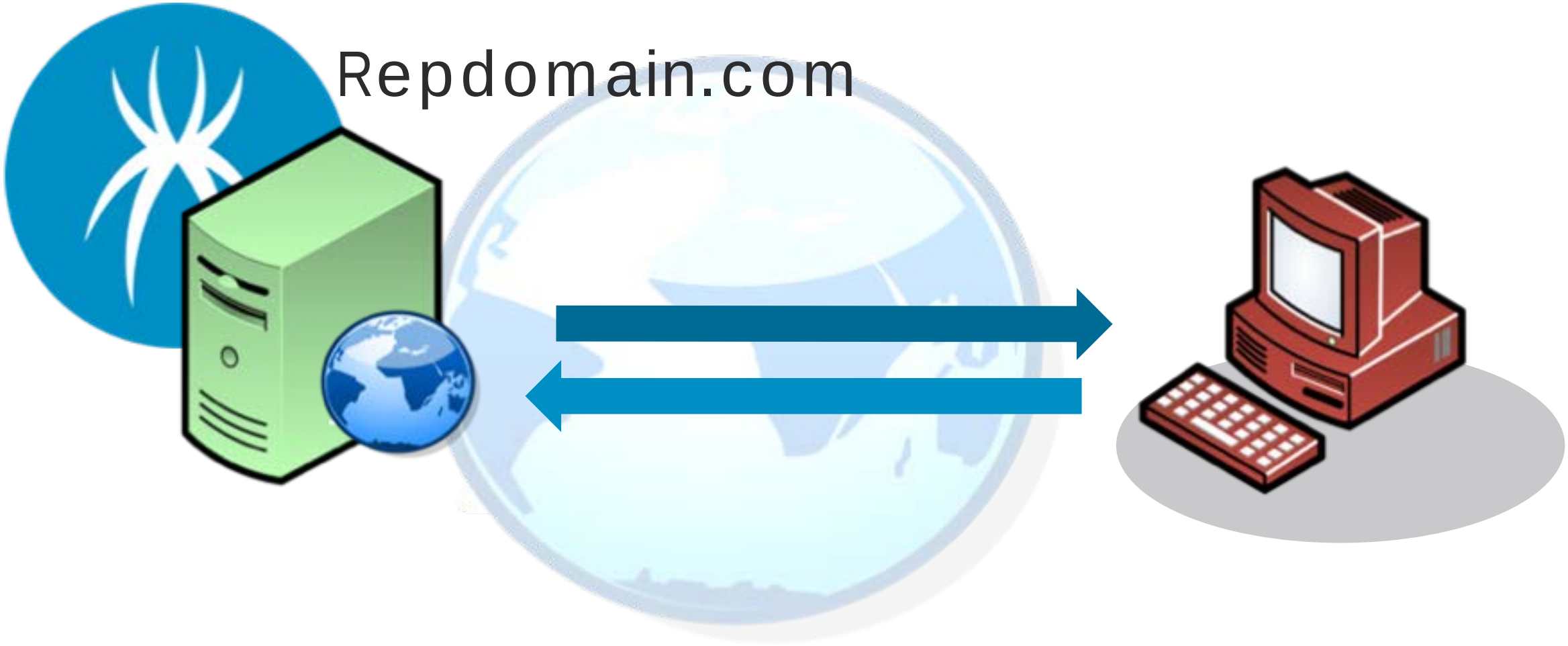
Protecting the core



Redirectors

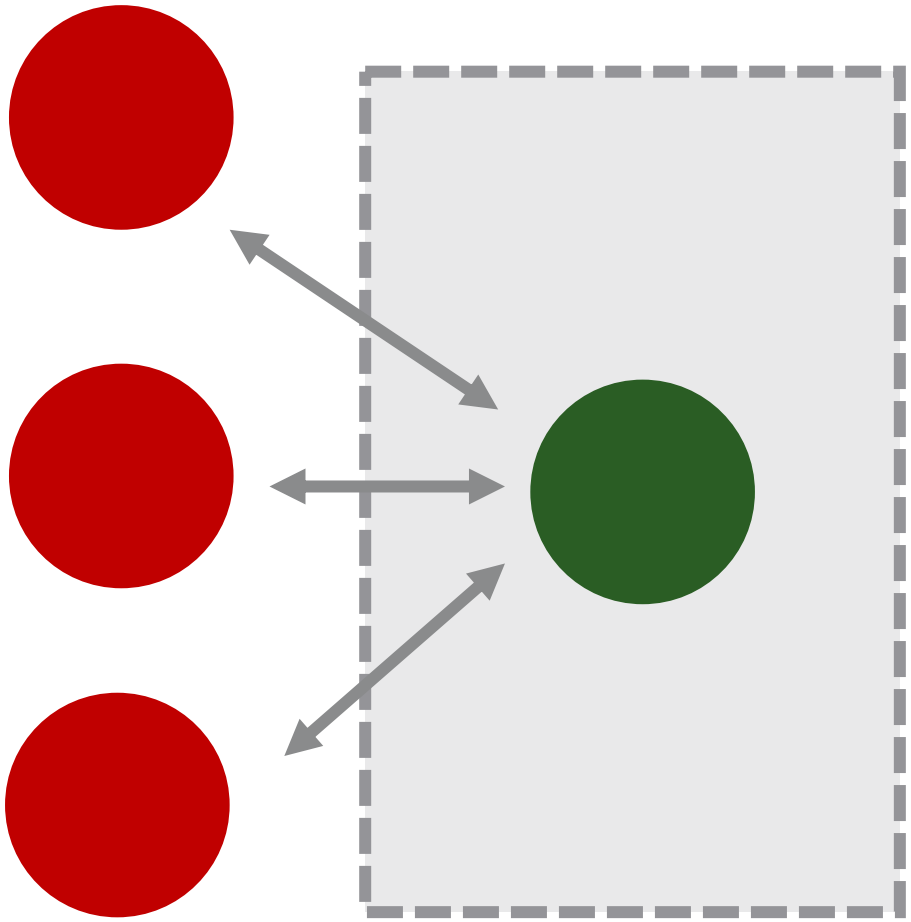


Redirectors

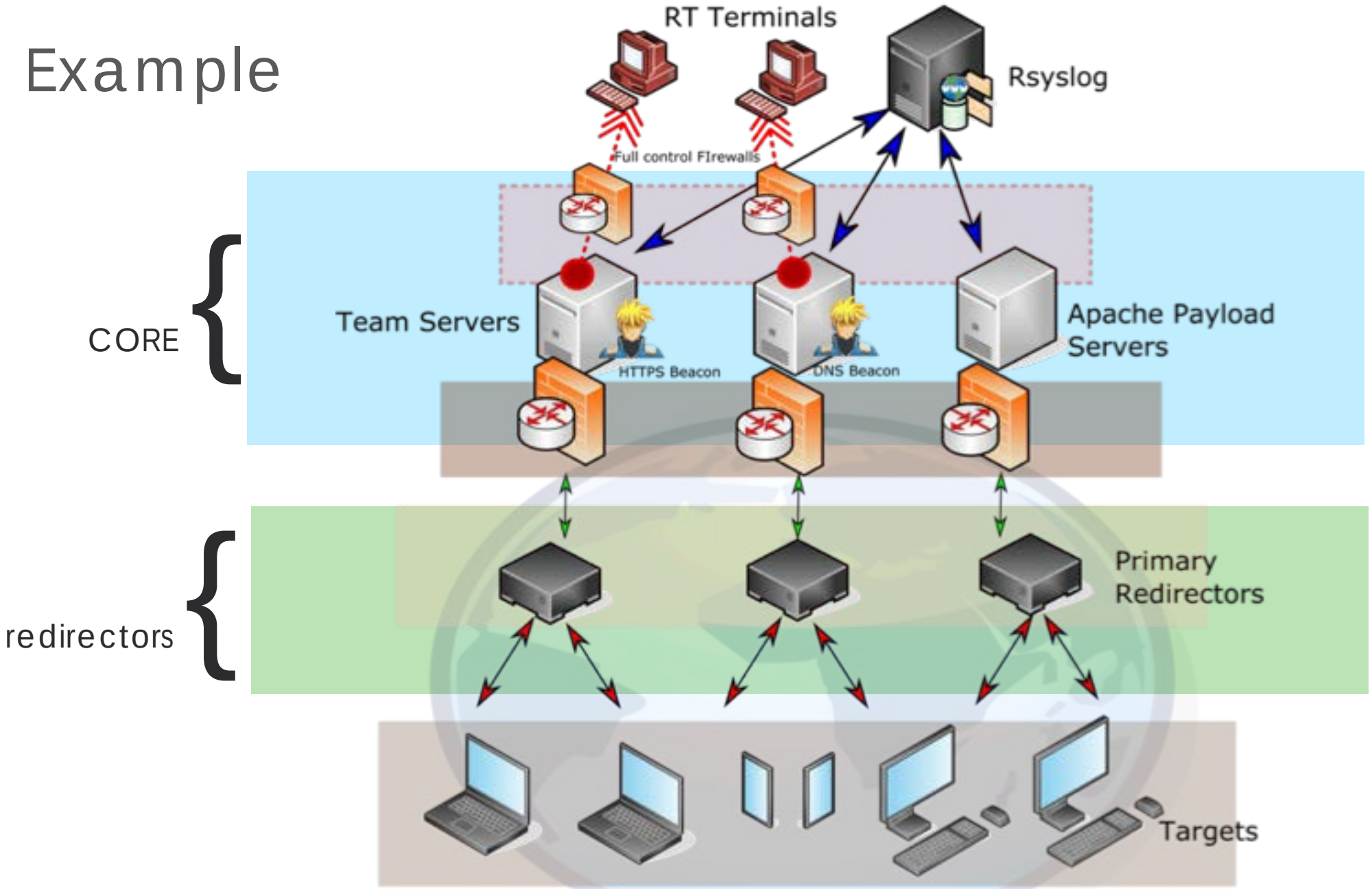


Redirectors

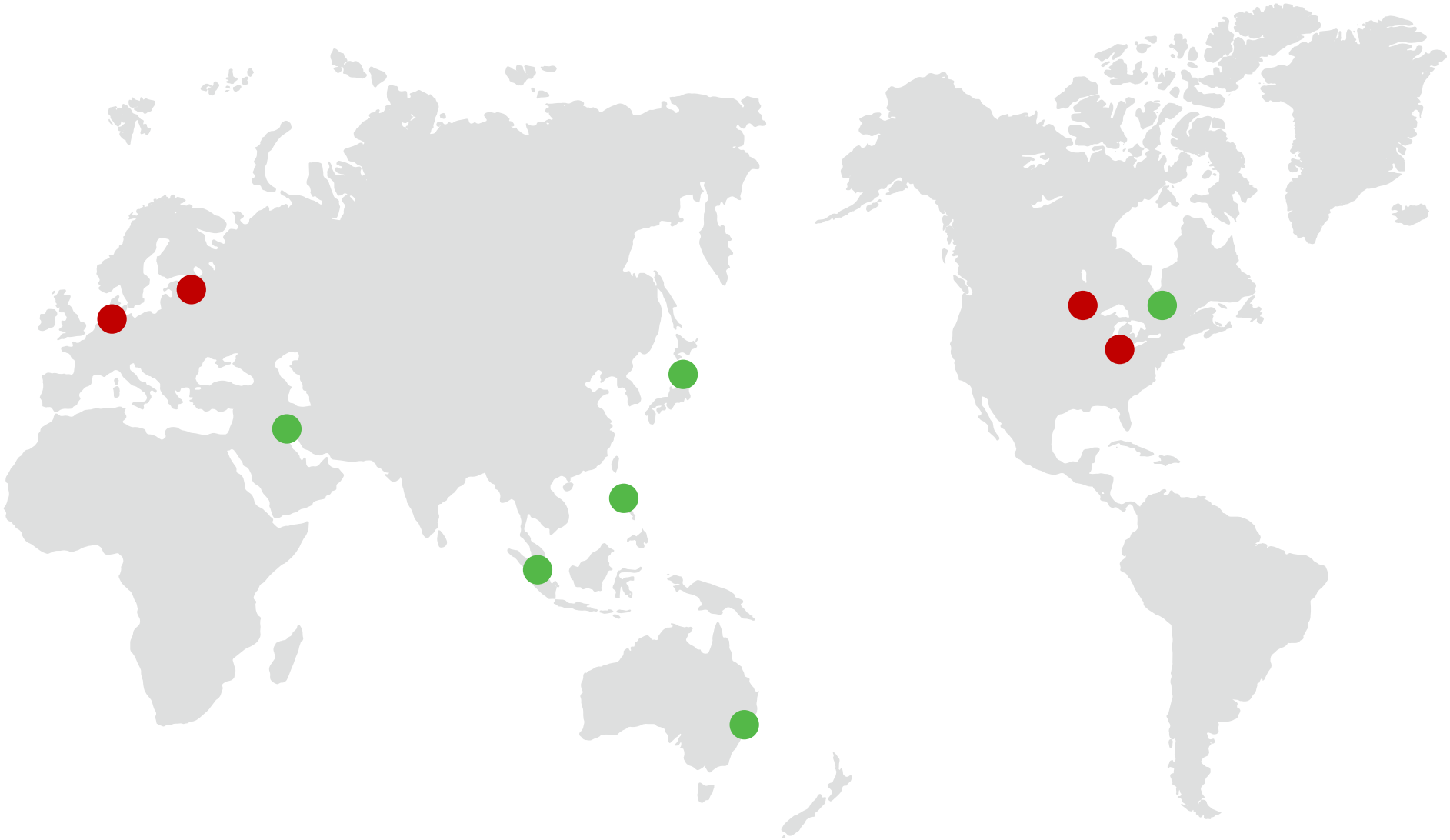
- Socat
- Apache Rewrite Modules
- Nginx
- Haproxy
- Domain Fronting
- Custom proxy
- Tor



Example


RT Terminals
Rsyslog
Full control FIrewalls
CORE
Team Servers
HTTPS Beacon
DNS Beacon
Apache Payload Servers
redirectors
Primary Redirectors
Targets

Distributed Operations



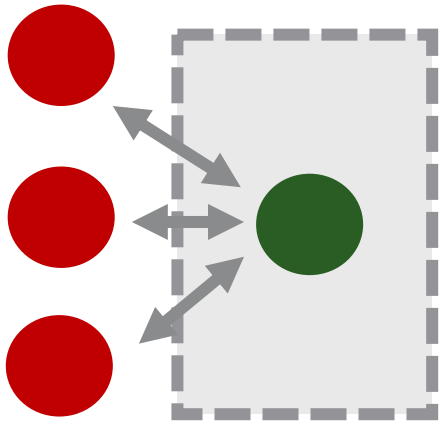
Core

Redirectors

Are we leaving a breadcrumb trail?

Domain Registration

IP Addresses for redirectors

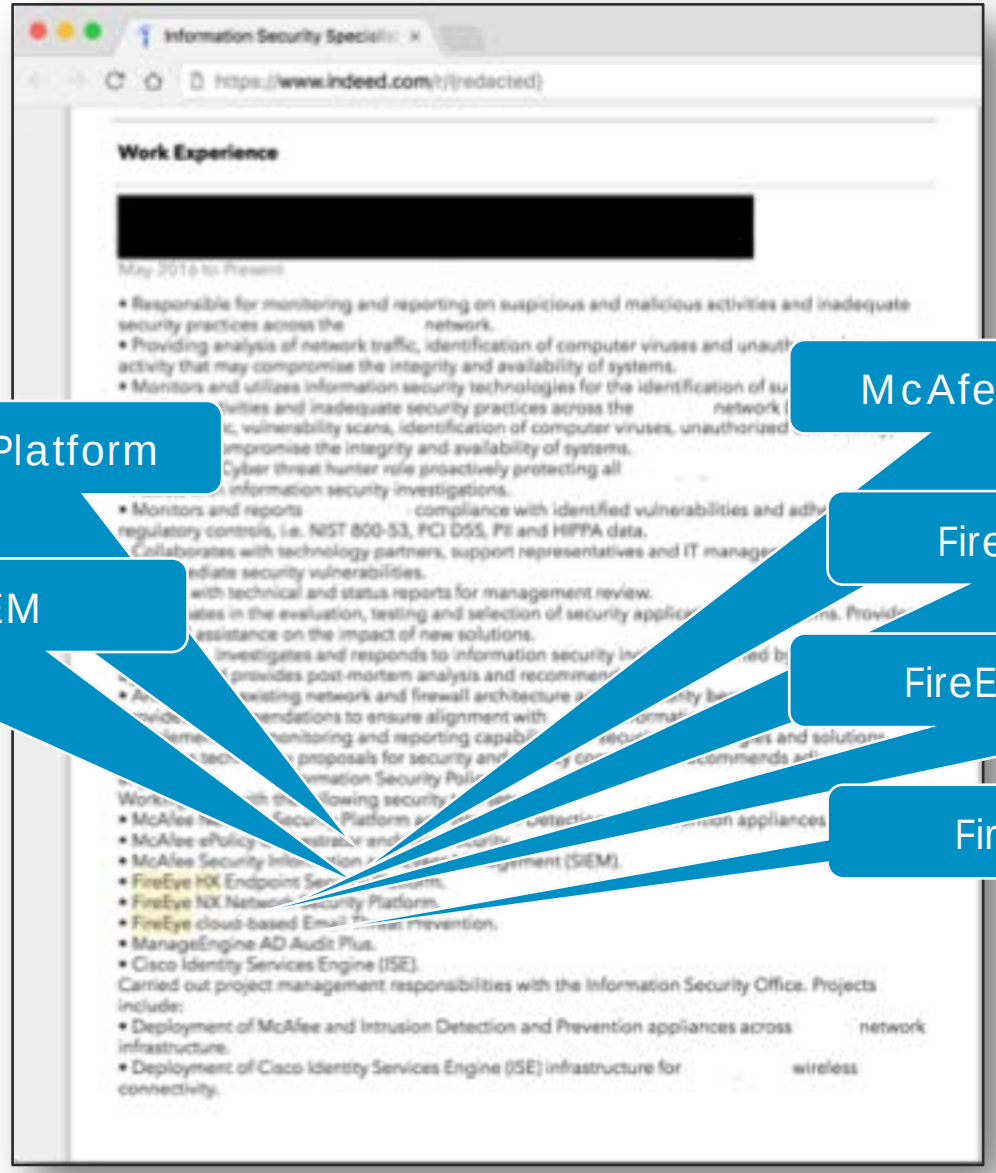


```
Updated Date: 2018-06-19T12:50:01Z
Creation Date: 2018-06-19T12:50:00Z
Registry Expiry Date: 2019-06-19T12:50:00Z
Registrar:
Registrar
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
```

Commence Attack

Information Leakage?

Open-Source Intelligence



McAfee Network Security Platform

McAfee NitroSecurity SIEM

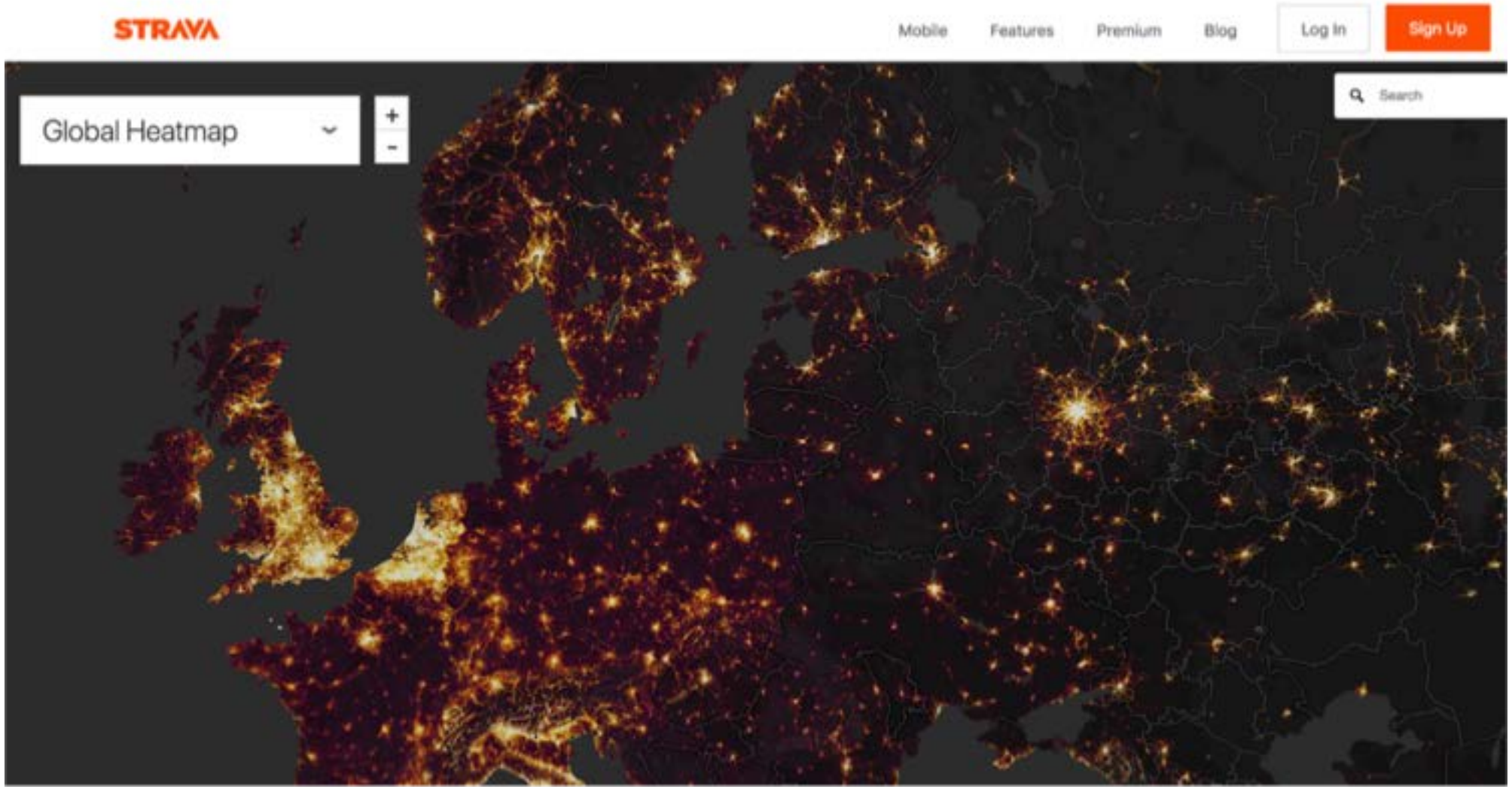
McAfee Endpoint Security Agents

FireEye Endpoint Security (HX)

FireEye Network Security (NX)

FireEye Cloud Email Security

Fitness Trackers

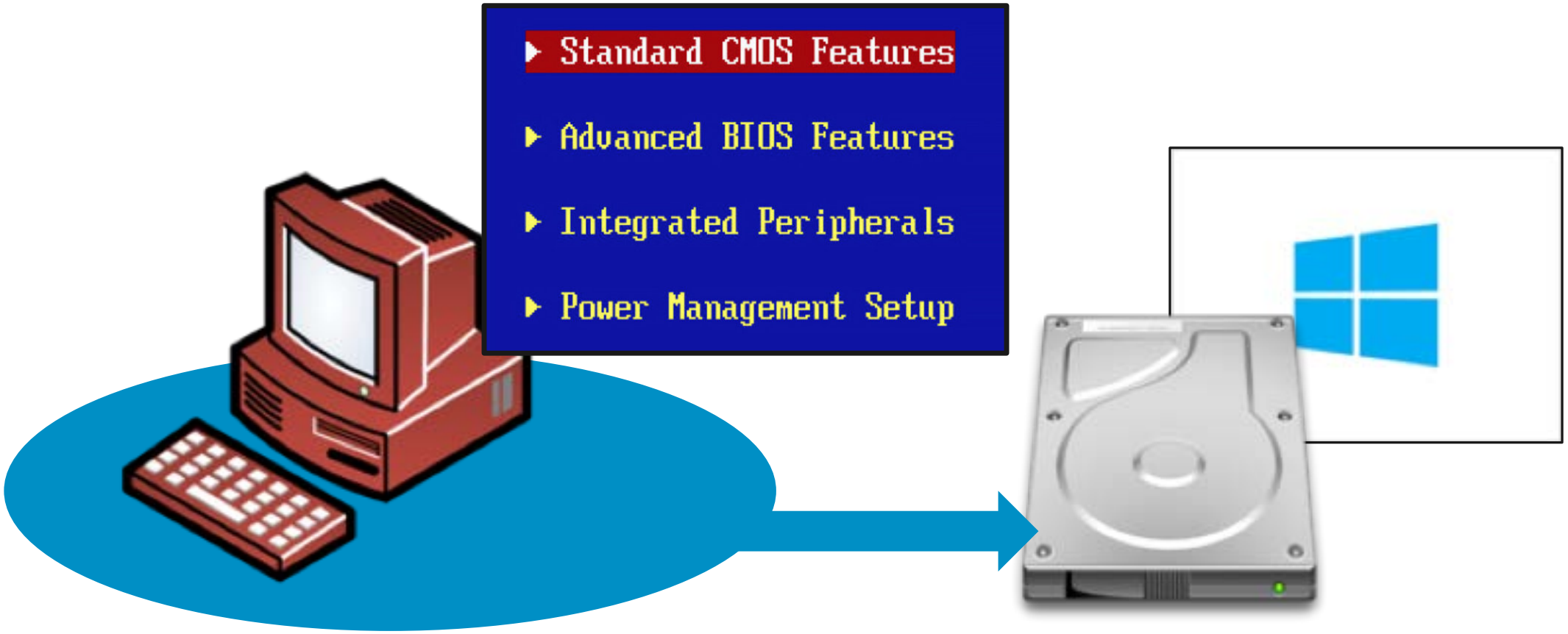


https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html?noredirect=on&utm_term=.99aaa799a484

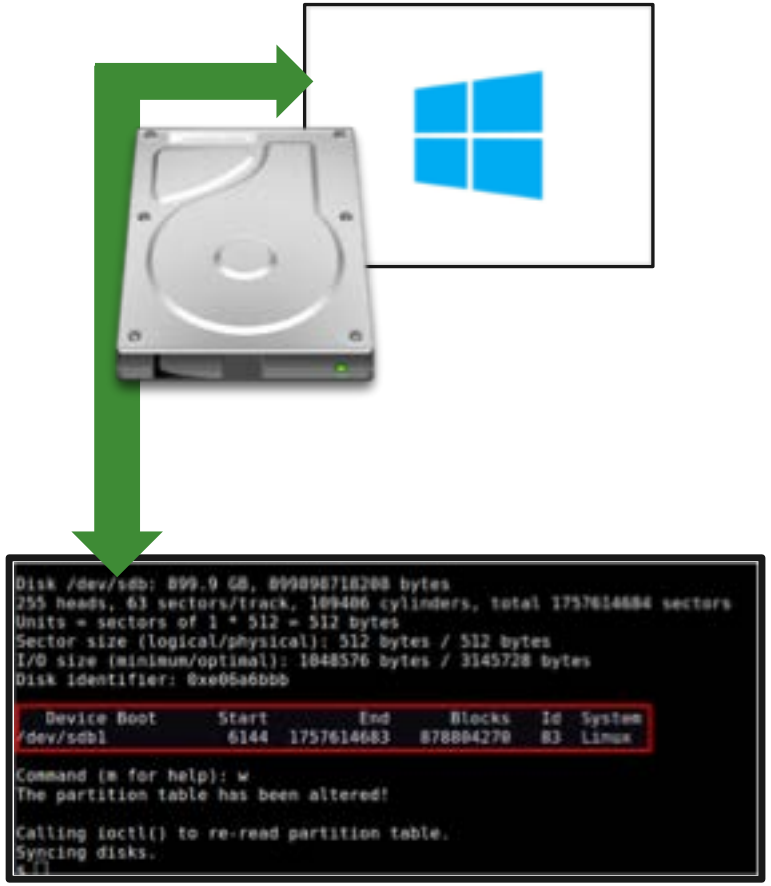
Fitness Trackers

Physical

BIOS Controls



BIOS Controls



BIOS Controls

Switch Port Controls

MAC address Controls

If MAC looking is implemented on a network switch port then this means that the port will only accept the mac address of a specific device.

Most desktop peripherals, such as desktop VoIP phones have information stickers.

MAC address Controls

MAC address Controls

It is trivial to spoof MAC addresses in Linux, and it is also possible to spoof them within Windows.

By impersonating a MAC address, this would give an attacker access to a port and any network segment configured to control the devices, such as a specific VLAN.

Spoof MAC Address

```
katana ¬> ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.173.249  netmask 255.255.255.0  broadcast 172.16.173.255
        inet6 fe80::250:56ff:fe3f:e5e0  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:3f:e5:e0  txqueuelen 1000  (Ethernet)
        RX packets 432787  bytes 615309157 (586.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 140282  bytes 11964965 (11.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Spoof MAC Address

```
[ ~ ]
katana ¬> macchanger -m 00:11:22:33:44:55 eth0
Current MAC:   00:50:56:3f:e5:e0 (VMware, Inc.)
Permanent MAC: 00:50:56:3f:e5:e0 (VMware, Inc.)
New MAC:       00:11:22:33:44:55 (CIMSYS Inc)


[ ~ ]
katana ¬> ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.173.249  netmask 255.255.255.0  broadcast 172.16.173.255
        inet6 fe80::250:56ff:fe3f:e5e0  prefixlen 64  scopeid 0x20<link>
        ether 00:11:22:33:44:55  txqueuelen 1000  (Ethernet)
        RX packets 432789  bytes 615309559 (586.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 140283  bytes 11965307 (11.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

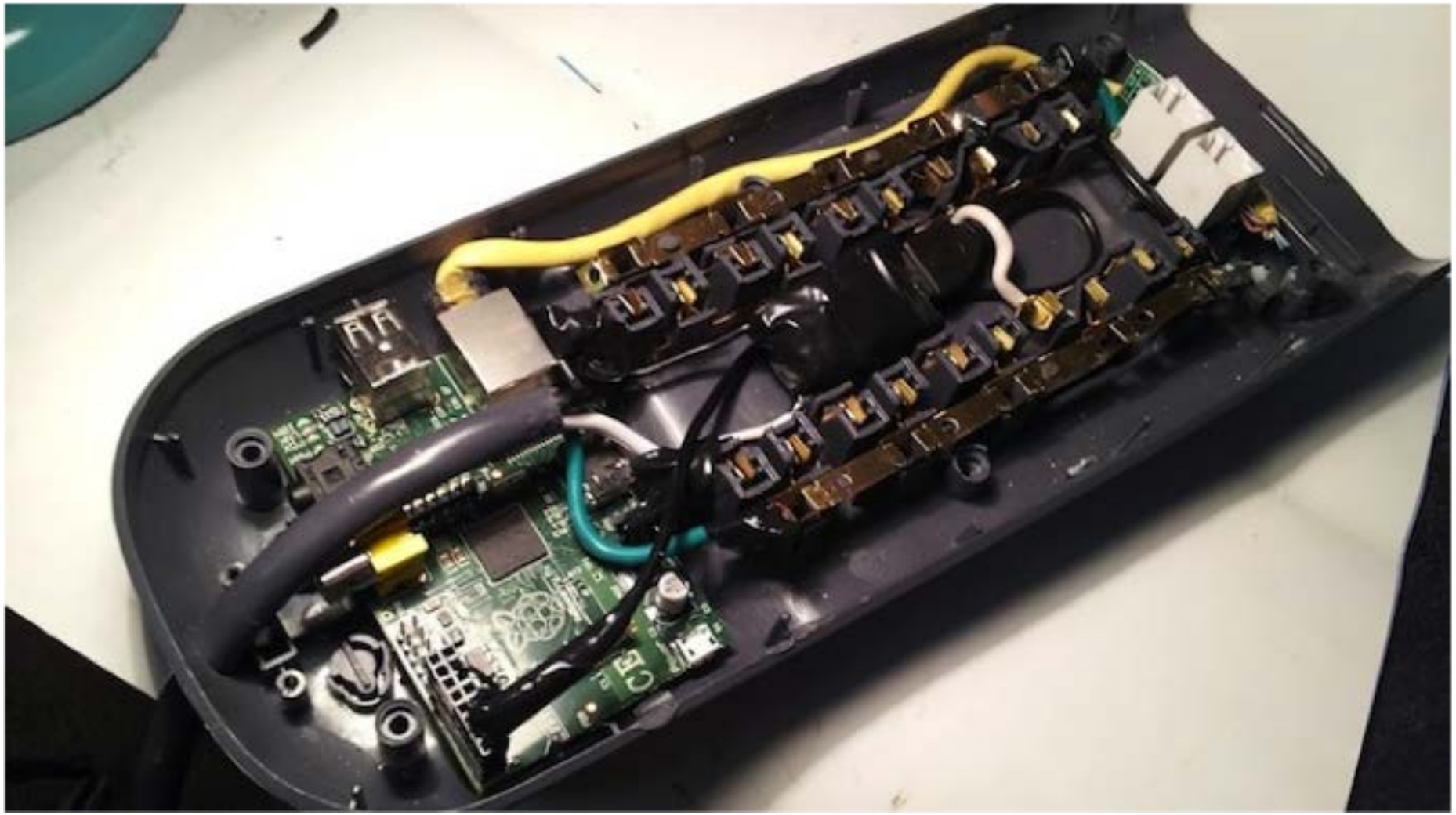
Physical Implants

Network Drop Boxes

Raspberry Pi's and other small ARM based computer devices make excellent physical network drop boxes. The idea is to plug these devices into a network and then gain a reverse connection out of the network.

Can be concealed into other devices to look more legitimate.

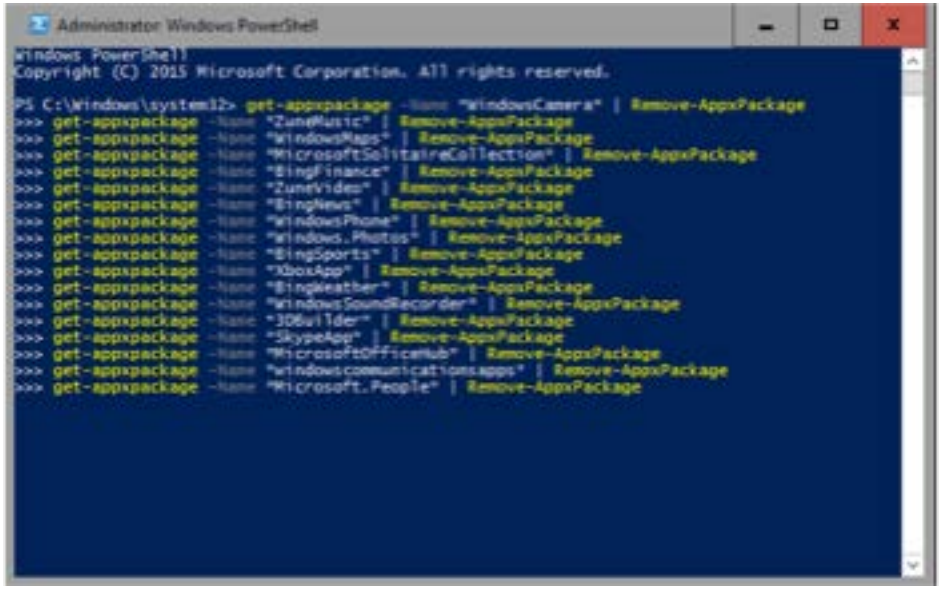
Raspberry PI Surge Projector



PowerShell


KEEP
CALM
AND
LEARN
POWERSHELL


KEEP
CALM
AND
LEARN
POWERSHELL
C#



Powershell.exe is a flag that responders signature on.

Excellent projects such as ‘unmanaged Powershell’ that call .dotNET assemblies, or writing custom csharp and compiling this in realtime are good approaches

Phishing

Benign Phishing

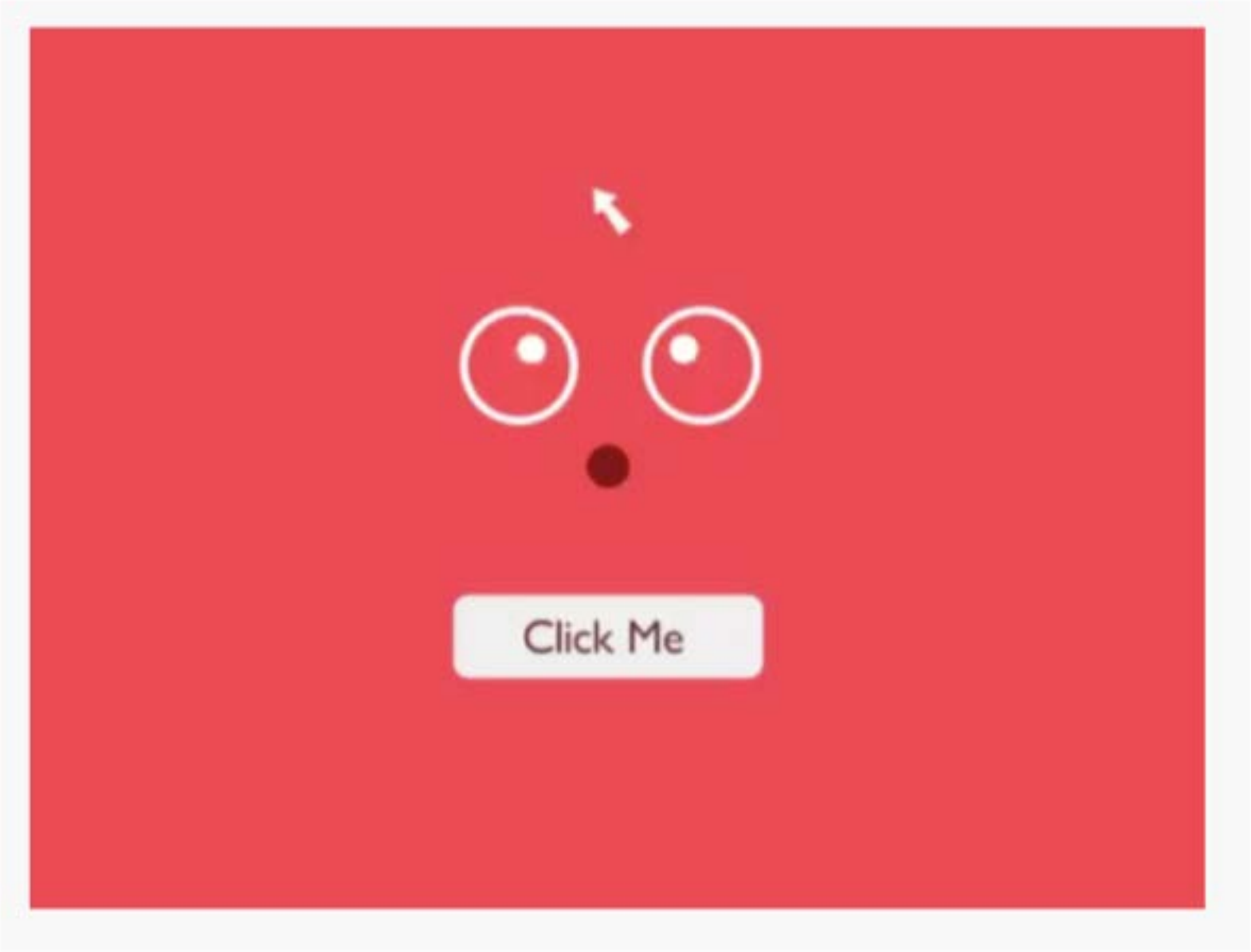
Benign Phishing

Benign Phishing

Delivery

Don’t **EVER** include any links or files when sending your first one or two spear phishes. Don’t try and emphasize urgency, or come off as aggressive. You want to write a nice realistic “note”, and quietly drop it in their inbox.

https://medium.com/@adam.toscher/top-five-ways-the-red-team-breached-the-external-perimeter-262f99dc9d17

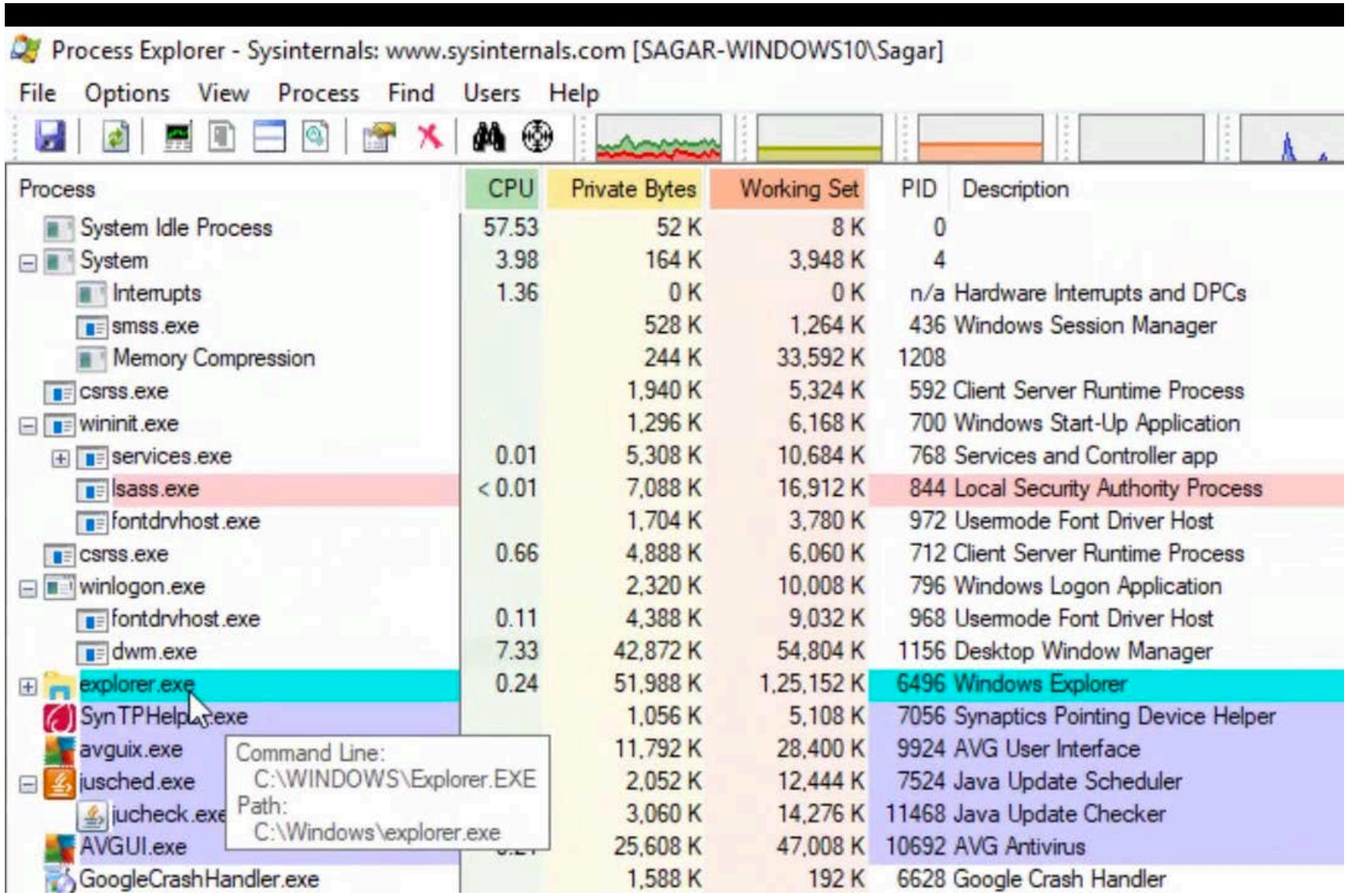

Click Me

De-chaining

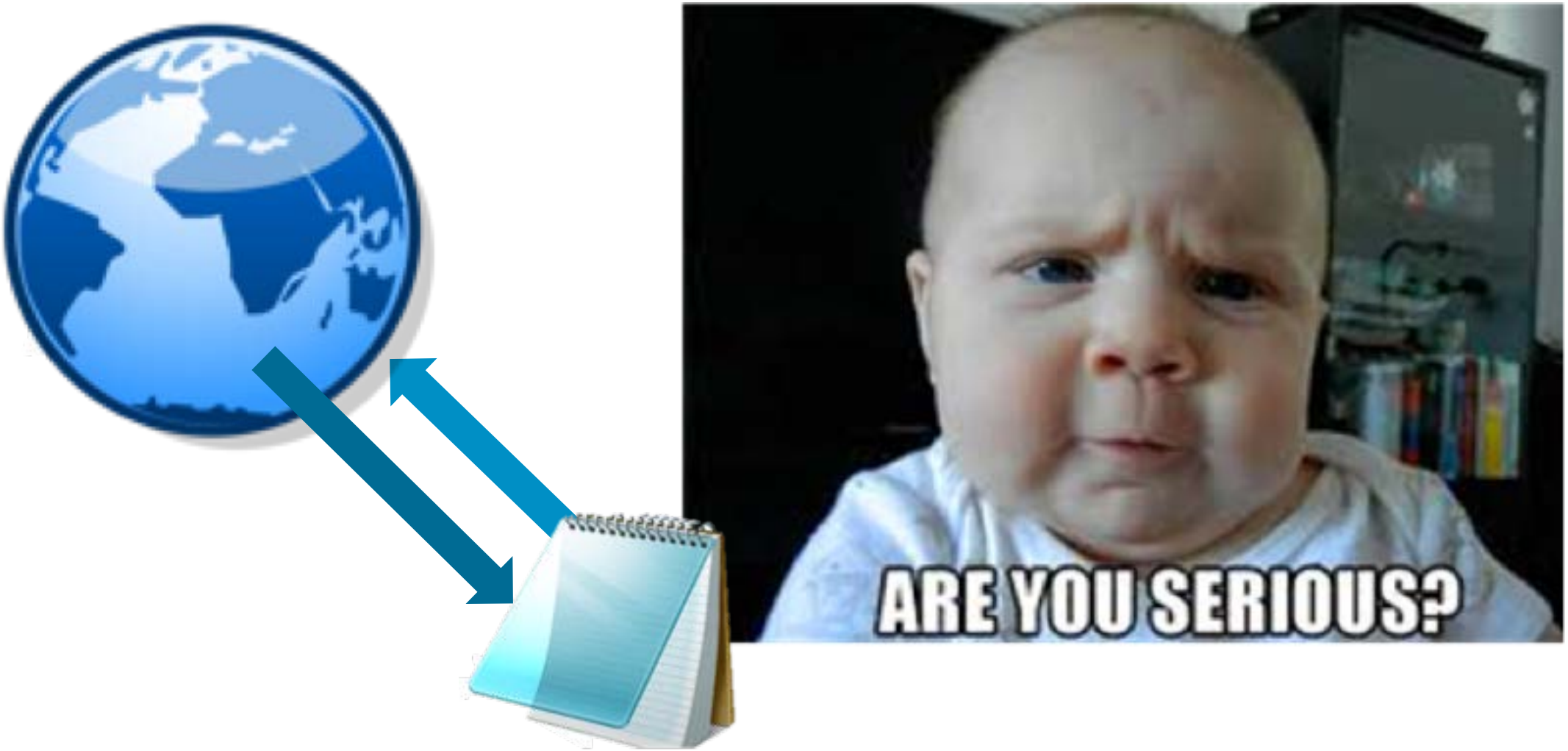
Foothold

Parent -> Child Processes

Processes


Process Explorer - Sysinternals: www.sysinternals.com [SAGAR-WINDOWS10\Sagar]
File Options View Process Find Users Help
Process CPU Private Bytes Working Set PID Description
System Idle Process 57.53 52 K 8 K 0
System 3.98 164 K 3,948 K 4
Interrupts 1.36 0 K 0 K n/a Hardware Interrupts and DPCs
smss.exe 528 K 1,264 K 436 Windows Session Manager
Memory Compression 244 K 33,592 K 1208
csrss.exe 1,940 K 5,324 K 592 Client Server Runtime Process
wininit.exe 1,296 K 6,168 K 700 Windows Start-Up Application
services.exe 0.01 5,308 K 10,684 K 768 Services and Controller app
lsass.exe < 0.01 7,088 K 16,912 K 844 Local Security Authority Process
fontdrvhost.exe 1,704 K 3,780 K 972 Usermode Font Driver Host
csrss.exe 0.66 4,888 K 6,060 K 712 Client Server Runtime Process
winlogon.exe 2,320 K 10,008 K 796 Windows Logon Application
fontdrvhost.exe 0.11 4,388 K 9,032 K 968 Usermode Font Driver Host
dwm.exe 7.33 42,872 K 54,804 K 1156 Desktop Window Manager
explorer.exe 0.24 51,988 K 1,25,152 K 6496 Windows Explorer
SynTPHelper.exe 1,056 K 5,108 K 7056 Synaptics Pointing Device Helper
avguix.exe 11,792 K 28,400 K 9924 AVG User Interface
jusched.exe 2,052 K 12,444 K 7524 Java Update Scheduler
jucheck.exe 3,060 K 14,276 K 11468 Java Update Checker
AVGUI.exe 25,608 K 47,008 K 10692 AVG Antivirus
GoogleCrashHandler.exe 1,588 K 192 K 6628 Google Crash Handler
Command Line:
C:\WINDOWS\Explorer.EXE
Path:
C:\Windows\explorer.exe

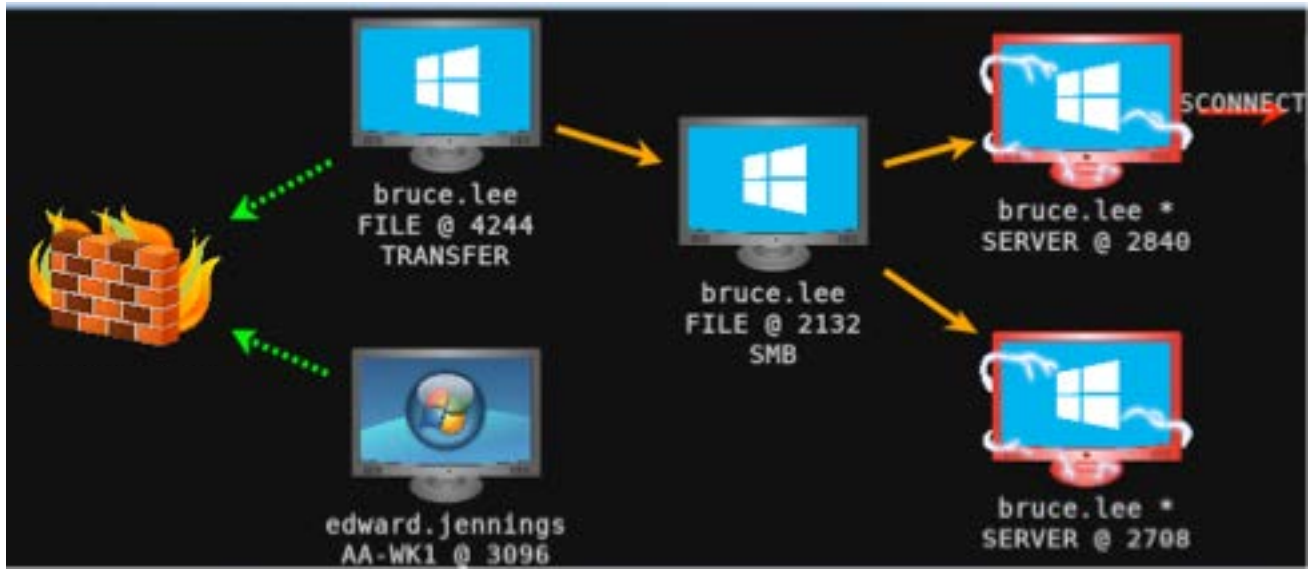
Notepad



Lateral Movement

Lateral Movement

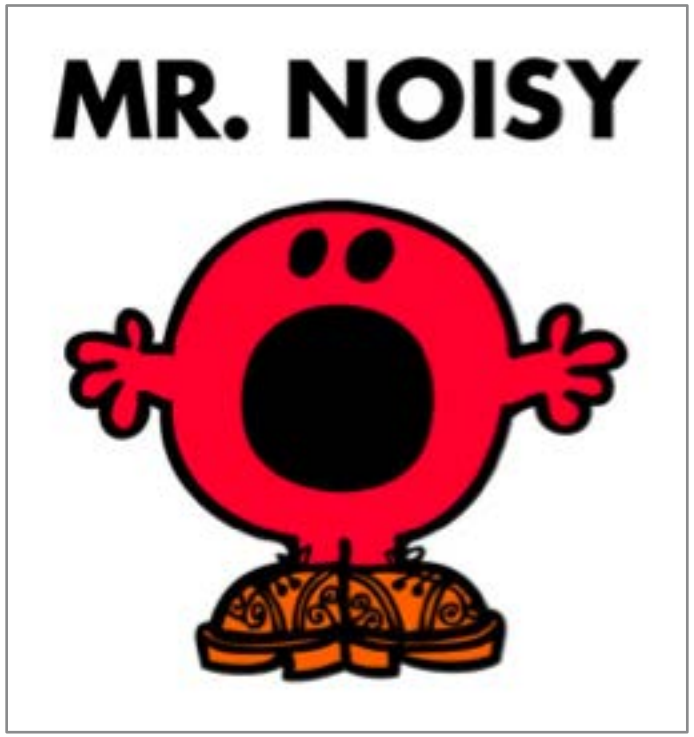
SMB Named Pipes



Initial footholds should be the pivot out of the network and ideally traffic should route via these initial pivots. Points of persistence if needed.

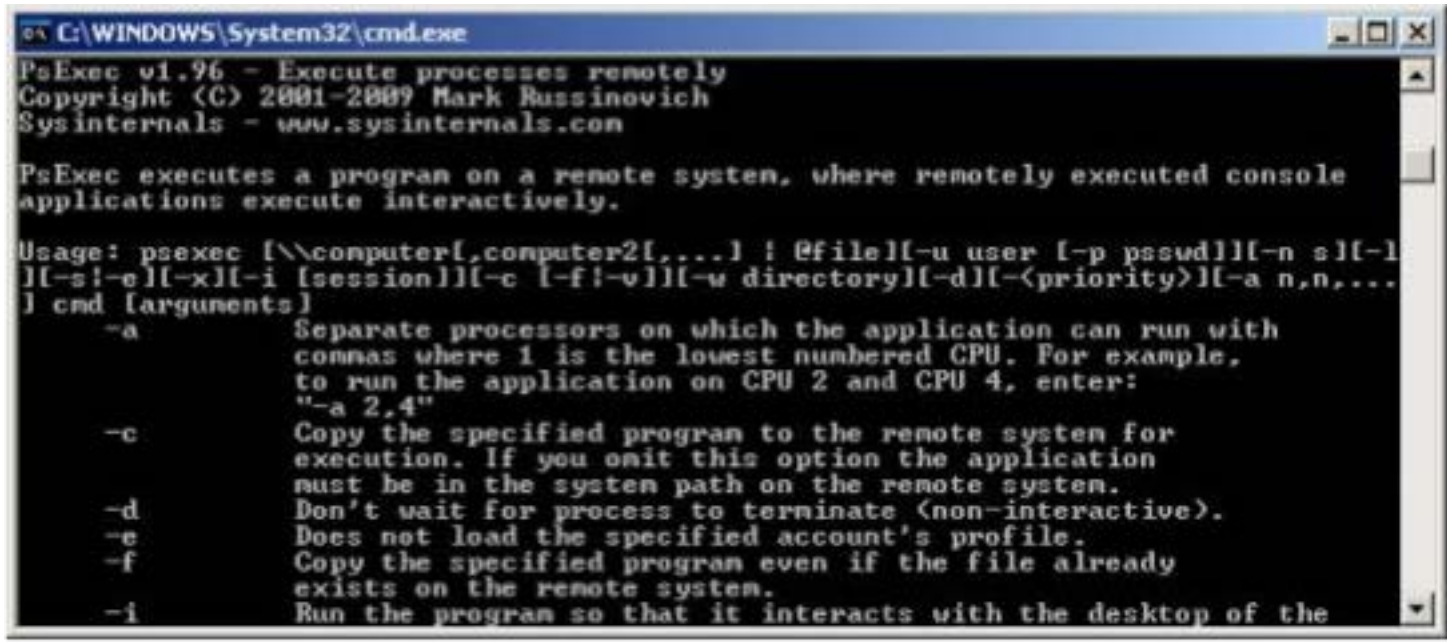
Use of SMB named pipes for lateral movement between hosts.

Sysinternals PsExec



Starts a service

Leaves an EVENT ID trace - 7045



Reporting

MITRE ATT&CK Framework

MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK™

ATT&CK Matrix for Enterprise

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

Skills Progression

practice makes perfect

perfect practice makes perfect

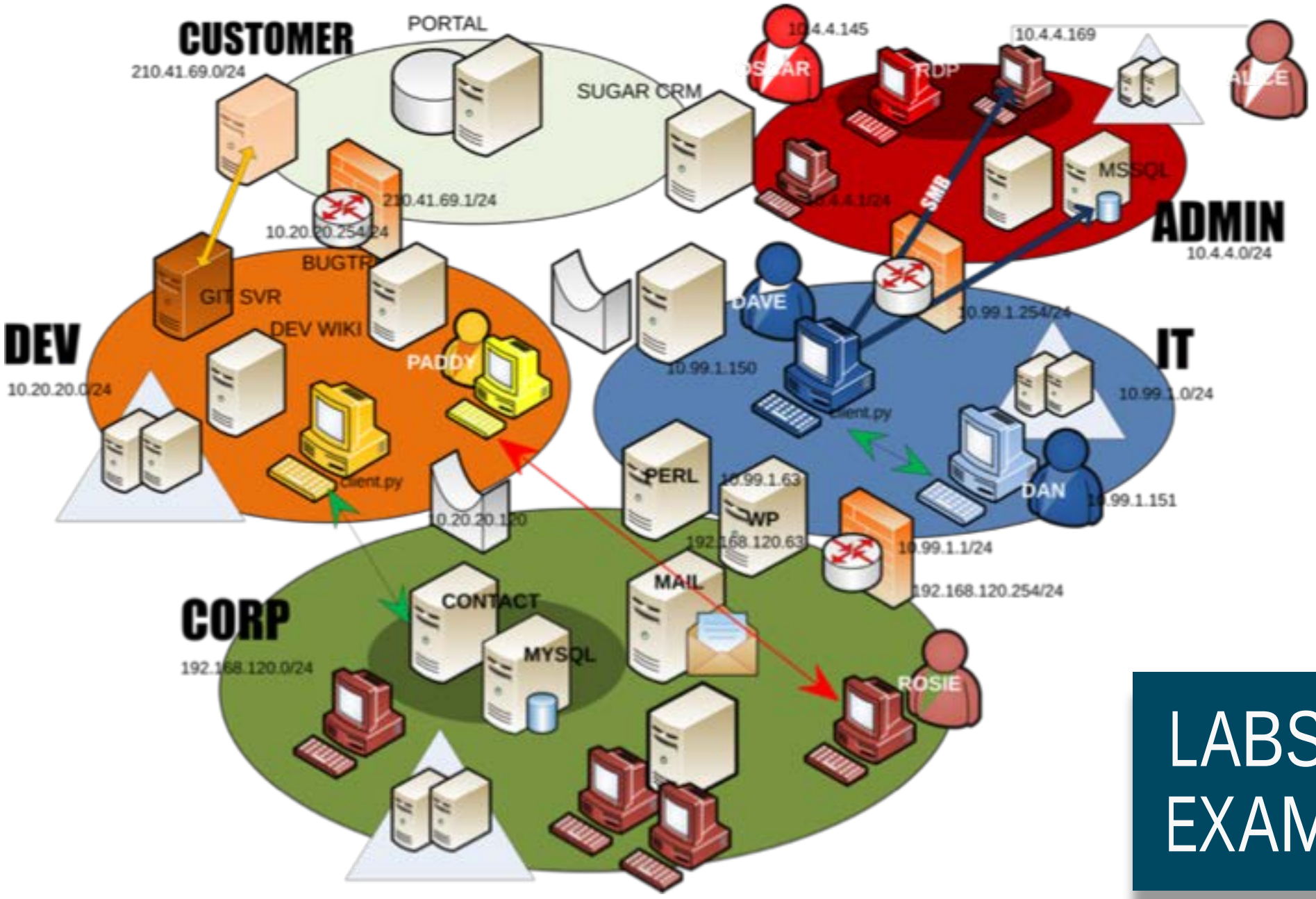
“You can shoot eight hours a day, but if your technique is wrong, all you become is good at shooting the wrong way. Get the fundamentals down and the level of everything you do will rise.”

Michael Jordan: American Basket Ball Star

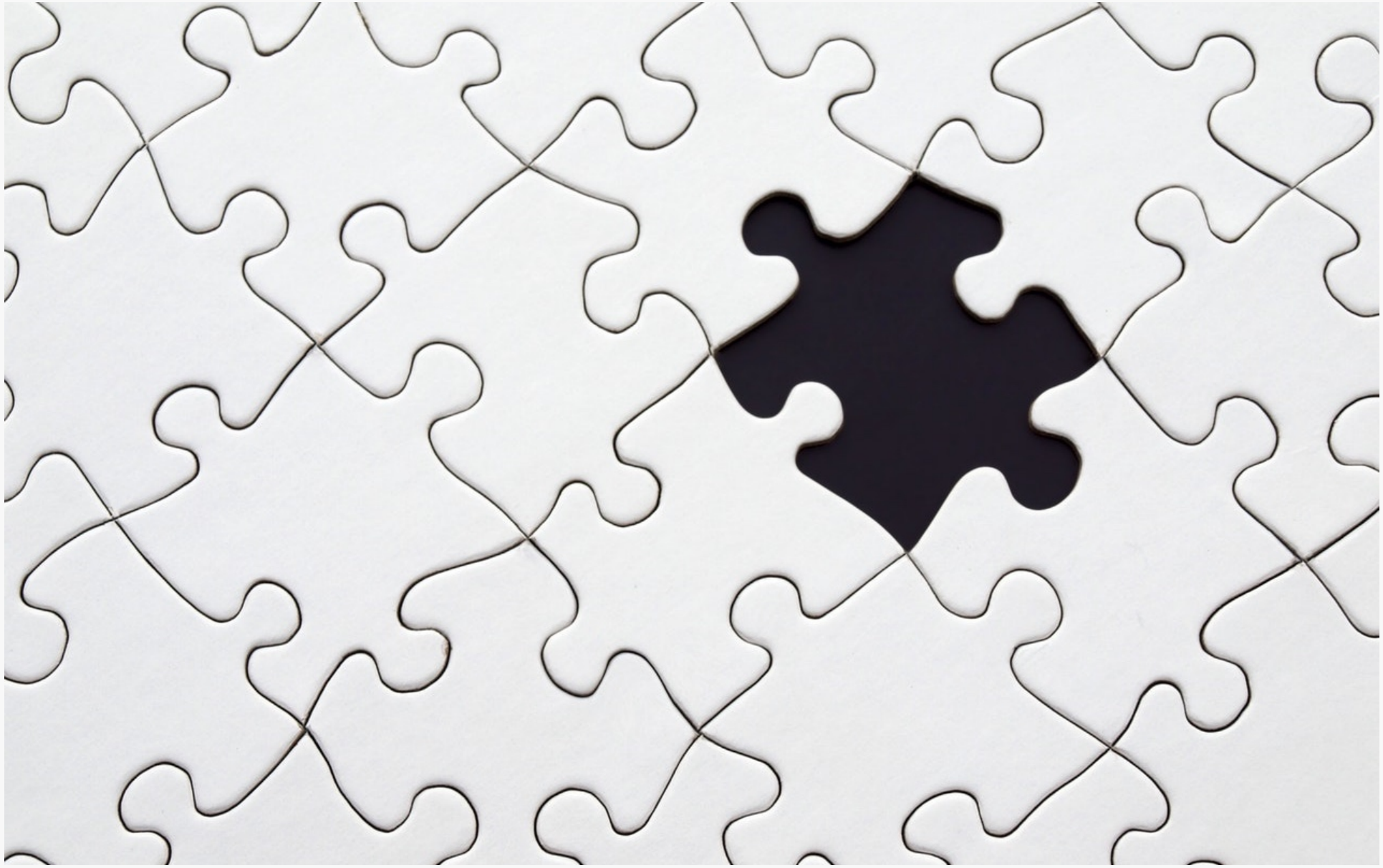
Internal Lab Infrastructure

Ensure your Lab environments have working Windows Server and Clients Active Directory, Microsoft Office and the current version of A/V. Ideally you can test more advanced threat detection products like Fire Eye or Crowd Strike in a LAB environment.

https://medium.com/@adam.toscher/top-five-ways-the-red-team-breached-the-external-perimeter-262f99dc9d17



LABSEED EXAMPLE



people

SheepL

SheepL

- Written in python3 and generates valid AutoIT language
- tasks – creating documents, browsing, command lines
- emulation of key strokes
- amount of time to complete them
- random time intervals
- compiled into a binary that can be run at startup/login

SheepL

https://www.github.com/SpiderLabs/sheepl

Summary

- Redirectors should be in place of all C2 infrastructure
- Know the thy target
- Parent -> Process relationships – Spawn/migrate to ‘expected’ processes
- Outbound HTTP calls should be from a process that normally makes Internet requests

Trustwave®

Smart security on demand