Purple Network Eaters

A Practical Demonstration of Hacking and Defending Your Organization

Disclaimer

The information contained herein is general in nature and is not intended, and should not be construed, as legal, accounting, or tax advice or opinion provided by CliftonLarsonAllen LLP to the user. The user also is cautioned that this material may not be applicable to, or suitable for, the user's specific circumstances or needs, and may require consideration of non-tax and other tax factors if any action is to be contemplated. The user should contact his or her CliftonLarsonAllen LLP or other tax professional prior to taking any action based upon this information. CliftonLarsonAllen LLP assumes no obligation to inform the user of any changes in tax laws or other factors that could affect the information contained herein.

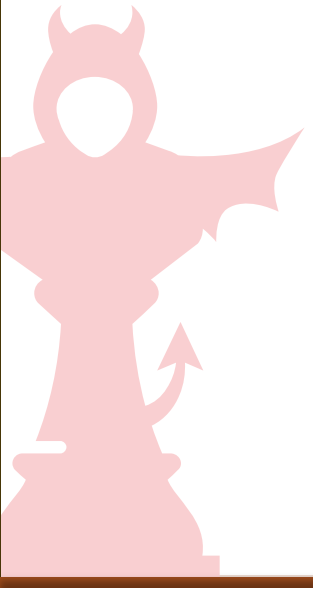
Learning Objectives

By the end of this session, you will be able to:

- Describe the attacker's methodology
- Identify the ways to detect malicious activity
- Describe defensive tools and mitigating controls that assist network administrators secure their environment

Outline

- Introductions
  - Presenters
  - Presentation format
  - Cyber kill chain example
- Anatomy of an Attack
  - External Recon
  - Weaponization
  - Delivery
  - Exploitation
  - Command and Control
  - Internal Network Recon
  - Capture the flag
  - Exfiltration



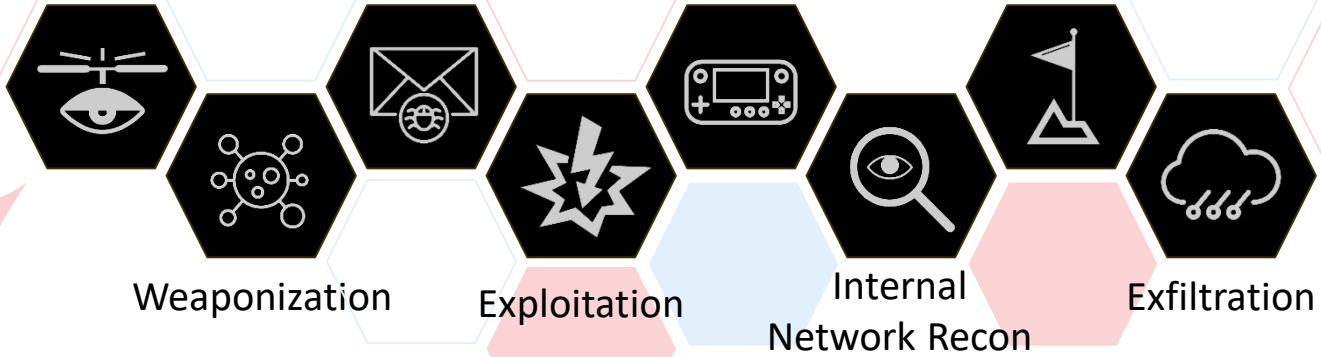
$ whoami

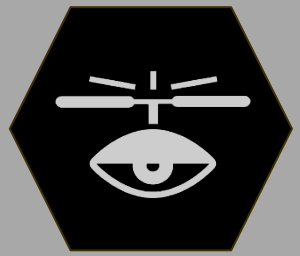
- Forrest Kasler, CPA
  - CPA Turned Hacker
  - Repeat Black Hat USA Presenter
  - Oversee and participate in:
    - Penetration Testing
    - Social Engineering
    - Vulnerability Assessments
    - IT Security audits
    - Code Reviews

$ whoami

- David Anderson
  - Farmer turned hacker
  - Offensive Security Certified Professional (OSCP)
  - Oversee cybersecurity team

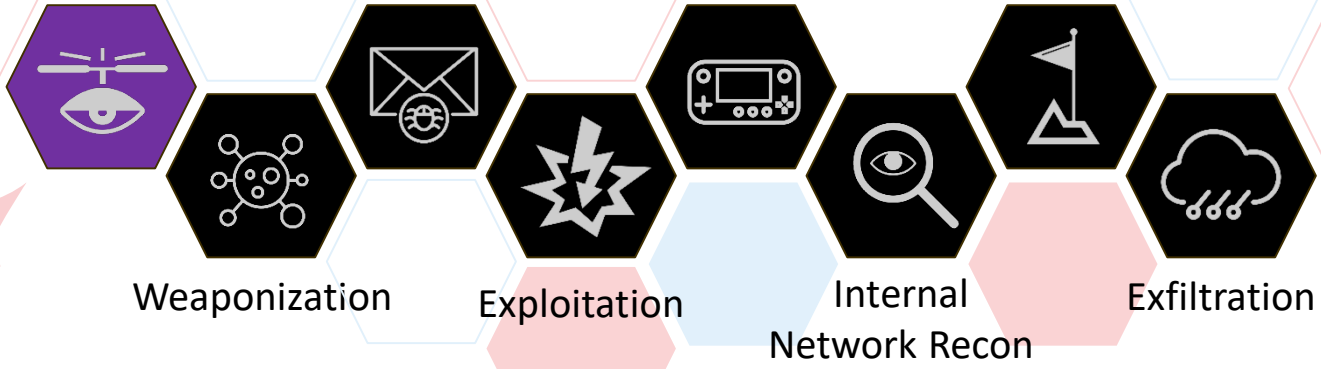
The Cyber Kill Chain





External Recon

CyberKill Chain



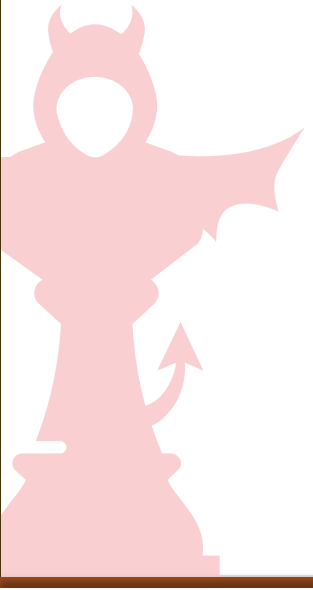
External Recon

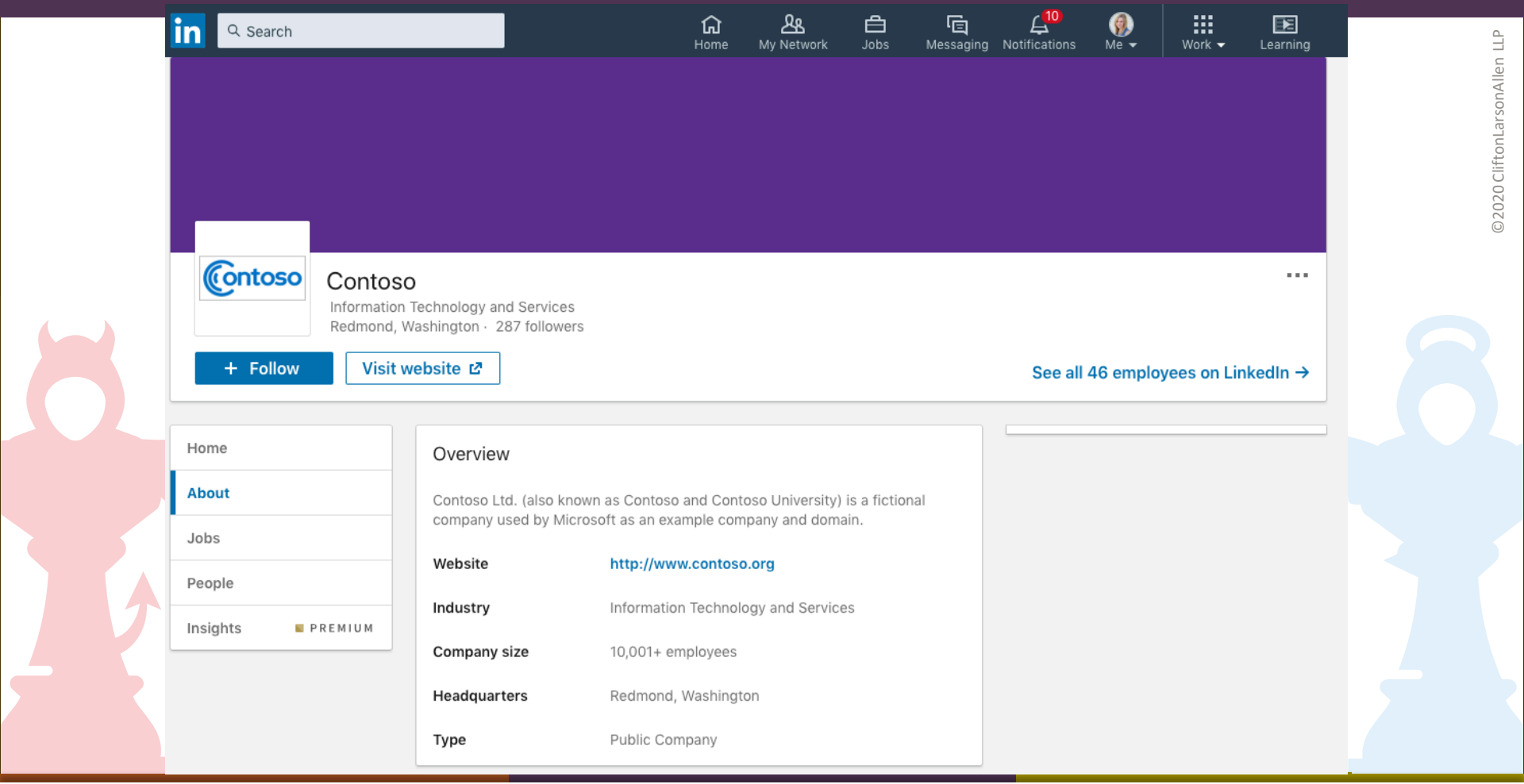
- Systems
  - Shodan
  - DNS brute forcing
  - Port and Service enumeration
  - TLS Certificate information
  - Whois Database Mining

External Recon

- **Employees**
  - Website
  - Social media
  - Search engines
  - Hosted documents

[DEMO]





Showing 42 results

Hilda Cavallari • 3rd
Recruiter @ Contoso
Washington D.C. Metro Area

Message

LinkedIn Member
Contoso administrator at Contoso
Hamburg Area, Germany

LinkedIn Member
Customer at Contoso
Wichita, Kansas Area

LinkedIn Member
Technician at Contoso
Columbus, Ohio Area

LinkedIn Member
Testing Specialist at Contoso
Kansas City, Missouri Area

LinkedIn Member
Customer Service Manager at Contoso
Greater Seattle Area

LinkedIn Member
Juriste junior chez Contoso
France

John Peter • 3rd
Senior Business Consultant at Contoso International
United Arab Emirates

Connect

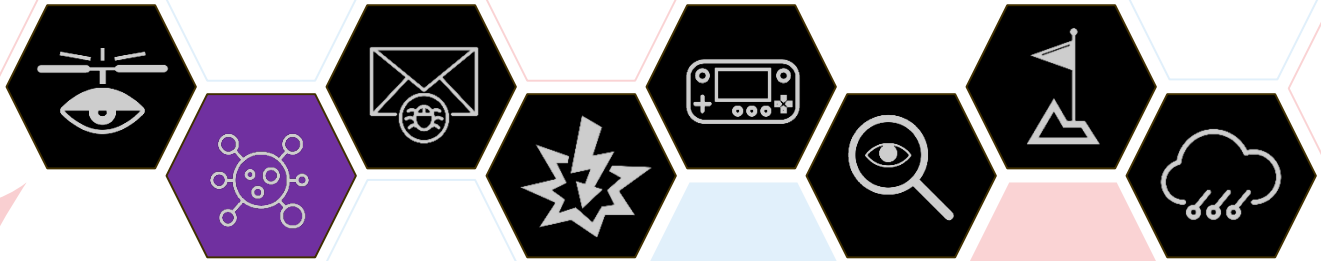
External Recon

- Documentation
  - Network map
    - ◊ Data flow
  - IP range
  - External access
  - Policies and procedures

Basic CIS Controls

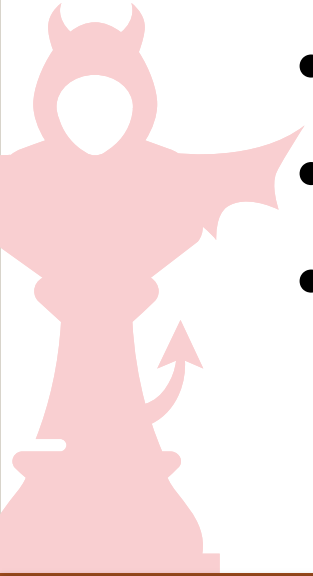
1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets

CyberKill Chain



Weaponization

- Exploit announcements
- Exploit research
- Creation of an exploit or attack vector
- Purchase an exploit
- **Abusing default configurations (Macros, HTAs, OVA, RAR)**



Weaponization

- Awareness of current threats
  - Vendor advisories
  - Security feeds (e.g. SANS, US-CERT, etc.)
- Mitigate Gaps
  - Tool tuning
- Ongoing training on new technology

AA20-245A: Technical Approaches to Uncovering and Remediating Malicious Activity

Inbox ×

US-CERT <US-CERT@ncas.us-cert.gov>
to me

Tue, Sep 1, 11:11 AM (2 days ago)

You are subscribed to National Cyber Awareness System Alerts for Cybersecurity and Infrastructure Security Agency. This information has recently been updated, and is now available.

AA20-245A: Technical Approaches to Uncovering and Remediating Malicious Activity

09/01/2020 08:30 AM EDT

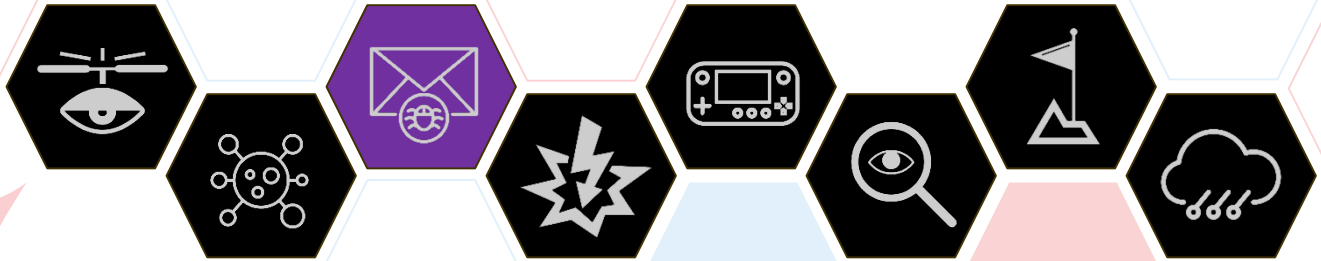
Original release date: September 1, 2020

Summary

This joint advisory is the result of a collaborative research effort by the cybersecurity authorities of five nations: Australia,[1] Canada,[2] New Zealand,[3][4] the United Kingdom,[5] and the United States.[6] It highlights technical approaches to uncovering malicious activity and includes mitigation steps according to best practices. The purpose of this report is to enhance incident response among partners and network administrators along with serving as a playbook for incident investigation.

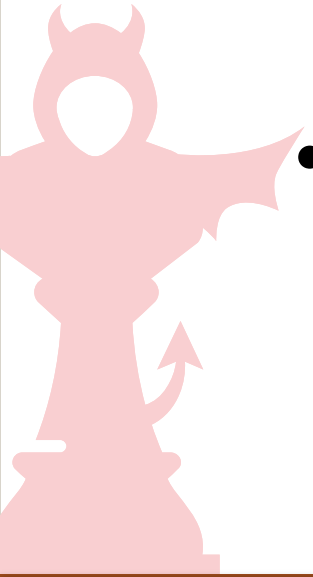
Delivery

CyberKill Chain

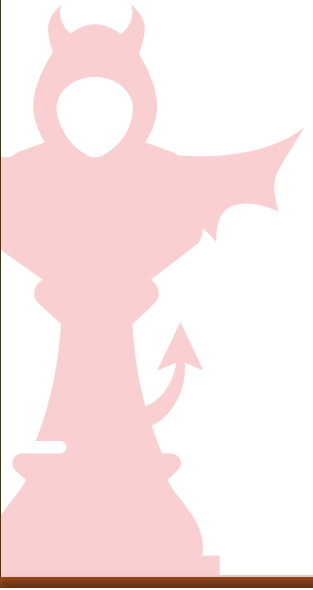


Delivery

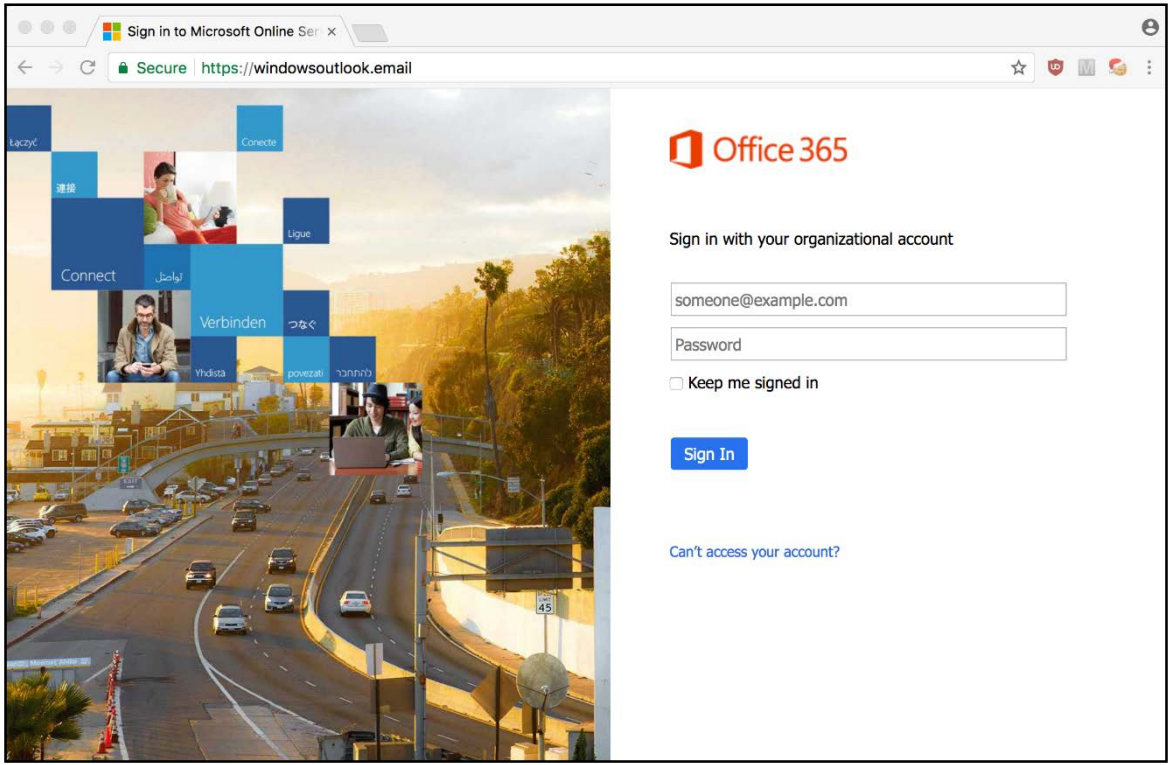
- Direct exploit of publicly available service
- Malicious hardware
  - ”Free” USB drive from vendors
- Social Engineering
  - Call spoofing
  - In-Person Visits (Printer Guy)
  - **Phishing**



[DEMO]



Phishing Website



Poor Email Filtering

Connected to mail.cogentco.com (38.9.X.X).

MAIL FROM: <hacker@contoso.com>

250 OK

RCPT TO: <david.anderson@claconnect.com>

250 Accepted

SMTP Envelope

DATA

354 Enter message, ending with "." on a line by itself

FROM: <ElonMusk@tesla.com>

TO: <david.anderson@claconnect.com>

Subject: Free Tesla Car

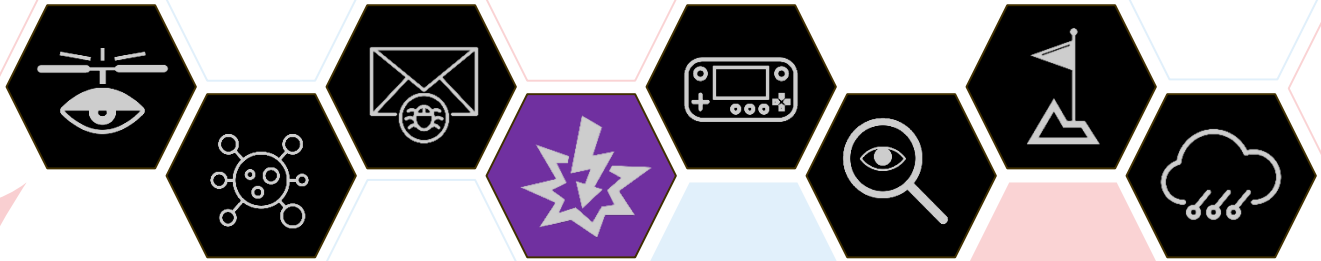
SMTP Message

Delivery

- Mail Security Controls
- Security Assessments of email system
  - Cloud - offsite
  - OWA - onsite
- Spam Filters
  - Flag external emails (e.g. banner)
  - Custom filter to block your domain in SMTP Message
- Awareness Training

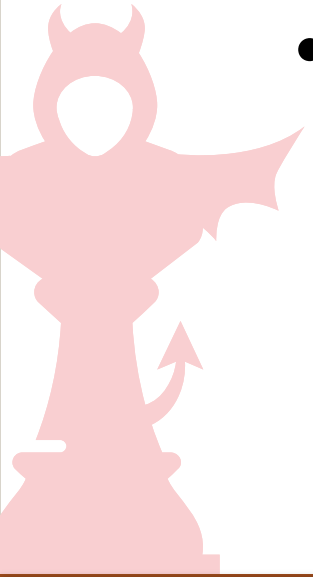
Exploitation

CyberKill Chain



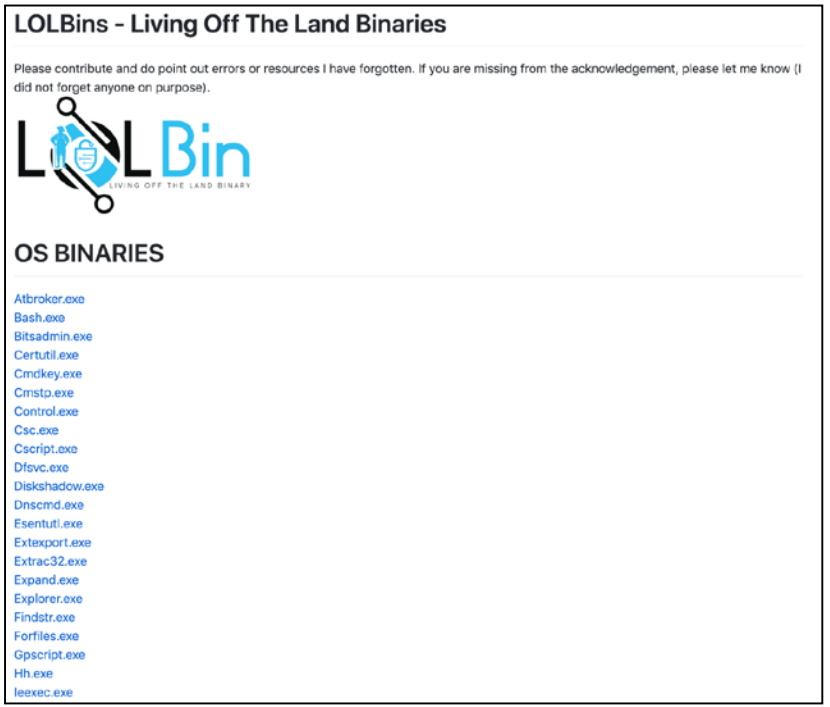
Exploitation

- Missing patches
  - MS17-010 (WannaCry / ETERNALBLUE)
- System Configuration
  - Malicious Office documents (Macros, OLE, etc.)
  - **HTML Applications (.HTA)**
  - PowerShell is often utilized to run/deliver the code



Living Off the Land Binaries (LOLBINS)

https://lolbas-project.github.io/



[DEMO]

Exploitation

- Application whitelisting
  - AppLocker
  - Windows Device Guard
- Protect Office Applications
  - Block Macros
  - Windows Defender Exploit Guard
- Log Management

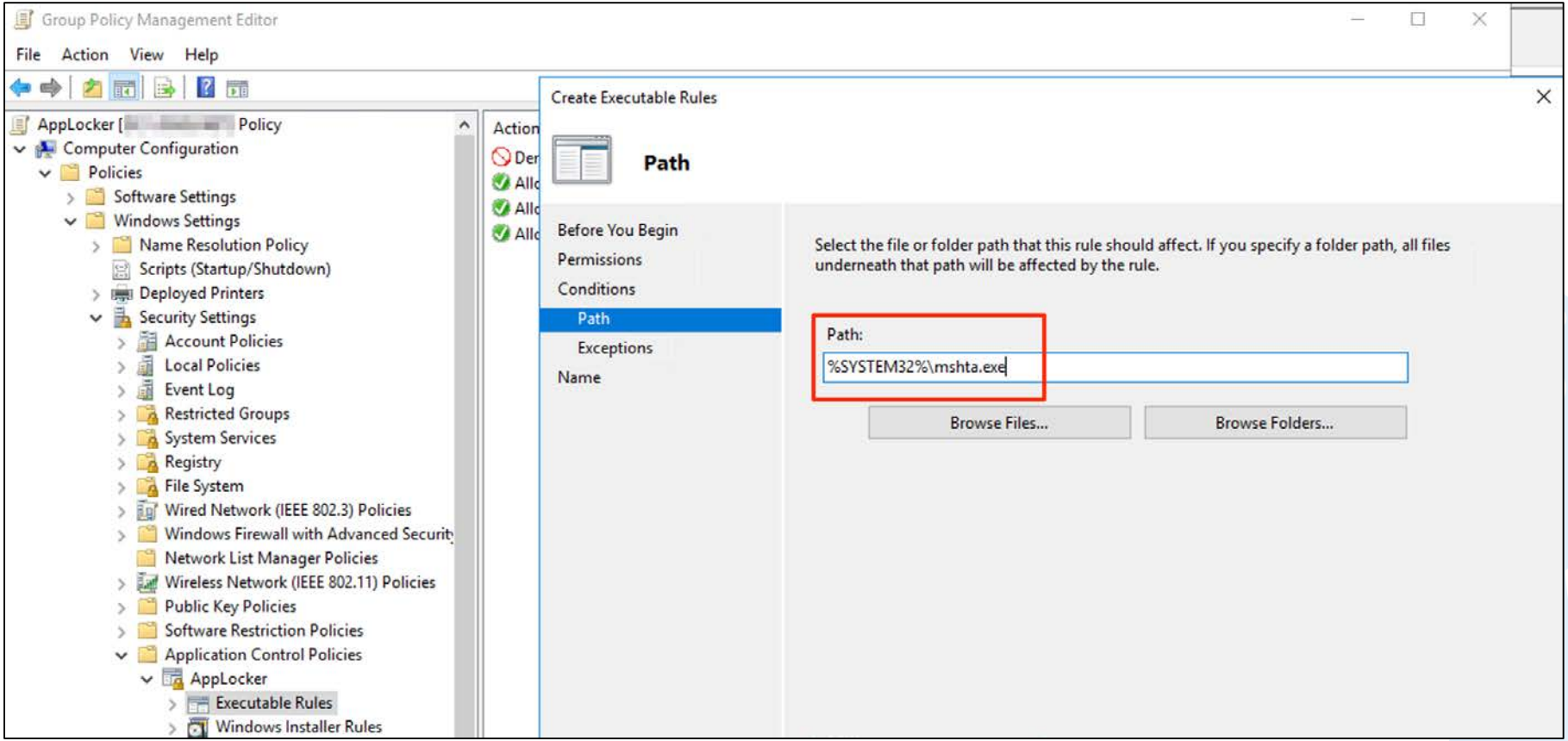
Exploitation

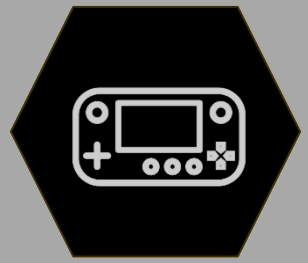
Security Baseline

- “Golden Image”
- Desired State Configuration
- GPO
  - ◊ User
  - ◊ machine
- Benchmarks
  - ◊ CIS
  - ◊ NIST
  - ◊ STIGS
  - ◊ USGCB

Exploitation

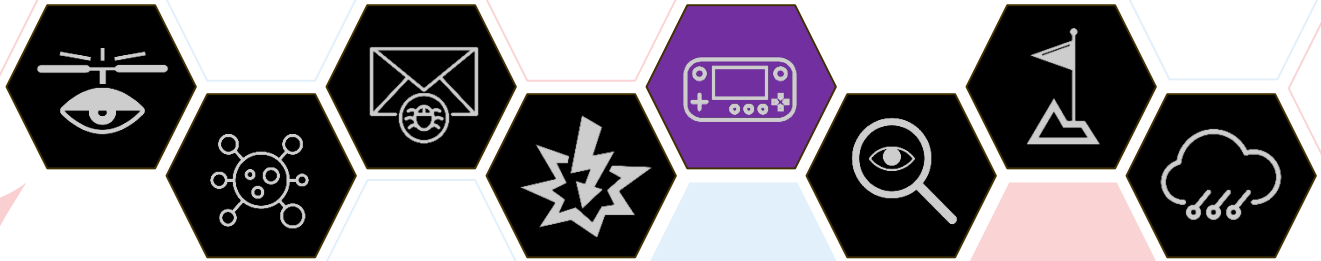
- Tools
  - Group Policy / Desired State Configuration
  - SysInternals suite
  - LAPS
  - Sysmon
- Patch management
  - Evaluation
  - Testing
  - ASAP





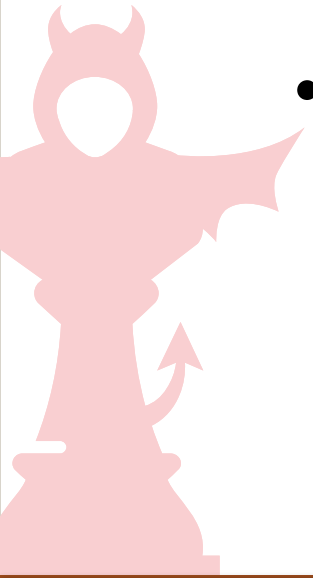
Command and Control

CyberKill Chain

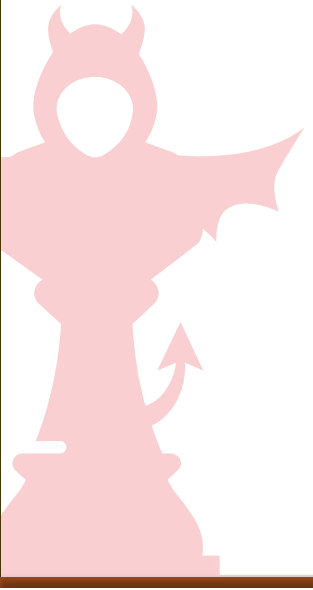


Command and Control

- Remote access tool
  - Stabilize connection
  - Allows attacker to run commands and custom binaries
- Communication
  - Encrypted
  - Mimic “real” network traffic
    - HTTPS / DNS

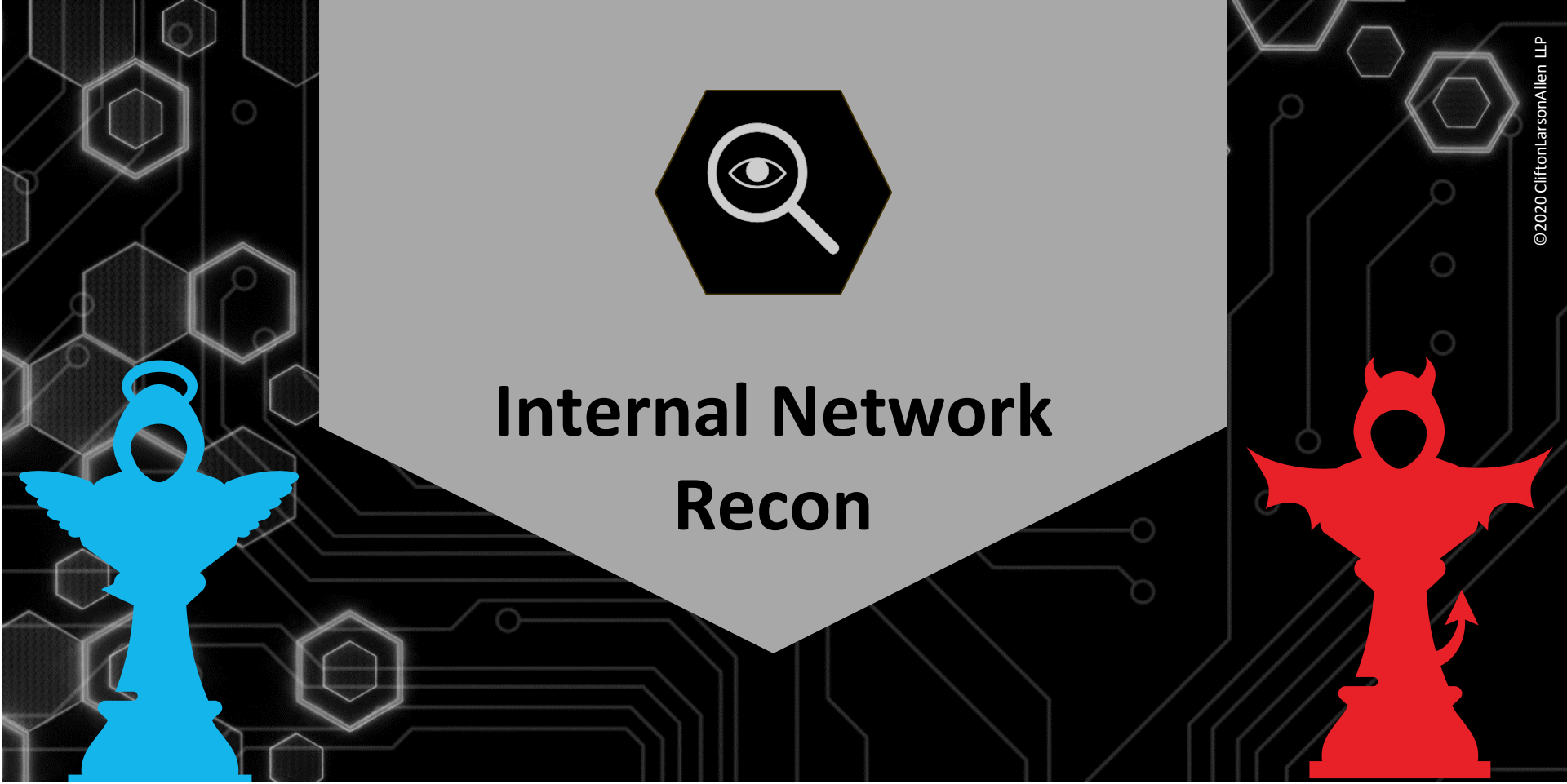


[DEMO]

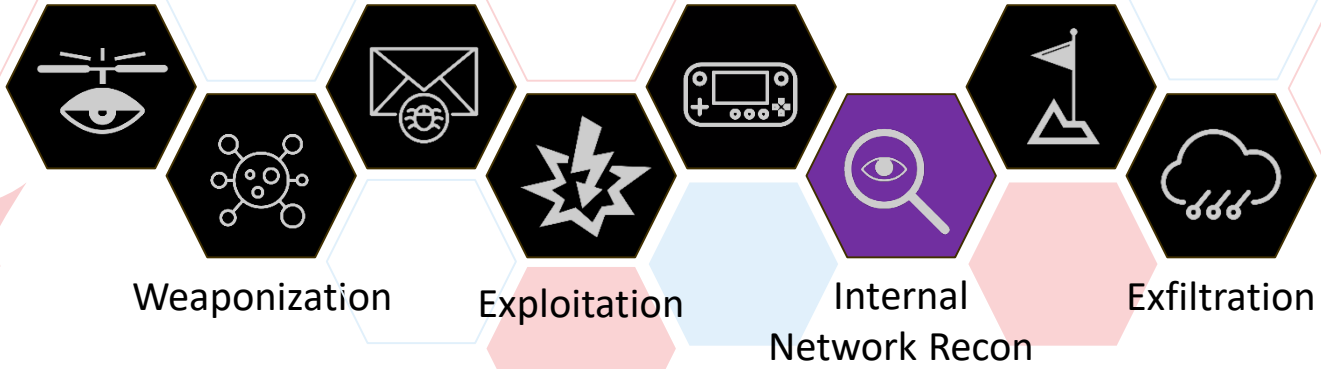


Command and Control

- Strict egress filtering
  - Inspect HTTPS traffic (via web proxy or firewall)
  - Geo-blocking
- Indicators of Compromise
  - DNS logs
  - Review ’autoruns’
  - Registry changes
  - New files/services/schedules tasks
  - ….APPDATA…

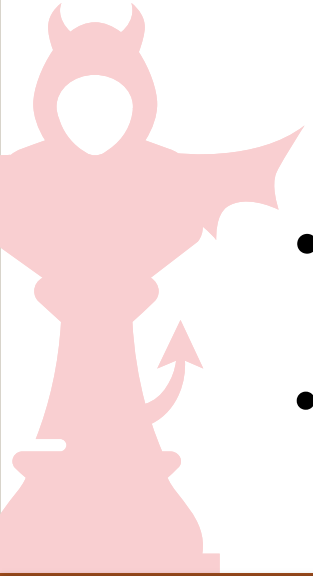


CyberKill Chain

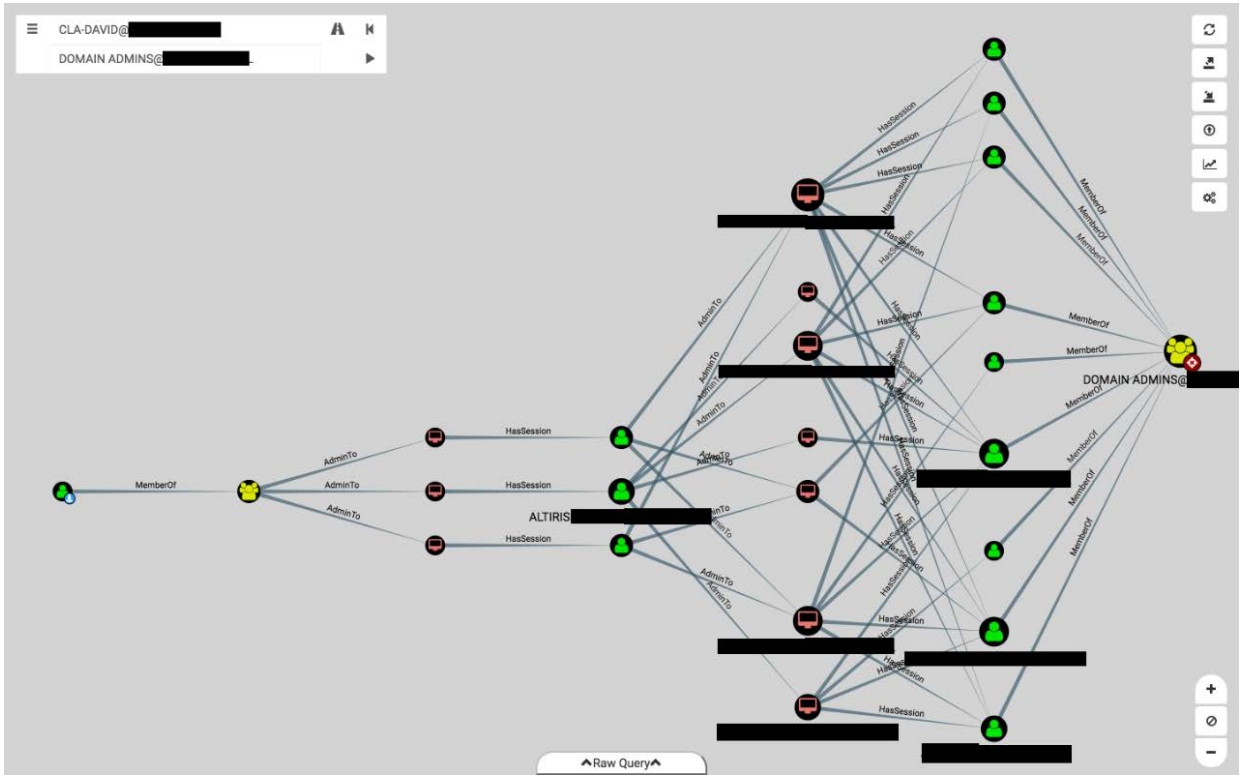


Internal Network Recon

- Who is on the network?
  - netstat
  - Port scans
  - DNS enumeration
  - AD enumeration
- Who are the administrators?
  - BloodHound
- PowerShell, again, is heavily utilized
  - ”Live off the land”



BloodHound

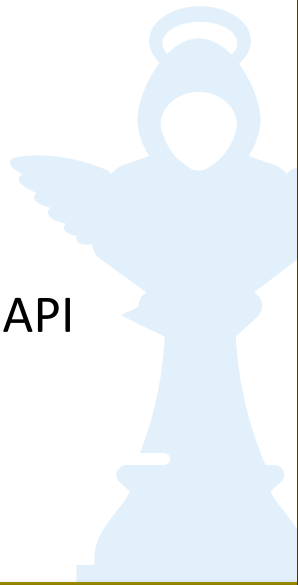


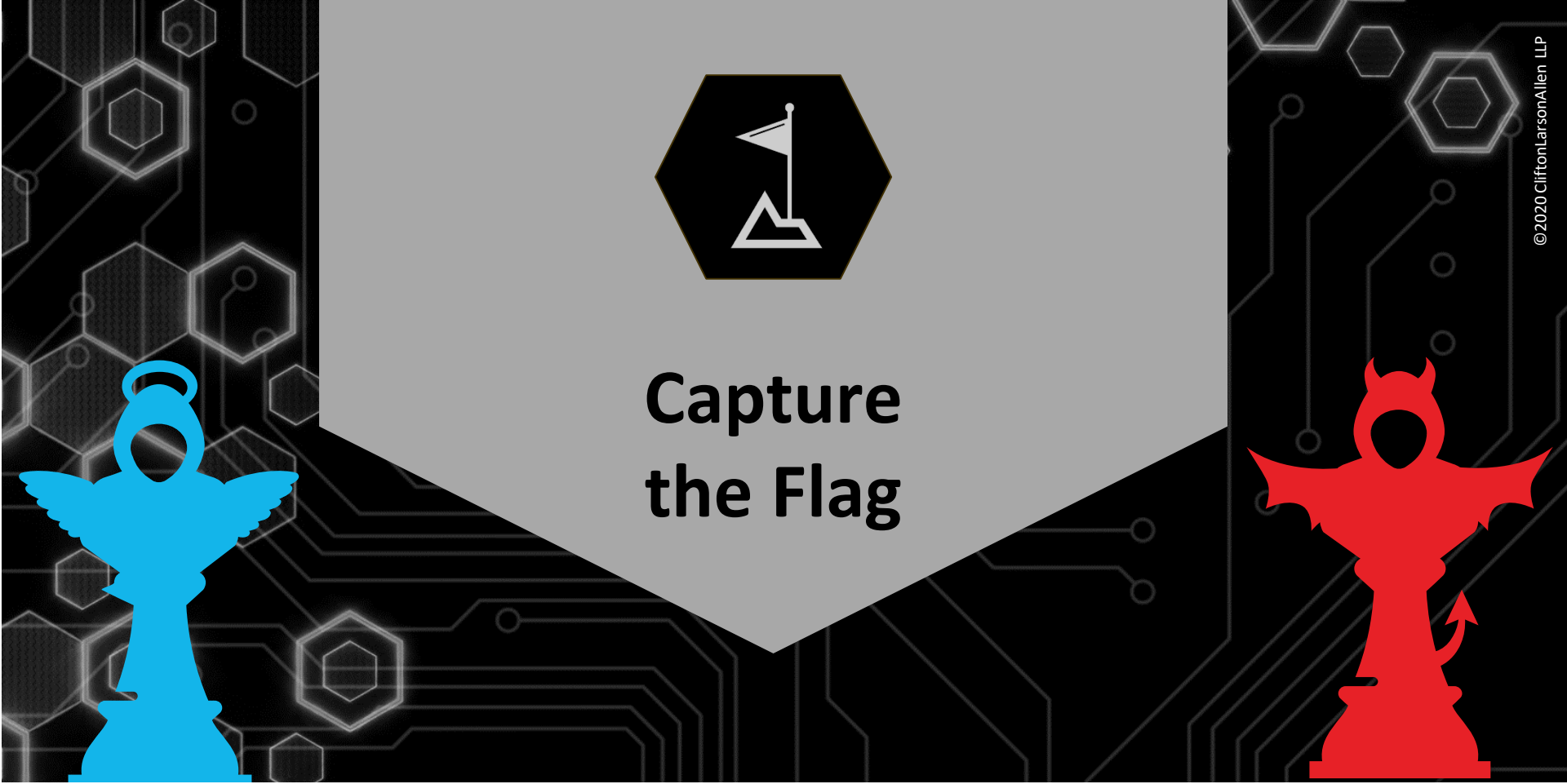
Internal Network Recon

- Secure Network
  - Network Segmentation
- Network Monitoring
  - Netflow
  - Endpoint logs
  - “user” behavior
  - Sensor alerts
  - Log analysis

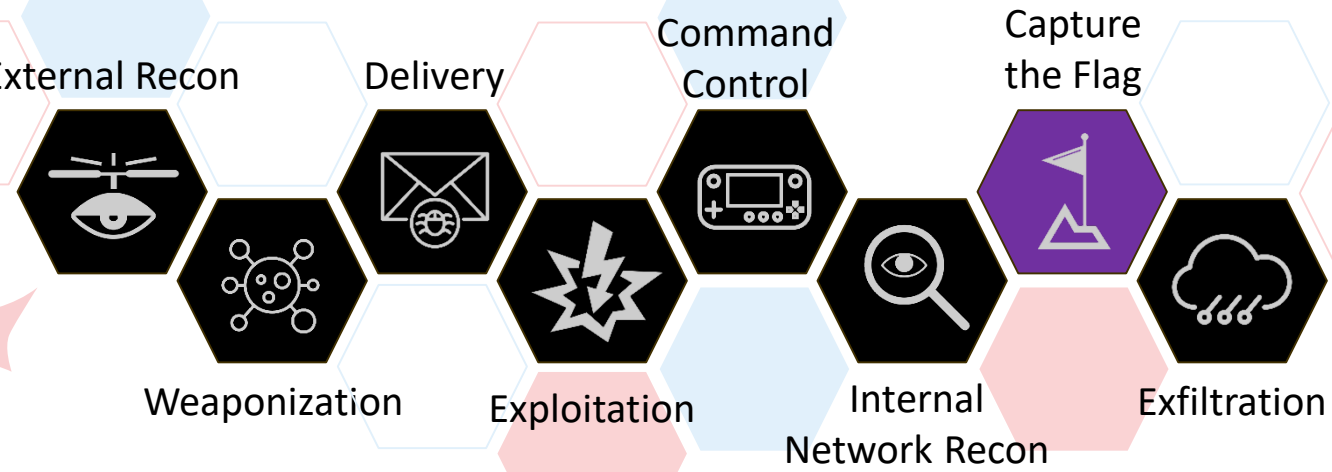
PowerShell Security

- Upgrade to PowerShell v5
- Remove PowerShell v2 (if old .NET is installed)
- Enable Script Block Logging
- Enable Script Transcription
- OPTIONAL: Configure Constrained Language Mode
  - Prevents advanced features, such as .NET execution, Windows API calls, and COM access
  - This may cause issues with managing systems with PowerShell





CyberKill Chain



Capture the Flag

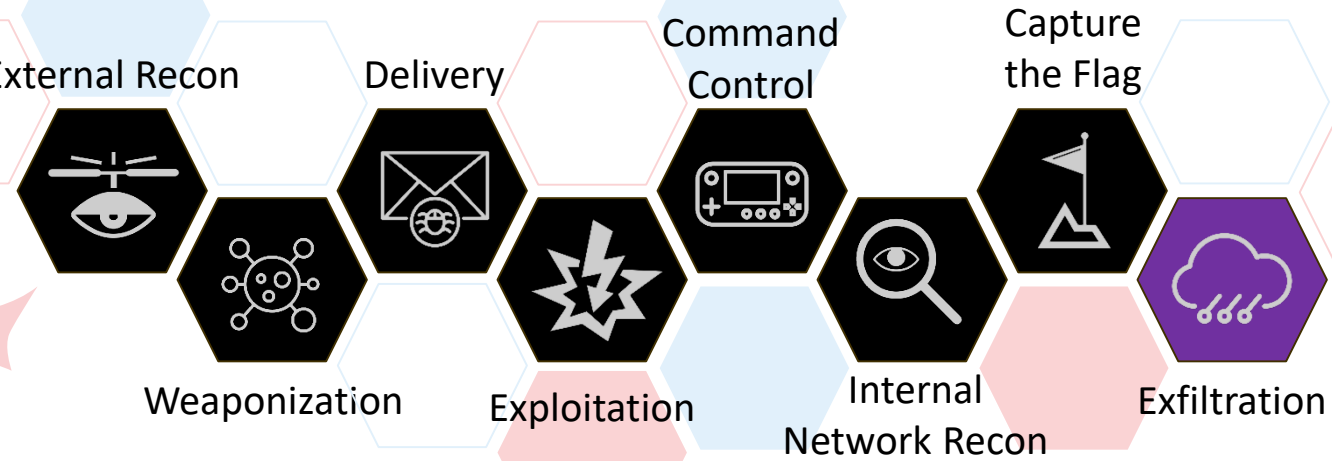
- Privileged Accounts
  - Based on OSINT
  - IT / Finance / Execs
- Asset Identification
  - Data of interest
- Asset Acquisition
  - Gaining access to data

Capture the Flag

- Network Map
  - “Treasure map”
- Encryption
  - “at rest” encryption
- Logging
  - PowerShell
  - File access
  - User behavior analytics

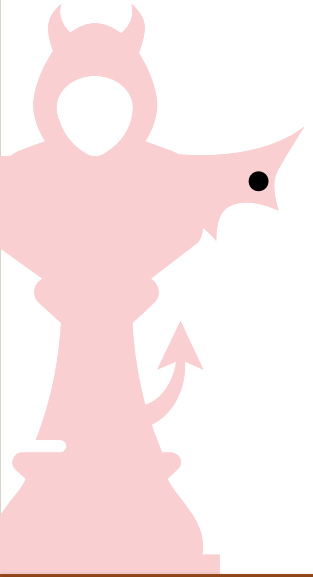
Exfiltration

CyberKill Chain



Exfiltration

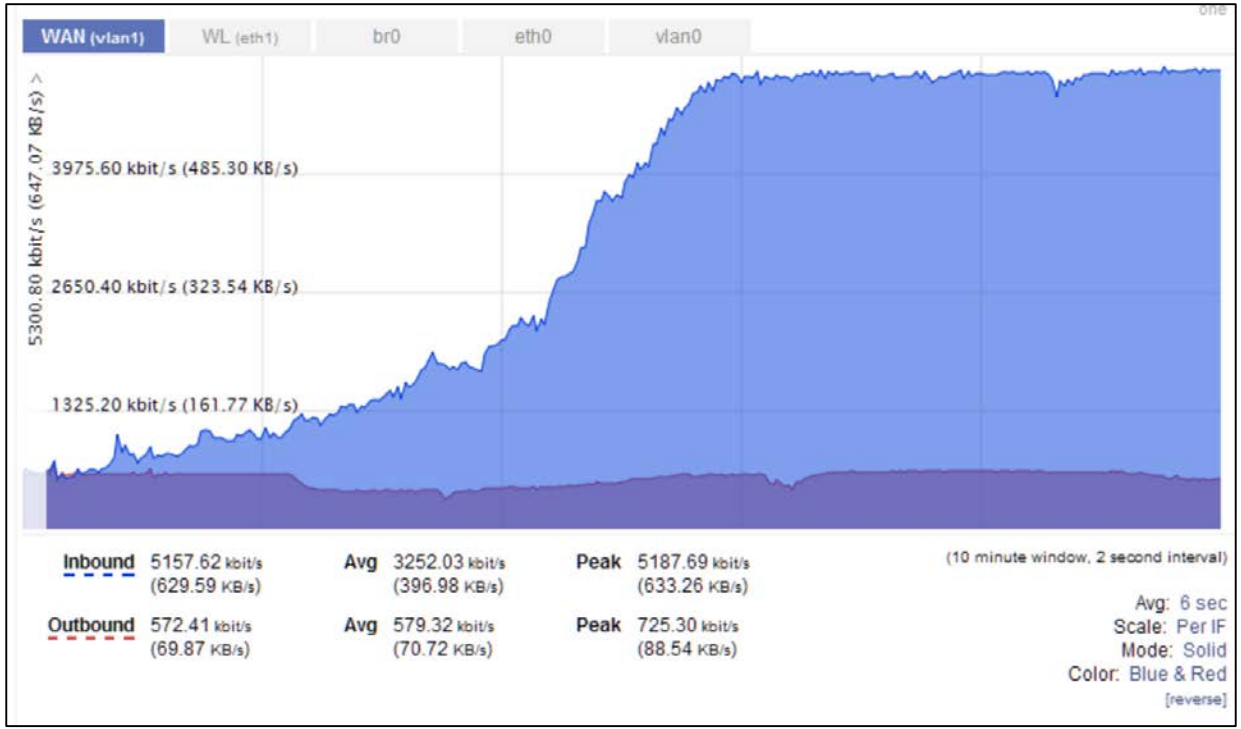
- Collection point
- Package it up
  - Compress
  - Encrypt
- Send it out
  - What is allowed to egress your network?
  - FTP, SSH, HTTP(S), ICMP, etc…



Exfiltration

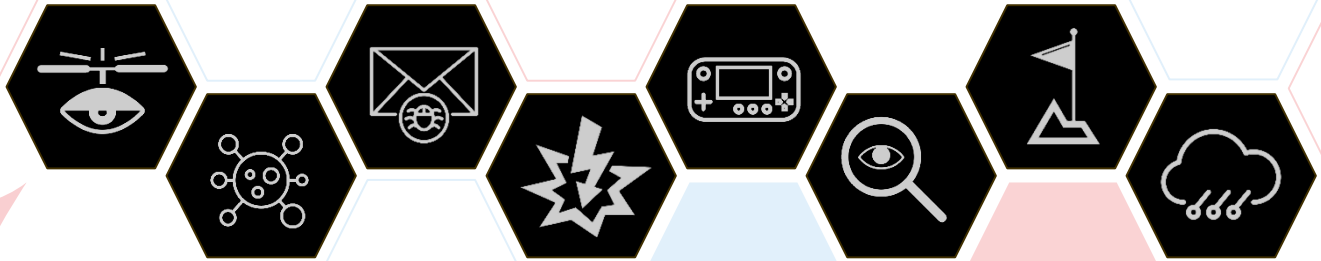
- Network Monitoring
  - Bandwidth
  - SSL/TLS inspection
  - Understand what is normal
- Firewall Rules
  - Strict egress firewall rules
  - Geo-blocking

Bandwidth logs



Summary

Summary



Thank you!

Forrest Kasler
704-998-5297
forrest.kasler@claconnect.com

David Anderson
612-376-4699
david.anderson@claconnect.com