Understanding the Attacker You Know

- A walk through of a malicious employee threat scenario and the lessons it can teach

Brian Read
Security Practice Manager
Conexsys Communications Ltd.
Who is Conexsys Communications?

- Security service provider and integrator

- 55 years in the Canadian IT Market

- Trusted advisor to many large customers in the financial, oil and gas and government sectors.
Technology Integration Services

- Design, Installation, Configuration
- Support, Training
- Specialize in multi-vendor environments
Conexsys: Our Partners

Check Point
We Secure the Internet

A10 Networks

ForeScout

CYBERArk
Platinum Partner

SOURCEfire

The Security Division of EMC

Damballa

nitrosecurity

Cisco Systems

FIRE MON

NetOptics

McAfee
An Intel Company

ForeScout

Lumension
SECURITY

NetScout

Oracle

Websense
ESSENTIAL INFORMATION PROTECTION

FireEye
• Controls Design and Strategy
• Vulnerability Assessments
• Penetration Tests
• New Technology Evaluation
Who am I?

• Security Practice Manager at Conexsys Communications Ltd.
• SME for PIDM, Vulnerability Management Solutions
• Advise clients on controls design and other strategic security projects
• Lead the VA and PenTest team
Today’s Goals

• Walk thru a malicious employee case study
• Outline the lessons you can learn from the scenario
• Takeaways:
  – 3 publicly available scripts that you can use to simulate an insider threat
  – 1 free tool that can find hundreds of holes in your AD deployment

The single best control for measuring the threat from malicious employees
The Malicious Employee Threat

- Employee with a corporate system on the inside network
- Restricted access to their system
- Restricted access to organizational resources
- Not a skilled hacker
The Malicious Employee Threat

- Employee with a restricted user account
- Not compiling custom malware
- Not developing Zero-Days
- No expensive testing tools
- Not a professional hacker
The Malicious Employee

• Employee with a restricted user account
• An organizational system on the network
• Restricted access to resources
• Not a skilled hacker
• Doesn’t want to compromise their employment or go to jail
The Malicious Employee

- Employee with a restricted user account
- No phishing
- No rogue WiFi access points
- No USB in coworkers system
- Minimize traceable changes

Not a professional hacker

- Doesn’t want to compromise their employment or go to jail
The Malicious Employee

- Employee with a restricted user account
- An organizational system on the network
- Restricted access to resources
- Not a skilled hacker
- Doesn’t want to compromise their employment or go to jail
Outsider Threat Kill Chain

1. Recon
2. Weaponization
3. Exploitation
4. Command and Control
5. Maintain Persistence
6. Escalate Privileges Locally
7. Steal Other Credentials
8. Move Laterally
9. Accomplish Goal

Note: The process is cyclical, with each step leading back to Recon.
Insider Threat Kill Chain

- Recon
- Delivery
- Exploitation
- Command and Control
- Maintain Persistence
- Escalate Privileges Locally
- Steal Other Credentials
- Move Laterally
- Accomplish Goal
Insider Threat Kill Chain

- Recon
- Weaponization
- Exploitation
- Command and Control
- Maintain Persistence
- Escalate Privileges Locally
- Steal Other Credentials
- Move Laterally
- Accomplish Goal

SECTOR
CELEBRATING 10 YEARS

CONEXSYS
COMMUNICATIONS LIMITED
How to Hack From Your Workstation

• Trend towards using functionality built into windows
• Net commands, Batch Files
• Sysinternal or other support tools
• VB Script, JavaScript
• CScript, Windows Scripting Host
• Windows Subsystem for Linux
• Access to all aspects of windows functionality
• Bypass AV: No requirement to save files to disk
PowerShell – Tough to Restrict

• Can’t remove – built into windows
• Tough to restrict – usually needs to be whitelisted
• Lots of techniques for breaking current containment controls and running scripts
PowerShell – Premade Attack Tools

• Many standalone scripts to choose from
• One repository collectively known as PowerSploit
• Started by Matt Graeber with help from many other contributors.
  – https://github.com/PowerShellMafia/PowerSploit/graphs/contributors
Escalating Local Privileges

- Escalate Privileges Locally
- Steal Other Credentials
- Move Laterally
- Accomplish Goal
• Use group policy to push down local settings including administrator or other local account passwords

• Promotes sharing passwords across multiple systems, insecure storage of passwords

• Phased out in May 2013 (but legacy passwords remain)
Exploiting– Group Policy Preferences

- PowerSploit: Get-GPPPassword
- Can be run by any domain user
- Just need a powershell prompt
- Decrypts and exposes passwords
Exploiting – Group Policy Preferences
• Services with misconfigured ACL’s or lax permissions
• Scheduled tasks running with admin\system rights
• Registry keys with lax permissions
Gaining Local Admin – Other Techniques

[*] Checking service permissions...

ServiceName: AdobeARMservice
Path: "C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe"
StartTime: LocalSystem
AbuseFunction: Invoke-ServiceAbuse -ServiceName 'AdobeARMservice'

ServiceName: AdobeFlashPlayerUpdateSvc
Path: C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe
StartTime: LocalSystem
AbuseFunction: Invoke-ServiceAbuse -ServiceName 'AdobeFlashPlayerUpdateSvc'

ServiceName: AeLookupSvc
Path: C:\Windows\system32\svchost.exe -k netsvcs
StartTime: LocalSystem
AbuseFunction: Invoke-ServiceAbuse -ServiceName 'AeLookupSvc'

ServiceName: ALG
Path: C:\Windows\System32\alg.exe
StartTime: NT AUTHORITY\LocalService
AbuseFunction: Invoke-ServiceAbuse -ServiceName 'ALG'

ServiceName: AppIDSvc
Path: C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation
StartTime: NT AUTHORITY\LocalService
AbuseFunction: Invoke-ServiceAbuse -ServiceName 'AppIDSvc'

ServiceName: Appinfo
Path: C:\Windows\system32\svchost.exe -k netsvcs
StartTime: LocalSystem
AbuseFunction: Invoke-ServiceAbuse -ServiceName 'Appinfo'

ServiceName: Apple Mobile Device Service
Path: "C:\Program Files\Common Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe"
StartTime: LocalSystem
AbuseFunction: Invoke-ServiceAbuse -ServiceName 'Apple Mobile Device Service'
Invoke-AllChecks Results

- Create secondary admin account
- Reset local admin password
Gain Other Credentials

- Escalate Privileges Locally
- Gain Other Credentials
- Move Laterally
- Accomplish Goal
Collect Local and AD Credentials
- Mimikatz

  - Can find unencrypted creds
  - Can find hashes from previous cached logins
- Powersploit: Invoke-Mimikatz
Accessing Other Credentials – Invoke-Mimikatz

```
minikatz 2.0 alpha (x64) release "Kiwi en C" (Dec 14 2015 19:16:34)

Benjamin DEPLY 'gentilkiwi' (benjamin@gentilkiwi.com)
http://blog.gentilkiwi.com/minikatz
with 17 modules ** **/

minikatz(powershell) # sekurlsa::logonpasswords

Authentication Id:    0 : 5067773 (00000000:004d53fd)
User Name:           Administrator
Domain:              WIN-IF4N4IKUC6C
Logon Server:        WIN-IF4N4IKUC6C
Logon Time:          6/29/2016 10:01:24 AM
SID:                 S-1-5-21-940593217-2901869181-200383700-500

Authentication Id:    0 : 144493 (00000000:0002346d)
Session:             Service from 0
User Name:           PasswordVault\_webAccessPool
Domain:              IIS_APPPOOL

* Username: Administrator
  * Domain: WIN-IF4N4IKUC6C
  * Password: Password123

* Username: Administrator
  * Domain: WIN-IF4N4IKUC6C
  * Password: Password123

* Username: Administrator
  * Domain: WIN-IF4N4IKUC6C
  * Password: Password123
```

Use Accounts to Access Other Systems

- Escalate Privileges Locally
- Gain Other Credentials
- Move Laterally
- Accomplish Goal
Lateral Movement – PowerShell Remoting

Use PSRemoting or enable it if it is not currently running then…

• PowerSploit Invoke-Mimikatz to view their passwords
• PowerSploit Get-Keystrokes to capture their keystrokes
• PowerSploit Get-TimedScreenshots to capture their screen shots
Lessons Learned From the Walk Thru

- Escalate Privileges Locally
- Steal Other Credentials
- Move Laterally

Accomplish Goal
Lesson 1 - Review Key Controls For Focus on the Insider

- For example:
  1. Windows Hardening and End Point Controls
  2. Privileged Identity Management
  3. NAC and Network Segmentation
  4. Alert on Suspicious Activity

...
Lesson 2 - Review Windows Hardening Details

Does our current combination of endpoint controls and windows hardening prevent local escalation?

– Group Policy Preferences reveal passwords
– Poorly configured services allow escalation
– Settings securing credentials stored in memory
What is our plan for mitigating the risks while still allowing for necessary PowerShell functionality?

- PowerShell v5
- Constrained Language Mode
- PowerShell Module Logging
- 100% whitelisting of scripts
Lesson 3 – Lateral Movement is Made Much Easier by Poor PIDM

How does our organization enforce:

• Unique local administrator passwords
• Restricting admin rights for IT Admins
• Removing unnecessary accounts

• Detecting with real time alerting
• Validating with a Periodic scan
Lesson 3 – Lateral Movement is Made Much Easier by Poor PIDM

Do you mandate:

- Unique local administrator passwords
- Restricting admin rights for IT Admins
- Removing unnecessary accounts
- Detecting with real-time alerting
- Validating with periodic scans

Lesson 3 – Lateral Movement is Made Much Easier by Poor PIDM

Do you mandate:

- Unique local administrator passwords
- Restricting admin rights for IT Admins
- Removing unnecessary accounts
- Detecting with real-time alerting
- Validating with periodic scans

![Image of CyberArk DNA™ Executive Summary Dashboard](image)

- Machines Scanned:
  - Windows: 13
  - Unix: 0
  - Total machines scanned: 13

- Accounts Discovered:
  - Non-privileged: 88
  - Privileged: 80

- Total non-compliant:
  - Windows: 25
  - Non-privileged: 25

- Least privilege risk - Windows business users:
  - Workstations: 0%
  - Servers: 55%

- Embedded/hard-coded credentials discovery:
  - Employee: 5%
  - Executive/VP: 20%
Cant We Just Use an “Insider Threat” Checklist or Something?

• Develop your own checklist…
The Internal PenTest

• Focus the PenTest on a malicious employee scenario
• Tip1: Clean up the low hanging fruit (like some of the items in this presentation)
• Should definitely receive technical recommendations on system level exploits

• Tip 2: Demand high level recommendations on:
  – containment
  – data exfiltration
Thank You

- Follow Conexsys on Twitter: @conexsyscomm

- For any pdf of this presentation or any technical questions come by the Conexsys booth or contact me at brianr@conexsys.net

- Drop off a card at the booth and win a GoPro