The Current State of Security an Improv-pection

Sean Metcalf
Nick Carr
Why are we here?

• Click to add text
Whose Plan Is It Anyway?

• Introductions
• Agenda
• Invoke-Improv (lather, rinse, repeat)
• Best Defenses

Sean Metcalf (@Pyrotek3) & Nick Carr (@ItsReallyNick)
About: Sean Metcalf  @PyroTek3

• Active Directory Security guy & one-time EvilCorp CIO impersonator
• Founder Trimarc, a security company.
• Microsoft Certified Master (MCM) Directory Services
• Microsoft MVP (2016)
• Speaker: Black Hat, BSides, DEF CON, DerbyCon, Shakacon, Sp4rkCon
• Own & Operate ADSecurity.org (Microsoft platform security info)
About: Sean Metcalf @PyroTek3

- Active Directory Security guy & one-time EvilCorp CIO impersonator
- Founder Trimarc, a security company.
- Microsoft Certified Master (MCM) Directory Services
- **Microsoft MVP (2016)**
- Speaker: Black Hat, BSides, DEF CON, DerbyCon, Shakacon, Sp4rkCon
- Own & Operate ADSecurity.org
  (Microsoft platform security info)
About: Nick Carr  @ItsReallyNick

• Mandiant investigator & FireEye Advanced Practices Team
• Crisis manager, friend of lawyers
• Speaker: DerbyCon, Shmoocon, Blue Hat
• Noted spook & a very nasty piece of work
• On the periphery of fascinating
Agenda

Today's agenda:
1) Be stylin' and profilin' ✓
2) Lunch
3) Go home
Ready... go!
Wait – we don’t know anything about improv.

...yes, and?
Get-AuthenticodeSignature -FilePath C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ISE\ise.ps1

Directory: C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ISE

<table>
<thead>
<tr>
<th>SignerCertificate</th>
<th>Status</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>93859EBF98AFDEB488CCFA263899640E81BC49F1</td>
<td>Valid</td>
<td>ise.ps1</td>
</tr>
</tbody>
</table>

Get-AuthenticodeSignature -FilePath .\HelloSignedWorld.ps1

Directory: C:\Test

<table>
<thead>
<tr>
<th>SignerCertificate</th>
<th>Status</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>93859EBF98AFDEB488CCFA263899640E81BC49F1</td>
<td>Valid</td>
<td>HelloSignedWorld.ps1</td>
</tr>
</tbody>
</table>
Things We Need

1. Your help!
Things We Need

1. Your help!
2. All of your ideas.
Things We Need

1. Your help!
2. All of your ideas.

Sean Metcalfe (@Pyrotek3) & Nick Carr (@ItsReallyNick)
Things We Need

1. Your help!
2. All of your ideas.
Things We Need

1. Your help!
2. All of your ideas.
Things We Need

1. Your help!
2. All of your ideas.
Part 1.

Arrival: Fly-Away Kit
and... SCENE.

Sean Metcalf (@Pyrotek3) & Nick Carr (@ItsReallyNick)
Part 2.
The Model CISO
and... SCENE.

Sean Metcalf (@Pyrotek3) & Nick Carr (@ItsReallyNick)
Part c: \nThe Out-brief
and...

SCENE.
Part 404: SLIDE NOT FOUND
The Pitch
and... SCENE.

Sean Metcalf (@Pyrotek3) & Nick Carr (@ItsReallyNick)
Let’s talk about how to avoid a Krebs article about your company

**07 Breach at Equifax May Impact 143M Americans**

Equifax, one of the “big-three” U.S. credit bureaus, said today a data breach at the company may have affected 143 million Americans, jeopardizing consumer Social Security numbers, birth dates, addresses and some driver’s license numbers.

In a press release today, Equifax [NYSE:EFX] said it discovered the “unauthorized access” on July 29, after which it hired an outside forensics firm to investigate. Equifax said the
Best Defenses

Sean Metcalf (@Pyrotek3) & Nick Carr (@ItsReallyNick)
Effective Mitigation: Initial Foothold

• Deploy PowerShell v5.1
• Enable PowerShell logging (v3+) & cmd process logging.
• Control Microsoft Office macros.
  • Block macros from internet files.
  • Only allow signed macros.
  • Use TrustedDocuments location when macro workflow is required.
• Deploy security tooling that monitors for suspicious behavior.

Sean Metcalf (@Pyrotek3) & Nick Carr (@ItsReallyNick)
Effective Mitigation: Protect Admin Creds

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

• Explicitly block privileged admin accounts from being used on lower tiered workstations, laptops, and servers.

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

• Enforce Restricted Admin RDP

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

Sean Metcalf (@Pyrotek3) & Nick Carr (@ItsReallyNick)
Effective Mitigation: Strengthen

- Audit/Restrict NTLM.
- Enforce LDAP signing.
- Disable WDigest authentication (kb2871997 + reg key change)
- Enable SMB signing (& encryption where poss.).
- Disable WPAD & LLMNR & work to disable NetBIOS.
- Work to remove SMBv1 from all systems (update storage systems for SMBv2 support, ex. NetApp).
- Windows 10, remove:
  - SMB 1.0/CIFS
  - Windows PowerShell 2.0
Non-Windows

• Patch Apache Struts.
Conclusion

• This was ___ and hopefully we talked about some interesting things.
• Maybe you learned something 😊
• Avoid FUD. Data matters!
• Improving security can be done: start small and build on success.

Nick Carr (@ItsReallyNick)
nick.carr [@] mandiant.com
fireeye.com

Sean Metcalf (@Pyrotek3)
sean [@] TrimarcSecurity.com
www.ADSecurity.org
TrimarcSecurity.com

Slides: Presentations.ADSecurity.org