# The Current State of Security an Improv-spection

Sean Metcalf

Nick Carr

DERBYCON
VII
LEGACY
LOUISVILLE 2017 KENTUCKY

# Why are we here?

- Click to add text

# Whose Plan Is It Anyway?

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

# About: Sean Metcalf @PyroTek3

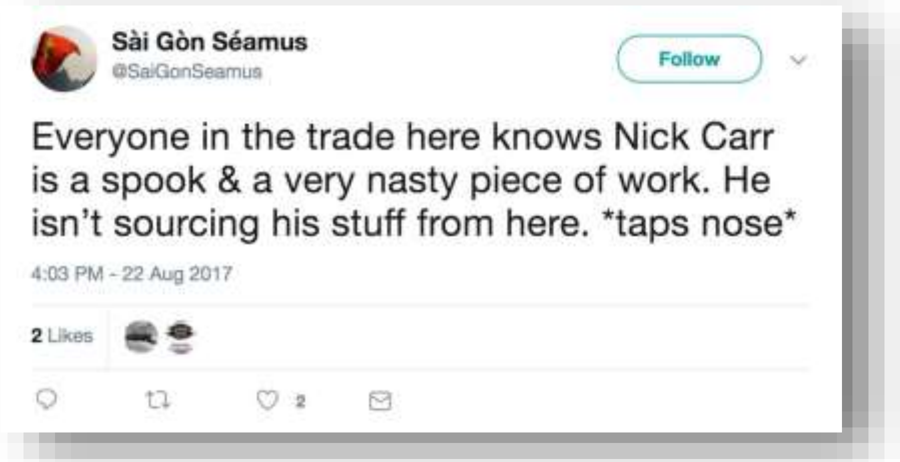
- Active Directory Security guy & one-time EvilCorp CIO impersonator
- Founder Trimarc, a security company.
- Microsoft Certified Master (MCM) Directory Services
- Microsoft MVP (2016)
- Speaker: Black Hat, BSides, DEF CON, DerbyCon, Shakacon, Sp4rkCon
- Own & Operate ADSecurity.org
  (Microsoft platform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



Sài Gòn Séamus
@SaiGonSeamus

Everyone in the trade here knows Nick Carr is a spook & a very nasty piece of work. He isn't sourcing his stuff from here. *taps nose*

4:03 PM - 22 Aug 2017

2 Likes

# Agenda

Todays agenda:

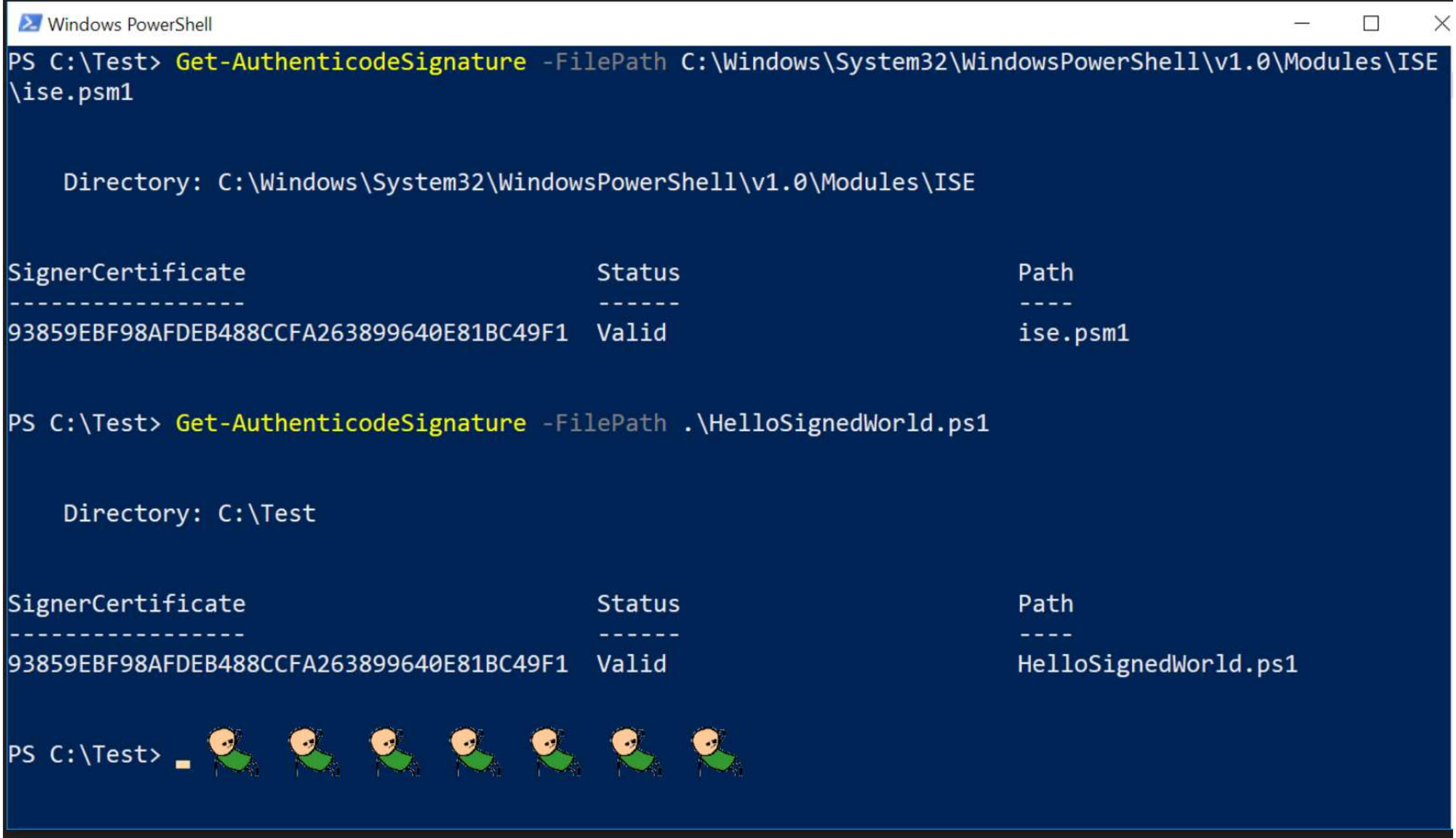
1) Be stylin' and profilin' ✅
2) Lunch
3) Go home

# Ready… go!

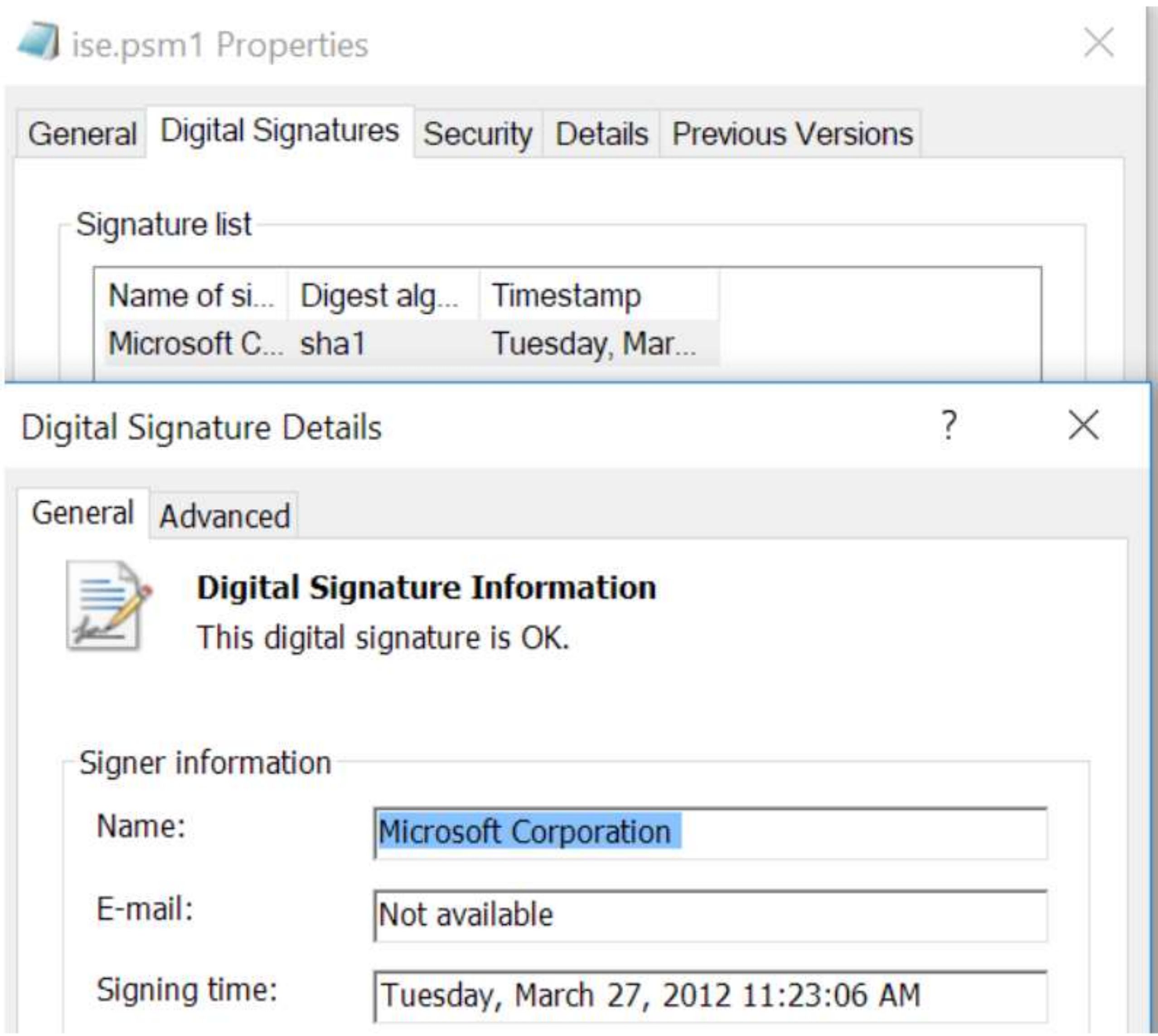
WARNING
MAY BE PRONE TO
SHENANIGANS,
HOOLIGANISM
AND
MALARKEY

# Wait – we don't know anything about improv.

…yes, and?



```
PS C:\Test> Get-AuthenticodeSignature -FilePath C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ISE
\ise.psm1


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


SignerCertificate                         Status                                 Path
-----------------                         ------                                 ----
93859EBF98AFDEB488CCFA263899640E81BC49F1  Valid                                  ise.psm1


PS C:\Test> Get-AuthenticodeSignature -FilePath .\HelloSignedWorld.ps1


    Directory: C:\Test


SignerCertificate                         Status                                 Path
-----------------                         ------                                 ----
93859EBF98AFDEB488CCFA263899640E81BC49F1  Valid                                  HelloSignedWorld.ps1


PS C:\Test> _
```



Signature list

| Name of si... | Digest alg... | Timestamp |
|---|---|---|
| Microsoft C... | sha1 | Tuesday, Mar... |

**Digital Signature Information**

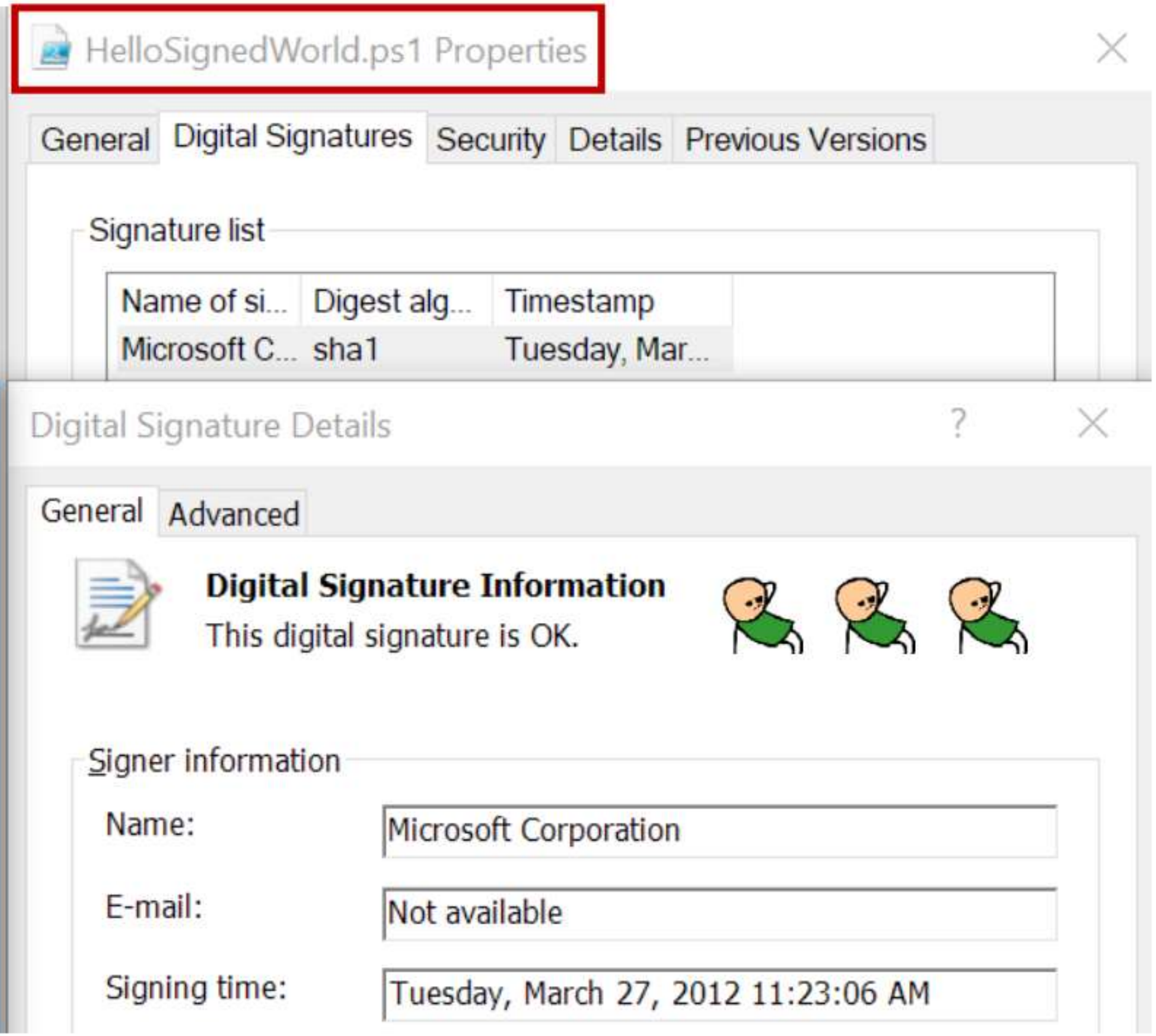
This digital signature is OK.

Signer information

Name: Microsoft Corporation

E-mail: Not available

Signing time: Tuesday, March 27, 2012 11:23:06 AM



Signature list

| Name of si... | Digest alg... | Timestamp |
|---|---|---|
| Microsoft C... | sha1 | Tuesday, Mar... |

**Digital Signature Information**

This digital signature is OK.

Signer information

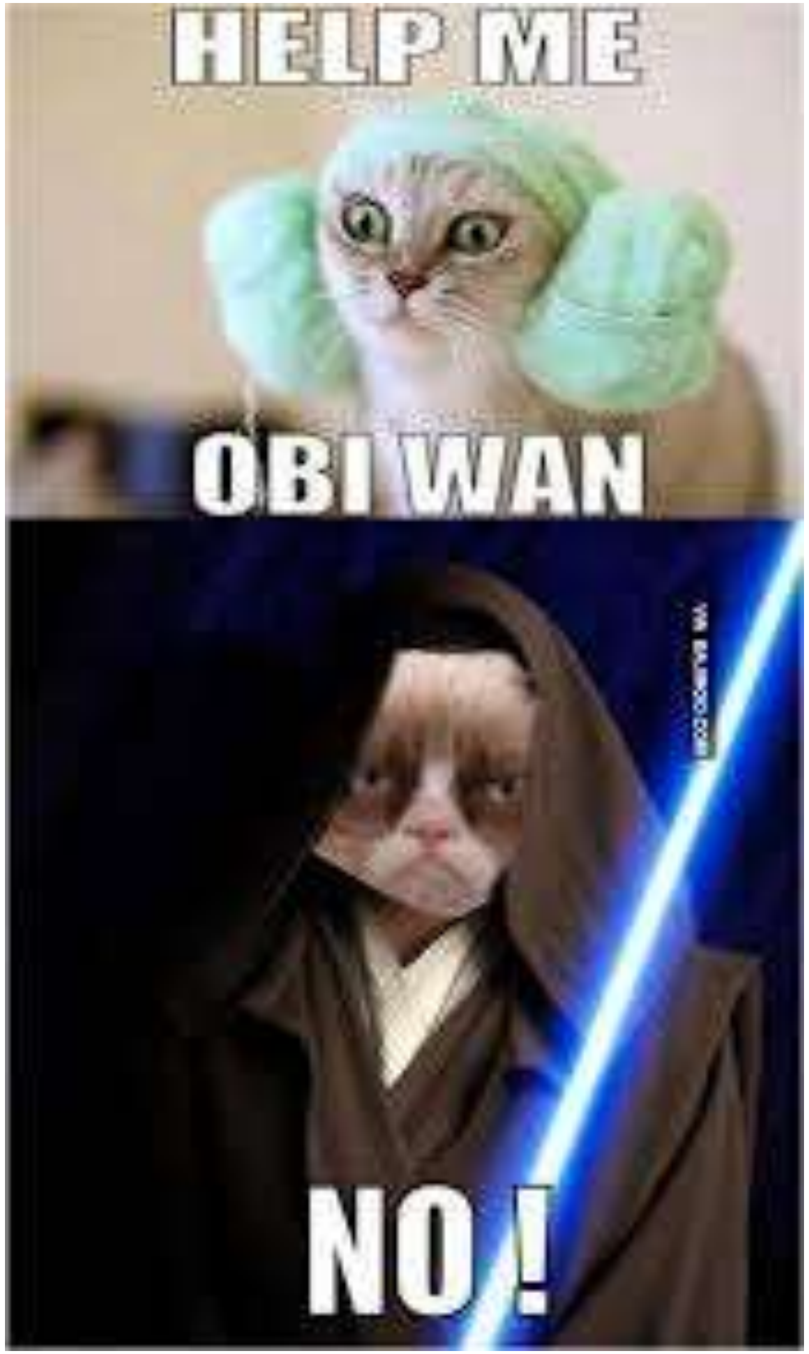
Name: Microsoft Corporation

E-mail: Not available

Signing time: Tuesday, March 27, 2012 11:23:06 AM

# Things We Need

1. Your help!



# Things We Need

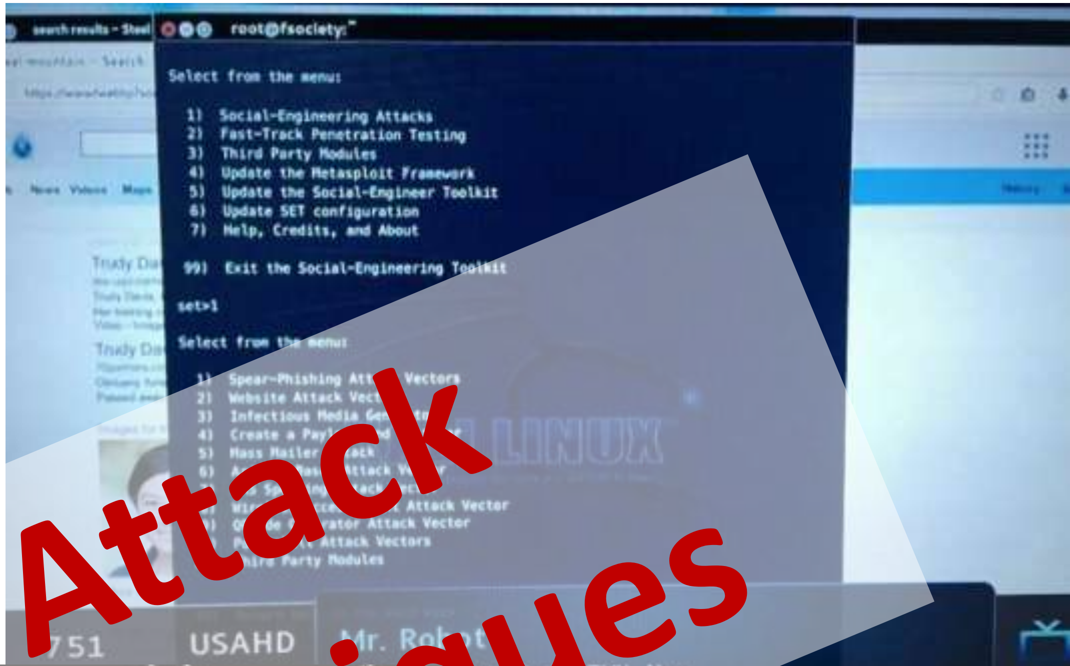
1. Your help!
2. All of your ideas.

# Things We Need

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

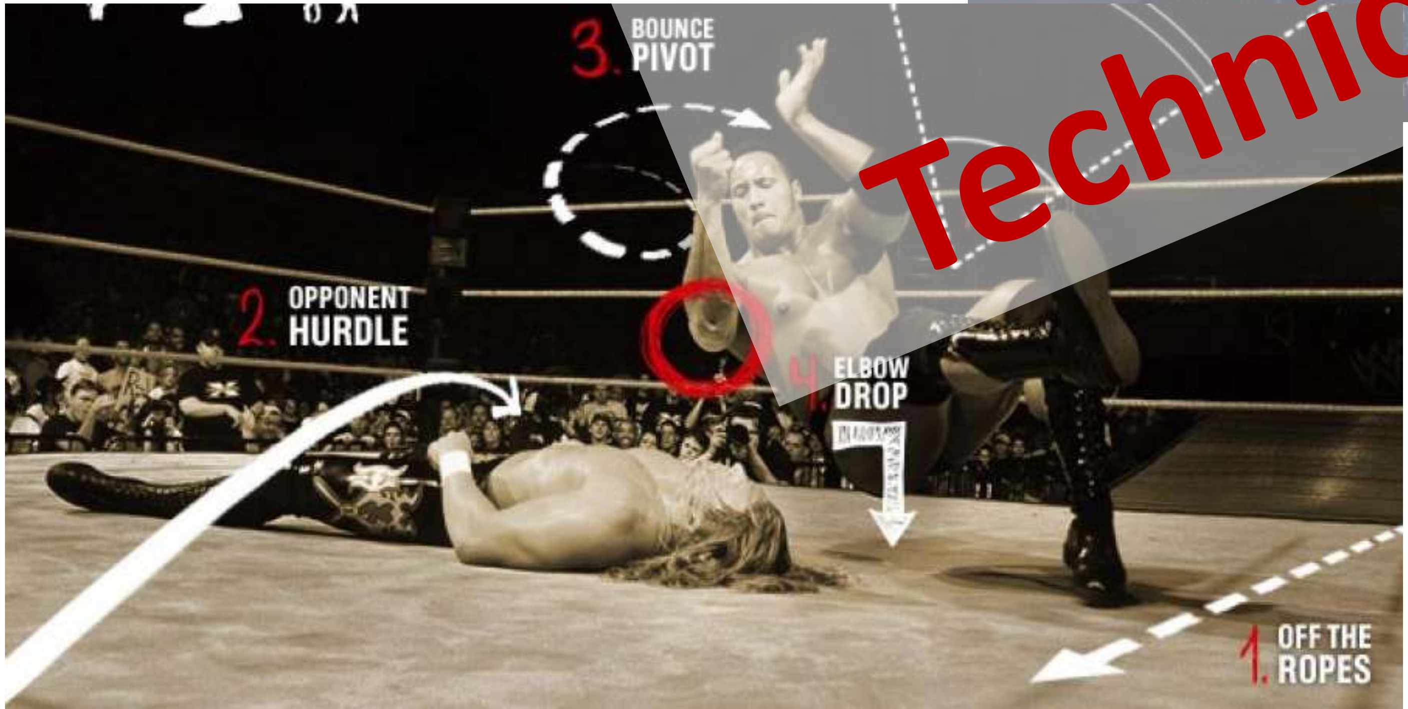
# Things We Need

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



```
root@fsociety:~

Select from the menu:

  1)  Social-Engineering Attacks
  2)  Fast-Track Penetration Testing
  3)  Third Party Modules
  4)  Update the Metasploit Framework
  5)  Update the Social-Engineer Toolkit
  6)  Update SET configuration
  7)  Help, Credits, and About

 99)  Exit the Social-Engineering Toolkit

set>1

Select from the menu:

   1)  Spear-Phishing Attack Vectors
   2)  Website Attack Vectors
   3)  Infectious Media Generator
   4)  Create a Payload and Listener
   5)  Mass Mailer Attack
   6)  Arduino-Based Attack Vector
   7)  Wireless Access Point Attack Vector
   8)  QRCode Generator Attack Vector
   9)  Powershell Attack Vectors
  10)  Third Party Modules
```

search results - Steel
751
USAHD
Mr. Robot
TVY New
l0its.wmv - Fsociety attempts to
te Steel Mountain, the most secure da...
Othe
2015
LINUX

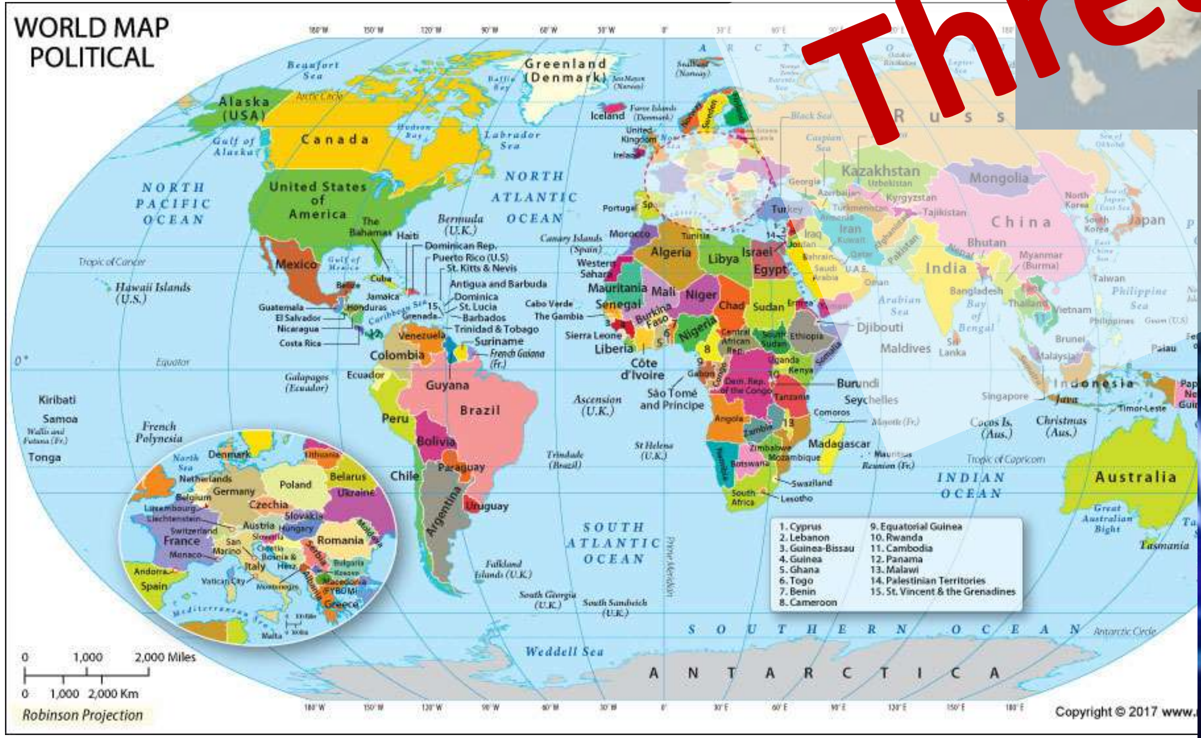


Attack Techniques

# Things We Need

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

Threat Intel



# Things We Need

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

# Part 1.

# Arrival: Fly-Away Kit

*and…* SCENE.

# Part 2.
## The Model CISO

*and…* SCENE.

# Part c:\

## The Out-brief

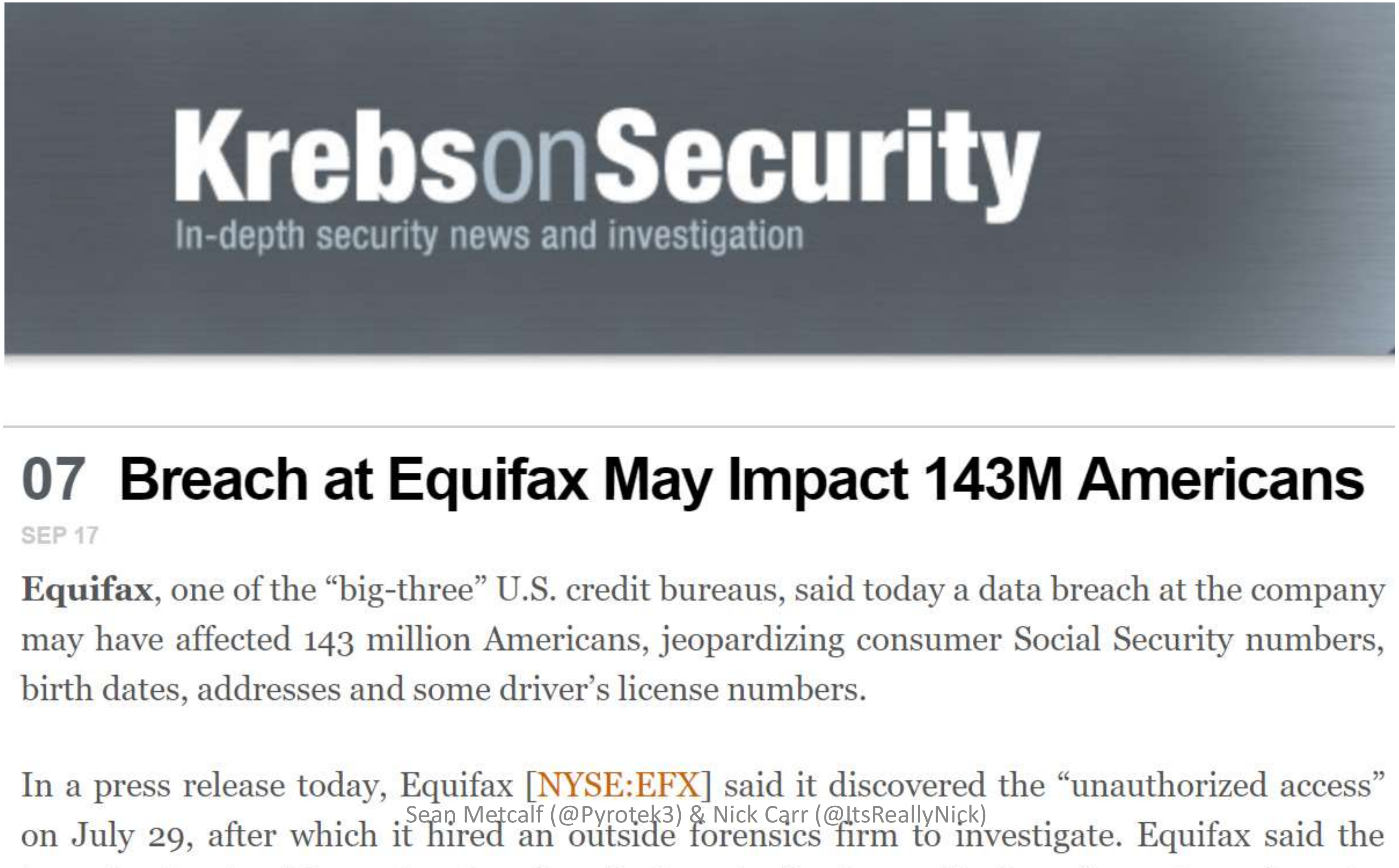
*and…* SCENE.

# Part 404: SLIDE NOT FOUND

## The Pitch

*and…* SCENE.

# Let’s talk about how to avoid a Krebs article about your company



KrebsonSecurity

In-depth security news and investigation

## 07 Breach at Equifax May Impact 143M Americans

SEP 17

**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

# 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.

# 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.

# 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