RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: AIR-F02

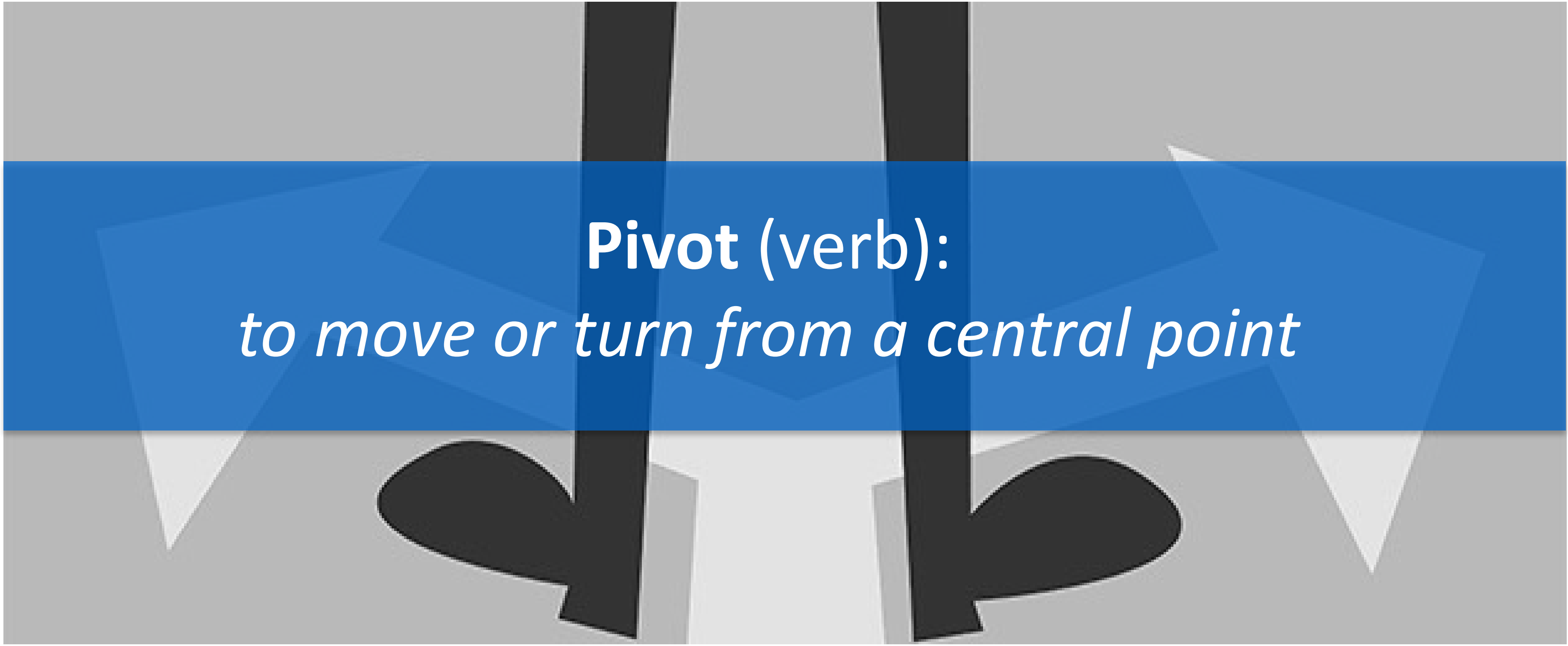
The Pivot

Jonathan Trull

Office of the CISO
Optiv
@jonathantrull

#RSAC

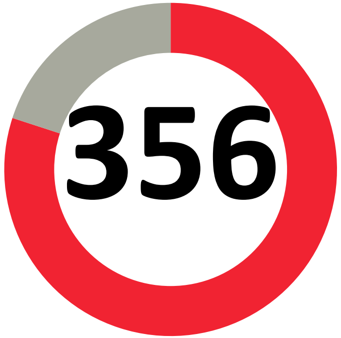
The Pivot



Pivot (verb):

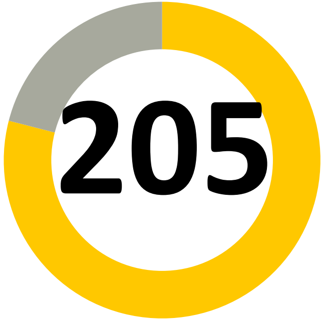
to move or turn from a central point

Dwell Time



APT1

APT1 maintained access to victim networks for an average of 356 days

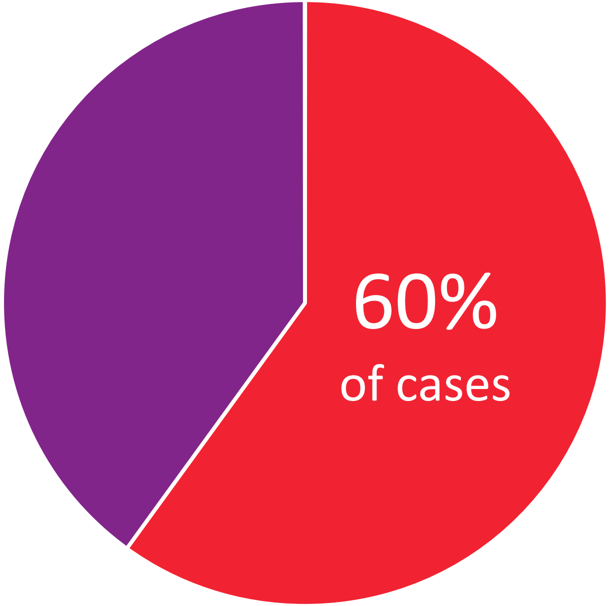


Dwell Time

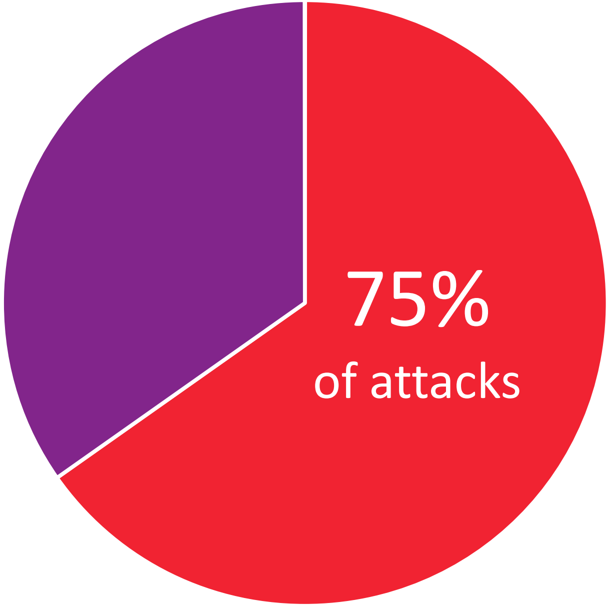
Attackers had free reign of victim networks for 205 days in 2015

Detection Deficit

Source: 2015 Verizon Data Breach Report

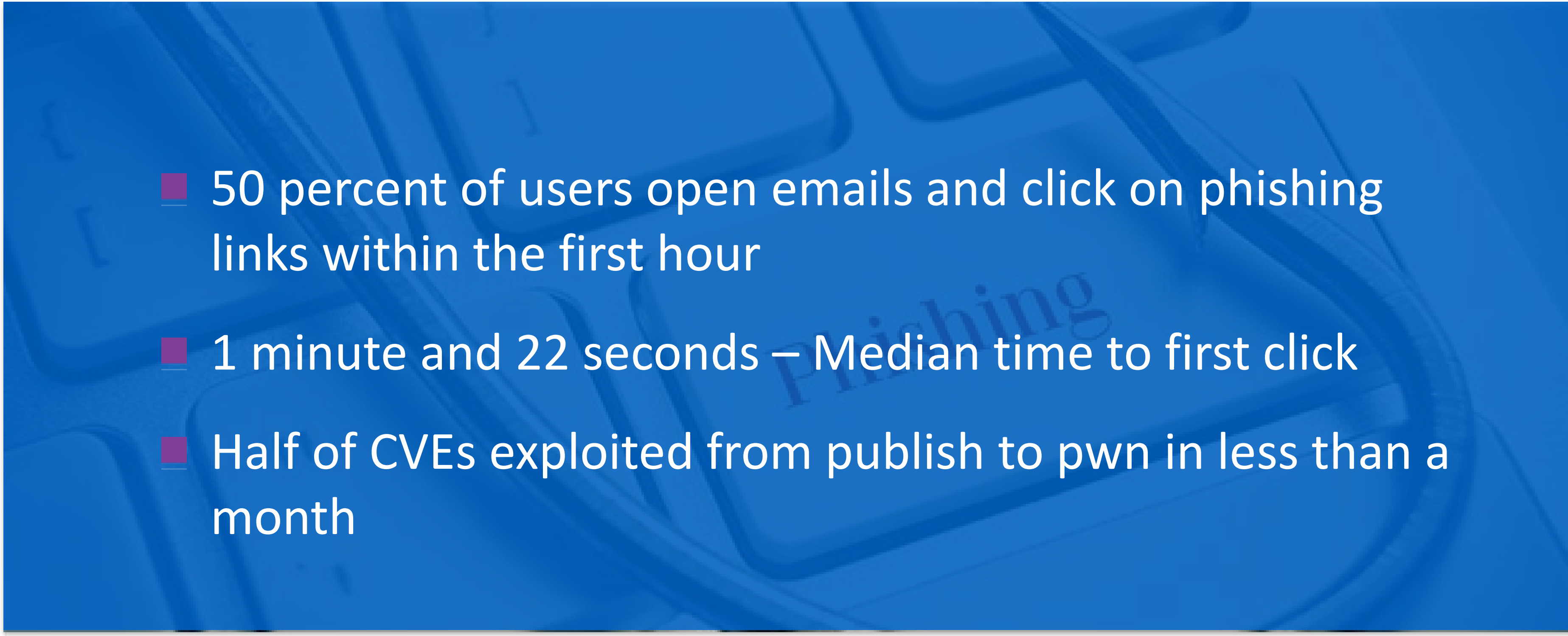


Attackers are able to compromise an organization within minutes



Spread from Victim 0 to Victim 1 within one day (24 hours)

Time is not on your side



- 50 percent of users open emails and click on phishing links within the first hour
- 1 minute and 22 seconds – Median time to first click
- Half of CVEs exploited from publish to pwn in less than a month

Session Objectives

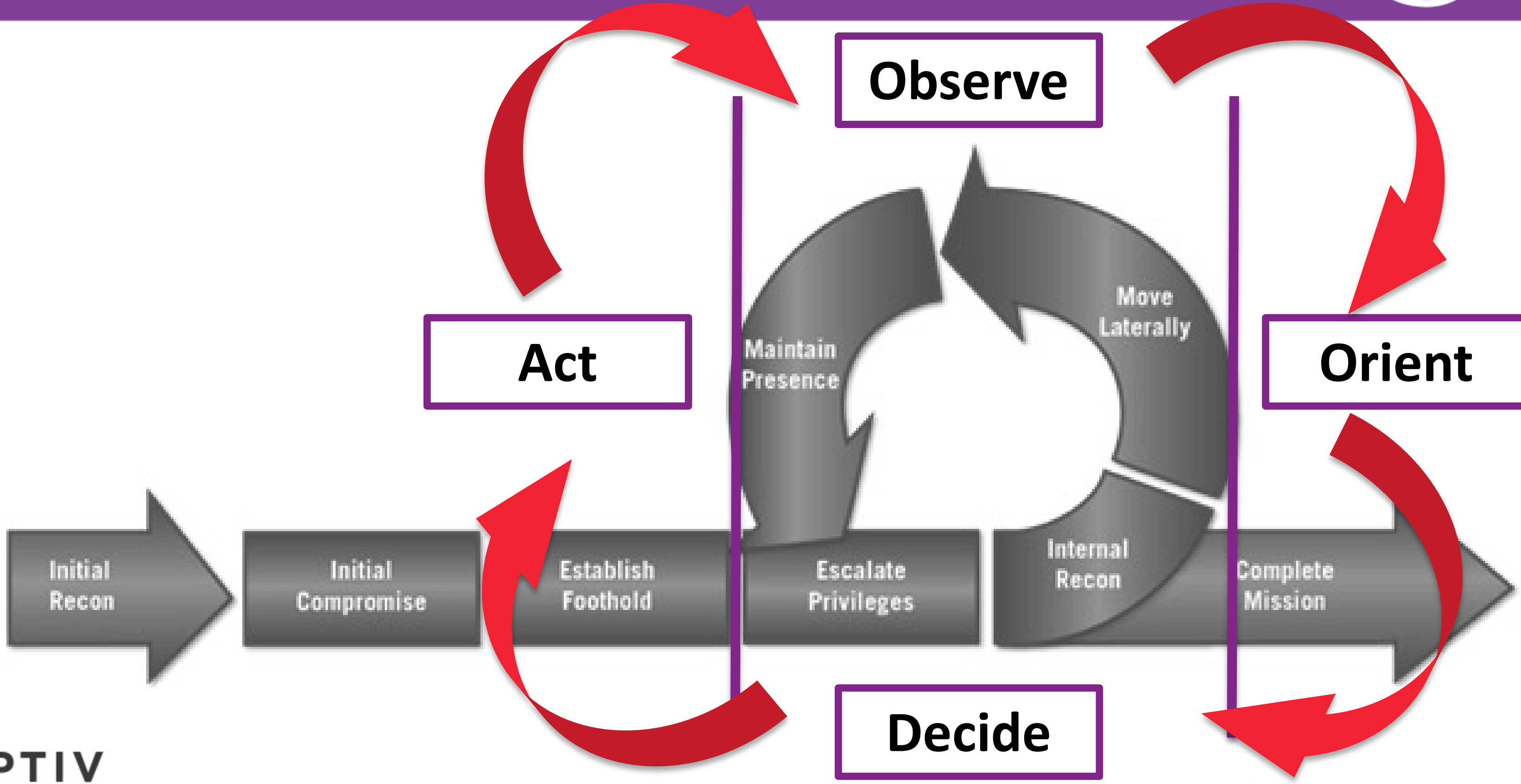
How attackers pivot and move laterally through an organization

How to identify the telltale signs of a pivot

Identify the steps to defend against it

How Attackers Pivot and Move Laterally

Attacker Lifecycle



Optiv Simulated Attack Lifecycle

Stages	Use Cases
Code Execution	UC-01.003: Host Exploit Flash CVE-2014-0497 UC-02.001: Malware Installation Zeus UC-02.002: Malware Installation Custom (Veil AES) UC-02.004: Malware Installation Custom (Excel Macro) UC-02.008: Disrupt Security Software UC-02.009: Persistence
Lateral Movement	UC-02.010: Install Tools UC-03.001: Credential Theft UC-04.001: Lateral Movement Reconnaissance UC-04.002: Lateral Movement Malware Installation
Exfiltrate Data	UC-05.001: Data Exfiltration Zeus UC-05.002: Data Exfiltration UC-06.001: Cover Tracks

Story of a Hack

Medium-sized Pharmaceutical Company

- Significant R&D
- Microsoft environment

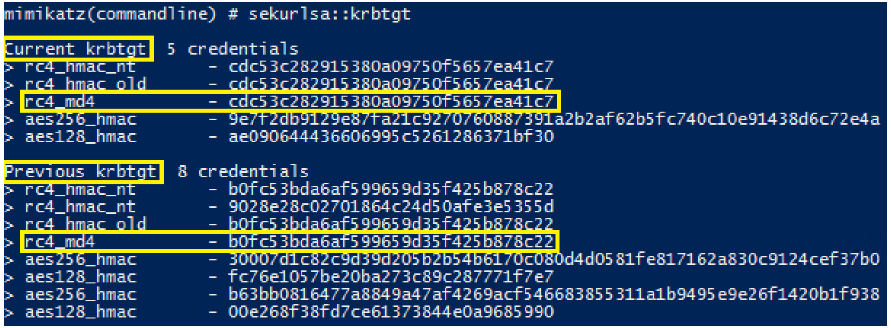
Patient Zero

Windows 7 Enterprise Desktop

- User running with local administrator privileges
- Spear phishing email / Link to watering hole

We don’t need no stinking badges

- After initial compromise, attackers are leveraging native tools:
  - cmd.exe
  - Powershell scripts
  - at.exe
  - Net use
  - WMI

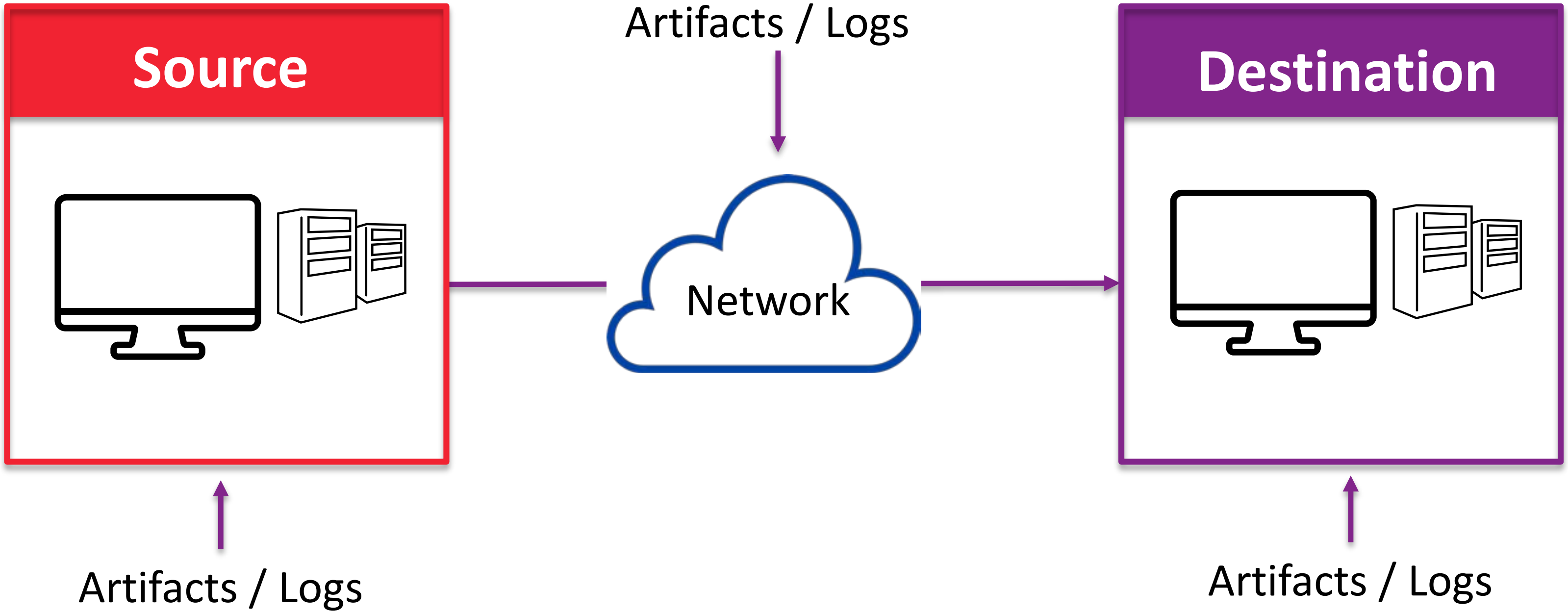


```
mimikatz(commandline) # sekurlsa::krbtgt

Current krbtgt  5 credentials
> rc4_hmac_nt         - cdc53c282915380a09750f5657ea41c7
> rc4_hmac_old        - cdc53c282915380a09750f5657ea41c7
> rc4_md4             - cdc53c282915380a09750f5657ea41c7
> aes256_hmac         - 9e7f2db9129e87fa21c9270760887391a2b2af62b5fc740c10e91438d6c72e4a
> aes128_hmac         - ae090644436606995c5261286371bf30

Previous krbtgt  8 credentials
> rc4_hmac_nt         - b0fc53bda6af599659d35f425b878c22
> rc4_hmac_nt         - 9028e28c02701864c24d50afe3e5355d
> rc4_hmac_old        - b0fc53bda6af599659d35f425b878c22
> rc4_md4             - b0fc53bda6af599659d35f425b878c22
> aes256_hmac         - 30007d1c82c9d39d205b2b54b6170c080d4d0581fe817162a830c9124cef37b0
> aes128_hmac         - fc76e1057be20ba273c89c287771f7e7
> aes256_hmac         - b63bb0816477a8849a47af4269acf546683855311a1b9495e9e26f1420b1f938
> aes128_hmac         - 00e268f38fd7ce61373844e0a9685990
```

- Compromised credentials are commonly used during pivot:
  - Mimikatz
  - wce

Signs of a Pivot (Indicators of Pivot or IOPs)

Indicators on Two or More Machines



Recon Stage

Domains, Users and Systems

- whoami
- net view /domain
- net users
- net group "Domain Admins" / <domain >
- net view /domain:<Domain Name>

Sessions and Open Shares

- net session
- net file

Open Ports

- Ping
- FPORT

Remote Code Execution

Native Tools

- Scheduled Tasks
  - at.exe
- WMI
- PowerShell
- Remote Desktop (RDP)

Third-Party Tools

- SysInternals PsExec
- Netcat
- Metasploit

Remote Code Execution Examples

- Windows Management Instrumentation (WMI):
  - wmic /domain:host process call create “c:\rootkit.exe”
- Powershell
  - Invoke-Command host {c:\rootkit.exe}
- SysInternals PsExec
  - Psexec \\host -e c:\rootkit.exe

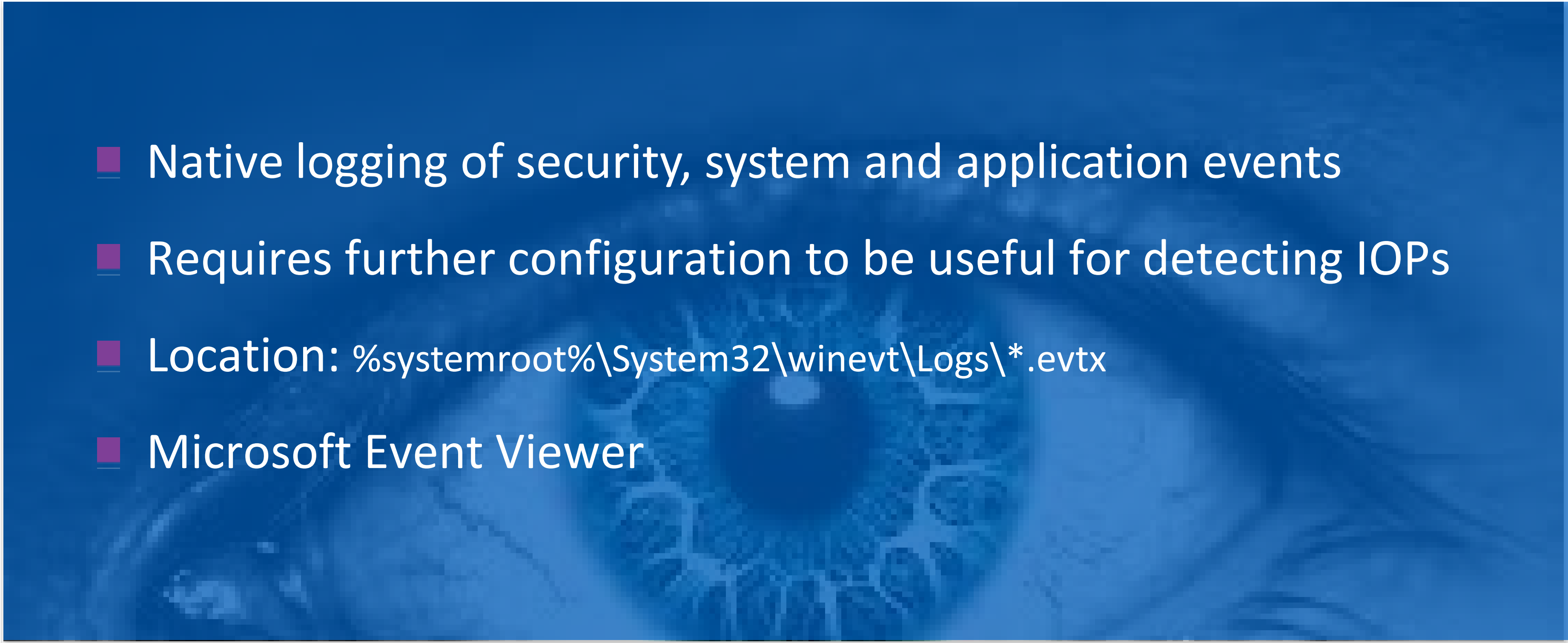
Mapping Shares

- Allows for limited interaction with destination host for attacker
- However, share may contain valuable data
- Usage:
  - Map Network Drive wizard
  - CLI -> net use z: \\host\drive /user <username> <password>

Scheduled Tasks

- at.exe or schtasks.exe creates tasks on local or remote host
- Typically used to remotely execute malware or other malicious tools
- Requires admin privileges
- Runs under context of SYSTEM

Windows Event Logs



- Native logging of security, system and application events
- Requires further configuration to be useful for detecting IOPs
- Location: %systemroot%\System32\winevt\Logs\*.evtx
- Microsoft Event Viewer

Windows Account Usage

	ID	Level	Event Log	Event Source
Account Lockouts	4740	Informational	Security	Microsoft-Windows-Security-Auditing
User Added to Privileged Group	4728, 4732, 4756	Informational	Security	Microsoft-Windows-Security-Auditing
Security-Enabled Group Modification	4735	Informational	Security	Microsoft-Windows-Security-Auditing
Successful User Account Login	4624	Informational	Security	Microsoft-Windows-Security-Auditing
Failed User Account Login	4625	Informational	Security	Microsoft-Windows-Security-Auditing
Account Login with Explicit Credentials	4648	Informational	Security	Microsoft-Windows-Security-Auditing

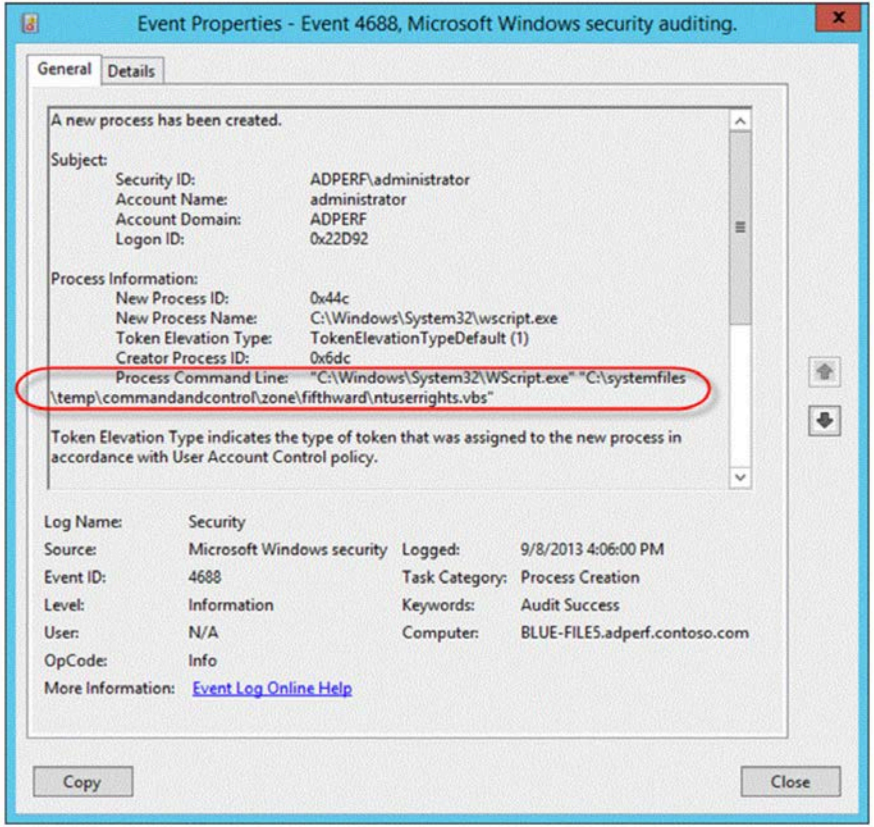
Windows Logon Types

Type	Code	Example
Interactive	2	At the console of a computer
Network Logons	3	Connections to shared folders or printers
Batch	4	Scheduled tasks
Service	5	Windows service started
Unlock	7	Unlock computer screen
NetworkCleartext	8	Similar to network logons but in clear text
NewCredentials	9	RunAs used to start program under different user account
Remoteinteractive	10	RDP, terminal services, remote assistance
CacheInteractive	11	Remote logon with domain account

Process Creation

- Event ID 4688: A new process has been created
- Documents each program that is executed, who the program ran as and the process that started this process
- Disabled by default:
  - Enable by editing GPO
  - Policy location: Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Configuration > Detailed Tracking
- Missing process command line arguments by default
  - Enable via GPO – "Include command line in process creation events"

Created Process with Command Line



Event Properties - Event 4688, Microsoft Windows security auditing.
General
Details

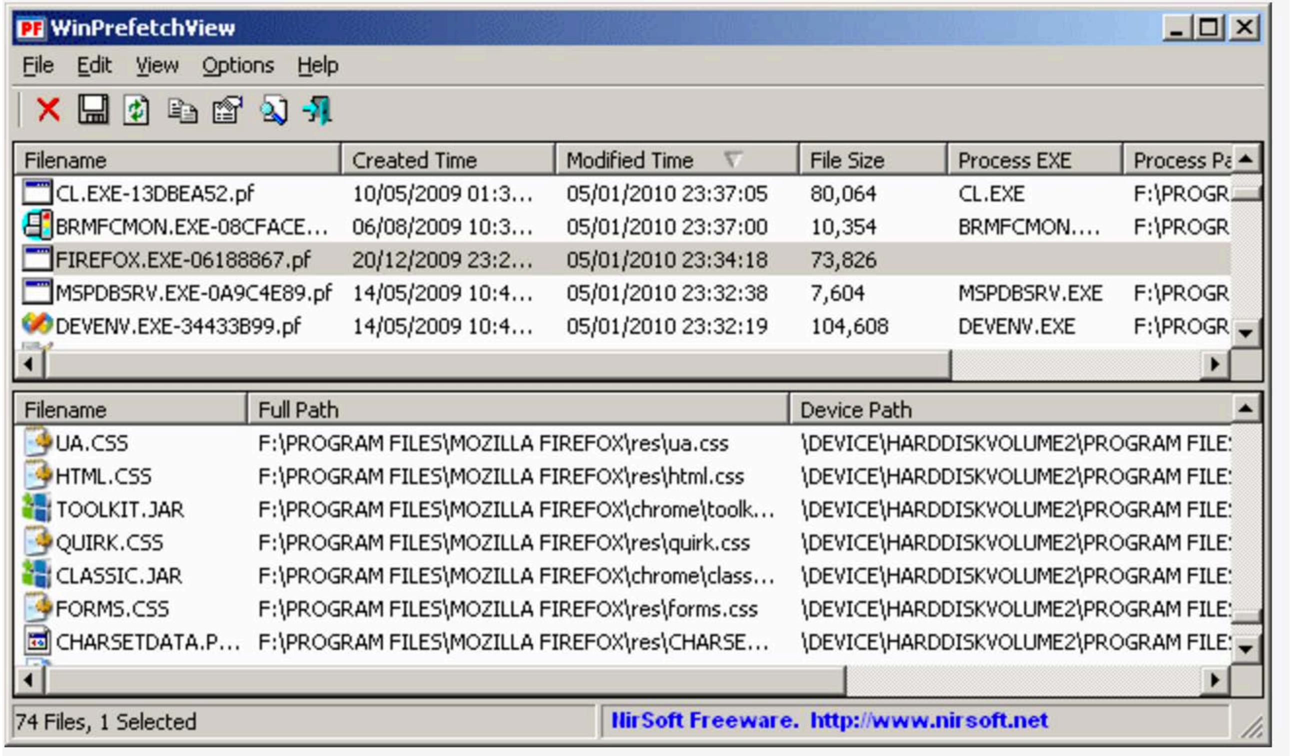
```
A new process has been created.

Subject:
        Security ID:            ADPERF\administrator
        Account Name:           administrator
        Account Domain:         ADPERF
        Logon ID:               0x22D92

Process Information:
        New Process ID:         0x44c
        New Process Name:       C:\Windows\System32\wscript.exe
        Token Elevation Type:   TokenElevationTypeDefault (1)
        Creator Process ID:     0x6dc
        Process Command Line:   "C:\Windows\System32\WScript.exe" "C:\systemfiles
\temp\commandandcontrol\zone\fifthward\ntuserrights.vbs"

Token Elevation Type indicates the type of token that was assigned to the new process in
accordance with User Account Control policy.
```

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	9/8/2013 4:06:00 PM
Event ID:	4688	Task Category:	Process Creation
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	BLUE-FILES.adperf.contoso.com
OpCode:	Info		
More Information:	Event Log Online Help		

Prefetch Files

- Introduced in Windows XP
- Designed to speed up application startup processes
- Location: %systemroot%\prefetch\*.pf
- Contain name of the executable, Unicode list of DLLs used, count of times .exe run, and timestamp indicating last run time

Viewing Pre-fetch Files



Filename	Created Time	Modified Time	File Size	Process EXE	Process Pa
CL.EXE-13DBEA52.pf	10/05/2009 01:3...	05/01/2010 23:37:05	80,064	CL.EXE	F:\PROGR
BRMFCMON.EXE-08CFACE...	06/08/2009 10:3...	05/01/2010 23:37:00	10,354	BRMFCMON....	F:\PROGR
FIREFOX.EXE-06188867.pf	20/12/2009 23:2...	05/01/2010 23:34:18	73,826		
MSPDBSRV.EXE-0A9C4E89.pf	14/05/2009 10:4...	05/01/2010 23:32:38	7,604	MSPDBSRV.EXE	F:\PROGR
DEVENV.EXE-34433B99.pf	14/05/2009 10:4...	05/01/2010 23:32:19	104,608	DEVENV.EXE	F:\PROGR

Filename	Full Path	Device Path
UA.CSS	F:\PROGRAM FILES\MOZILLA FIREFOX\res\ua.css	\DEVICE\HARDDISKVOLUME2\PROGRAM FILE:
HTML.CSS	F:\PROGRAM FILES\MOZILLA FIREFOX\res\html.css	\DEVICE\HARDDISKVOLUME2\PROGRAM FILE:
TOOLKIT.JAR	F:\PROGRAM FILES\MOZILLA FIREFOX\chrome\toolk...	\DEVICE\HARDDISKVOLUME2\PROGRAM FILE:
QUIRK.CSS	F:\PROGRAM FILES\MOZILLA FIREFOX\res\quirk.css	\DEVICE\HARDDISKVOLUME2\PROGRAM FILE:
CLASSIC.JAR	F:\PROGRAM FILES\MOZILLA FIREFOX\chrome\class...	\DEVICE\HARDDISKVOLUME2\PROGRAM FILE:
FORMS.CSS	F:\PROGRAM FILES\MOZILLA FIREFOX\res\forms.css	\DEVICE\HARDDISKVOLUME2\PROGRAM FILE:
CHARSETDATA.P...	F:\PROGRAM FILES\MOZILLA FIREFOX\res\CHARSE...	\DEVICE\HARDDISKVOLUME2\PROGRAM FILE:

74 Files, 1 Selected

NirSoft Freeware. http://www.nirsoft.net

Scheduled Tasks

Source
Prefetch files of program execution => at.exe or schtasks.exe
Destination
Service being started => Event ID 7035/7036

Windows Special Groups

- Event ID 4964
- Introduced in Windows 2008
- Use to track logon of particular accounts on systems

IOP #1 – Successful PtH

Event ID	Event Log	Level	Logon Type	Auth Package
4624	Security	Informational	3	NTLM

View filter -> Not a domain logon and not the ANONYMOUS LOGON account

IOP #2 – Failed PtH

Event ID	Event Log	Level	Logon Type	Auth. Package
4625	Security	Informational	3	NTLM

View Filter -> Not a domain logon and not the ANONYMOUS LOGON account

IOP #3 – New Scheduled Task

- Alert on new Event ID 7035 created by at[#].exe

IOP # 4 – Privilege Escalation

- Alarm on login from non-workstation host to another non-workstation host
- Alarm on login from one workstation to another workstation
- Alarm on login attempts using known service accounts
- Alarm on creation of new domain admin account or elevation of account

Defending the Pivot

Levels of Defense

100,000 Foot View

- Layered preventive and detective controls
- IOP hunting
- User behavior analytics
- Configure auditing / EDR or Sysmon
- Honeypot deployment

In the Weeds

- Remove / restrict use of Powershell on endpoints
- Look for IOP artifacts at the host and network levels
- Mitigate Pass-the-Hash attacks

Optiv Research Methodology

- We selected seven solutions that span across all endpoint categories
- The endpoint product was the only point of defense
- All endpoints were unpatched and vulnerable to the selected attacks
- Goal was to compare and contrast results from different types of endpoint solutions

Types of Solutions Tested

Endpoint Protection Platform (EPP)

Exploitation Mitigation

EDR and App Control

Endpoint Detection and Response (EDR)

Testing Highlights

Lateral Movement

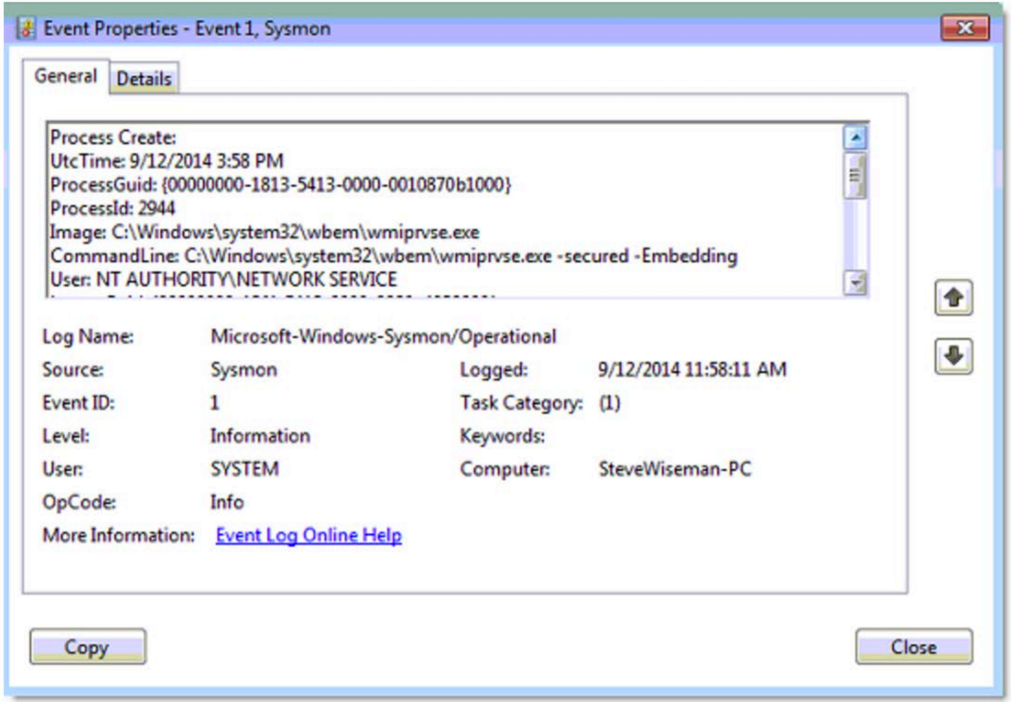
- No silver bullets
- Look for odd usage of scripts
- Use threat modeling to identify how attackers would pivot through your network and build detection rules to identify IOPs
- Leverage Windows event logs and timeline analysis
- Control user-to-user communication and powershell script execution
- Use enhanced authentication (OTP/2fa) for domain admin accounts
- Implement mitigation strategies for Pass-the-Hash attacks

Detailed Results

	Endpoint Protection Platform			Anti-Exploitation	EDR + App Control	EDR	
Use Case	Vendor # 1	Vendor # 2	Vendor # 3	Vendor # 4	Vendor # 5	Vendor # 6	Vendor # 7
UC-02.010: Install Tools	Pass	Pass	Pass	Fail	Partial	Fail	Partial
UC-03.001: Credential Theft	Partial	Partial	Partial	Fail	Partial	Fail	Partial
UC-04.001: Lateral Movement Reconnaissance	Fail	Fail	Fail	Fail	Partial	Fail	Partial
UC-04.002: Lateral Movement Malware Installation	Pass	Fail	Pass	Pass	Partial	Partial	Partial

Enable Sufficient Logging

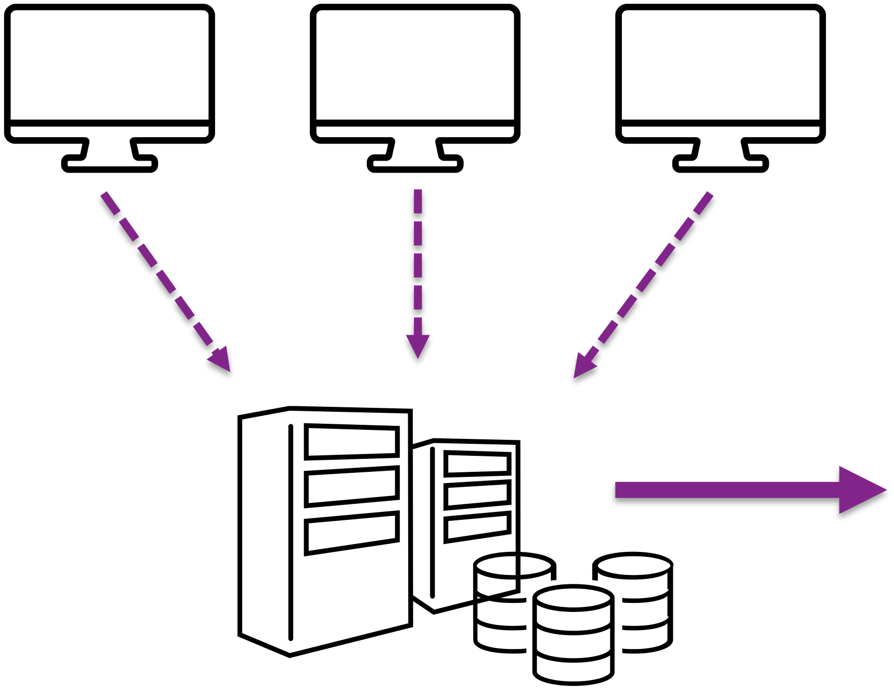
- Sysmon
- EDR
- Audit policy configuration

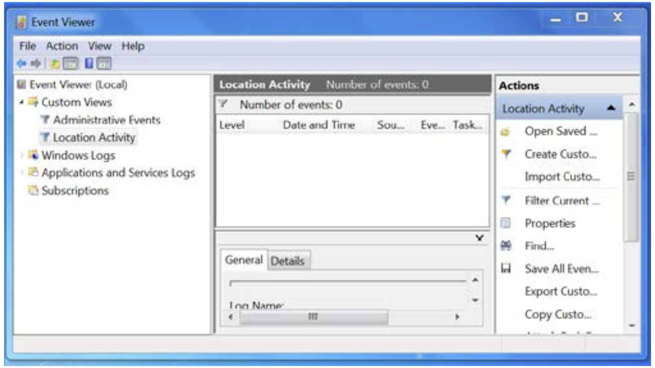


```
Process Create:
UtcTime: 9/12/2014 3:58 PM
ProcessGuid: {00000000-1813-5413-0000-0010870b1000}
ProcessId: 2944
Image: C:\Windows\system32\wbem\wmiprvse.exe
CommandLine: C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding
User: NT AUTHORITY\NETWORK SERVICE
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	9/12/2014 11:58:11 AM
Event ID:	1	Task Category:	(1)
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	SteveWiseman-PC
OpCode:	Info		
More Information:	Event Log Online Help		

Central Logging and Analysis





Location Activity Number of events: 0

Number of events: 0

Level	Date and Time	Sou...	Eve...	Task...

Honeypots

For More Detailed Information

www.secopslabs.com

Apply What You Have Learned Today!

- **Next week you should:**
  - Ensure sufficient logging is enabled to detect IOPs
  - Develop a detailed threat model for how attackers would pivot through your organization to gain access to your crown jewels
- **In the first three months following this presentation you should:**
  - Perform daily IOP hunting on your endpoints using either an EDR solution or Microsoft event logs
  - Deploy honeypots to the DMZ and user and server subnets
- **Within six months you should:**
  - Implement enhanced authentication for domain admin accounts and pass-the-hash mitigation strategies

References

- www.ultimatewindowssecurity.com
- https://technet.microsoft.com/security/advisory/3004375
- http://sysforensics.org/2014/01/lateral-movement/
- www.optiv.com
- http://windowsir.blogspot.com/2013/07/howto-track-lateral-movement.html
- https://www.nsa.gov/ia/_files/app/spotting_the_adversary_with_windows_event_log_monitoring.pdf