علیرضا رضایی – تحقیق جلسه دهم

DCShadow

Resources:

https://www.dcshadow.com/

First disclosure

DCShadow has been presented at the Bluehat IL 2018 conference by Vincent LE TOUX and Benjamin Delpy

It was already possible to simulate a domain controller or to alter its internal database.

For example, by installing in a virtual machine a customized version of SAMBA. But given the fact that running a virtual machine needs hardware instruction (on x64 CPU it is disabled by default), a physical interaction with the computer may be required to enable them in the BIOS/EFI. In addition the size and time needed for a VM is not scalable.

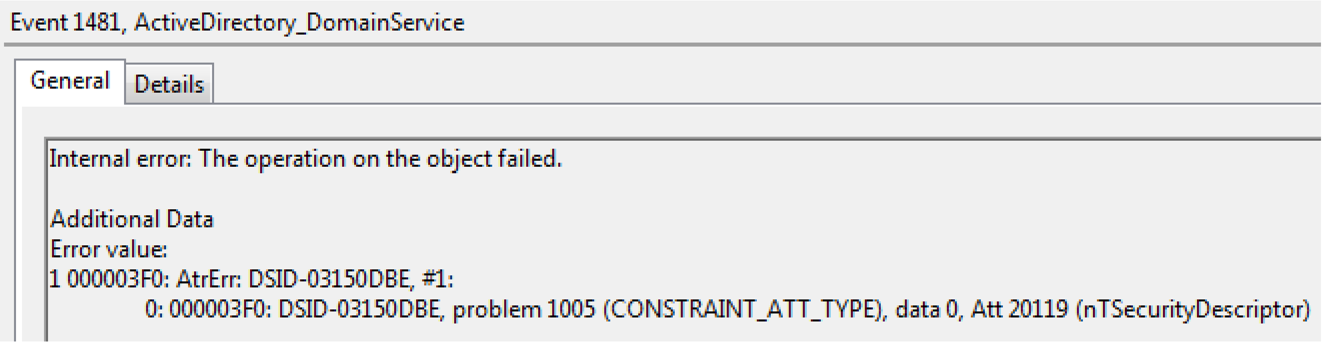
DSInternals powershell tools already allows the editing of an existing AD database, but in offline mode. Putting it online requires to use the AD recovery mode which is not straight forward.

Description of the attack

The attacks is done using the following steps:

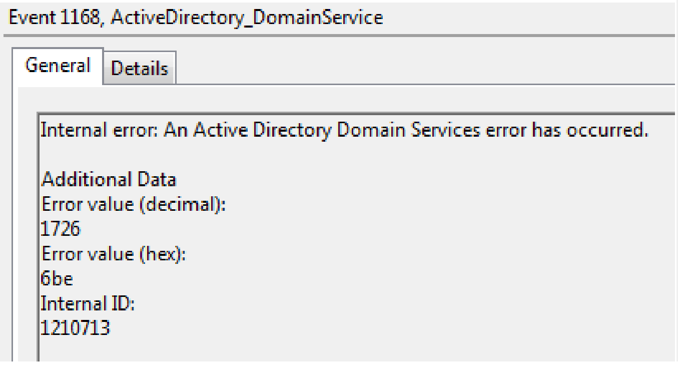
- registering the "DC" by creating 2 objects in the CN=Configuration partition and altering the SPN of the computer used.
- Pushing the data (triggered using DrsReplicaAdd, KCC or other internal AD events)
- Removing the object previously created to demote the DC

Here is an example of error when pushing an incorrect DACL (in this case the Owner part was missing)

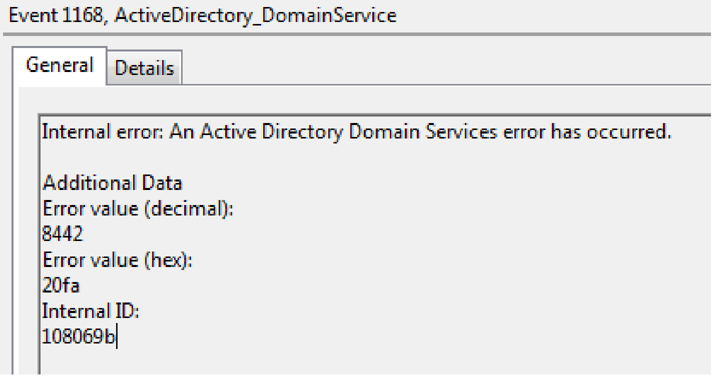


```
Internal error: The operation on the object failed.

Additional Data
Error value:
1 000003F0: AtrErr: DSID-03150DBE, #1:
        0: 000003F0: DSID-03150DBE, problem 1005 (CONSTRAINT_ATT_TYPE), data 0, Att 20119 (nTSecurityDescriptor)
```

And some other example of invalid data



```
Internal error: An Active Directory Domain Services error has occurred.

Additional Data
Error value (decimal):
1726
Error value (hex):
6be
Internal ID:
1210713
```



```
Internal error: An Active Directory Domain Services error has occurred.

Additional Data
Error value (decimal):
8442
Error value (hex):
20fa
Internal ID:
108069b
```

Is it a vulnerability ?

No, because the protocols used are documented:

- MS-ADTS
- MS-DRSR

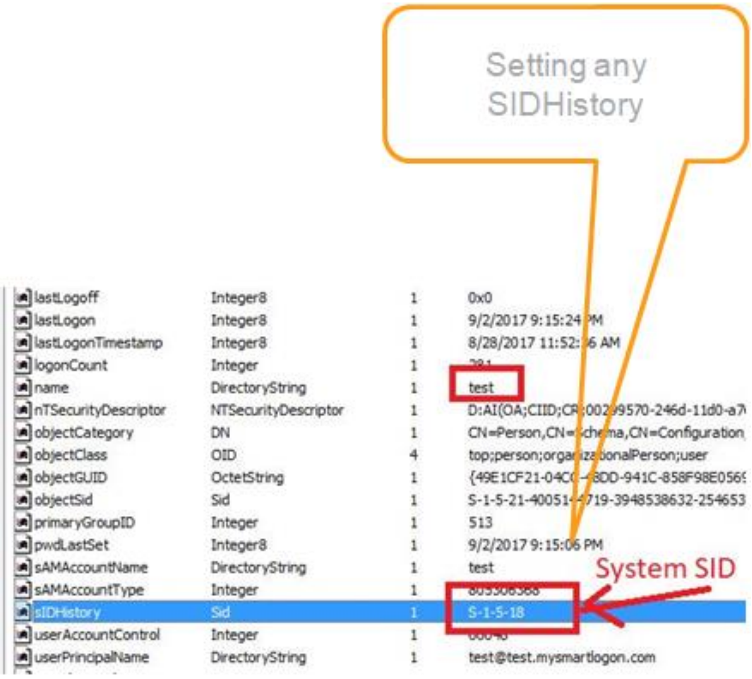
It is a post exploitation attack (also called domination attack) because it requires domain admin (or enterprise admin) privileges

Why is it a game changer ?

Functionally

At a functional level:

- It can create new backdoor such as SIDHistory, ntpwdHistory, ...
- It is a tool to erase the attacker traces (replication metadata, schemasignatureinfo, ...)
- Create unseen XSS attack on administration reports



Setting any SIDHistory

System SID

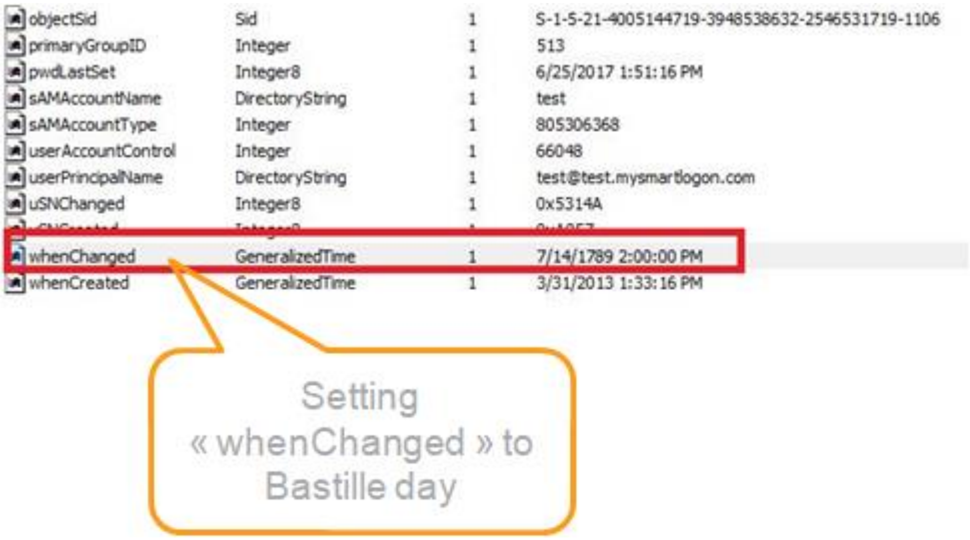
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	9/2/2017 9:15:24 PM
lastLogonTimestamp	Integer8	1	8/28/2017 11:52:?6 AM
logonCount	Integer	1	281
name	DirectoryString	1	test
nTSecurityDescriptor	NTSecurityDescriptor	1	D:AI(OA;CIID;CR;00299570-246d-11d0-a7
objectCategory	DN	1	CN=Person,CN=Schema,CN=Configuration,
objectClass	OID	4	top;person;organizationalPerson;user
objectGUID	OctetString	1	{49E1CF21-04C0-48DD-941C-858F98E0569
objectSid	Sid	1	S-1-5-21-4005144719-3948538632-254653
primaryGroupID	Integer	1	513
pwdLastSet	Integer8	1	9/2/2017 9:15:06 PM
sAMAccountName	DirectoryString	1	test
sAMAccountType	Integer	1	805306368
sIDHistory	Sid	1	S-1-5-18
userAccountControl	Integer	1	66048
userPrincipalName	DirectoryString	1	test@test.mysmartlogon.com

Technically

At a technical level:

- The modifications done are made without any logging
- Modifications done only by a DC such as setting the SID History or WhenChanged can be done without logging
- Partial changes such as changing only the previous password without the new one can be done without logging
- Modifications not compliant with the AD data such as a very long sAMAccountName (< 16 characters) can be done without logging

In short it bypasses the SIEM monitoring done on the Active Directory

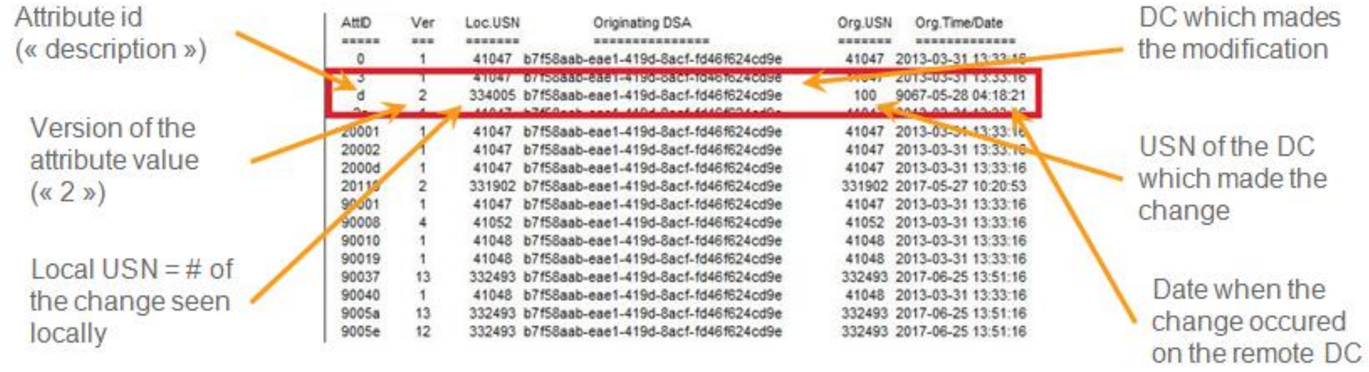


```
objectSid            Sid                 1    S-1-5-21-4005144719-3948538632-2546531719-1106
primaryGroupID       Integer             1    513
pwdLastSet           Integer8            1    6/25/2017 1:51:16 PM
sAMAccountName       DirectoryString     1    test
sAMAccountType       Integer             1    805306368
userAccountControl   Integer             1    66048
userPrincipalName    DirectoryString     1    test@test.mysmartlogon.com
uSNChanged           Integer8            1    0x5314A
uSNCreated           Integer8            1    0xA057
whenChanged          GeneralizedTime     1    7/14/1789 2:00:00 PM
whenCreated          GeneralizedTime     1    3/31/2013 1:33:16 PM
```

Setting « whenChanged » to Bastille day

Forensics of the attack

Because DCShadow is pushing replication information, DCShadow is responsible for pushing replication metadata. This metadata is accessible to anyone (including from trusted domains) and available throught LDAP or RPC.
This metadata is used by forensic analysts to rebuild the history of change and understand what happened on a domain. Well, this data cannot be trusted anymore.



```
AttID    Ver    Loc.USN         Originating DSA                    Org.USN  Org.Time/Date
=====    ===    =======    ================                        =======  =============
    0      1      41047 b7f58aab-eae1-419d-8acf-fd46f624cd9e         41047  2013-03-31 13:33:16
    3      1      41047 b7f58aab-eae1-419d-8acf-fd46f624cd9e         41047  2013-03-31 13:33:16
    d      2     334005 b7f58aab-eae1-419d-8acf-fd46f624cd9e           100  9067-05-28 04:18:21
[illegible]
20001      1      41047 b7f58aab-eae1-419d-8acf-fd46f624cd9e         41047  2013-03-31 13:33:16
20002      1      41047 b7f58aab-eae1-419d-8acf-fd46f624cd9e         41047  2013-03-31 13:33:16
2000d      1      41047 b7f58aab-eae1-419d-8acf-fd46f624cd9e         41047  2013-03-31 13:33:16
20119      2     331902 b7f58aab-eae1-419d-8acf-fd46f624cd9e        331902  2017-05-27 10:20:53
90001      1      41047 b7f58aab-eae1-419d-8acf-fd46f624cd9e         41047  2013-03-31 13:33:16
90008      4      41052 b7f58aab-eae1-419d-8acf-fd46f624cd9e         41052  2013-03-31 13:33:16
90010      1      41048 b7f58aab-eae1-419d-8acf-fd46f624cd9e         41048  2013-03-31 13:33:16
90019      1      41048 b7f58aab-eae1-419d-8acf-fd46f624cd9e         41048  2013-03-31 13:33:16
90037     13     332493 b7f58aab-eae1-419d-8acf-fd46f624cd9e        332493  2017-06-25 13:51:16
90040      1      41048 b7f58aab-eae1-419d-8acf-fd46f624cd9e         41048  2013-03-31 13:33:16
9005a     13     332493 b7f58aab-eae1-419d-8acf-fd46f624cd9e        332493  2017-06-25 13:51:16
9005e     12     332493 b7f58aab-eae1-419d-8acf-fd46f624cd9e        332493  2017-06-25 13:51:16
```

Attribute id
(« description »)

Version of the
attribute value
(« 2 »)

Local USN = # of
the change seen
locally

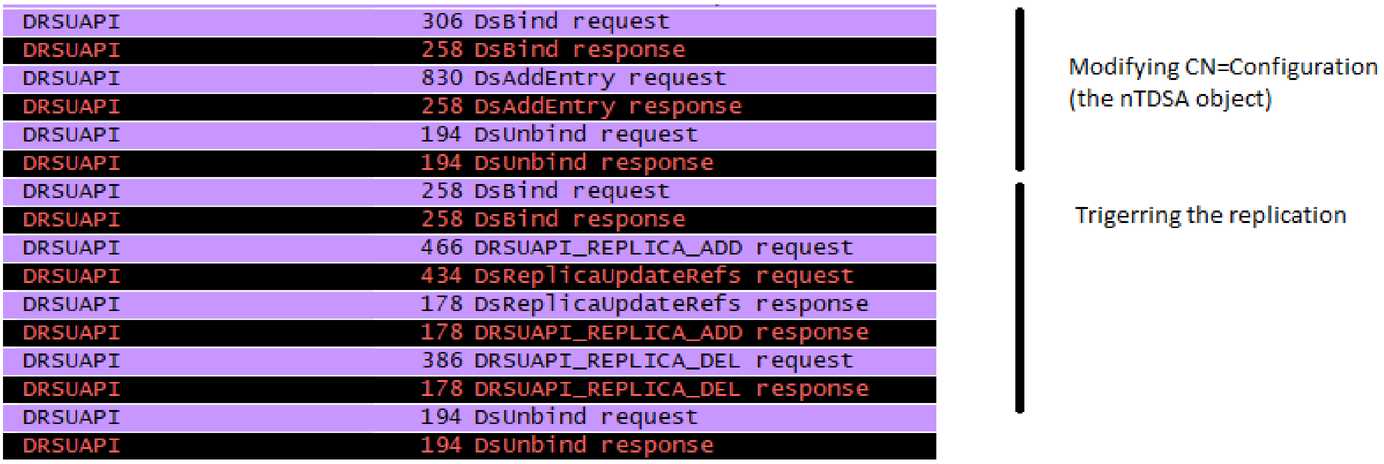
DC which mades
the modification

USN of the DC
which made the
change

Date when the
change occured
on the remote DC

How can it be detected ?

DCShadow is easy to detect at network level. API like DrsAddEntry or DrsReplicaAdd are called only from a DC so a call from another computer should be considered as suspicious.



```
DRSUAPI      306 DsBind request
DRSUAPI      258 DsBind response
DRSUAPI      830 DsAddEntry request
DRSUAPI      258 DsAddEntry response
DRSUAPI      194 DsUnbind request
DRSUAPI      194 DsUnbind response
DRSUAPI      258 DsBind request
DRSUAPI      258 DsBind response
DRSUAPI      466 DRSUAPI_REPLICA_ADD request
DRSUAPI      434 DsReplicaUpdateRefs request
DRSUAPI      178 DsReplicaUpdateRefs response
DRSUAPI      178 DRSUAPI_REPLICA_ADD response
DRSUAPI      386 DRSUAPI_REPLICA_DEL request
DRSUAPI      178 DRSUAPI_REPLICA_DEL response
DRSUAPI      194 DsUnbind request
DRSUAPI      194 DsUnbind response
```

Modifying CN=Configuration
(the nTDSA object)

Trigerring the replication

Using logs DCShadow can be detected when objects in the Configuration partition is added or when the computer object is changed. However a DC does not replicate the modifications immediately and regroup the changes when it replicates (a few minutes). As a consequence, the changes can be observed only on the DC attacked. This can be avoided by reusing a demoted DC (the information needed is already present in the configuration partition).

DCShadow does set the SPN GC/* or E3514235-4B06-11D1-AB04-00C04FC2DCD2/* on computers object (via DrsAddEntry)

Using LDAP cookie (LDAP_SERVER_DIRSYNC_OID) is also a way to be notified of LDAP modification

Using Audit Detailed Directory Service Replication events 4928 An Active Directory replica source naming context was established. and 4929 An Active Directory replica source naming context was removed.

Also @gentilkiwi is providing a splunk script for its detection: https://gist.github.com/gentilkiwi/dcc132457408cf11ad2061340dcb53c2