

https://blog.alsid.eu/dcshadow-explained-4510f52fc19d?gi=c426ac876c48

Go

JAN FEB 03 2018 MAR

Follow

1 capture 03 Feb 2018

Get started

About this capture

HOME NEWS STORIES SECURITY LABS KNOWLEDGE CENTER



Luc Delsalle

Follow

Security researcher focus on MS Active Directory Infrastructures • Former redteamer and systems security engineer

Jan 28 · 13 min read

DCShadow explained: A technical deep dive into the latest AD attack technique



On January 24th 2018, Benjamin Delpy and Vincent Le Toux, two security researchers, have released during the “BlueHat IL” security conference a


Never miss a story from **Alsid blog**, when you sign up for Medium. Learn more

GET UPDATES


03 Feb 2018




JAN 2017
FEB 03 2018
MAR 2019




Get started

About this capture

[HOME](#)
[NEWS STORIES](#)
[SECURITY LABS](#)
[KNOWLEDGE CENTER](#)


in this article, we will explain the technical foundations the attack relies on and discuss the consequences for the security of a running Active Directory infrastructure. Finally, we will shed a light on how blue teams could detect this kind of attack.

What is the DCShadow attack and why is it new?

The holy grail for red teamers or attackers willing to compromise an Active Directory infrastructure is to be able to obtain users and computers credentials without being noticed by detection countermeasures.

For this purpose, several attack techniques have been developed through time: LSASS injection, abusing Shadow Copy, NTFS volume parsing, ESE NT operations, sensitive attribute manipulation, etc. More details are available on the impressive synthesis from [ADSecurity.org](https://adsecurity.org).

Among all these noisy attacks, one of them is connected to the “[DCShadow](#)” attack. Introduced in 2015, the “[DCSync](#)” attack relies on the ability for the members of the Domain Admins or Domain Controllers groups to ask a domain controller (DC) for data replication (to achieve this task, the GetChangeAll right, granted by default to administrative accounts and DCs, was necessary). In fact, as described in the MS-DRSR specification for

Never miss a story from **Alsid blog**, when you sign up for Medium. Learn more



03 Feb 2018



JAN
2017

FEB
03
2018

MAR
2019



Get started for
About this capture

[HOME](#) [NEWS STORIES](#) [SECURITY LABS](#) [KNOWLEDGE CENTER](#) 

DCSync attack with mimikatz tool

One of the main limitation of the “DCSync” attack is the impossibility for an attacker to inject new objects in the targeted AD domain. Of course, this attacker could take ownership of an administrative account using the good old Pass-The-Hash technique and inject objects afterwards, but it requires more efforts, more steps, meaning a greater probability of being busted by blue teams. The “DCShadow” attack removes this limitation by *reversing* the “DCSync” attack paradigm.

Never miss a story from **Alsid blog**, when you sign up for Medium. [Learn more](#)


03 Feb 2018



JAN 2017

FEB 03 2018

MAR 2019



Get started for free

About this capture

[HOME](#) [NEWS STORIES](#) [SECURITY LABS](#) [KNOWLEDGE CENTER](#) 

The idea of a rogue domain controller is not new and has been mentioned multiple times in previous security publications but required invasive techniques (like installing a virtual machine with Windows Server) and to log on a regular domain controller to promote the VM into a DC for the targeted domain. Not very discrete.

Never miss a story from **Alsid blog**, when you sign up for Medium. Learn more


03 Feb 2018



JAN
2017

FEB
03
2018

MAR
2019



Get started for
About this capture

[HOME](#) [NEWS STORIES](#) [SECURITY LABS](#) [KNOWLEDGE CENTER](#) 

Understanding what a domain controller is

As described in MS-ADTS (Active Directory Technical Specification), Active Directory is a multi-master architecture relying on dedicated services. The DC is the service (or the server hosting this service depending on your point of view) which hosts the data store for AD objects and interoperates with other DCs to ensure that a local change to an object replicates correctly across all DCs.

When a DC is operating as RW DC, the DC contains full naming context (NC) replicas of the configuration, the schema, and one of the domain naming context of its forest. In this way, every RW DC holds all objects of a domain, including credentials and any kind of secrets (like private or session keys). As such, there is no need to remind that DCs are the one and only elements blue teams should be focused on protecting (Administrative accounts or permissions are just two of the many ways to access a DC).

Services provided by a domain controller

Describing in detail the technical ways and means of a DC could be complex and will not help to understand the purpose of the “DCShadow” attack. To

Never miss a story from **Alsid blog**, when you sign up for Medium. Learn more


03 Feb 2018



JAN 2017

FEB 03 2018

MAR 2019



Get started for

About this capture

[HOME](#) [NEWS STORIES](#) [SECURITY LABS](#) [KNOWLEDGE CENTER](#) 

- an authentication provider accessible through Kerberos, NTLM, Netlogon or WDigest protocols
- a configuration management system called GPO, relying on SMB and LDAP protocols
- an (optional) DNS provider used by clients to locate resources and support authentication

Synthesize of services provided by a DC

Focus on Active Directory replication

In addition to hosting these services, a domain controller in the making should be registered in the directory infrastructure to be accented by

Never miss a story from **Alsid blog**, when you sign up for Medium. [Learn more](#)


03 Feb 2018



JAN 2017

FEB 03 2018

MAR 2019



Get started for

About this capture

[HOME](#) [NEWS STORIES](#) [SECURITY LABS](#) [KNOWLEDGE CENTER](#) 

The major function of the KCC is to generate and maintain the replication topology for replication within and between sites. In other words, the KCC process elects which DC will communicate to which other to create an efficient replication process. Within a site, each KCC generates its own connections. For replication between sites, a single KCC per site generates all connections. The following schema illustrates the two kinds of replication.

Never miss a story from **Alsid blog**, when you sign up for Medium. [Learn more](#)


03 Feb 2018



JAN
2017

FEB
03
2018

MAR
2019



Get started for
f

About this capture

[HOME](#) [NEWS STORIES](#) [SECURITY LABS](#) [KNOWLEDGE CENTER](#) 

and ensures that domain controllers are not orphaned in the replication topology. Fun fact, historically Active Directory replication process could have been made through RPC (like DrsAddEntry) but also through SMTP (for the Schema and Configuration partition only)!

Registry key defining the replication time period

One part of the great job made by the researchers behind “DCShadow” was to identify the minimal set of changes required to inject a new server in the replication topology and therefore inject malicious information abusing this process while remaining stealthy.

Never miss a story from **Alsid blog**, when you sign up for Medium. [Learn more](#)


03 Feb 2018



JAN 2017

FEB 03 2018

MAR 2019



Get started for

About this capture

[HOME](#) [NEWS STORIES](#) [SECURITY LABS](#) [KNOWLEDGE CENTER](#) 

aims to register new domain controllers to inject malicious AD objects and so create backdoors or any kind of illegitimate access or right. To reach this goal, “DCShadow” attack must modify the targeted AD infrastructure database to authorize the rogue server to be part of the replication process.



Register a new domain controller

As mentioned in the MS-ADTS specification, a domain controller is represented in the AD database by an object of class nTDSDSA that is always located in the configuration naming context of a domain. More precisely, each DC is stored in the sites container (object class sitesContainer), as a child item of a server object.

Never miss a story from **Alsid blog**, when you sign up for Medium. [Learn more](#)






1 capture
03 Feb 2018



JAN
2017

FEB
03
2018

MAR
2019



Get started for
f

About this capture


[HOME](#) [NEWS STORIES](#) [SECURITY LABS](#) [KNOWLEDGE CENTER](#) 

In blue, the containers storing the NTDS-DSA object. In red, the object itself.



A quick look at the schema shows that NTDS-DSA objects can only be created as children of server objects, which in turn can only be part of organization or server objects:

- the server objects can only be stored in serversContainer objects which are only found in the Configuration NC.
- the organization objects can only be stored in locality, country or domainDNS objects which can be found in the domain NC

Never miss a story from **Alsid blog**, when you sign up for Medium. [Learn more](#)





1 capture
03 Feb 2018



JAN
2017

FEB
03
2018

MAR
2019



Get started for
f

About this capture

[HOME](#) [NEWS STORIES](#) [SECURITY LABS](#) [KNOWLEDGE CENTER](#) 

The schema indicates where ntds-dsa objects can be created

In this way, domain controllers (nTDSDSA objects) can only be created in the Configuration or Domain NC. In practice, it seems only the nTDSDSA objects stored in the site container (sitesContainer object) are taken into consideration. As the KCC relies on the site information to compute its replication topology, it seems logical that only these objects are used. Note that creating an nTDSDSA object is not possible using the LDAP protocol.

You would have understood it, the main action made by the “DCShadow” attack is to create a new server and nTDSDSA objects in the Configuration partition of the schema. Doing so provides the ability to generate malicious replication data and inject them to other domain controllers.

Never miss a story from **Alsid blog**, when you sign up for Medium. [Learn more](#)




[HOME](#) [NEWS STORIES](#) [SECURITY LABS](#) [KNOWLEDGE CENTER](#) 

only BUILTIN\Administrators, DOMAIN\Domain Admins, DOMAIN\Enterprise Admins and NT AUTHORITY\SYSTEM have control rights on the targeted containers.

Never miss a story from **Alsid blog**, when you sign up for Medium. [Learn more](#)



1 capture
03 Feb 2018



JAN
2017

FEB
03
2018

MAR
2019



Get started for free

About this capture

HOME NEWS STORIES SECURITY LABS KNOWLEDGE CENTER  gain privileges but

give them another solution to become persistent or to make illegitimate actions in a directory infrastructure. It should thus be added in the category of another sneaky AD persistence trick and not as a vulnerability to fix.

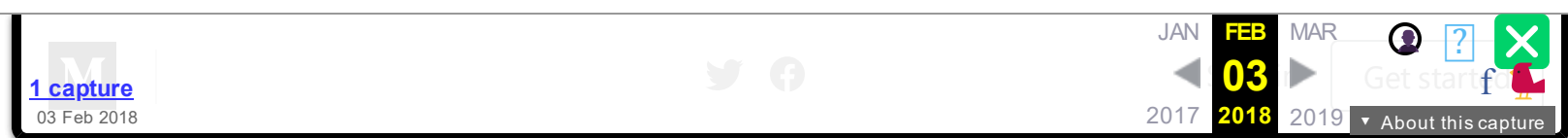
Trust the new domain controller

As described in the previous paragraph, the “DCShadow” attack relies on the addition of a new nTDSDSA object in the Configuration partition to register itself as a new member of the replication process. However, adding this sole object is not enough to allow our rogue server to initiate replication. In fact, to be part of the replication process we need to take care of two requirements:

- be trusted by other servers, meaning that we need to have valid authentication credential.
- provide authentication support to let other DCs to connect to our rogue server when we need to replicate data.

By using a valid computer account, a rogue server can be treated as a trustworthy AD server. The Kerberos SPN attributes will provide authentication support for other DCs. Therefore, every nTDSDSA object is linked to the computer object through the serverReference attribute.

Never miss a story from **Alsid blog**, when you sign up for Medium. Learn more



The serverReference attribute acts as the link between a nTDSDSA object and its related computer object

Despite the theoretical possibility to achieve this with a user account, it seems much easier and stealthy to use a computer account. In fact, it will be automatically registered in the DNS infrastructure (which will allow other DCs to locate our resource), will natively have the required attributes set and will have its authentication secret automatically managed.

In this way, the “DCShadow” attack will use a legitimate computer account to be able to authenticate to other DCs. Although the computer object and the nTDSDSA object will bring the ability to authenticate to other DCs, the “DCShadow” attack still needs to let other DCs to connect to the rogue server to replicate illegitimate information from it.

This last requirement is fulfilled using the Kerberos Service Principal Name

Never miss a story from **Alsid blog**, when you sign up for Medium. Learn more

03 Feb 2018



JAN 2017

FEB 03 2018

MAR 2019



Get started for...

About this capture

[HOME](#) [NEWS STORIES](#) [SECURITY LABS](#) [KNOWLEDGE CENTER](#) 

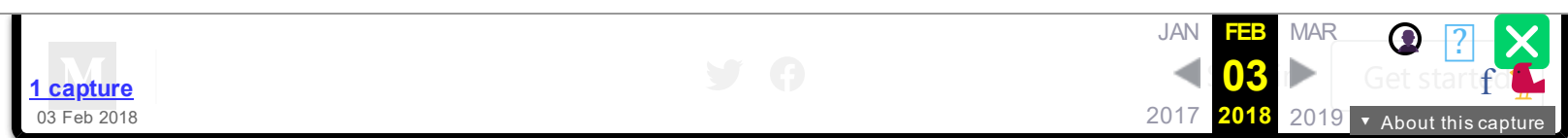
One of the key findings of Benjamin Delpy and Vincent Le Toux was to isolate the minimum set of SPNs required for the replication process to go through. The results of their studies show that two SPNs are required to let another DC to connect to the rogue server:

- the DRS service class (which has the well-known GUID E3514235–4B06–11D1–AB04–00C04FC2DCD2)
- the Global Catalog service class (which has the string “GC”)

For example, the two SPNs required by our rogue server (named “roguedc” with the DSA GUID 8515DDE8–1CE8–44E5–9C34–8A187C454208 in the alsid.corp domain) are as follows:

```
E3514235-4B06-11D1-AB04-00C04FC2DCD2/8515DDE8-1CE8-44E5-9C34-8A187C454208/alsid.corp
GC/roguedc.alsid.corp/alsid.corp
```

Never miss a story from **Alsid blog**, when you sign up for Medium. [Learn more](#)



HOME NEWS STORIES SECURITY LABS KNOWLEDGE CENTER 🔍

A rogue computer account having the SPN of a DC

When triggering its attack, “DCShadow” will set those two SPNs to its targeted computer account. More precisely, the SPNs will be set using the DRSAddEntry RPC function as described in the CreateNtdsDsa function documentation (more details about MS-DRSR RPC are provided in the next section).

For now, we can register our rogue domain controller into the replication process and be authenticated by another DC. The remaining step is now to force the DC to initiate the replication process with our malicious data.

Never miss a story from **Alsid blog**, when you sign up for Medium. [Learn more](#)


03 Feb 2018



JAN
2017

FEB
03
2018

MAR
2019



Get started for
About this capture

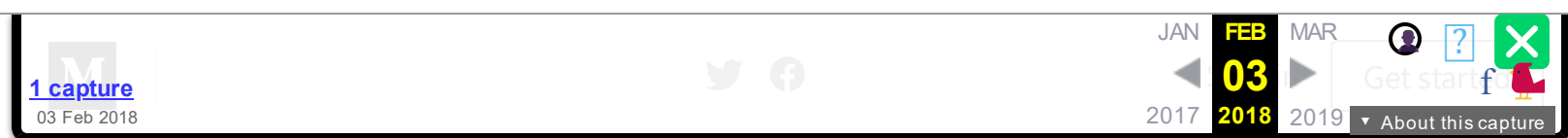
[HOME](#) [NEWS STORIES](#) [SECURITY LABS](#) [KNOWLEDGE CENTER](#)  [DCS infrastructure.](#)

To serve illegitimate data, the rogue domain controller will have to implement the minimal set of RPC functions required by the MS-DRSR specifications: IDL_DRSBind, IDL_DRSUnbind, IDL_DRSGetNCChanges, IDL_DRSUpdateRefs. The IDL of this function are provided by Microsoft in its open specifications and are now implemented into Benjamin Delpy's Mimikatz tool.

The final step of the “DCShadow” attack is to trigger the replication process. To do so, two strategies can be conducted:

- Wait for the KCC process of another DC to initiate the replication process (requires 15 minutes delay)
- Force the replication by invoking the DRSReplicaAdd RPC function. It will change the content of the repsTo attribute which will start an immediate data replication.

Never miss a story from **Alsid blog**, when you sign up for Medium. [Learn more](#)



[HOME](#) [NEWS STORIES](#) [SECURITY LABS](#) [KNOWLEDGE CENTER](#) [Q](#)


Extract of the MS-DRSR specification describing the DRSReplicaAdd IDL



Forcing the replication with the IDL_DRSReplicaAdd RPC is the last step taken during a “DCShadow” attack. It allows to inject arbitrary data into a targeted AD infrastructure. Doing so, it becomes trivial to add any backdoor in the domain (by adding new member on an administrative group, or by setting SID history on a controlled user account for example).

Process summary

The following chart summarizes the different operations achieved during a “DCShadow” attack.

Never miss a story from **Alsid blog**, when you sign up for Medium. [Learn more](#)




1 capture
03 Feb 2018



JAN
2017

FEB
03
2018

MAR
2019


Get started for
About this capture

[HOME](#) [NEWS STORIES](#) [SECURITY LABS](#) [KNOWLEDGE CENTER](#) 


DCShadow attack synthetized process

. . .



The consequences of “DCShadow” for blue team strategies

As explained in the [research paper](#), blue teams in charge of AD security monitoring usually rely on event log collection. Computers that are members of a domain are configured to push their logs to a central [SIEM](#) to be analyzed.

Never miss a story from **Alsid blog**, when you sign up for Medium. [Learn more](#)






1 capture
03 Feb 2018



JAN
2017

FEB
03
2018

MAR
2019



Get started for free

About this capture

[HOME](#) [NEWS STORIES](#) [SECURITY LABS](#) [KNOWLEDGE CENTER](#) 

A simplified SIEM architecture pushing event log through WinRM Event Forwarding protocol


The first problem with this approach is that only legitimate computers send their logs to the log collector. During the “DCShadow”, the event logs related to the injection of new data are only created on the attacker’s machine, which will obviously not signal itself by sending events to the SIEM. In this way, the “DCShadow” attack can be stealthy as only a few event logs will be generated by legitimate computers.

In fact, this article explains that several prerequisites actions should be made before injecting the rogue data information into the targeted AD. Unfortunately, the AD modifications involved in setting-up a rogue DC are rarely included in logging policies. For example, Configuration NC changes

Never miss a story from **Alsid blog**, when you sign up for Medium. [Learn more](#)



03 Feb 2018



JAN

FEB

MAR

◀


03

▶

2017

2018

2019



Get started for free

About this capture


[HOME](#) [NEWS STORIES](#) [SECURITY LABS](#) [KNOWLEDGE CENTER](#) 

Blue teams need a complete redesign of their strategy and shift their focus from log analysis to AD configuration analysis. The naïve approach would be to monitor replications (DrsGetNCChanges RPC changes). In fact, by default, a SACL entry set on the root object of the domain logs the use of extended rights except for domain controllers. In this way, a replication with a user account or non-DC machine must be pretty easy to identified. However, we do not feel this method is the most efficient one. From our point view, three strategies should be implemented to detect “DCShadow” attacks:

1. The Configuration partition of the schema should be looked at carefully. nTDSDSA objects in the sites container should be matched with regular domain controllers in the Domain Controllers organizational unit (or better: a list of known DC manually maintained by the administration team). Any object showing up in the first but not in the second should be investigated. Please notice that the rogue nTDSDSA object is removed right after the publication of the illegitimate objet. To be efficient, detection measure should be able to catch object creation.
2. As shown in the previous paragraphs, DCs need an authentication provider. To be able to push changes, a rogue DC will need to have one accessible through Kerberos, with a specific service. In practical terms, it means having a Service Principal Name (SPN) beginning with the “GC/”

Never miss a story from **Alsid blog**, when you sign up for Medium. [Learn more](#)





JAN **FEB** MAR
2017 **03** 2018 2019
Get started
About this capture

HOME NEWS STORIES SECURITY LABS KNOWLEDGE CENTER 🔍

3. Using “DCShadow” requires an attacker to have elevated privileges.

Analyzing and monitoring the permissions present in the Configuration partition will allow blue teams to make sure nobody is able to alter it except legitimate administrators. Any DACL granting access to a non-privileged entity can also be a sign of a possible backdoor.

...

Final thoughts


What is most important to take away from this analysis is that “DCShadow” is not a vulnerability but an innovative way to inject illegitimate data into an AD infrastructure.

No unprivileged attacker will ever be able to use it to escalate their privileges and gain administrative access to your AD using “DCShadow”. Bottom-line is: if your AD is properly configured and secured, you do not need to take any urgent actions.

“DCShadow” does not require any urgent patching campaign nor special configuration to be applied, this has nothing to do with WannaCry/NotPetya incident response.

Not being a vulnerability, “DCShadow” will not be patched by a Microsoft

Never miss a story from **Alsid blog**, when you sign up for Medium. Learn more



03 Feb 2018



JAN 2017

FEB 03 2018

MAR 2019



Get started

About this capture

[HOME](#) [NEWS STORIES](#) [SECURITY LABS](#) [KNOWLEDGE CENTER](#) 

broke, don't fix it. AD is not broken.

However, the fact that a new attack method is publicly available for anyone to use needs to be considered. It offers an extremely stealthy way for privileged attackers to perform actions, so detection strategies should be updated to reflect this new threat. Traditional event log analysis methods will probably fail to detect “DCShadow” usage. To efficiently detect this attack technique, it requires being able to continuously monitor the AD database to isolate illegitimate changes. This is what we do at Alsid and we are very proud to already protect our customers against this attack. For more information on how we tackle this challenge, head to www.alsid.eu.

Active Directory

Cybersecurity

Dcshadow

Mimikatz

Information Security

One clap, two clap, three clap, forty?

By clapping more or less, you can signal to us which stories really stand out.



114



Luc Delsalle

Security researcher
focus on MS Active
Directory
Infrastructures ·
Former redteamer


Follow

Alsid blog

Detect directory
breaches before
attackers do.



Follow

Never miss a story from **Alsid blog**, when you sign up for Medium. Learn more



1 capture

03 Feb 2018



JAN

◀

2017

FEB




03

2018

MAR

▶

2019



Get started for

▼ About this capture

HOME NEWS STORIES SECURITY LABS KNOWLEDGE CENTER 🔍

Never miss a story from **Alsid blog**, when you sign up for Medium. [Learn more](#)