
ALSID

Uncover DCShadow

Efficiently detect latest Active Directory attacks

Tuesday, May 29th 2018

Romain COLTEL – Senior Security Researcher
Luc DELSALLE – Chief Technology Officer

Who we are

Alsid security team

Romain COLTEL

Senior Security Researcher

Former senior security auditor specialized in red-teaming missions

During his spare time Romain is teaching the well-received SANS SEC660 in France

Maintainer of various security software as Dislocker or the AES-XEX and XTS modes for the mbedTLS library.

romain.cotel@alsid.eu

@aorimn

Luc DELSALLE

Chief Technology Officer

Five years leading large-scale cyber-defense operations and red-teaming governmental entities at the ANSSI.

Former senior security researcher in Microsoft technologies Published several scientific papers.

Academic professor in several engineering schools and security related masters (EPITA, ENSIIE, SecureSphere, etc.)

luc.delsalle@alsid.eu

@ldelsalle

Introducing Alsid

Efficiently protect directory infrastructures

Design innovative solutions to help companies secure their Active Directory or Samba services

Provide field-experienced products to make companies resilient against advanced cybersecurity threats

A technical expertise recognized worldwide and awarded by numerous prestigious prizes

Today agenda

1. The DCShadow attack
2. Consequences for blue teams strategies
3. Designing an efficient detection approach
4. Introducing Uncover-DCShadow
5. Final thoughts
6. Q & A

ALSID

Introducing DC Shadow attack

The latest post-exploitation attack against Active Directory

On January 24th 2018, Benjamin Delpy and Vincent Le Toux have released during the BlueHat IL security conference a new attack technique against Active Directory infrastructure.

Named “DCShadow”, this attack allows an attacker having the appropriate rights to create a rogue domain controller able to replicate malicious objects into a running AD infrastructure.

Various attack techniques throughout history.

LSASS injection, abusing Shadow Copy, NTFS volume parsing, ESE NT operations, sensitive attribute manipulation, etc.

Focus on the DCSync attack.

Members of the Domain Admins or Domain Controllers groups can ask a domain controller (DC) for **data replication.**

Problem with the DCSync attack: it cannot inject new objects.

DCSync attack cannot inject new objects in the targeted AD domain, it only gets existing objects.

Reversing the paradigm.

DCShadow don’t ask for data replication, it enforces a new one.

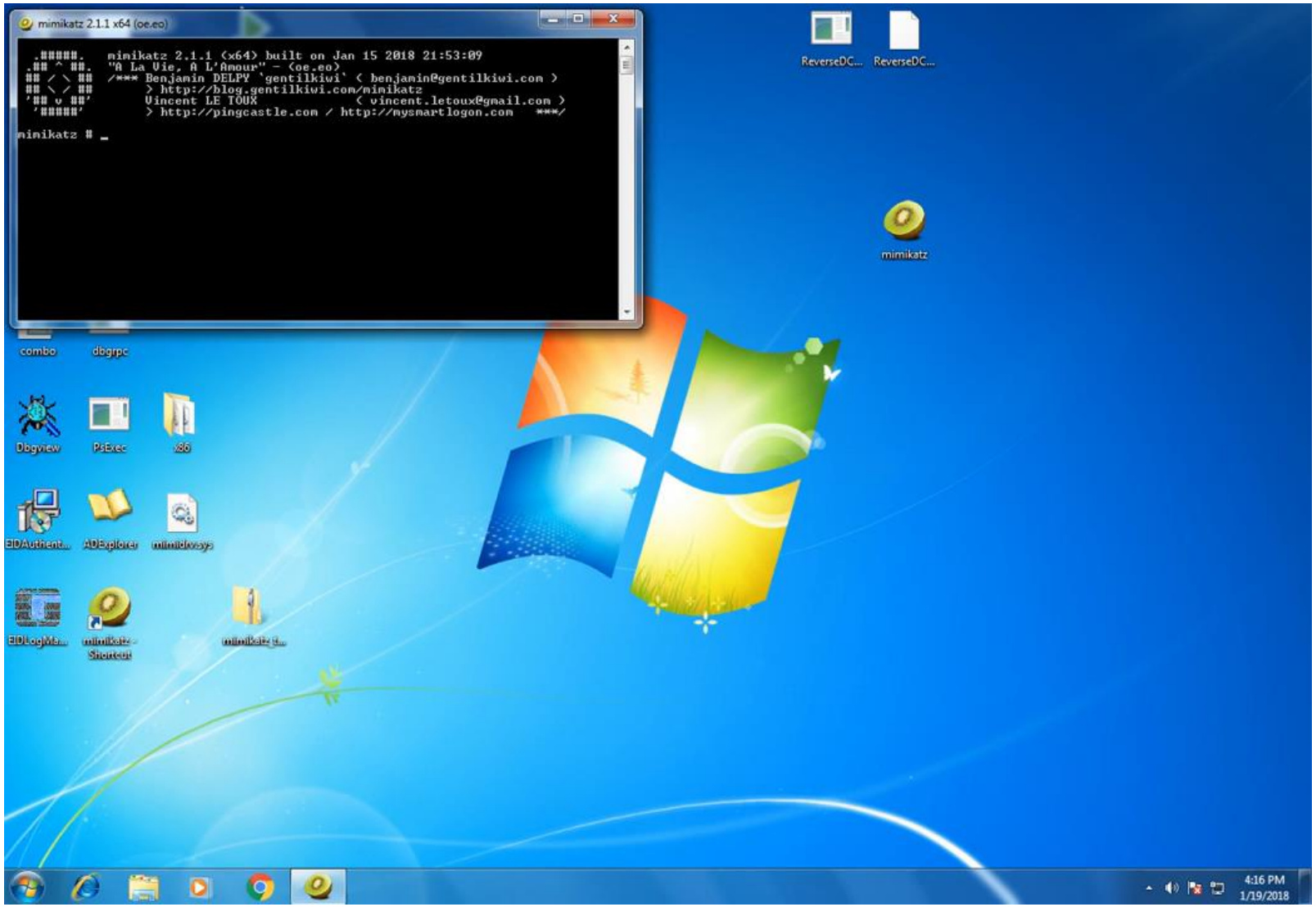
Promoting a regular, new DC is very noisy.

Install a new machine, enter the domain, promote to DC: lot of logs.

Post-exploitation attack.

DCShadow requires administrative rights, thus being a new way to inject rogue objects (backdoor, new users, etc.) not a privilege escalation technique.

DC Shadow in action



Understanding what a domain controller is

A database engine
NTDS through LDAP and RPC

Host the domain information and configuration using abstract objects.
Is accessible through the LDAP and RPC protocols.

An authentication service
MS Kerberos

Implement a single-sign-on authentication protocol using the ticket paradigm.
Kerberos is used each time a user authenticates to a service (website, mailbox, file share, etc.)

A policy service
Group Policy engine (SMB/LDAP)

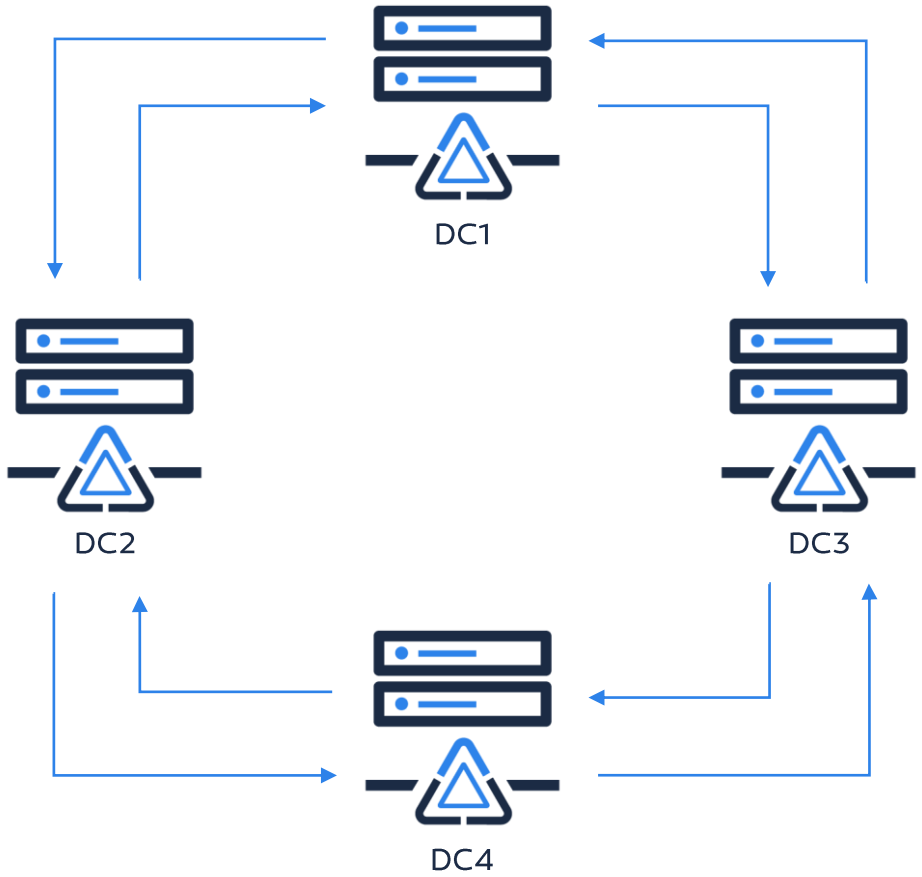
Manage resources (users, computers, services) of a domain.
Security policies are deployed using GPOs, a combination of SMB files and LDAP objects.

A name resolution service
DNS infrastructure

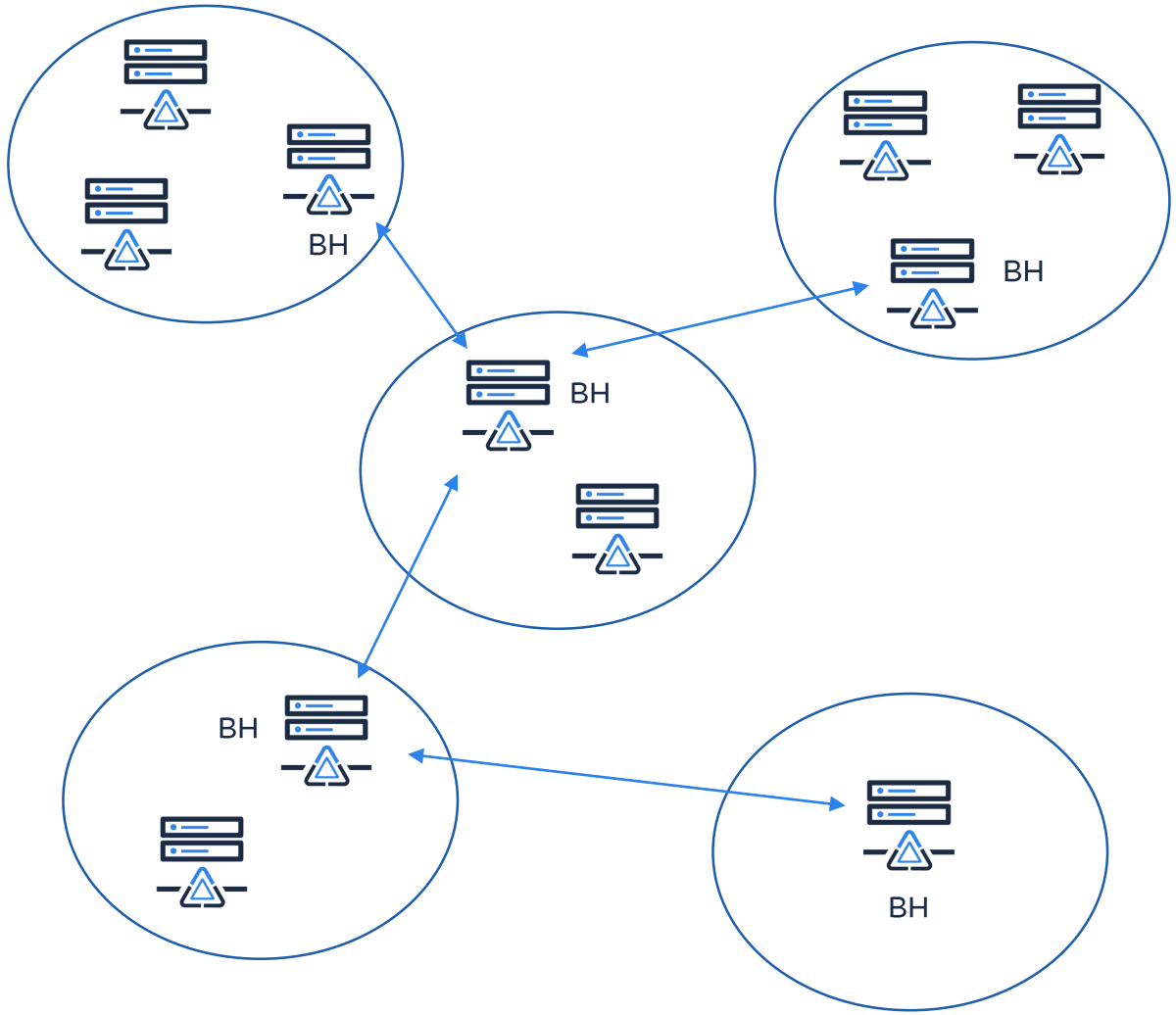
Locate the resources in the corporate network and compute the AD topology (computer.domain.corp, DOMAIN\user, user@domain.corp).

Replication and topology at a glance

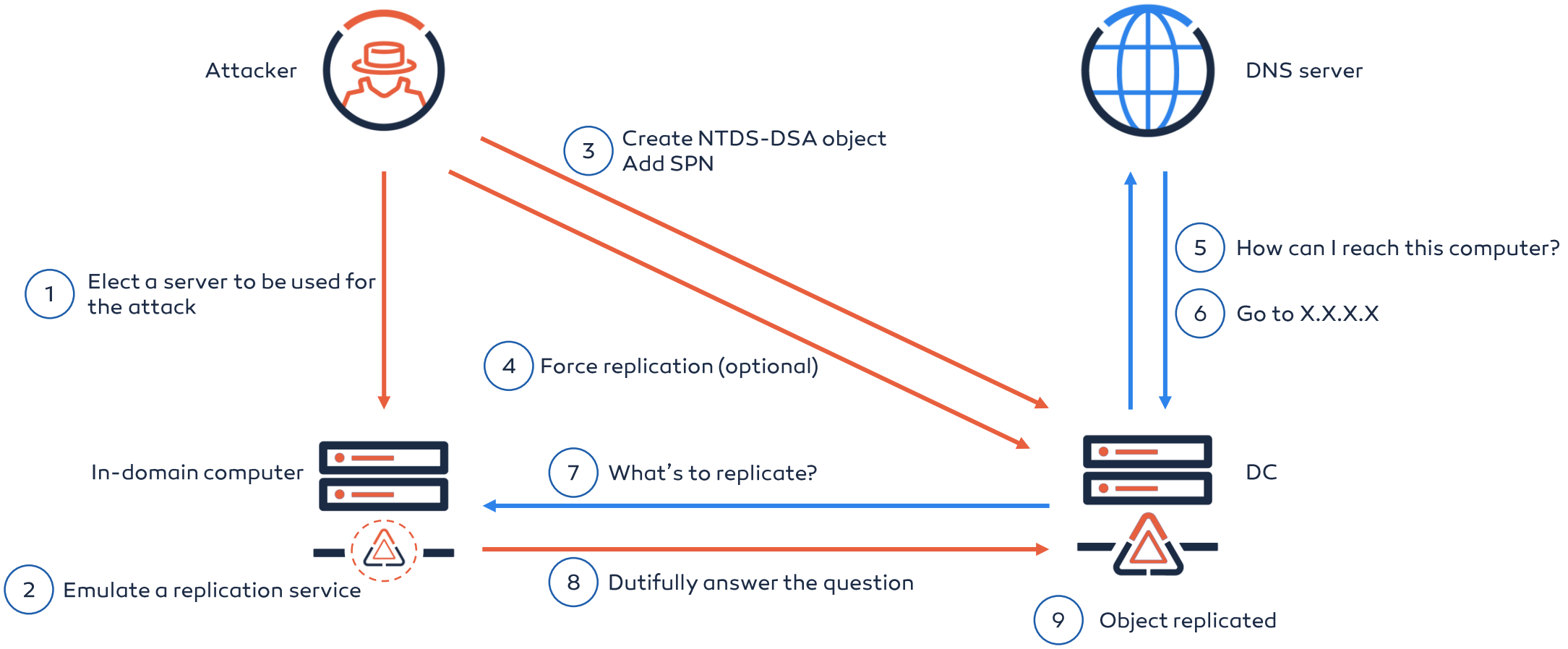
Intra-site replication



Inter-sites replication



How DC Shadow actually works



DCShadow process summary

1. Obtain highly privileged account
Like a domain or enterprise admins. account

2. Set required SPNs on a computer account
The DRS and GC SPNs are mandatory

3. Create the NTDS-DSA object
In the Configuration partition, in a server container

4. Impersonate environment as the computer account
Use the authentication context of the computer holding the replication SPNs

5. Start the appropriate RPC server
Legitimate DCs need to invoke several RPCs (like `DrsGetNCChanges`)

6. Force the replication process
Call `DrsReplicaAdd` on an impersonated environment

7. Profit
Play with AD objects to create and hide backdoors

Why DC Shadow requires to rethink detection strategies

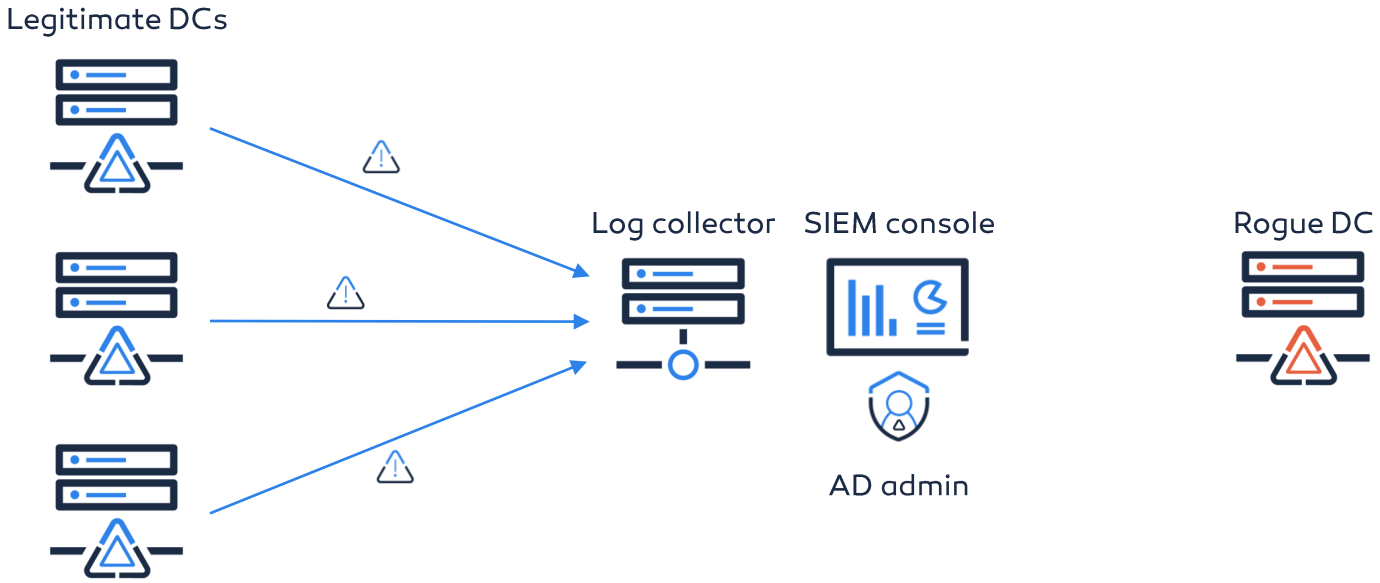
Most of the discriminating events of the attack are held by the rogue DC

Only legitimate computers send their logs to the log collector.

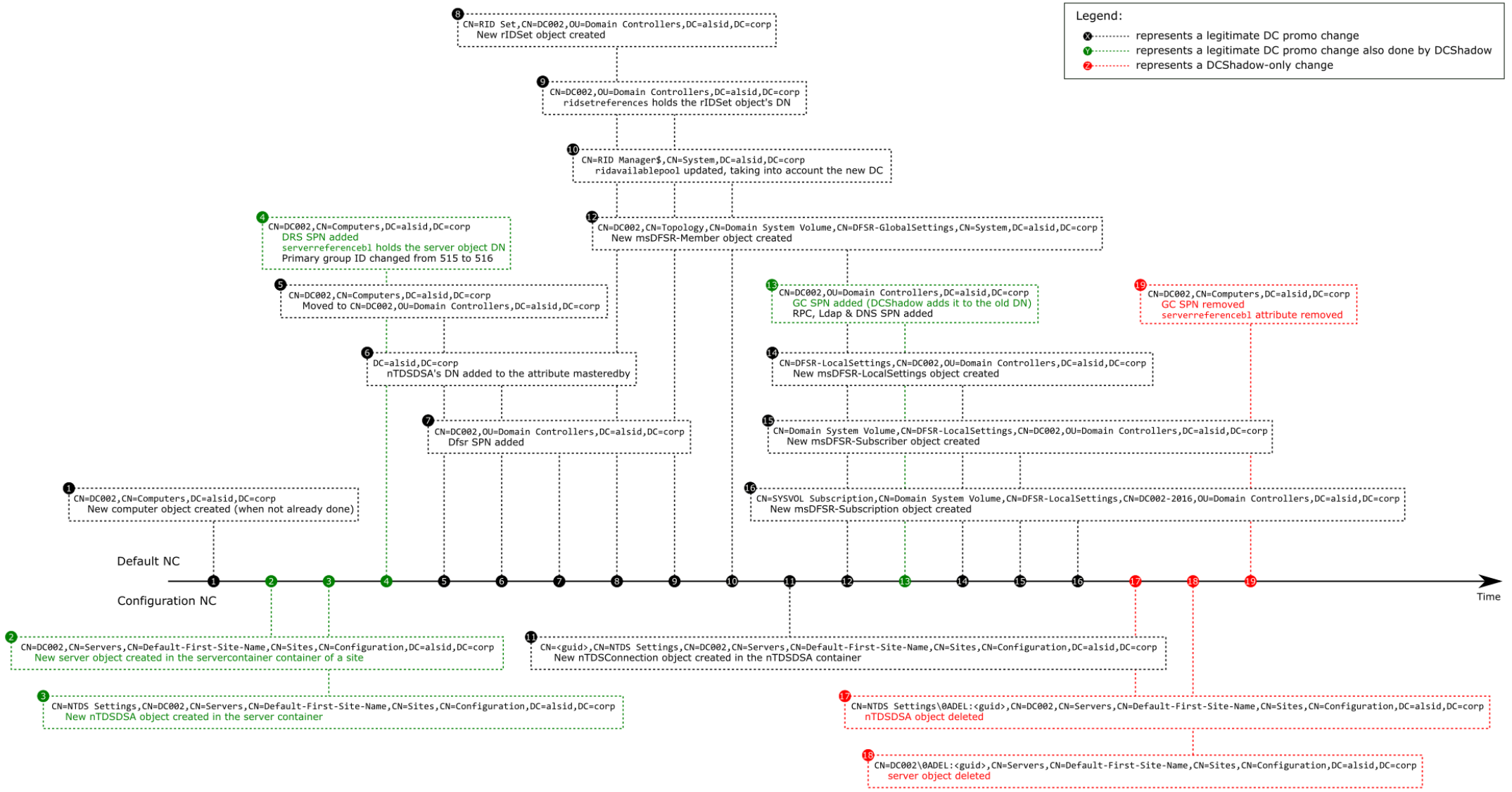
Event logs related to the injection of new data are only created on the attacker's machine.

The DCShadow attack can be stealthy as only a few event logs will be generated by legitimate computers.

To detect DCShadow, Blue teams need to shift their focus from log analysis to AD configuration analysis.



Comparison between legitimate DC promotion and a DC Shadow attack



Key differences between DCShadow and legitimate DCPromo

Regular DC promotion

Create a computer object

Move computer object to DC OU

Add NTDSDSA object information into root domain object

Add Dfsr SPN to the computer object

Include computer object into the KCC replication policy

Create NTDSConnection under the NTDSDSA object

DCShadow-only events

NTDSDSA object deleted

Server object deleted

GC SPN removed from the computer object

All those differences makes the detection possible

Challenge: detect all these changes, made in a split of a second

Efficiently detect DCShadow attacks

Monitor NTDS-DSA objects.

nTDSDSA objects in the sites container should be matched with regular domain controllers in the Domain Controllers organizational unit.

Even better: a list of known DC should be manually maintained by the administration team.

Detect the creation of specific SPNs.

Computer objects having the GC or DRS (E3514235–4B06–11D1-AB04–00C04FC2DCD2) SPNs and not being stored in the DC OU should be carefully investigated.

Isolate abnormal replica sources on specific events.

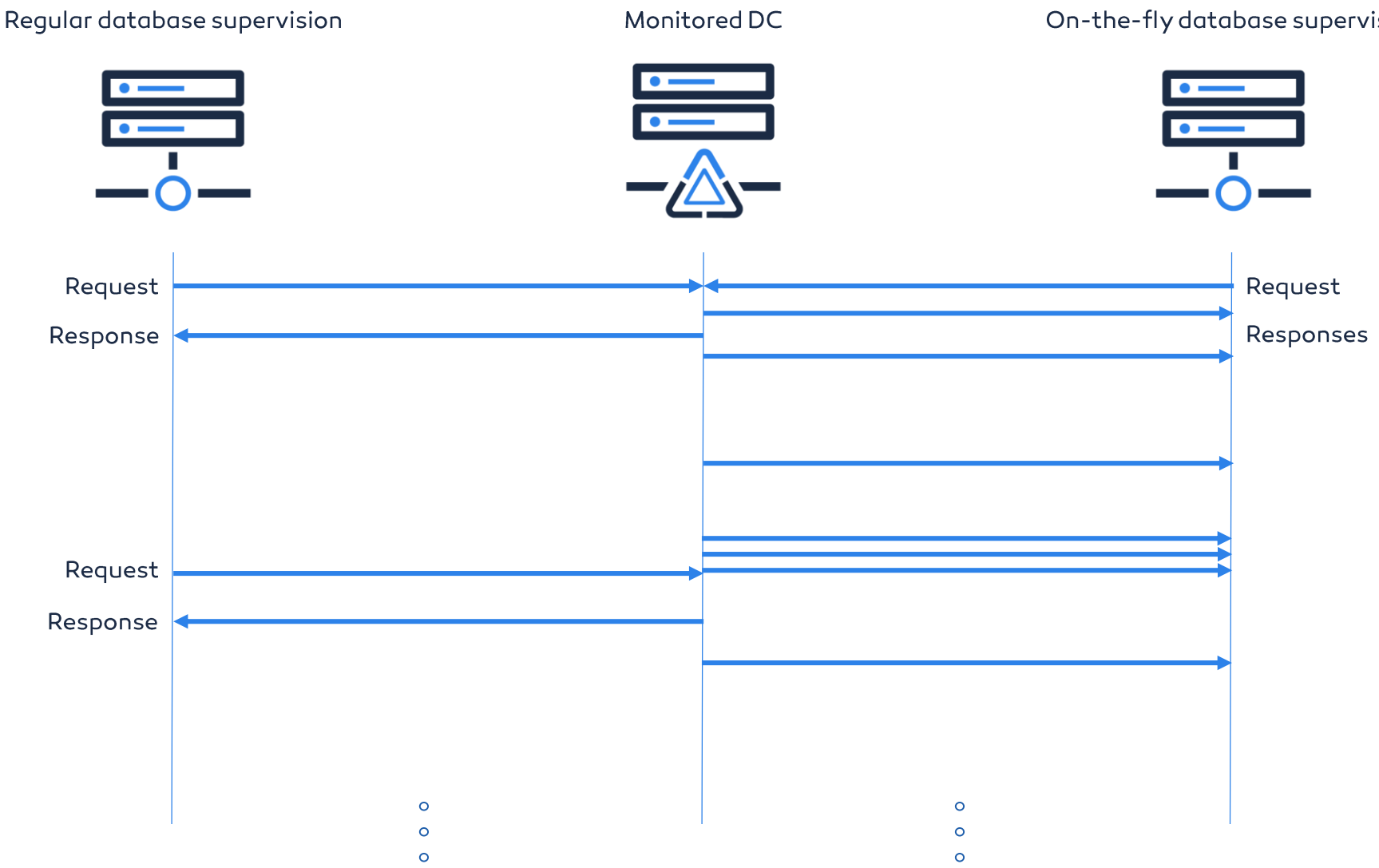
Using advanced logging features, it is possible to generate event ID 4929 (from “Microsoft Windows security” provider) and isolate abnormal replication sources in the “Source address” field.

Bonus: prevent privilege escalations.

Using DCShadow requires an attacker to have elevated privileges.

No need to detect DCShadow if you are able to maintain strong security boundaries on your AD.

Introducing asynchronous notifications

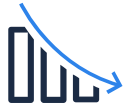


Benefits of LDAP asynchronous notifications

Continous monitoring.

Detect the issue as soon as it appears.

Reduced number of changes to investigate.



At the end of the day, reduced costs.

Presenting Uncover-DCShadow

Detect DCShadow attacks using asynchronous notifications

UncoverDCShadow is a proof-of-concept developed in PowerShell, designed to help blue teams detect the use of the DCShadow attack on their Active Directory infrastructure.

These helpers have been designed to illustrate how security monitoring can be achieved without requiring network tap or event log forwarding.

Open-source tool.

The software can be downloaded on Alsid GitHub repository: https://github.com/AlsidOfficial/UncoverDCShadow/

Released 7 days after attack publication.

Despite the fact the attack is new, the foundation elements (replication process) are well-known and documented.

Rely on LDAP asynchronous notifications.

The tool uses the same principles as described in this slideshow.

Implement DCShadow attack detection.

The tool can forward detection events to a SIEM to industrialize the detection of this kind of attack.

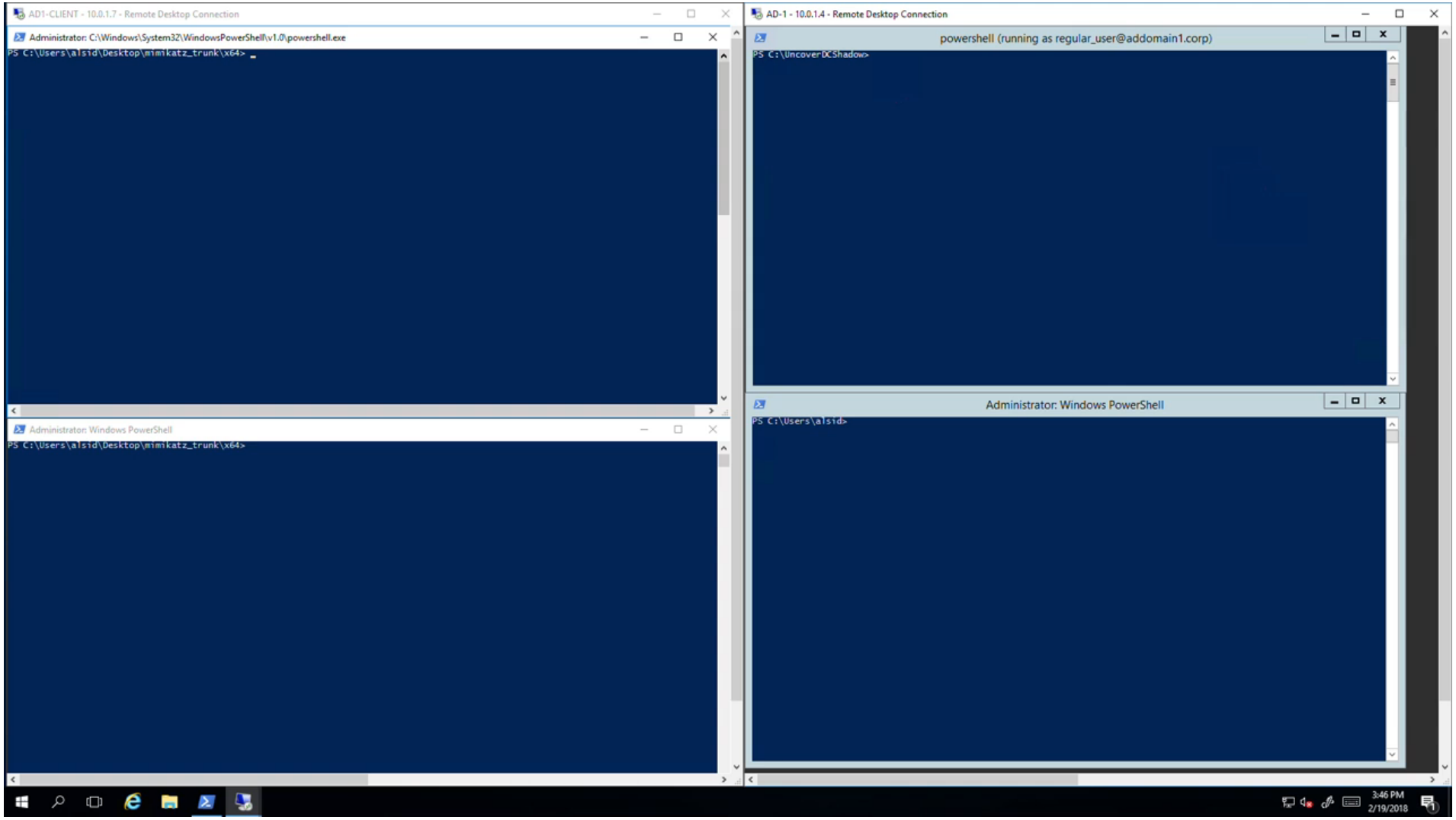
Can monitor any directory change.

Using advanced options, the tool can listen to pretty much any kind of change.

Part of Alsid commercial product.

DCShadow is one of the 50+ attacks scenario detected by Alsid's product.

Uncover-DCShadow in action



Takeaways

DCShadow is not a vulnerability but an innovative way to inject illegitimate data.

No unprivileged attacker will ever be able to use it to escalate their privileges.

Not being a vulnerability, DCShadow will not be patched by a Microsoft update.

However, it offers many opportunities to mess with the AD database (more to come during BlackHat 2018, « So I became a domain controller »).

References and documentation

What can make your million dollar SIEM go blind?

V. LE TOUX & B. DELPY BlueHat IL conference

http://www.bluehatil.com/files/Active%20Directory%20What%20Can%20Make%20Your%20Million%20Dollar%20SIEM%20Go%20Blind.pdf

Uncover-DCShadow

Alsid technical article

https://blog.alsid.eu/dcshadow-explained-4510f52fc19d

Uncover-DCShadow

Alsid Github repository

https://github.com/AlsidOfficial/UncoverDCShadow

Active Directory Technical Specification

Microsoft Open Specification for AD

https://msdn.microsoft.com/en-us/library/cc223122.aspx

Directory Replication Service (DRS) Remote Protocol

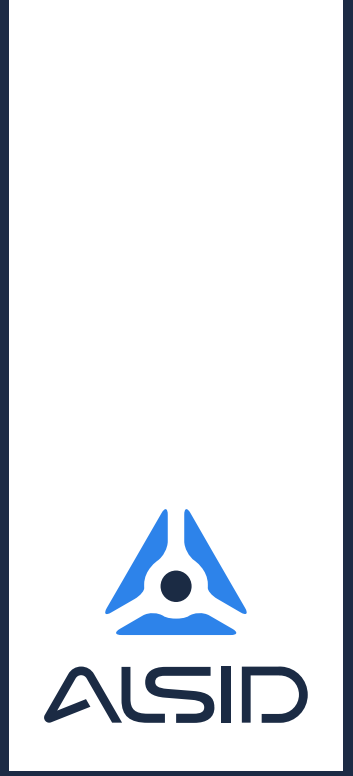
Microsoft Open Specification for Replication services

https://msdn.microsoft.com/en-us/library/cc228086.aspx

Mimikatz Source Code

B. DELPY Github repository

https://github.com/gentilkiwi/mimikatz



hello@alsid.eu

alsid.eu

AlsidOfficial

@AlsidOfficial

THANK YOU!