



# ADTimeline

## Active Directory forensics with replication metadata

<https://github.com/ANSSI-FR/ADTimeline>



# Whoami

```
Administrateur : Windows PowerShell
PS C:\> Get-ADUser leonard.savina -properties * | fl SID, Giv*, sn, Compa*, Dep*, Cit*, Ema*, alt*, bus*

SID                : S-1-5-21-3634504526-1236365413-3814638018-3121
GivenName          : Leonard
sn                 : Savina
Company            : ANSSI
Department         : CERT-FR
City               : Paris
EmailAddress       : leonard.savina@ssi.gouv.fr
altSecurityIdentities : {C=US/O=Twitter Inc./CN=@ldap389}
businessCategory   : {Active Directory, Exchange}

PS C:\> █
```

<https://github.com/ANSSI-FR/ADTimeline>

# **ACTIVE DIRECTORY AND REPLICATION METADATA.**

# Active Directory - Overview

## Rare problem blamed for Glasgow health board IT crash

8 November 2013



A "rare corruption" in a vital computer programme has been blamed for a systems crash which hit hospital appointments at Scotland's largest health board.

An independent investigation into the NHS Greater Glasgow and Clyde (GGC) crash, however, could not establish "the exact root cause of the failure".

The report makes eight recommendations for improvements.

The systems crash, between 1 and 3 October, resulted in 709 patients having hospital appointments postponed.

The independent investigation into the system failure was commissioned by NHS GGC and the Scottish government.

It confirmed that the source of the problem related to a rare corruption in a programme known as **Active Directory**.



## LockerGoga Ransomware Sends Norsk Hydro Into Manual Mode

By Ionut Ilascu

March 19, 2019 09:48 AM 1

### NorCERT warns companies on LockerGoga attack

According to media outlet NRK, NorCERT alerted a number of partners about LockerGoga ransomware, warning that Norsk Hydro is one of its victims.

The notification from Norway's cybersecurity body says that the attack involved **Active Directory** used for authenticating and authorizing all users and systems on a Windows domain type network.

"NorCERT warns that Hydro is exposed to a LockerGoga attack. The attack was combined with an attack on Active Directory (AD)," reads the alert.

3,421 views | Mar 27, 2018, 10:26am

## Increased Hacker Attacks On Active Directory



Christopher P. Skrou  
I focus on the Intersection

PCWorld  
FROM IDG

NEWS REVIEWS HOW-TO VIDEO DEALS BUSINESS LAPTOPS SMARTPHONES HARDWARE SECURITY

Privacy Encryption Antivirus

AdChoices

Open VPN

Cyber Breach

Data Breach

Home / Security

NEWS

## Hacker: This is how I broke into Hacking Te

Breach of surveillance vendor highlights lessons for companies



By Lucian Constantin

Romania Correspondent, IDG News Service | APRIL 18, 2016 07:12 AM PT

Using the password on the **live server** allowed the hacker to extract additional credentials, including the one for the Windows domain admin. The lateral movement through the network continued using tools like PowerShell.

## The Untold Story of NotPetya, the Most Devastating Cyberattack in History

get to work, do whatever needs to be done," he says.

Early in the operation, the IT staffers rebuilding Maersk's network came to a sickening realization. They had located backups of almost all of Maersk's individual servers, dating from between three and seven days prior to NotPetya's onset. But no one could find a backup for one crucial layer of the company's network: its domain controllers, the servers that function as a detailed map of Maersk's network and set the basic rules that determine which users are allowed access to which systems.

SHARE

SHARE 20578

TWEET

COMMENT

# Active Directory - Overview

Active Directory is often the core of the IT infrastructure, it is installed on domain controllers (DCs) fulfilling the following roles:

- > LDAP directory.
- > DNS service.
- > NTP service.
- > Authentication services (Kerberos and NTLM).
- > Windows clients configuration with GPOs.

# Active directory - Replication

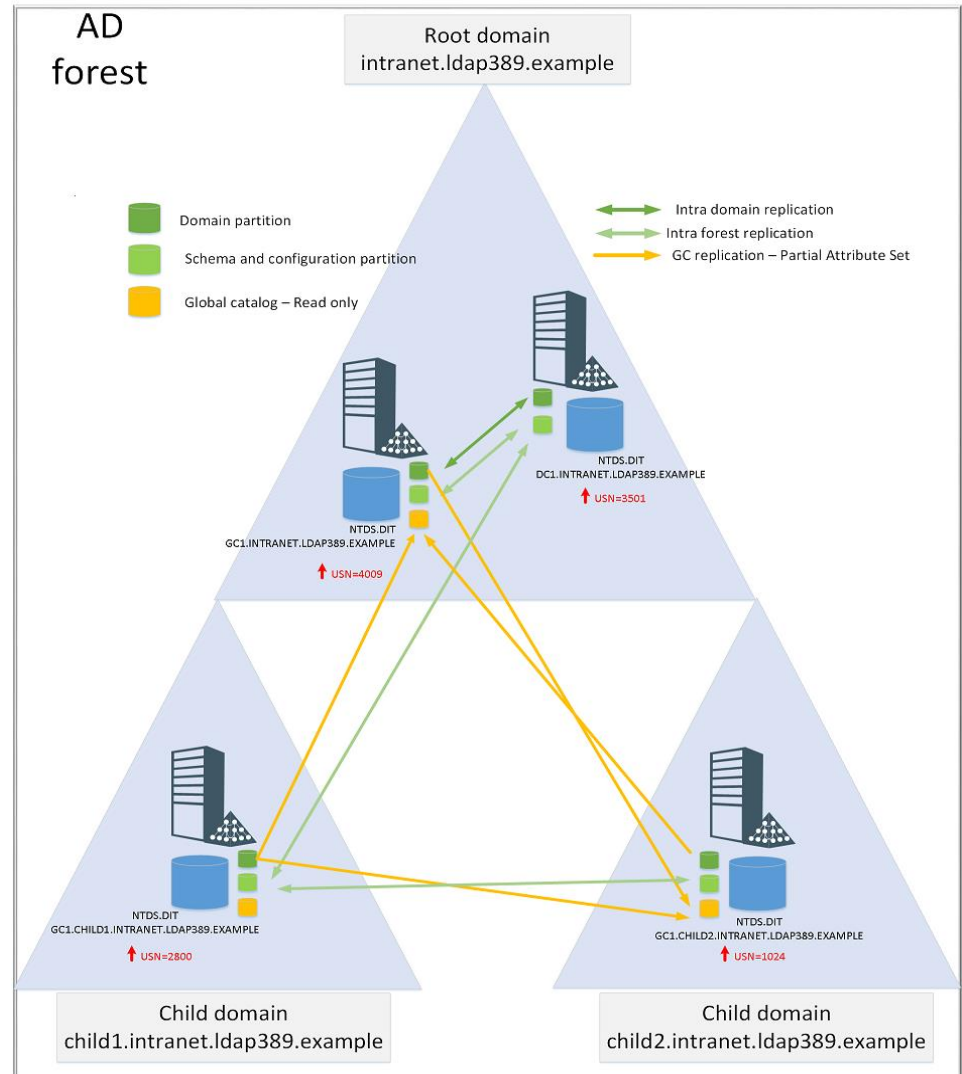
One or more domains in one forest.

AD must be a highly available service.

Many DCs in each domain replicating the various partitions of the NTDS database.

Replication can be intra domain, intra forest or via Global Catalog (*Partial Attribute Set*).

A DC GUID and a USN (*Update Sequence Number*) identify a change in the Active Directory database.



# AD replication metadata – msDS-ReplAttributeMetaData

> A *constructed attribute* in XML format:

```
PS Z:\> Get-ADGroup HR_RW -Properties msDS-ReplAttributeMetaData | Select-Object -ExpandProperty msDS-ReplAttributeMetaData
<DS_REPL_ATTR_META_DATA>
  <pszAttributeName>objectCategory</pszAttributeName>
  <dwVersion>1</dwVersion>
  <ftimeLastOriginatingChange>2018-07-17T15:27:16Z</ftimeLastOriginatingChange>
  <uuidLastOriginatingDsaInvocationID>d391fb4c-852c-418f-9fe2-015cc980cf38</uuidLastOriginatingDsaInvocationID>
  <usnOriginatingChange>532806</usnOriginatingChange>
  <usnLocalChange>532806</usnLocalChange>
  <pszLastOriginatingDsaDN>CN=NTDS Settings,CN=RWDC,CN=Servers,CN=SIEGE,CN=Sites,CN=Configuration,DC=labo,DC=local</pszLastOriginatingDsaDN>
</DS_REPL_ATTR_META_DATA>
<DS_REPL_ATTR_META_DATA>
  <pszAttributeName>groupType</pszAttributeName>
  <dwVersion>1</dwVersion>
  <ftimeLastOriginatingChange>2018-07-17T15:27:16Z</ftimeLastOriginatingChange>
  <uuidLastOriginatingDsaInvocationID>d391fb4c-852c-418f-9fe2-015cc980cf38</uuidLastOriginatingDsaInvocationID>
  <usnOriginatingChange>532806</usnOriginatingChange>
  <usnLocalChange>532806</usnLocalChange>
  <pszLastOriginatingDsaDN>CN=NTDS Settings,CN=RWDC,CN=Servers,CN=SIEGE,CN=Sites,CN=Configuration,DC=labo,DC=local</pszLastOriginatingDsaDN>
</DS_REPL_ATTR_META_DATA>
```

- > It gives you the time at which each attribute for a given object was last changed.
- > It applies only to replicated attributes.

# AD replication metadata – msDS-ReplAttributeMetaData

For each replicated attribute msDS-ReplAttributeMetaData contains :

- > pszAttributeName : The attribute name.
- > ftimeLastOriginatingChange : Time the attribute was last changed.
- > dwVersion : Counter incremented every time the attribute is changed.
- > usnOriginatingChange : USN on the originating server at which the last change to this attribute was made.
- > pszLastOriginatingDsaDN : DC on which the last change was made to this attribute.
- > uuidLastOriginatingDsaInvocationID : ID corresponding to pszLastOriginatingDsaDN ;
- > usnLocalChange : USN on the destination server (the server your LDAP bind is made) at which the last change to this attribute was applied.



# AD replication metadata– msDS-ReplValueMetaData

Replication metadata for *linked attributes*:

Pairs of attributes in which the system calculates the values of one attribute (the *back link* e.g. *MemberOf*) based on the values set on the other attribute (the *forward link* e.g. *Member*) throughout the forest.

In the case of group objects, the member attribute has the same information as *msDS-ReplAttributeMetaData* and in addition:

- > *pszObjectDn* : The group member DistinguishedName.
- > *ftimeCreated* : Contains the time the member was added in the group.
- > *ftimeDeleted* : Contains the time the member was removed from the group.

# AD replication metadata – Tools

> With command line:

```
PS Z:\> repadmin /showobjmeta rwdc.labo.local "CN=HR_RW,DC=labo,DC=local"
```

USN loc	DSA source	USN org.	Heure/date org.	Attribut	ver
532806	SIEGE\RWDC	532806	2018-07-17 17:27:16	1 objectClass	
532806	SIEGE\RWDC	532806	2018-07-17 17:27:16	1 cn	
532842	SIEGE\RWDC	532842	2018-07-17 17:39:28	2 description	3
532806	SIEGE\RWDC	532806	2018-07-17 17:27:16	1 instanceType	
532806	SIEGE\RWDC	532806	2018-07-17 17:27:16	1 whenCreated	1
532806	SIEGE\RWDC	532806	2018-07-17 17:27:16	1 nTSecurityDescriptor	
532806	SIEGE\RWDC	532806	2018-07-17 17:27:16	1 name	
532806	SIEGE\RWDC	532806	2018-07-17 17:27:16	1 objectSid	
532806	SIEGE\RWDC	532806	2018-07-17 17:27:16	1 sAMAccountName	
532806	SIEGE\RWDC	532806	2018-07-17 17:27:16	1 sAMAccountType	
532806	SIEGE\RWDC	532806	2018-07-17 17:27:16	1 groupType	
532806	SIEGE\RWDC	532806	2018-07-17 17:27:16	1 objectCategory	

2 entrées.

Type	Attribut	Heure dern mod.	DSA source	USN loc	USN org	Ver
PRÉSENT	member	2018-07-17 17:30:14	SIEGE\RWDC	532836	532836	1
ABSENT	member	2018-07-17 17:44:03	SIEGE\RWDC	532855	532855	2

> With Powershell 4.0+ :

```
PS Z:\> Get-ADReplicationAttributeMetadata "CN=HR_RW,DC=labo,DC=local" -Server rwdc.labo.local | select -last 1
```

AttributeName	: member
AttributeValue	: CN=Morty,DC=labo,DC=local
FirstOriginatingCreateTime	: 17/07/2018 17:30:14
IsLinkValue	: True
LastOriginatingChangeDirectoryServerIdentity	: CN=NTDS Settings,CN=RWDC,CN=Servers,CN=SIEGE,CN=Sites,CN=Configuration,DC=labo,DC=local
LastOriginatingChangeDirectoryServerInvocationId	: d391fb4c-852c-418f-9fe2-015cc980cf38
LastOriginatingChangeTime	: 17/07/2018 17:44:03
LastOriginatingChangeUsn	: 532855
LastOriginatingDeleteTime	: 17/07/2018 17:44:03
LocalChangeUsn	: 532855
Object	: CN=HR_RW,DC=labo,DC=local
Server	: RWDC.labo.local
Version	: 2

# AD replication metadata – Existing work

> Pierre Audonnet :

<https://blogs.technet.microsoft.com/pie/2014/08/25/metadata-0-metadata-what-is-it-and-why-do-we-care>

> Gregory Lucand (FR):

<https://adds-security.blogpost.com>

> Will Schroeder :

<https://harmj0y.net/blog/defense/hunting-with-active-directory-replication-metadata>

<https://github.com/ANSSI-FR/ADTimeline>

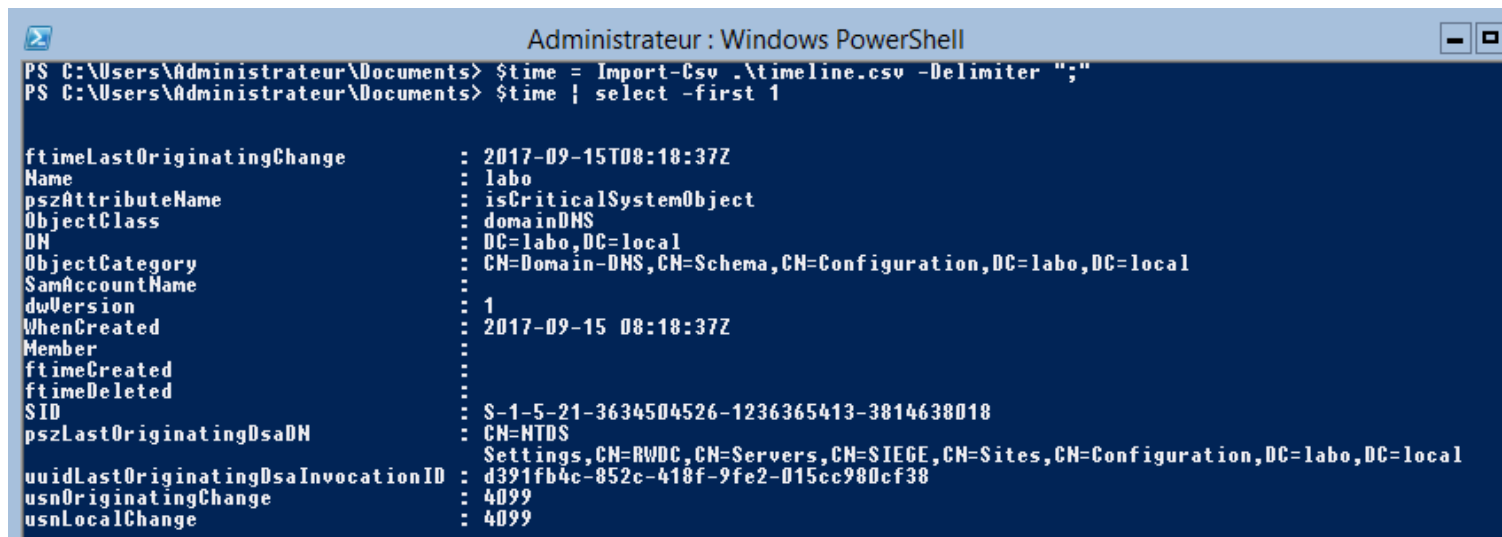
# THE ADTIMELINE TOOL

## ADTimeline - Overview

- > Objects considered of interest are gathered by the script.
- > For each object replication metadata is retrieved: *msDS-RepLAttributeMetaData* for every objectclass. For group objectclass, *msDS-RepLValueMetaData* is also retrieved.
- > Generate a timeline by sorting replication metadatas by *fTimeLastOriginatingChange*.
- > Tool has an online and offline mode.

# ADTimeline – Files generated

Timeline in CSV format (metadata + some attributes): *Import-Csv -delimiter ';'.*



```
Administrateur : Windows PowerShell
PS C:\Users\Administrateur\Documents> $time = Import-Csv .\timeline.csv -Delimiter ";"
PS C:\Users\Administrateur\Documents> $time | select -first 1

ftimeLastOriginatingChange      : 2017-09-15T08:18:37Z
Name                             : labo
pszAttributeName                : isCriticalSystemObject
ObjectClass                      : domainDNS
DN                               : DC=labo,DC=local
ObjectCategory                   : CN=Domain-DNS,CN=Schema,CN=Configuration,DC=labo,DC=local
SamAccountName                   :
dwVersion                        : 1
WhenCreated                      : 2017-09-15 08:18:37Z
Member                           :
ftimeCreated                     :
ftimeDeleted                     :
SID                              : S-1-5-21-3634504526-1236365413-3814638018
pszLastOriginatingDsaDN         : CN=NTDS
                                Settings,CN=RWDC,CN=Servers,CN=SIEGE,CN=Sites,CN=Configuration,DC=labo,DC=local
uuidLastOriginatingDsaInvocationID : d391fb4c-852c-418f-9fe2-015cc980cf38
usnOriginatingChange            : 4099
usnLocalChange                   : 4099
```

All objects retrieved via LDAP and their attributes values (ADObjects.xml) and all objects retrieved via Global Catalog (GCADObjects.xml) : *Import-CliXML.*

log-adexport.log : Log file.

# Demo 1 – Mail exfiltration

Attack scenario:

- > Attacker grants a user mailbox read rights on a database and the ability to export emails as a PST archive.
- > Attacker searches with that user for valuable intel to exfiltrate by browsing employees webmail.
- > Attacker exfiltrates with that user interesting emails as a PST archive with *New-MailboxExportRequest* (Hacking Team breach: <http://pastebin.com/raw/0SNSvyjJ>)

```
Administrator: powershell.exe (running as labo\administrateur)
LABO\Propriétaires créateurs de la stratégie de groupe           Group
      S-1-5-21-3634504526-1236365413-3814638018-520 Mandatory
group, Enabled by default, Enabled group
LABO\Organization Management                                   Group
      S-1-5-21-3634504526-1236365413-3814638018-1105 Mandatory
group, Enabled by default, Enabled group
LABO\Administrateurs du schéma                               Group
      S-1-5-21-3634504526-1236365413-3814638018-518 Mandatory
group, Enabled by default, Enabled group
LABO\Administrateurs de l'entreprise                         Group
      S-1-5-21-3634504526-1236365413-3814638018-519 Mandatory
group, Enabled by default, Enabled group
LABO\Import-ExportMBX                                       Group
      S-1-5-21-3634504526-1236365413-3814638018-1190 Mandatory
group, Enabled by default, Enabled group
Authentication authority asserted identity                   Well-
known group S-1-18-1                                        Mandatory
group, Enabled by default, Enabled group
LABO\Groupe de réplication dont le mot de passe RODC est refusé Alias
      S-1-5-21-3634504526-1236365413-3814638018-572 Mandatory
group, Enabled by default, Enabled group, Local Group
Mandatory Label\High Mandatory Level                       Label
      S-1-16-12288

PS C:\Windows\system32>
```

Recy  
Comr

Close, Search, Help icons

exchange

endedri  
r Rick



## ADTimeline - Processing the results

- > Search for suspicious attribute modifications:  
*NTSecurityDescriptor, SIDHistory, defaultSecurityDescriptor, UserAccountControl, Searchflags...*
- > Objects deletion (*Tombstone*).
- > User accounts added and removed from groups.
- > Inconsistency in the timeline (*USN/ftimeLastOriginatingChange, dwVersion, WhenCreated*).

When a suspicious behavior is spotted, retrieve the DCs event logs (*pszLastOriginatingDsaDN* Domain Controller backup).

# ADTimeline - Objects considered of interest

Objetcts in the domain partition	Objects in other partitions
Domain root and objects located directly under the root.	Domain roots located in the AD forest.
Objects protected by the SDProp process	Domain trusts and CertificationAuthority objects.
The Pre Windows 2000 compatible access, Cert publishers, GPO creator owners and DNS Admins groups.	Class Schema objects and attributes with particular SearchFlags (Do not audit or confidential).
Objects having an ACE on the domain root.	Domain controllers (Computer objects, ntdsdsa and server objects).
Deleted users (i.e. tombstoned) and dynamic objects.	DNS zones.
Organizational Units.	Accounts with suspicious SIDHistory (scope is forest wide).
Existing and deleted Group Policy objects.	AD Site, the directory service and RID manager objects.
Objects under the System container.	Extended rights and Cross Reference containers.
Objects with Kerberos delegation enabled.	Exchange RBAC roles and accounts assigned to a role.
Kerberoastable and AS-REP roastable accounts.	Exchange mail flow and storage configuration objects.
Custom groups which have to be manually defined.	Deleted objects under the configuration partition.

## ADTimeline - Using offline and online mode.

- > Online mode: Launch on a privileged access workstation having ADDS Powershell module installed and with a domain admin account (*tombstone* read rights). Works with standard user also.
- > Offline mode: In case the analyst has to process a disk image or a NTDS backup/snapshot. Mount the NTDS file with *dsamain.exe* (part of ADLDS role) on an analysis machine with ADDS Powershell module installed.

## Demo 2 – Mimikatz DCShadow

Attack scenario:

- > *PhoneNumber* attribute modification on admin accounts in order to bypass the 2FA authentication setup by the security team on a critical application. First factor being AD password, second being security code sent by SMS.
- > Use of *Mimikatz DCShadow* in order to bypass SIEM alerting (Windows security event logs) and replication metadata tampering in order to slow down investigation.

```
Administrateur : C:\Windows\system32\cmd.exe
C:\Users\administrateur>
```

```
Administrateur : Invite de commandes
C:\Users\administrateur>
```



# AD replication metadata vs security event logs

> Replication metadata **IS NOT AN EXCUSE NOT TO** centralize, store and analyse your AD security event logs !

> Perimeter :

Metadata : Concerns every objectclass but only replicated attributes.

Event logs : Depends on your audit policy.

The screenshot shows the Active Directory Administrative Center interface. On the left, the configuration tree is expanded to 'CN=Certification Authorities', which is circled in red. On the right, the 'Audit' tab is selected and also circled in red. The 'Propriétaire' field shows 'Administrateurs de l'entreprise (LABO\Administrateurs de l'entreprise)'. Below the tabs, there is a message: 'Pour obtenir des informations supplémentaires, double-cliquez sur une entrée d'audit. Pour modifier l'entrée et cliquez sur Modifier (si disponible)'. Below this is a table with the following columns: Type, Principal, Accès, and Hérité de. The table is currently empty. At the bottom, there are three buttons: 'Ajouter', 'Supprimer', and 'Afficher'.

# AD replication metadata vs security event logs

## > Centralization :

Metadata : Replicated and stored in the NTDS database of every DC.

Event logs : Setup your centralized windows event log management (<http://aka.ms/WEF>)

## > History :

Metadata : Data since your domain creation but only the last modification of each replicated attribute.

Event logs : Depends on your event logs retention strategy.

## > Data available:

Metadata : You do not know who made the modification and the attribute value before vs after.

Event logs : All the data required is present.

## > Ability to tamper the data:

Metadata : Yes (e.g. *Mimikatz*, *DCShadow*)

Event logs : Yes (e.g. *DanderSpritz*, *Eventlogedit*)

<https://github.com/ANSSI-FR/ADTimeline>

# QUESTIONS?

Additional resources:

Hideaki Ihara from JSOC

<http://port139.hatenablog.com/>