# ACTIVE DIRECTORY BACKDOORS: Myth or Reality
# BTA: an open source framework to analyse AD

Philippe Biondi, Joffrey Czarny — Airbus Group Innovations

BlackHat Arsenal — 2015-08-06

AIRBUS
GROUP

# Summary

# Summary

# Context

## Active Directory

- Manage authentication and authorization for users and computers
- Security policies
- Baseline

$\Longrightarrow$ Corner stone for Microsoft information system

$\Longrightarrow$ Target of choice for intruder

$\Longrightarrow$ Pain to secure...

## Auditors, Incident handlers, Admins need to audit Active Directory

- Find bad practices (admins are sometimes lazy?)
- Hunting (Searching for a needle in a haystack!)
- Incident response (what has changed in timeframe?)

# Two case study

Now, let's start hunting. I'll show you two backdoors, and we'll try to find them.

## Backdoor 1 - Domain Admins members

Administrator:
"It seems someone can manipulate Domain Admins group and users!"

## Backdoor 2 - AdminSDHolder

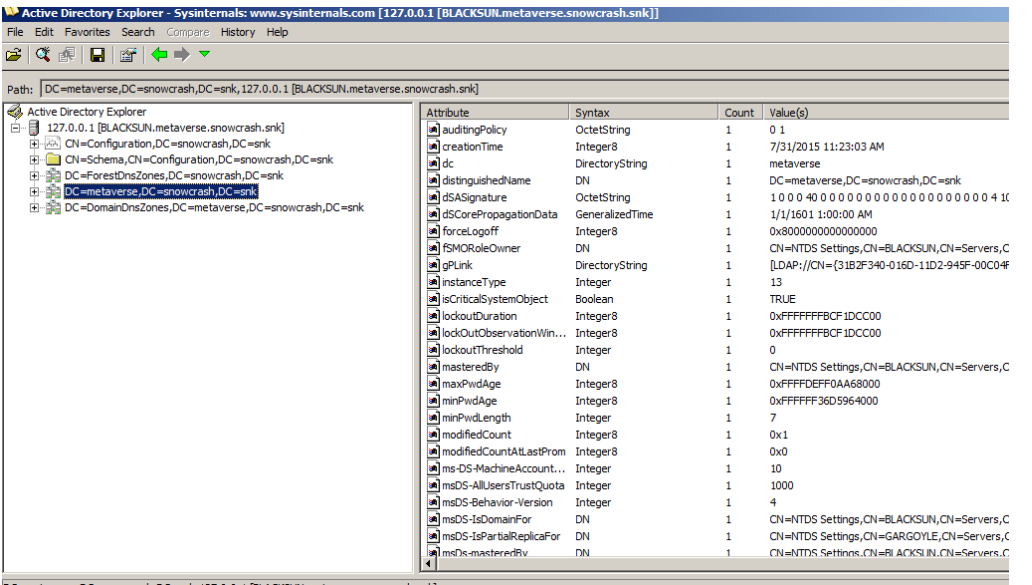
Administrator:
"I removed some permissions but they came back!"

# Backdoor 1 description - Domain Admins members

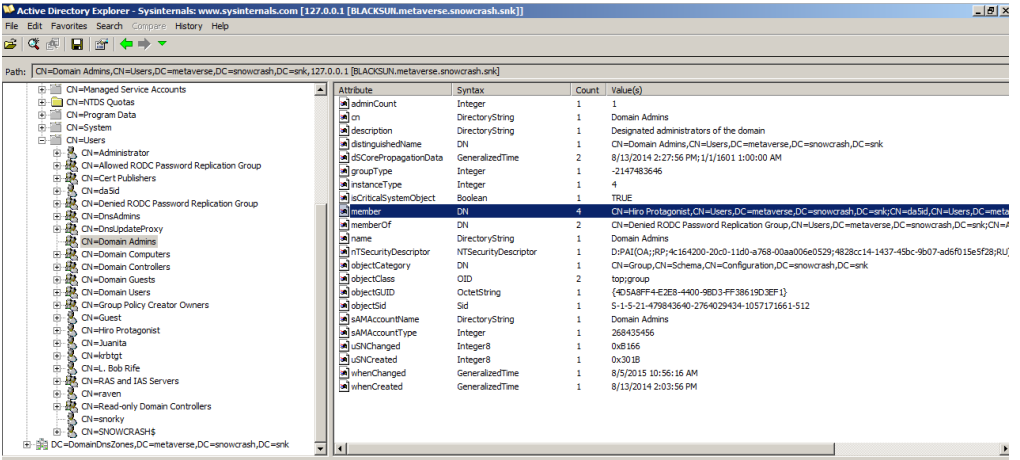
## Who is (or could become) Domain admin?

- Can I justify membership for every one of them?
- Who has permission on this group?
  - Who can add members?
  - Who manage members?
- Who has permission on these members?
  - Who can reset their passwords?
- Can I know when a member has been removed?

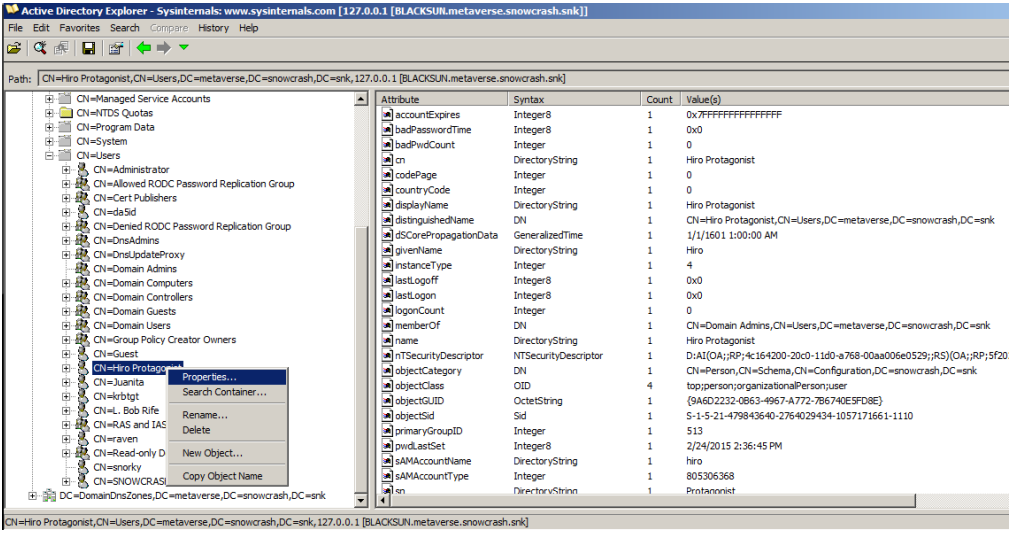
Let's try to find it using Microsoft-provided tools : AD explorer


Active Directory Explorer - Sysinternals: www.sysinternals.com [127.0.0.1 [BLACKSUN.metaverse.snowcrash.snk]]
File Edit Favorites Search Compare History Help
Path: DC=metaverse,DC=snowcrash,DC=snk,127.0.0.1 [BLACKSUN.metaverse.snowcrash.snk]
Active Directory Explorer
127.0.0.1 [BLACKSUN.metaverse.snowcrash.snk]
CN=Configuration,DC=snowcrash,DC=snk
CN=Schema,CN=Configuration,DC=snowcrash,DC=snk
DC=ForestDnsZones,DC=snowcrash,DC=snk
DC=metaverse,DC=snowcrash,DC=snk
DC=DomainDnsZones,DC=metaverse,DC=snowcrash,DC=snk
Attribute Syntax Count Value(s)
auditingPolicy OctetString 1 0 1
creationTime Integer8 1 7/31/2015 11:23:03 AM
dc DirectoryString 1 metaverse
distinguishedName DN 1 DC=metaverse,DC=snowcrash,DC=snk
dSASignature OctetString 1 1 0 0 0 40 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 4 10
dSCorePropagationData GeneralizedTime 1 1/1/1601 1:00:00 AM
forceLogoff Integer8 1 0x8000000000000000
fSMORoleOwner DN 1 CN=NTDS Settings,CN=BLACKSUN,CN=Servers,C
gPLink DirectoryString 1 [LDAP://CN={31B2F340-016D-11D2-945F-00C04F
instanceType Integer 1 13
isCriticalSystemObject Boolean 1 TRUE
lockoutDuration Integer8 1 0xFFFFFFFFBCF1DCC00
lockOutObservationWin... Integer8 1 0xFFFFFFFFBCF1DCC00
lockoutThreshold Integer 1 0
masteredBy DN 1 CN=NTDS Settings,CN=BLACKSUN,CN=Servers,C
maxPwdAge Integer8 1 0xFFFFDEFF0AA68000
minPwdAge Integer8 1 0xFFFFFF36D5964000
minPwdLength Integer 1 7
modifiedCount Integer8 1 0x1
modifiedCountAtLastProm Integer8 1 0x0
ms-DS-MachineAccount... Integer 1 10
msDS-AllUsersTrustQuota Integer 1 1000
msDS-Behavior-Version Integer 1 4
msDS-IsDomainFor DN 1 CN=NTDS Settings,CN=BLACKSUN,CN=Servers,C
msDS-IsPartialReplicaFor DN 1 CN=NTDS Settings,CN=GARGOYLE,CN=Servers,C
msDs-masteredBy DN 1 CN=NTDS Settings,CN=BLACKSUN,CN=Servers,C
DC=metaverse,DC=snowcrash,DC=snk,127.0.0.1 [BLACKSUN.metaverse.snowcrash.snk]

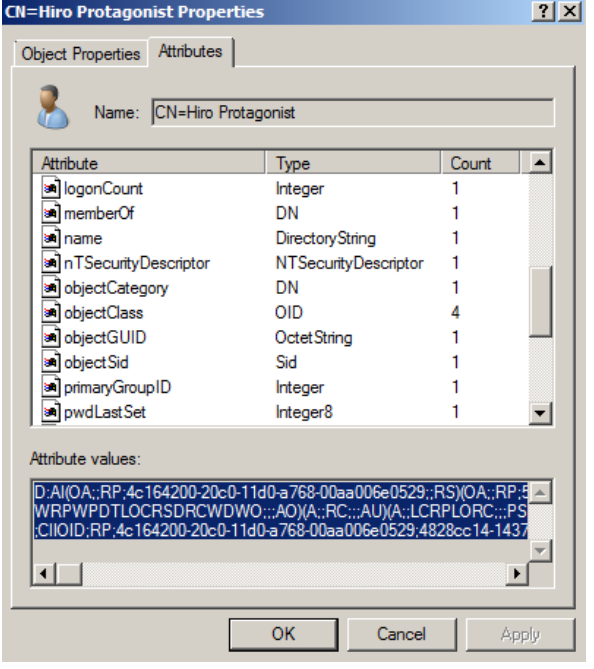
AD explorer

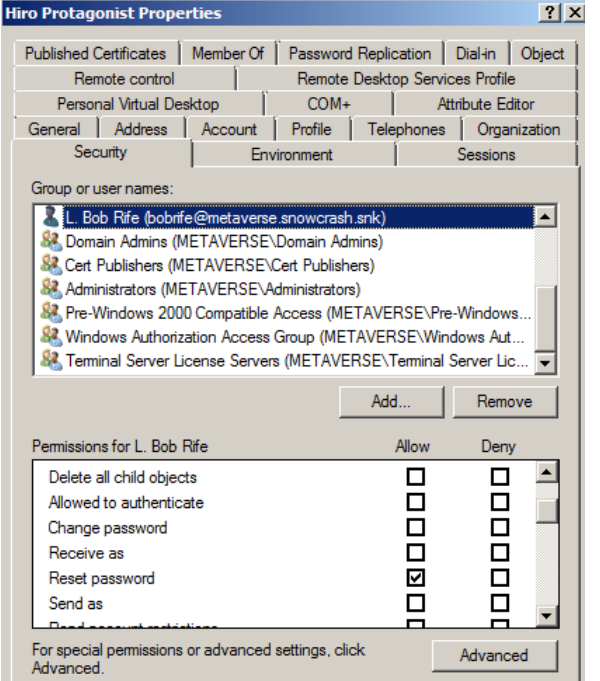



Members of Domain Admins




User properties


CN=Hiro Protagonist Properties
Object Properties
Attributes
Name: CN=Hiro Protagonist
Attribute
Type
Count
logonCount
Integer
1
memberOf
DN
1
name
DirectoryString
1
nTSecurityDescriptor
NTSecurityDescriptor
1
objectCategory
DN
1
objectClass
OID
4
objectGUID
OctetString
1
objectSid
Sid
1
primaryGroupID
Integer
1
pwdLastSet
Integer8
1
Attribute values:
D:AI(OA;;RP;4c164200-20c0-11d0-a768-00aa006e0529;;RS)(OA;;RP;5
WRPWPDTLOCRSDRCWDWO;;;AO)(A;;RC;;;AU)(A;;LCRPLORC;;;PS
;CIIOID;RP;4c164200-20c0-11d0-a768-00aa006e0529;4828cc14-1437
OK
Cancel
Apply

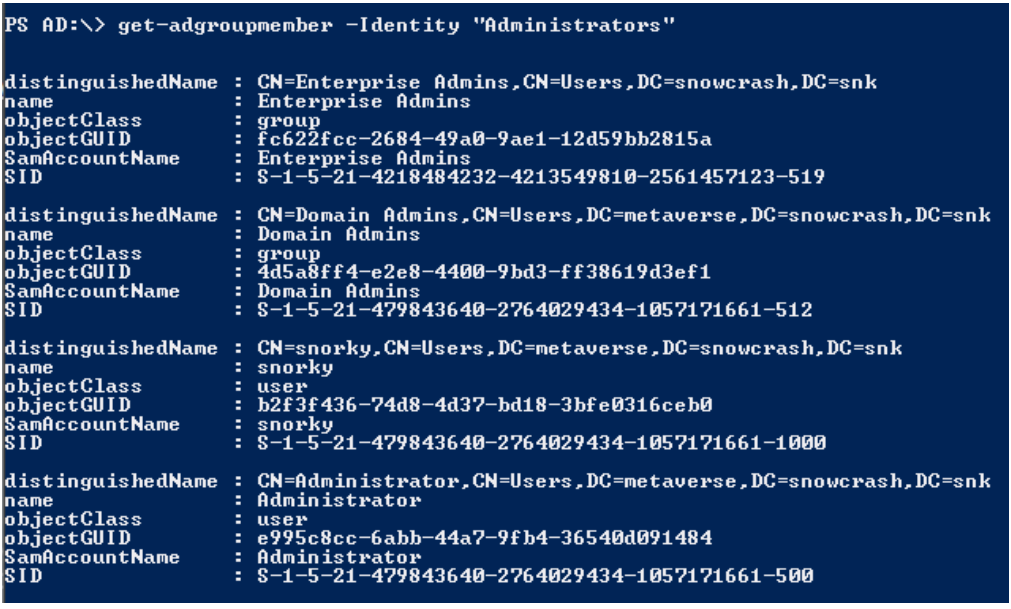

Hiro Protagonist Properties
Published Certificates
Member Of
Password Replication
Dial-in
Object
Remote control
Remote Desktop Services Profile
Personal Virtual Desktop
COM+
Attribute Editor
General
Address
Account
Profile
Telephones
Organization
Security
Environment
Sessions
Group or user names:
L. Bob Rife (bobrife@metaverse.snowcrash.snk)
Domain Admins (METAVERSE\Domain Admins)
Cert Publishers (METAVERSE\Cert Publishers)
Administrators (METAVERSE\Administrators)
Pre-Windows 2000 Compatible Access (METAVERSE\Pre-Windows...
Windows Authorization Access Group (METAVERSE\Windows Aut...
Terminal Server License Servers (METAVERSE\Terminal Server Lic...
Add...
Remove
Permissions for L. Bob Rife
Allow
Deny
Delete all child objects
Allowed to authenticate
Change password
Receive as
Reset password
Send as
For special permissions or advanced settings, click Advanced.
Advanced

# Backdoor 1 (Domain Admins members) hunting using AD Explorer: results

## Problems

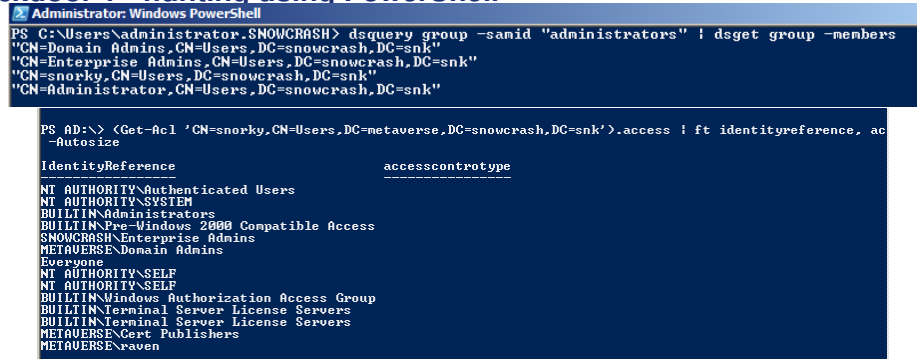
- Several clicks to obtain this information with AD explorer or MS GUI tools

- Ok, it kind of works, but it's way too complicated.
- Moreover not all information is obtained.
- Let's try using powershell!




PowerShell request for AD

# Backdoor 1 - hunting using PowerShell




## Problems

- Powershell Cmdlets required, run on the host or via network, sometimes complex PS requests

# Backdoor 2 description: AdminSDHolder

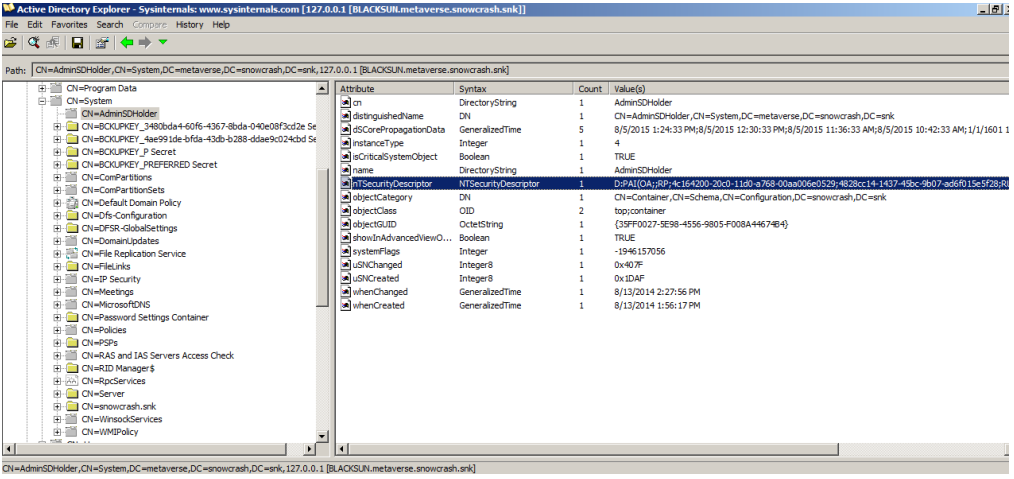
## AdminSDHolder

- Some users / groups can be "protected" (`adminCount=1` attribute)
- `AdminSDHolder` is a Master Security Descriptor (list of permissions)
- Every 60 minutes, LSASS applies these permissions to protected users

Checks:

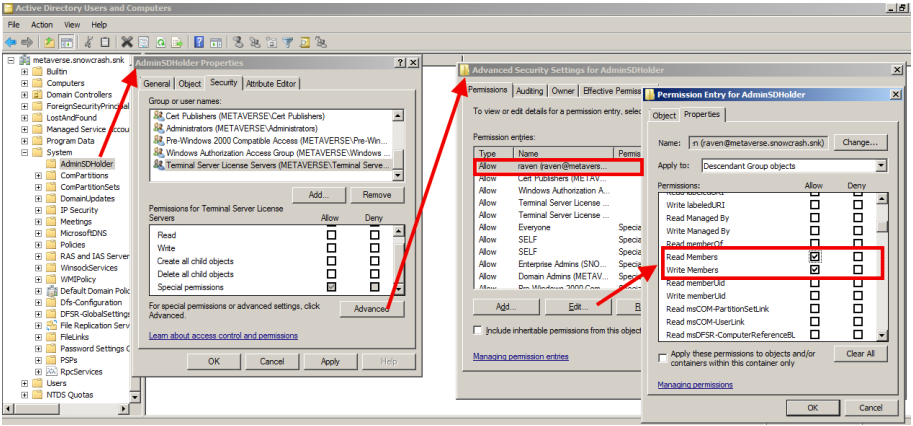
- Which groups/users are protected?
- ACL template has been changed?

Let's try to find it using Microsoft-provided tools: AD explorer & Powershell




AdminSDHolder

# Backdoor 2 (AdminSDHolder) hunting using PowerShell



# Backdoor 2 (AdminSDHolder) hunting using AD Explorer

```
PS AD:\> (Get-Acl 'CN=AdminSDHolder,CN=System,DC=metaverse,DC=snowcrash,DC=snk').access | ft identityrefer
ntrotype -Autosize

IdentityReference                       accesscontrotype
-----------------                       ----------------
NT AUTHORITY\Authenticated Users
NT AUTHORITY\SYSTEM
BUILTIN\Administrators
BUILTIN\Pre-Windows 2000 Compatible Access
SNOWCRASH\Enterprise Admins
METAVERSE\Domain Admins
Everyone
NT AUTHORITY\SELF
NT AUTHORITY\SELF
BUILTIN\Windows Authorization Access Group
BUILTIN\Terminal Server License Servers
BUILTIN\Terminal Server License Servers
METAVERSE\Cert Publishers
METAVERSE\raven
```

## Problems

- AdminSDHolder ACEs' have been changed: Raven account has been added

# How can I proceed?

## Currently

- Manual checks using a GUI is inefficient
- Powershell requires “one-shot” commands for each control; little re-use
- Online tools need admins credential over network connection

## Wishlist for a perfect tool

- Do multiple checks on several objects
- Easy way to identify bad practices
- Help to clean up regularly
- Find anomalies or backdoors

So, we decided to develop a tool that will help us and find backdoors in AD.

# BTA: an open source framework to analyze Active Directory

## State of the project

- No Logo!
- No Press release!
- No fees for use!

## But

- Functional and tested in real life :)
- Could help you to improve your AD security!

$\Longrightarrow$ Why?

# Summary

# BTA

## BTA

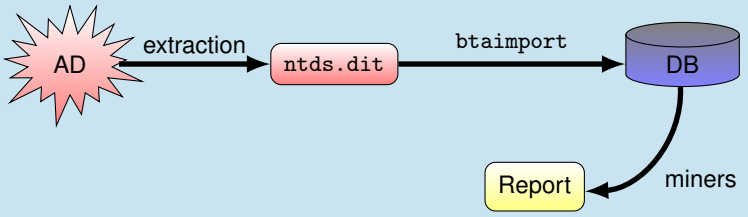
- Airbus {Group {CERT|Innovations}|DS CyberSecurity}
- Open Source (GPLv2)
- `https://bitbucket.org/iwseclabs/bta`

## BTA can help solve the following issues:

- Quick access, without filtering, to all Active Directory data
- Works offline
- Set of controls points ($\neq$ exploratory tool)
- Determinism
- Periodic review of AD (reproductibility)
- Modularity

# Global view of BTA operation

## BTA architecture, global view




| | |
|---|---|
| `btaimport` | `NTDS.dit` ⟶ Mongo + postprocessing |
| `btamanage` | Manage imported NTDS bases |
| `btaminer` | Call *miners* |
| `btadiff` | Diff between two states of imported AD |

# Import

## Overview of MongoDB data: a field of `datatable`


```
{ "cn" : "ACS-Enable-ACS-Service",
  "1DAPDisplayName" : "aCSEnableACSService",
  "name" : "ACS-Enable-ACS-Service",
  "adminDescription" : "ACS-Enable-ACS-Service",
  "adminDisplayName" : "ACS-Enable-ACS-Service",
  "isVisibleInAB" : 42,
  "objectClass" : [ 196622, 65536 ],
  "schemaIDGUID" : "7f561287-5301-11d1-a9c5-0000f80367c1",
  "objectGUID" : "925af73d-e447-40c0-9655-b5a8603fb49f",
  "time_col" : ISODate("2009-02-11T18:37:08Z"),
  "distinguishedName" : 23,
  "systemFlags" : 16,                                    "attributeID" : 590594,
  "nTSecurityDescriptor" : 7,                            "cnt_col" : 1,
  "RDNtyp_col" : 3,                                      "attributeSyntax" : 524296,
  "isSingleValued" : 1,                                  "showInAdvancedViewOnly" : 1,
  "instanceType" : 4,                                    "DNT_col" : 23,
  "oMSyntax" : 1,                                        "OBJ_col" : 1,
  "uSNCreated" : 15,
  "recycle_time_col" : NumberLong("3038287259199220266"),
  "whenCreated" : ISODate("2009-02-11T18:37:08Z"),
  "replPropertyMetaData" : BinData(0,"AQAAAAAAAATAAAAAAAAAAAAAABAAAAC+mLCAMAAAAvmvLtKEtaQqTKmYSWdi8vDwAAAAAAAAAPAAAAAAAAAM....
  "whenChanged" : ISODate("2009-02-11T18:37:08Z"),
  "PDNT_col" : 1811,
  "objectCategory" : 14,
  "Ancestors_col" : BinData(0,"AgAAAPsGAAD8BgAA/QYAABMHAAAXAAAA"),
  "NCDNT_col" : 1811,
  "uSNChanged" : 15  }
```

# Backdoor 1: Domain Admins

`ListGroup` ***miner***

```
$ btaminer -t ReST -C ::mabase  ListGroup --match "Domain Admins"
+----------------+---------------------+-----------------------------------+---------------+
| Name           | Deletion            | Flags                             | Recursive     |
+================+=====================+===================================+===============+
| L. Bob Rife    |                     | normalAccount, dontExpirePassword | srv-grp-admin |
| svc-mcafee     | 2014-02-23 14:10:11 | normalAccount, accountDisable     |               |
| svc-oracle     |                     | normalAccount, dontExpirePassword |               |
| Sqladmin       | 2014-08-15 04:45:04 | normalAccount, dontExpirePassword |               |
| svc-security   |                     | normalAccount, accountDisable     |               |
+----------------+---------------------+-----------------------------------+---------------+
```

## Results: in 10s

- All accounts are listed recursively
- Deletion information is provided by `link_table` with a retention of 180 days
  - Sqladmin has been removed at a supicious time!

Easier than with MS tools

# Backdoor 1: Domain Admins

`ListGroup` ***miner***

```
$ btaminer -C::snktest -t ReST ListGroup --match "Domain Admins"

Analysis by miner [ListGroup]
=============================


+====================+==========+===============+===========+
| snorky             |          | normalAccount |           |
| Administrator      |          | normalAccount |           |
+--------------------+----------+---------------+-----------+
User snorky (S-1-5-21-1154669122-758131934-2550385761-1154)
+-------------------+---------+---------------------+-----------------------+
| Trustee           | Member  | ACE Type            | Object type           |
+===================+=========+=====================+=======================+
| Domain Admins     | snorky  | AccessAllowedObject | (none)                |
[...]
| Everyone          | snorky  | AccessAllowedObject | User-Change-Password  |
| raven             | snorky  | AccessAllowedObject | (none)                | <==
| Self              | snorky  | AccessAllowedObject | User-Change-Password  |
| Self              | snorky  | AccessAllowedObject | Private-Information    |
| Domain Admins     | snorky  | AccessAllowed       | (none)                |
| Administrators    | snorky  | AccessAllowed       | (none)                |
| System            | snorky  | AccessAllowed       | (none)                |
| Everyone          | snorky  | SystemAudit         | (none)                |
| Everyone          | snorky  | SystemAuditObject   | GP-Link               |
| Everyone          | snorky  | SystemAuditObject   | GP-Options            |
+-------------------+---------+---------------------+-----------------------+
```

## Results: in 10s

- Raven have full privilege on an account which is domain admin member

# Backdoor 2: AdminSDHolder

List objects protected by *AdminSDHolder*

```
$ btaminer -C::snktest SDProp --list

Analysis by miner: [SDProp]
===========================

+------------------------------+-------+-----------------------------------------------+
| cn                           | type  | SID                                           |
+==============================+=======+===============================================+
| Account Operators            | Group | S-1-5-32-548                                  |
| Administrators               | Group | S-1-5-32-544                                  |
| Backup Operators             | Group | S-1-5-32-551                                  |
| Domain Admins                | Group | S-1-5-21-479843640-2764029434-1057171661-512  |
| Domain Controllers           | Group | S-1-5-21-479843640-2764029434-1057171661-516  |
| Print Operators              | Group | S-1-5-32-550                                  |
| Read-only Domain Controllers | Group | S-1-5-21-479843640-2764029434-1057171661-521  |
| Replicator                   | Group | S-1-5-32-552                                  |
| Server Operators             | Group | S-1-5-32-549                                  |
| Administrator                | User  | S-1-5-21-479843640-2764029434-1057171661-500  |
| da5id                        | User  | S-1-5-21-479843640-2764029434-1057171661-1107 |
| Hiro Protagonist             | User  | S-1-5-21-479843640-2764029434-1057171661-1110 |
| krbtgt                       | User  | S-1-5-21-479843640-2764029434-1057171661-502  |
| Sqladmin                     | User  | S-1-5-21-479843640-2764029434-1057171661-1106 | <==
| snorky                       | User  | S-1-5-21-479843640-2764029434-1057171661-1000 |
+------------------------------+-------+-----------------------------------------------+
```

# Backdoor 2: AdminSDHolder

Check ACEs linked to *AdminSDHolder*

```
$ btaminer -C ::snktest SDProp --checkACE

Analysis by miner: [SDProp]
===========================

+-----------------------------------+--------------------+---------------------------------+
| cn                                | type               | SID                             |
+===================================+====================+=================================+
| Administrators                    | AccessAllowed      | ALL                             |
| Authenticated Users               | AccessAllowed      | ALL                             |
| Cert Publishers                   | AccessAllowedObject | X509-Cert                       |
| Domain Admins                     | AccessAllowed      | ALL                             |
| Enterprise Admins                 | AccessAllowed      | ALL                             |
| Everyone                          | AccessAllowedObject | User-Change-Password            |
| Everyone                          | SystemAudit        | ALL                             |
| Everyone                          | SystemAuditObject  | Organizational-Unit             |
| Everyone                          | SystemAuditObject  | Organizational-Unit             |
| Pre-Windows 2000 Compatible Access | AccessAllowed      | ALL                             |
| raven                             | AccessAllowedObject | Group                           | <==
| Self                              | AccessAllowedObject | User-Change-Password            |
| Self                              | AccessAllowedObject | Private-Information              |
| System                            | AccessAllowed      | ALL                             |
| Terminal Server License Servers   | AccessAllowedObject | Terminal-Server                 |
| Terminal Server License Servers   | AccessAllowedObject | Terminal-Server-License-Server  |
| Windows Authorization Access Group | AccessAllowedObject | Token-Groups-Global-And-Universal |
+-----------------------------------+--------------------+---------------------------------+
```

# Summary

# The main stages

## `NTDS.dit` file domain controller extraction

- Via *ntdsutil* under 2008 infrastructure
- Via *vssadmin* under 2003 infrastructure

## Import of `NTDS.dit` file

- *btaimport* is responsible for importing the data into mongoDB database
- Preprocessing of basic data and adding new collections

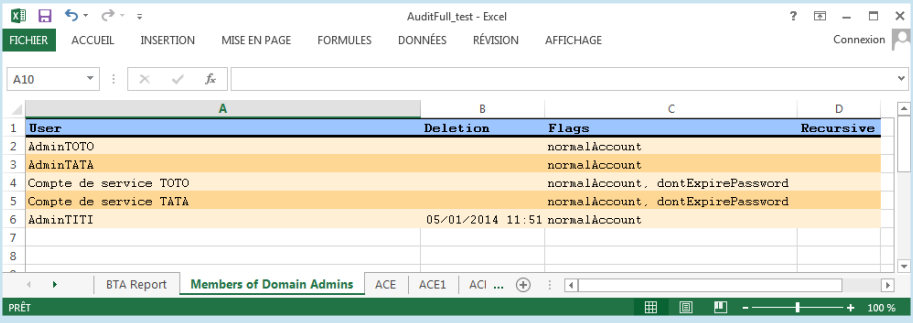
## Queries execution in base and correlation of results

- *btaminer* allows querying the data in base
- Check results with an Active Directory administrator

# Report

## Example: Excel output

```
btaminer -C ::mabase -t excel -o my_report.xlsx Audit_Full
```



# Some control points

## btaminer

- Check extended rights

```
btaminer -C ::snktest ListACE -type 00299570-246d-11d0-a768-00aa006e0529
```

- List accounts which never logged on Active Directory

```
btaminer -C ::snktest passwords -never-logged
```

- List accounts which have not authenticated on AD since 6 months

```
btaminer -C ::snktest passwords -last-logon 182
```

- Number of unsuccessful login attempts per account

```
btaminer -C ::snktest passwords -bad-password-count
```

- List accounts which have a specific *UserAccountControl* flag

```
btaminer -C ::snktest CheckUAC -check passwdCantChange
```

# SIDhistory control points

## Exploiting the SIDHistory attribute

- Modify SIDHistory attribute in order to elevate its privileges.
- Control the Forest from a domain via 'Enterprise Admin' SID.

## Check *SIDHistory* attribute

```
$ btaminer -C::snktest SIDHitory --list

RESA, Micheline      | S-1-5-21-45967694-1012334923-556814060-21624
GAUCI, Sandro        | S-1-5-21-45967694-1012334923-556814060-16537
VIGNON, Georgette    | S-1-5-21-45967694-1012334923-556814060-4438
ABOUHALI, Mouad      | S-1-5-21-45967694-1012334923-556814060-4733
BIONDI, Philippe     | S-1-5-21-45967694-1012334923-556814060-2139
Sqladmin             | S-1-5-21-9778442445-3353794244-6340767225-519  <===
RIGO, Raphael        | S-1-5-21-45967694-1012334923-556814060-4981
```

# Control extended rights

`ListACE` ***miner***

## Objectives

- List users which have specific extended rights:
  - *User-Force-Change-Password* (type `00299570-246d-11d0-a768-00aa006e0529`)
  - *Self-Membership* (type `bf9679c0-0de6-11d0-a285-00aa003049e2`)
  - ...

## btaminer ListACE

```
$ btaminer -C::snktest -t ReST ListACE \
           --type 00299570-246d-11d0-a768-00aa006e0529

Analysis by miner [ListACE]
===========================

+-------------+----------------+----------------------------+
| Trustee     | Subjects       | Object type                |
+=============+================+============================+
| jean dupond | Administrateur | User-Force-Change-Password |
+-------------+----------------+----------------------------+
```

# Miners

***miner*: passwords**

```
$ btaminer -t ReST -C ::mabase passwords --never-logged

Analysis by miner: [passwords]
==============================

+-------------------//-------------+----------------------//---------------+----------------------+
| name              \\             |                       \\              |  userAccountControl  |
+===================//=============+=======================//===============+======================+
| guest             \\             | GUEST of labz (s-1-5-\\               | accountDisable:True  |
| intru             //             | intru (s-1-5-21-11546//               | accountDisable:False |
| krbtgt            \\             | KRBTGT of labz (s-1-5\\               | accountDisable:True  |
| SystemMailbox{1f05//7}           | SystemMailbox{1f05a92//121)           | accountDisable:True  |
| SystemMailbox{e0dc\\9}           | SystemMailbox{e0dc1c2\\122)           | accountDisable:True  |
| DiscoverySearchMai//E09334BB852} | DiscoverySearchMailbo//50385761-1123) | accountDisable:True  |
| FederatedEmail.4c1\\42           | FederatedEmail.4c1f4d\\125)           | accountDisable:True  |
| auditor           //             | auditor (s-1-5-21-115//               | accountDisable:False |
+-------------------\\-------------+-----------------------\\--------------+----------------------+
```

# Check collected informations

## Exchange with Active Directory teams

- Active Directory system is lively → daily changes
- Review elements with AD administrators → could explain some bad practices

# Differential between two instances of AD

## Differential with `btadiff`

- Allows to compare AD at two points in time

$\Longrightarrow$ Allows to monitor an objet in time

$\Longrightarrow$ Allows to check suspicious changes

```
$ btadiff --CA ::clean --CB ::backdoor1 --ignore-defaults

===============
Starting diffing sd_table
---------------
AB, 101: [] *sd_refcount['14'=>'15']
AB, 108: [] *sd_refcount['39'=>'41']
A , 229: []
A , 372: []
AB, 423: [] *sd_refcount['3'=>'2']
 B, 424: []
 B, 425: []
 B, 428: []
---------------
Table [sd_table]: 160 records checked, 2 disappeared, 3 appeared, 3 changed
```

# Summary

# Hardware requirements

## Computer for analysis

- it could be run on a good laptop
  - Xeon 3GHz 4 cores
  - 12GB RAM
  - SSD drive

## Import performance

- 8 GB NTDS base (831121 Objects / 76778 ACEs)
- Imported in MongoDB: 26 GB
- 8h30

## Analysis performance

- Generally negligible time analysis

# Problems encountered in real life

## `NTDS.dit` import

- Bad extraction of `NTDS.dit` file
- Extraction methodology provided not followed by administrators

## Consistency of objects

- Objects always referenced in an ACE but not anymore present in AD
- Migrating a French language environment to English

# Audit results

## Feedback from the field

- After receiving the `NTDS.dit` file, the auditor is autonomous - little interaction is required
  - Once the `NTDS.dit` file has been provided
- Organizations work in different ways; the auditor has to adapt to each AD's peculiarities
- Unable to prejudge the rightness/legitimacy of assigned rights in AD

  $\Longrightarrow$ it is important to check information with administrators

# Audit results

## Common results between different audits

- Often bad practices
  - Too many generic admin accounts
  - Many accounts whose password never expires
  - ...
- Lack of homogeneity on creation templates, e.g.: user...
- Active accounts that have never been used

# Conclusion

## BTA

- Provides in time constrained deterministic results
- Helps to cleanup AD bad practices
- Allow a recurring audit
  reproducibility $\Rightarrow$ comparing results of 2 audits

## Next developments

- LDAP acces
- Unit tests on *miners*
- Improved differential analysis

# Thanks for your attention

## Questions

- joffrey[0x2e]czarny[0x40]airbus[0x2e]com

## Don't forget it is open source

- `https://bitbucket.org/iwseclabs/bta`

## Greetings

- Joachim Metz for the awesome Libesedb
- Of course Philippe Biondi for lots of things
- Xavier & Raphael for their reviews
- My Wife and my kids :)