USE WSUS TO HANG ITS CLIENTS
Who we are, what we do...

- Yves Le Provost
  - Security auditor for more than 10 years
  - Currently works for French cyber defense Agency (ANSSI)
  - Specializes in SCADA and database assessments, but masters any other field ;-) 

- Romain Coltel
  - Former security auditor
  - Currently works for a disruptive startup
  - Developing next-gen Active Directory security product
How do you **compromise** an Active Directory domain?
Sample of an Active Directory domain

Users workstations  Servers  Domain controllers
First step

1. Targeted phishing email, with malware: get a foothold in the network
Next step

2. Propagate compromise between workstations until...
3. You get a server administrative account, and use it to continue propagation...
4. Until you get an Active Directory administrative account
Next step

5. Get domain secrets

Users workstations → Servers → Domain controllers

- Users workstations
- Servers
- Domain controllers
6. Use secrets to access all data
How do you compromise an ESAE-managed forest?
Classic administration

Production forest(s)

Admin workstations

Various resources

Various resources
Tier administration model

Production forest(s)

Tier 0
- Control of enterprise identities in the environment

Tier 1
- Control of enterprise servers and applications

Tier 2
- Control of user workstations and devices
Better administration

Production forest(s)

Tier 0

Tier 1

Tier 2

So, what is an ESAE?

Enhanced Security Administrative Environment

Production forest(s)

Tier 0

- Single forest, single domain
- One-way trust, using selective authentication, with the production forest(s)

Tier 1

- Contains small number of ESAE administrative accounts
  - Dedicated to ESAE

Tier 2

- Contains production forest(s) tier 0 administrators
  - Simple users in the ESAE forest
  - Only connect to tier 0 resources on production
  - Highly secured accounts
- Workstations/servers hardened
Why use an ESAE?

- Users workstations
- Servers
- Domain controllers
Why use an ESAE?

Tier 2

Tier 1

Tier 0
Why use an ESAE?

- Helps protect tier 0 resources against compromise
  - Which helps to protect against an overall compromise
Why use an ESAE?

- Helps protect tier 0 resources against compromise
  - Which helps to protect against an overall compromise

- Can use the same Active Directory account to administrate multiple forests
  - In fact, don’t use an ESAE for only one forest...
Why use an ESAE?

- Helps protect tier 0 resources against compromise
  - Which helps to protect against an overall compromise

- Can use the same Active Directory account to administrate multiple forests
  - In fact, don’t use an ESAE for only one forest...

- Doesn’t protect enterprise’s assets, but a mandatory step to get to that
How do you compromise an ESAE-managed forest?

Well, you can’t, that’s the point.
What if a WSUS server serves updates to the DCs?

Tier 2

Tier 1

Tier 0

WSUS server
Can you compromise an ESAE-managed forest using a WSUS server?
Windows Server Update Services (WSUS) architecture

- Microsoft Update
- WWW
- HTTPS
- XML
- Enterprise network
- WSUS server
- WSUS clients
Windows Server Update Services (WSUS) architecture

Microsoft Update → WWW (HTTP) → WSUS server (HTTPS) → Enterprise network → WSUS clients

- Microsoft Update
- WWW (HTTP)
- WSUS server (HTTPS)
- Enterprise network
- WSUS clients
Windows Server Update Services (WSUS) architecture

Microsoft Update

HTTP

HTTPS

Enterprise network

WSUS server

WSUS clients

www
WSUS server components

- Microsoft Update
- Synchronization
- Windows service
- Web service
- Database
- Deployment
- WSUS server
- WSUS clients
Updates journey within a WSUS server

Microsoft Update → Windows service → Database → Web service → WSUS clients

- Windows service
- Web service
- Database
- WSUS server

BSUSPEN

Yves Le Provost & Romain Coltel
1. Windows service downloads update metadata (binaries size, download URL, command-line arguments, ...)

Updates journey within a WSUS server

- Microsoft Update
- Windows service
- Web service
- Database
- WSUS server
- WSUS clients
Updates journey within a WSUS server

2. Windows service transmits the metadata to the database
Updates journey within a WSUS server

3. The database uses functions to parse metadata inputs, incorporates them into its tables.
Updates journey within a WSUS server

4. Updates are approved, either by an admin or by automatic approval rules

Microsoft Update

WSUS server

- Windows service
- Web service
- Database

WSUS clients

- Microsoft Update
- WSUS server

Yves Le Provost & Romain Coltel
Updates journey within a WSUS server

5. Approved updates binaries (psf, cab, exe, ...) are downloaded
Updates journey within a WSUS server

6. Each binary signature is checked
Updates journey within a WSUS server

7. Each binary is stored for the Web service to be able to get them

Microsoft Update

WSUS server

Windows service

Web service

Database

WSUS clients

7. Each binary is stored for the Web service to be able to get them.
Updates journey within a WSUS server

8. Clients are looking for new updates; Web service gets approved updates metadata from the database.

Microsoft Update

Windows service

Web service

Database

WSUS server

WSUS clients

8. Clients are looking for new updates; Web service gets approved updates metadata from the database.
Updates journey within a WSUS server

9. Web service transmits the metadata to the WSUS clients
Updates journey within a WSUS server

10. Each client evaluates if the updates is installable

Microsoft Update

WSUS server

Windows service

Web service

Database

WSUS clients

Microsoft Update

XML

XML

XML
Updates journey within a WSUS server

11. If an update is installable on a client, the associated binary is downloaded.
Updates journey within a WSUS server

12. Each downloaded binary's signature is checked
Updates journey within a WSUS server

13. Each binary is executed, with SYSTEM privileges, with possible command line parameters from the metadata
**How to connect to the database**

**HKLM\Software\Microsoft\Update Services\Server\Setup**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PortNumber</td>
<td>REG_DWORD</td>
<td>0x00002152 (8530)</td>
</tr>
<tr>
<td>ServicePackLevel</td>
<td>REG_DWORD</td>
<td>0x00000000 (0)</td>
</tr>
<tr>
<td>SqlAuthenticationMode</td>
<td>REG_SZ</td>
<td>WindowsAuthentication</td>
</tr>
<tr>
<td>SqlDatabaseName</td>
<td>REG_SZ</td>
<td>SUSDB</td>
</tr>
<tr>
<td>SqlEncryptedPassword</td>
<td>REG_SZ</td>
<td>MICROSOFT##WID</td>
</tr>
<tr>
<td>SqlServerName</td>
<td>REG_SZ</td>
<td>%ProgramFiles%\Update Services\</td>
</tr>
<tr>
<td>SqlUserName</td>
<td>REG_SZ</td>
<td>0x00000000 (0)</td>
</tr>
<tr>
<td>TargetDir</td>
<td>REG_SZ</td>
<td>0x00000005 (5)</td>
</tr>
<tr>
<td>UsingSSL</td>
<td>REG_SZ</td>
<td>10.0.14393.0</td>
</tr>
<tr>
<td>Version</td>
<td>REG_SZ</td>
<td>S-1-5-21-3553850934-3542133063-197517862-1000</td>
</tr>
<tr>
<td>VersionString</td>
<td>REG_SZ</td>
<td>S-1-5-21-3553850934-3542133063-197517862-1001</td>
</tr>
</tbody>
</table>
How to connect to the database

HKLM\Software\Microsoft\Update Services\Server\Setup

SqlServerName = "MICROSOFT##WID" →
What’s in the database?

Everything:
- Full WSUS configuration
- Updates metadata
- Approvement states
- ...

Some stats:
- 31 views
- 35 triggers
- 52 functions
- 108 tables
- 380 stored procedures
WSUS attacks: Black Hat USA 2015, WSUSpect
State-of-the-art

1. Get a mitm position

Enterprise network

WSUSpect

Microsoft Update

WSUS server

WSUS clients
State-of-the-art

2. Intercepts new update queries
State-of-the-art

3. Infects the on-network metadata with a new, malicious update
State-of-the-art

4. The client sees a new available and installable update
5. Fetches the related binary
6. Checks if binary signature is okay: it is.
7. Installs the binary, with SYSTEM privileges, with metadata command-line arguments
WSUS attacks: Black Hat USA 2015, WSUSpect

Awesome attack!

But some limitations:
- Gain a mitm position
  - Meaning no network limitation is in place
- Get a useful one
  - Meaning TLS has to be disabled

→ Doesn’t give us access to the ESAE-managed domain controllers 😞
So, where are we?

We know:
- That injecting into the metadata between WSUS server/client is possible
- Where metadata are stored: in the database
- How to connect to this database

We want:
- To inject a metadata to compromise a client, without a network attack
So, where are we?

We know:
- That injecting into the metadata between WSUS server/client is possible
- Where metadata are stored: in the database
- How to connect to this database

We want:
- To inject a metadata to compromise a client, without a network attack

So, let’s try to inject a new update into the database!
So, where are we?

We know:
- That injecting into the metadata between WSUS server/client is possible
- Where metadata are stored: in the database
- How to connect to this database

We want:
- To inject a metadata to compromise a client, without a network attack

So, let’s try to inject a new update into the database!

...let’s start by studying how updates are inserted...
How to check for inserted rows on SQLServer?

First try:
- Look for update information in tables
How to check for inserted rows on SQLServer?

First try:
- Look for update information in tables
- Find update information in some tables
How to check for inserted rows on SQLServer?

First try:
- Look for update information in tables
- Find update information in some tables
- Try to insert data in one of the identified tables
How to check for inserted rows on SQLServer?

First try:
- Look for update information in tables
- Find update information in some tables
- Try to insert data in one of the identified tables
- Get slapped by a trigger...
How to check for inserted rows on SQLServer?

First try:
- Look for update information in tables
- Find update information in some tables
- Try to insert data in one of the identified tables
- Get slapped by a trigger...
- Read and understand the trigger
How to check for inserted rows on SQLServer?

First try:
- Look for update information in tables
- Find update information in some tables
- Try to insert data in one of the identified tables
- Get slapped by a trigger...
- Read and understand the trigger
- Try to respect this trigger by inserting into another table
How to check for inserted rows on SQLServer?

First try:
- Look for update information in tables
- Find update information in some tables
- Try to insert data in one of the identified tables
- Get slapped by a trigger...
- Read and understand the trigger
- Try to respect this trigger by inserting into another table
- Second slap, this time by a foreign key...
How to check for inserted rows on SQLServer?

First try:
- Look for update information in tables
- Find update information in some tables
- Try to insert data in one of the identified tables
- Get slapped by a trigger...
- Read and understand the trigger
- Try to respect this trigger by inserting into another table
- Second slap, this time by a foreign key...
- Study the relation between tables
How to check for inserted rows on SQLServer?

First try:
- Look for update information in tables
- Find update information in some tables
- Try to insert data in one of the identified tables
- Get slapped by a trigger...
- Read and understand the trigger
- Try to respect this trigger by inserting into another table
- Second slap, this time by a foreign key...
- Study the relation between tables
- Take an aspirin
How to check for inserted rows on SQLServer?

First try:
- Look for update information in tables
- Find update information in some tables
- Try to insert data in one of the identified tables
- Get slapped by a trigger...
- Read and understand the trigger
- Try to respect this trigger by inserting into another table
- Second slap, this time by a foreign key...
- Study the relation between tables
- Take an aspirin
- Try to insert data into a table to respect the trigger and the foreign keys constraints
How to check for inserted rows on SQL Server?

First try:
- Look for update information in tables
- Find update information in some tables
- Try to insert data in one of the identified tables
- Get slapped by a trigger...
- Read and understand the trigger
- Try to respect this trigger by inserting into another table
- Second slap, this time by a foreign key...
- Study the relation between tables
- Take an aspirin
- Try to insert data into a table to respect the trigger and the foreign keys constraints
- Get kicked by another trigger
How to check for inserted rows on SQLServer?

First try:
- Look for update information in tables
- Find update information in some tables
- Try to insert data in one of the identified tables
- Get slapped by a trigger…
- Read and understand the trigger
- Try to respect this trigger by inserting into another table
- Second slap, this time by a foreign key…
- Study the relation between tables
- Take an aspirin
- Try to insert data into a table to respect the trigger and the foreign keys constraints
- Get kicked by another trigger…
- Throw laptop across the room
How to check for inserted rows on SQLServer?

Second try:
- Define triggers on tables (remember: 108 tables) to trace inserts
- Get SQLServer to activate audit logs

Way too complicated...
SQL profiler to the rescue

- Monitors SQL queries as done on the database
- Use it while WSUS is synchronizing with Microsoft Update

Import update sample:

Notice the horizontal slider? It's a very large XML
Isolate the right calls

- WSUS service is only using stored procedure calls

- Calls five stored procedures to insert one update:
  - spImportUpdate
  - spSaveXmlFragment (actually called a bunch of times)
  - spSetBatchURL
  - spDeploymentAutomation
  - spProcessPrerequisitesForRevision
Isolate the right calls

- WSUS service is only using stored procedure calls

- Calls five stored procedures to insert one update:
  - spImportUpdate
  - spSaveXmlFragment (actually called a bunch of times)
  - spSetBatchURL
  - spDeploymentAutomation
  - spProcessPrerequisitesForRevision
- Lessons learned:
  - Image-typed columns can store cab files
    - Which can store a file named “blob”
    - Which can store an even bigger XML
    - Ones bigger than SQLServer’s NVARCHAR max size (8K)

\[
\text{spSaveXmlFragment NULL,4D53434600000000FB07...}
\]
- Lessons learned:
  - Minimalization cannot be pushed too far
    - Works on Windows 7 and Windows 10:1607
Copy/Paste a valid update

- Lessons learned:
  - Minimalization cannot be pushed too far
    - Works on Windows 7 and Windows 10: 1607
    - Doesn’t work on versions in-between
    - Doesn’t work on server versions

- Windows 8
  - 2008(R2)
  - 2012(R2)

- 1511

- 1607

- 2016
Introducing WSUSpendu®

Open-source: https://github.com/AlsidOfficial/WSUSpendu

Microsoft Update

Enterprise network

WSUS server

WSUS clients

Thx Maman
Introducing WSUSpendu

1. Injects update metadata in the database, signed binary in the Web service
Introducing WSUSpendu

2. The client sees a new available and installable update
Introducing WSUSpendu

3. Fetches the related binary
Introducing WSUSpendu

4. Checks if binary signature is okay: it is.
Introducing WSUSpendu

5. Installs the binary, with SYSTEM privileges, with metadata command-line arguments
What if a WSUS server serves updates to the DCs?
Compromise an ESAE-managed forest

Tier 2

Tier 1

Tier 0

WSUS server
Compromise an ESAE-managed forest

Tier 2

Tier 1

WSUS server

Tier 0
Sometimes, even compromise the ESAE forest itself

- WSUS server in the ESAE, which distributes its updates to the ESAE resources
Sometimes, even compromise the ESAE forest itself

- WSUS server in the ESAE, which distributes its updates to the ESAE resources
- This WSUS server takes its updates from the production environment
  - Not in Microsoft ESAE's blueprint, but happens （-deals）
Sometimes, even compromise the ESAE forest itself

- WSUS server in the ESAE, which distributes its updates to the ESAE resources
- This WSUS server takes its updates from the production environment
  - Not in Microsoft ESAE's blueprint, but happens「(つodus)」
  - Technically possible due to WSUS server-chaining
Upstream/Downstream update servers notion

Microsoft Update → WWW

HTTPS

WWW → WSUS

HTTP

WSUS → WSUS clients

Enterprise network
Upstream/Downstream update servers notion

Enterprise network

WSUS1

WSUS1 clients

WWW

Microsoft Update

HTTPS

HTTP

WSUS2

www

Yves Le Provost & Romain Coltel
Upstream/Downstream update servers notion

Microsoft Update

WWW

HTTPS

HTTP

Enterprise network

WSUS1

WSUS1 clients

WSUS2

WSUS2 clients
Upstream/Downstream update servers notion

Microsoft Update

WWW

HTTPS

HTTP

Enterprise network

WSUS Upstream

WSUS clients

WSUS clients

WSUS Downstream

Yves Le Provost & Romain Coltel
Upstream/Downstream update servers notion

Microsoft Update

www

HTTPS

HTTP

WSUS

Upstream

WSUS clients

WSUS clients

Enterprise network

Downstream
Upstream/Downstream update servers notion

Enterprise network

WSUS

Microsoft Update

WWW

HTTPS

HTTP

WSUS clients

WSUS clients

WSUS clients
Upstream/Downstream update servers notion

Microsoft Update

Enterprise network

WSUS

Downstream

HTTP

HTTPS

WSUS clients

Microsoft Update

WWW

Yves Le Provost & Romain Coltei
Upstream/Downstream update servers notion

Upstream

Microsoft Update

HTTPS

WWW

WSUS Downstream

Downstream

WSUS clients

WSUS clients

Enterprise network

HTTP
Compromising Microsoft’s most secure environment was almost too easy.
We need to go deeper...
Disconnected network case

Internet-connected network
Disconnected network case

Internet-connected network

Disconnected network

Physical boundary
Using disconnected network

Why?
- Protect sensitive data, classified information
- Protect industrial networks
- Just don’t want to be connected to the Internet...
Using disconnected network

Why?
- Protect sensitive data, classified information
- Protect industrial networks
- Just don’t want to be connected to the Internet...

For which security improvement?
- Isolation as protection
- "No reach, no issue"
Using disconnected network

Why?
- Protect sensitive data, classified information
- Protect industrial networks
- Just don’t want to be connected to the Internet...

For which security improvement?
- Isolation as protection
- "No reach, no issue"

Is it sufficient? ... Due to sensitivity, you have to:
- continue securing your network/servers/apps/...
- thus, stay up-to-date
Updates for disconnected network

Microsoft Update

WWW

HTTPS

HTTP

WSUS

Enterprise network

WSUS clients

Microsoft Update

SSL
Updates for disconnected network

Microsoft Update → WWW (HTTPS)

Enterprise network

WSUS

WSUS clients

External device

Microsoft Update → WSUS (HTTP)

External device → WSUS (HTTPS)
Updates for disconnected network

Microsoft Update

HTTPS

WWW

HTTP

WSUS

Enterprise network

WSUS clients

External device

WSUS on disconnected network
Get updates to the disconnected network

Microsoft solution:
- wsusutil, export / import tool for metadata
- Binaries need to be transferred manually

Note:
It can take three to four hours for the WSUS database to validate newly imported content.
Get updates to the disconnected network

Microsoft solution:
- `wsusutil`, export / import tool for metadata
- Binaries need to be transferred manually

Mostly-used solution:
- WSUS on a Virtual Machine
- Clone the VM
- Transfer the clone onto the disconnected network

**Note**

It can take three to four hours for the WSUS database to validate newly imported content.
Once metadata are imported, still needs approbation  
- Approbation through auto-approval rules  
- Social Engineering

Airgap-attack ready  
- Inject malicious update in database  
- Disconnected database is syncronised with connected database  
- Update is approved and deployed  
- Payload is executed on designated target...
Compromise a disconnected network

Internet-connected network

Disconnected network

Physical boundary
Compromise a disconnected network

Internet-connected network

Disconnected network

Physical boundary
Compromise a disconnected network

Internet-connected network

Disconnected network

Physical boundary
That’s scary and all good, but how do I **protect** myself?
How to protect your architecture

WSUS recommendations
- Activate TLS

Windows Server Update Services allows administrators to manage the download and installation of updates from the Microsoft Update website to the local network.

Things to note:
- At least one WSUS server in a network must be able to download updates from Microsoft Update. Other WSUS servers can get updates either from that server or from Microsoft Update.

WSUS server-to-server and server-to-client communications should be set up to use the Secure Sockets Layer (SSL).
How to protect your architecture

WSUS recommendations
- Activate TLS
- Include WSUS server in tier-0

Tier 2

Tier 1

WSUS server

Tier 0

www
WSUS recommendations
- Activate TLS
- Include WSUS server in tier-0
How to protect your architecture

WSUS recommendations
- Activate TLS
- Include WSUS server in tier-0
How to protect your architecture

WSUS recommendations
- Activate TLS
- Include WSUS server in tier-0
How to protect your architecture

WSUS recommendations
- Activate TLS
- Include WSUS server in tier-0
How to protect your architecture

WSUS recommendations
- Activate TLS
- Include WSUS server in tier-0
- Independant network $\rightarrow$ Independant WSUS server

Physical boundary

Internet-connected network

Disconnected network
How to protect your architecture

WSUS recommendations
- Activate TLS
- Include WSUS server in tier-0
- Independant network  → Independant WSUS server

- Dedicated network
- Internet-connected network
- Physical boundary
- Disconnected network
WSUS recommendations
- Activate TLS
- Include WSUS server in tier-0
- Independant network → Independant WSUS server
Seen on a Windows 10 1703 (Creators update):

“[metadataintegrity]GetFragmentSigningConfig failed with 0x8024402C. Using default enforcement mode: Audit.”
Stop updating
Conclusion

Stop updating 😊

Control relationship WSUS server → clients
Thank you all.