WSUSpendu

USE WSUS TO HANG ITS CLIENTS

Yves Le Provost & Romain Coltel
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
Sometimes, compromising a network is not that easy.
Compromise scenario

You
Compromise scenario

Internet-connected network

Domain controllers

Servers

Workstations

You
Compromise scenario

Internet-connected network

Domain controllers

Servers

Workstations

You
Compromise scenario

Internet-connected network

Domain controllers

Servers

Workstations

You
Compromise scenario

Internet-connected network

- Domain controllers
- Servers
- Workstations

Disconnected network

- Domain controllers
- Physical boundary
- Servers
- Workstations

You
Sometimes, **compromising** a network might not be as far as we think.
Potential compromise scenario

Internet-connected network

Disconnected network

Physical boundary
Potential compromise scenario

Internet-connected network

Disconnected network

Physical boundary

WSUS Server

WSUS Server
Windows Server Update Services (WSUS)

Enterprise network

Microsoft Update

HTTP

HTTPS

WWW

WSUS

Microsoft Update

HTTP

HTTPS

WWW

Enterprise network

WSUS
Windows Server Update Services (WSUS)

Microsoft Update → WSUS
  HTTPS
  HTTP

Enterprise network

WSUS

WSUS clients

Microsoft Update
WWW

Yves Le Provost & Romain Coltel
Windows Server Update Services (WSUS)

Microsoft Update

Enterprise network

WSUS upstream

WSUS downstream

WSUS clients

Microsoft Update

WWW

HTTPS

HTTP

Yves Le Provost & Romain Coltel
Windows Server Update Services (WSUS)

Enterprise network

WSUS upstream

WSUS downstream

Microsoft Update

External device

Disconnected WSUS

HTTPS

HTTP

HTTPS

WSUS clients

WSUS clients
Updates journey within a WSUS server

Microsoft Update

Windows service

Web service

Database

WSUS server

WSUS clients
Updates journey within a WSUS server

1. Windows service downloads update metadata (binaries size, download URL, command-line arguments, ...)

Microsoft Update

Windows service

Web service

Database

WSUS server

WSUS clients
2. Windows service transmits the metadata to the database

Microsoft Update

Windows service

Web service

Database

WSUS server

WSUS clients
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

Windows service

Web service

Database

WSUS server

WSUS clients

Microsoft Update

WSUS server

Windows service

Web service

Database
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
Updates journey within a WSUS server

1. Clients are looking for new updates.
2. Web service gets approved updates metadata from the database.
3. Metadata is sent to WSUS clients.

Microsoft Update

Windows service

Web service

Database

WSUS server

WSUS clients
Updates journey within a WSUS server

9. Web service transmits the metadata to the WSUS clients

Microsoft Update

Windows service

Web service

Database

WSUS server

WSUS clients

Microsoft Update

Web service transmits the metadata to the WSUS clients.
10. Each client evaluates if the updates is installable
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

Windows service

Web service

Database

WSUS server

WSUS clients

Microsoft Update

Microsoft Update

Microsoft Update

Microsoft Update

Microsoft Update

Microsoft Update

Microsoft Update
Updates journey within a WSUS server

13. Each binary is executed, with SYSTEM privileges, with possible command line parameters from the metadata.
WSUS attacks: Black Hat USA 2015, WSUSpect

State-of-the-art
State-of-the-art

1. Get a mitm position

Enterprise network

Microsoft Update

WSUS spect

WSUS server

WSUS clients
State-of-the-art

2. Intercepts new update queries
3. Infects the on-network metadata with a new, malicious update
4. The client sees a new available and installable update
5. Fetches the related binary
State-of-the-art

6. Checks if binary signature is okay: it is.
State-of-the-art

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 disconnected network 😞
Introducing WSUSpendu®

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

Enterprise network

Microsoft Update

WWW

WSUS
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
Demonstration...
Compromise a connected network

Internet-connected network

Disconnected network

Physical boundary
We need to go deeper...
Compromise a disconnected network
Compromise a disconnected network

Physical boundary

Internet-connected network

Disconnected network
Stop updating ☺

Control relationship WSUS server → clients
Thank you all.