master Code

2

README.md

WSUSpendu.ps1

README.md

WSUSpendu? What for?

At BlackHat USA 2015, the WSUSpect attack scenario has been released.

Approximately at the same time, some french engineers have been wondering if it would be possible to use a compromised WSUS server to extend the compromise to its clients, similarly to this WSUSpect attack. After letting this topic rest for almost two years, we've been able, at Alsid and ANSSI, to demonstrate this attack.

The `WSUSpendu.ps1` script is the accomplishment of the research. With it, a pentester can create a new update, inject it in the WSUS server database, and distribute it to the appropriate client. The binary will then

About

Implement WSUSpendu attack

wsus pentest airgap

Readme

Releases

No releases published

Packages

No packages published

Languages

PowerShell 100.0%

be executed on the client under the SYSTEM account, with the update-provided arguments.

Some limitations apply for using this tool, mainly the binary used by the [illegible] must be signed by Microsoft, or more generally, by a certificate approved for code signing in the *Trusted Root Certification Authorities* or the *Trusted Publishers* stores. You will also, obviously, need to get access to the WSUS database.

From our experience, the easiest way to get access to the WSUS database is to compromise the domain the WSUS server is in and use an administrator account. From that point, note that the WSUS service might be running as Network Service and that only this user might have th eright to connect to the database.

The topic has been presented during a talk at the French conference SSTIC-2017. Our slides and paper can be found here: https://www.sstic.org/2017/presentation/wsus_pendu/.

FAQ

How do I use this script?

Copy the script and the payload file - which has to be signed by Microsoft - to the WSUS server and run the script with the appropriate parameters (see `Get-Help Wsuspendu.ps1 -Examples`). Wait for the client to get its update and profit!

I've used WSUSpendu.ps1 but the update doesn't seem to be downloaded by the clients

Multiple possible answers here as this topic is very large:

- Firstly, did you approve the update? The script will automatically approve the update if you specify a computer during the update injection, but won't in any other case, so you'll have to manually approve your update or count on the autoapproval rules.

- Secondly, did you wait for the binary to be downloaded by the WSUS server before trying to force-update your client (in a lab environment for instance)? The WSUS server might take a while to download the binary you provided with the update, and the client doesn't see any new update until the binary is downloaded on the server.

I'm in the real world and not in a lab environment, I've done all that, why isn't my payload being executed on the clients?

You might find that your payload is executed, but that you cannot verify it due to network limitations. Another reason is the delay for the update to apply, as the Windows Update Agent on clients might not have yet received the fact that a new update is available.

Authors

Romain Coltel - Alsid Yves Le Provost - ANSSI