

[Home](#) [Services](#) [Products & Freebies](#)

[Case Studies](#) [Contact Us](#)

Posted on [2016-03-10](#)

[← Previous](#) [Next →](#)

Beyond good ol' Run key, Part 36

Last Updated 2023-02-25

Added xdbg32 from Trend Micro article.

Last Updated 2019-09-20

A few more updates thanks to [@bartblaze](#) !!!

Last Updated 2018-10-18

Updated mistake in tplcdclr.exe → wtsapi32.dll → wts.chm combo and added VeetlePlayer.exe → libvlc.dll → mtcReport.ktc; thanks to [@KyleHanslovan](#) !!!

Last Updated 2017-01-26

At the end of [last post](#) I mentioned PlugX. The idea used by this malware is pretty clever and relies on taking a legitimate signed .exe that is dependent on a DLL and swapping the DLL with the malicious replacement which – when loaded – decrypts/loads the final payload to memory. The trick used by PlugX is referred to as DLL Side-loading and I thought it will be nice to try summarizing various versions of this persistence trick described by various blogs.

The below are triplets describing the following PlugX components:

- legitimate .exe ['Source' refers to the article/blog/WP describing it]
 - DLL Side-loaded .dll
 - Payload

Here they are...

- ASHld.exe [\[Source\]](#)
 - ASHldRes.DLL
 - ASHldRes.DLL.asr
- CamMute.exe [\[Source\]](#)
 - CommFunc.dll
 - CommFunc.jax
- chrome_frame_helper.exe [\[Source PDF\]](#) Thx to [@bartblaze](#)
 - chrome_frame_helper.dll
 - chrome_frame_helper.dll.rom
- dvcemumanager.exe [\[Source\]](#)
 - DESqmWrapper.dll
 - DESqmWrapper.wrapper
- fsguidll.exe [\[Source\]](#)
 - fslapi.dll
 - fslapi.dll.gui
- fsstm.exe [\[Source\]](#)
 - FSPMAPL.dll
 - FSPMAPL.dll.fsp
- Gadget.exe [\[Source\]](#)
 - Sidebar.dll
 - Sidebar.dll.doc
- hhc.exe [\[Source\]](#)
 - hha.dll
 - hha.dll.bak
- hkcmd.exe [\[Source\]](#)
 - hccutils.dll
 - hccutils.dll.res
- LoLTWLauncher.exe [\[Source\]](#) Thx to [@bartblaze](#)
 - NtUserEx.dll
 - NtUserEx.dat
- Mc.exe [\[Source\]](#)

- McUtil.dll
 - McUtil.dll.url
- mcf.exe [\[Source\]](#)
 - mcutil.dll
 - mcf.ep
- mcupdui.exe [\[Source\]](#)
 - McUtil.dll
 - McUtil.dll.ping
- mcut.exe [\[Source\]](#)
 - McUtil.dll
 - mcutil.dll.bbc
- MsMpEng.exe [\[Source\]](#)
 - MpSvc.dll
 - MpSvc
- msseces.exe [\[Source\]](#) Thx to [@bartblaze](#)
 - mPclient.dll
 - msseces.asm
- NvSmart.exe [\[Source\]](#)
 - NvSmartMax.dll
 - boot.ldr
- OInfoP11.exe [\[Source\]](#)
 - OInfo11.ocx
 - OInfo11.ISO
- OleView.exe [\[Source\]](#)
 - ACLUI.DLL
 - ACLUI.DLL.UI
- OleView.exe [\[Source\]](#) Thx to [@KyleHanslovan](#)
 - iviewers.dll
 - <unknown>
- POETWLauncher.exe [\[Source\]](#) Thx to [@bartblaze](#)
 - NtUserEx.dll
 - NtUserEx.dat
- RasTls.exe [\[Source\]](#)
 - RasTls.dll
 - RasTls.dll.msc or RasTls.dll.config
- rc.exe [\[Source\]](#) Thx to [@KyleHanslovan](#)
 - rc.dll

- rc.hlp
- RunHelp.exe [\[Source\]](#)
 - ssMUIDLL.dll
 - ssMUIDLL.dll.conf
- sep_NE.exe [\[Source\]](#) Thx to [@KyleHanslovan](#)
 - winmm.dll
 - sep_NE.slf
- Setup.exe [\[Source\]](#)
 - msi.dll
 - msi.dll.dat
- sx.exe [\[Source\]](#) Thx to [@bartblaze](#)
 - SXLOC.DLL
 - SXLOC.ZAP
- tplcdclr.exe [\[Source\]](#) Thx to [@KyleHanslovan](#)
 - wtsapi32.dll
 - wts.chm
- Ushata.exe [\[Source\]](#)
 - Ushata.dll
 - Ushata.fox
- VeetlePlayer.exe [\[Source; PDF warning\]](#) Thx to [@KyleHanslovan](#)
 - libvlc.dll
 - mtcReport.ktc
- x32dbg.exe [\[Source\]](#)
 - x32bridge.dll
 - x32bridge.dat

There is also a potential combo:

- AFLogVw.exe [\[Source\]](#)
 - Ahnl2.dll
 - <unknown>

Now, a request – if you know any other combo that I have not included on the list, please let me know+provide a reference/source and I will add it to the list. Thanks!

This entry was posted in [Anti-Forensics](#), [Autostart \(Persistence\)](#), [Compromise Detection](#), [Forensic Analysis](#), [Incident Response](#), [Malware Analysis](#) by [adam](#). Bookmark the [permalink](#).

[Privacy Policy](#) | Proudly powered by [WordPress](#)