

Picking locky

By f0wL

Published: 2019-07-30 · Archived: 2026-04-06 00:38:55 UTC

Tue 30 July 2019 in [Ransomware](#)

Back in 2016 Locky was (one of) the first to commercialize the "art" of holding data for ransom. I picked this strain because I would like a bit more of a challenge in terms of obfuscation and anti-disassembly techniques, so strap in for this OG Ransomware

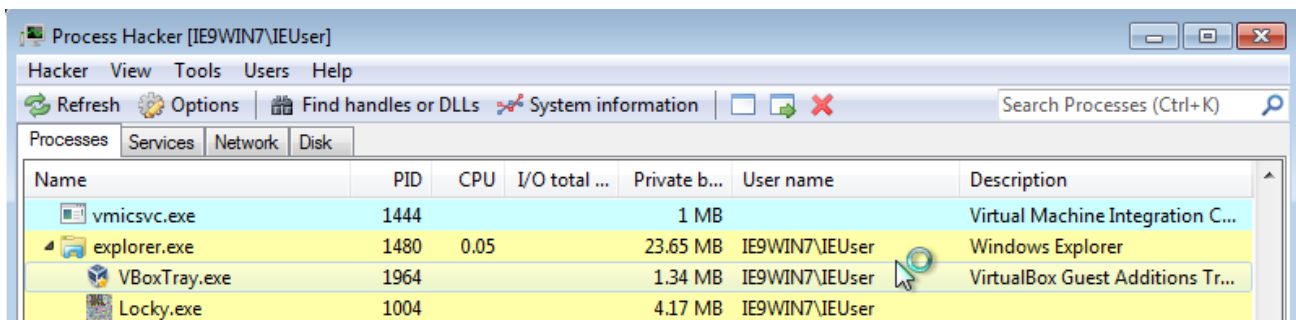
Locky (at least the first few versions) is said to be created by the makers of the Dridex/Cridex banking trojans. For example the spreading mechanism via macros in Word or Excel documents sent out via carefully crafted spear-phishing emails is exactly the same for both of these strains.

A general disclaimer as always: downloading and running the samples linked below will lead to the encryption of your personal data, so be f\$cking careful. Also check with your local laws as owning malware binaries/ sources might be illegal depending on where you live.

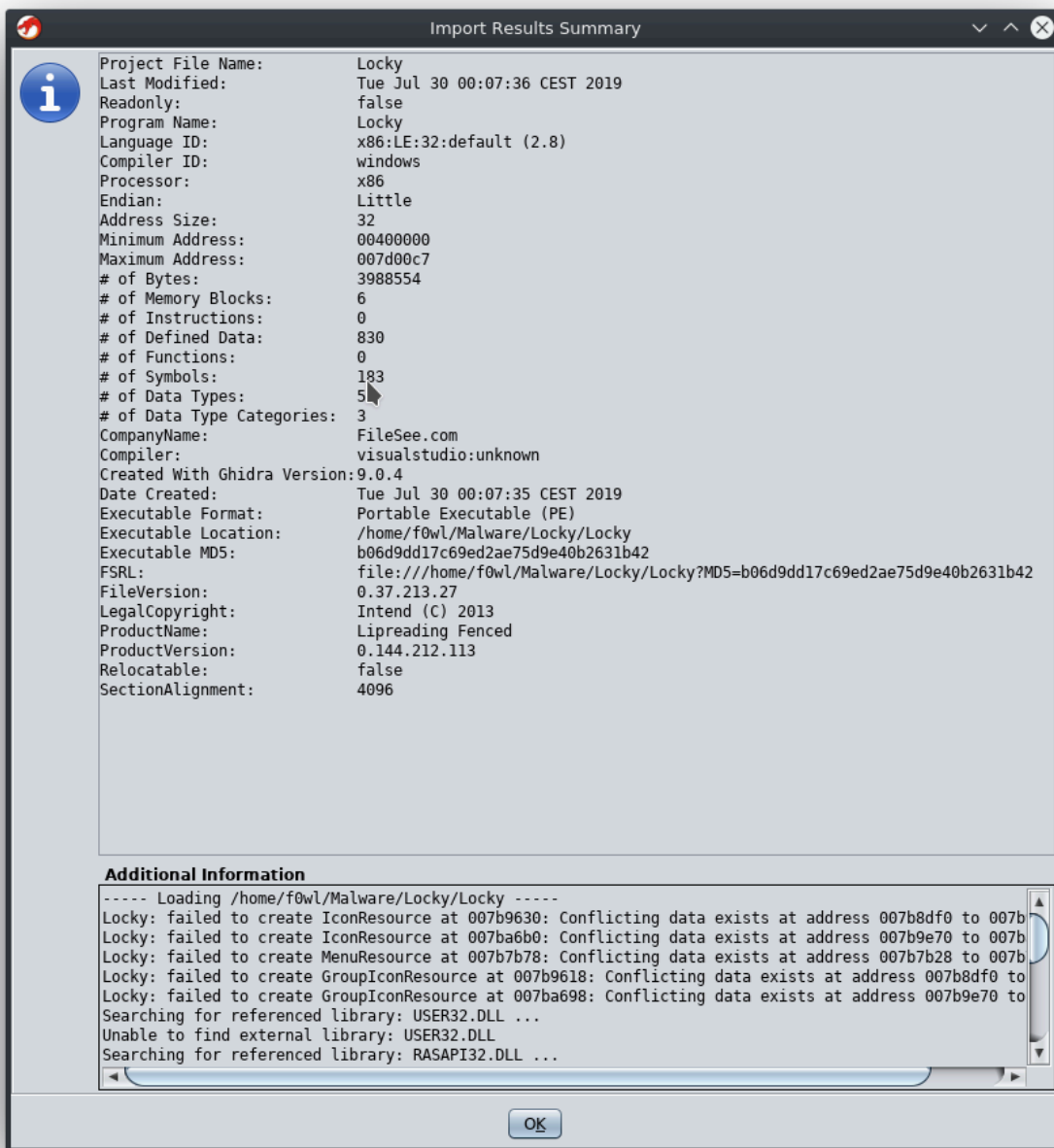
Todays samples are brought to you by:

Locky #1 available @ <https://github.com/ytisf/theZoo/tree/master/malwares/Binaries/Ransomware.Locky> sha256
bc98c8b22461a2c2631b2feec399208fdc4ecd1cd2229066c2f385caa958daa3

Locky.AZ available @ <https://dasmalwerk.eu/> sha256
2e4319ff62c03a539b2b2f71768a0cfc0adcaedbcca69dbf235081fe2816248b

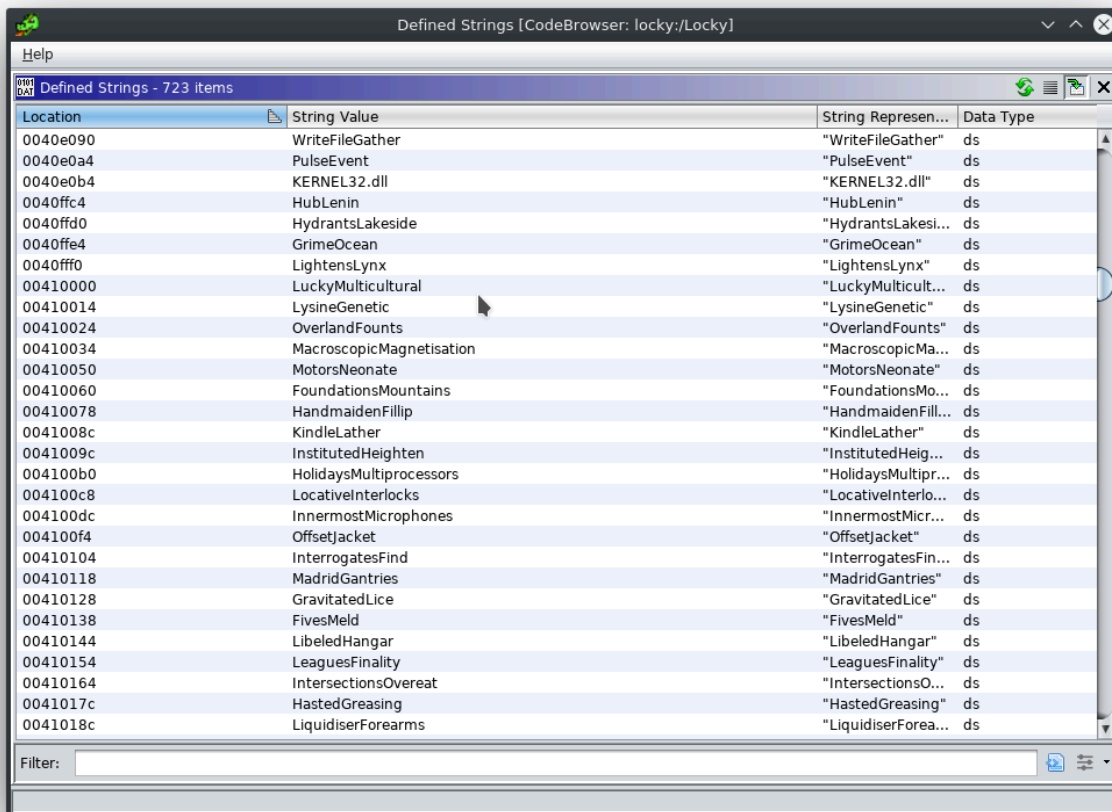


Running this first Locky Sample was pretty unspectacular since nothing really happend 🤔. Let's take a look at the binary first:





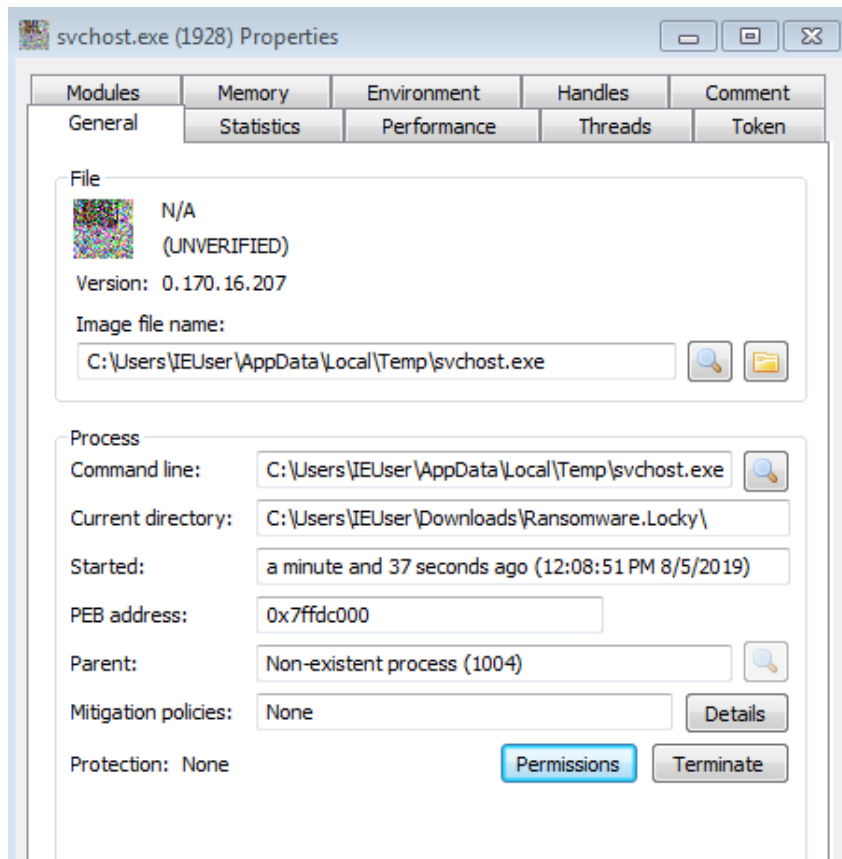
Would you look at that! We found ourselves some poor mans obfuscation :D A whole bunch of random strings to make the analyst's life just a little bit harder. We'll come back to this later to see if we can simplify our strings output a bit.



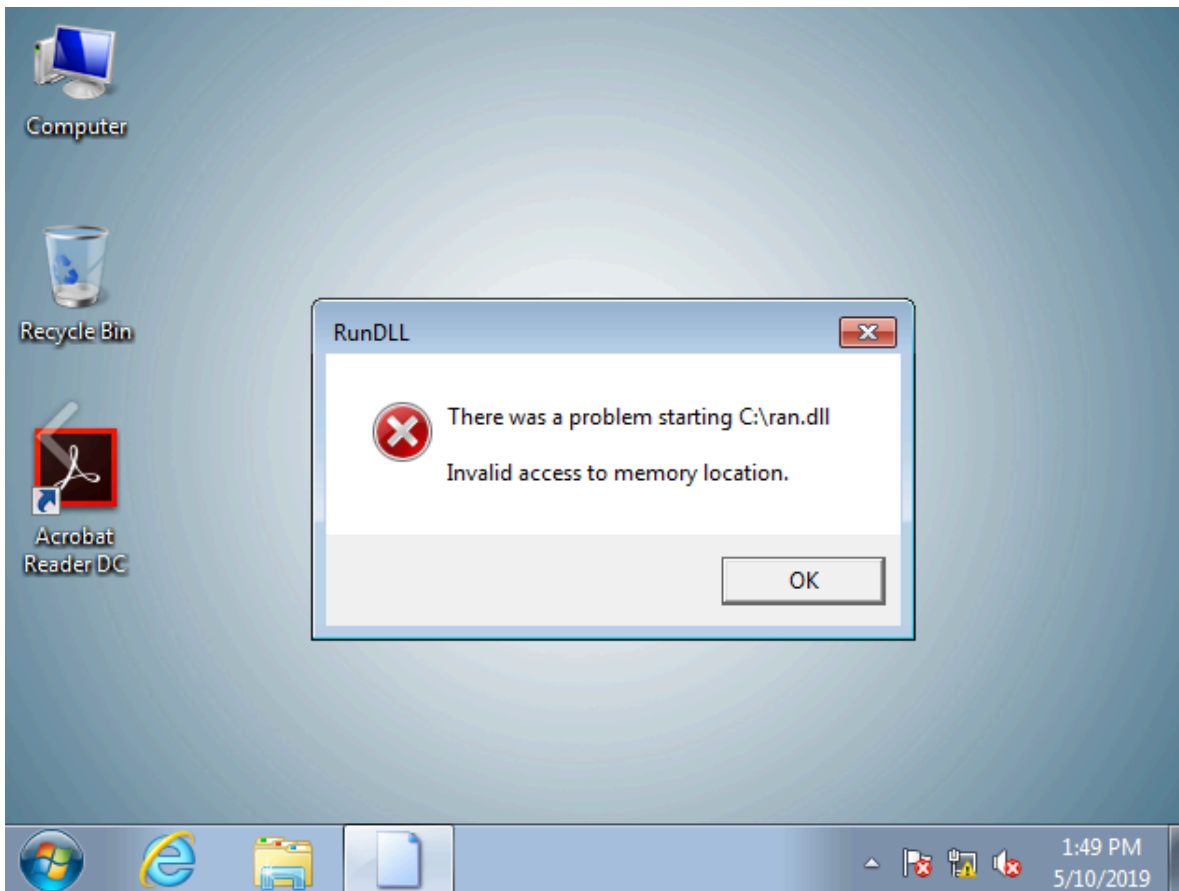
After a couple of seconds it spawns a new `svchost.exe` process with the same icon as `Locky.exe` had previously. Of course we'll dump the process memory to a file (just right-click the listing in Process Hacker and choose *Create dump* from the context menu).

ProcessHacker.exe	5068	1.28	7 MB	IE9WIN7\IEUser	Process Hacker
svchost.exe	1928		5.23 MB	IE9WIN7\IEUser	

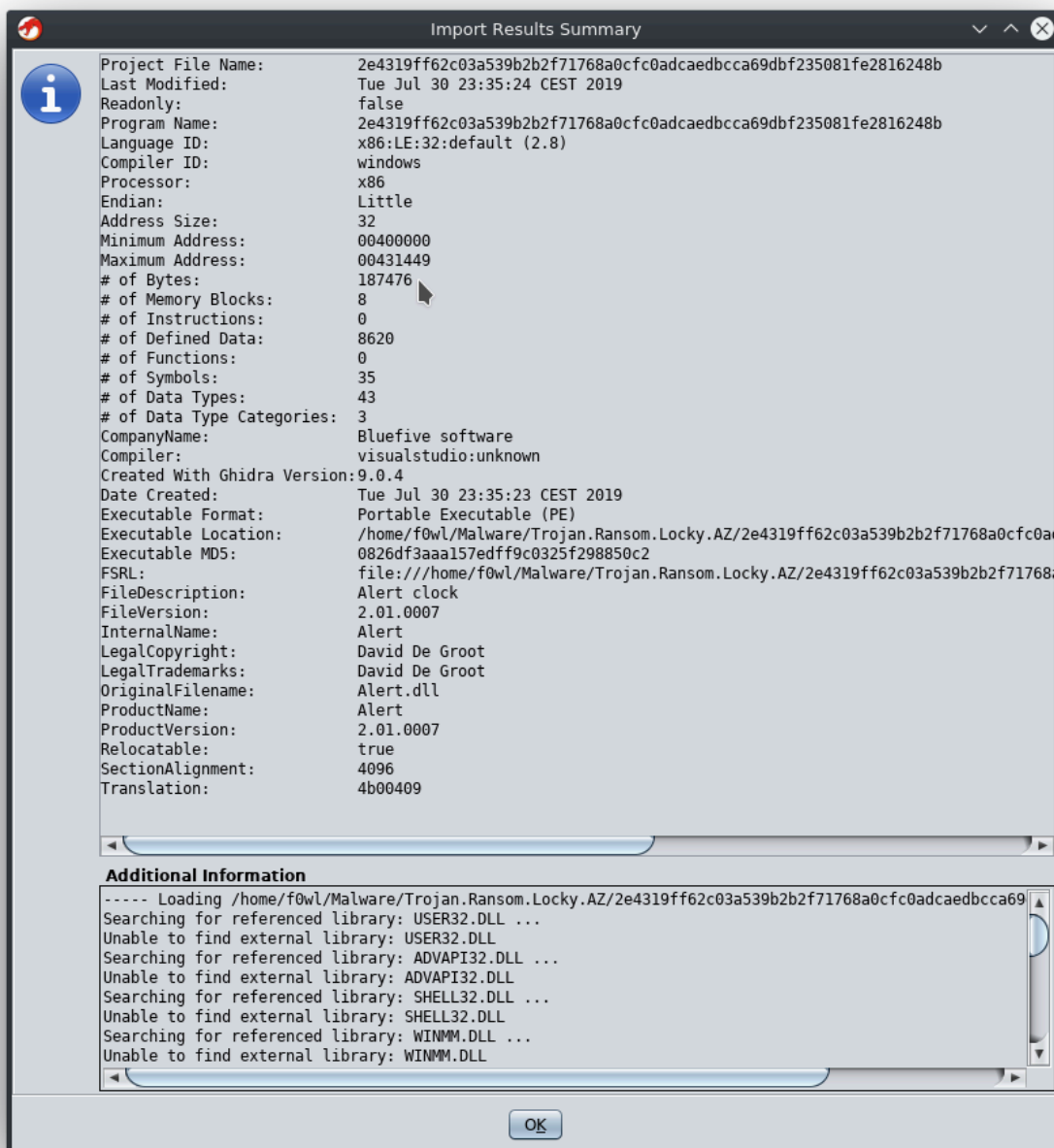
Looking at the properties of the new `svchost.exe` process we can see that it is actually run from `C:\Users\IEUser\AppData\Local\Temp\` and it's unsigned as well.



Trojan.Ransom.Locky.AZ



https://www.hybrid-analysis.com/sample/2e4319ff62c03a539b2b2f71768a0cfc0adcaedbcca69dbf235081fe2816248b/5cd5813d028838383d3ab408



This article is a work in progress, updates going to follow soon

IOCs

Locky (SHA256)

2e4319ff62c03a539b2b2f71768a0cfc0adcaedbcca69dbf235081fe2816248b
5ed2f09e648dca8f0ca75466b1442f6e599afddc80777e0559fb6881c6cd9ff3

3b60fde281d91cc3e7ea3e343ee5b13a31def564903c0136ae928f70e25c3c02
6afc78b5630726c907a69d62a6c8a7d86326e21383fe3aae1efc715342238e02

Source: <https://dissectingmalwa.re/picking-locky.html>