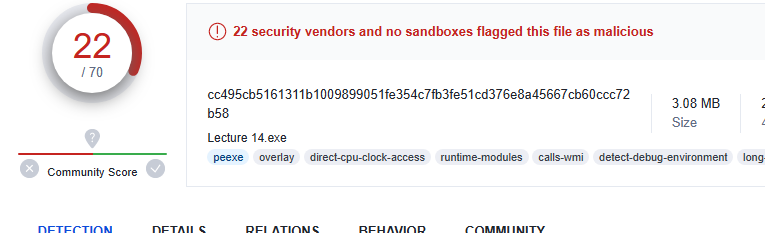
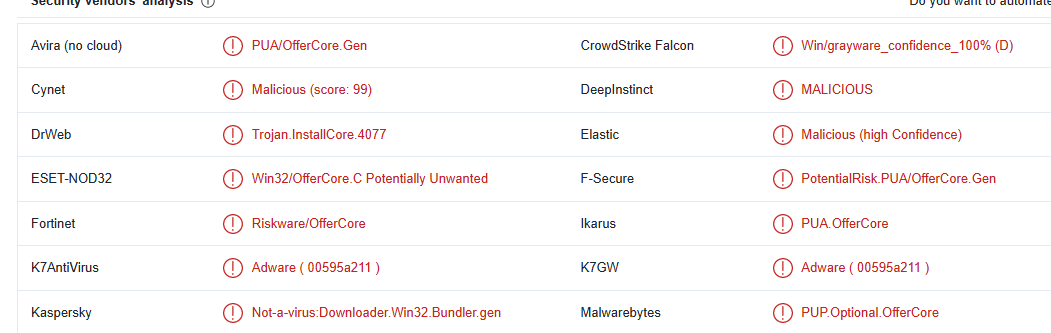
**Upload the file to**[**http://www.VirusTotal.com/**](http://www.virustotal.com/)**. Does the file match any existing antivirus signatures?**

Yes. It matches 22 of 70 vendor signatures.



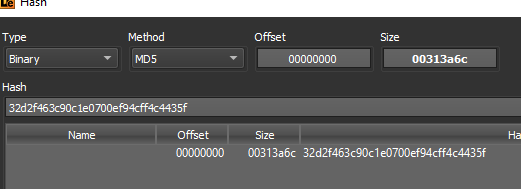
**What is this file known as?**

The security vendor naming conventions are quite generic and don’t point to a specific malware name. But based off of the naming conventions, it appears this might be adware. The CrowdStrike signature identifies it as “grayware”, not necessarily being malware but also not fully-legitimate. The other naming conventions suggest it is a PUP or PUA, so this is most likely part of a family of installers that install unwanted popups. Specifically, the name “OfferCore”, in conjunction with the other generic names, leads to this assumption. (Malware bytes definition of PUP OfferCore [here](https://www.malwarebytes.com/blog/detections/pup-optional-offercore)).



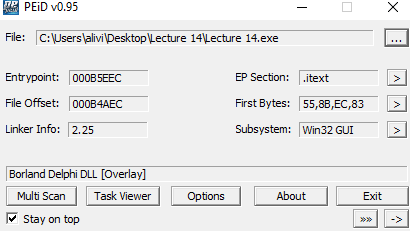
**What is the hash of the file?**

MD5: 32d2f463c90c1e0700ef94cff4c4435f

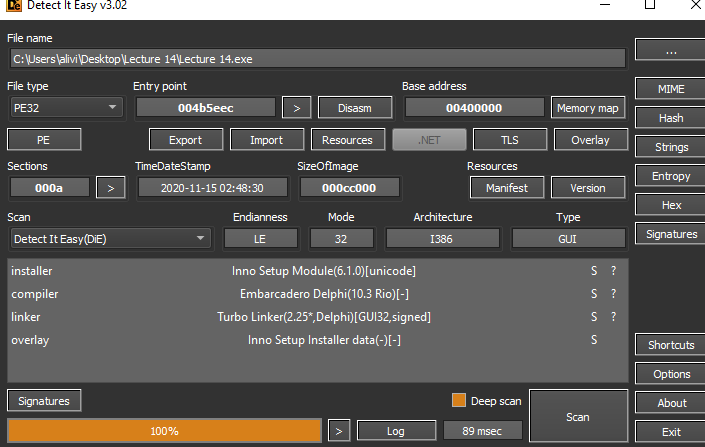


**Using the tools we have discussed so far, conduct your static analysis and present your findings. What stands out as a malicious "thing"**

The file could not be extracted with UniExtract nor 7zip due to the Borland Delphi DLL overlay. This is similar to last week’s discussion malware. Borland Delphi is an IDE that contains functionality to pack files.

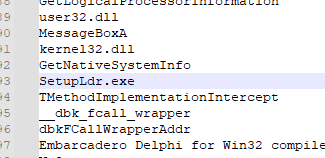


DIE found this too along with an installer that I do not recognize: Inno Setup Module. After a search, it is a free installer for Windows programs that can customize the installation process.

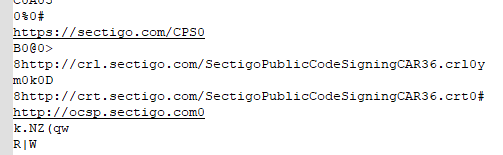


Strings

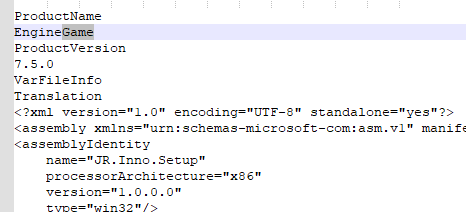
SetupLdr.exe was the only .exe import found. This isn’t suspicious in and of itself as it is a generic name. No .sys files were found.



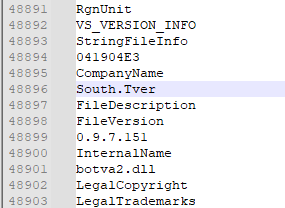
A website of sectigo.com was found, but it is a legitimate website that provides security solutions and digital certificates. Another website of comodoca.com was found, a legitimate digital certificate authority.



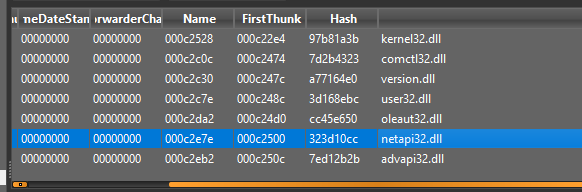
There were strings that indicated this file might be a game with the name of EngineGame. Most results from a search were for game engines (such as Unreal), but one URL of engine-game.com was suspiciously-generic.



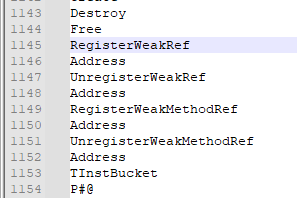
Two suspicious strings are “South.Tver” and “botva2.dll”. Apparently, South.Tver is the company that developed this program and botva2.dll is a file developed by them ([link](https://systemexplorer.net/file-database/file/botva2-dll/2860193)). On threatinfo.net [here](https://threatinfo.net/companies/South.Tver), this company is associated with one .dll file (isgsg.dll) that is identified as the Ramnit worm which creates a botnet and steals data ([link](https://www.f-secure.com/v-descs/virus_w32_ramnit.shtml)).



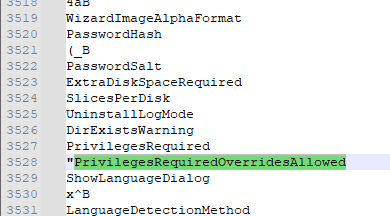
There are multiple .dll imports that are native to the Windows and have been discussed and analyzed in-depth in previous assignments. Unknown as to what the purpose of the PE is, it is tough to determine how any of these would be suspicious on their face.



There are registry-related strings, but are not part of normal Windows .dll files. Suspicious.

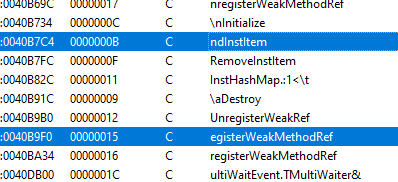


One specific string was the one highlighted below. This allows users to override security checks that require elevated privileges. It is not normal in PE files and therefore VERY suspicious. Additionally, there is the string PasswordHash which could prove useful to find during dynamic analysis in case this is a form of ransomware.

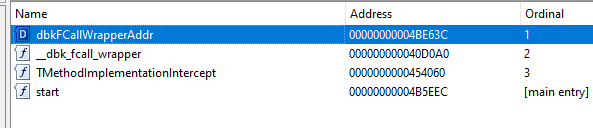


IDA

The strings window showed a pattern of the first character of strings being cut off on multiple occasions. Example:



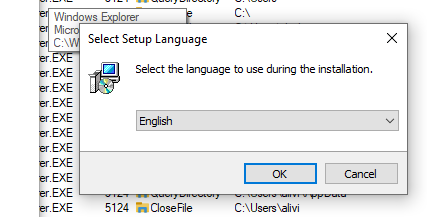
One export is dbkFCallWrapperAddr. This is associated with some malware, but it also might be a default .dll export for the Delphi IDE.



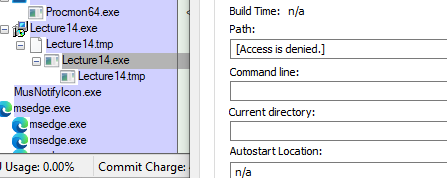
This program is enormous and IDA didn’t yield any findings that were particularly suspicious. If I had about 1,000 hours to pick through it, then maybe I could find something.

**Using the tools we have discussed so far, conduct your dynamic analysis and present your findings. What stands out as a malicious "thing"**

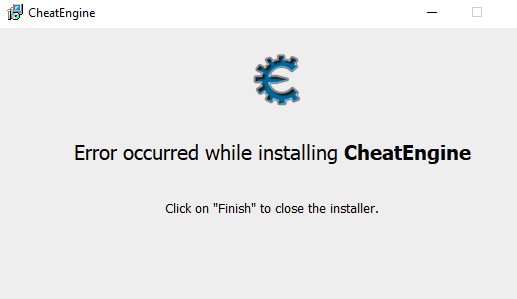
An initial run of the file through app.any.run showed that the file will bring up an installer window and also drop a PE in the Appdata\Local\Temp folder. The installer came up when it was run.



In Process explorer, the PE showed three child processes, but their paths were hidden when looking at the properties. The files were found in the expected folder, but only when the process was running.

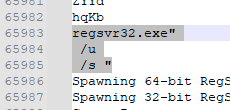


After clicking through, I was presented with an error window and closed it. Prior to this error message, there was a message that appeared briefly on the screen stating that it was downloading additional files. However, no network traffic was detected

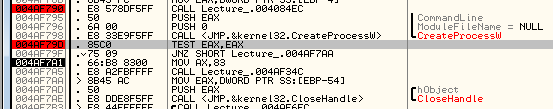


OllyDbg

When running Olly, a .tmp file was created in AppData\Local\Temp that contained a lot of string information. A command was found to ungregister a .dll file.



In the snippet below, the file creates a process which launches the installer window. However, every time it runs, it does the “jnz” instruction. This was bypassed by changing the EAX value from 1 to 0 prior to “test” being invoked.



The program did some file cleanup, such as removing the .tmp file, but I could not find anything that was inherently suspicious. Some registry values were created, but again, nothing that I could find overtly suspicious.

**Over the last 14 weeks, you have been able to tackle multiple types of malware. Would you consider this malware to be more difficult compared to the previous few weeks samples based of your experiences so far?**

Yes. I don’t even know what it does. I couldn’t find any new services created nor new drivers. No network traffic was detected. This is a very weird piece of malware that I could not find the answer to.

Go to two other students' posts and observe their findings. Post if you agree or disagree with their analysis.

* This would be the last part of the Modern Malware series, which one was your favorite.

<https://d2l.arizona.edu/d2l/le/1243099/discussions/threads/9853443/View>

<https://d2l.arizona.edu/d2l/le/1243099/discussions/threads/9855478/View>