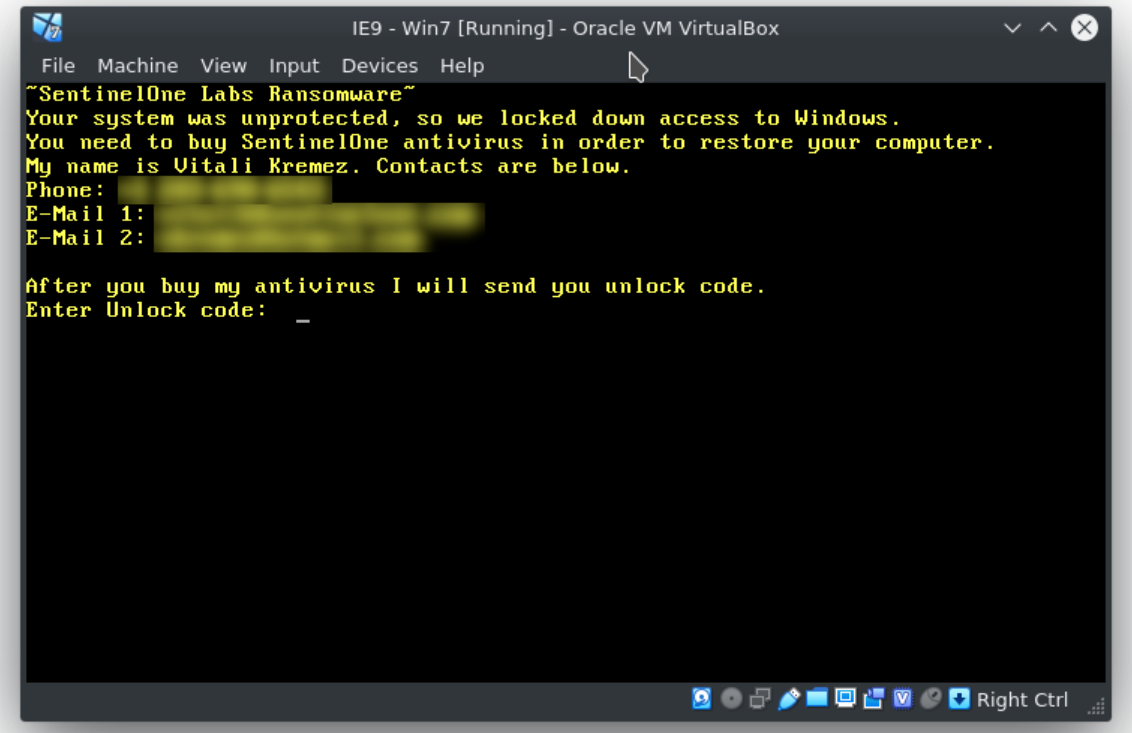
The Blame Game - About False Flags and overwritten MBRs

dissectingmalwa.re/the-blame-game-about-false-flags-and-overwritten-mbrs.html

Mon 13 April 2020 in Ransomware

MBR Lockers have become popular again with Skids. Let's look at a sample that was spread yesterday and caught a lot of attention.

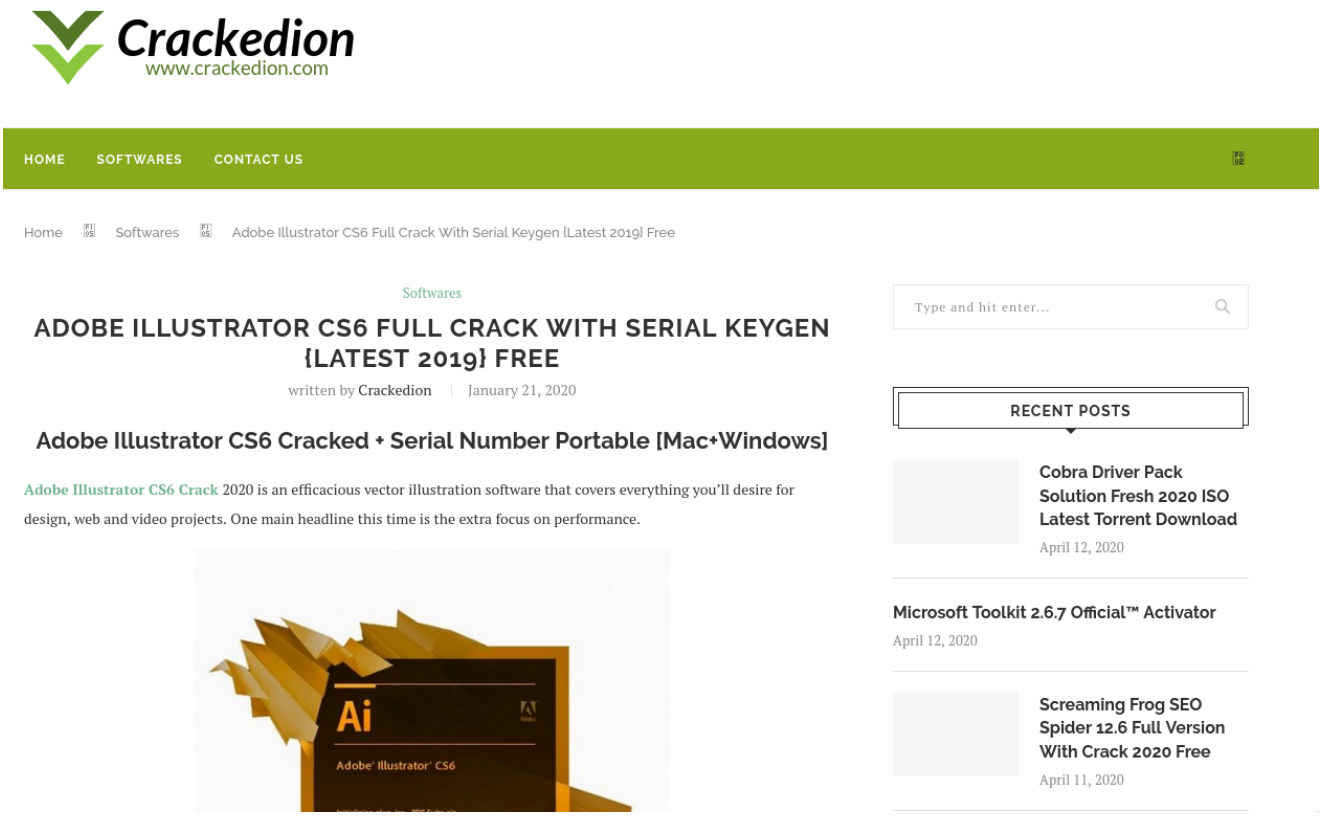
Let's start right off with a short introduction: The Malware analyzed here is a so-called MBR (Master Boot Record) Locker. It is targeting (like most of the time) only PCs running Windows. The good news is: in this case there is neither encryption nor deletion happening on the file system so there's a good chance for victims to recover their files. A possible mitigation for suers woulds be running MBRFilter which is developed by Talos Intelligence. Now to the Message displayed in the VM below: Pressing CTRL+ALT+ESC for a possible bypass / failsafe to boot the OS (described in this BleepingComputer article) doesn't seem to work for this sample.



After Vitali published the tweet below a whole crowd formed in the emerging thread to please unlock their PCs. Both Vitali Kremez and MalwareHunterTeam made it clear multiple times that they are not affiliated with this campaign in any way, but some of the victims still seemed to miss this fact and got quite worked up about their PCs being compromised. Unfortunately this was not the first and won't be the last time that respected ethical researchers are targeted in such decreditation acts. I'm not qualified to talk about any psychological reasoning behind such actions, but it's either an attempt to a Denial of Service (Vitalis Twitter DMs and Mentions were filled with complaints and accusations) or looking for attention (not in this case because there were no hints on the malware actors) like the Maze Team.

> [*] Beware: Some scams utilize my name and impersonate myself to amplify extortions. pic.twitter.com/wk9Mxkqxpz
>
> — Vitali Kremez (@VK_Intel) April 12, 2020

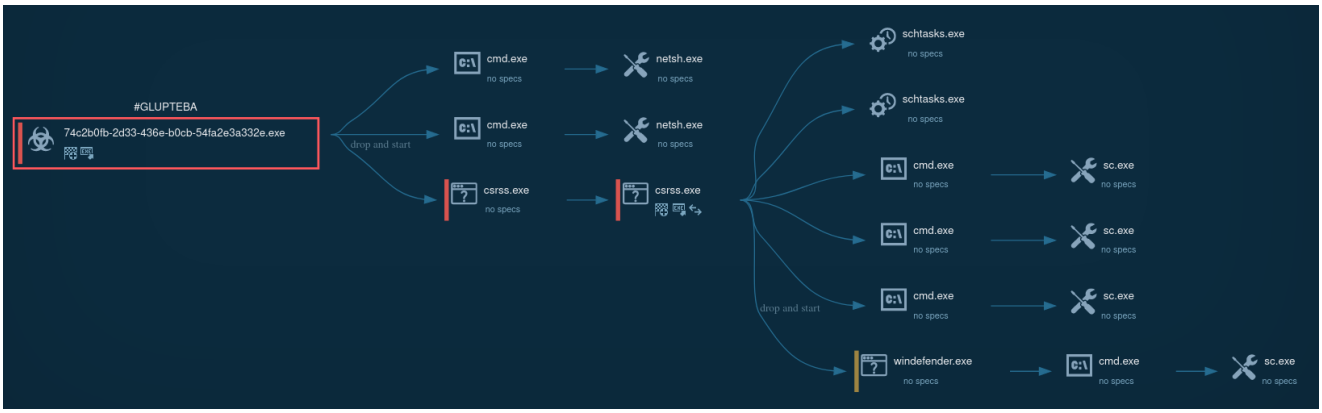
After talking to a victim to clarify the infection method and origin of the malware I received a link to this pirated Version of Adobe Illustrator. Lures like this one are often trojanized with malware or straight-up malicious from the start like in this case. Obviously this cannot be considered common knowledge for every user and this is what criminals are taking advantage of for years and years to come.



A quick check confirmed my suspicion that every download on this site is "spiked" with malware. The Filenames of the executables contain a unique-per-download string. The victim will be redirected to a second site where a user agent check for Windows and matching Browsers (IE, Edge) is performed. The executable is downloaded from another URL from a directory called **ru53332** which might give us a hint as to where the malware originated from (this looks like a client subfolder, this host might spread other strains as well).

```
├── Adobe+Illustrator+CS6+Full+Crack+With+Serial+Keygen+{Latest+2019}+Free-RTMD-ACPFlF7nlgAAvhwCAERFFwASAJB5ctUA.exe
├── windefender.exe
├── Winmon.exe
├── WinmonFS.exe
└── WinmonProcessMonitor.exe
```

Below you can see a process graph of the Glupteba Infection generated by Any.Run. This is just a subsection of the whole graph and since there was so much going on it was pretty difficult to make out if the MBR Locker actually was delivered with this installer. None of my tests in VMs or on a physical test machine resulted in a corrupted MBR, so at the moment I can neither confirm nor deny that the Locker was actually delivered via crackedion[.]com.



Interestingly all the executables named WinmonX.sys had broken certificate chains which should be a red flag for AVs running on the vicitims system. There were startup tasks scheuduled for all three of these files.

Signature Info

Signature Verification

⚠ A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider.

File Version Information

Date signed 9:39 PM 4/13/2020

X509 Signers

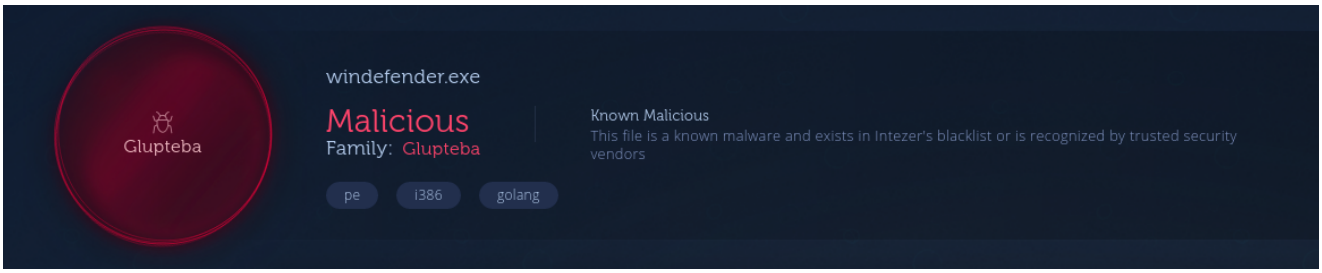
– WDKTestCert Admin,131480495282941941

Name	WDKTestCert Admin,131480495282941941
Issuer	WDKTestCert Admin,131480495282941941
Valid From	2017-08-24 11:58:49
Valid To	2027-08-24 00:00:00
Algorithm	sha1RSA
Thumbprint	B9C5C2EA53B67DFFD9F39E9BC76AF8F69F33CB55
Serial Number	6F 9A 31 7C FC FC 08 8B 4F 6E 19 8A 73 A1 19 CE

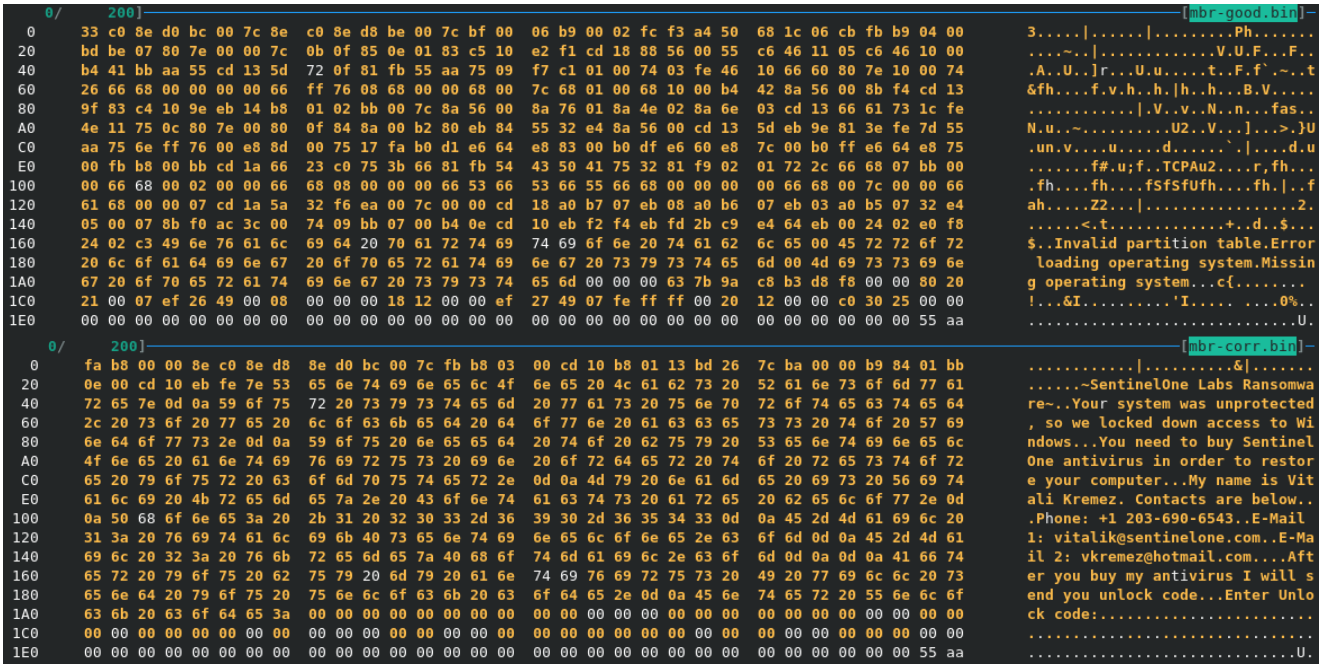
WinMonProcessManager contains a list of ca. 600 Anti-Virus executable names and it's only purpose is to disable all AV services while the trojan does its "magic":

```
exantivirus-cnet.exe, zonealarm.exe, ldnetmon.exe, norton_internet_secu_3.0_407.exe,
antivirus.exe, netmon.exe, AvastPE2.exe, avast_free_antivirus_setup_online.exe,
EmsisoftAntiMalwareSetup.exe, drweb32.exe, nod32.exe, f-prot95.exe, f-prot.exe,
drwebupw.exe, AvastUI.exe, mcshield.exe ... and so on 😉
```

The Detection Signatures from different engines on VT and the Intezer Analysis declared the dropped executables as parts of the Glupteba Trojan, which has been around for some time now. Additionally there were hints to another Strain called RanumBot that I have not ivestigated further up until now. In the screenshot you can see the **windefender.exe** sample that was submitted to Intezer. It was written in Go, packed with UPX and was stuffed with strings. I did not investigate this executable further, but at first I thought that this could have been the MBR Locker because it contains strings related to Poly1305/ChaCha20.



To show the effect of the MBR Locker on the OS Drive I simply used a live system to write the first sector of the Disk to a file (*sudo dd if=/dev/sdX of=mbrdump.bin bs=512 count=1*). The top dump shows the standard MBR contents and below is the corrupted version displaying only the message to the user.



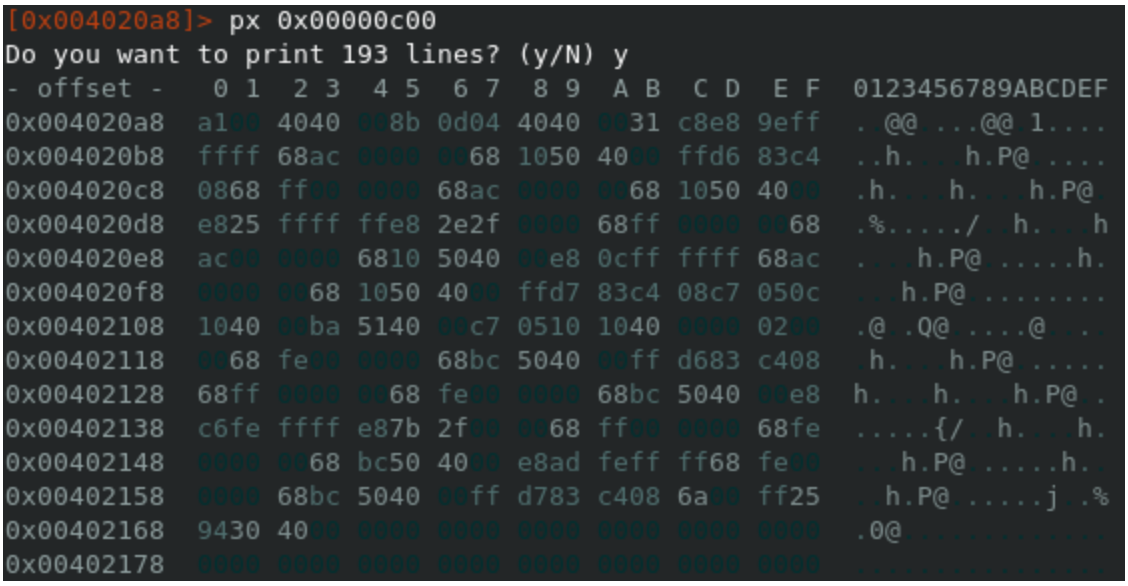
Reading the imports with Rabin2 there's nothing out of the ordinary, but there are a few things I wanted to see here. I expected to see CreateFile, which would be used to write the MBR Text playload to the first sector of the disk (**\\.\PhysicalDrive0**) later. Unlike Petya, which checked whether the PartitionStyle of the drive is actually an MBR (via DeviceIoControl), this MBR Locker isn't too concerned about that. There is also some generic anti-debugging via IsDebuggerPresent, but I didn't expect any further measures since the overall design of the malware is very poor.

```
"f sym.KERNEL32.DLL_imp.CloseHandle 0 0x00403088"
"f sym.KERNEL32.DLL_imp.CopyFileW 0 0x0040308c"
"f sym.KERNEL32.DLL_imp.CreateFileW 0 0x00403090"
"f sym.KERNEL32.DLL_imp.ExitProcess 0 0x00403094"
"f sym.KERNEL32.DLL_imp.GetModuleFileNameW 0 0x00403098"
"f sym.KERNEL32.DLL_imp.IsDebuggerPresent 0 0x0040309c"
"f sym.KERNEL32.DLL_imp.VirtualAlloc 0 0x004030a0"
"f sym.KERNEL32.DLL_imp.VirtualFree 0 0x004030a4"
"f sym.KERNEL32.DLL_imp.VirtualProtect 0 0x004030a8"
"f sym.KERNEL32.DLL_imp.WriteFile 0 0x004030ac"
"f sym.KERNEL32.DLL_imp.lstrcatW 0 0x004030b0"
"f sym.SHELL32.DLL_imp.SHGetSpecialFolderPathW 0 0x0040316c"
"f sym.SHELL32.DLL_imp.ShellExecuteW 0 0x00403170"
```

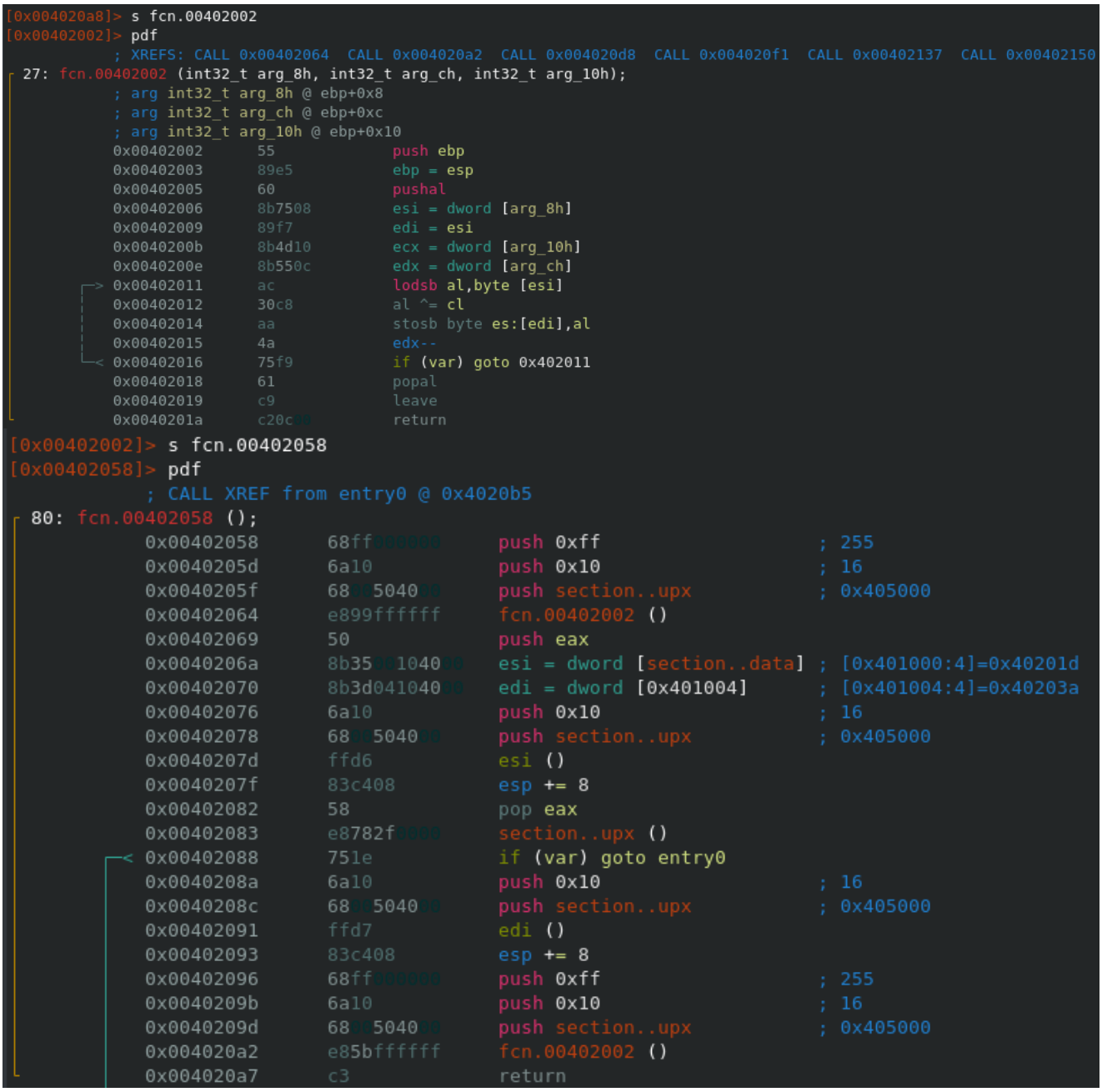
Taking a look at the sections of the binary we can spot a *.upx* section. This looks suspicious because a sample packed with UPX would have three sections named upx0 (packed), upx1 (stub) and optionally upx2 (unpacked) like in the image below.

```
nth paddr        size vaddr        vsize perm name
-------------------------------------------------
0   0x00000400  0x200 0x00401000  0x1000 -rw- .data
1   0x00000600  0x200 0x00402000  0x1000 -r-x .code
2   0x00000800  0x200 0x00403000  0x1000 -rw- .idata
3   0x00000a00  0x200 0x00404000  0x1000 -r-- .rsrc
4   0x00000c00  0x400 0x00405000  0x1000 -rw- .upx
nth paddr           size vaddr          vsize perm name
------------------------------------------------------
0   0x00000200       0x0 0x00401000  0x2af000 -rwx UPX0
1   0x00000200  0x1e4c00 0x006b0000  0x1e5000 -rwx UPX1
2   0x001e4e00     0x200 0x00895000    0x1000 -rw- UPX2
```

Printing the contents of the **.upx** section we can see that the text payload is encrypted.



The decryption routine is found very quickly since the executable only contains three functions in total. As one might have guessed already the text payload is XORed and therefore has to be decrypted before writing to the MBR. The screenshot below shows the decryption function and south of that you can see the text extraction out of the **.upx** section we discussed earlier.



The good-ish news is, that in this case the changes made to the Master Boot Record are reversible with a Backup of the MBR Sector. Alternatively victims can try to repair the MBR with Microsoft's *bootrec /fixmbr and /fixboot*. Sucess in this case depends on the partition style of the Windows install (since the MBR in GPT layouts is reserved for protective Reasons; on MBR installs bootrec may not be able to recover the Partition table because the whole sector is overwritten. See Vitalis Tweet here). I verified on a physical GPT install that LBA 1 and following is not affected by the MBRLocker and should keep the GPT recoverable. TestDisk is theoretically capable of recovering both partitioning layouts. I'd advise victims to use File Recovery software like Photorec as an option for data recovery if a clean install is necessary.

In one case a victim contacted me about an additional STOP Ransomware Infection (.mpaj extension, online keyed), but at the moment I can't confirm that this incident happend in conjunction with the pirated Software Installer / MBRLocker.

As there is currently no public sample of the second version of the MBR Locker I will update this article once it is available. Stay tuned :)

MITRE ATT&CK

T1059 --> Command-Line Interface --> Execution

T1179 --> Hooking --> Persistence

T1215 --> Kernel Modules and Extensions --> Persistence

T1179 --> Hooking --> Privilege Escalation

T1112 --> Modify Registry --> Defense Evasion

T1179 --> Hooking --> Credential Access

T1012 --> Query Registry --> Discovery

IOCs

VK-Wiper MBR Locker

```
Glupteba related:
=================

Adobe+Illustrator+CS6+Full+Crack+With+Serial+Keygen+{Latest+2019}+Free-
UNIQUESTRING.exe --> SHA256:
5e00e50d04130b470825d6c1bd58542d32a0a4f52c4d6e6ff01ea1cfad8fce3e

SSDEEP: 98304:luH/zVSNmGHjYKNC/qPqaMy25WJTZsRvO6Y:8HBymGDY/O4ikvO

windefender.exe --> SHA256:
28e8776a07789daf08629815da0a6eb69613410912447c189a51002f54d956ca
                    SSDEEP:
49152:mFeWvXwa1xkJrwBskK0CCD/ozKc3k8HxmYfJpz4U+TiAGTeI6h6gHquAb7/i:CvXwaerwBIbKcrxmYfJ


Winmon.exe --> SHA256:
889fb266c4c01bb4ef67635249c8daeb641fc86ce62fc280b34beec415fb6129
               SSDEEP:
96:/XAUM8mqN18vwLvVfjm3ZAeyRYOiRIfad/WrJ37CgES:7pNuv2LSZA1fEWrR7vES

WinmonFS.exe --> SHA256:
eb0be2ac3833c843214a55b14c31125a7b600d5272bdf322c4871f42627576e4
                 SSDEEP:
384:WVYr1nH9XRl8iueNYUaNhuqO3t6PsPJVPswHEvDdvHqciss+E96Vg:vrRlFpaNhuqO3njovpPTtTK

WinmonProcessMonitor.exe --> SHA256:
f609c6656a0c451dafa5173df0cd848f7cb7f22c4f150f8d16716c12593de66c
                             SSDEEP:
384:s+B62cfu4RaQNDEiULv/oGUOY1wR7OLwOMEP5PkdkQE:sOmu4RLNAiUL/oGGS7OLDP5PkdkQE

MBR Locker V1:
==============

sentinelone.scr --> SHA256:
4cd23a989a8f196b1f49e5e66c6ecfa0cebf63f04950ae4d64127aaedda9e89c
                    SSDEEP:
48:Zvt+BLdtWU2ew9FRCfH8BArSXXmzdh4vMASG2HvzqEsG8V:Z1+9dtWU2ew9rC/8Kiidh4vMASNHvzB
```

URLs

```
hxxp://crackedion[.]com
hxxp://dataf0ral1[.]com
hxxp://1podcast[.]best/ru53332/
```

Ransomnote V1

```
~SentinelOne Labs Ransomware~
Your system was unprotected, so we locked down access to Windows.
You need to buy SentinelOne antivirus in orer to restore your computer.
My name is Vitali Kremez. Contacts are below.
Phone: [Redacted]
E-mail 1: [Redacted]
E-mail 2: [Redacted]

After you buy my antivirus I will send you unlock code.
Enter Unlock code:
```
