

The blame game - about false flags and overwritten mbrs

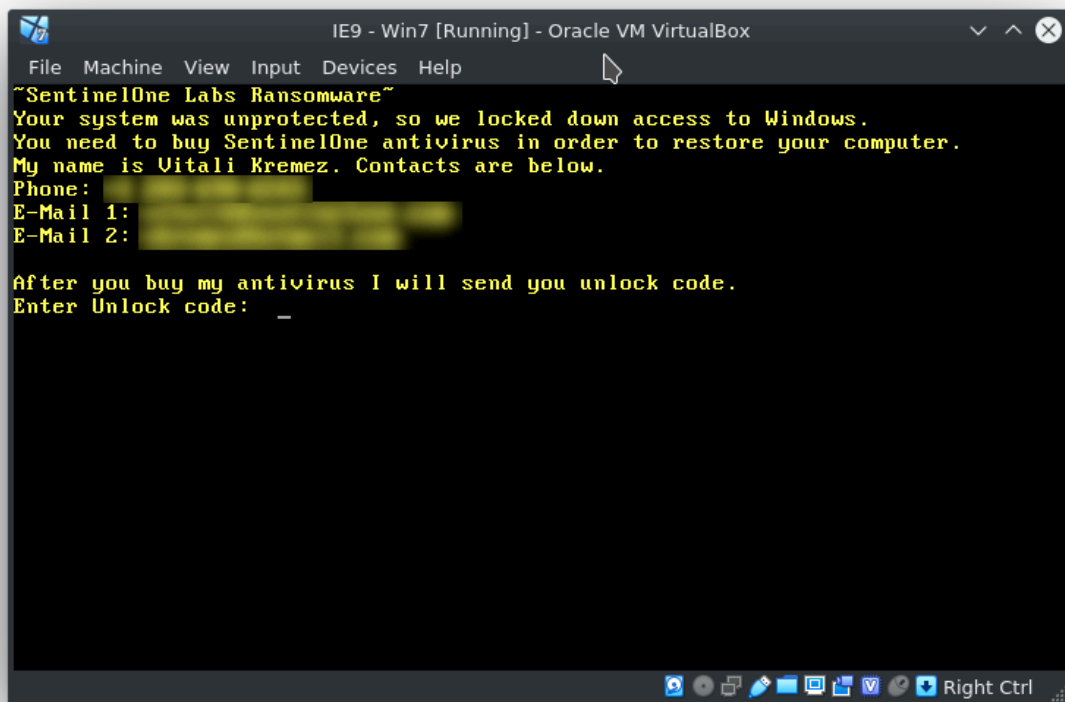
By f0wL

Published: 2020-04-13 · Archived: 2026-04-05 20:55:26 UTC

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 users would 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](#).

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.



HOME SOFTWARES CONTACT US

Home Software Adobe Illustrator CS6 Full Crack With Serial Keygen (Latest 2019) Free

Softwares

ADOBE ILLUSTRATOR CS6 FULL CRACK WITH SERIAL KEYGEN {LATEST 2019} FREE

written by Crackedion | January 21, 2020

Adobe Illustrator CS6 Cracked + Serial Number Portable [Mac+Windows]

Adobe Illustrator CS6 Crack 2020 is an efficacious vector illustration software that covers everything you'll desire for design, web and video projects. One main headline this time is the extra focus on performance.

RECENT POSTS

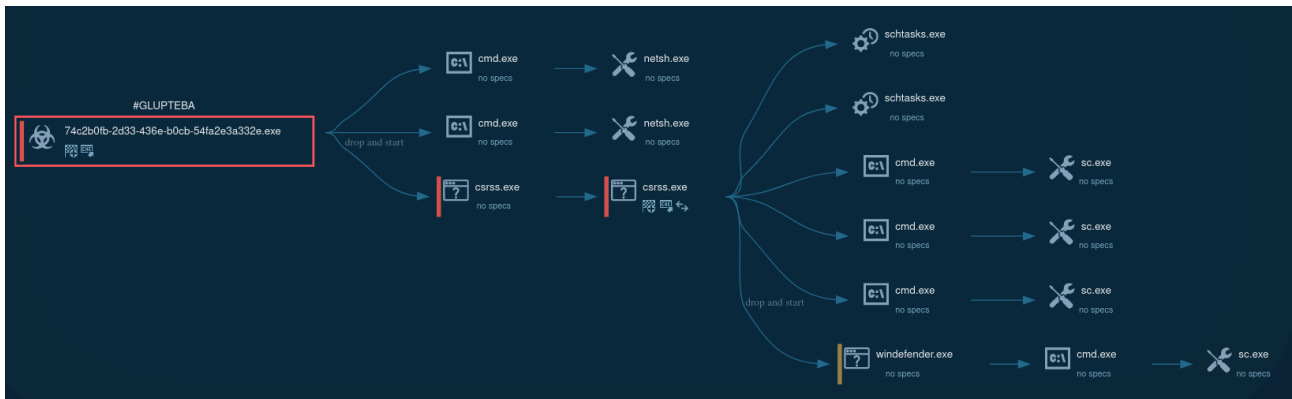
- Cobra Driver Pack Solution Fresh 2020 ISO Latest Torrent Download April 12, 2020
- Microsoft Toolkit 2.6.7 Official™ Activator April 12, 2020
- Screaming Frog SEO Spider 12.6 Full Version With Crack 2020 Free April 11, 2020

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-ACPF7nlgAAvhwCAERFFwASAJB5ctUA.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 victims system. There were startup tasks scheduled 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

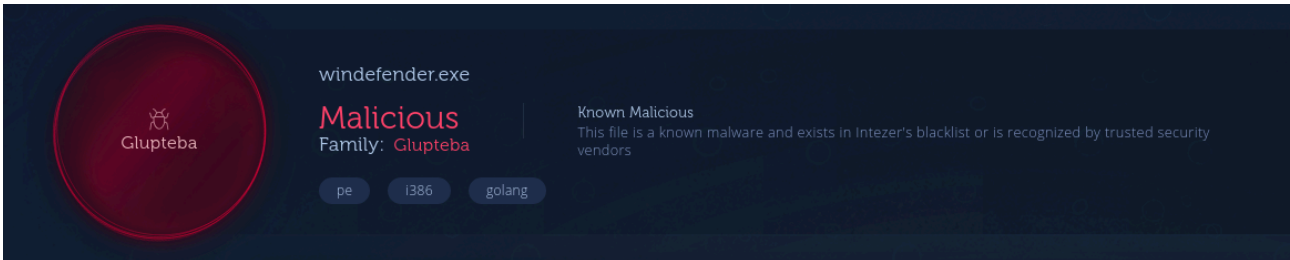
Name	WDKTestCert Admin,131480495282941941
Issuer	WDKTestCert Admin,131480495282941941
Valid From	2017-08-24 11:58:49
Valid To	2027-08-24 00:00:00
Algorithm	sha1RSA
Thumbprint	B9C5C2EA53B67DFFD9F39E9BC76AF8F69F33CB55
Serial Number	6F 9A 31 7C FC FC 08 8B 4F 6E 19 8A 73 A1 19 CE

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,

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 investigated 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.

```
0/ 200] [mbr-good.bin]
0 33 c0 8e d0 bc 00 7c 8e c0 8e d8 be 00 7c bf 00 06 b9 00 02 fc f3 a4 50 68 1c 06 cb fb b9 04 00 3.....|.....|.....Ph....|
20 bd be 07 80 7e 00 00 7c 0b 0f 85 0e 01 83 c5 10 e2 f1 cd 18 88 56 00 55 c6 46 11 05 c6 46 10 00 .....|.....|.....V.U.F...F..
40 b4 41 bb aa 55 cd 13 5d 72 0f 81 fb 55 aa 75 09 f7 c1 01 00 74 03 fe 46 10 66 60 80 7e 10 00 74 .A.U..]r...U.u.....t..F.f'~.t
60 26 66 68 00 00 00 00 66 ff 76 08 68 00 00 68 00 7c 68 01 00 68 10 00 b4 42 8a 56 00 8b f4 cd 13 &fh...f.v.h..h.|h..h...B.V....
80 9f 83 c4 10 9e eb 14 b8 01 02 bb 00 7c 8a 56 00 8a 76 01 8a 4e 02 8a 6e 03 cd 13 66 61 73 1c fe .....|V..v..N...n...fas...
A0 4e 11 75 0c 80 7e 00 80 0f 84 8a 00 b2 80 eb 84 55 32 e4 8a 56 00 cd 13 5d eb 9e 81 3e fe 7d 55 N.u.~.....U2..V...].>.)U
C0 aa 75 6e ff 76 00 e8 8d 00 75 17 fa b0 d1 e6 64 e8 83 00 b0 df e6 60 e8 7c 00 b0 ff e6 64 e8 75 .un.v...u.....d.....|.....d.u
E0 00 fb b8 00 bb cd 1a 66 23 c0 75 3b 66 81 fb 54 43 50 41 75 32 81 f9 02 01 72 2c 66 68 07 bb 00 .....f#;u;f..TCPau2...r.fh...
100 00 66 68 00 02 00 00 66 68 08 00 00 66 53 66 53 66 55 66 68 00 00 00 00 66 68 00 7c 00 00 66 .fh...fh...fSfSfUfh...fh.|..f
120 61 68 00 00 07 cd 1a 5a 32 f6 ea 00 7c 00 00 cd 18 a0 b7 07 eb 08 a0 b6 07 eb 03 a0 b5 07 32 e4 ah....Z2...|.....+.d.$...
140 05 00 07 8b f0 ac 3c 00 74 09 bb 07 00 b4 0e cd 10 eb f2 f4 eb fd 2b c9 e4 64 eb 00 24 02 e0 f8 $.<t.....+..d.$...
160 24 02 c3 49 6e 76 61 6c 69 64 20 70 61 72 74 69 74 69 6f 6e 20 74 61 62 6c 65 00 45 72 72 6f 72 $.Invalid partition table.Error
180 20 6c 6f 61 64 69 6e 67 20 6f 70 65 72 61 74 69 6e 67 20 73 79 73 74 65 6d 00 4d 69 73 73 69 6e loading operating system.Missin
1A0 67 20 6f 70 65 72 61 74 69 6e 67 20 73 79 73 74 65 6d 00 00 00 63 7b 9a c8 b3 d8 f8 00 00 80 20 g operating system....c{.....
1C0 21 00 07 ef 26 49 00 00 00 00 00 18 12 00 00 ef 27 49 07 fe ff ff 00 20 12 00 00 c0 30 25 00 00 !..&I.....'I.....0%..
1E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....|.....|.....U..

0/ 200] [mbr-corr.bin]
0 fa b8 00 00 8e c0 8e d8 8e d0 bc 00 7c fb b8 03 00 cd 10 b8 01 13 bd 26 7c ba 00 00 b9 84 01 bb .....|.....|.....&|.....
20 0e 00 cd 10 eb fe 7e 53 65 6e 74 69 6e 65 6c 4f 6e 65 20 4c 61 62 73 20 52 61 6e 73 6f 6d 77 61 .....-SentinelOne Labs Ransomwa
40 72 65 7e 0d 0a 59 6f 75 72 20 73 79 73 74 65 6d 20 77 61 73 20 75 6e 70 72 6f 74 65 63 74 65 64 re...Your system was unprotected
60 2c 20 73 6f 20 77 65 20 6c 6f 63 6b 65 64 20 64 6f 77 6e 20 61 63 63 65 73 73 20 74 6f 20 57 69 , so we locked down access to Wi
80 6e 64 6f 77 73 2e 0d 0a 59 6f 75 20 6e 65 65 64 20 74 6f 20 62 75 79 20 53 65 6e 74 69 6e 65 6c ndows...You need to buy Sentinel
A0 4f 6e 65 20 61 6e 74 69 76 69 72 75 73 20 69 6e 20 6f 72 64 65 72 20 74 6f 20 72 65 73 74 6f 72 One antivirus in order to restor
C0 65 20 79 6f 75 72 20 63 6f 6d 70 75 74 65 72 2e 0d 0a 4d 79 20 6e 61 6d 65 20 69 73 20 56 69 74 e your computer...My name is Vit
E0 61 6c 69 20 4b 72 65 6d 65 7a 2e 20 43 6f 6e 74 61 63 74 73 20 61 72 65 20 62 65 6c 6f 77 2e 0d ali Kremez. Contacts are below..
100 0a 50 68 6f 6e 65 3a 20 2b 31 20 32 30 33 2d 36 39 30 2d 36 35 34 33 0d 0a 45 2d 4d 61 69 6c 20 .Phone: +1 203-690-6543..E-Mail
120 31 3a 20 76 69 74 61 6c 69 6b 40 73 65 6e 74 69 6e 65 6c 6f 6e 65 2e 63 6f 6d 0d 0a 45 2d 4d 61 1: vitalik@sentinelone.com..E-Ma
140 69 6c 20 32 3a 20 76 6b 72 65 6d 65 7a 40 68 6f 74 6d 61 69 6c 2e 63 6f 6d 0d 0a 0d 0a 41 66 74 il 2: vkremez@hotmail.com...Aft
160 65 72 20 79 6f 75 20 62 75 79 20 6d 69 20 61 6e 74 69 76 69 72 75 73 20 49 20 77 69 6c 6c 20 73 er you buy my antivirus I will s
180 65 6e 64 20 79 6f 75 20 75 6e 6c 6f 63 6b 20 63 6f 64 65 2e 0d 0a 45 6e 74 65 72 20 55 6e 6c 6f end you unlock code...Enter Unlo
1A0 63 6b 20 63 6f 64 65 3a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ck code:.....|.....|.....U..
1C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....|.....|.....U..
1E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....|.....|.....U..
```

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 payload 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.

```
[0x004020a8]> px 0x00000c00
Do you want to print 193 lines? (y/N) y
- offset - 0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0x004020a8 a100 4040 008b 0d04 4040 0031 c8e8 9eff ..@@ ...@@ 1...
0x004020b8 ffff 68ac 0000 0068 1050 4000 ffd6 83c4 ..h...h.P@ ....
0x004020c8 0868 fff0 0000 68ac 0000 0068 1050 4000 .h...h...h.P@
0x004020d8 e825 ffff ffe8 2e2f 0000 68ff 0000 0068 .%..../ h...h
0x004020e8 ac00 0000 6810 5040 00e8 0cff ffff 68ac ...h.P@ ....h.
0x004020f8 0000 0068 1050 4000 ffd7 83c4 08c7 050c ...h.P@ .....
0x00402108 1040 00ba 5140 00c7 0510 1040 0000 0200 .@ .Q@ ...@ ...
0x00402118 0068 fe00 0000 68bc 5040 00ff d683 c408 .h...h.P@ ....
0x00402128 68ff 0000 0068 fe00 0000 68bc 5040 00e8 .h...h...h.P@ .
0x00402138 c6fe ffff e87b 2f00 0068 fff0 0000 68fe .....{/ h...h.
0x00402148 0000 0068 bc50 4000 e8ad feff ff68 fe00 ...h.P@ ....h.
0x00402158 0000 68bc 5040 00ff d783 c408 6a00 ff25 ..h.P@ .....j .%
0x00402168 9430 4000 0000 0000 0000 0000 0000 0000 .0@
0x00402178 0000 0000 0000 0000 0000 0000 0000 0000
```

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.

```
[0x004020a8]> s fcn.00402002
[0x00402002]> pdf
; XREFS: CALL 0x00402064 CALL 0x004020a2 CALL 0x004020d8 CALL 0x004020f1 CALL 0x00402137 CALL 0x00402150
27: fcn.00402002 (int32_t arg_8h, int32_t arg_ch, int32_t arg_10h);
; arg int32_t arg_8h @ ebp+0x8
; arg int32_t arg_ch @ ebp+0xc
; arg int32_t arg_10h @ ebp+0x10
0x00402002 55          push ebp
0x00402003 89e5        ebp = esp
0x00402005 60          pushal
0x00402006 8b7508      esi = dword [arg_8h]
0x00402009 89f7        edi = esi
0x0040200b 8b4d10      ecx = dword [arg_10h]
0x0040200e 8b550c      edx = dword [arg_ch]
0x00402011 ac          lodsb al,byte [esi]
0x00402012 30c8        al ^= cl
0x00402014 aa          stosb byte es:[edi],al
0x00402015 4a          edx--
0x00402016 75f9        if (var) goto 0x402011
0x00402018 61          popal
0x00402019 c9          leave
0x0040201a c20c00      return
```

```
[0x00402002]> s fcn.00402058
[0x00402058]> pdf
; CALL XREF from entry0 @ 0x4020b5
80: fcn.00402058 ();
0x00402058 68ff0000    push 0xff          ; 255
0x0040205d 6a10        push 0x10         ; 16
0x0040205f 68050400    push section..upx ; 0x405000
0x00402064 e899ffffff  fcn.00402002 ()
0x00402069 50          push eax
0x0040206a 8b3500104000 esi = dword [section..data] ; [0x401000:4]=0x40201d
0x00402070 8b3d04104000 edi = dword [0x401004] ; [0x401004:4]=0x40203a
0x00402076 6a10        push 0x10         ; 16
0x00402078 68050400    push section..upx ; 0x405000
0x0040207d ffd6        esi ()
0x0040207f 83c408      esp += 8
0x00402082 58          pop eax
0x00402083 e8782f0000  section..upx ()
0x00402088 751e        if (var) goto entry0
0x0040208a 6a10        push 0x10         ; 16
0x0040208c 68050400    push section..upx ; 0x405000
0x00402091 ffd7        edi ()
0x00402093 83c408      esp += 8
0x00402096 68ff0000    push 0xff          ; 255
0x0040209b 6a10        push 0x10         ; 16
0x0040209d 68050400    push section..upx ; 0x405000
0x004020a2 e85bffffff  fcn.00402002 ()
0x004020a7 c3          return
```

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`. Success 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: [redacted]
SSDEEP: [redacted]

windefender.exe --> SHA256: 28e8776a07789daf08629815da0a6eb69613410912447c189a51002f54d956ca
SSDEEP: 49152:mFeWvXwa1xkJrWbSkK0CCD/ozKc3k8HxmYfJpz4U+TiAGTeI6h6gHquAb7/i:CvXwa

Winmon.exe --> SHA256: 889fb266c4c01bb4ef67635249c8daeb641fc86ce62fc280b34beec415fb6129
SSDEEP: 96:/XAUM8mqN18vwlVfjm3ZAeyRY0iRIfad/WrJ37CgES:7pNuv2LSZA1fEWrR7vES

WinmonFS.exe --> SHA256: eb0be2ac3833c843214a55b14c31125a7b600d5272bdf322c4871f42627576e4
SSDEEP: 384:WVYr1nH9XRl8iueNYUaNhucQ3t6PsPJPswHEvDdvHqciss+E96Vg:vrRlFpaNhuq03njov

WinmonProcessMonitor.exe --> SHA256: f609c6656a0c451dafa5173df0cd848f7cb7f22c4f150f8d16716c12593de66
SSDEEP: 384:s+B62cfu4RaQNDEiULv/oGUOY1wR7OLwOMEp5PkdkQE:s0mu4RLNAiUL/oG

MBR Locker V1:

=====

```
sentinelone.scr --> SHA256: 4cd23a989a8f196b1f49e5e66c6ecfa0cebf63f04950ae4d64127aaedda9e89c  
SSDEEP: 48:Zvt+BLdtWU2ew9FRCfH8BArSXXmzdh4vMASG2HvzqEsG8V:Z1+9dtWU2ew9rC/8Kiidh4
```

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 order 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:
```

Source: <https://dissectingmalwa.re/the-blame-game-about-false-flags-and-overwritten-mbrs.html>