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 <u>MBRFilter</u> 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 <u>BleepingComputer</u> 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 <u>Maze Team</u>.

[*] Beware: Some scams utilize my name and impersonate myself to amplify extortions. <u>pic.twitter.com/wk9Mxkqxpz</u>

— 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.



HOME SOFTWARES CONTACT US

Home 🖩 Softwares 📓 Adobe Illustrator CS6 Full Crack With Serial Keygen (Latest 2019) Free

	Type and hit enter Q
LATEST 2019] FREE	
written by Crackedion January 21, 2020	RECENT POSTS
Adobe Illustrator CS6 Cracked + Serial Number Portable [Mac+Windows]	r
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.	Cobra Driver Pack Solution Fresh 2020 ISO Latest Torrent Download
	April 12, 2020
	Microsoft Toolkit 2.6.7 Official™ Activator April 12, 2020
Ai 🔝 Adober Illustrator' CS6	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).



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.

F0 02



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 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 Issuer WDKTestCert Admin,131480495282941941 Issuer WDKTestCert Admin,131480495282941941 Valid From 2017-08-24 11:58:49 Valid To 2027 08 24 00:00:00	Signature Info 🕕							
 ▲ 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 Ta 2027 08 24 00:00:00 	Signature Verification							
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	▲ A certificate chain p	rocessed, but terminated in a root certificate which is not trusted by the trust provider.						
Date signed 9:39 PM 4/13/2020 X509 Signers	File Version Information							
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	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	V500 01							
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	X509 Signers							
Name WDKTestCert Admin,131480495282941941 Issuer WDKTestCert Admin,131480495282941941 Valid From 2017-08-24 11:58:49 Valid To 2027_08_24_00:00:00	 WDKTestCert Adm 	in,131480495282941941						
Issuer WDKTestCert Admin,131480495282941941 Valid From 2017-08-24 11:58:49 Valid To 2027_08_24_00:00:00	Name	WDKTestCert Admin,131480495282941941						
Valid From 2017-08-24 11:58:49	Issuer	WDKTestCert Admin,131480495282941941						
Valid Ta 2027 08 24 00:00:00	Valid From	2017-08-24 11:58:49						
Valid 10 2027-00-24 00.00	Valid To	2027-08-24 00:00:00						
Algorithm sha1RSA	Algorithm	sha1RSA						
Thumbprint B9C5C2EA53B67DFFD9F39E9BC76AF8F69F33CB55	Thumbprint	B9C5C2EA53B67DFFD9F39E9BC76AF8F69F33CB55						
Serial Number 6F 9A 31 7C FC FC 08 8B 4F 6E 19 8A 73 A1 19 CE	Serial Number	6F 9A 31 7C FC FC 08 8B 4F 6E 19 8A 73 A1 19 CE						
	I							

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.

θ	/ 200]		[mbr-good.bin]-
Θ	33 c0 8e d0 bc 00 7c 8e	e 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.FF
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	.AU]rU.utF.f`.~t
60	26 66 68 00 00 00 00 66	6 ff 76 08 68 00 00 68 00 7c 68 01 00 68 10 00 b4 42 8a 56 00 8b f4 cd 13	&fhf.v.hh. hhB.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	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~
C0	aa 75 6e ff 76 00 e8 8d	l 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.vud`. d.u
EΘ	00 fb b8 00 bb cd 1a 66	5 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;fTCPAu2r,fh
100	00 66 68 00 02 00 00 66	6 68 08 00 00 66 53 66 53 66 55 66 68 00 00 00 00 66 68 00 7c 00 00 66	.fhfhfSfSfUfhfh. f
120	61 68 00 00 07 cd 1a 5a	1 32 f6 ea 00 7c 00 00 cd 18 a0 b7 07 eb 08 a0 b6 07 eb 03 a0 b5 07 32 e4	ah22
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 systemc{
1C0	21 00 07 ef 26 49 00 08	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
1E0	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]-
Θ	fa b8 00 00 8e c0 8e d8	3 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	3 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	5 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	9 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	a 59 6f 75 20 6e 65 65 64 20 74 6f 20 62 75 79 20 53 65 6e 74 69 6e 65 6c	ndowsYou need to buy Sentinel
A0	4f 6e 65 20 61 6e 74 69	9 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
CO	65 20 79 6f 75 72 20 63	3 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 computerMy name is Vit
EΘ	61 6c 69 20 4b 72 65 6d	i 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: +1 203-690-6543E-Mail
120	31 3a 20 76 69 74 61 6c	c 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.comE-Ma
140	69 6c 20 32 3a 20 76 6b	o 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.comAft
160	65 72 20 79 6f 75 20 62	2 75 79 20 6d 79 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	9 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 codeEnter Unlo
1A0	63 6b 20 63 6f 64 65 3a	a 00 00 00 00 00 00 00 00 00 00 00 00 00	ck code:
100	00 00 00 00 00 00 00 00	0 00 00 00 00 00 00 00 00 00 00 00 00 0	
1E0	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 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 DeviceloControl), 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	<pre>sym.SHELL32.DLL_imp.SHGetSpecialFolderPathW 0 0x0040316c'</pre>
"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 1 2 3 4	0x00000400 0x00000600 0x00000800 0x00000800 0x00000800 0x00000000	0x200 0x200 0x200 0x200 0x200 0x400	0x00401000 0x00402000 0x00403000 0x00404000 0x00405000	0×1000 0×1000 0×1000 0×1000 0×1000	- rw- - r - x - rw- - r - rw-	.data .code .idat .rsrc .upx	а
nth	paddr	si	ze vaddr	۷	/size	perm	name
0 1 2	0x00000200 0x00000200 0x001e4e00	0 0x1e4c 0x2	x0 0x004010 00 0x006b00 00 0x008950	00 0x2a 00 0x1e 00 0x	af000 25000 (1000	- rwx - rwx - rw-	UPX0 UPX1 UPX2

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

[0x004020a8]	> px	0×00	000c00)					
Do you want	to p	rint	193 li	ines?	(y/N)	У			
- offset -	01	23	45	67	89	ΑB	СD	ΕF	0123456789ABCDEF
0x004020a8		4040	008b	0d04	4040	0031			. @@ @@ . 1
0x004020b8		68ac		668	1050	4000	ffd6		h. h.P@
0x004020c8	0868			68ac		668	1050	4000	.h. h. h.P@
0x004020d8	e825			2e2f		68ff		0068	.%/.hh
0x004020e8			6810	5040				68ac	h.P@h.
0x004020f8		0068	1050	4000					h.P@
0x00402108	1040		5140		0510	1040		0200	.@Q@@
0x00402118	0068			68bc	5040		d683	c408	h. h.P@
0x00402128	68ff		0068			68bc	5040		h. h. h.P@ .
0x00402138			e87b	2f00	0068			68fe	{/hh.
0x00402148		0068	bc50	4000	e8ad		ff68		h.P@h.
0x00402158		68bc	5040		d783	c408	6a00	ff25	h.P@j.%
0x00402168	9430	4000							.00
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								
			CALL 0x004020d8 CALL 0x004020f1 (
_ 27: fcn.00402002 (int32_t a	arg_8h, int32_	t arg_ch, int:	32_t arg_10h);					
; arg int32_t arg	g_8h @ ebp+0x8							
; arg int32_t arg	g_ch @ ebp+0xc							
; arg 1nt32_t arg	g_ton @ epp+ox. ==	LU puch ohn						
0x00402002	2005	obp – osp						
0x00402005	60	nushal						
0x00402006	8b7508	esi = dword	[arg 8h]					
0×00402009		edi = esi						
0x0040200b	8b 4d 10		[arg_10h]					
0x0040200e			[arg_ch]					
-> 0x00402011		lodsb al,byt	e [esi]					
0×00402012	30c8	al ^= cl						
0x00402014		stosb byte e	s:[edi],al					
0X00402015	4a 75 fo	edx	- 0×402011					
-< 0x00402016	7019 61	II (Var) gou	0 0x402011					
0x00402010	c9	leave						
0x0040201a		return						
$[0 \times 0.0402002]$ s for 00	402058							
[0x00402002]> s ref.00	402030							
	E from ontr	0 0 0 00 400						
; CALL ARE		yo @ 0x4020						
80: TCN.00402058 ();								
0x00402058	68ff0		push 0xff		255			
0x0040205d	6a10		push 0x10		16			
0x0040205f	68005	04000			0x405000			
0x00402064	e899f		fcn.00402002 ()					
0x00402069	50		push eax					
0x00402063	8h350	104000	esi – dword [section_data]		[0x401000:4]-0x40201d			
0×00402000	obedo	4104000	di = dword [ecclion.idata]		[0x401004:4]_0x402030			
0x00402070	6.10	4104000 6			[00401004.4]=00402058			
0X00402076	6a10		push exie		16			
0x00402078	68005	0400			0x405000			
0x0040207d			esi ()					
0x0040207f			esp += 8					
0x00402082	58		pop eax					
0x00402083	e8782		sectionupx ()					
-< 0x00402088	7510		if (var) goto entryA					
0x00402000	6510		ouch av10		16			
0x00402088	0a10				10			
0X0040208C	68005	04000	pusn sectionupx		0X405000			
0x00402091	. t†d7		edi ()					
0x00402093			esp += 8					
0x00402096	68ff		push 0xff					
0x0040209b	6a10		push 0x10		16			
0x0040209d	68005	04000	push sectionupx		0x405000			
0x00402022	e85hf		fcn.00402002 ()					
0x004020a2			roturn					
0x004020a7	63		recurn					

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 <u>here</u>). I verified on a physical GPT install that LBA 1 and following is not affected by the MBRLocker and should keep the GPT recoverable. <u>TestDisk</u> is theoretically capable of recovering both partitioning layouts. I'd advise victims to use File Recovery software like <u>Photorec</u> 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/qPqaMy25WJTZsRv06Y:8HBymGDY/04ikv0
windefender.exe --> SHA256:
28e8776a07789daf08629815da0a6eb69613410912447c189a51002f54d956ca
                    SSDEEP:
49152:mFeWvXwa1xkJrwBskK0CCD/ozKc3k8HxmYfJpz4U+TiAGTeI6h6qHquAb7/i:CvXwaerwBIbKcrxmYfJ
Winmon.exe --> SHA256:
889fb266c4c01bb4ef67635249c8daeb641fc86ce62fc280b34beec415fb6129
               SSDEEP:
96:/XAUM8mqN18vwLvVfjm3ZAeyRY0iRIfad/WrJ37CqES:7pNuv2LSZA1fEWrR7vES
WinmonFS.exe --> SHA256:
eb0be2ac3833c843214a55b14c31125a7b600d5272bdf322c4871f42627576e4
                 SSDFFP:
384:WVYr1nH9XRl8iueNYUaNhuq03t6PsPJVPswHEvDdvHqciss+E96Vg:vrRlFpaNhuq03njovpPTtTK
WinmonProcessMonitor.exe --> SHA256:
f609c6656a0c451dafa5173df0cd848f7cb7f22c4f150f8d16716c12593de66c
                             SSDEEP:
384:s+B62cfu4RaQNDEiULv/oGU0Y1wR70Lw0MEP5PkdkQE:s0mu4RLNAiUL/oGGS70LDP5PkdkQE
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: