Paper

Bitdefender

Everything we know about GoldenEye

An attack against Ukraine's critical infrastructure disguised as ransomware

On January 27th, reports of a rapidly spreading ransomware attack started to emerge from Ukraine. The speed at which critical infrastructure networks were shutting down pointed to a ransomware application with a wormable component, whose virality called to mind the WannaCry ransomware. In less than three hours, the infection crippled banks, ATMs, public transport and an airport, as well as utilities provider Kyivenergo. Then it spread outside the Ukraine.

As multiple critical infrastructure networks reported major blackouts, Bitdefender started an internal investigation over the isolated malware samples to trace the attack's origin and better understand what it targeted, and how. The following report is based on our internal telemetry and reflects what we know as of the moment of writing.

Initial context and delivery

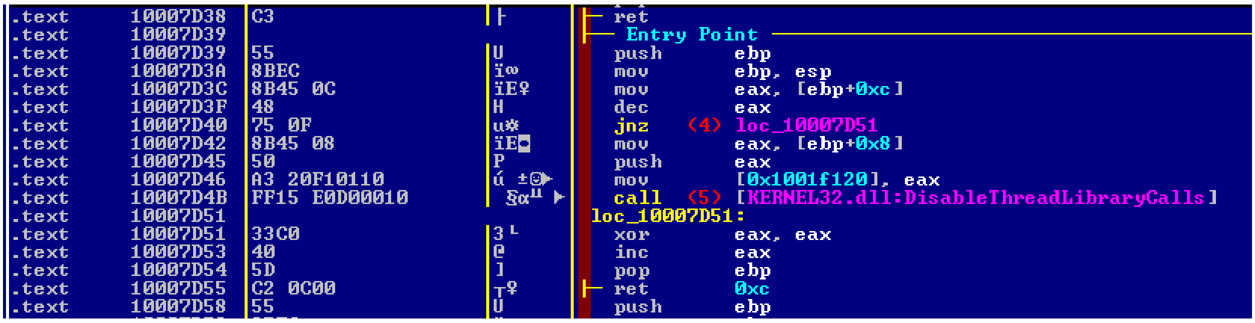
Our initial assessment reveals the threat is similar to a variant of the GoldenEye ransomware, a strain that naturally evolved from the first commercial bootloader encryptor, Petya. This threat comes in the form of a DLL executed via the rundll32.exe process as part of a largely complex scheme involving a supply chain compromise.

A look inside our telemetry revealed multiple Bitdefender products sending over threat intelligence about blocked instances of GoldenEye during the first wave of attacks. In all such circumstances, the process execution flow shows **explorer.exe** spawning **ezvit.exe** – the main executable of a Ukrainian accounting and invoicing software utility called MeDoc - which in turn executes **rundll32.exe** with the ransomware's DLL as parameter.

Bitdefender research supports the theory that a bad update of the MeDoc accounting app also supplied the malicious DLL payload and was used to trigger the initial infections inside company networks. The infection then spread from the machines running the accounting software to the other computers in the network via a number of lateral movement techniques.

A technical dive into the sample

The isolated sample identified with a SHA1 of **34f917aaba5684fbe56d3c57d48ef2a1aa7cf06d** is a DLL file with an EntryPoint that doesn't reveal any malicious actions. This DLL has no exports by name, only an ordinal which seems to be the actual EntryPoint:



```
.text     10007D38  C3               ├    ├ ret
.text     10007D39                        ├ Entry Point ──────────
.text     10007D39  55               U      push      ebp
.text     10007D3A  8BEC             ï∞     mov       ebp, esp
.text     10007D3C  8B45 0C          ïE♀    mov       eax, [ebp+0xc]
.text     10007D3F  48               H      dec       eax
.text     10007D40  75 0F            u☼     jnz  (4)  loc_10007D51
.text     10007D42  8B45 08          ïE◘    mov       eax, [ebp+0x8]
.text     10007D45  50               P      push      eax
.text     10007D46  A3 20F10110      ú ±☺►  mov       [0x1001f120], eax
.text     10007D4B  FF15 E0D00010     §α╨ ► call (5)  [KERNEL32.dll:DisableThreadLibraryCalls]
.text     10007D51                        loc_10007D51:
.text     10007D51  33C0             3└     xor       eax, eax
.text     10007D53  40               @      inc       eax
.text     10007D54  5D               ]      pop       ebp
.text     10007D55  C2 0C00          ┬♀   ├ ret       0xc
.text     10007D58  55               U      push      ebp
```

Figure 1: Asssembler view of the DLL's entry point section

When executed, the malware starts checking the privilege level the current logged in user has on the computer, particularly seeking the SeDebugPrivilege permission, which is required to debug and adjust the memory of a process owned by another account.

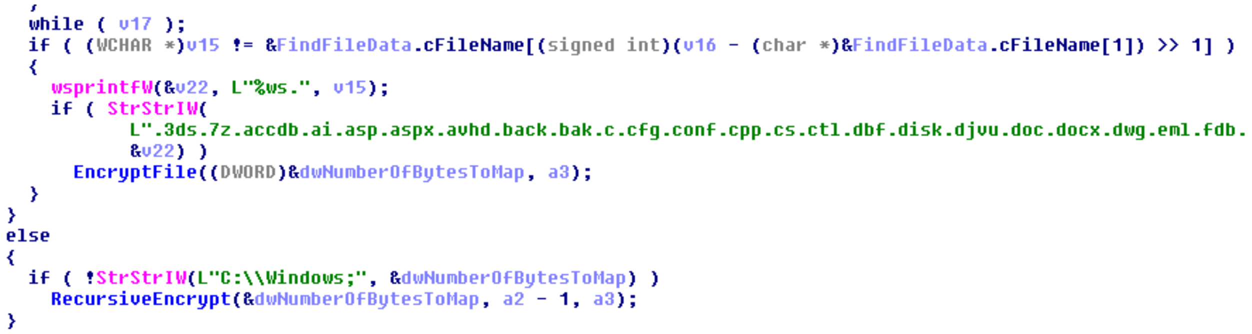
Depending on whether the malware has SeDebugPrivilege access, it performs file encryption or something that looks to be irreversible disk damage. The encryption process is also fingerprinting running processes on the machine by comparing hashes. A routine inside the code looks for several processes associated with antimalware products, as shown in the Layer 2 encryption chapter below..

Layer 1 encryption – holding files at ransom

The first layer of encryption targets specific file formats on storage devices connected to the victim computer. The malware looks for the following file formats to be encrypted. The file extensions colored in red show disk image files or virtual env files:

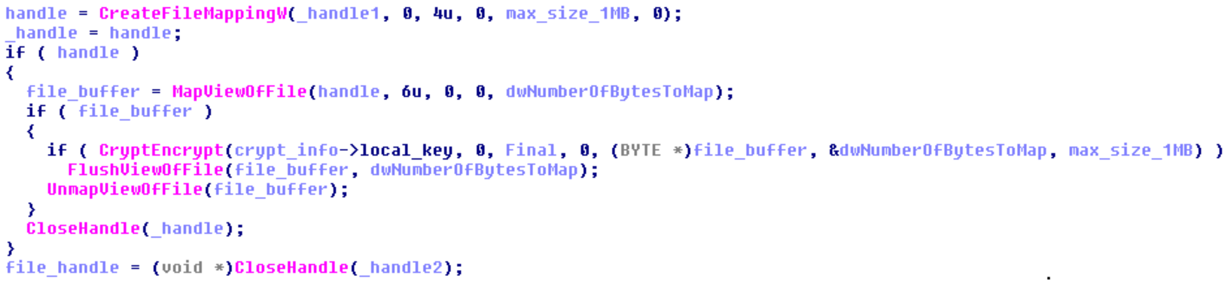
.3ds
.7z
.accdb
.ai
.asp
.aspx
.avhd
.back
.bak
.c
.cfg
.conf
.cpp
.cs
.ctl
.dbf
.disk
.djvu
.doc
.docx
.dwg
.eml
.fdb
.gz
.h
.hdd
.kdbx
.mail
.mdb
.msg
.nrg
.ora
.ost
.ova
.ovf
.pdf
.php
.pmf
.ppt
.pptx
.pst
.pvi
.py
.pyc
.rar
.rtf
.sln
.sql
.tar
.vbox
.vbs
.vcb
.vdi
.vfd
.vmc
.vmdk
.vmsd
.vmx
.vsdx
.vsv
.work
.xls
.xlsx
.xvd
.zip

The encryption routine uses an embedded RSA public key formatted as a base64 string. It is used to encrypt particular AES128 keys randomly generated for file encryption. At the end of each file, the malware appends the AES128 key encrypted with the RSA key.



```
  ;
  while ( v17 );
  if ( (WCHAR *)v15 != &FindFileData.cFileName[(signed int)(v16 - (char *)&FindFileData.cFileName[1]) >> 1] )
  {
    wsprintfW(&v22, L"%ws.", v15);
    if ( StrStrIW(
           L".3ds.7z.accdb.ai.asp.aspx.avhd.back.bak.c.cfg.conf.cpp.cs.ctl.dbf.disk.djvu.doc.docx.dwg.eml.fdb.
           &v22) )
      EncryptFile((DWORD)&dwNumberOfBytesToMap, a3);
  }
}
else
{
  if ( !StrStrIW(L"C:\\Windows;", &dwNumberOfBytesToMap) )
    RecursiveEncrypt(&dwNumberOfBytesToMap, a2 - 1, a3);
}
```

Figure 2: Encryption started from recursive scan

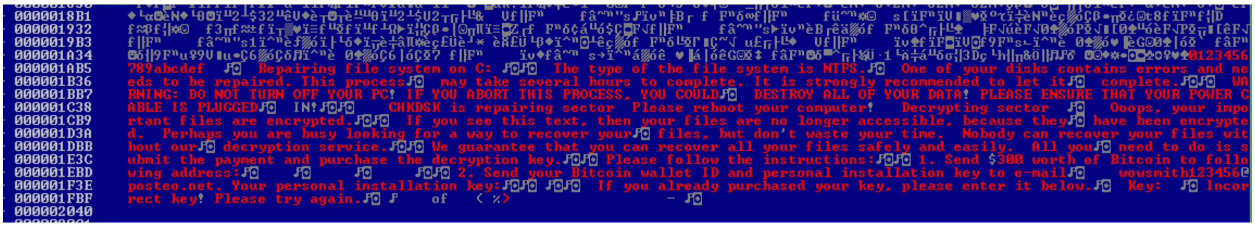


```
handle = CreateFileMappingW(_handle1, 0, 4u, 0, max_size_1MB, 0);
_handle = handle;
if ( handle )
{
  file_buffer = MapViewOfFile(handle, 6u, 0, 0, dwNumberOfBytesToMap);
  if ( file_buffer )
  {
    if ( CryptEncrypt(crypt_info->local_key, 0, Final, 0, (BYTE *)file_buffer, &dwNumberOfBytesToMap, max_size_1MB) )
      FlushViewOfFile(file_buffer, dwNumberOfBytesToMap);
    UnmapViewOfFile(file_buffer);
  }
  CloseHandle(_handle);
}
file_handle = (void *)CloseHandle(_handle2);
```

Figure 3: The file encryption routine

Layer 2 encryption – compromising the MBR and MFT Structures

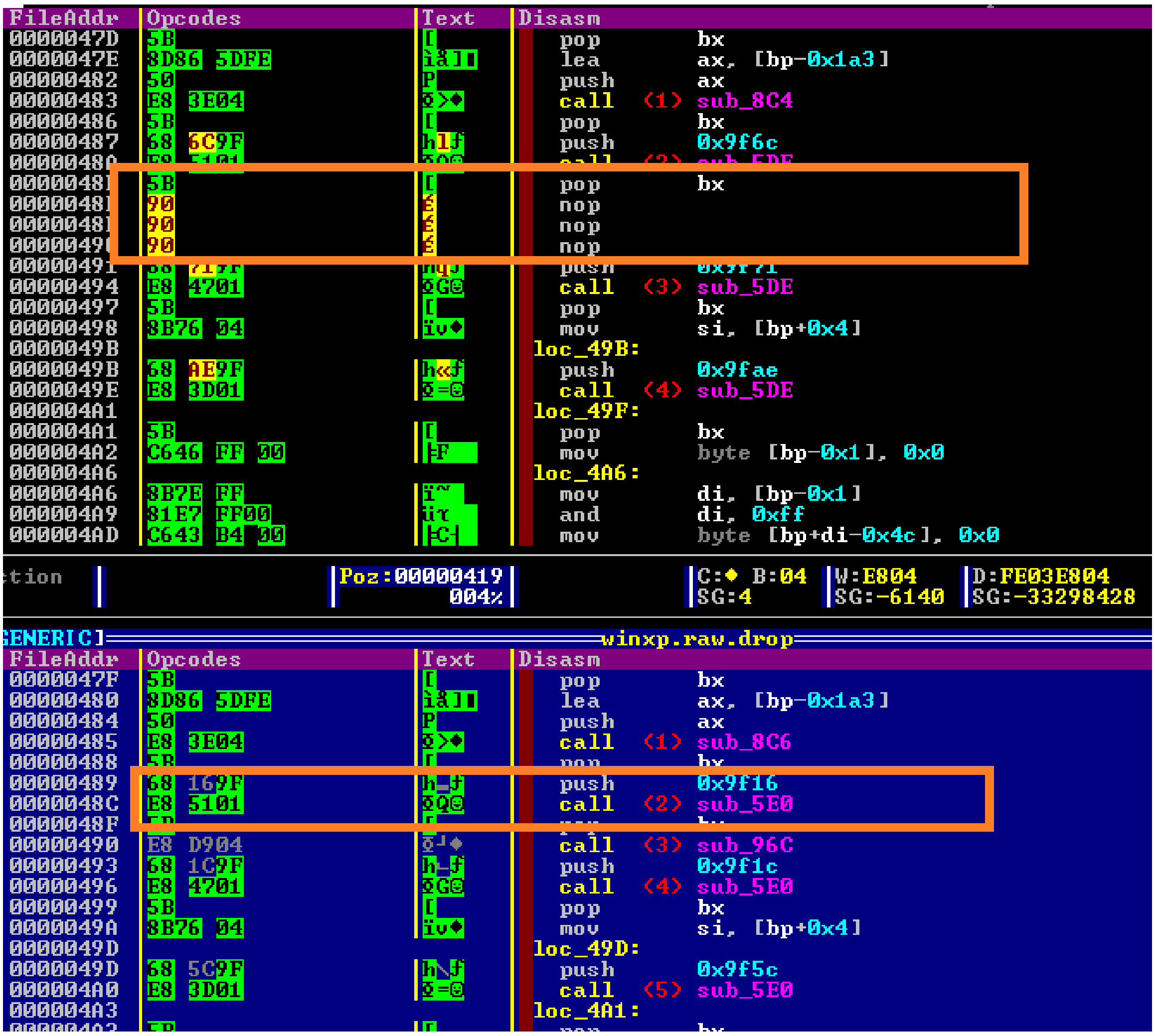
If the malware has SeDebugPrivilege permission, it starts the disk encryption by overwriting the master boot loader with a custom boot manager nearly identical to the one found in older versions of the GoldenEye ransomware.



```
000018B1   ◆└α☻èN◆╙0☻ï╜2┴$32╜êV◆è┬☻┬è╧╜0ï╜2┴$U2┬╓├╙&  Vf||F"    fâ~"'s♪iv"├B┌ f  F"δ∞f||F"     fü~"☼☺  s[ïF"ïV▮▓♥Ω°┐ï╪èN"èç▒óÇβ•╥Ω¿☺t8fïF"f╣|D
00001932   f≈βf╡|☼☺  f3╥f≈±fï┬▓♥ï≡f╙Ωfï╙f┴Ω►ï╟Çβ•|☺╥Πï≡▬Z┌f  F"δ¢á╙ó$Ç▬F√f||F"    fâ~"'s►ïv"èB┌êä▒óf  F"δθ^┌├╙♠  ├F√úèF√0♠▒óPΩ√▮[0♠╙óèF√PΩ╤▮[êF√
000019B3   f||F"    fâ~"'s1ï^"èf▒óï├╙δ♦ï╤è╪âΠ☼èçƒÜè┘* èÅƒÜ╙β♦ï^"◘┴êç▒óf  F"δ╙Γ▮Ç~√ uƒ┌├╙♦  Vf||F"     ïv♠fïF◘ïV◘f9F"s└ï^"è  0♠▒ó♥ ▐èG☺0♠|óΩ  fâF"
00001A34   ☻δ||9F"u♀9V▮u•Ç6▒óÇóΠï^"è  0♠▒óÇ6|óÇΩ7 f||F"     ïv♦fâ~" s→ï^"á▒óê ♥▐á|óêG☺Ω↨ fâF"☻δ▀^┌├¼Ü·1 ╙á╪á╙δσ╡3Dç ╙h╢╓&Ö||ƒƒδ ☻☺♦☼•◘◘☼♀♥♠0123456
00001AB5   789abcdef  ♫◘  Repairing file system on C: ♫◘♫◘  The type of the file system is NTFS.♫◘  One of your disks contains errors and ne
00001B36   eds to be repaired. This process♫◘  may take several hours to complete. It is strongly recommended to let it♫◘  complete.♫◘♫◘  WA
00001BB7   RNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD♫◘  DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER C
00001C38   ABLE IS PLUGGED♫◘  IN!♫◘♫◘    CHKDSK is repairing sector  Please reboot your computer!   Decrypting sector  ♫◘   Ooops, your impo
00001CB9   rtant files are encrypted.♫◘♫◘  If you see this text, then your files are no longer accessible, because they♫◘ have been encrypte
00001D3A   d.  Perhaps you are busy looking for a way to recover your♫◘ files, but don't waste your time.  Nobody can recover your files wit
00001DBB   hout our♫◘ decryption service.♫◘♫◘ We guarantee that you can recover all your files safely and easily.  All you♫◘ need to do is s
00001E3C   ubmit the payment and purchase the decryption key.♫◘♫◘ Please follow the instructions:♫◘♫◘ 1. Send $300 worth of Bitcoin to follo
00001EBD   wing address:♫◘    ♫◘     ♫◘     ♫◘♫◘ 2. Send your Bitcoin wallet ID and personal installation key to e-mail♫◘    wowsmith123456@
00001F3E   posteo.net. Your personal installation key:♫◘♫◘ ♫◘♫◘  If you already purchased your key, please enter it below.♫◘  Key:  ♫◘ Incor
00001FBF   rect key! Please try again.♫◘ ♪    of   ( %)            - ♫◘
00002040
```

Figure 4: 16-bit code running at reboot

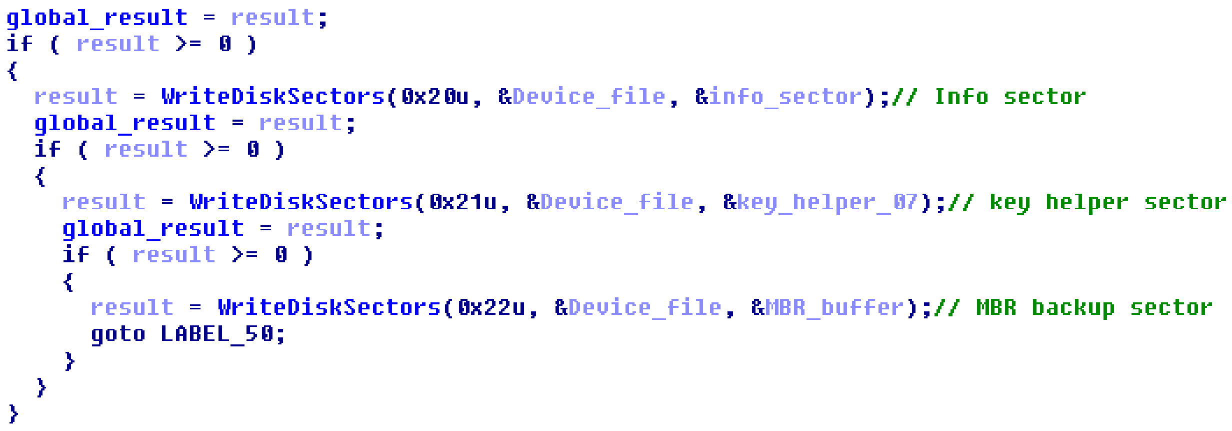
This specific boot manager code looks like a manually patched version of GoldenEye, rather than a new build from modified source code. The image below shows a function call patched with NOPs, while its body is still there. The patching process suppresses an additional call to get_key_pressed, that used to verify the validity of the decryption key as the user typed it in for the original version of Petya.



```
FileAddr |Opcodes          |Text  |Disasm
0000047D |5B               |[     |  pop        bx
0000047E |8D86 5DFE        |ìå]■  |  lea        ax, [bp-0x1a3]
00000482 |50               |P     |  push       ax
00000483 |E8 3E04          |Φ>♦   |  call  (1)  sub_8C4
00000486 |5B               |[     |  pop        bx
00000487 |68 6C9F          |hlƒ   |  push       0x9f6c
0000048A |E8 5101          |ΦQ☺   |  call  (2)  sub_5DE
0000048D |5B               |[     |  pop        bx
0000048E |90               |É     |  nop
0000048F |90               |É     |  nop
00000490 |90               |É     |  nop
00000491 |68 719F          |hqƒ   |  push       0x9f71
00000494 |E8 4701          |ΦG☺   |  call  (3)  sub_5DE
00000497 |5B               |[     |  pop        bx
00000498 |8B76 04          |ïv♦   |  mov        si, [bp+0x4]
0000049B |                 |      |loc_49B:
0000049B |68 AE9F          |h«ƒ   |  push       0x9fae
0000049E |E8 3D01          |Φ=☺   |  call  (4)  sub_5DE
000004A1 |                 |      |loc_49F:
000004A1 |5B               |[     |  pop        bx
000004A2 |C646 FF 00       |╞F    |  mov        byte [bp-0x1], 0x0
000004A6 |                 |      |loc_4A6:
000004A6 |8B7E FF          |ï~    |  mov        di, [bp-0x1]
000004A9 |81E7 FF00        |üτ    |  and        di, 0xff
000004AD |C643 B4 00       |╞C┤   |  mov        byte [bp+di-0x4c], 0x0

tion  |            |Poz:00000419|       |C:♦  B:04 |W:E804   |D:FE03E804
      |            |        004%|       |SG:4      |SG:-6140 |SG:-33298428

GENERIC]══════════════════════════winxp.raw.drop══════════════════════════
FileAddr |Opcodes          |Text  |Disasm
0000047F |5B               |[     |  pop        bx
00000480 |8D86 5DFE        |ìå]■  |  lea        ax, [bp-0x1a3]
00000484 |50               |P     |  push       ax
00000485 |E8 3E04          |Φ>♦   |  call  (1)  sub_8C6
00000488 |5B               |[     |  pop        bx
00000489 |68 169F          |h▬ƒ   |  push       0x9f16
0000048C |E8 5101          |ΦQ☺   |  call  (2)  sub_5E0
0000048F |5B               |[     |  pop        bx
00000490 |E8 D904          |Φ┘♦   |  call  (3)  sub_96C
00000493 |68 1C9F          |h∟ƒ   |  push       0x9f1c
00000496 |E8 4701          |ΦG☺   |  call  (4)  sub_5E0
00000499 |5B               |[     |  pop        bx
0000049A |8B76 04          |ïv♦   |  mov        si, [bp+0x4]
0000049D |                 |      |loc_49D:
0000049D |68 5C9F          |h\ƒ   |  push       0x9f5c
000004A0 |E8 3D01          |Φ=☺   |  call  (5)  sub_5E0
000004A3 |                 |      |loc_4A1:
000004A3 |5B               |[     |  pop        bx
```

Figure 5: Comparison between the current version of GoldenEye (top) and the old version of GoldenEye (bottom)

Before initiating encryption, the malware takes a backup of the Master Boot Record, encrypts it with XOR 7 and writes this backup on sector 34, as follows:



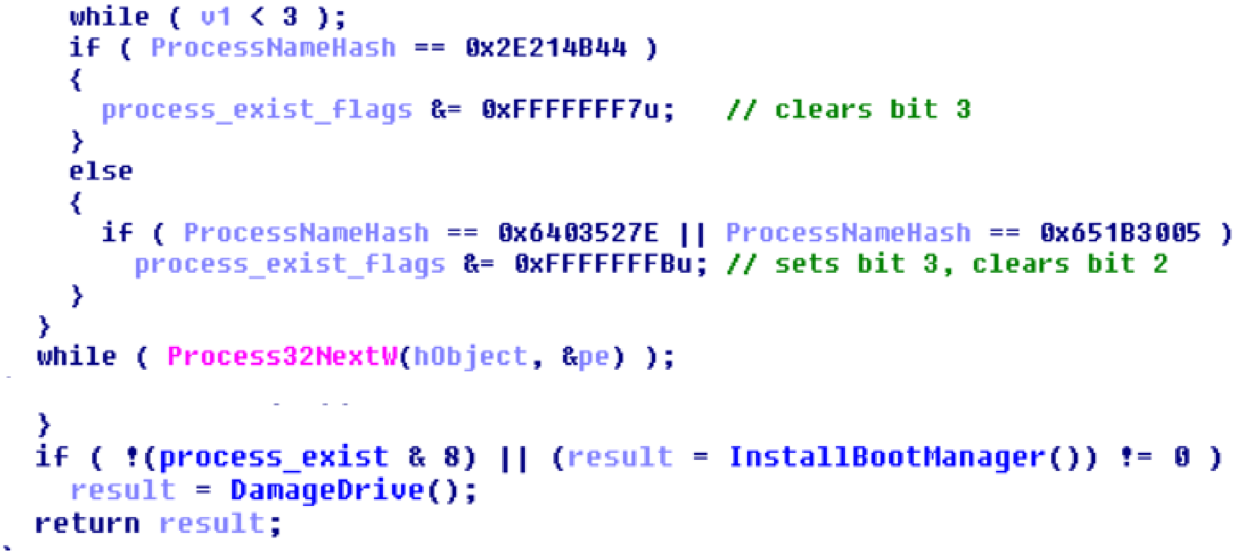
```
global_result = result;
if ( result >= 0 )
{
  result = WriteDiskSectors(0x20u, &Device_file, &info_sector);// Info sector
  global_result = result;
  if ( result >= 0 )
  {
    result = WriteDiskSectors(0x21u, &Device_file, &key_helper_07);// key helper sector
    global_result = result;
    if ( result >= 0 )
    {
      result = WriteDiskSectors(0x22u, &Device_file, &MBR_buffer);// MBR backup sector
      goto LABEL_50;
    }
  }
}
```

Figure 5: Writing sectors 32,33,34

Amid so much speculations as to whether the ransomware can decrypt the MBR if ransom is paid, it is important to say that a decryption routine for the MBR is inside the code.

Kaspersky users get a free pass

However, there is one exception to this rule: if the process list hashing function returns the presence of AVP.exe on the compromised machine, the malware switches to data destruction mode and overwrites the first 10 disk sectors with junk data.



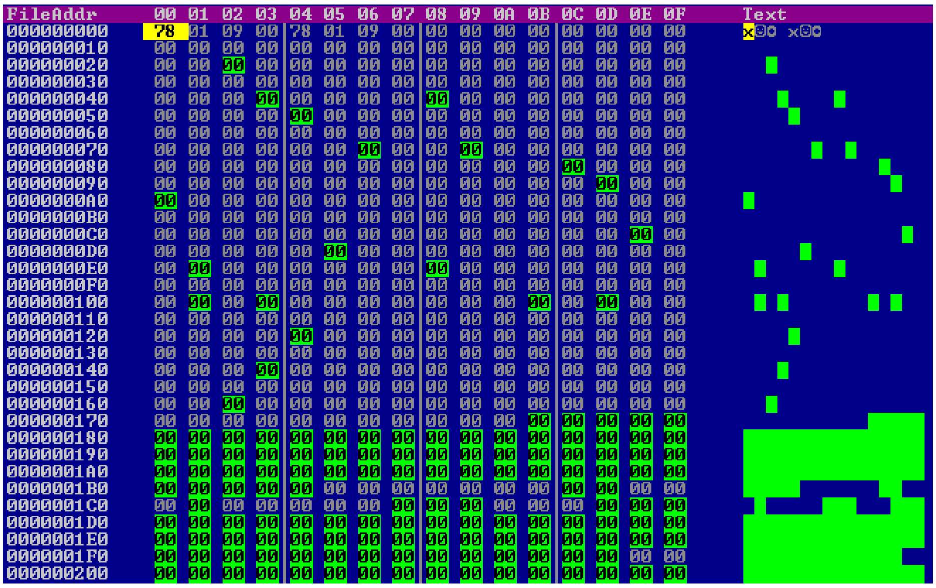
```
    while ( v1 < 3 );
    if ( ProcessNameHash == 0x2E214B44 )
    {
      process_exist_flags &= 0xFFFFFFF7u;   // clears bit 3
    }
    else
    {
      if ( ProcessNameHash == 0x6403527E || ProcessNameHash == 0x651B3005 )
        process_exist_flags &= 0xFFFFFFFBu; // sets bit 3, clears bit 2
    }
  }
  while ( Process32NextW(hObject, &pe) );

  }
  if ( !(process_exist & 8) || (result = InstallBootManager()) != 0 )
    result = DamageDrive();
  return result;
```

Figure 6: process probing and disk trashing routines

This process has been inaccurately reported by the research community as potentially destructive to the data stored on the disk drive. This is wrong, as the first 10 sectors of the disk only hold the Master Boot Record and 9 other empty sectors. if AVP.exe (a process related to Kaspersky security solutions) is identified on the infected machine, the malware simply overwrites the MBR - a reversible operation that can be counteracted by booting from an installation medium, then issuing the FIXMBR command. As this command replaces the

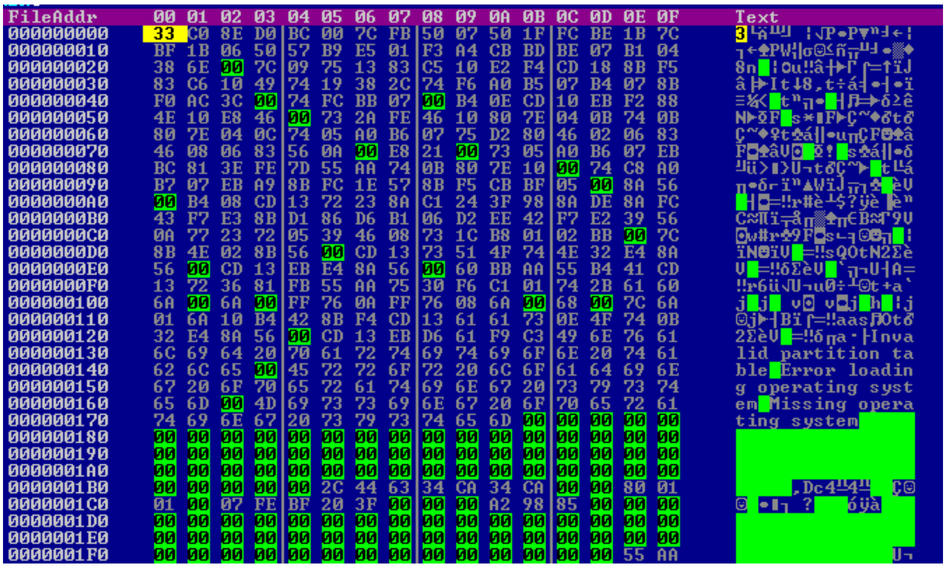
MBR with a valid one but does not fix the partition table (partition is still missing), victims have to use dedicated software to reference the partition in the partition table, then root FIXBOOT to recover the lost sector of the Windows Boot Manager.

MBR DAMAGED:



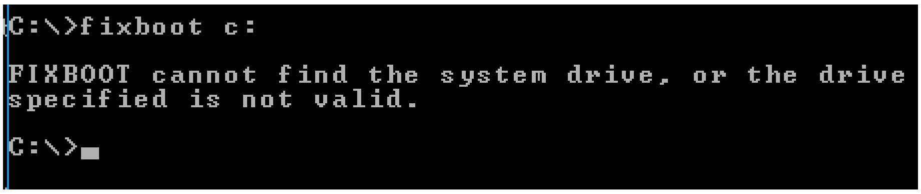
```
FileAddr    00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F    Text
000000000   78 01 09 00|78 01 09 00|00 00 00 00|00 00 00 00    x☺○ x☺○
000000010   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
000000020   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
000000030   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
000000040   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
000000050   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
000000060   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
000000070   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
000000080   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
000000090   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
0000000A0   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
0000000B0   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
0000000C0   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
0000000D0   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
0000000E0   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
0000000F0   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
000000100   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
000000110   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
000000120   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
000000130   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
000000140   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
000000150   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
000000160   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
000000170   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
000000180   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
000000190   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
0000001A0   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
0000001B0   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
0000001C0   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
0000001D0   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
0000001E0   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
0000001F0   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
000000200   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
```

MBR OK (after running FIXMBR)



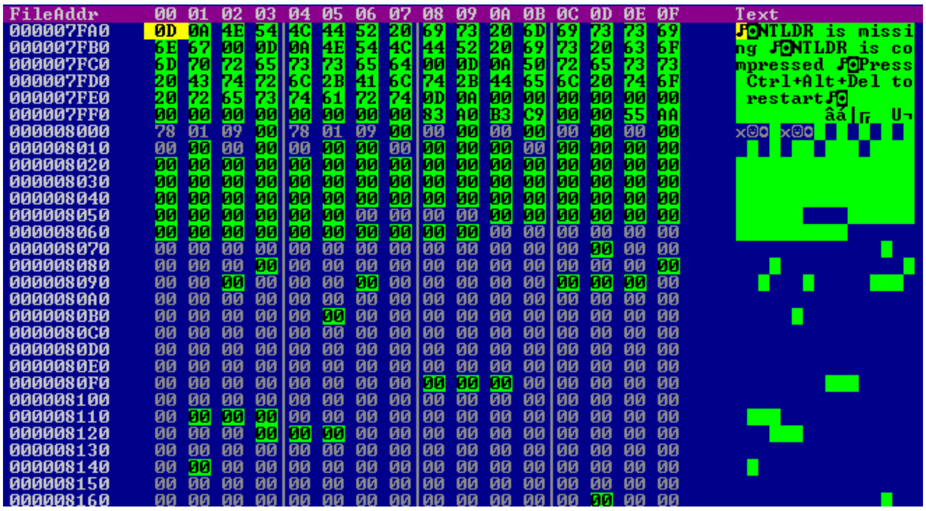
```
FileAddr    00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F    Text
000000000   33 C0 8E D0|BC 00 7C FB|50 07 50 1F|FC BE 1B 7C    3└Ä╨╝ ¦√P•P▼ⁿ╛←¦
000000010   BF 1B 06 50|57 B9 E5 01|F3 A4 CB BD|BE 07 B1 04    ┐←♠PW╣σ☺≤ñ╦╜╛•▒♦
000000020   38 6E 00 7C|09 75 13 83|C5 10 E2 F4|CD 18 8B F5    8n ¦○u‼â┼►Γ⌠═↑ï⌡
000000030   83 C6 10 49|74 19 38 2C|74 F6 A0 B5|07 B4 07 8B    â╞►It↓8,t÷á╡•┤•ï
000000040   F0 AC 3C 00|74 FC BB 07|00 B4 0E CD|10 EB F2 88    ≡¼< tⁿ╗• ┤♫═►δ≥ê
000000050   4E 10 E8 46|00 73 2A FE|46 10 80 7E|04 0B 74 0B    N►ΦF s*■F►Ç~♦♂t♂
000000060   80 7E 04 0C|74 05 A0 B6|07 75 D2 80|46 02 06 83    Ç~♦♀t♣á╢•u╥ÇF☻♠â
000000070   46 08 06 83|56 0A 00 E8|21 00 73 05|A0 B6 07 EB    F◘♠âV◙ Φ! s♣á╢•δ
000000080   BC 81 3E FE|7D 55 AA 74|0B 80 7E 10|00 74 C8 A0    ╝ü>■}U¬t♂Ç~► t╚á
000000090   B7 07 EB A9|8B FC 1E 57|8B F5 CB BF|05 00 8A 56    ╖•δ⌐ïⁿ▲Wï⌡╦┐♣ èV
0000000A0   00 B4 08 CD|13 72 23 8A|C1 24 3F 98|8A DE 8A FC     ┤◘═‼r#è┴$?ÿè▐èⁿ
0000000B0   43 F7 E3 8B|D1 86 D6 B1|06 D2 EE 42|F7 E2 39 56    C≈πï╤å╓▒♠╥εB≈Γ9V
0000000C0   0A 77 23 72|05 39 46 08|73 1C B8 01|02 BB 00 7C    ◙w#r♣9F◘s∟╕☺☻╗ ¦
0000000D0   8B 4E 02 8B|56 00 CD 13|73 51 4F 74|4E 32 E4 8A    ïN☻ïV ═‼sQOtN2Σè
0000000E0   56 00 CD 13|EB E4 8A 56|00 60 BB AA|55 B4 41 CD    V ═‼δΣèV `╗¬U┤A═
0000000F0   13 72 36 81|FB 55 AA 75|30 F6 C1 01|74 2B 61 60    ‼r6ü√U¬u0÷┴☺t+a`
000000100   6A 00 6A 00|FF 76 0A FF|76 08 6A 00|68 00 7C 6A    j j  v◙ v◘j h ¦j
000000110   01 6A 10 B4|42 8B F4 CD|13 61 61 73|0E 4F 74 0B    ☺j►┤Bï⌠═‼aas♫Ot♂
000000120   32 E4 8A 56|00 CD 13 EB|D6 61 F9 C3|49 6E 76 61    2ΣèV ═‼δ╓a∙├Inva
000000130   6C 69 64 20|70 61 72 74|69 74 69 6F|6E 20 74 61    lid partition ta
000000140   62 6C 65 00|45 72 72 6F|72 20 6C 6F|61 64 69 6E    ble Error loadin
000000150   67 20 6F 70|65 72 61 74|69 6E 67 20|73 79 73 74    g operating syst
000000160   65 6D 00 4D|69 73 73 69|6E 67 20 6F|70 65 72 61    em Missing opera
000000170   74 69 6E 67|20 73 79 73|74 65 6D 00|00 00 00 00    ting system
000000180   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
000000190   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
0000001A0   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
0000001B0   00 00 00 00|00 2C 44 63|34 CA 34 CA|00 00 80 01         ,Dc4╩4╩  Ç☺
0000001C0   01 00 07 FE|BF 20 3F 00|00 00 A2 98|85 00 00 00    ☺ •■┐ ?   óÿà
0000001D0   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
0000001E0   00 00 00 00|00 00 00 00|00 00 00 00|00 00 00 00
0000001F0   00 00 00 00|00 00 00 00|00 00 00 00|00 00 55 AA                  U¬
```

Fixboot not working after executing FIXMBR



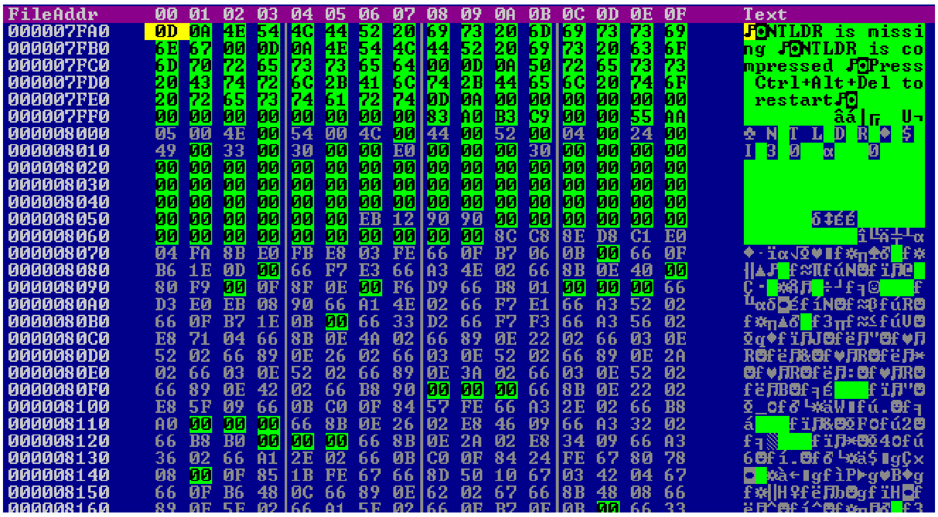
```
C:\>fixboot c:

FIXBOOT cannot find the system drive, or the drive
specified is not valid.

C:\>_
```

BAD sector 2 of the boot manager:



```
FileAddr    00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F    Text
000007FA0   0D 0A 4E 54 4C 44 52 20 69 73 20 6D 69 73 73 69   ♪◙NTLDR is missi
000007FB0   6E 67 00 0D 0A 4E 54 4C 44 52 20 69 73 20 63 6F   ng ♪◙NTLDR is co
000007FC0   6D 70 72 65 73 73 65 64 00 0D 0A 50 72 65 73 73   mpressed ♪◙Press
000007FD0   20 43 74 72 6C 2B 41 6C 74 2B 44 65 6C 20 74 6F    Ctrl+Alt+Del to
000007FE0   20 72 65 73 74 61 72 74 0D 0A 00 00 00 00 00 00    restart♪◙
000007FF0   00 00 00 00 00 00 00 00 83 A0 B3 C9 00 00 55 AA           âá│╔  U¬
000008000   78 01 09 00 78 01 09 00 00 00 00 00 00 00 00 00   x☺○ x☺○
000008010   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000008020   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000008030   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000008040   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000008050   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000008060   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000008070   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000008080   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000008090   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000080A0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000080B0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000080C0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000080D0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000080E0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0000080F0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000008100   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000008110   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000008120   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000008130   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000008140   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000008150   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000008160   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

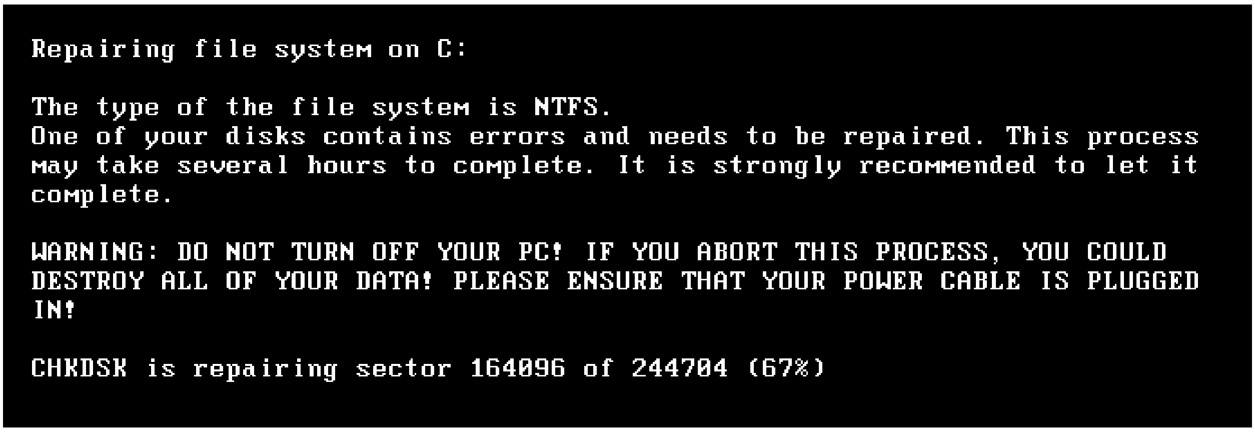
Sector 2 of the boot manager (recovered by fixboot after referencing partition table in MBR):



```
FileAddr    00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F    Text
000007FA0   0D 0A 4E 54 4C 44 52 20 69 73 20 6D 69 73 73 69   ♪◙NTLDR is missi
000007FB0   6E 67 00 0D 0A 4E 54 4C 44 52 20 69 73 20 63 6F   ng ♪◙NTLDR is co
000007FC0   6D 70 72 65 73 73 65 64 00 0D 0A 50 72 65 73 73   mpressed ♪◙Press
000007FD0   20 43 74 72 6C 2B 41 6C 74 2B 44 65 6C 20 74 6F    Ctrl+Alt+Del to
000007FE0   20 72 65 73 74 61 72 74 0D 0A 00 00 00 00 00 00    restart♪◙
000007FF0   00 00 00 00 00 00 00 00 83 A0 B3 C9 00 00 55 AA           âá│╔  U¬
000008000   05 00 4E 00 54 00 4C 00 44 00 52 00 04 00 24 00   ♣ N T L D R ♦ $
000008010   49 00 33 00 30 00 00 E0 00 00 00 30 00 00 00 00   I 3 0  α   0
000008020   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000008030   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000008040   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000008050   00 00 00 00 00 00 EB 12 90 90 00 00 00 00 00 00         δ↕ÉÉ
000008060   00 00 00 00 00 00 00 00 00 00 8C C8 8E D8 C1 E0             î╚Ä╪┴α
000008070   04 FA 8B E0 FB E8 03 FE 66 0F B7 06 0B 00 66 0F   ♦·ïα√Φ♥■f☼╖♠♂ f☼
000008080   B6 1E 0D 00 66 F7 E3 66 A3 4E 02 66 8B 0E 40 00   ╢▲♪ f≈πfúN☻fï♫@
000008090   80 F9 00 0F 8F 0E 00 F6 D9 66 B8 01 00 00 00 66   Ç∙ ☼Å♫ ÷┘f╕☺   f
0000080A0   D3 E0 EB 08 90 66 A1 4E 02 66 F7 E1 66 A3 52 02   ╙αδ◘ÉfíN☻f≈ßfúR☻
0000080B0   66 0F B7 1E 0B 00 66 33 D2 66 F7 F3 66 A3 56 02   f☼╖▲♂ f3╥f≈≤fúV☻
0000080C0   E8 71 04 66 8B 0E 4A 02 66 89 0E 22 02 66 03 0E   Φq♦fï♫J☻fë♫"☻f♥♫
0000080D0   52 02 66 89 0E 26 02 66 03 0E 52 02 66 89 0E 2A   R☻fë♫&☻f♥♫R☻fë♫*
0000080E0   02 66 03 0E 52 02 66 89 0E 3A 02 66 03 0E 52 02   ☻f♥♫R☻fë♫:☻f♥♫R☻
0000080F0   66 89 0E 42 02 66 B8 90 00 00 00 66 8B 0E 22 02   fë♫B☻f╕É   fï♫"☻
000008100   E8 5F 09 66 0B C0 0F 84 57 FE 66 A3 2E 02 66 B8   Φ_○f♂└☼äW■fú.☻f╕
000008110   A0 00 00 00 66 8B 0E 26 02 E8 46 09 66 A3 32 02   á   fï♫&☻ΦF○fú2☻
000008120   66 B8 B0 00 00 00 66 8B 0E 2A 02 E8 34 09 66 A3   f╕░   fï♫*☻Φ4○fú
000008130   36 02 66 A1 2E 02 66 0B C0 0F 84 24 FE 67 80 78   6☻fí.☻f♂└☼ä$■gÇx
000008140   08 00 0F 85 1B FE 67 66 8D 50 10 67 03 42 04 67   ◘ ☼à←■gfìP►g♥B♦g
000008150   66 0F B6 48 0C 66 89 0E 62 02 67 66 8B 48 08 66   f☼╢H♀fë♫b☻gfïH◘f
000008160   89 0E 5E 02 66 A1 5E 02 66 0F B7 0E 0B 00 66 33   ë♫^☻fí^☻f☼╖♫♂ f3
```

The infection flow for non-Kaspersky customers

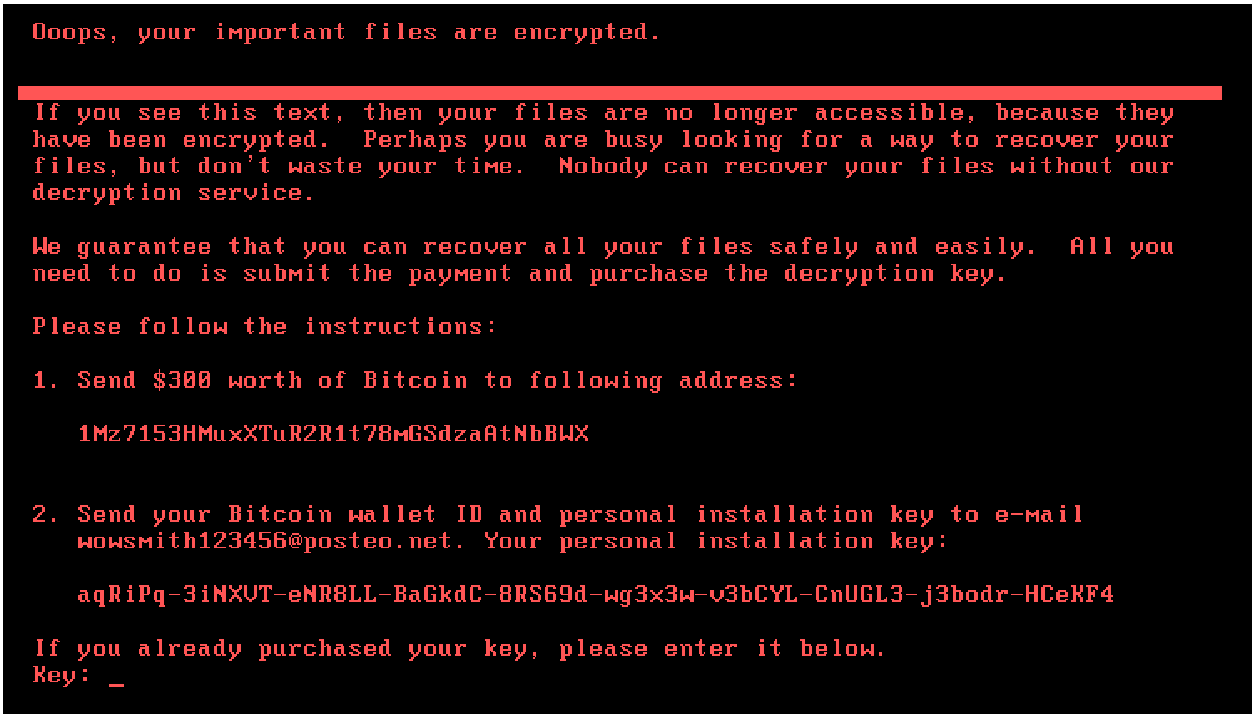
When the computer is rebooted, the encryption process is concealed under an alleged disk-checking process with chkdsk.exe



```
Repairing file system on C:

The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process
may take several hours to complete. It is strongly recommended to let it
complete.

WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD
DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED
IN!

CHKDSK is repairing sector 164096 of 244704 (67%)
```

Figure 7: Fake chkdsk.exe screen that conceals the encryption process

When the drive encryption finishes, the ransomware force-crashes the computer to make it boot from the new boot manager and display the ransom note:



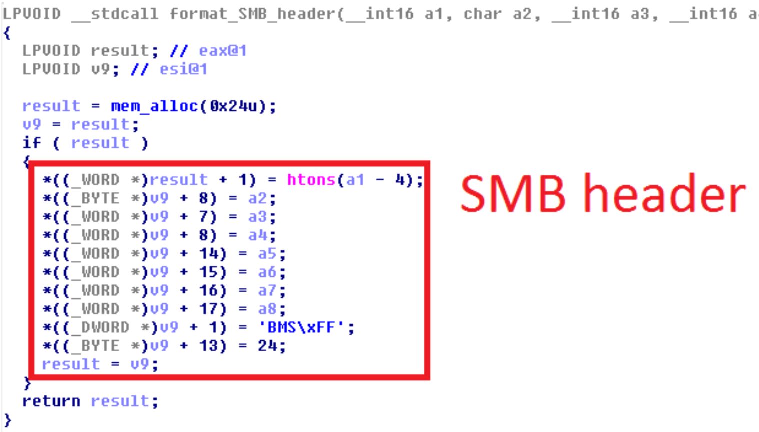
```
Ooops, your important files are encrypted.


If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   aqRiPq-3iNXVT-eNR8LL-BaGkdC-8RS69d-wg3x3w-v3bCYL-CnUGL3-j3bodr-HCeKF4

If you already purchased your key, please enter it below.
Key: _
```

Figure 8: Ransom note displayed after the encryption process has finished

Lateral movement inside the network

Once it has compromised a target on the network, the malware attempts to move laterally inside the organization via two zero day-exploits, as well as via credential dumping.

Exploit-based lateral movement has been covered extensively by the research community as it uses two already notorious vulnerabilities leaked by ShadowBrokers in a trove of exploits allegedly from the NSA. GoldenEye uses EternalBlue and EternalRomance, two exploits against the Server Message Block (SMB) - CVE-2017-0144 and CVE-2017-0145. To exploit potential vulnerabilities and spread across the network, the ransomware generates a SMBv1 buffer and formats it before sending it, as follows:



```
LPVOID __stdcall format_SMB_header(__int16 a1, char a2, __int16 a3, __int16 a4, __int16 a5, __int16 a6, __int16 a7, __int16 a8)
{
  LPVOID result; // eax@1
  LPVOID v9; // esi@1

  result = mem_alloc(0x24u);
  v9 = result;
  if ( result )
  {
    *((_WORD *)result + 1) = htons(a1 - 4);
    *((_BYTE *)v9 + 8) = a2;
    *((_WORD *)v9 + 7) = a3;
    *((_WORD *)v9 + 8) = a4;
    *((_WORD *)v9 + 14) = a5;
    *((_WORD *)v9 + 15) = a6;
    *((_WORD *)v9 + 16) = a7;
    *((_WORD *)v9 + 17) = a8;
    *((_DWORD *)v9 + 1) = 'BMS\xFF';
    *((_BYTE *)v9 + 13) = 24;
    result = v9;
  }
  return result;
}
```

Figure 8: SMB header formatting before sending the buffer

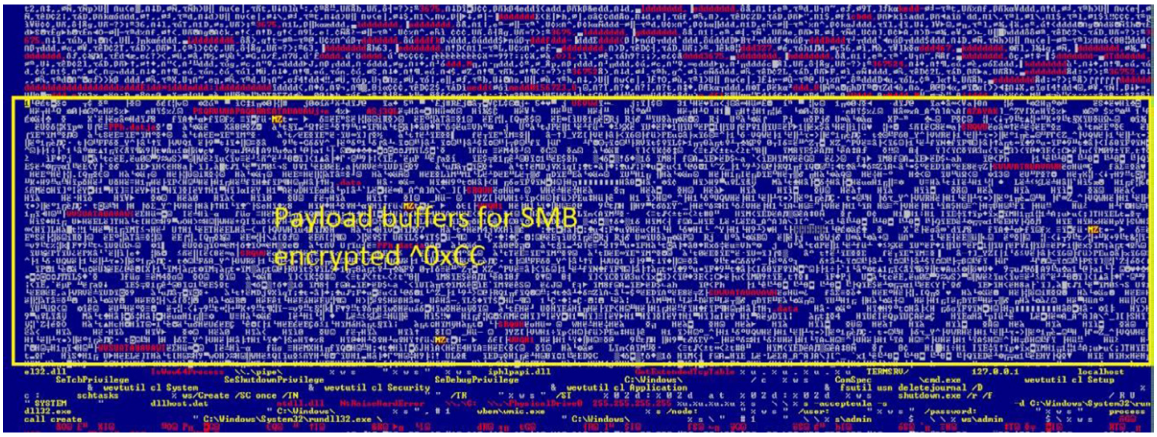


Figure 9: SMB payloads encrypted with 0xCC @100123B0:

As both exploits have been addressed in security updates from the operating system vendor, the malware also has a third lateral movement vector comprised of a credentials dumper for accounts stored in memory and two legit administration tools called PsExec and WMIC. All three tools are stored as ZLIB-compressed resources and are dropped in the temporary folder by the malware when needed.

The credentials dumping tool is similar to the Mimikatz utility and only serves one purpose: to dump usernames and credentials from the memory. These credentials are used to establish connections with other computers on the network on ports **139 (TCP)** and **445 (TCP)**. It also scans for administrative shares (admin$) across the network and copies itself on these shares. These copies get executed on the new nodes via PsExec or WMIC:

```
Psexec:  \\%s -accepteula -s, process call create, wbem\wmic.exe, %s /node:”, “%ws” /
```

```
user:"%ws", "%ws" /password:"%ws"
```

Conclusions

The chain of events that led to the infection, the extent of damage inflicted to one particular country (Ukraine), the complete lack of interest in monetizing the attack as well as the fact that the malware has no contingencies hard-coded to avoid multiple infections of the same host, suggest that this is no ordinary, money-seeking ransomware campaign.

The extremely well designed lateral movement techniques, the prudent probing of the environment for potentially "threatening" antimalware solutions, as well as a highly specialized infection vector (the Ukrainian accounting software) leads us to believe that this ransomware attack is actually an attempt to destroy data and decommission computers inside several Ukrainian organizations.

Because of its wormable behavior, though, it has broken outside of the confines of regional networks and caused havoc all over the world, grabbing news headlines for days.

Bitdefender is a global security technology company that delivers solutions in more than 100 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a leading security provider in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has elevated the highest standards of security excellence in both its number-one-ranked technology and its strategic alliances with the world's leading virtualization and cloud technology providers. More information is available at
http://www.bitdefender.com/

FOR MORE INFORMATION VISIT: enterprise.bitdefender.com