ANOMALI THREATSTREAM

ALERT - Petya Ransomware's Comeback using NSA Hacking Tools

Posted on 2017-06-27 15:08:24 +0000
Last modified on 2017-06-27 17:12:00 +0000

Stage **New**

User Assignment **elie.nasrallah@hitrustalliance.net**
Org Assignment **hitrustalliance.net**

Traffic-Light Protocol **TLP:Green**

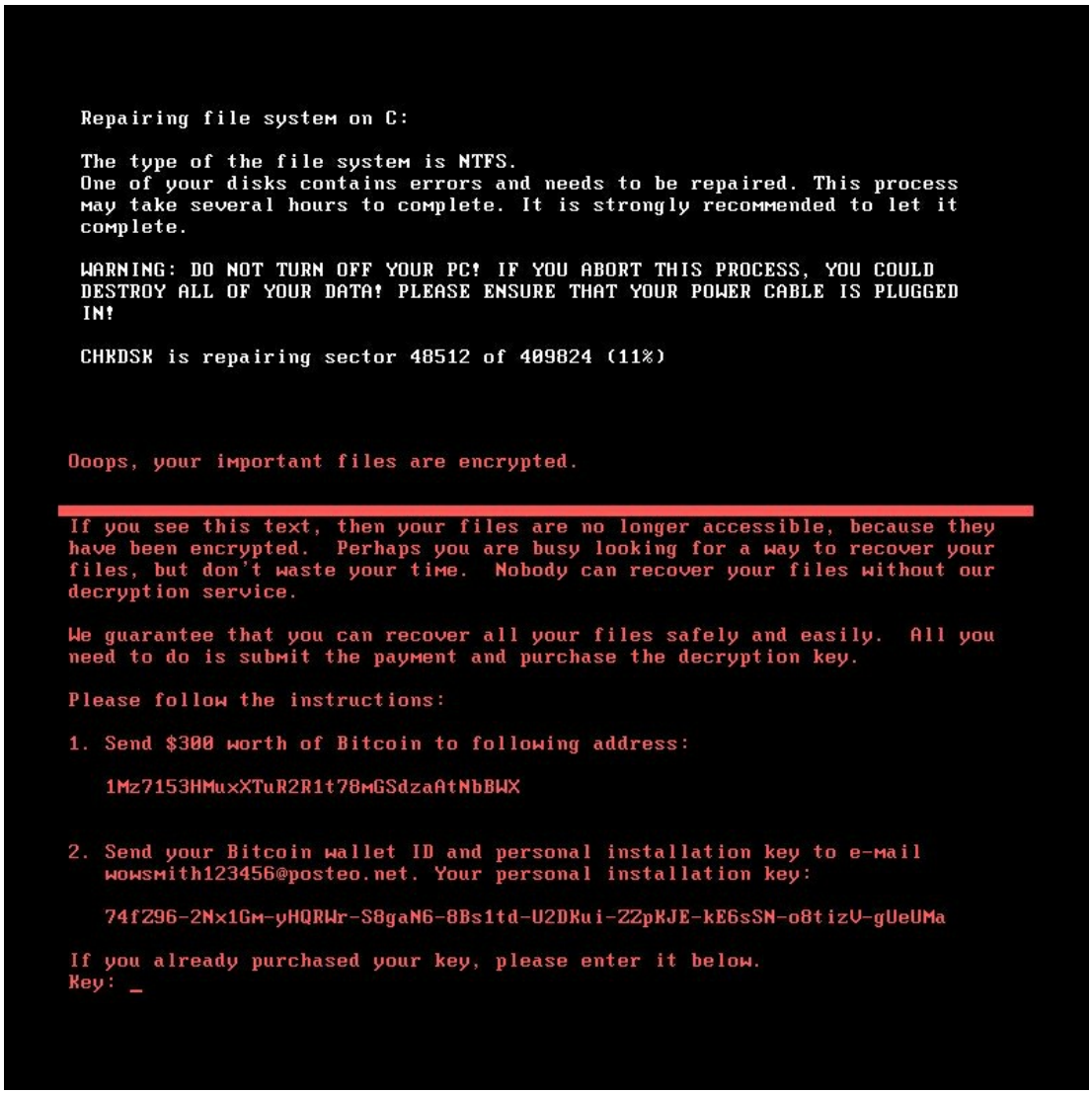
Classification **Trusted Circles**

Shared with Trusted Circles CTX - Academic Medical Centers | CTXIOCTEST | CTX-Pediatric Hospitals and Health Systems | HITRUST-Advanced | HITRUST-Core

---

HITRUST is currently monitoring Petya Ransomware's Comeback, the latest outbreak which has targeted businesses in the Ukraine, India, France, Russia, and Spain. HITRUST will continue to monitor and update this Threat Bulletin.

This new variant of Petya encrypts the MBR and utilizes a set of file extensions as follows: .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.Youssef J. (06/27/17 12:04 PM)
The attacks utilize a new variant of the Petya ransomware and uses a fake Microsoft digital signature in the process.



UPDATE #1: This ransomware is using NSA's EternalBlue code (image below).

Pseudocode-B

```
1  int __stdcall exploit_host(char *cp, int a2, int a3, int a4, int a5, int a6, int a7)
2  {
3    int v7; // edi@1
4    int result; // eax@2
5    int v9; // esi@3
6    char Dst; // [esp+8h] [ebp-54h]@1
7
8    memset(&Dst, 0, 0x54u);
9    LOWORD(dword_1001FB48) = GetTickCount();
10   byte_1001F8FD = 0;
11   v7 = eternal_blue_exploit_host((int)&Dst, cp, 445u, 0, a2, a3, a4, a5, a6, a7);
12   if ( v7 )
13   {
14     sub_10002068((SOCKET *)&Dst);
15     result = v7;
16   }
17   else
18   {
19     byte_1001F8FD = 0;
20     v9 = eternal_blue_exploit_host((int)&Dst, cp, 445u, (int)sub_10001F74, a2, a3, a4, a5, a6, a7);
21     sub_10002068((SOCKET *)&Dst);
22     result = v9;
23   }
24   return result;
25 }
```

UPDATE #2: This variant is using the same exploits as WannaCry, targeting SMB v.1 with the EternalBlue exploit and as such, the mitigation measures that were implemented for WannaCry v2.0 should cover this attack surface.
UPDATE #3: Main IOCs include:

027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745 (sample file name: petwrap.exe)
f8dbabdfa03068130c277ce49c60e35c029ff29d9e3c74c362521f3fb02670d5 (sample file name: dllhost.dat)
benkow{.}

UPDATE #4: This ransomware worm variant does not seem to have a “KillSwitch” like WannaCry v2.0. We recommend great caution!
UPDATE 5: The following Trend Micro update offers additional details. https://success.trendmicro.com/solution/1117665-petya-2017-ransomware-attack-information

HITRUST CTX Enhanced IOC participants can leverage their **Deep Discovery Inspector Rule 2383**: CVE-2017-0144 - Remote Code Execution - SMB (Request)

Import Session

Session 221110 (0)

No Indicators for this import session.

Comments

T_Boardman (Licking Memorial Health Systems) on 2017-06-27 15:21:53 +0000

Breakdown of this particular strain of Petya

https://securelist.com/petrwrap-the-new-petya-based-ransomware-used-in-targeted-attacks/77762/

History

elie.nasrallah (hitrustalliance.net)	Updated Report	2017-06-27 17:12:00 +0000
elie.nasrallah (hitrustalliance.net)	Updated Report	2017-06-27 16:11:09 +0000
elie.nasrallah (hitrustalliance.net)	Updated Report	2017-06-27 15:39:48 +0000
elie.nasrallah (hitrustalliance.net)	Updated Report	2017-06-27 15:29:02 +0000
Trevor Boardman (Licking Memorial Health Systems)	Created Comment	2017-06-27 15:21:53 +0000
elie.nasrallah (hitrustalliance.net)	Created Report	2017-06-27 15:08:25 +0000