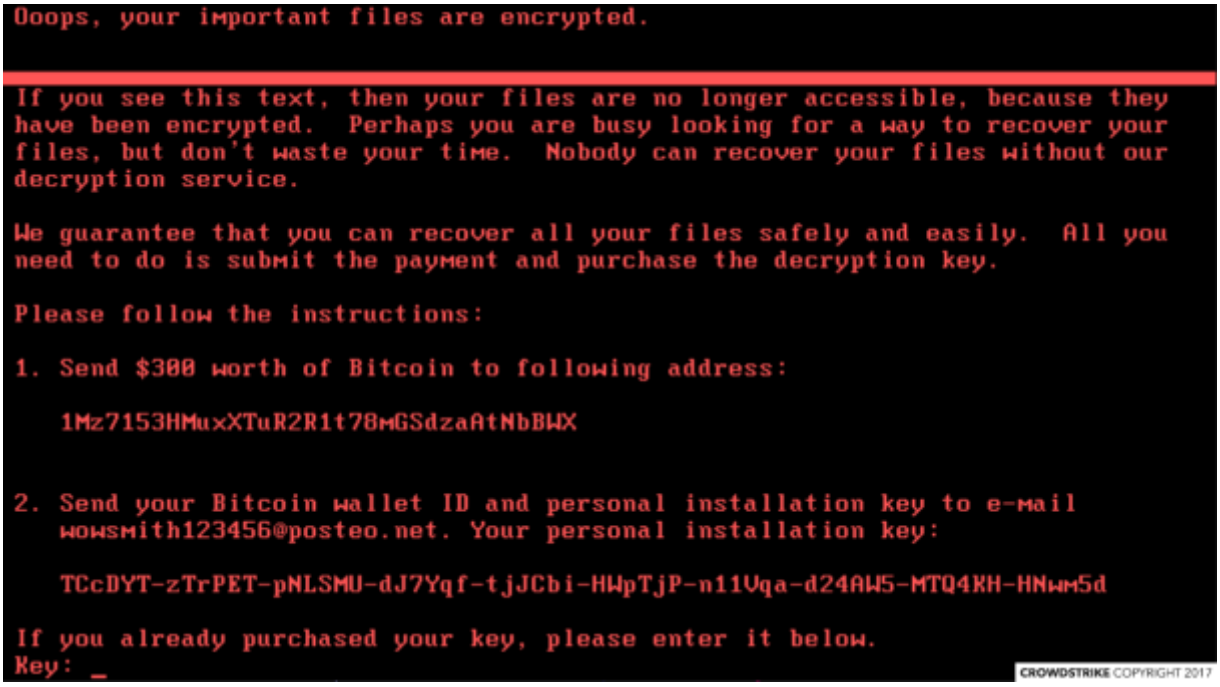
CrowdStrike Intelligence

CSA-17159 Large-Scale Ransomware Attack: Spreading Strategy Combines ETERNALBLUE Exploit and SMB Credential Stealing

CrowdStrike Intelligence has identified a new ransomware family that is currently spreading rapidly across multiple countries. The family, referred to as *PetrWrap* in public reporting, spreads to Microsoft Windows machines using the ETERNALBLUE exploit for the CVE-2017-0144 vulnerability in the SMB service that Microsoft reported on in MS17-010 and that was published as part of the Shadow Brokers release on 14 April 2017.

This new ransomware family is believed to have already caused a significant number of infections from a campaign that was first detected on 27 June 2017. Attacks are being reported across the globe to include Ukraine, Russia, India, France, Spain, Denmark, Poland, and the Netherlands. Sectors impacted by this attack include government, energy, financial, defense, telecom, small business, maritime, aviation, and transportation sectors.

The ETERNALBLUE exploit is used to autonomously spread to and compromise vulnerable machines without user interaction. A similar exploit was used by the *WannaCry* ransomware in a campaign that broke out on 12 May 2017 (see CSA-17124, CSA-17127, and CSA-17130). In addition, infected machines are harvested for Windows user credentials using custom tools packaged into the malware. These credentials are then used to propagate in local networks.



Once the malware is deployed on a victim machine, it creates a scheduled task to reboot the host an hour after the infection, likely in order to allow it to spread further before launching its

2017 CROWDSTRIKE, INC. ALL RIGHTS RESERVED

destructive payload. To achieve this, the malware drops and runs either an x86 or an x64 version of a credential stealer executable from a resource that contains code similar to the well-known *mimikatz* tool.

The ransomware payload uses a combination of 2048-bit RSA and 128-bit AES in Cipher Block Chaining (CBC) mode to encrypt files with extensions matching entries from a hard-coded list. Public reporting mentions similarities with the *Petya* ransomware; however, CrowdStrike was not able to confirm any links, and assesses that the code structure of this new family is different from Petya's.

The criminal operators of this ransomware are currently using the Bitcoin (BTC) wallet 1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX for ransom payment. Since the campaign began, this wallet has received a total of approximately 1.5 BTC in 13 transactions, each being roughly $300 USD.

The following YARA signatures detect the new ransomware payload based on unique hard-coded chunks of data used during the ETERNALBLUE exploitation process and other characteristics in the executable:

```
rule CrowdStrike_SmbRansomware_01 : smb ransomware
{
  meta:
    copyright = "CrowdStrike, Inc"
    description = "SMB Ransomware"
    version = "1.0"
    last_modified = "2017-06-27"
    yara_version = "[>=1.3]"
    in_the_wild = true
  strings:
    $email = "wowsmith123456@posteo.net" wide
    $exts =
".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.m
ail.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.vm
dk.vmsd.vmx.vsdx.vsv.work.xls.xlsx.xvd.zip" wide
    $keymsg_1 = "Your personal installation key:" wide
    $keymsg_2 = "Incorrect key! Please try again."
    $reboot_1 = "schtasks %ws/Create /SC once /TN \"\" /TR \"%ws\" /ST %02d:%02d" wide
    $reboot_2 = "shutdown.exe /r /f" wide
    $func_1 = "SeShutdownPrivilege" wide
    $func_2 = "GetExtendedTcpTable"
    $func_3 = "CryptGenRandom"
    $func_4 = "ConnectNamedPipe"
  condition:
    all of ($func_*) and 3 of ($email, $exts, $keymsg_*, $reboot_*)
}
rule CrowdStrike_SmbRansomware_02 : smb ransomware
{
```

2017 CROWDSTRIKE, INC. ALL RIGHTS RESERVED

```
  meta:
    copyright = "CrowdStrike, Inc"
    description = "SMB Ransomware encoded components"
    version = "1.0"
    last_modified = "2017-06-27"
    yara_version = "[>=1.3]"
    in_the_wild = true
  strings:
    $hdr_10010BB8 = { 2c ed 84 02 e7 80 94 25 33 25 32 25 31 25 30 37 }
    $hdr_100123B0 = { fd 0c 8c 5c b8 c4 24 c5 cc cc cc 0e e8 cc 24 6b }
    $hdr_10012D27 = { 45 20 8d 93 8d 92 8d 91 8d 90 92 93 91 97 0f 9f }
    $hdr_100131A8 = { fd 0c 8c 5c c3 48 5c ca cc cc 24 cc cc cc cc 94 }
  condition:
    all of them
}
rule CrowdStrike_SmbRansomware_03 : smb ransomware
{
  meta:
    copyright = "CrowdStrike, Inc"
    description = "Certificate used by SMB Ransomware"
    version = "1.0"
    last_modified = "2017-06-27"
    yara_version = "[>=1.3]"
    in_the_wild = true
  strings:
    $serial = { 61 01 cf 3e 00 00 00 00 00 0f }
    $rsa_key = { 30 82 01 0a 02 82 01 01 00 bd 30 89 fb 45 72 a8
                 53 6b 9e 89 4f 00 23 c0 be d4 1d 3d b1 59 40 38
                 f3 73 91 82 26 e6 96 12 00 53 d9 1c 82 0e 3c ce
                 1d bb bd f7 42 8d 97 d4 fc 38 1a e4 b9 f9 e3 ec
                 d3 61 03 bf a0 d3 d6 75 4d 5c 46 a9 ed 5e f0 d2
                 e2 69 5b 1a 73 ea b3 1c 8d 04 cd 29 44 a0 64 59
                 2f 1e 98 5d 6e c7 ab 18 39 82 65 c4 a7 bc ab 75
                 88 19 ea 87 97 14 26 b3 7f 26 76 a4 d4 38 39 84
                 e3 b3 26 d5 18 f9 2b e9 d2 c9 16 5a 54 21 f2 97
                 8d 87 86 29 fe f4 49 2c e6 8b f8 04 3f 7d cd cd
                 96 92 86 0d 71 03 e2 d0 fe 0c 42 35 ff d7 b8 3f
                 dd 8e 45 0a 7d f6 d7 4b ad 5b f0 76 72 1d 77 23
                 7d 89 35 c4 1c 5d b2 50 03 4b 47 6d 07 a7 55 88
                 98 06 80 a6 81 ad 54 4e d8 81 d6 fa bf 42 c0 31
                 be 55 0d 99 d5 53 49 12 30 eb e5 a5 88 7c 5e c4
                 7a 5a 14 87 08 b4 37 69 a0 eb 32 24 8c 08 eb f9
                 d4 14 ba e0 fc cd ea a4 15 02 03 01 00 01 }
  condition:
    all of them
}
```

Further information on this evolving threat and campaign will be provided in follow-on CrowdStrike Intelligence.

2017 CROWDSTRIKE, INC. ALL RIGHTS RESERVED