CERT-MU

THE WANNACRY RANSOMWARE

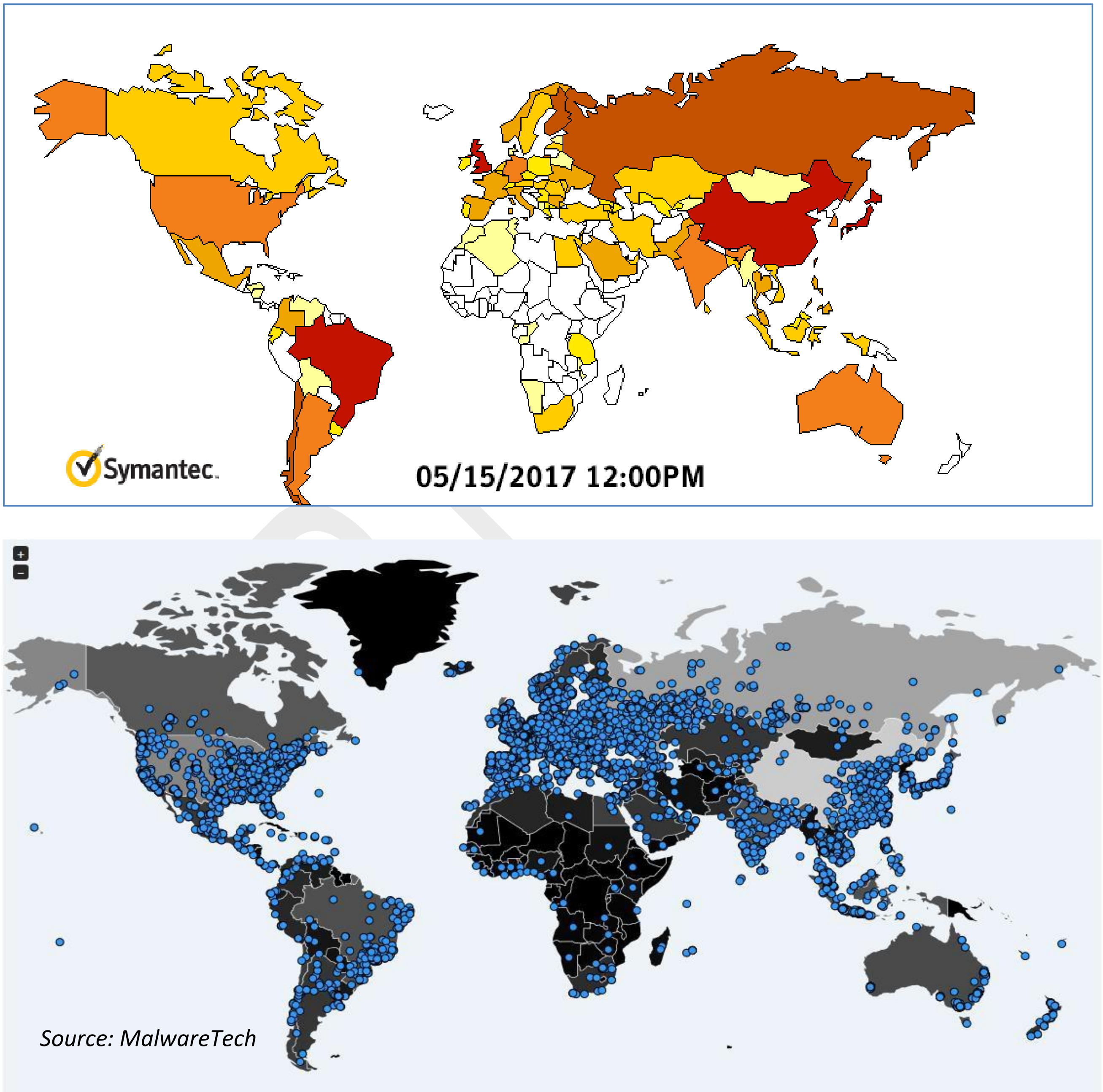
Whitepaper

Prepared By CERT-MU

May 2017

CERT-MU White Paper

THE MASSIVE WANNACRY GLOBAL RANSOMWARE ATTACK



Source: MalwareTech

Maps showing WannaCry Infections around the world

MAY 2017

CONTENTS

1.0 INTRODUCTION

The world has experienced a massive global ransomware cyber-attack known as **“WannaCrypt”** or **“WannaCry”** (Ransom: Win32/WannaCrypt) since Friday, May 12 2017. Hundreds of thousands computers worldwide have been hit and affected more than 150 countries. WannaCry is far more dangerous than other common ransomware types because of its ability to spread itself across an organisation’s network by exploiting a critical vulnerability in Windows computers, which was patched by Microsoft in March 2017 (MS17-010). The exploit, known as “Eternal Blue,” was released online in April in the latest of a series of leaks by a group known as the Shadow Brokers, who claimed that it had stolen the data from the Equation cyber espionage group.

The malware has the capability to scan heavily over TCP port 445 (Server Message Block/SMB), spreading similar to a worm, compromising hosts, encrypting files stored on them then demanding a ransom payment in the form of Bitcoin. It is important to note that this is not a threat that simply scans internal ranges to identify where to spread, it is also capable of spreading based on vulnerabilities it finds in other externally facing hosts across the internet.

Microsoft provided an emergency patch for older system versions on the day of the outbreak. This widespread attack is of high severity, and although the vulnerability being exploited by the attackers should have been patched a while back, many organizations have been hit and the count keeps rising. New versions and variants of this malware are constantly being released, making mitigation harder.

The threat is still under active investigation; the situation may change as we learn more. CERT-MU will continue to actively monitor and analyze this situation for new developments and respond accordingly.

2.0 AFFECTED SYSTEMS

Windows XP through 8.1 (Windows 10 is not vulnerable)

Microsoft released a patch MS17-010 (ETERNALBLUE) on 14 March. More information about the patch is available on:

https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Microsoft released a patch for the older unsupported Windows versions on 12 May, which can be found on:

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

3.0 MALWARE VERSIONS / VARIANTS

The first version broke out on Friday 12 May and the identified malware variants are as follows:

- VARIANT 1: .wcry
- VARIANT 2: WCRY (+ .WCRYT for temp)
- VARIANT 3: .WNCRY (+ .WNCRYT for emp)

A new version, with different kill-switch domain, has been observed on 14 May. This domain has been registered and points to a sinkhole as well. Only 2 letters differ:

www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com becomes

www[.]ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com

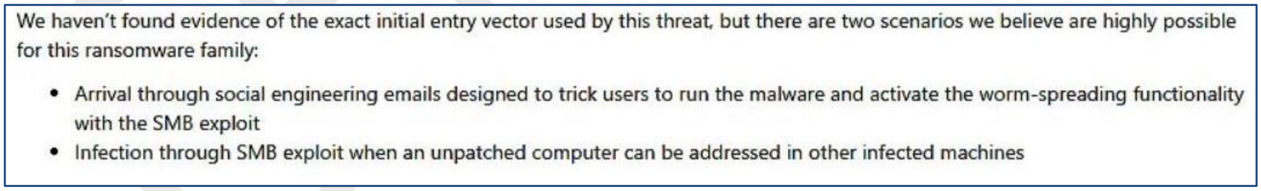
A new version was found on Sunday 14 May that has the kill-switch domain check edited out. This was confirmed by the analysis provided by Rendition Infosec to back up this statement.

A report appeared in the media about a new version (dubbed "2.0" in the media) on Saturday 13 May7. This version was said not to have the kill-switch domain. This was retracted as an error the next day.

4.0 TECHNICAL ANALYSIS OF THE ATTACK

4.1 Distribution of the WannaCry Ransomware

As per Microsoft's analysis report, it is still unclear what the initial infection vector is:



We haven't found evidence of the exact initial entry vector used by this threat, but there are two scenarios we believe are highly possible for this ransomware family:

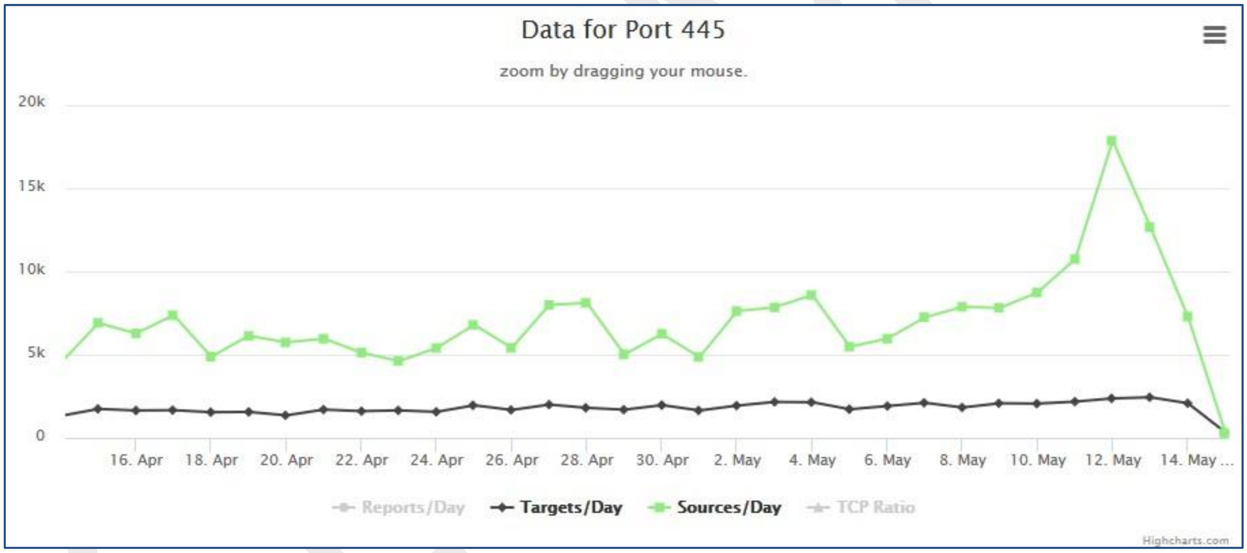
- Arrival through social engineering emails designed to trick users to run the malware and activate the worm-spreading functionality with the SMB exploit
- Infection through SMB exploit when an unpatched computer can be addressed in other infected machines

Once the malware is on a system, its worm capability will try to spread further through SMB. After initializing the functionality used by the worm, two threads are created. The first thread scans hosts on the LAN. The second thread gets created 128 times and scans hosts on the wider Internet.

The scanning thread tries to connect to port 445, and if so creates a new thread to try to exploit the system using the ETERNALBLUE SMB vulnerability (MS17-010). If the exploitation attempts take over 10 minutes, then the exploitation thread is stopped.

As per Cisco Intelligence, WannaCry made use of DOUBLEPULSAR which is a persistent backdoor that is generally used to access and execute code on previously compromised systems. This allows for the installation and activation of additional software, such as malware. This backdoor is typically installed following successful exploitation of SMB vulnerabilities addressed as part of Microsoft Security Bulletin MS17-010. This backdoor is associated with an offensive exploitation framework that was released as part of the Shadow Brokers cache that was recently released to the public. Since its release it has been widely analyzed and studied by the security industry as well as on various underground hacking forums.

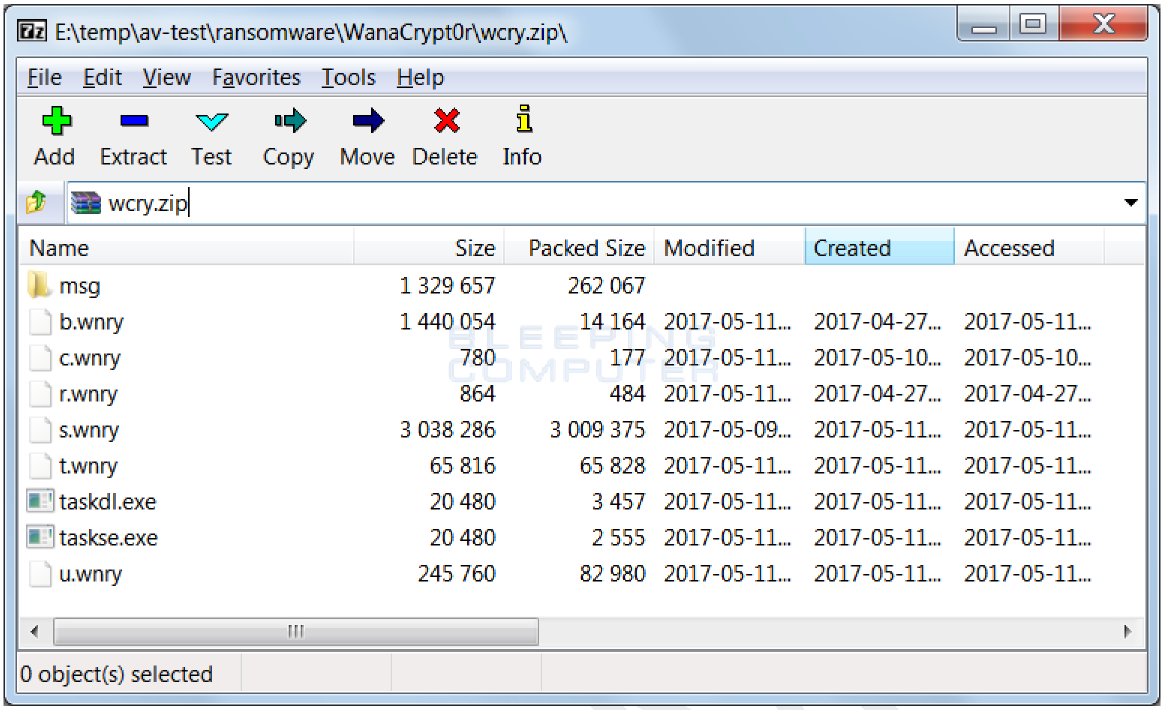
WannaCry appears to primarily utilize the ETERNALBLUE modules and the DOUBLEPULSAR backdoor. The malware uses ETERNALBLUE for the initial exploitation of the SMB vulnerability. If successful, it will then implant the DOUBLEPULSAR backdoor and utilize it to install the malware. If the exploit fails and the DOUBLEPULSAR backdoor is already installed the malware will still leverage this to install the ransomware payload.



Source: https://isc.sans.edu/port.html?port=445

5.0 TECHNICAL ANALYSIS: ENCRYPTION

When a computer becomes infected with Wana Decrypt0r, the installer will extract an embedded file into the same folder that the installer is located in. This embedded resource is a password-protected zip folder that contains a variety of files that are used by and executed by WanaCrypt0r.


E:\temp\av-test\ransomware\WanaCrypt0r\wcry.zip\
File Edit View Favorites Tools Help
Add
Extract
Test
Copy
Move
Delete
Info
wcry.zip
BLEEPING COMPUTER
0 object(s) selected

Name	Size	Packed Size	Modified	Created	Accessed
msg	1 329 657	262 067			
b.wnry	1 440 054	14 164	2017-05-11...	2017-04-27...	2017-05-11...
c.wnry	780	177	2017-05-11...	2017-05-10...	2017-05-10...
r.wnry	864	484	2017-05-11...	2017-04-27...	2017-04-27...
s.wnry	3 038 286	3 009 375	2017-05-09...	2017-05-11...	2017-05-11...
t.wnry	65 816	65 828	2017-05-11...	2017-05-11...	2017-05-11...
taskdl.exe	20 480	3 457	2017-05-11...	2017-05-11...	2017-05-11...
taskse.exe	20 480	2 555	2017-05-11...	2017-05-11...	2017-05-11...
u.wnry	245 760	82 980	2017-05-11...	2017-05-11...	2017-05-11...

Embedded Password Protected Zip File

The WanaDecrypt0r loader will then extract the contents of this zip file into the same folder and perform some startup tasks. It will first extract localized version of the ransom notes into the **msg** folder. The currently supported languages are:

Bulgarian, Chinese (simplified), Chinese (traditional), Croatian, Czech, Danish, Dutch, English, Filipino, Finnish, French, German, Greek, Indonesian, Italian, Japanese, Korean, Latvian, Norwegian, Polish, Portuguese, Romanian, Russian, Slovak, Spanish, Swedish, Turkish, Vietnamese.

WanaCrypt0r will then download a TOR client from: https://dist.torproject.org/torbrowser/6.5.1/tor-win32-0.2.9.10.zip and extract it into the **TaskData** folder.

This TOR client is used to communicate with the ransomware C2 servers at: x7ekbenv2riucmf.onion

- 7g7spgrzlojinas.onion
- xxlvbrloxvriy2c5.onion
- 76jdd2ir2embyv47.onion
- cwwnhwhlz52maqm7.onion

In order to prep the computer so that it can encrypt as many files as possible, WanaCrypt0r will now execute the command **icacls . /grant Everyone:F /T /C /Q** in order to change give everyone full permissions to the files located in the folder and subfolders under where the ransomware was executed. It then terminates processes associated with database servers and mail servers so it can encrypt databases and mail stores as well.

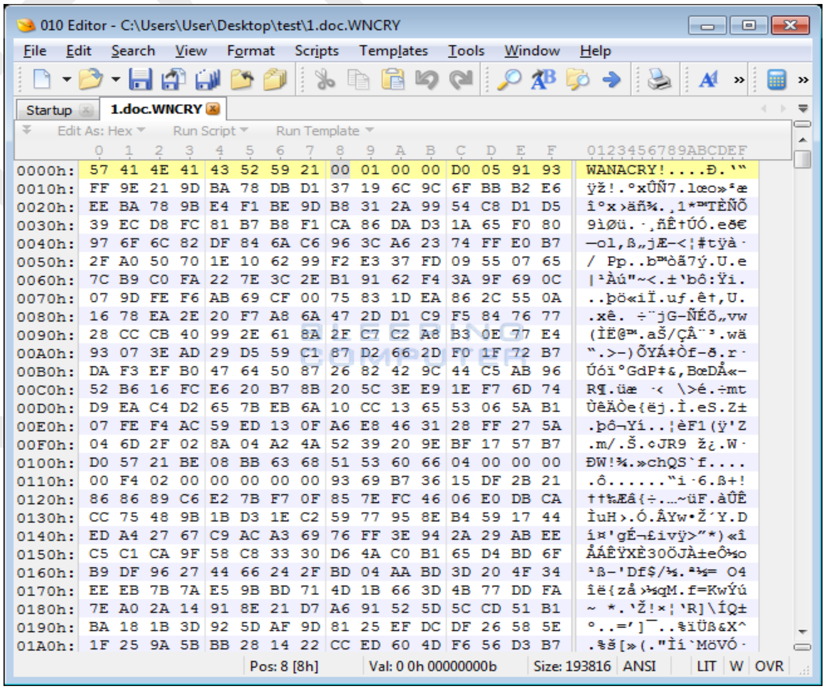
The commands that are executed to terminate the database and exchange server processes are:

```
taskkill.exe /f /im mysqld.exe
taskkill.exe /f /im sqlwriter.exe
taskkill.exe /f /im sqlserver.exe
taskkill.exe /f /im MSExchange*
taskkill.exe /f /im Microsoft.Exchange.*
```

Now, Wana Decrypt0r is ready to start encrypting the files on the computer. When encrypting files, WanaDecrypt0r will scan all drives and mapped network drives for files that have one of the following extensions:

.der, .pfx, .key, .crt, .csr, .pem, .odt, .ott, .sxw, .stw, .uot, .max, .ods, .ots, .sxc, .stc, .dif, .slk, .odp, .otp, .sxd, .std, .uop, .odg, .otg, .sxm, .mml, .lay, .lay6, .asc, .sqlite3, .sqlitedb, .sql, .accdb, .mdb, .dbf, .odb, .frm, .myd, .myi, .ibd, .mdf, .ldf, .sln, .suo, .cpp, .pas, .asm, .cmd, .bat, .vbs, .dip, .dch, .sch, .brd, .jsp, .php, .asp, .java, .jar, .class, .wav, .swf, .fla, .wmv, .mpg, .vob, .mpeg, .asf, .avi,.mov, .mkv, .flv, .wma, .mid, .djvu, .svg, .psd, .nef, .tiff, .tif, .cgm, .raw, .gif, .png, .bmp, .jpg, .jpeg, .vcd, .iso, .backup, .zip, .rar, .tgz, .tar, .bak, .tbk, .PAQ, .ARC, .aes, .gpg, .vmx, .vmdk, .vdi, .sldm, .sldx, .sti, .sxi, .hwp, .snt, .onetoc2, .dwg, .pdf, .wks, .rtf, .csv, .txt, .vsdx, .vsd, .edb, .eml, .msg,.ost, .pst, .potm, .potx, .ppam, .ppsx, .ppsm, .pps, .pot, .pptm, .pptx, .ppt, .xltm, .xltx, .xlc, .xlm, .xlt, .xlw, .xlsb, .xlsm, .xlsx, .xls, .dotx, .dotm, .dot, .docm, .docb, .docx, .doc.

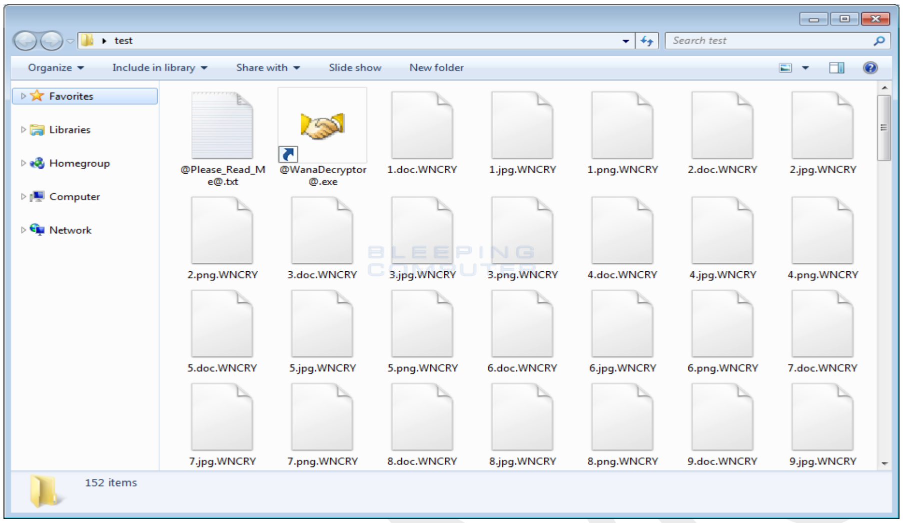
When encrypting a file it will add the **WANACRY!** string, or file marker, to the beginning of the encrypted file,



```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0000h: 57 41 4E 41 43 52 59 21 00 01 00 00 D0 05 91 93  WANACRY!....Ð.‘“
0010h: FF 9E 21 9D BA 78 DB D1 37 19 6C 9C 6F BB B2 E6  ÿž!.ºxÛÑ7.lœo»²æ
0020h: EE BA 78 9B E4 F1 BE 9D B8 31 2A 99 54 C8 D1 D5  îºx›äñ¾.¸1*™TÈÑÕ
0030h: 39 EC D8 FC 81 B7 B8 F1 CA 86 DA D3 1A 65 F0 80  9ìØü.·¸ñÊ†ÚÓ.eð€
0040h: 97 6F 6C 82 DF 84 6A C6 96 3C A6 23 74 FF E0 B7  —ol‚ß„jÆ–<¦#tÿà·
0050h: 2F A0 50 70 1E 10 62 99 F2 E3 37 FD 09 55 07 65  / Pp..b™òã7ý.U.e
0060h: 7C B9 C0 FA 22 7E 3C 2E B1 91 62 F4 3A 9F 69 0C  |¹Àú"~<.±‘bô:Ÿi.
0070h: 07 9D FE F6 AB 69 CF 00 75 83 1D EA 86 2C 55 0A  ..þö«iÏ.uƒ.ê†,U.
0080h: 16 78 EA 2E 20 F7 A8 6A 47 2D D1 C9 F5 84 76 77  .xê. ÷¨jG-ÑÉõ„vw
0090h: 28 CC CB 40 99 2E 61 8A 2F C7 C2 A8 B3 0E 77 E4  (ÌË@™.aŠ/ÇÂ¨³.wä
00A0h: 93 07 3E AD 29 D5 59 C1 87 D2 66 2D F0 1F 72 B7  “.>)ÕYÁ‡Òf-ð.r·
00B0h: DA F3 EF B0 47 64 50 87 26 82 42 9C 44 C5 AB 96  Úóï°GdP‡&‚BœDÅ«–
00C0h: 52 B6 16 FC E6 20 B7 8B 20 5C 3E E9 1E F7 6D 74  R¶.üæ ·‹ \>é.÷mt
00D0h: D9 EA C4 D2 65 7B EB 6A 10 CC 13 65 53 06 5A B1  ÙêÄÒe{ëj.Ì.eS.Z±
00E0h: 07 FE F4 AC 59 ED 13 0F A6 E8 46 31 28 FF 27 5A  .þô¬Yí..¦èF1(ÿ'Z
00F0h: 04 6D 2F 02 8A 04 A2 4A 52 39 20 9E BF 17 57 B7  .m/.Š.¢JR9 ž¿.W·
0100h: D0 57 21 BE 08 BB 63 68 51 53 60 66 04 00 00 00  ÐW!¾.»chQS`f....
0110h: 00 F4 02 00 00 00 00 00 93 69 B7 36 15 DF 2B 21  .ô......“i·6.ß+!
0120h: 86 86 89 C6 E2 7B F7 0F 85 7E FC 46 06 E0 DB CA  ††‰Æâ{÷.…~üF.àÛÊ
0130h: CC 75 48 9B 1B D3 1E C2 59 77 95 8E B4 59 17 44  ÌuH›.Ó.ÂYw•Ž´Y.D
0140h: ED A4 27 67 C9 AC A3 69 76 FF 3E 94 2A 29 AB EE  í¤'gÉ¬£ivÿ>”*)«î
0150h: C5 C1 CA 9F 58 C8 33 30 D6 4A C0 B1 65 D4 BD 6F  ÅÁÊŸXÈ30ÖJÀ±eÔ½o
0160h: B9 DF 96 27 44 66 24 2F BD 04 AA BD 3D 20 4F 34  ¹ß–'Df$/½.ª½= O4
0170h: EE EB 7B 7A E5 9B BD 71 4D 1B 66 3D 4B 77 DD FA  îë{zå›½qM.f=KwÝú
0180h: 7E A0 2A 14 91 8E 21 D7 A6 91 52 5D 5C CD 51 B1  ~ *.‘Ž!×¦‘R]\ÍQ±
0190h: BA 18 1B 3D 92 5D AF 9D 81 25 EF DC DF 26 58 5E  º..=’]¯..%ïÜß&X^
01A0h: 1F 25 9A 5B BB 28 14 22 CC ED 60 4D F6 56 D3 B7  .%š[»(."Ìí`MöVÓ·
              Pos: 8 [8h]  Val: 0 0h 00000000b  Size: 193816  ANSI  LIT  W  OVR
```

File Marker

It will then append the **.WNCRY** extension to the encrypted file to denote that the file has been encrypted. For example, a file called **test.jpg** would be encrypted and have a new name of **test.jpg.WNCRY**.



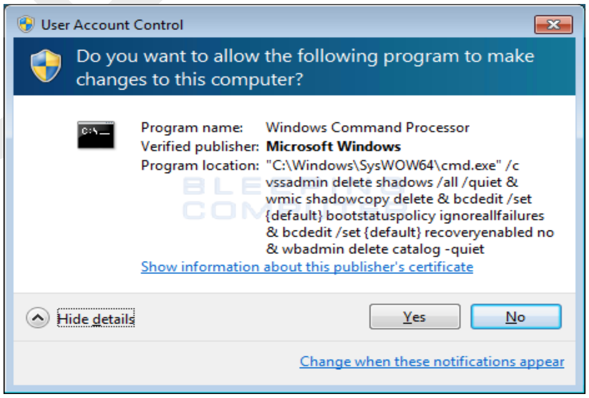
When encrypting files, it will also store a **@Please_Read_Me@.txt** ransom note and a copy of the

@WanaDecryptor@.exe decryptor in every folder that a file was encrypted. We will take a look at those files later.

Finally, WanaCrypt0r will issue some commands that clear the Shadow Volume Copies, disable Windows startup recovery, clear Windows Server Backup history. The commands that are issued are:

```
C:\Windows\SysWOW64\cmd.exe /c vssadmin delete shadow /all /quiet & wmic shadowcopy delete & bcdedit /set {default} boostatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -quiet
```

As these commands require Administrative privileges, victims will see a UAC prompt similar to the one below:

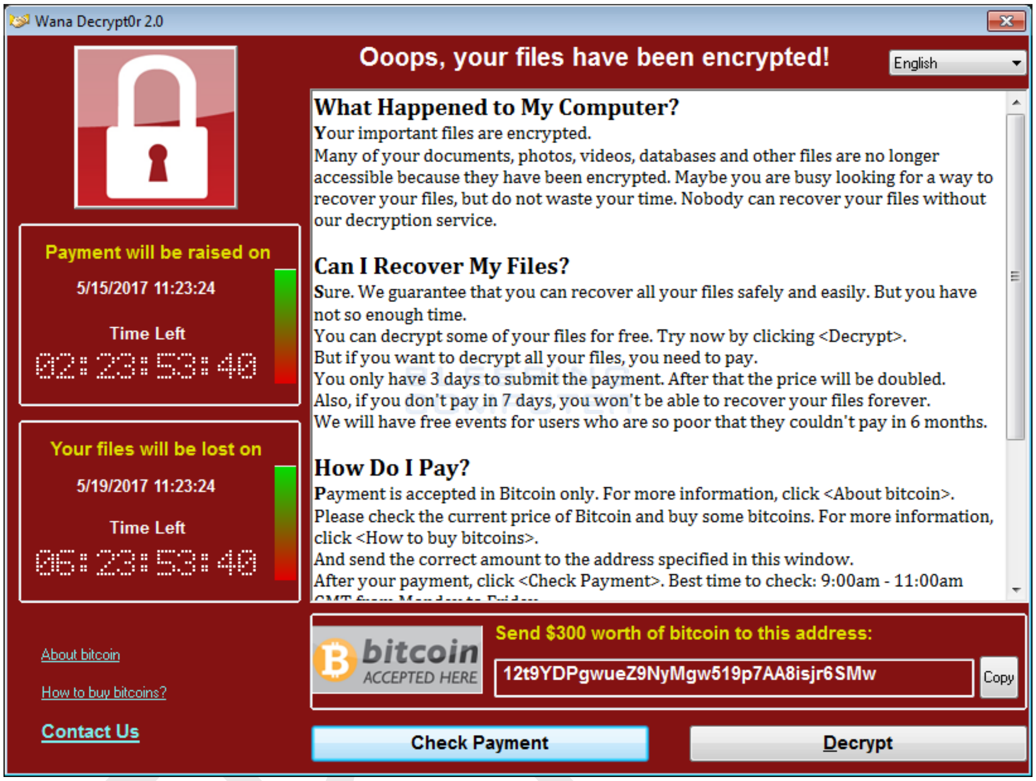

User Account Control
Show information about this publisher's certificate
Hide details
Yes
No
Change when these notifications appear
BLEEPING COMPUTER

Do you want to allow the following program to make changes to this computer?

Program name: Windows Command Processor
Verified publisher: **Microsoft Windows**
Program location: "C:\Windows\SysWOW64\cmd.exe" /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -quiet

UAC Prompt

Finally, the installer will execute the **@WanaDecryptor@.exe** program so that the Wana Decryptor 2.0 lock screen will be displayed. This screen contains further information as to how the ransom can be paid and allows you to select one of the languages listed above. Once you see this screen and realize you are infected, it is important to terminate all the malware processes as Wana Decrypt0r will continue to encrypt new files as they are made.



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on

5/15/2017 11:23:24

Time Left

02:23:53:40

Your files will be lost on

5/19/2017 11:23:24

Time Left

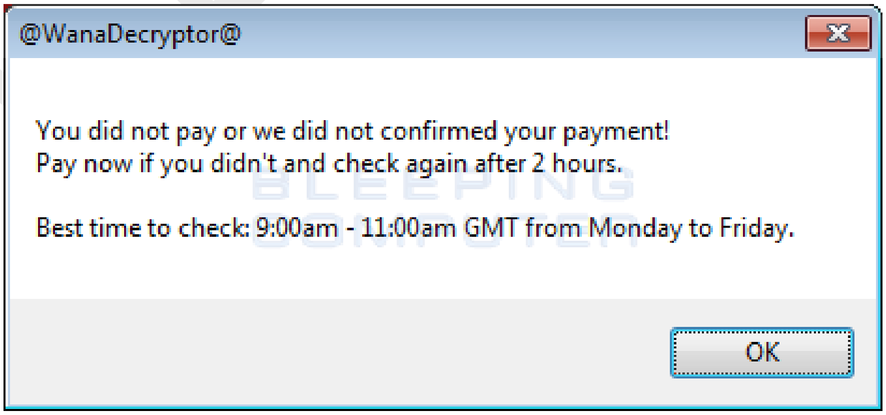
06:23:53:40

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Wana Decrypt0r 2.0 Lock Screen

When you click on the **Check Payment** button, the ransomware connects back to the TOR C2 servers to see if a payment has been made. Even If one was made, the ransomware will automatically decrypt your files. If payment has not been made, you will see a response like the one below.



@WanaDecryptor@

You did not pay or we did not confirmed your payment!
Pay now if you didn't and check again after 2 hours.

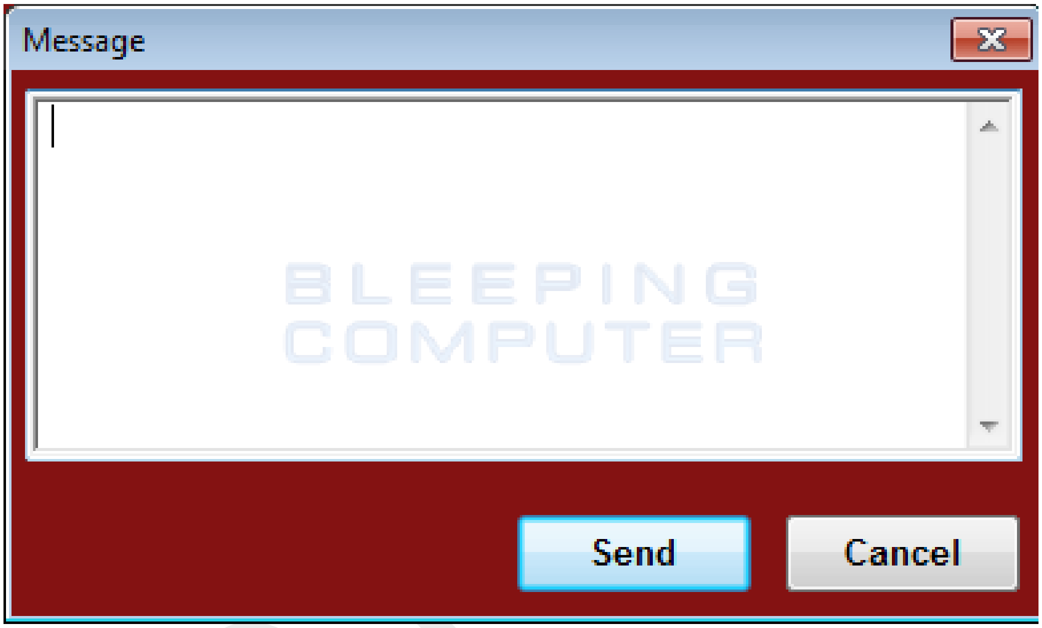
Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment not made Response

There are three bitcoin addresses in the WanaCrypt0r ransomware and they are:

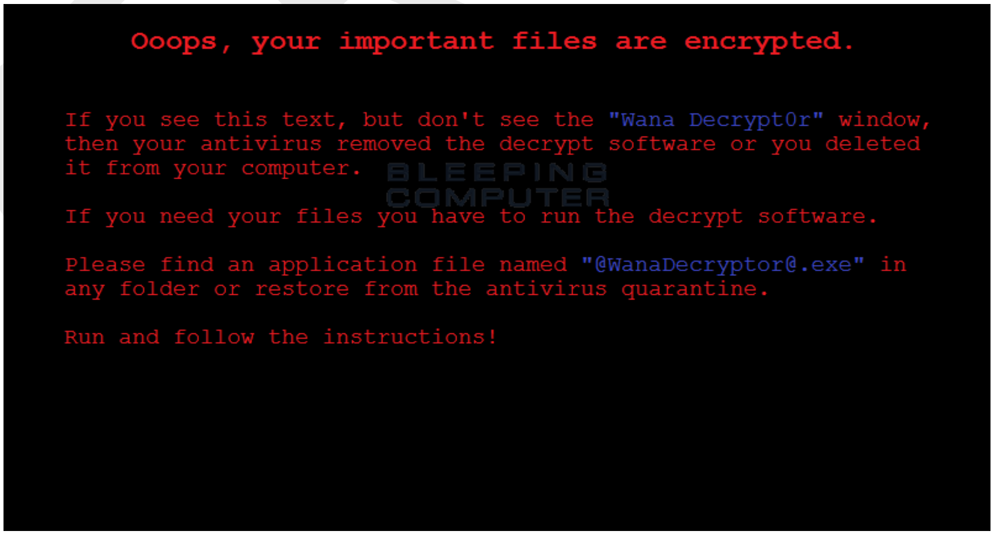
- 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
- 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
- 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn.

The Wana Decryptor 2.0 screen also has a **Contact Us** label that opens a form where you can contact the ransomware developer.



Contact Us Form

The ransomware will also configure your Desktop wallpaper to display another ransom note as shown below:



Ooops, your important files are encrypted.

If you see this text, but don't see the "Wana Decrypt0r" window, then your antivirus removed the decrypt software or you deleted it from your computer.

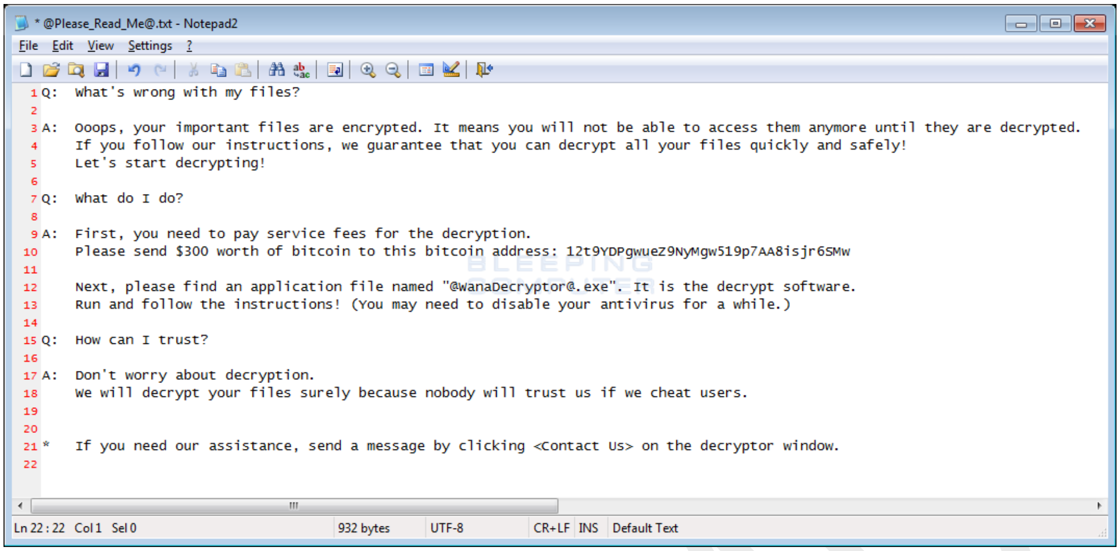
If you need your files you have to run the decrypt software.

Please find an application file named "@WanaDecryptor@.exe" in any folder or restore from the antivirus quarantine.

Run and follow the instructions!

Desktop Wallpaper

Finally, a ransom note will be left on the desktop that contains more information and answers to frequently asked questions. This is shown in the screenshot below:

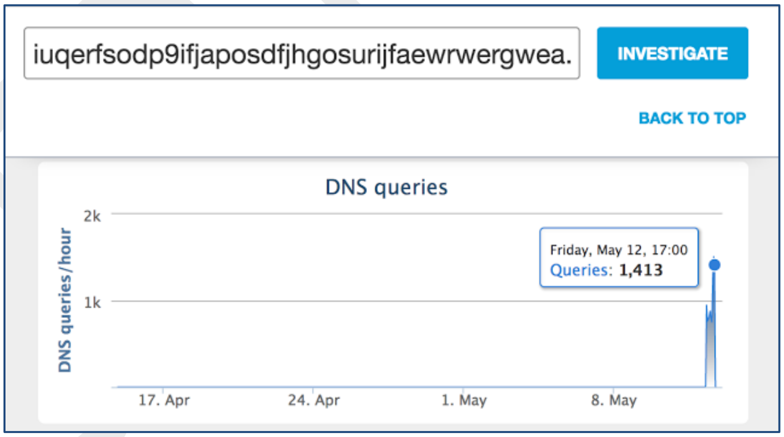


```
Q:  What's wrong with my files?

A:  Ooops, your important files are encrypted. It means you will not be able to access them anymore until they are decrypted.
    If you follow our instructions, we guarantee that you can decrypt all your files quickly and safely!
    Let's start decrypting!

Q:  What do I do?

A:  First, you need to pay service fees for the decryption.
    Please send $300 worth of bitcoin to this bitcoin address: 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

    Next, please find an application file named "@WanaDecryptor@.exe". It is the decrypt software.
    Run and follow the instructions! (You may need to disable your antivirus for a while.)

Q:  How can I trust?

A:  Don't worry about decryption.
    We will decrypt your files surely because nobody will trust us if we cheat users.


    If you need our assistance, send a message by clicking <Contact Us> on the decryptor window.
```

@Please_Read_Me@.txt Ransom Note

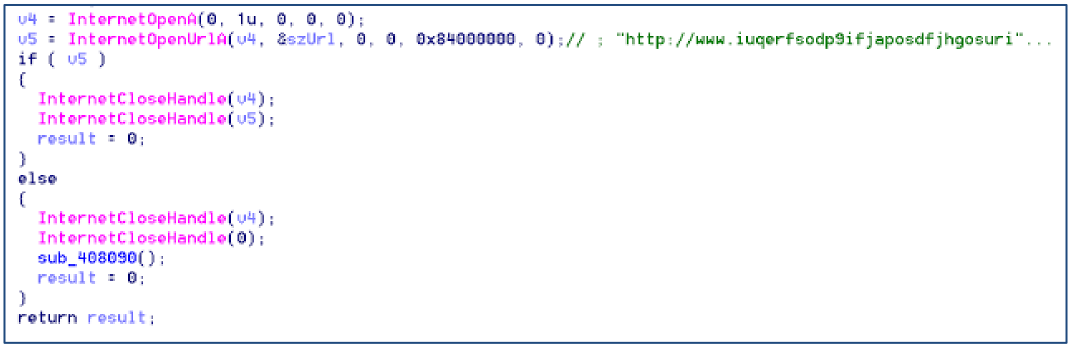
6.0 TECHNICAL ANALYSIS: INFRASTRUCTURE

Cisco researchers first observed requests for one of WannaCry's killswitch domains (**iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com**) starting at 07:24 UTC, then rising to a peak of just over 1,400 nearly 10 hours later.



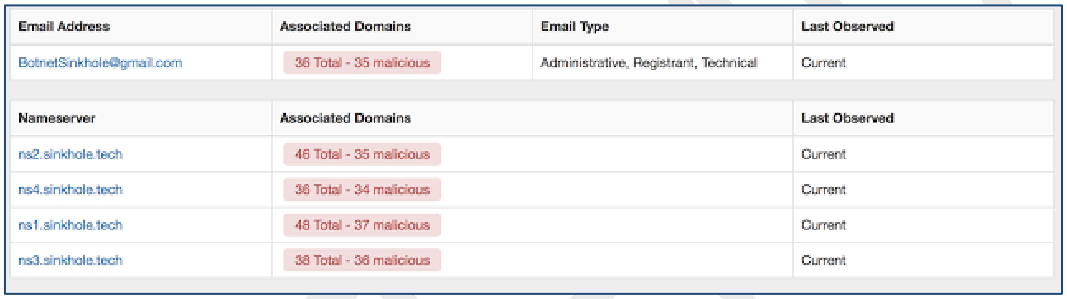
Source: http://blog.talosintelligence.com/2017/05/wannacry.html

The domain composition looks almost human typed, with most characters falling into the top and home rows of a keyboard. Communication to this domain might be categorized as a kill switch domain due to its role in the overall execution of the malware:



```
v4 = InternetOpenA(0, 1u, 0, 0, 0);
v5 = InternetOpenUrlA(v4, &szUrl, 0, 0, 0x84000000, 0);// ; "http://www.iuqerfsodp9ifjaposdfjhgosuri"...
if ( v5 )
{
  InternetCloseHandle(v4);
  InternetCloseHandle(v5);
  result = 0;
}
else
{
  InternetCloseHandle(v4);
  InternetCloseHandle(0);
  sub_408090();
  result = 0;
}
return result;
```

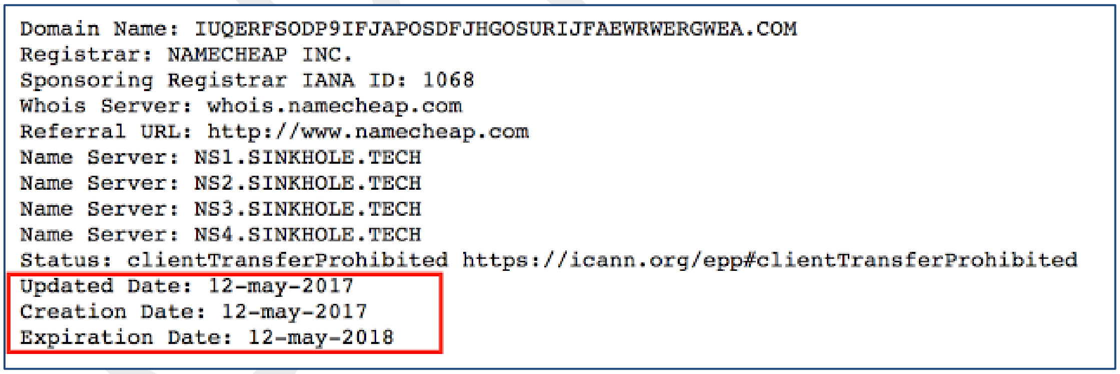
The above subroutine attempts an HTTP GET to this domain, and if it fails, continues to carry out the infection. However if it succeeds, then the subroutine exits. The domain is registered to a well- known sinkhole, effectively causing the sample to terminate its malicious activity.



Email Address	Associated Domains	Email Type	Last Observed
BotnetSinkhole@gmail.com	38 Total - 35 malicious	Administrative, Registrant, Technical	Current

Nameserver	Associated Domains	Last Observed
ns2.sinkhole.tech	46 Total - 35 malicious	Current
ns4.sinkhole.tech	36 Total - 34 malicious	Current
ns1.sinkhole.tech	48 Total - 37 malicious	Current
ns3.sinkhole.tech	38 Total - 36 malicious	Current

The raw registration information re-enforces this as it was registered on 12 May 2017:



```
Domain Name: IUQERFSODP9IFJAPOSDFJHGOSURIJFAEWRWERGWEA.COM
Registrar: NAMECHEAP INC.
Sponsoring Registrar IANA ID: 1068
Whois Server: whois.namecheap.com
Referral URL: http://www.namecheap.com
Name Server: NS1.SINKHOLE.TECH
Name Server: NS2.SINKHOLE.TECH
Name Server: NS3.SINKHOLE.TECH
Name Server: NS4.SINKHOLE.TECH
Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Updated Date: 12-may-2017
Creation Date: 12-may-2017
Expiration Date: 12-may-2018
```

7.0 KILL-SWITCH AND KILL-MUTEX

A kill switch is an event that is used to stop a program from continuing to execute. In the case of WannaCry, the kill switch is a domain name that the Worm component of WannCry connects to when it starts.

When the WannaCry worm was released on March 12th, the kill switch domain was set to **www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com**

The malware stops if it finds the following domain exists:
www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com

It is to be noted that organisations that use proxies will not benefit from the kill-switch, unless it is a transparent proxy. The malware is not proxy-aware, so it will not be able to connect to the kill-switch domain and thus the malware will not be stopped. The malware tries to create a mutex named **MsWinZonesCacheCounterMutexA.** If it exists already, the encryption phase will not be done.

8.0 MALWARE INDICATORS

SHA256 hashes

```
593bbcc8f34047da9960b8456094c0eaf69caaf16f1626b813484207df8bd8af
5ad4efd90dcde01d26cc6f32f7ce3ce0b4d4951d4b94a19aa097341aff2acaec
5c1f4f69c45cff9725d9969f9ffcf79d07bd0f624e06cfa5bcbacd2211046ed6
5d26835be2cf4f08f2beeff301c06d05035d0a9ec3afacc71dff22813595c0b9
62d828ee000e44f670ba322644c2351fe31af5b88a98f2b2ce27e423dcf1d1b1
6bf1839a7e72a92a2bb18fbedf1873e4892b00ea4b122e48ae80fac5048db1a7
7108d6793a003695ee8107401cfb17af305fa82ff6c16b7a5db45f15e5c9e12d
72af12d8139a80f317e851a60027fdf208871ed334c12637f49d819ab4b033dd
76a3666ce9119295104bb69ee7af3f2845d23f40ba48ace7987f79b06312bbdf
78e3f87f31688355c0f398317b2d87d803bd87ee3656c5a7c80f0561ec8606df
7a828afd2abf153d840938090d498072b7e507c7021e4cdd8c6baf727cafc545
7c465ea7bcccf4f94147add808f24629644be11c0ba4823f16e8c19e0090f0ff
7e369022da51937781b3efe6c57f824f05cf43cbd66b4a24367a19488d2939e4
85ce324b8f78021ecfc9b811c748f19b82e61bb093ff64f2eab457f9ef19b186
9588f2ef06b7e1c8509f32d8eddfa18041a9cc15b1c90d6da484a39f8dcdf967
97ebce49b14c46bebc9ec2448d00e1e397123b256e2be9eba5140688e7bc0ae6
9b60c622546dc45cca64df935b71c26dcf4886d6fa811944dbc4e23db9335640
9cc32c94ce7dc6e48f86704625b6cdc0fda0d2cd7ad769e4d0bb1776903e5a13
9e60269c5038de8956a1c6865ebea8627a440a6e839f61e940a8d5f2c6ea4982
9fb39f162c1e1eb55fbf38e670d5e329d84542d3dfcdc341a99f5d07c4b50977
a1d9cd6f189beff28a0a49b10f8fe4510128471f004b3e4283ddc7f78594906b
a3900daf137c81ca37a4bf10e9857526d3978be085be265393f98cb075795740
a897345b68191fd36f8cefb52e6a77acb2367432abb648b9ae0a9d708406de5b
a93ee7ea13238bd038bcbec635f39619db566145498fe6e0ea60e6e76d614bd3
aee20f9188a5c3954623583c6b0e6623ec90d5cd3fdec4e1001646e27664002c
b3c39aeb14425f137b5bd0fd7654f1d6a45c0e8518ef7e209ad63d8dc6d0bac7
b43b234012b8233b3df6adb7c0a3b2b13cc2354dd6de27e092873bf58af2693c
b47e281bfbeeb0758f8c625bed5c5a0d27ee8e0065ceeadd76b0010d226206f0
b66db13d17ae8bcaf586180e3dcd1e2e0a084b6bc987ac829bbff18c3be7f8b4
b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25
be22645c61949ad6a077373a7d6cd85e3fae44315632f161adc4c99d5a8e6844
```

```
c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7badaf9
ca29de1dc8817868c93e54b09f557fe14e40083c0955294df5bd91f52ba469c8
d5e0e8694ddc0548d8e6b87c83d50f4ab85c1debadb106d6a6a794c3e746f4fa
d8a9879a99ac7b12e63e6bcae7f965fbf1b63d892a8649ab1d6b08ce711f7127
dff26a9a44baa3ce109b8df41ae0a301d9e4a28ad7bd7721bbb7ccd137bfd696
e14f1a655d54254d06d51cd23a2fa57b6ffdf371cf6b828ee483b1b1d6d21079
e18fdd912dfe5b45776e68d578c3af3547886cf1353d7086c8bee037436dff4b
e8450dd6f908b23c9cbd6011fe3d940b24c0420a208d6924e2d920f92c894a96
eb47cd6a937221411bb8daf35900a9897fb234160087089a064066a65f42bcd4
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
eeb9cd6a1c4b3949b2ff3134a77d6736b35977f951b9c7c911483b5caeb1c1fb
f7c7b5e4b051ea5bd0017803f40af13bed224c4b0fd60b890b6784df5bd63494
f8812f1deb8001f3b7672b6fc85640ecb123bc2304b563728e6235ccbe782d85
fb0b6044347e972e21b6c376e37e1115dab494a2c6b9fb28b92b1e45b45d0ebc
fc626fe1e0f4d77b34851a8c60cdd11172472da3b9325bfe288ac8342f6c710a
```

9.0 COMMAND AND CONTROL SERVERS (ON THE TOR NETWORK)

The malware uses the following C&C Servers to connect:

- 57g7spgrzlojinas.onion
- 76jdd2ir2embyv47.onion
- cwwnhwhlz52ma.onion
- gx7ekbenv2riucmf.onion
- sqjolphimrr7jqw6.onion
- xxlvbrloxvriy2c5.onion

10. 0 IMPACT OF THE ATTACK

Ransomware not only targets home users; businesses can also become infected with ransomware, leading to negative consequences, including:

- temporary or permanent loss of sensitive or proprietary information,
- disruption to regular operations,
- financial losses incurred to restore systems and files, and
- potential harm to an organization's reputation.

Paying the ransom does not guarantee the encrypted files will be released; it only guarantees that the malicious actors receive the victim's money, and in some cases, their banking information. In addition, decrypting files does not mean the malware infection itself has been removed.

11.0 DETECTION OF THE ATTACK BY ANTI-VIRUS

Microsoft Anti-Malware products detect the present version of this WannaCry ransomware as ***Ransom:Win32.WannaCrypt*** from definition version 1.243.291.0

Various anti-virus software detect the malware as:

- Ransom.Wannacry
- Ransom.CryptXXX
- Trojan.Gen.8!Cloud
- Trojan.Gen.2

12.0 CAN THE ENCRYPTED FILES BE RECOVERED?

Decryption is not available at this time but security firms are working on it. Users are strongly recommended not to pay the ransom. Encrypted files should be restored from back-ups where possible.

13.0 WORKAROUNDS

Recommended Steps for Prevention

- Apply the Microsoft patch for the MS17-010 SMB vulnerability dated March 14, 2017.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate in-bound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching the end users.

- Ensure anti-virus and anti-malware solutions are set to automatically conduct regular scans.

- Manage the use of privileged accounts. Implement the principle of least privilege. No users should be assigned administrative access unless absolutely needed. Those with a need for administrator accounts should only use them when necessary.

- Configure access controls including file, directory, and network share permissions with least privilege in mind. If a user only needs to read specific files, they should not have write access to those files, directories, or shares.

- Disable macro scripts from Microsoft Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Office suite applications.
- Develop, institute, and practice employee education programs for identifying scams, malicious links, and attempted social engineering.
- Run regular penetration tests against the network, no less than once a year. Ideally, run these as often as possible and practical.
- Test your backups to ensure they work correctly upon use.

13.1 Recommendations for Network Protection

Apply the patch (MS17-010). If the patch cannot be applied, consider:

- Disabling SMBv1 and
- blocking all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

Note: *disabling or blocking SMB may create problems by obstructing access to shared files, data, or devices. The benefits of mitigation should be weighed against potential disruptions to users.*

13.2 Consider implementing the following best practices:

- Segregate networks and functions.
- Limit unnecessary lateral communications.
- Harden network devices.
- Secure access to infrastructure devices.
- Perform out-of-band network management.
- Validate integrity of hardware and software.

13.3 Recommended Steps for Remediation

- Implement your security incident response and business continuity plan. Ideally, organizations should ensure they have appropriate backups so their response is simply to restore the data from a known clean backup.

13.4 **Defending Against Ransomware Generally**

Precautionary measures to mitigate ransomware threats include:

- Ensure anti-virus software is up-to-date.
- Implement a data back-up and recovery plan to maintain copies of sensitive or proprietary data in a separate and secure location. Backup copies of sensitive data should not be readily accessible from local networks.
- Scrutinize links contained in emails, and do not open attachments included in unsolicited emails.
- Only download software, especially free software - from sites you know and trust.
- Enable automated patches for your operating system and Web browser.

14.0 REFERENCES

https://www.bleepingcomputer.com/news/security/wana-decryptor-wanacrypt0r-technical-nose-dive/
http://blog.talosintelligence.com/2017/05/wannacry.html
https://blog.malwarebytes.com/threat-analysis/2017/05/the-worm-that-spreads-wanacrypt0r/
https://securingtomorrow.mcafee.com/executive-perspectives/analysis-wannacry-ransomware-outbreak/
https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html
https://blog.didierstevens.com/2017/05/13/quickpost-wcry-killswitch-check-is-not-proxy-aware/
https://blog.fox-it.com/2017/05/12/massive-outbreak-of-ransomware-variant-infects-large-amounts-of-computers- around-the-world/
https://www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis
https://securingtomorrow.mcafee.com/mcafee-labs/analysis-wannacry-ransomware/
https://www.anomali.com/blog/wanacry#When:02:43:00Z
https://www.ncsc.gov.uk/news/statement-international-ransomware-cyber-attack
https://www.us-cert.gov/ncas/current-activity/2017/05/12/Multiple-Ransomware-Infections-Reported
https://www.us-cert.gov/ncas/alerts/TA17-132A
http://blog.fortinet.com/2017/05/12/protecting-your-organization-from-the-wcry-ransomware
https://www.thaicert.or.th/alerts/user/2017/al2017us001.html
https://auscert.org.au/resources/blog/ongoing-global-ransomware-attack
https://www.csa.gov.sg/singcert/news/advisories-alerts/wanacrypt0r-aka-wannacry--what-you-need-to-know-and- the-actions-to-take
https://circl.lu/pub/tr-41/#proactive-measures-for-the-wannacry-ransomware
https://www.pcrisk.com/removal-guides/10942-wcry-ransomware#a2
https://isc.sans.edu/diary/22420
http://www.bbc.co.uk/news/health-39899646
https://digital.nhs.uk/article/1491/Statement-on-reported-NHS-cyber-attack
https://www.infosecurity-magazine.com/news/massive-ransomware-attack-hits-nhs/
https://arstechnica.com/information-technology/2017/05/nhs-ransomware-cyber-attack/
https://krebsonsecurity.com/2017/05/u-k-hospitals-hit-in-widespread-ransomware-attack/
https://www.bleepingcomputer.com/news/security/telefonica-tells-employees-to-shut-down-computers-amid- massive-ransomware-outbreak/
http://www.reuters.com/article/us-spain-cyber-idUSKBN1881TJ?feedType=RSS&feedName=technologyNews
https://www.theregister.co.uk/2017/05/12/spain_ransomware_outbreak/
https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/
http://www.reuters.com/article/us-portugal-cyber-idUSKBN1882AP?feedType=RSS&feedName=technologyNews
https://www.ncsc.gov.uk/blog-post/finding-kill-switch-stop-spread-ransomware-0

https://www.dhs.gov/news-releases/press-releases

http://www.csoonline.com/article/3196237/security/a-ransomware-attack-is-spreading-worldwide-using-alleged-nsa- exploit.html

https://blog.avast.com/ransomware-that-infected-telefonica-and-nhs-hospitals-is-spreading-aggressively-with-over-

50000-attacks-so-far-today

https://isc.sans.edu/diary/Massive+wave+of+ransomware+ongoing/22412

https://www.cyberscoop.com/unprecedented-ransomware-outbreak-spreads-across-england-and-spain/

http://www.darkreading.com/attacks-breaches/wannacry-rapidly-moving-ransomware-attack-spreads-to-74- countries/d/d-id/1328874

https://www.infosecurity-magazine.com/news/nhs-ransomware-attack-goes-global/

https://www.bleepingcomputer.com/news/security/wana-decrypt0r-ransomware-using-nsa-exploit-leaked-by- shadow-brokers-is-on-a-rampage/

https://blog.malwarebytes.com/cybercrime/2017/05/wanacrypt0r-ransomware-hits-it-big-just-before-the-weekend/

https://motherboard.vice.com/en_us/article/a-massive-ransomware-explosion-is-hitting-targets-all-over-the-world

https://nakedsecurity.sophos.com/2017/05/12/wanna-decrypter-2-0-ransomware-attack-what-you-need-to-know/

http://researchcenter.paloaltonetworks.com/2017/05/palo-alto-networks-protections-wanacrypt0r-attacks/

https://arstechnica.com/security/2017/05/an-nsa-derived-ransomware-worm-is-shutting-down-computers- worldwide/

http://thehackernews.com/2017/05/wannacry-ransomware-unlock.html

https://www.theregister.co.uk/2017/05/13/wannacrypt_ransomware_worm/

https://threatpost.com/leaked-nsa-exploit-spreading-ransomware-worldwide/125654/

http://blog.trendmicro.com/trendlabs-security-intelligence/massive-wannacrywcry-ransomware-attack-hits-various- countries/

https://www.welivesecurity.com/2017/05/13/wanna-cryptor-ransomware-outbreak/

https://www.arbornetworks.com/blog/asert/wannacry/

https://twitter.com/MalwareJake/status/863263885280673792

https://gist.github.com/rain-1/989428fa5504f378b993ee6efbc0b168

http://www.bangkokpost.com/news/world/1248938/asia-assesses-ransomware-damage

https://krebsonsecurity.com/2017/05/global-wana-ransomware-outbreak-earned-perpetrators-26000-so-far/

https://www.troyhunt.com/everything-you-need-to-know-about-the-wannacrypt-ransomware/

https://labsblog.f-secure.com/2017/05/13/wcry-knowns-and-unknowns/

https://www.theguardian.com/technology/2017/may/13/accidental-hero-finds-kill-switch-to-stop-spread-of- ransomware-cyber-attack

https://www.bleepingcomputer.com/news/security/wana-decrypt0r-ransomware-outbreak-temporarily-stopped-by- accidental-hero-/

http://news.softpedia.com/news/wannacry-ransomware-spread-halted-by-hero-researcher-515690.shtml

https://securingtomorrow.mcafee.com/executive-perspectives/wannacry-old-worms-new/

http://www.mailguard.com.au/blog/global-cyber-attack-wannacry-ransomware-creates-havoc

http://www.darkreading.com/partner-perspectives/malwarebytes/wanacrypt0r-hits-worldwide-/a/d-id/1328876

https://www.itnews.com.au/news/british-hospitals-telefonica-hit-by-ransomware-with-nsa-exploit-461566

http://money.cnn.com/2017/05/12/technology/ransomware-attack-nsa-microsoft/index.html

https://www.helpnetsecurity.com/2017/05/12/massive-ransomware-campaign/

https://blog.fox-it.com/2017/05/13/faq-on-the-wanacry-ransomware-outbreak/

https://www.itnews.com.au/news/wannacrypt-ransomware-what-you-need-to-know-461717

https://www.bleepingcomputer.com/news/security/honeypot-server-gets-infected-with-wannacry-ransomware-6- times-in-90-minutes/

https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware

https://nakedsecurity.sophos.com/2017/05/14/wannacry-benefits-from-unlearned-lessons-of-slammer-conficker/

https://www.bleepingcomputer.com/news/government/microsoft-exec-blames-wannacry-ransomware-on-nsa- vulnerability-hoarding-program/

http://blog.trendmicro.com/wannacry-reality-of-patching/

https://www.helpnetsecurity.com/2017/05/14/wannacry-ransomware/

https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

https://krebsonsecurity.com/2017/05/microsoft-issues-wanacrypt-patch-for-windows-8-xp/

http://www.csoonline.com/article/3196725/security/microsoft-patches-windows-xp-and-server-2003-due-to- wannacrypt-attacks.html

https://www.infosecurity-magazine.com/news/microsoft-xp-patch-wannacry/

https://www.itnews.com.au/news/microsoft-releases-wannacrypt-patch-for-windows-xp-server-2003-461640

https://www.bleepingcomputer.com/news/security/microsoft-releases-patch-for-older-windows-versions-to-protect- against-wana-decrypt0r/

https://arstechnica.com/security/2017/05/wcry-is-so-mean-microsoft-issues-patch-for-3-unsupported-windows- versions/

http://thehackernews.com/2017/05/wannacry-ransomware-windows.html

https://threatpost.com/microsoft-releases-xp-patch-for-wannacry-ransomware/125671/

http://thehackernews.com/2017/05/wannacry-ransomware-cyber-attack.html

https://www.ncsc.gov.uk/guidance/ransomware-latest-ncsc-guidance

https://motherboard.vice.com/en_us/article/round-two-wannacry-ransomware-that-struck-the-globe-is-back

https://twitter.com/craiu/status/863718940870139904

http://news.softpedia.com/news/wannacry-ransomware-variant-with-no-kill-switch-discovered-515693.shtml

https://www.renditioninfosec.com/2017/05/wanacrypt0r-worm-with-kill-switch-patched-out/

https://www.bleepingcomputer.com/news/security/with-the-success-of-wannacry-imitations-are-quickly-in- development/

http://blog.checkpoint.com/2017/05/14/wannacry-paid-time-off/

The Computer Emergency Response Team of Mauritius (CERT-MU)

National Computer Board
7th Floor, Stratton Court,
La Poudriere Street, Port Louis

Tel: 210 5520
Fax: 208 0119

Website: www.cert-mu.org.mu

Incident Reporting
Hotline: 800 2378
Email: incident@cert.ncb.mu

Vulnerability Reporting
Email: vulnerability@cert.ncb.mu

For Queries
Email: contact@cert.ncb.mu

Subscription to Mailing Lists
Email: subscribe@cert.ncb.mu