WannaCry ransomware that infected Telefonica and NHS hospitals is spreading aggressively, with over 50,000 attacks so far today

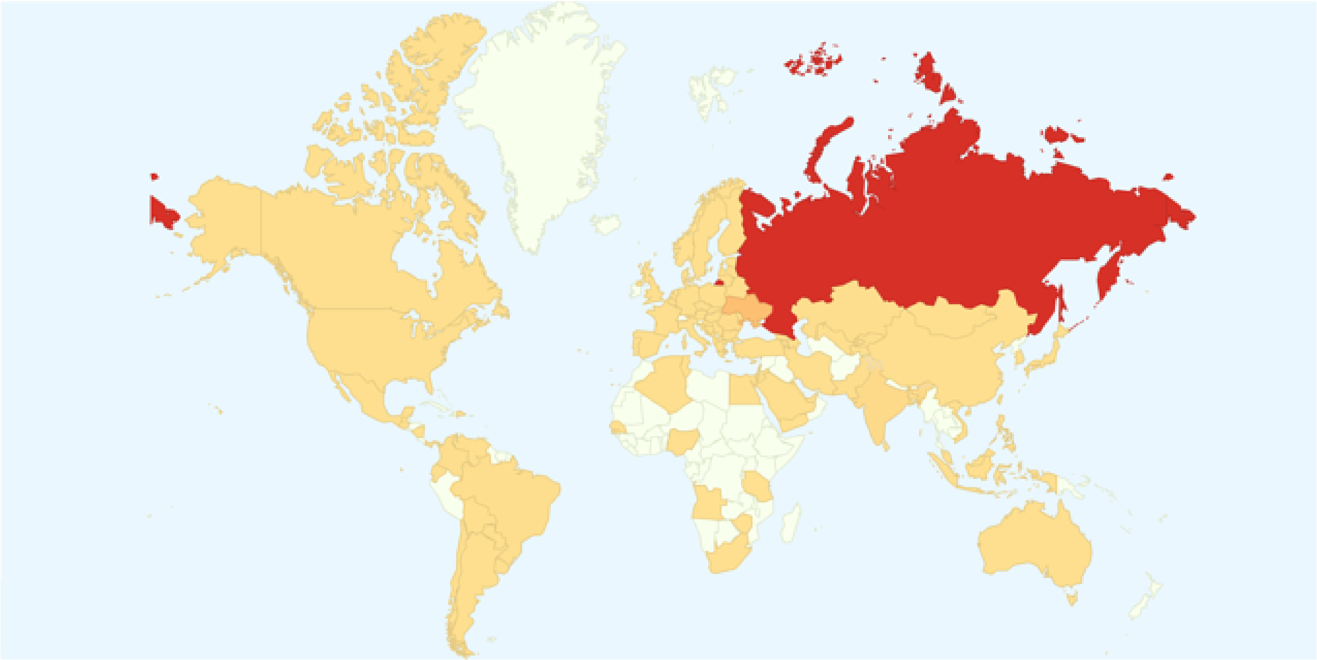
blog.avast.com/ransomware-that-infected-telefonica-and-nhs-hospitals-is-spreading-aggressively-with-over-50000-attacks-so-far-today

Avast protects you from WannaCry ransomware that infected NHS and Telefonica.

Update (4:23 CET, Monday, May 15th): We are now seeing more than 213,000 detections of WannaCry, in 112 countries.

We have observed a massive peak in WannaCry (aka WCry) ransomware attacks today, with more than 57,000 detections, so far. According to our data, the ransomware is mainly being targeted to Russia, Ukraine and Taiwan, but the ransomware has successfully infected major institutions, like hospitals across England and Spanish telecommunications company, Telefonica.

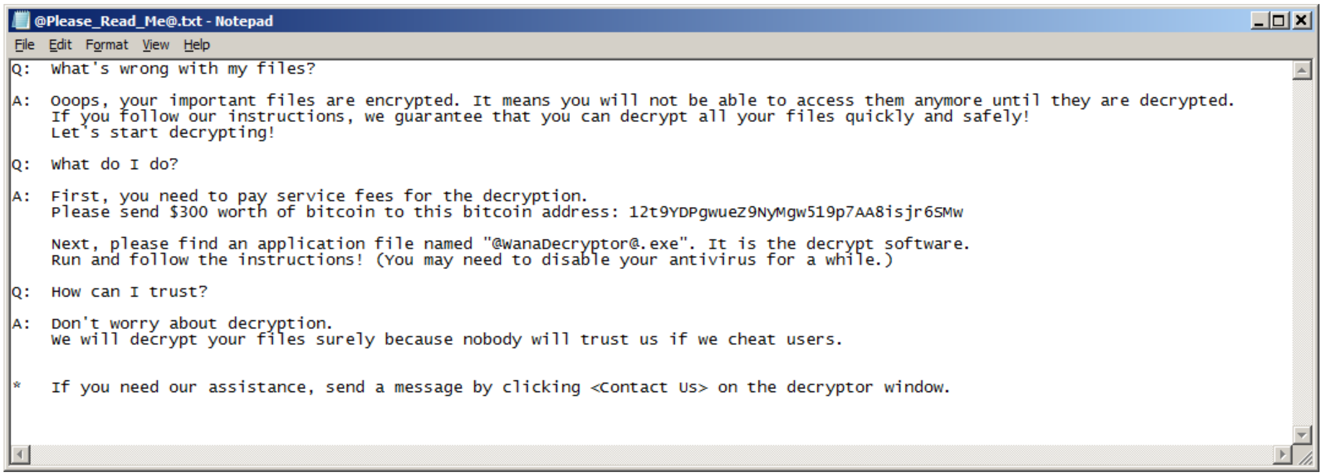
Below is a map showing the countries being targeted most by WannaCry:



We saw the first version of WannaCry in February and now the ransomware is available in 28 different languages, from languages like Bulgarian to Vietnamese. Today at 8 am CET, we noticed an increase in activity of this strain, which quickly escalated into a massive spreading, beginning at 10 am.

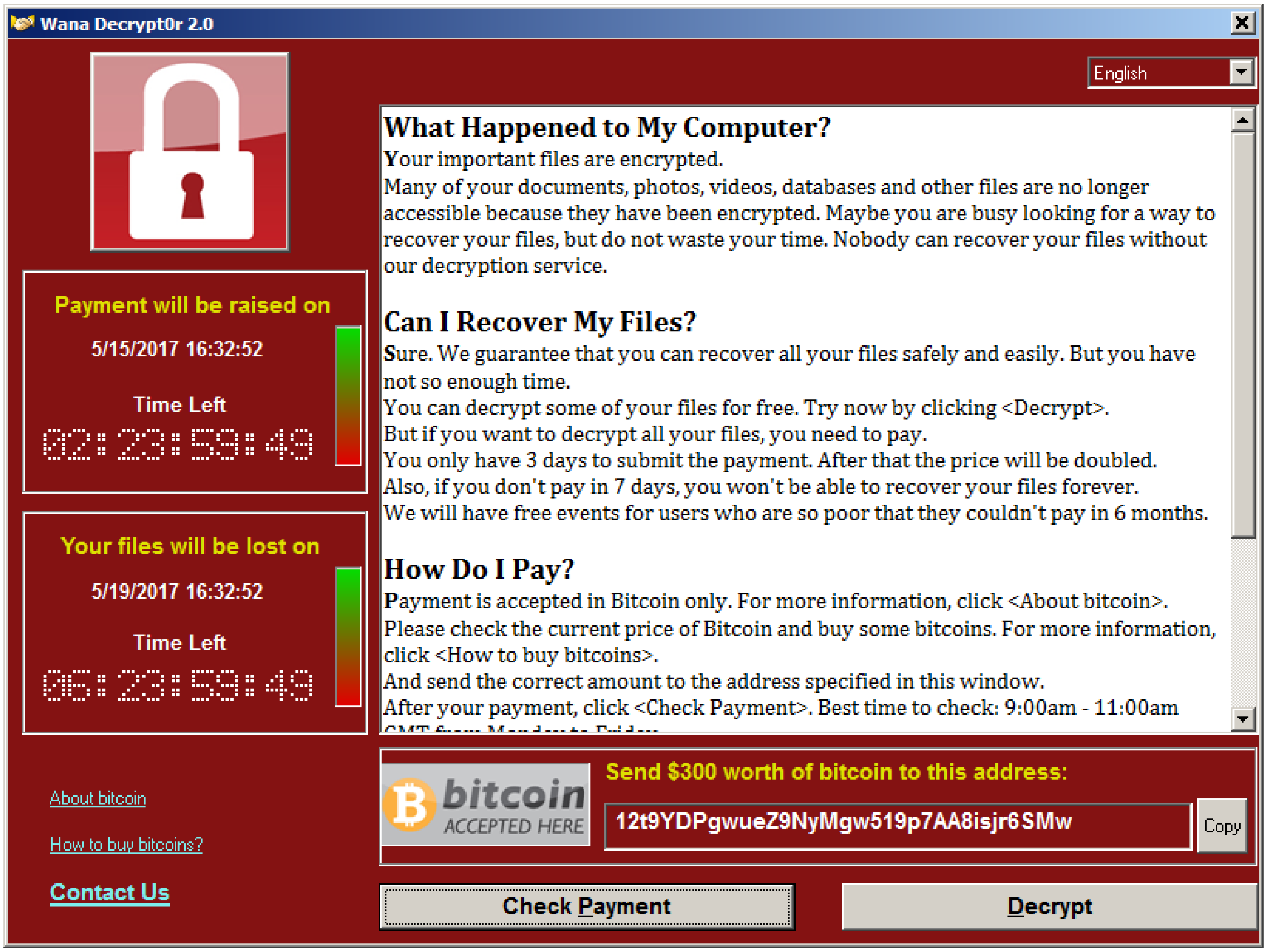
The ransomware changes the affected file extension names to ".WNCRY", so an infected file will look something like: *original_name_of_file.jpg.WNCRY,* for example. The encrypted files are also marked by the "WANACRY!" string at the beginning of the file.

This ransomware drops the following ransom notes in a text file:



```
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.
```

Furthermore, the ransom being demanded is $300 worth of bitcoins. The ransom message, where instructions on how to pay the ransom, an explanation of what happened, and a countdown timer are displayed in what the cybercriminals behind the ransomware are referring to as "Wana Decrypt0r 2.0":



Payment will be raised on

5/15/2017 16:32:52

Time Left

02:23:59:49

Your files will be lost on

5/19/2017 16:32:52

Time Left

06:23:59:49

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.

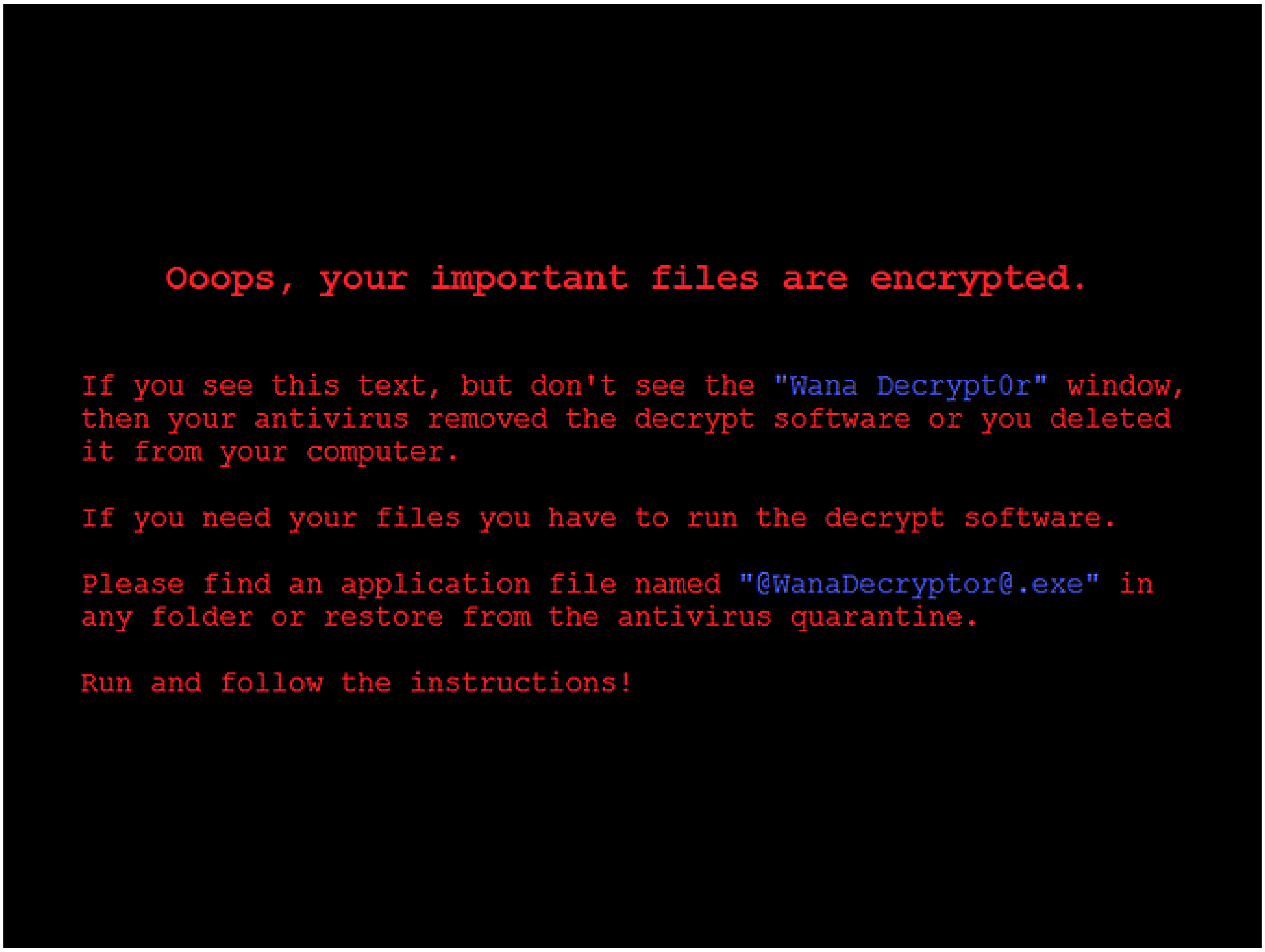
How Do I Pay?

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.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Additionally, the victim’s wallpaper is changed to the following image:



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!

This attack once again proves that ransomware is a powerful weapon that can be used against consumers and businesses alike. Ransomware becomes particularly nasty when it infects institutions like hospitals, where it can put people's lives in danger.

Infection vector: WannaCry

WannaCry is most likely spreading on so many computers by using an exploit the Equation Group, which is a group that is widely suspected of being tied to the NSA, used for its dirty business. A hacker group called ShadowBrokers has stolen Equation Group's hacking tools and has publicly released them. As confirmed by security researcher, Kafeine, the exploit, known as ETERNALBLUE or MS17-010, was probably used by the cybercriminals behind WannaCry and is a Windows SMB (Server Message Block, a network file sharing protocol) vulnerability.

Avast antivirus detects all known versions of WannaCry, but we strongly recommend all Windows users fully update their system with the latest available patches. We will continue to monitor this outbreak and update this blog post when we have further updates.

IOCs:

09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa

24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c

2584e1521065e45ec3c17767c065429038fc6291c091097ea8b22c8a502c41dd

2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d

4A468603FDCB7A2EB5770705898CF9EF37AADE532A7964642ECD705A74794B79

B9C5D4339809E0AD9A00D4D3DD26FDF44A32819A54ABF846BB9B560D81391C25

d8a9879a99ac7b12e63e6bcae7f965fbf1b63d892a8649ab1d6b08ce711f7127

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa

f8812f1deb8001f3b7672b6fc85640ecb123bc2304b563728e6235ccbe782d85