

Things you should know about WannaCry (Cyber Attack)

A motion-blog by

i⇨engage



WannaCry 2.0

Here are the
things you should
now about
“Ransomware
Attack”.

WannaCry ransomware attack is an ongoing cyber attack worldwide. It is a computer worm, targeting Windows OS and demanding ransom payments in Bitcoins.





What's happening?

1

“Ransomware”, encrypting files and demanding \$300 – \$1200 from the victim in order to regain access to the files on his or her computer.



2

It encrypts most or even all of the files on a user's computer.



3

There are over 200,000 victims and more than 230,000 computers infected in over 150 countries.

4

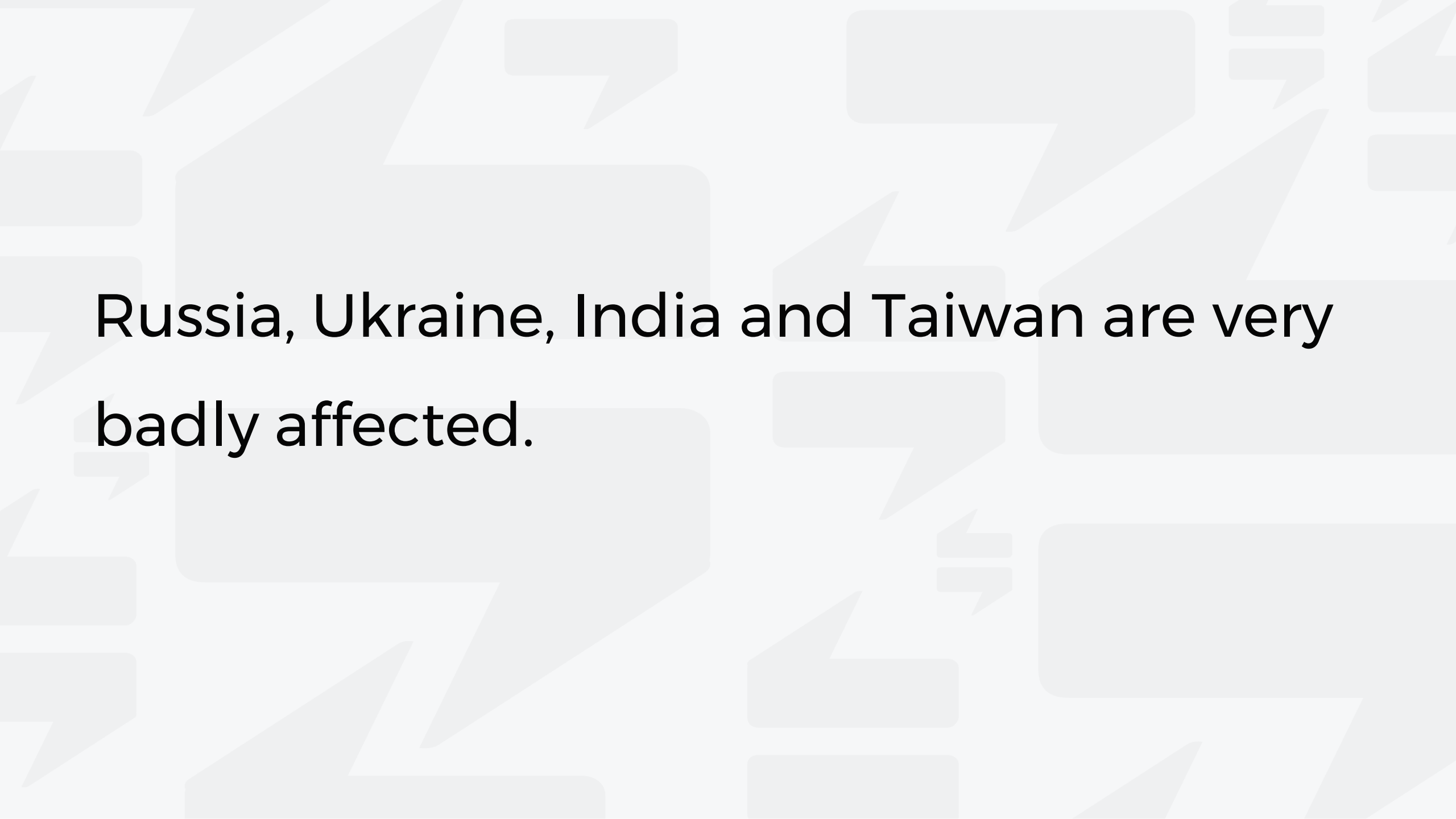
A blogger flipped an kill switch by registering a domain name he found in the code of the ransomware, this slowed the spread of infection.

How Ransomware was created?

WannaCry used the EternalBlue exploit & DoublePulsar backdoor developed by the U.S. National Security Agency (NSA) to spread through local networks.



Effects of “Ransomware”?



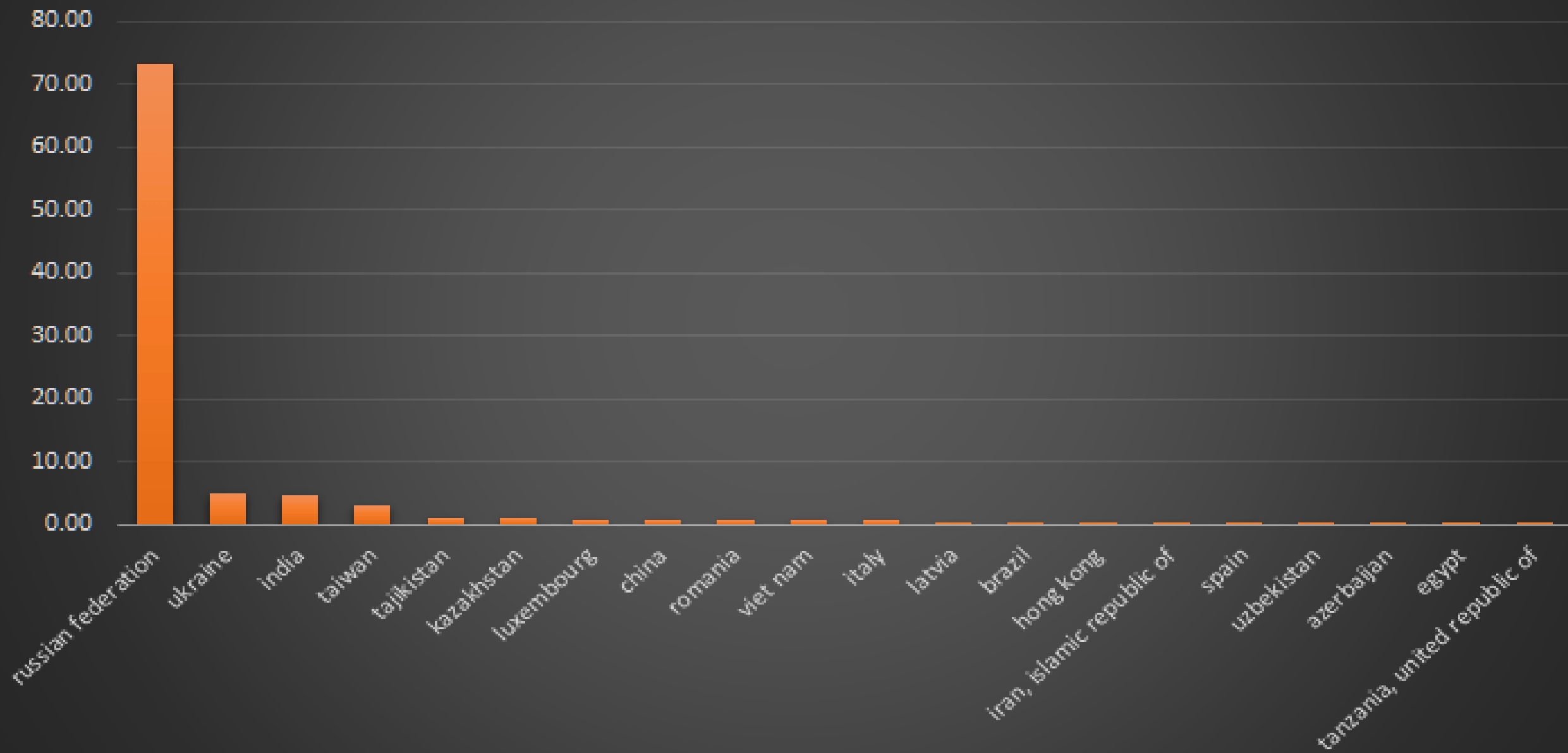
Russia, Ukraine, India and Taiwan are very badly affected.

The attack affected working of computers, MRI scanners, blood-storage refrigerators and theatre equipment.

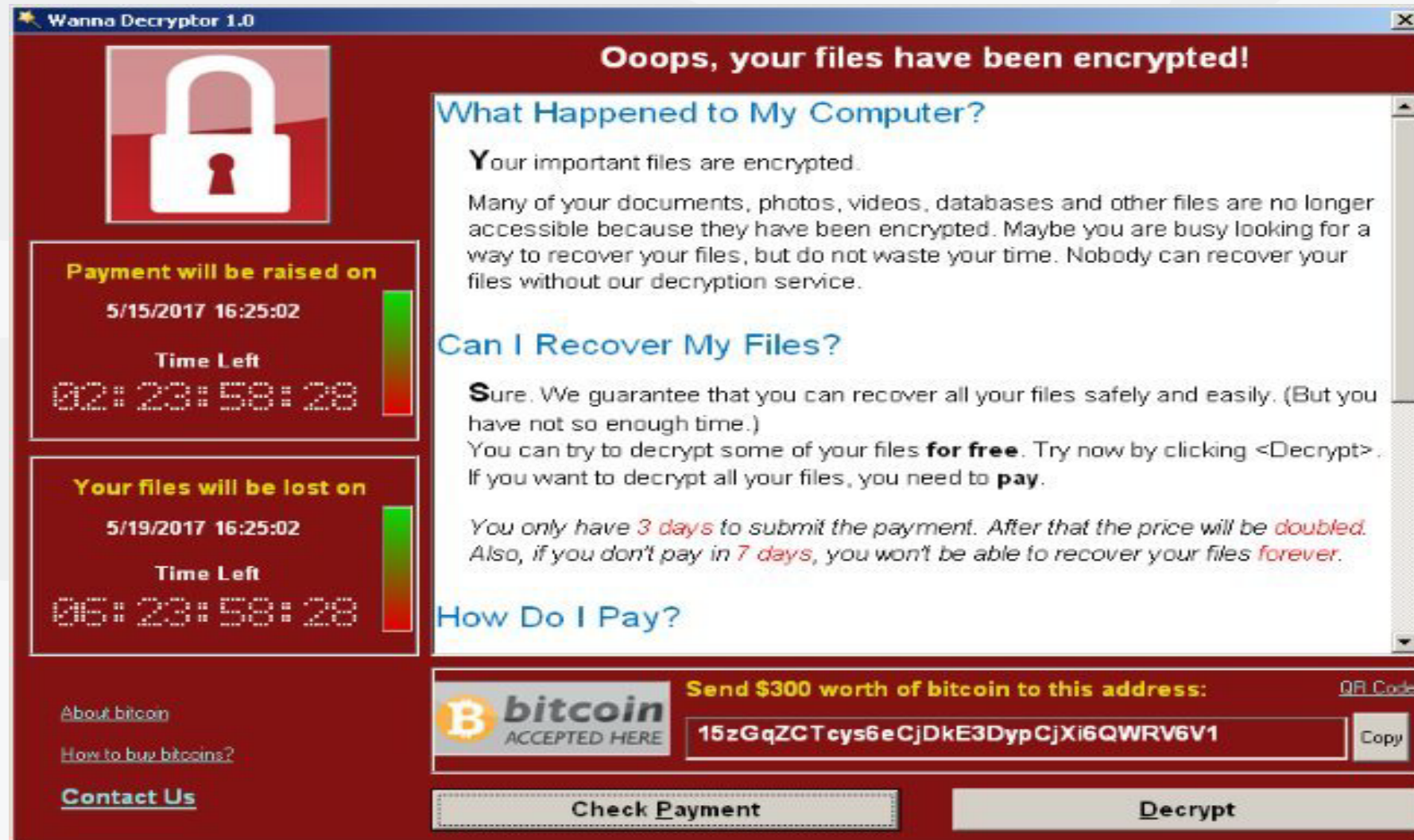
Business of several large companies closed
& Banks, Hospitals, and Other Government
Agencies were also very badly affected.

WannaCry Ransomware

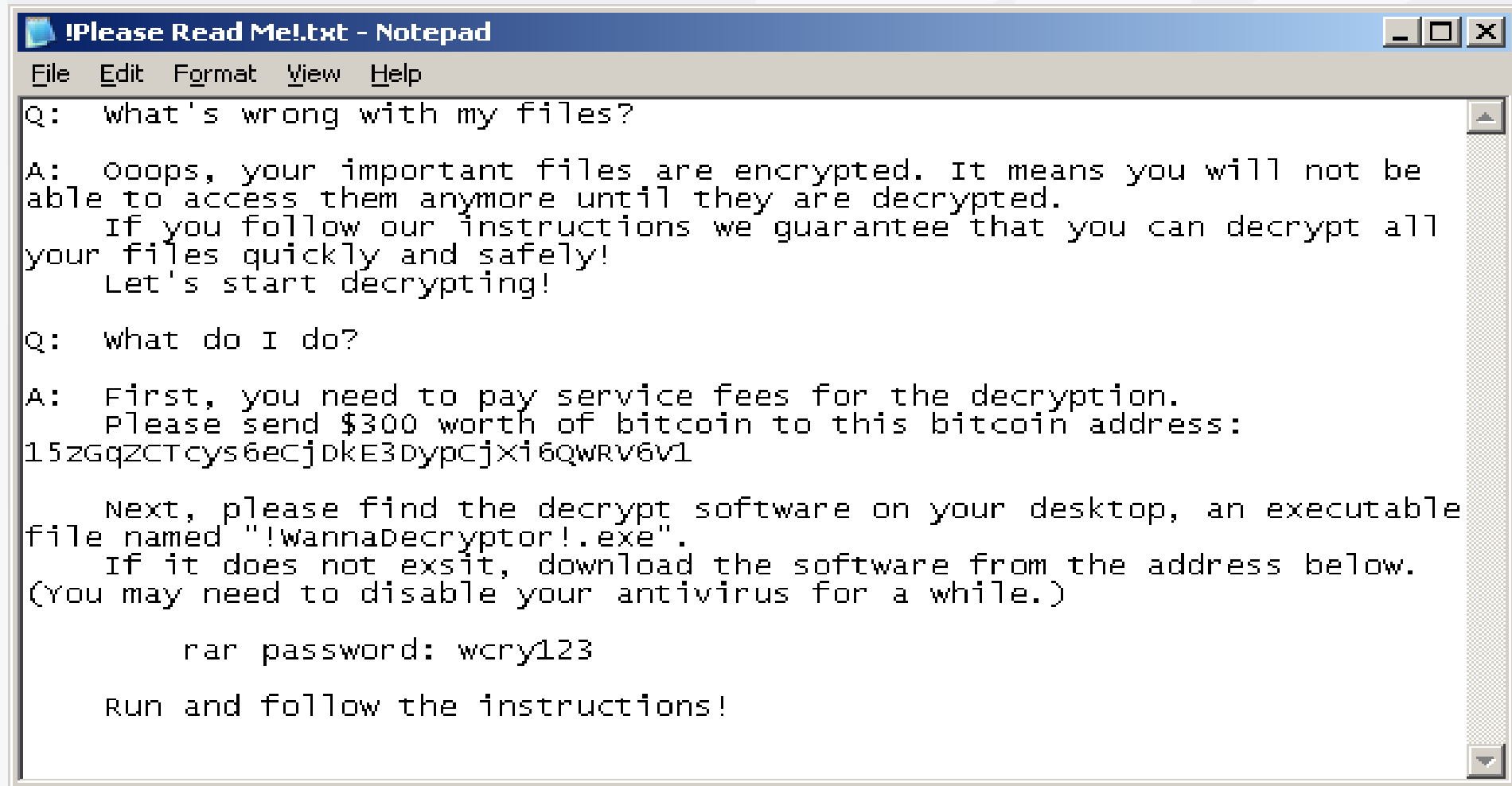
Attack distribution by country - top 20



Computer Screen after Ransomware Virus attack.



It also installs a text file with the following note:



```
!Please Read Me!.txt - Notepad
File Edit Format View Help
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:
    15zGqZCTcys6ecjDkE3DypcjXi6QWRV6v1
    Next, please find the decrypt software on your desktop, an executable
    file named "!wannadecryptor!.exe".
    If it does not exist, download the software from the address below.
    (You may need to disable your antivirus for a while.)
    rar password: wcry123
    Run and follow the instructions!
```

How to protect your computer from ransomware:

- Run windows update regularly.
- Install latest antivirus update of Microsoft.
- Back up your data.
- Be careful what you open.

Share this video to let everyone know about it

Connect with us on



/iengageonline

or visit

www.i-engage.in