

Date: 13-05-2017

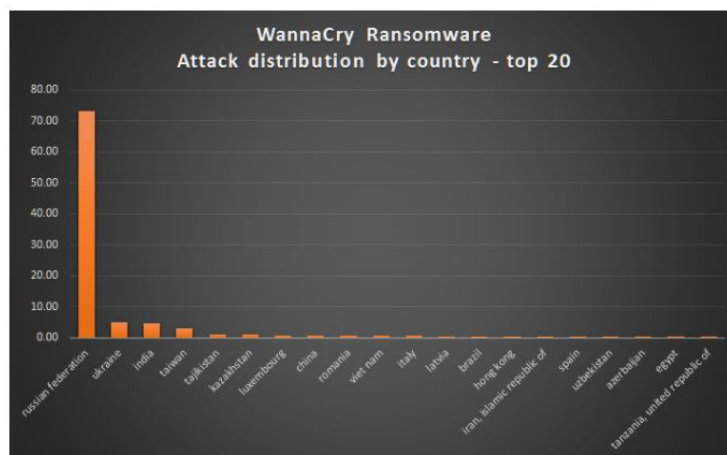
## Brief Description: WannaCry Ransomware

A large number of ransomware attacks have been reported around the world. In these attacks, data is encrypted with the extension “.WCRY” added to the filenames.

The attack, dubbed “WannaCry”, is initiated through an SMBv2 remote code execution in Microsoft Windows. This exploit (codenamed “EternalBlue”) has been made available on the internet through the Shadowbrokers dump of the tools, used by the USA’s National Security Agency, on April 14th, 2017 and patched by Microsoft on March 14.

The attack is targeting organisations that have not yet installed the patch. (MS17-010)

Kaspersky has recorded more than 45,000 attacks of the WannaCry ransomware in 74 countries around the world. The top three countries being Russia, Ukraine and India.



## Affected Systems:

The ransomware affects systems running Microsoft Windows.

## Severity:

WannaCry encrypts data files and ask users to pay a US\$300 ransom in bitcoins. The ransom note indicates that the payment amount will be doubled after three days. If payment is not made after seven days, the encrypted files will be deleted.

## What needs to be done:

1. Install the official patch ([MS17-010](#)) from Microsoft as applicable, which closes the affected SMB Server vulnerability used in this attack.
2. Update your Anti-Virus/IPS/IDS signatures as most of them can detect and prevent the malware.

## How does it spread?

It spreads via compromised email and affected websites. There is still no clarity on this. However, we assume it would be through spear phishing and phishing emails + compromised websites.

Reference:

[Kaspersky](#)

[Symantec](#)

Login Register Subscribe Rewards Search Video

## The Telegraph

ALL SECTIONS

PREMIUM | NEWS | SPORT | BUSINESS | MONEY | OPINION | TECH & SCIENCE | CULTURE | TRAVEL | LIFESTYLE

### NHS CYBER ATTACK

# Government under pressure after NHS crippled in cyber attack as weekend of chaos looms

- ♦ Operations cancelled and some trusts telling patients not to come to A&E
- ♦ Nearly 100 countries hit in 'biggest attack in history'
- ♦ Russia's interior ministry and Germany's Deutsche Bahn affected

<http://www.telegraph.co.uk/news/2017/05/12/nhs-hit-major-cyber-attack-hackers-demanding-ransom/>

[https://en.wikipedia.org/wiki/WannaCry\\_ransomware\\_attack](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack)

<https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/>