

Since Friday 12<sup>th</sup> May 2017,  150 countries and 200,000 victims, including NHS, have been affected by “WannaCry” ransomware. Source: BBC News

# RANSOMWARE



Ransomware is a malicious software that encrypts your files or devices, limiting the access to your files and devices. It then forces you to pay ransom to regain access to your files and devices.

## CAN I SEE AN EXAMPLE?



## How your device gets infected?



**MALICIOUS WEBSITE** that is distributing malware or a website that has been compromised.



**EMAIL ATTACHMENT** that downloads and deploys ransomware onto your device once you have opened it.



**FILES SHARED ON THE CLOUD AND USB STICKS** when opened, then the ransomware will automatically install on your device.



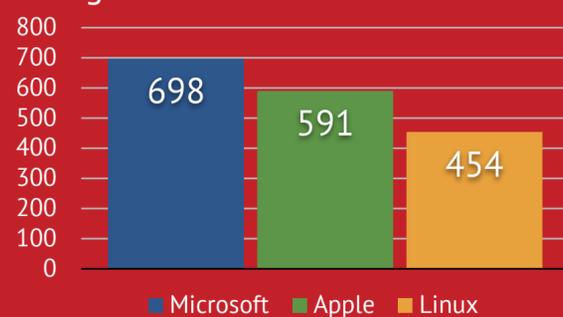
**OTHER SOFTWARE** that has been modified by criminals to distribute ransomware.



**MALICIOUS WEBLINKS** that are usually sent via emails, SMS, social media posts and chats, directing you to a malicious website.

**I DON'T USE WINDOWS, WILL I NEED TO BE CONCERNED?**

**YES.** Although the majority of ransomware happens on Microsoft Windows operating systems (OS), this doesn't mean Apple OSX, iOS, Linux and Android devices are not affected. Some ransomware encrypt only files and therefore device types and OS are secondary. This year, Microsoft and Apple was on the top of the list in the number of software vulnerabilities. Criminals can use these software bugs as their avenue to attack us.



Source: CVE Details

## REMEMBER TO

**REGULARLY BACKUP YOUR FILES** and test it if the backup is not managed by IT Services

**UPDATE YOUR SOFTWARE EARLY AND OFTEN** if IT Services is not managing your devices

**ENCRYPT YOUR DEVICES** if you have not done so yet; otherwise contact IT Services

**REPORT SUSPICIOUS LINKS AND ATTACHMENTS** to IT Services

**CONTACT IT SERVICES** if you suspect an infection on your devices

**NEVER PAY ANY RANSOM;** ask IT Services if your devices/files are infected