*A case story on WannaCry:-*

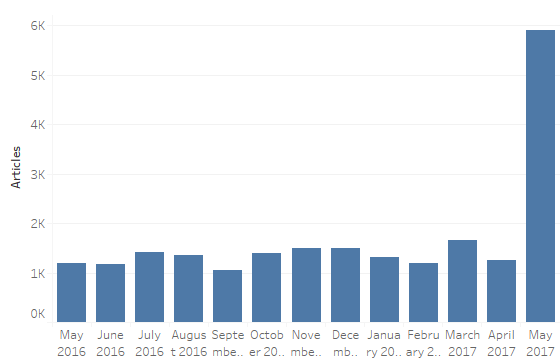
The WannaCry ransomware attack was a May 2017 worldwide cyberattack by the WannaCryransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.

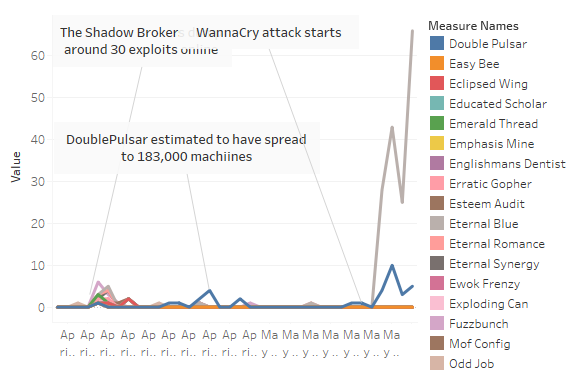
**What is a ransomware**Ransomware is a type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

**Attack Summary**  
At 8am CET on Friday May 12th, the WannaCry attack began, and by that evening it had infected over 50,000 machines in 70 countries. By the following Monday, that had risen to 213,000 infections, paralyzing computer systems in hospitals, factories, and transport networks as well as personal devices. WannaCry is a ransomware virus – it encrypts all of the data on computers it infects, with users only having their data decrypted after they had paid 300 or 600 ransom to the hackers. Users who have had their device infected can only see the screen below until they have paid the ransom.

**The Tale of Vulnerability**

* The attack was enabled by tools that exploit security vulnerabilities called DoublePulsar and EternalBlue of Windows' Server Message Block (SMB) protocol.
  + SMB:-In computer networking, Server Message Block (SMB), one version of which was also known as Common Internet File System (CIFS) operates as an application-layer network protocol mainly used for providing shared access to files, printers, and serial ports and miscellaneous communications between nodes on a network.
* These tools EternalBlue essentially allow someone to access every file on your computer by avoiding the security built into your operating system.
* The vulnerabilities were originally discovered by the *National Security Agency* (NSA) in the US, but were leaked by a hacker group called *The Shadow Brokers* on 8 April 2017, along with other tools apparently leaked from Equation Group.
* Microsoft eventually discovered the vulnerability, and on Tuesday, March 14, 2017, and announced that patches had been released for all Windows versions.
* Supported Operating System:
  + Windows 7, 8.1, 10
  + Windows Server 2008, 2012, 2016
  + Windows Vista
  + Windows XP
* However, many Windows users had not installed the patches when, two months later on May 12, 2017, WannaCry used the EternalBlue vulnerability to spread itself.

  
 Monthly count of articles mentioning “malware” or “ransomware” over the last 12 months  
 *Source:- blog.aylien.com/media-monitoring-case-study-wannacry-malware-attack/*

  
 Mentions of each of the exploit tools dumped in April and May *Source:- blog.aylien.com/media-monitoring-case-study-wannacry-malware-attack/*

**The Attack**



Fig: WannaCry Traditional Payload screen

On 12 May 2017, WannaCry began affecting computers worldwide, with evidence pointing to an initial infection in Asia at 7:44am. The initial infection was likely through an exposed vulnerable SMB port rather than email phishing as initially assumed.

* When executed, the malware first checks the "kill switch" domain name.
* If it is not found, then the ransomware encrypts the computer's data.
* Then attempts to exploit the SMB vulnerability to spread out to random computers on the Internet and "laterally" to computers on the same network.
* As with other modern ransomware, the payload displays a message informing the user that files have been encrypted, and demands a payment of around $300 in bitcoin within three days, or $600 within seven days.
* Three hardcoded bitcoin addresses, or "wallets", are used to receive the payments of victims.
* AKA Ransom.Wannacry, Ransom.CryptXXX, Trojan/Win32.WannaCryptor