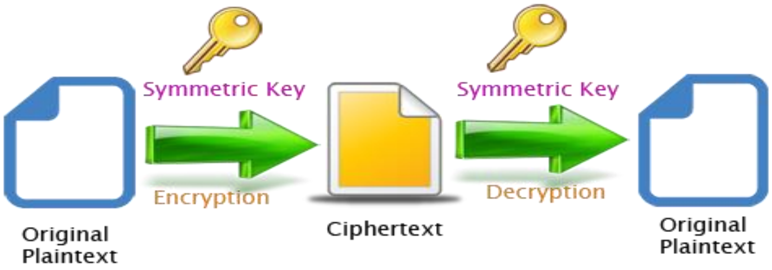
RANSOMWARE

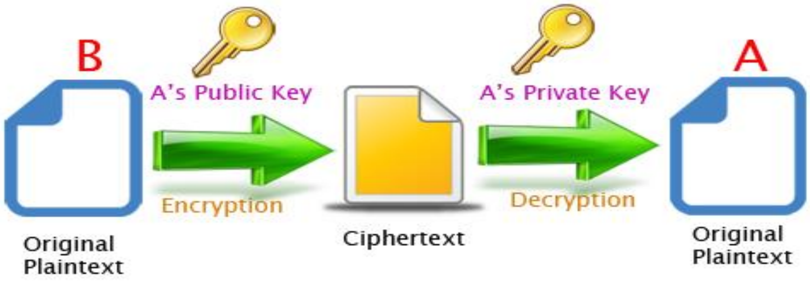
Ransomware is the malicious software which encrypts all the files in your computer. It leaves a message demanding money to decrypt all the files and warns the users that the files would be deleted if the ransom is not paid. The method of downloading the software on the user's computer varies greatly but the virus is usually sent as an attachment through email. The integral part of any ransomware attack is encryption. There are two types of encryption: (1) Symmetric and (2) Asymmetric.

AES (Advanced Encryption Standard) uses symmetric keys. It uses the same key to encrypt and decrypt data. The image for symmetric cryptography is shown below:



An example of symmetric cryptography is the very first ransomware: "PC Cyborg" created in 1989 by Harvard biologist Dr. Joseph L. Popp. He used very primitive method of distributed which was 20,000 floppy disks. This ransomware infected the computer by modifying the AUTOEXEC.BAT file. This file stores the information of how and where to load operating system from. The infection encrypted all the files and hid the directories after 90 reboots. The biggest drawback of this ransomware was that it used symmetric cryptography. The keys for decryption could be obtained from the Trojan virus itself. The universal decryption key for the virus was made available soon which made the virus very ineffective.

Asymmetric encryption is called RSA after Ron Rivest, Adi Shamir and Leonard Aldeman who made this algorithm in 1978. This encryption uses two different keys for encryption and decryption. It uses a public key which everyone has access to for encrypting the data. It uses private key which only a specific person or organization has access to for decrypting the data. The image for asymmetric cryptography is shown below:



An example of this kind of encryption would be WannaCry. It was the worst ransomware attack up to date. It infected over 230,000 computers in 150 countries using 20 different languages to demand $300 for decryption from users using Bitcoin cryptocurrency.

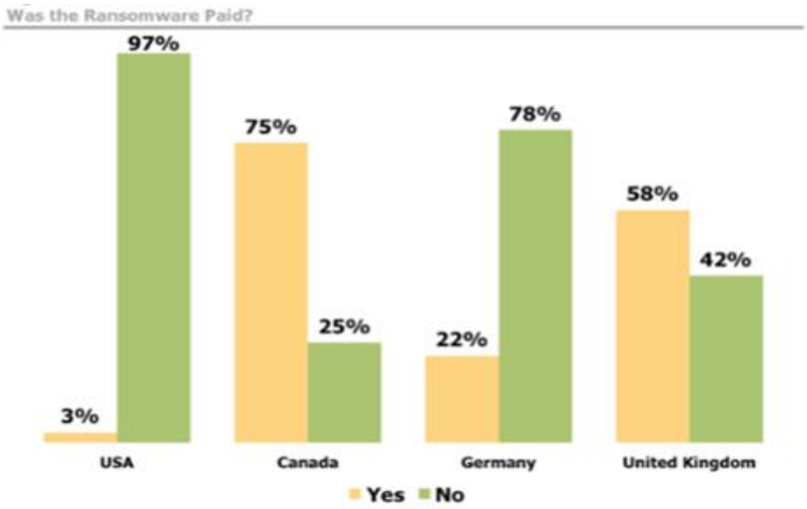
WannaCry used an exploit vector named EternalBlue. It was developed by U.S. National Security Agency (NSA) and leaked by Shadow Brokers Hacker group. EternalBlue exploited a vulnerability in Microsoft's Server Message Block (SMB) protocol. The vulnerability exists because the SMB version 1 (SMBv1) server in various versions of Microsoft Windows mishandles specially crafted packets from remote attackers, allowing them to execute arbitrary code on the target computer. EternalBlue has 7 exploits, whereas WannaCry only has 2 exploits and is equipped with a kill switch. EternalBlue is considered to be deadlier than WannaCry. The NSA eventually warned Microsoft after learning about EternalBlue's possible theft. The company prepared a software patch issued in March 2017, after cancelling all security patches in February 2017. On Tuesday, March 14, 2017, Microsoft issued security bulletin MS17-010, which detailed the flaw and announced that patches had been released for all Windows versions. However, two months later on May 12, 2017, when the WannaCry attacked, most window users had not installed the patches which made the windows computers vulnerable to the ransomware attack. The day after the attack, Microsoft released emergency security patches for Windows.

There are two types of ransomware in trend: Crypto Ransomware and Locker Ransomware. Crypto Ransomware searches for all the valuable files and encrypts them. It only shows the malware message once the data is encrypted. Until then, it stays low. It uses RSA-2048 encryption: asymmetric cryptography. Locker Ransomware tracks the geographical location of victim and shows a fake notice from the law enforcement agency of that country to pay fine for getting caught in an illegal activity online. Initial versions of this malware only locked the computer. So, if the malware is removed, user do not have to pay the ransom. Because of this property, the newer versions of this malware lock the computer and then encrypt files. This ransomware uses ECC (Elliptic Curve Cryptography) RSA + AES encryption. AES key is used to encrypt files. This key is encrypted with a RSA public key embedded in the malware, which requires a private key to decrypt it.

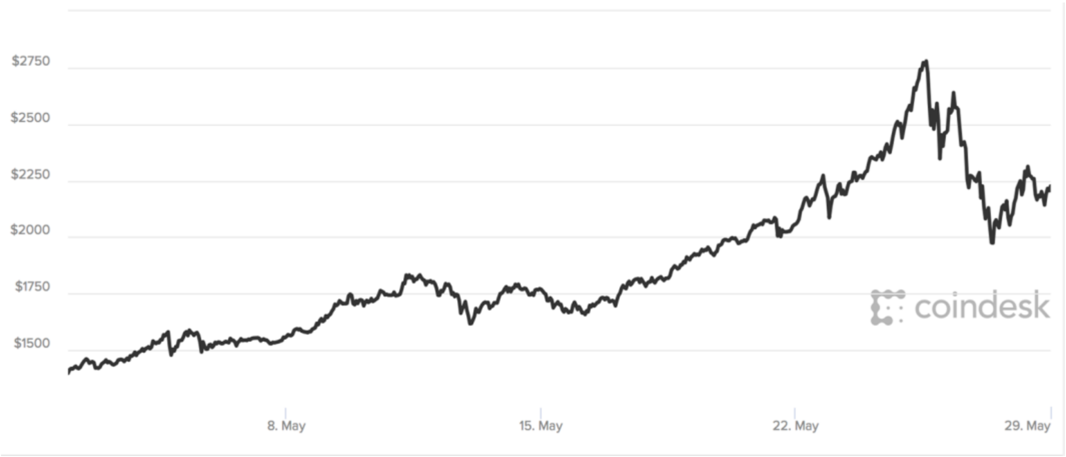
Many tech companies like Symantec and MalwareBytes are funding the research reports to gain better understanding of how virus spreads, patch their software before it goes viral and prevent their customers from becoming victims. Companies are developing software like CryptoDrop. CryptoDrop is not designed to replace the current anti-malware software on the computer but to halt processes even when anti-virus software fails. CryptoDrop is an early detection system. It alerts users about any suspicious file activity and halts any process that appears to be tampering with the user's data. By combining a set of indicators common to ransomware, the system can be parameterized for rapid detection with low false positives. Experimental analysis of CryptoDrop suggests that it can stop ransomware from executing with a median loss of only 10 files (out of nearly 5,100 available files). Careful analysis of ransomware behavior can produce an effective detection system that significantly mitigates the amount of victim data loss.

There are three main Indicators for CryptoDrop: a) File Type changes, b) Similarity Measurement and c) Shannon Entropy. Similarity measurement of any suspected file is done by testing it against 492 real-world ransomware samples. Shannon's Entropy would be large for a zipped file or an encrypted file. Shannon entropy could be used to check if the file is being encrypted or is already encrypted. This is the first ransomware detection system that monitors user data for changes that may indicate transformation rather than attempting to identify ransomware by inspecting its execution (e.g., API call monitoring) or contents. This allows CryptoDrop to detect suspicious activity regardless of the delivery mechanism or previous benign activity

Ransomware attacks globally impacts businesses, cryptocurrencies and the rate of attacks. Different trends have been observed because of the attacks. Due to the successes of the recent ransomware attacks, targeted attacks on the businesses are becoming more frequent. Every 10 seconds, a consumer gets hit with ransomware which was 20 seconds in 2016. Every 40 seconds, a company gets hit with ransomware which was 2 minutes in 2016. Phishing email attachments have become the #1 delivery vehicle for ransomware. Successful ransomware attacks have served as a motivation and new ransomware variants are being churned out at an alarming rate. The number of ransomware variants grew by a factor of 30x in 2016. Nearly 3/4 of organizations targeted by ransomware attacks don't have security in place that can prevent infection. The bar graph below shows the statistics of whether the ransom paid by different countries.



BitCoin is the usually preferred ransom currency as it provides anonymity and has a faint money trail. As soon as any ransomware hits, there is an increase in the purchase of BitCoins by the victims and companies which start stockpiling Bitcoins for future ransom. This boasts the price of the BitCoin significantly. Drop in the price of the BitCoins is observed as the attack ends. The graph below shows the increase in the price of a Bitcoin when WannaCry hit and the decline in the price after the attack ended.



There are some measures that can be taken to prevent the computer from being infected. Back up the data. Apply patches and keep the operating system, antivirus, browsers, Adobe Flash Player, Java, and other software up-to-date. Keep the Windows Firewall turned on and properly configured at all times. Use System Restore to get back to a known-clean state. Switch off unused wireless connections, such as Bluetooth or infrared ports. Do not visit unsafe and unreliable websites. Rather than clicking any web links, type out web address on address bar.

References

https://www.citrix.com/blogs/2018/01/31/on-the-origin-of-ransomware-species/

https://www.techrepublic.com/article/why-ransomware-attacks-are-making-bitcoin-more-expensive-for-everyone/

https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf

A brief study of Wannacry Threat: Ransomware Attack 2017 – IJARCS:
http://ijarcs.info/index.php/Ijarcs/article/download/4021/3642

https://www.cise.ufl.edu/~traynor/papers/scaife-icdcs16.pdf