1.WANNACRY:

Is a type of ransomware that’s spreads rapidly through across a number of computer networks. It was discovered in May 2017. After affecting, it encrypts folders on the computer’s hard drive targets computer running on Microsoft windows operating systems. Affected people usually pay through crypto currency (bitcoins). The exploit came through the Eternal Blue which was stolen and leaked by the shadow brokers a few months before the attack. Microsoft released patches to fix the exploits, but older versions were affected. WannaCry also took advantage of installing back doors on infected systems. In December 2017, the united states of America, United Kingdom, and Australlia realized it was North Korea behind the attack. The attack has estimated to have affected over 200,000 computers across 150 countries.

2.**EMOTET:**

Is a banking trojan designed to steal sensitive information from the banks. Sometimes designed to spread through emails spams. Identified in 2014, Emotet uses worm like capabilities to spread through connected computers. Emotet uses functionality that helps the software evade detection by some anti-malware products. The infection may arrive either via malicious script, macro-enabled document files, or malicious link. Emotet emails may contain familiar branding designed to look like a legitimate email (PHISHING EMAILS). It uses C&C server to receive updates. This works in the same way as the operating system updates on the computer. The primary distribution of Emotet is through malspam and uses brute force attack to crack protected files.

3.**GRANDCRAB:**

This is a type of malware that also encrypts important files and asks for a ransom to decrypt the files first. They work on all target windows systems. They provide you with ransom notes. They have extensions and these are examples: **gdcb.extentions** and **krab.extentions.** They hold important files on infected systems hostage unless and until the victims agree to pay the agreed sum demanded. Early 2018 by experts in cyber security firm **LMNTRIX** discovered the grandcrab malware. They announced themselves on 31 may 2019 after $2 billion dollars was made.

4.**GARB:**

A philosophy and malware campaign active since September 12th targeting individuals as well as financial organizations to steal important information. Domain has now been disabled. The campaign involves fake emails posing to be sent from Indian Income Tax Department (PHISHING EMAILS). A government cybersecurity agency has issued a warning to the taxpayers that an information-stealing computer malware under the garb of a message from the Income Tax Department. The lastest observations of the malware emails usually looks like ‘an attachment with extension “.img” which contains a malicious “.pif” file while the second variant lures the users to download a malicious ".pif” file hosted on a sharepoint page via a link of fraudulent domain incometaxindia. Counter measures have been put in place teaching educating workers on phishing and spam emails and teaching them things to look out when they receive such email.

5.**TRICKBOT:**

Trickbot is a type of banking trojan designed and targets users financial information and acts as a dropper for other malware uses in man in the browsers attacks to steal information such as login credentials and online banking information such as credit card details. Trickbot was developed in 2016 inspired by Dyreza (another banking trojan). Crypto currency is demanded as ransom sometimes after these information have been hijacked. It can spread using the Eternal blue exploit (MS17-010) affetcs windows. Trickbots usually creates folders to park its modules after its affected. However, a network admin will likely see changes in traffic or attempts to reach out to blacklisted IPs and domains, as the malware will communicate with trickbot’s command and control infrastructure to exfiltrate data and receive tasks.

6. **PEYTA:**

First discovered in 2016, a family encrypted ransomware. This malware targets windows-based systems, infecting the master boot and record to execute a payload that encrypts a hard drive file system. In 2017 June, a new peyta attack was used for a global cyber-attack targeting Ukraine external blue exploits. Peyta is a Russian name. On the day of the attack, Kaspersky lab reported infections in France, Germany and Italy but that the majority of infections targeted Russia and Ukraine, where more than 80 companies were initially attacked, including the Bank of Ukraine. Peyta overwrites windows bootloader and triggers a restart. Crypto currency payment (bitcoins) are usually demanded after the malware is executed.

References:

1. <https://en.m.wikipedia.org/wiki/WannaCry_ransomware_attack>
2. <https://www.malwarebytes.com/emotet/>
3. <https://www.knowbe4.com/gandcrab-ransomware> <https://krebsonsecurity.com/2019/07/whos-behind-the-gandcrab-ransomware/>
4. <https://www.firstpost.com/business/computer-malware-under-garb-of-i-t-department-message-circulating-in-indian-cyberspace-warns-govts-cybersecurity-agency-7399931.html>
5. <https://blog.malwarebytes.com/detections/trojan-trickbot/>
6. <https://en.wikipedia.org/wiki/Petya_(malware)>