Trends by Any.run

Malware prominent in 2019 and not in 2020 -

1. FlawedAmmyy - FlawedAmmmyy is a RAT type malware that can be used to perform actions remotely on an infected PC. This malware is well known for being featured in especially large campaigns with wide target demographics.
2. Gootkit - Gootkit an advanced banking trojan. It is extremely good at evading detection and has an incredibly effective persistence mechanism which makes it a dangerous malware that researchers and organizations should be aware of.
3. IcedID - IcedID is a banking Trojan type malware which allows attackers to utilize it to steal banking credentials of the victims. IcedID aka BokBot mainly targets businesses and steals payment information, it also acts as a loader and can deliver another viruses or download additional modules.
4. Nemty - Nemty is ransomware with an unusually complex encryption algorithm. This malware encrypts user files and demands money so that they can be unlocked again. It may be connected to other famous ransomware, but we don’t know for sure.
5. Adwind - Adwind RAT, sometimes also called Unrecom, Sockrat, Frutas, jRat and JSocket is a Malware As A Service Remote Access Trojan that attackers can use to collect information from infected machines.
6. Smoke Loader - The main function of Smoke Loader is dropping other, more destructive malware on infected machines. However, unlike many competing loaders this one can be extended via plugins to feature some destructive malicious info-stealing functions.
7. Troldesh - Troldesh is ransomware — a malware that demands a payment in order to unlock encrypted files. It is also can search and steal information from the banking programs if such are found on the infected machine.
8. Predator the Thief - Predator the Thief is an information stealer, meaning that it is a malware that steals data from infected systems. This virus can access the camera and spy on victims, steal passwords and login information as well as retrieve payment data from cryptocurrency wallets.

Malware prominent both in 2019 and 2020 -

1. Emotet - Emotet is one of the most dangerous trojans to have been created. Over the course of its lifetime, it was upgraded to become a very destructive malware. It targets mostly corporate victims but even private users get infected in mass spam email campaigns.
2. Agent Tesla - Agent Tesla is spyware that collects information about the actions of its victims by recording keystrokes and user interactions. It is falsely marketed as a legitimate software on the dedicated website where this malware is sold.
3. Lokibot - Lokibot was developed in 2015 to steal information from a variety of applications. Despite the age, this malware is still rather popular among cybercriminals.
4. njRAT - njRAT is a remote access Trojan. It is one of the most widely accessible RATs on the market that features an abundance of educational information. Interested attackers can even find tutorials on YouTube. This allows it to become one of the most popular RATs in the world.
5. Hawkeye - Hawkeye often gets installed in a bundle with other malware. This is a Trojan and keylogger that is used to retrieve private information such as passwords and login credentials. This is an advanced malware that features strong anti-evasion functions.
6. Trickbot - TrickBot is an advanced banking Trojan that attackers can use to steal payment credentials from the victims. It can redirect the victim to a fake banking cabinet and retrieve credentials typed in on the webpage.
7. Crimson RAT - Crimson is a Remote Access Trojan — a malware that is used to take remote control of infected systems and steal data. This particular RAT is known to be used by a Pakistani founded cybergang that targets Indian military objects to steal sensitive information.
8. Hancitor - Hancitor was created in 2014 to drop other malware on infected machines. It is also known as Tordal and Chanitor. This malware is available as a service which makes it accessible tools to criminals and contributes to the popularity of this virus.
9. Maze - Maze is a Ransomware — a malware that encrypts the victim’s files and restores the data in exchange for a ransom payment. One of the most distinguishable features of the Maze Ransomware is that it is one of the first malware of the kind to publicly release stolen data.
10. Dridex - Dridex is a very evasive and technically complex banking Trojan. Despite being based on a relatively old malware code, it was substantially updated over the years and became capable of using very effective infiltration techniques that make this malware especially dangerous.
11. Dharma - Dharma is an advanced Ransomware that has been observed in the wild since 2016. It is considered to be the second most profitable RaaS operation by the FBI. The malware targets hospitals and state organizations, encrypts files and demands a payment to restore access to lost information.
12. Sodinokibi - Sodinokibi, also called Revil is a dangerous ransomware-type malware. Among other tools, it uses advanced encryption techniques and can operate without connection to control servers. Sodinokibi is among the most complex Ransomware in the world.
13. Pony - Pony is a malware with two main functions — stealing information and dropping other viruses with different tasks on infected machines. It has been around since 2011 and it still actively attacks users in Europe and America.
14. WannaCry - WannaCry is a famous Ransomware that utilizes the EternalBlue exploit. This malware is known for infecting at least 200,000 computers worldwide and it continues to be an active and dangerous threat.
15. Netwire - Netwire is an advanced RAT — it is a malware that takes control of infected PCs and allows its operators to perform a variety of actions. Unlike many RATs, this one can target every major operating system, including Windows, Linux and MacOS.