An overview on attacks, threats, vulnerabilities

Viruses and worms

Malicious software, malware, malicious code or malcode – these describes piece of software that are designed to something bad, harmful, and unwanted thing:

- steal
- damage,
- illegitimate,
- disrupt,
- use resources (memory, processing), etc.

The classification of the malware is as follows: viruses, worms, trojans, bots.

A computer virus inserts a copy of itself into another program and becomes a part of it. Some of the viruses do something annoying, some damages your data, some may cause denial-of-service attacks. Generally, a virus exists on the computer as a part of an executable file. The infected host program may continue to work as before. Some viruses however destroy its host program.

The viruses can be transferred to other computers by

- network,
- external memory sticks,
- file sharing,
- email attachments,
- system upgrades,
- disk.

A computer worm can also replicate itself to another computer so that it can spread. A worm is a standalone program, it requires no host file to spread. Worms may exploit a vulnerability of to enter to the system.

Trojans were named after the Greek's wooden horse. Usually, it uses a trick to get into your system. Trojans may damage the host computer by stealing, deleting, encrypting your data, pen a backdoor and give access to other malicious code. Trojans have no replication capabilities.

Bots are automated processes; the name stems from the word robot. They intraduct with other network services. Bots may steal passwords, gather information, log keystrokes, relay spam messages.

Phases of their attack [[2]]:

Probe – identifies targets

Penetrate - transfers malicious code to the target

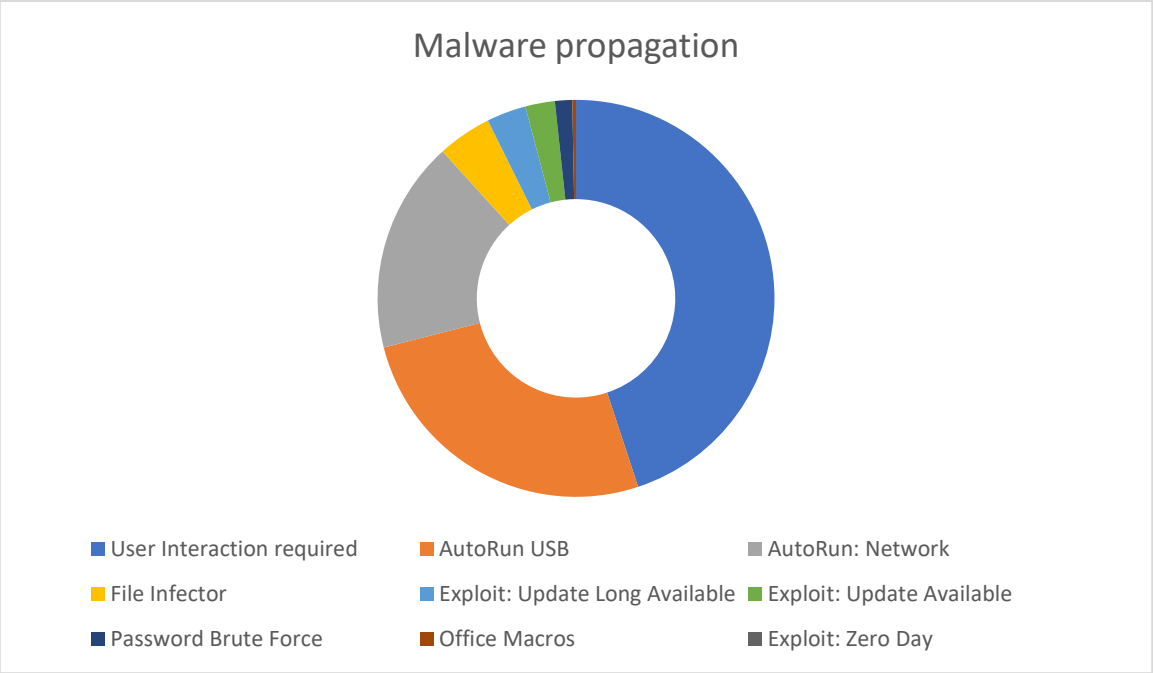
Persist – malware attempts to remain in the system

Propagate – extend to other systems

Paralyze – malware causes damage

According to the predictions in 2021 the cost of cybercrime will cause USD 6,000,000,000,000 (6 trillion USD) damage, and 12 people will be a victim in every second.

According to a Security Intelligence Report [[3]] the most popular propagation tactics are as follows:



- User Interaction required - 44.8%
- AutoRun USB - 26%
- AutoRun: Network - 17.2%
- File Infector - 4.4%
- Exploit: Update Long Available - 3.2%
- Exploit: Update Available - 2.4%
- Password Brute Force - 1.4%
- Office Macros - 0.3%
- Exploit: Zero Day - 0%

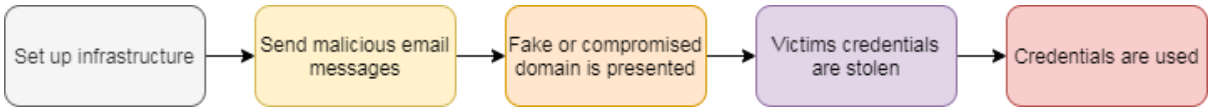
The key role of the defense is prevention.

1. Be careful!
    a. avoid unknown free software and avoid pirate software.
    b. avoid privileged accounts when not necessary.
    c. apply secure configurations.
    d. keep you machine up-to-date. Apply security updates for your browser, email client and operating system.
    e. isolate computers that can not be updated.
    f. use advanced protection for your browser and emails, use secure email gateway.
    g. use anti-malware tools.
    h. defense your network real time.
    i. teach users to be suspicious.
    j. .
2. Have access control!
    a. Use the least privilege required.
    b. Segment your network.
    c. Be careful when granting permissions to applications.
    d. Download application from reliable places such as app store.
    e. Have strong user restriction policy on running applications.
    f. Use whitelists of applications.

3. Have backups!
    a. It is vital to have automatic backups.
    b. You can use online services.
    c. Ensure your backup containing critical data can not be destroyed.
    d. Have a backup policy.
    e. Store your backups on at least two different storage types of which one is offsite.
4. Be aware!
    a. Check sensitive data requests.
    b. Take warnings seriously when clicking to web links.
    c. When computer is slower than usually.

Up until a few years ago, cybercriminals focused their efforts on malware attacks because they provided the greatest return on investment. More recently, they've shifted their focus to phishing attacks (~70%) with the goal of harvesting user credentials. [5] Its steps are:

1. Criminals set up their infrastructure: compromitted or fake domains. to gather information on potential targets.
2. Send malicious email messages.
3. Victim is directed to the fake domain.
4. Victim enters credentials into a fake form, or victim downloads malware which collects credentials on the device.
5. Criminals gain access to victim's network. Criminals use the same credentials on other sites.



References

[1] Microsoft Secure Blog Staff: The Emerging Era of Cyber Defense and Cybercrime
[2] Cox, Kerry J., and Christopher Gerg. *Managing Security with Snort & IDS Tools: Intrusion Detection with Open Source Tools*. " O'Reilly Media, Inc.", 2004.
[3] https://www.zdnet.com/article/which-is-the-most-popular-malware-propagation-tactic/
[4] https://clouddamcdnprodep.azureedge.net/gdc/gdc09FrGq/original
[5] Microsoft Digital Defense Report | September 2020