MALWARE

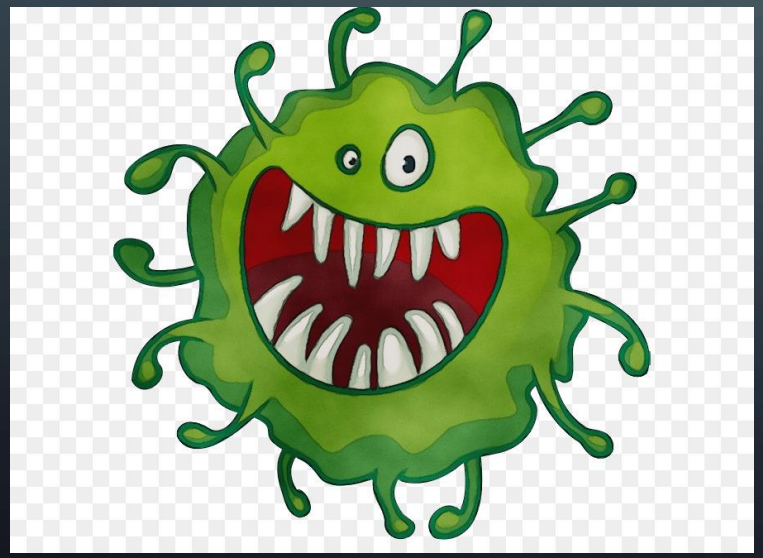
ELKINA GALINA, HERZEN UNIVERSITY, 2 YEARS OF CS&CE

Short review

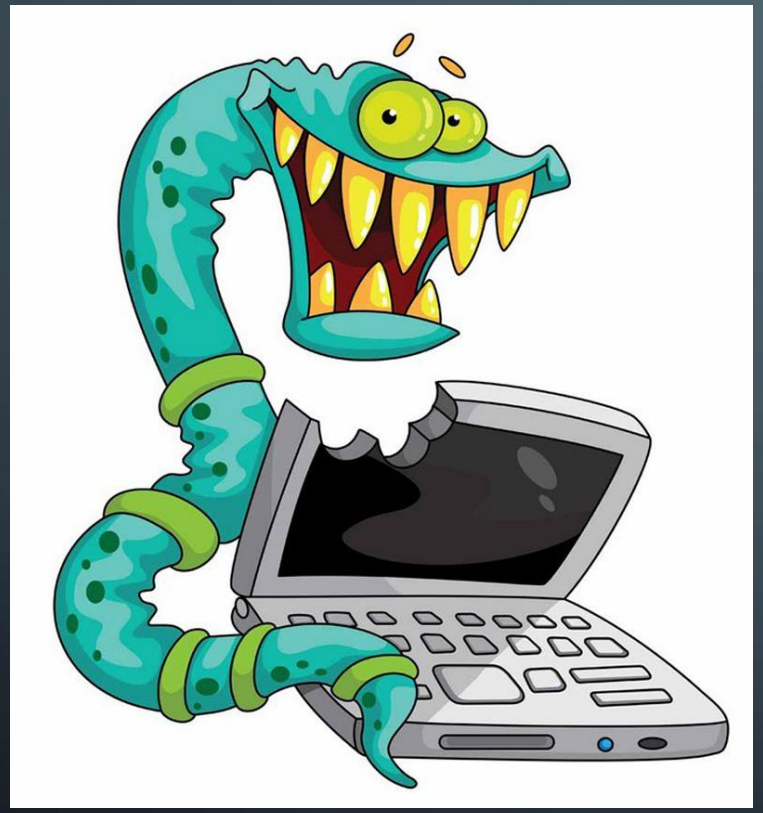
The term “malware” is used to describe any malware on a computer or mobile device. These programs are installed without the consent of users and can cause a number of unpleasant consequences, such as reduced computer performance, retrieving user personal data from the system, deletion of data, or even an impact on the operation of computer hardware. As cybercriminals come up with increasingly sophisticated ways of penetrating users' systems, the malware market has expanded significantly. Let's look at some of the most common types of malware that can be found on the Internet.

VİRUSES

- Computer viruses got their name for the ability to "infect" many files on the computer. They also spread to other machines when infected files are sent via email or transferred by users on physical media, such as USB drives or (earlier) on diskettes. According to the National Institute of Standards and Technology (NIST), the first computer virus called “Brain” was written in 1986 by two brothers to punish pirates who steal software from the company. The virus infects the boot sector of floppy disks and is transmitted to other computers through copied infected floppies.



WORMS



- Unlike viruses, worms do not require human intervention to spread: they infect one computer and then spread through computer networks to other machines without the participation of their owners. Using network vulnerabilities, such as flaws in email programs, worms can send thousands of copies of themselves and infect all new systems, and then the process begins again. In addition to the fact that many worms simply "eat up" system resources, thereby reducing computer performance, most of them now contain malicious "components" designed to steal or delete files.

ADWARE

- One of the most common types of malware is adware. Programs automatically deliver advertisements to host computers. Among the varieties of Adware are pop-up advertisements on web pages and ads that are part of “free” software. Some adware programs are relatively harmless, others use tracking tools to gather information about your location or history of visiting sites and display targeted ads on your computer screen. BetaNews announced the discovery of a new type of adware that can disable anti-virus protection. Since Adware is installed with the user's consent, such programs cannot be called malicious: they are usually identified as “potentially unwanted programs”.

SPYWARE

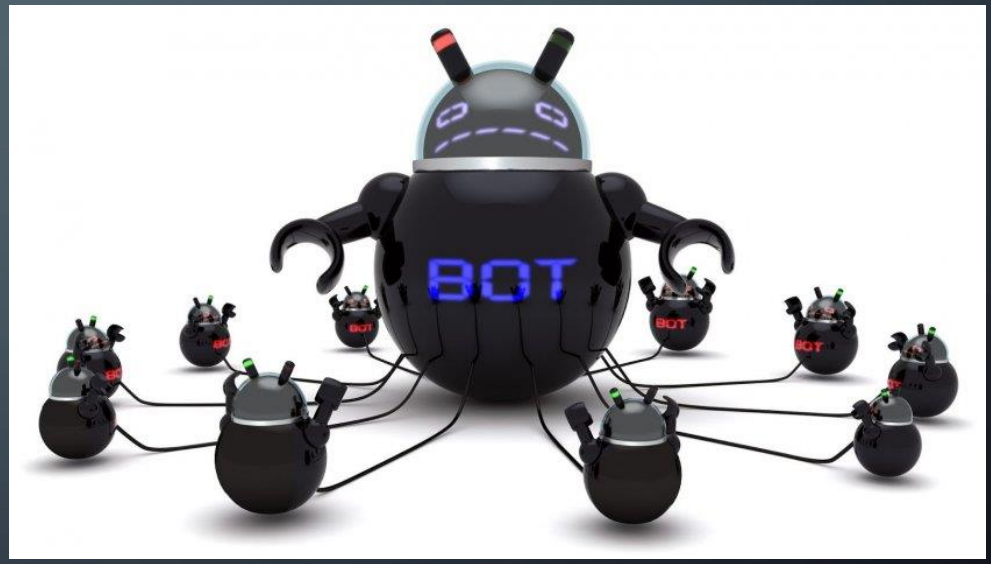
- Spyware does what its name implies - monitors your actions on the computer. It collects information (for example, it registers keystrokes on the keyboard of your computer, tracks which sites you visit and even intercepts your registration data), which is then sent to third parties, usually cybercriminals. It can also change certain security settings on your computer or interfere with network connections. According to TechEye, new types of spyware allow attackers to monitor user behavior (of course, without their consent) on different devices.

RANSOMWARE PROGRAMS

Ransomware infects your computer, then encrypts sensitive data, such as personal documents or photos, and requires a ransom for their decryption. If you refuse to pay, the data is deleted. Some types of ransomware programs can completely block access to your computer. They can impersonate their actions for the work of law enforcement agencies and accuse you of any unlawful acts. In June 2015, users who reported a financial loss totaling $ 18,000,000 as a result of the ransomware virus CryptoWall applied to the FBI Internet Reception Center for complaints about fraud on the FBI.

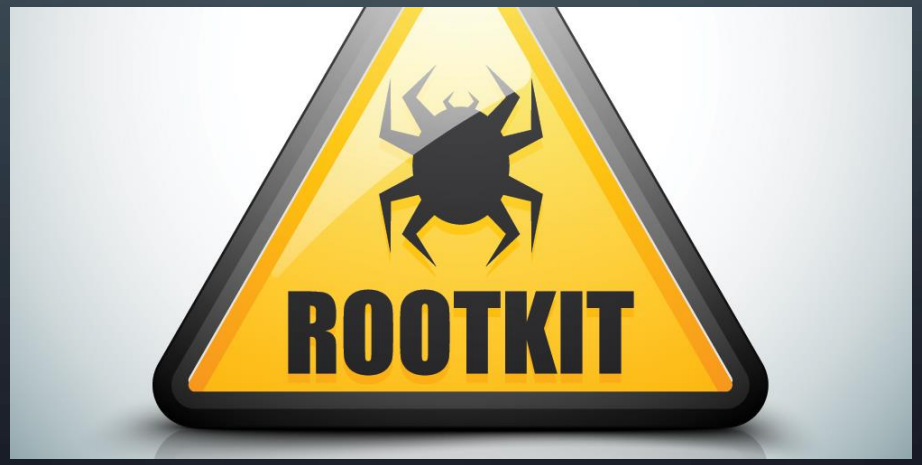
BOTS

- Bots are programs designed to automatically perform certain operations. They can be used for legitimate purposes, but attackers have adapted them for their malicious purposes. Having entered a computer, bots can force it to execute certain commands without approval or without the user's knowledge at all. Hackers can also try to infect several computers with the same bot to create a botnet, which will then be used to remotely control hacked machines — steal confidential data, monitor victim actions, automatically spread spam, or launch destructive DDoS attacks on computer networks.



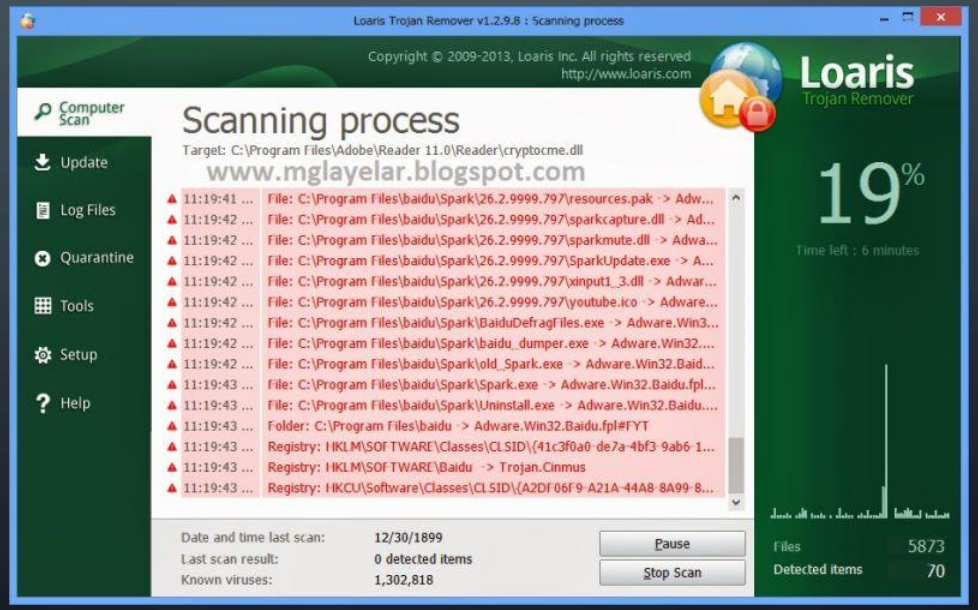
ROOTKİTS

- Rootkits allow a third party to remotely access and control a computer. These programs are used by IT specialists to remotely resolve network problems. But in the hands of intruders, they turn into a fraud tool: penetrating your computer, rootkits provide cybercriminals with the opportunity to gain control over it and steal your data or install other malicious programs. Rootkits are able to qualitatively mask their presence in the system in order to remain unnoticed for as long as possible. Detection of such malicious code requires manual monitoring of unusual behavior, as well as regular adjustments to the software and operating system to eliminate potential infection routes.



TROJAN PROGRAMS

- Better known as Trojans, these programs are disguised as legitimate files or software. After downloading and installing they make changes to the system and carry out malicious activities without the knowledge or consent of the victim.



BUGS

- Bugs - errors in fragments of a program code are not a type of malware, but errors made by a programmer. They can be detrimental to your computer, such as stopping, crashing, or slowing performance. At the same time, security bugs are an easy way for intruders to bypass the protection and infect your machine. Providing more effective security controls on the developer's side helps to eliminate errors, but it is also important to regularly make programmatic adjustments to eliminate specific bugs.

MYTHS AND FACTS

- *Any computer error message indicates a virus infection.* This is incorrect: error messages may also be caused by hardware or software errors.
- *Viruses and worms always need user interaction.* This is not true. In order for a virus to infect a computer, code must be executed, but this does not require user input. For example, a network worm can infect users' computers automatically if they have certain vulnerabilities.
- *Email attachments from reputable senders are secure.* This is not the case because these attachments can be infected with a virus and used to spread the infection. Even if you know the sender, do not reveal anything that you are not sure about.
- *Antivirus programs can prevent infection.* For their part, anti-virus vendors are doing everything possible to keep up with malware developers, but users must install on their computers a comprehensive Internet security class security solution that includes technologies specifically designed to actively block threats. Even though 100% protection does not exist. You just need to consciously approach to ensuring your own online security to reduce the risk of being attacked.
- *Viruses can cause physical damage to your computer.* What if malicious code overheats the computer or destroys critical microchips? Suppliers of protective solutions have repeatedly debunked this myth - such damage is simply impossible.
- Meanwhile, the growth in the number of devices interacting with each other on the Internet of Things (IoT) opens up additional interesting possibilities: what if an infected car drives off the road, or does an infected smart oven continue to heat up until normal load exceeds? Future malware can make such physical damage a reality.

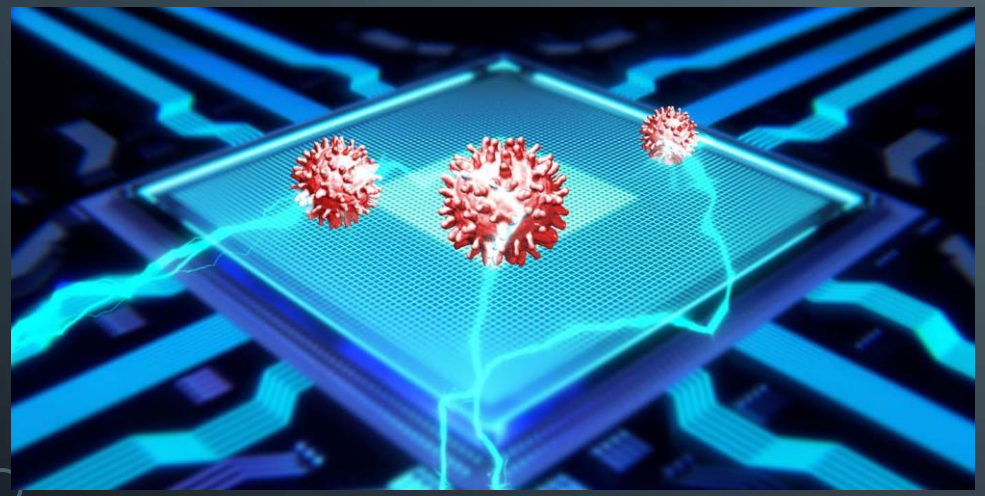
MYTHS AND FACTS

- Users have a number of misconceptions about malware: for example, *many believe that signs of infection are always noticeable and therefore they can determine that their computer is infected*. However, as a rule, malware does not leave traces, and your system will not show any signs of infection.
- Tweet:
  - ***As a rule, malware leaves no trace, and your system will not show any signs of infection. Tweet it!***
- Just *do not believe that all sites with a good reputation are safe*. They can also be hacked by cybercriminals. A visit to a legitimate website infected with a malicious code is an even greater chance for a user to part with his personal information. This, SecurityWeek writes, happened to the World Bank. Also, many users believe that their personal data - photos, documents and files - are of no interest to the creators of malware. Cybercriminals use publicly available data to attack individual users, or to gather information that will help them create phishing emails in order to penetrate the internal networks of organizations.

STANDARD İNFECTİON METHODS

- So, how does a computer virus or malware infection occur? There are several standard methods. These are links to malicious websites in emails or posts on social networks, a visit to an infected site (known as drive-by download) and the use of an infected USB drive on your computer. Vulnerabilities in the operating system and applications allow attackers to install malware on computers. Therefore, to reduce the risk of infection, it is very important to install security updates as they become available.

STANDARD İNFECTİON METHODS



- Cybercriminals often use social engineering techniques to trick you into doing something that threatens your security or the security of your company. Phishing messages are one of the most common methods. You get a seemingly absolutely legitimate email message in which you are persuaded to download an infected file or visit a malicious website. The goal of hackers is to write a message so that you find it convincing. This may be, for example, a warning about a possible virus infection or a notice from your bank or a message from an old friend.

STANDARD İNFECTİON METHODS

- Confidential data, such as passwords, is the main target of cybercriminals. In addition to using malware to intercept passwords when they are entered, attackers can also collect passwords from websites and other computers that they have cracked. That is why it is so important to use a unique and complex password for each account. It must consist of 15 or more characters, including letters, numbers and special characters. Thus, if cybercriminals succeed in hacking one account, they will not get access to all your accounts. Unfortunately, most users have very weak passwords: instead of coming up with a hard-to-use combination, they access standby-type passwords like “123456” or “Password123”, which criminals easily pick up. Even control questions can not always serve as an effective defense, because many people give the same answer to the question “Your favorite food?”, For example, if you are in the United States, then almost certainly the answer will be “Pizza”.

SİGNS OF İNFECTİON

- Although most malware does not leave any obvious traces, and your computer works fine, sometimes you can still notice signs of a possible infection. The very first of them is a decrease in performance, i.e. processes are slow, loading windows takes longer, some random programs are running in the background. Another warning sign can be considered as modified home pages in your browser or more frequent than usual pop-up ads. In some cases, malware can even affect the basic functions of a computer: Windows does not open, there is no connection to the Internet or access to higher-level system management functions. If you suspect your computer may be infected, immediately check your system. If the infection is not detected, but you are still in doubt, get a second opinion - run an alternative anti-virus scanner.

THANKS FOR YOUR ATTENTION!!!