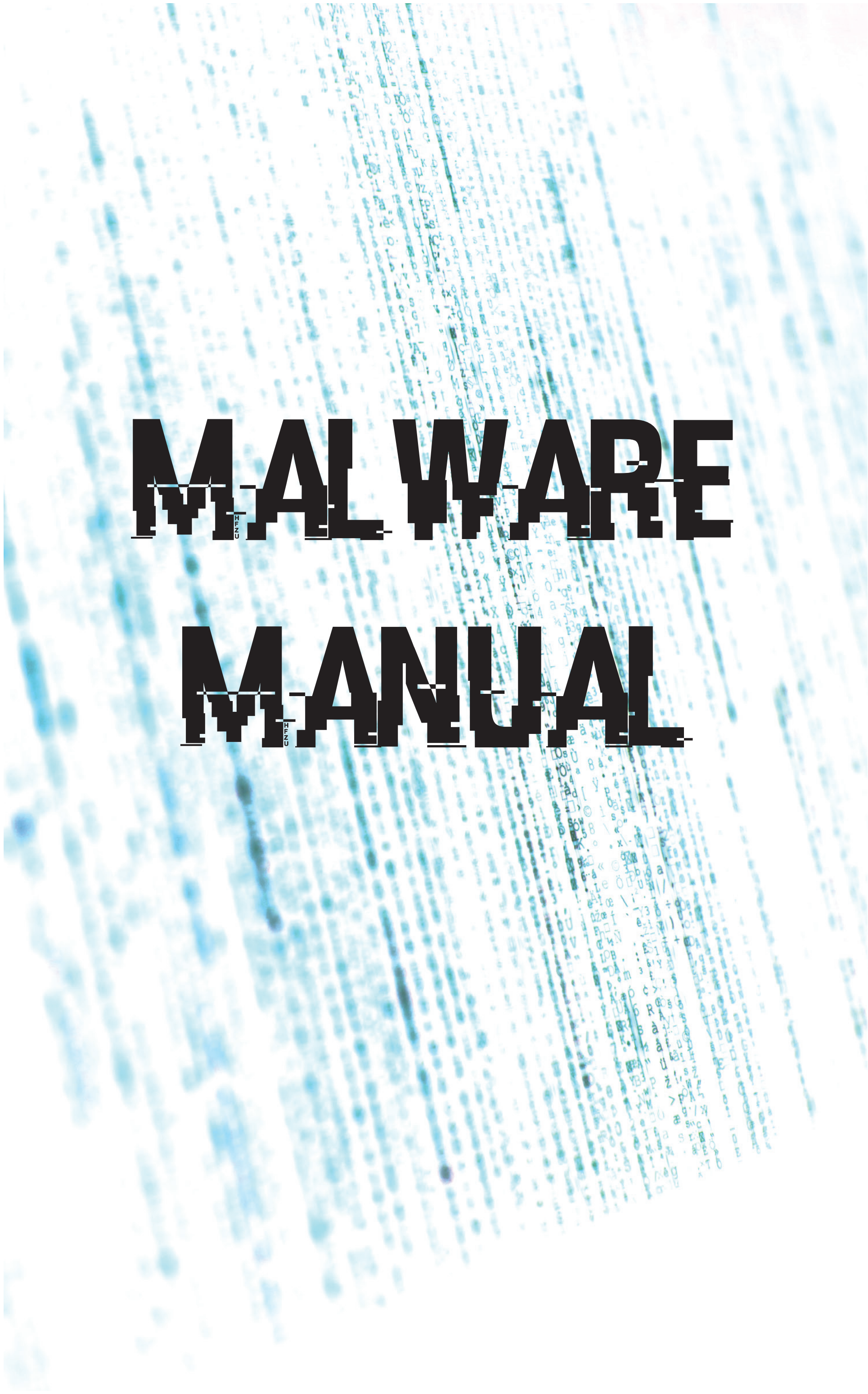
Provided by

ITS Security



MALWARE MANUAL

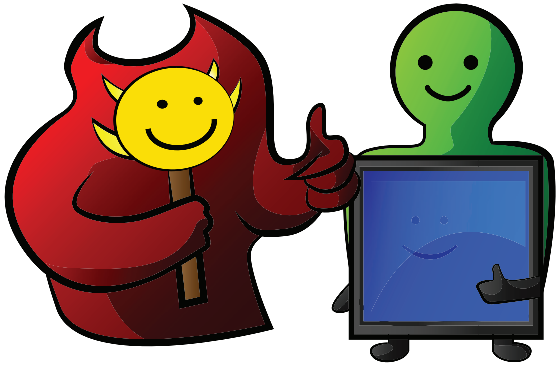
IMPORTANT TERMS:

Malware

Malicious software that intentionally attacks a machine.

User

The person(s) who uses a device and it's applications.



Social Engineering

Manipulation used to coerce people into performing actions or divulging confidential information.

Potentially Unwanted Applications

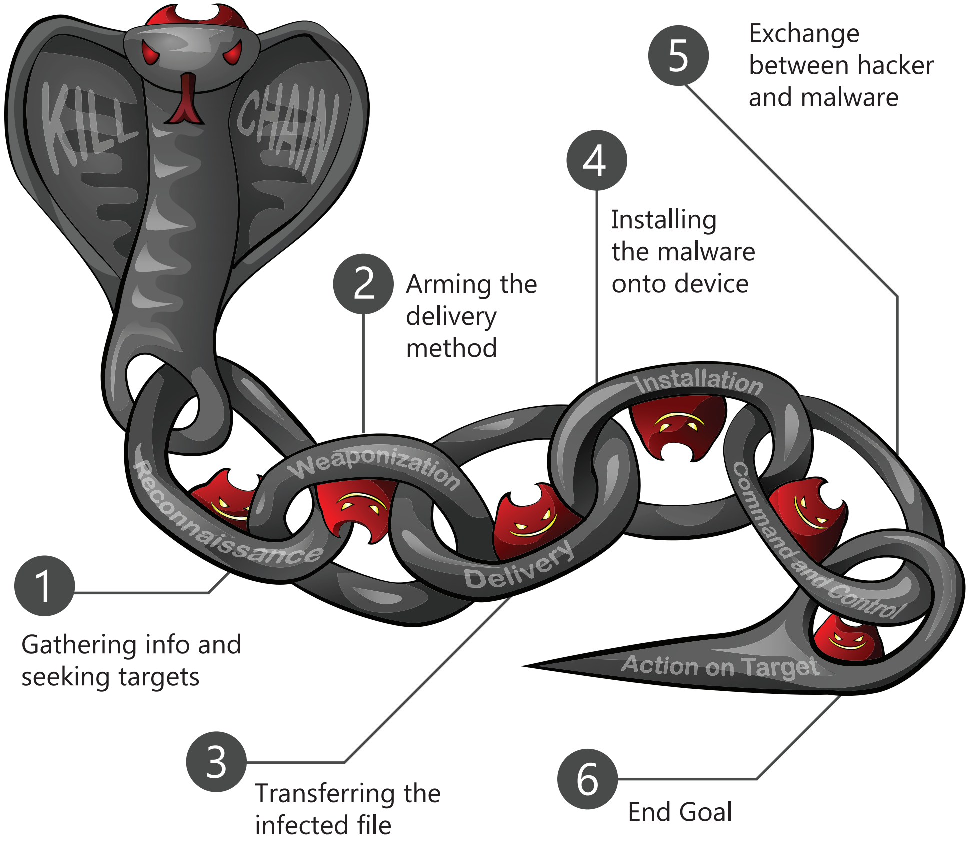
PUA, or Potentially Unwanted Applications, are installed by a third parties or unintentionally. While a PUA may not actively attack the machine, they often come bundled with malware and can open up avenues for Malware.

Devices

A computer, phone, tablet or other technology that can access the internet that runs an operating system such as Windows, Macintosh OS X, Linux etc. All devices are vulnerable to malware.

KILL CHAIN:

Detection of malware is usually only a red flag that explains only a part of the infection because it occurs in stages. These stages are called a kill chain. Know where you are and what malware does to know what is at risk.



1 Gathering info and seeking targets

2 Arming the delivery method

3 Transferring the infected file

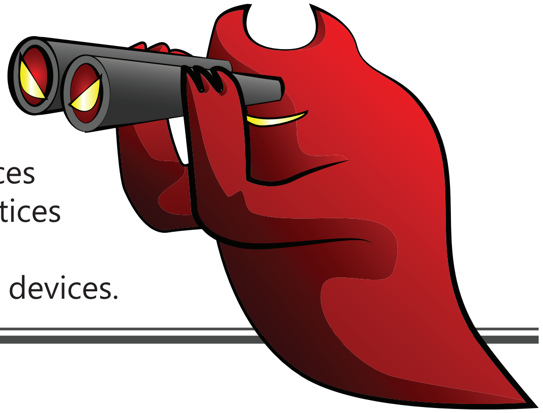
4 Installing the malware onto device

5 Exchange between hacker and malware

6 End Goal

Note that these steps are generalized and often have many different sub-steps depending the goal and methods of the attack.

1. RECONNAISSANCE:



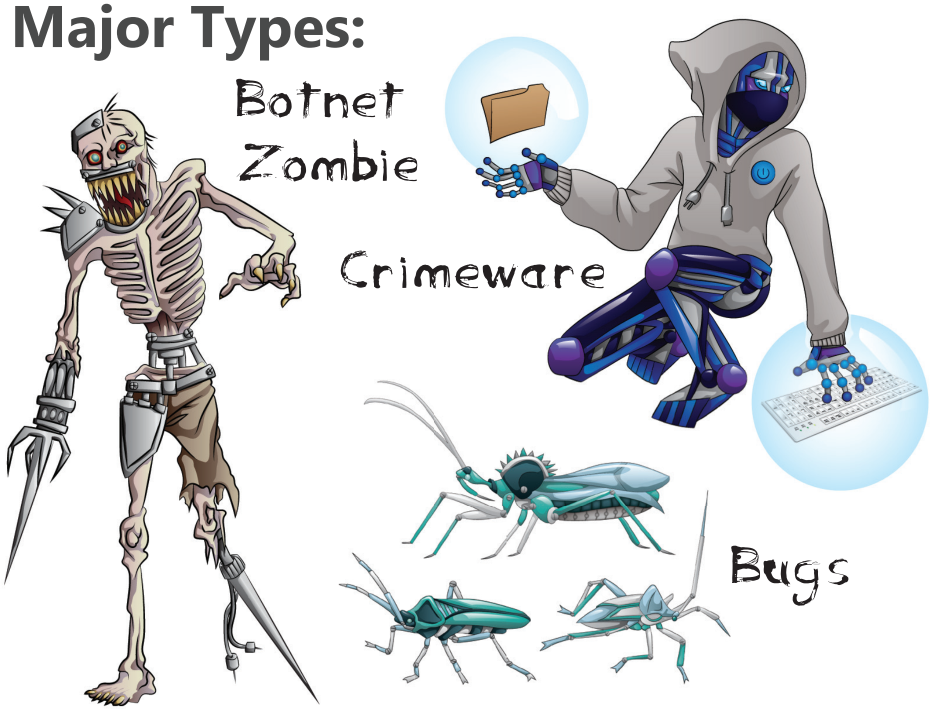
Reconnaisance is the stage of information gathering and seeking targets. Hackers gather information such as relationships between devices and people, organization practices and controls, and exploits and vulnerabilities on the web and devices.

Methods:

Scanning user activity

Phishing campaigns

Major Types:



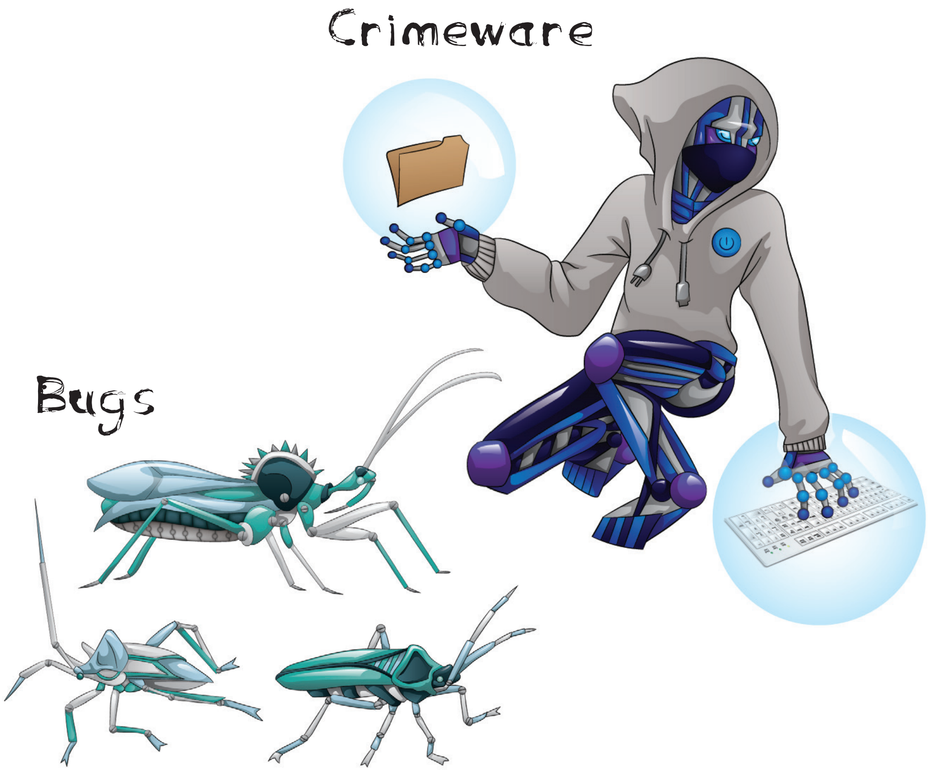
2. WEAPONIZATION:

Weaponization is inserting malicious content into delivery method.

Methods:

Injecting the script or attaching downloadable files to an email.

Major Types:



3. DELIVERY

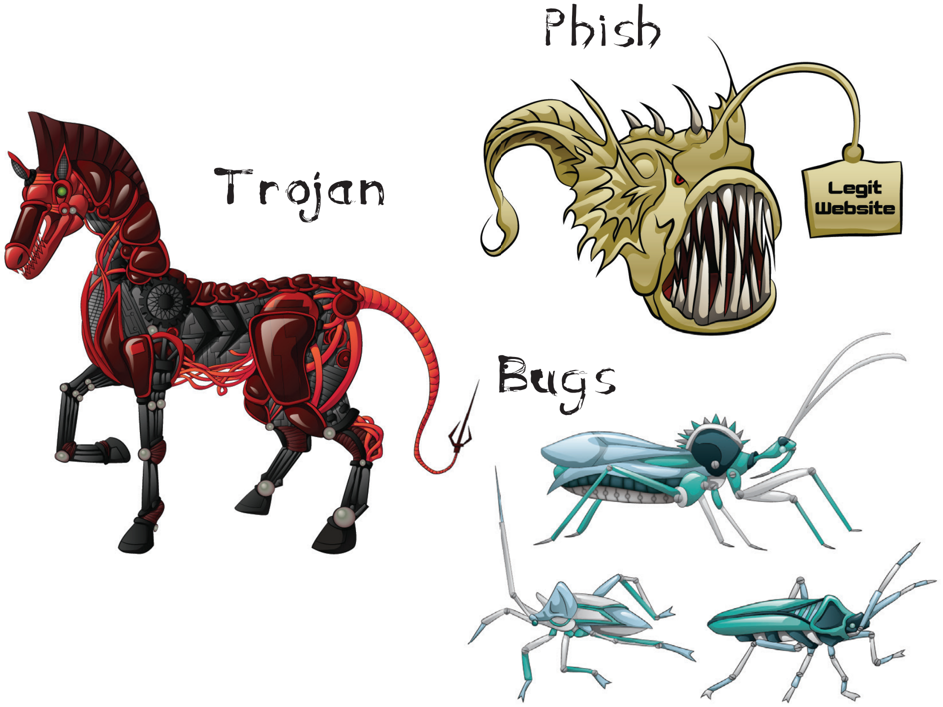
In this stage, the malware is sent to the machine through a network or direct connection (usb/cd/sd car).

Methods:

Exploit bugs to get malware to the machine

Convince the user that it is safe to download the malware.

Major Types:



4. INSTALLATION

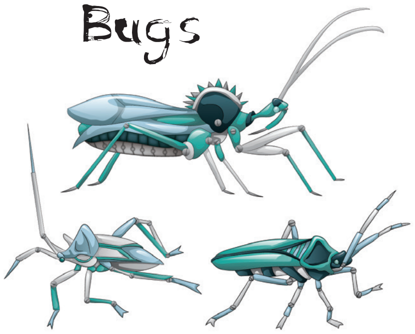
This is the process where libraries, tools, or the malware itself is installed on the machine.

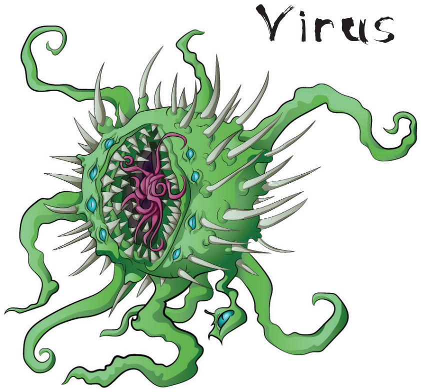
Methods:

User unknowingly runs malicious code

Bugs are exploited to run code automatically

Major Types:





5. COMMAND AND CONTROL

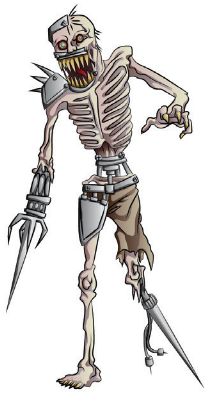
Command and Control, often called C&C, is the continual correspondence between malware and hacker. This communication is used most following installation.

Methods:

Sends information gathered to hacker

Opens a backdoor to the machine

Major Types:



6. ACTION ON TARGET:

Action on Target is the end goal of malware. Information and files are exploited in whatever way the hacker intended.

Methods:

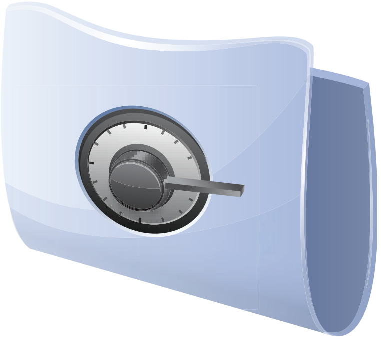
An action is run by a bot or instructions from the hacker through C&C

Major Types:

PROTECTION AND REMOVAL

Safe Choices:

Your security affects and is affected by the people with whom you interact. Keep your sensitive information private, well hidden, and difficult to discover. Traditional Anti-Virus is only one layer of security and can easily be compromised if you are careless with your information.



Anti-Virus

Anti-Virus prevents infections by searching your computer for malicious actions, blocking known malware, and blocking phishing or malicious websites. Unfortunately, Anti-Virus software can be bypassed or directly exploited because modern malware can avoid detection and removal.

Virtualization

Virtualization is the creation of a virtual environment (example: VM) that acts like a normal physical environment. Software executed in a virtual environment is a step removed from the underlying hardware. Virtualization is an additional security layer that can stop malware accessing anything outside of a virtual environment, prevent the spread of malware on a network, and allows for easy backup and recovery of corrupted files. Examples of virtualization are VMware, Virtualbox, Xenapp, Qubes, VLANs and more.

Firewall

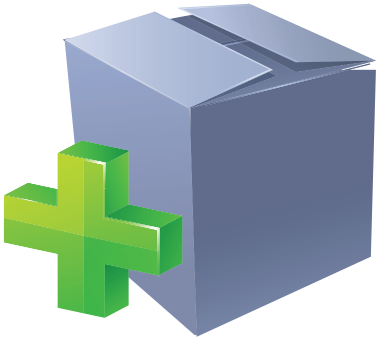
Firewalls are barriers between networks and their parts, creating a safety checkpoint for incoming and outgoing traffic. Most devices come equipped with one.

PRECAUTIONARY MEASURES

Frequent Back-ups

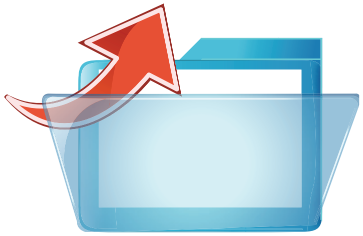
Frequent Back-ups make recovery of corrupted or lost files possible, or at least easier. Back-ups also provide a timeline of when the device was infected and when the malware was used.

Types include **cloud-based storage** that uploads to a service provider via the internet, such as Google Drive, Microsoft OneDrive, or Apple iCloud, and **local storage** using an external hard drive or a separated part of the hard drive, often called a partition.

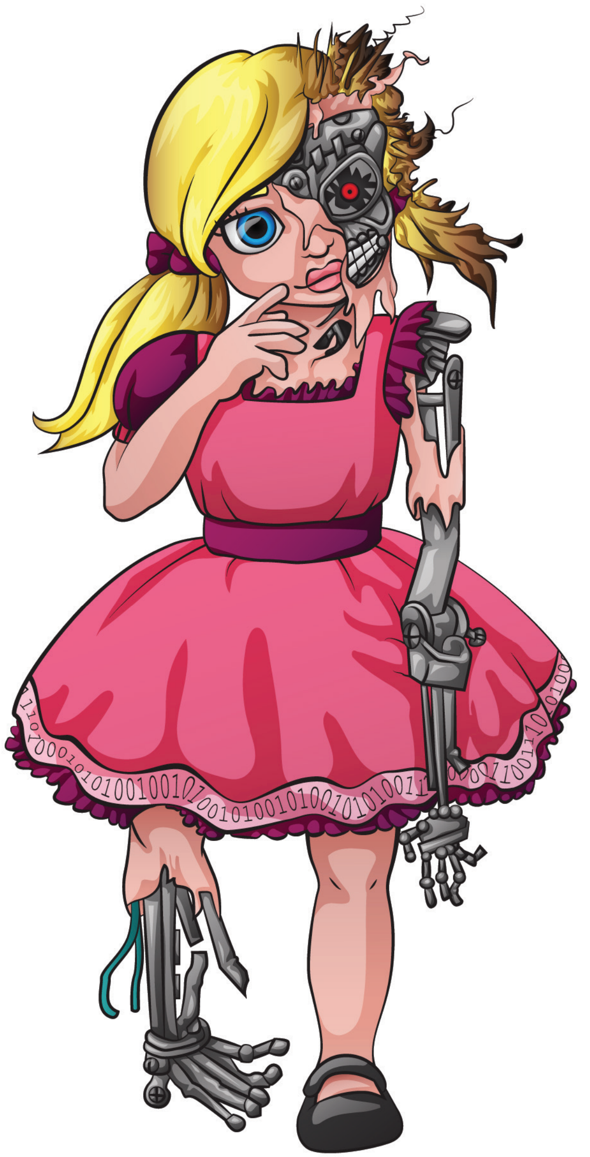


Reformatting

Reformatting a device is currently a reliable way to remove everything from a device, including hidden malware.



ABANDONWARE



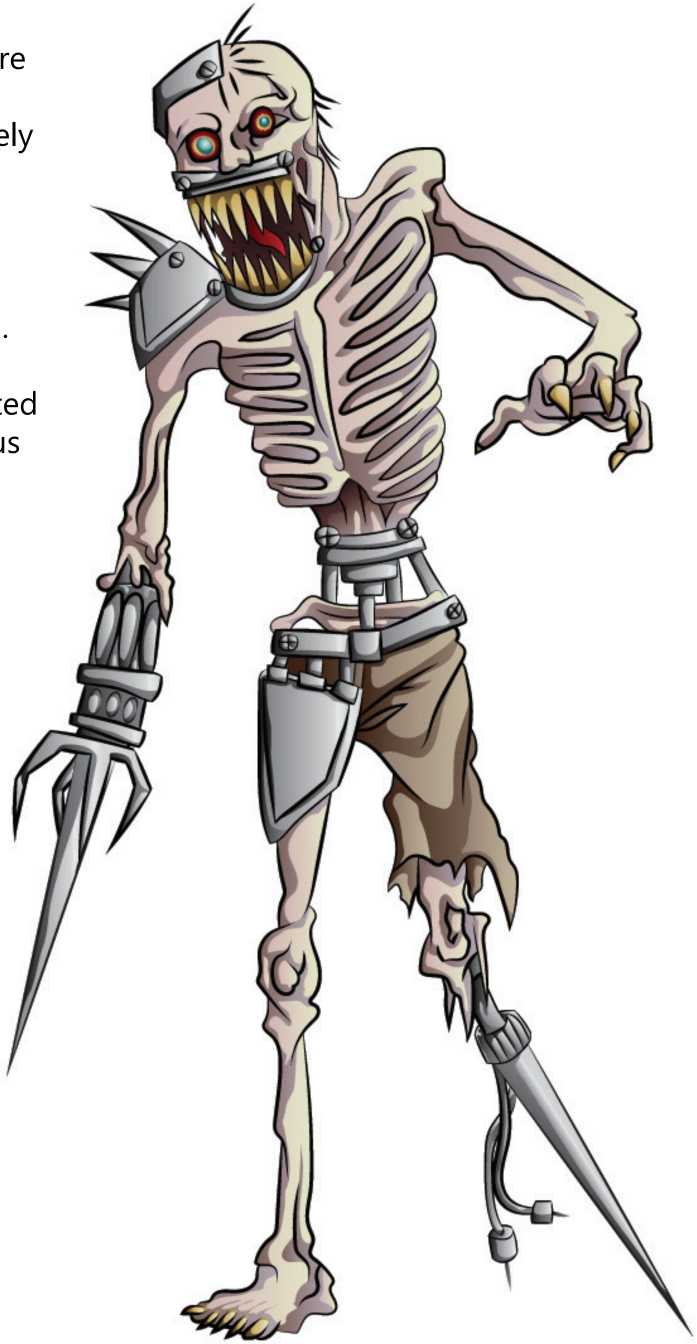
Abandonware is unsupported, old software that contains lots of bugs, such as old versions of operating systems and applications.

ADWARE

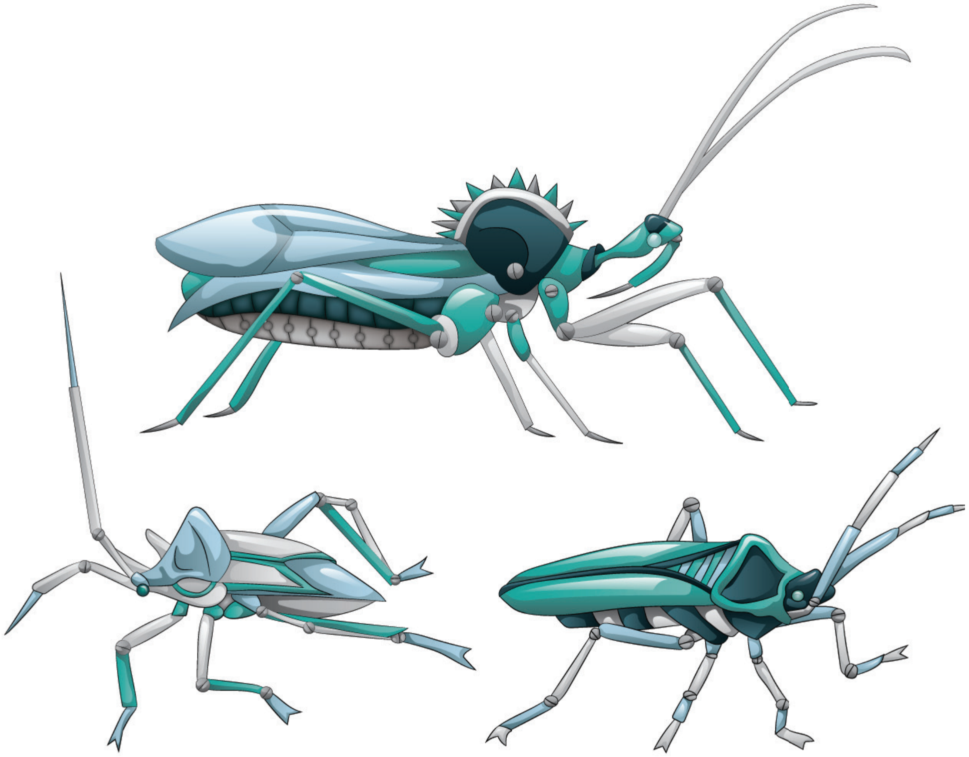
Adware is often a PUA that causes pop-ups or other ads when an application is run, such as an internet browser. This becomes malware when it installs, operates, or collects data without user consent or when it is difficult to install.

BOTNET ZOMBIES

Botnet Zombies are malware infected computers remotely controlled by a hacker through the internet. automatically perform an action. Bots, or software that runs automated tasks, are malicious when that was the intent of their creator.



BUGS



Bugs are not directly malicious, but create vulnerabilities that can lead to infection. These are flaws in software exploited by malware, like a weakened immune system is exploited by bacteria.

CRIMEWARE

Crimeware is a broad category that contains some legitimate software, but can be used to create, infect, or spread malware that can automate cybercrime. A specific and well known example of this is P2P, or peer to peer software, such as BitTorrent.

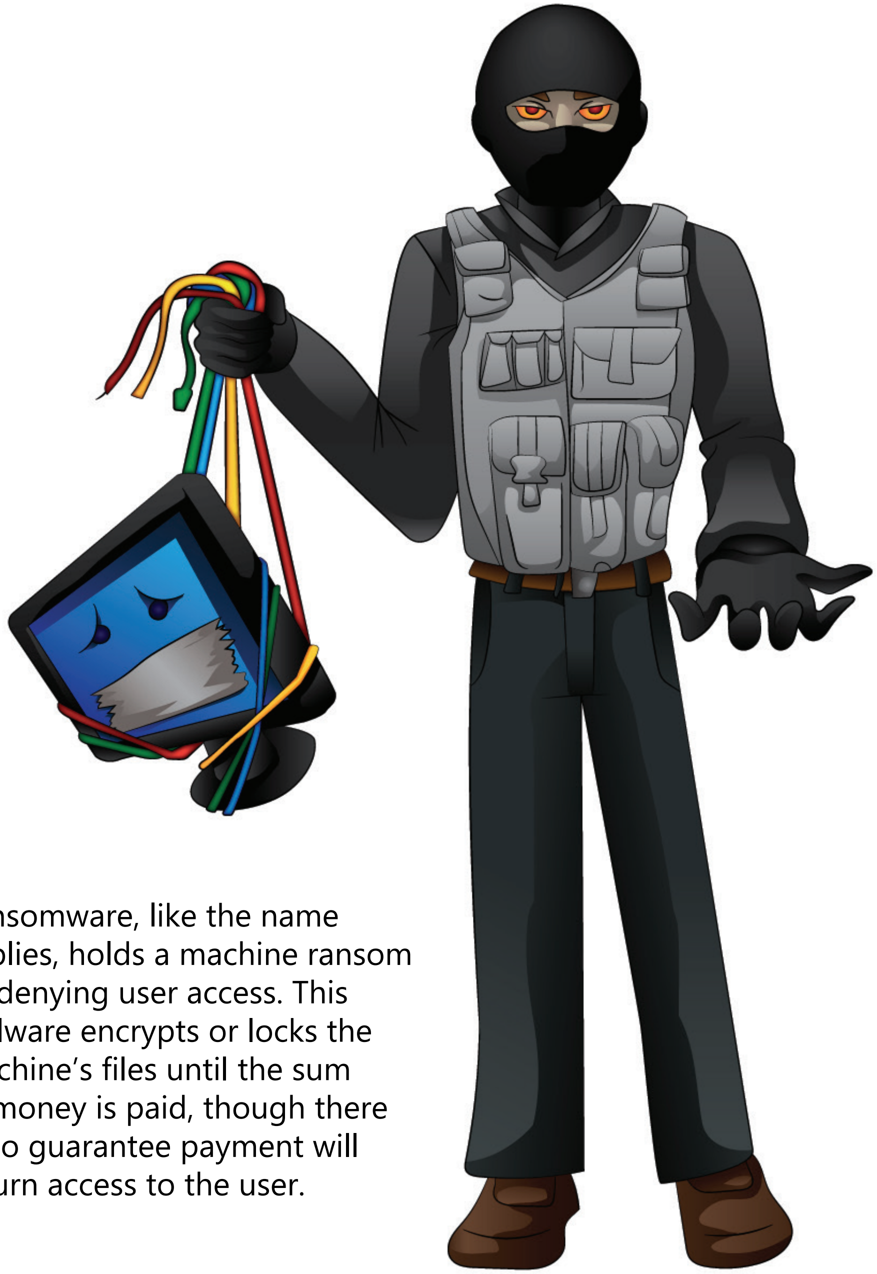
KEYLOGGERS

Keyloggers are a type of spyware that track what is typed on a computer.

PHISH

Phish are a type of social engineering tactic used to elicit action or get information. The most common type of phish are in the form of urgent messages prompting the user to click on a link, provide personal information, or download an attachment. Often, phish are paired with a Trojan or virus to get malware onto the machine.

RANSOMEWARE

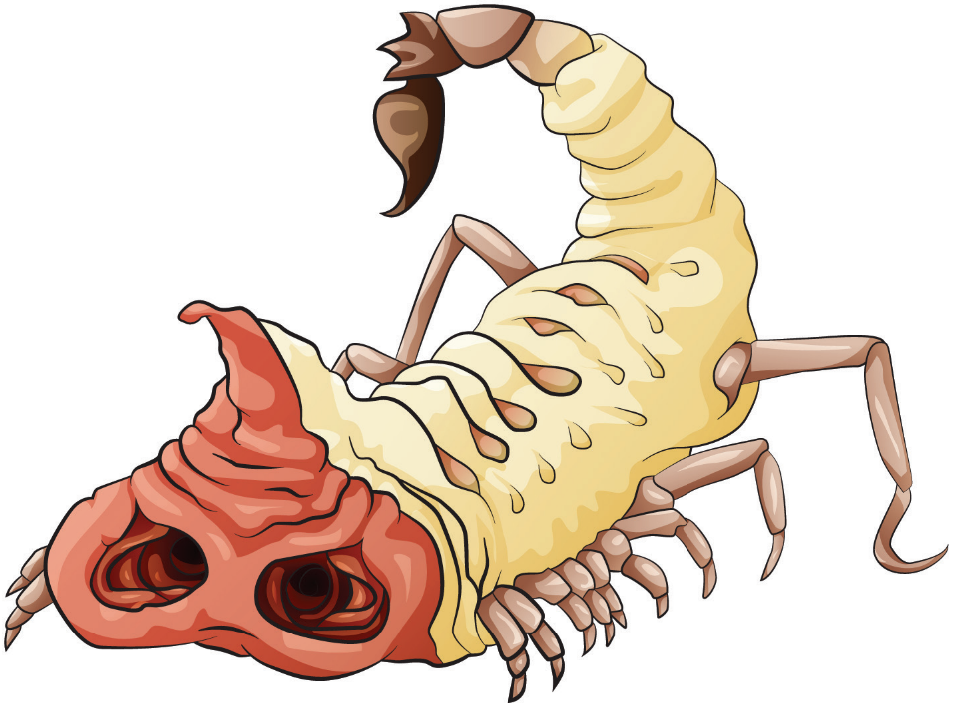


Ransomware, like the name implies, holds a machine ransom by denying user access. This malware encrypts or locks the machine's files until the sum of money is paid, though there is no guarantee payment will return access to the user.

ROOTKITS

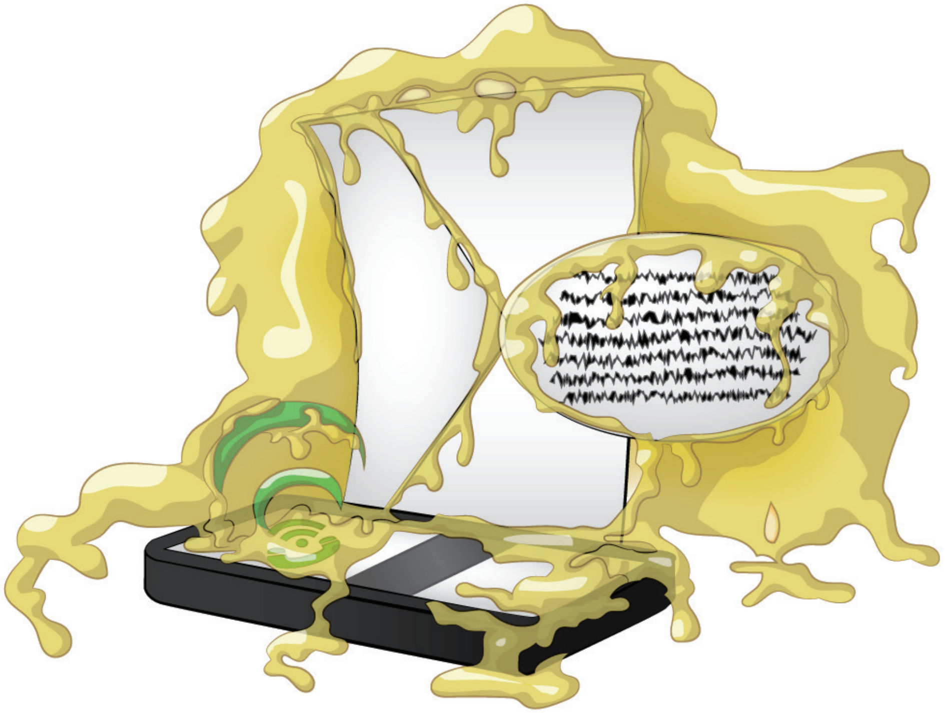
Rootkits actively conceals itself, other malware, and any processes they are running by providing root, or top-most, level access. This allows hackers using the rootkit to run malware, collect data, and infect machines without the user's knowledge.

SNIFFERS



Sniffers are a type of spyware that can intercept and log activity passing over a digital network, such as open wifi networks.

SPAM



Spam are relatively harmless and easy to spot online messages that occasionally carry malware as a phish, or try to sell something like adware.

SPOOFING

Spoofing is cyber forgery. An examples is the phishing method in which a sender address is disguised in a way that it seems like a legitimate sender.

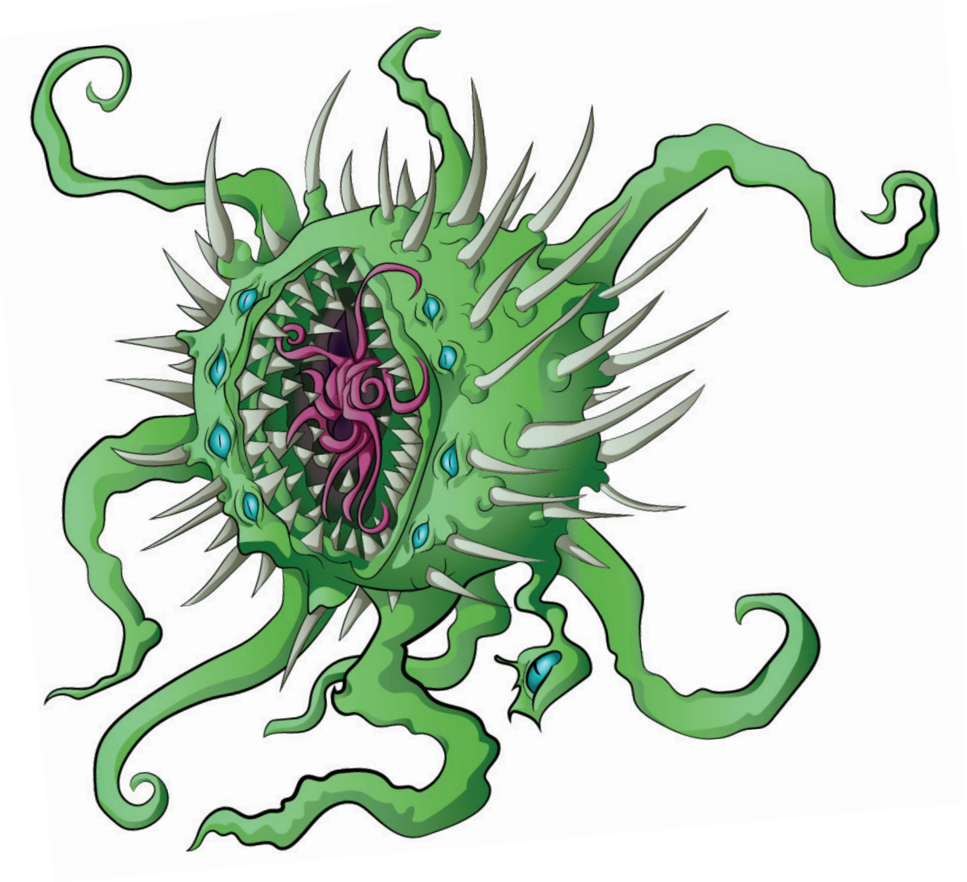
SPYWARE

Spyware tracks and records your activity online, and may actively attack a machine. It is commonly downloaded through websites, sometimes without the user's knowledge or through social engineering.

TROJAN

Trojan Horses, or Trojans, are a large group of malware that poses as legitimate software to get malware onto the machine. Trojans can pose as many different types of programs, such as anti-virus software, software updates, and many more.

VIRUS

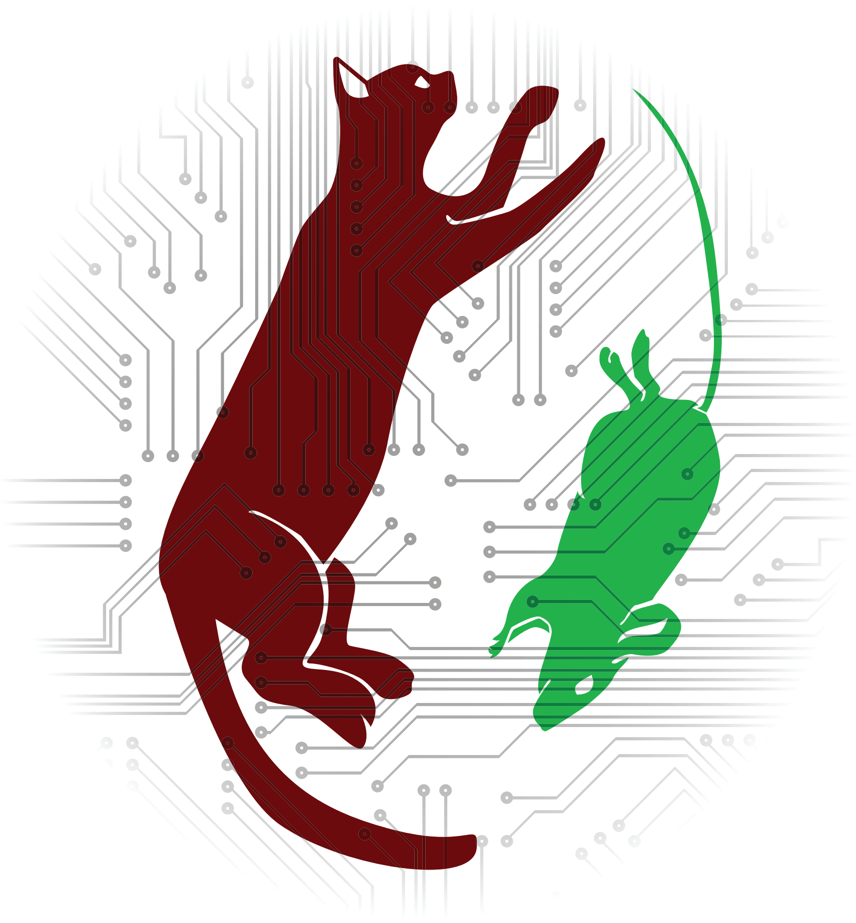


Viruses are malware that replicate themselves once spread to machines. This malware uses other, sometimes legitimate, software or files as a host to spread malware into and across machines. Virus spread by infecting files and thus require the user to run the infected file to run the virus.

WORM

Worms act like viruses in their ability to replicate themselves. This malware is different from viruses because it can move independently of user activity, and does not need a host file or program to spread.

Cat and Mouse



Malware adapts to security measures over time like bacteria grow immune to anti-biotics. Some malware is arising that can survive reformatting by embedding itself in the permanent software programmed into read-only memory of devices like a network card, sound card or even a keyboard or mouse. Some malware can easily re-infect a computer through an infected wifi access point, USB drive, or network storage.