The term malware is used to refer to computer software that, intentionally, violates some security policy. We use taxonomy to further break down the types of malware – though, most malware in today's ecosystem crosses boundaries between types and usually can be classified in a number of ways. Having a taxonomy is still useful though since it gives us a common language to communicate with.

To illustrate the fluidity of taxonomy, consider how you can classify malware in a number of different ways. Functional classification is based on distinguishing features of the malware (and is centred around the malware's goals); Behavioural classification is based on the actions performed by the malware (so the focus is on the behaviour exhibited to accomplish the malware's goal); Authorship classification is based on the author (or tools) used to create the malware (so the focus is on malware attribution). Among others. The type of classification you may choose to use when doing a write-up will depend on the purpose of that write up. For instance, if you are writing an article reporting on Advanced Persistent Threat (APT) groups, you will likely be concerned with attribution.

When you read about malware you will also come across the terms 'types', 'family', and 'sample'. A type is the broader genealogy of the malware (for example, a worm would be a type of malware). The family refers to a group of malware that are derivative of one another (for example, Cerber is the name of a ransomware family and there have been many variants under this umbrella). A sample is a specific instance of a malware and will have a unique signature (for example, this is a particular strain of ransomware that has infected a computer – if analysts were to isolate the malware, this would be a sample). Grouping malware together using these terms is an easier way of communicating, but also helps analysts identify trends.

Trojan horses are programs with a documented (or known) purpose and a undocumented (unexpected) purpose. For example, my dad downloaded a PDF converter onto his laptop (despite it having a windows OS that can already print to a PDF. WTF dad). It turned out that the PDF converter was actually ransomware in disguise, though it only triggered after a certain amount of time had passed*.

*Sometime between my dad downloading the PDF converter and the year before he turned that laptop on again.

Root Kits are trojan horses that hide themselves on systems so that they can carry out further actions without detection.

In the early days this means installing backdoors onto systems (so that the attacker had a way of accessing the system that didn't go through the laborious process they probably used to get the root kit on there in the first place). Then they changed the system programs that reported on the state of the system (stuff like file listing utilities or network status programs that would show network connections that the regular user wouldn't expect to see).

It wasn't difficult countering those types of rootkits. You could just run non-standard programs to get the information about the system status, stuff that would access files directly. You could also identify whether a program had been interfered with using a cryptographically strong checksum.

Then rootkits got sophisticated. They started altering parts of the kernel (which meant we could no longer bypass the rootkit by using non-standard programs or accessing the kernel directly).

Viruses are programs that insert themselves into one or more files. Usually they will then perform some action (but they don't have to: some virus' will just propagate seemingly harmlessly, presumably just to prove they could)

Viruses have two phases: the insertion phase and the execution phase. They explain themselves.

Worms are programs that self-replicate (but don't infect) that use network connections to spread themselves from system to system.

It's easy to get worms confused with viruses. Suffice to say: worms don't need anyone else. Whereas virus' require a host file to infect, and then spread (e.g by emailing the infected files out to be opened by unsuspecting victims), worms don't require a host program or human help to propagate.

Worms generally have three phases: Target selection, propagation, and execution. Again, they explain themselves.

Downloaders are malware that download malicious content via a network connection.

Droppers are designed to install additional malware that it already contains within itself.

Again, these two sound the same. The difference is the semantics of where they get their malicious program from.

Backdoors are used one a system is compromised to give an easy way back into the system (they bypass usual authentication procedures). Typically this will be a function of another malware (like a rootkit or remote access tool RAT)

Rabbit viruses is malware that absorbs all of some resource. It does this through making many copies of itself on a single computer.

With it's primary goal to irritate, you usually wont notice a rabbit virus until your computer crashes (which doesn't take long. Like it's namesake, it replicates very quickly). While this might seem annoying on a personal computer, if well done it can be almost impossible to run your computer long enough to delete it (if the rabbit launches at runtime). On a critical system, this can be deadly.

Logic bombs are programs that wait for an external event before executing. Like a certain date in the calendar.

Spyware are programs that record information about a system (like how you are using it). It might have open network connections that it's constantly sending information down or it could just be storing it somewhere on that system for later collection.

These are always designed with the intention of being invisible. A spy wouldn't be much good if you knew he was there.

Botnets are collections of bots (brain dead computers) that are controlled via a command and control cetnre to co-ordinate attacks.

Botnets these days mostly comprise of the legions of poorly secured IoT devices (all equipped with default admin passwords that the botnet masters make use of).

Ransomware is malware that holds your system (and it's resources) hostage until a ransom is paid.

These have been in the news recent and have created an unfortunate association with bitcoin (a monetary system that is good for those who wish to remain anonymous like, say, the masterminds of a ransomware campaign).

Wiper is a class of malware that wipes the drives/data of the computer it infects.

No purpose to this other than to be mean. Unless its a critical/important system – in which case the purpose can be to completely wipe out a business, collapse public infrastructure, or death.

Cryptominer malware is a new phenomenon which is designed to take over another systems resources for the costly business of mining cryptocurrency (see: bitcoin).

This is actually very commonly associated with the monroe cryptocurrency.

Grayware is the software on your devices that you don't want on your system but is there anyway. It's not technically harmful but it's really annoying (and can affect performance of your system and can introduce security risks)

Grayware includes bloatware, which is the software that comes pre-installed on you devices that you're not allowed to uninstall.

Adware is a type of trojan horse that collects info about you and your system for marketing purposes and displays adverts based on that info.

Adware can be benign – the user might've even consented to its presence. Symantec defined three levels of adware. The first is low severity (the adware that simply displays ads and does not transmit any information to a third party). Then there's medium severity (the type that transmits low risk information such as location and may display ads based on that low risk information). The worst type is high severity (this type of adware will transmit high risk information and will use it to tailor ads. And since they already don't respect your boundaries, you can be pretty sure they'll be aggressive about displaying those ads).