IT Documentation
What is malware?

Author: John Glynn
Date: 16th November 2016

Malware (short for "malicious software") is a file or code, typically delivered over a network that infects, explores, steals or conducts virtually any behaviour an attacker wants. Though varied in type and capability, malware commonly aims to achieve one of the following objectives:

- Provide remote control for an attacker to use an infected machine
- Collect and steal sensitive data
- Send spam from the infected machine to unsuspecting targets
- Investigate the infected user's local network

Malware is an inclusive term that covers all types of malicious software that includes, but is not limited to:

- **Viruses** – programs that copy themselves throughout a computer or network. Viruses piggyback themselves on existing programs and can only be activated when the user opens the program. At their worst, viruses can corrupt or delete computer data, use the user's email to spread, or erase everything on a hard disk.

- **Worms** – a self-replicating virus that exploits security vulnerabilities to automatically spread itself across computers and networks. Worms do not attach themselves to existing programs or alter files like many viruses. They are typically unnoticeable until replication reaches a scale that consumes significant system resources or network bandwidth.

- **Trojans** – malware disguised in what appears to be useful, legitimate software. Once activated, it will conduct any given form of damage it has been programed to carry out. Unlike viruses and worms, Trojans do not replicate or reproduce through infection. The name "Trojan" alludes to the mythological stratagem of special Greek forces hidden inside a wooden Trojan horse which was deceptively delivered as a gift to the enemy city of Troy.

- **Rootkits** – programs that provide privileged (root-level) access to a computer. Rootkits vary and hide themselves in the operating system.

- **Remote Access Tools (RATs)** – software that allows a remote operator to control the system. Originally built for legitimate use, but now used to control target computers. RATs enable administrative control, allowing the attacker to do almost anything on the infected computer. They are also difficult to detect, as they don't typically show up under lists of running programs or tasks, and its actions are often mistaken to be actions by legitimate programs.

- **Botnets** – short for "robot network," botnets are essentially networks of malware. Each botnet is composed of scores of unwittingly infected computers under the control of a single attacking party using Command and Control servers. They are very versatile (multi-functional), adaptable (updateable), and maintain resilience through the use of multiple redundant servers, and by utilizing infected computers to relay traffic. Botnets are often the army behind today's distributed denial of service attacks (DDoS)

- **Spyware** – malware that collects information about the usage of the infected computer and communicates it back to the attacker. The term spyware includes botnets, adware, backdoor behaviour, key loggers, data theft, and net-worms.

- **Polymorphic malware** – any of the above types of malware that has the capacity to change ("morph") regularly, changing the appearance of the code, but retaining the algorithm within. The alteration of surface appearance of the software, subverts detection via traditional virus signatures.