MALWARE GLOSSARY

Adware

Bombards the user with unwanted ads that pop-up onscreen and can be difficult to close, changes the browser homepage, slows computer performance / internet connection, adds new toolbars / plugins / extensions without consent or redirects to advertising pages. Potentially, ads could act as Spyware.

Botnet

Malware that links many internet connected devices together to perform a collective task. With the criminal in control of every infected device, they are capable of taking down websites through Distributed Denial of Service (DDoS) attacks, sending scam campaigns to millions, and other cyber criminal activity.

Keylogger

Records everything that is typed into the computer keypad. Cyber criminals use this method to capture confidential information, such as passwords, banking information, personally identifiable information, etc.
A keylogger can be a hardware device, which is why equipment should never be left unattended.

Malvertising

Spreading malware through online advertisements. Disguised as a genuine ad, it goes through normal advertising networks to display on legitimate websites used everyday. It could appear in the form of an alert or a great offer, something tempting to entice a user to click. Nevertheless, the malware gets onto the system by exploiting vulnerabilities.

Ransomware

Locks the user out of the device or file systems, holding them to ransom. There will be a threat of deleting or revealing the information or permanently locking the user out unless payment is made. It is not always guaranteed that the information will return, should the demand be met.

Rootkit

Hidden deep within the device, rootkits have the ability to work in the background and may go unnoticed for a very long time. They contain a collection of malicious tools to carry out various tasks. Stealing information and passwords, remotely accessing the device, corrupting the Operating System and processes, infecting genuine computer programs, releasing other forms of malware, and more. With privileged access they can have complete control of the system.

Scareware

Often a convincing alert that scares a user into thinking there is a problem with their device and manipulates them into downloading a malicious program to 'fix it'. These programs may even come at a cost, revealing banking information. Remain vigilant for fake pop-up security alerts from what appears to be a genuine source.

Spyware

Secretly monitors user activity, gathering information such as passwords, bank details, personally identifiable information, browsing habits, etc. Occasionally this information is sold onto third parties. Adware and Keyloggers are forms of spyware.

Trojan

Malware hidden in what appears to be a legitimate program, deceiving users into thinking it is genuine so that it gains access to systems. It can open backdoors into the device, allow criminals to take control, steal information, facilitate other malware and cause further damage.

Virus

A virus needs to attach to a host (such as a document) in order to be transported to a victim. Human interaction activates the malware (e.g. by clicking on infected files). Once activated, it has the capability of copying itself and can spread across the network. It corrupts the targeted device, destroys files, steals information, facilitates further attacks, and more.

Worm

Has the ability to copy itself and spread across networks, without any human action. There is no need for it to attach to a host (such as a document). Spreading from computer to computer, exploiting vulnerabilities, it increases the scope of the damage. It can facilitate further attacks or aim to deplete system resources.

PDSC
POLICE DIGITAL SECURITY CENTRE

www.policedsc.com