Technology Definitions

- **MSP** – A Managed Service Provider (MSP) is a company that manages information technology services for other companies via the Web. An MSP client may use internal operations or an ASP to run its business functions.
- **ASP** – Application Service Provider (ASP) is an enterprise that delivers application functionality and associated services across a network to multiple customers.
- **RMM** – A Remote Management and Monitoring (RMM) is a collection of information technology tools that are loaded to client workstations and servers. These tools gather information regarding the applications and hardware operating in the client's location as well as supply activity reports to the IT Service provider. The RMM is the proactive, remote tracking of network and computer health. It helps to enhance the overall performance of present technical support staff and take advantage of resources in a much better manner.
- **Server** – Is a computer program or a device that provides functionality for other programs or devices, called "clients". This architecture is called the client-server model, and a single overall computation is distributed across multiple clients, and a single client can use multiple servers. A client process may run on the same device or may connect over a network to a server on a different device. Typical servers are database servers, file servers, mail servers, printer servers, web servers, game servers, and application servers.
- **Network** – A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users.
- **Antivirus** – Also known as anti-malware software, is a computer software used to prevent, detect and remove malicious software (also known as malware). Originally developed to detect and remove computer viruses, it now protects from malicious browser helper objects (BHO), browser hijackers, ransomware, keylogging, rootkits, trojan horses, worms, LSPs, dialers, fraud tools, adware, and spyware. Antivirus also protects from malicious URLs, spam, scam, phishing attacks, online identity, online banking attacks, social engineering techniques, advanced persistent threat (APT), and botnet DDoS attacks.
- **Malware** – Any software used to disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising.
- **Ransomware** – A type of malicious software designed to block access to a computer system until a sum of money is paid.
- **Trojan Horses** – Any malicious computer program which misrepresents itself as useful, routine, or interesting in order to persuade a user to install it. Trojans breach the security of a computer system while seemingly performing some harmless function.
- **Rootkit** – Is a malicious software designed to enable access to a computer or areas of its software that would not otherwise be allowed (for example, to an unauthorized user) while at the same time masking its existence or the existence of other software.
- **Keylogging** – The use of a computer program to record every keystroke made by a computer user, especially in order to gain fraudulent access to passwords and other confidential information.
- **Worm** – A standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program.

- **Adware** – Any software that automatically displays or downloads advertising material (often unwanted) when a user is online.
- **Spyware** – Any software that enables a user to obtain covert information about another's computer activities by transmitting data covertly from their hard drive.
- **Spam** – Unsolicited e-mail, or junk mail.
- **Phishing** – The fraudulent practice of sending emails disguised to be from a trustworthy company in order to persuade individuals to reveal personal information, such as passwords, credit card numbers, and sometimes money.
- **APT** – Otherwise known as an Advanced Persistent Threat, is a set of stealthy and continuous computer hacking processes, often orchestrated by users targeting a specific entity. An APT usually targets organizations and/or nations for business or political motives. APT processes require a high degree of covertness over a long period of time.
- **Malicious URL** – A URL created with malicious purposes, among them, to download any type of malware to the affected computer, which can be contained in spam or phishing messages, or even improve its position in search engines using Blackhat SEO (Search Engine Optimization) techniques.
- **Browser Hijackers** – A form of unwanted software that modifies a web browser's setting without a user's permission, to inject unwanted advertising into the user's browser. A browser hijacker may replace the existing home page, error page, or search page with its own. These are generally used to force hits to a particular website, increasing its advertising revenue.
- **Fraud Tools** – Any malicious program that is used to take or alter electronic data, or to gain unlawful use of a computer or system.
- **LSP** – A Layered Service Provider (LSP) is a deprecated feature of the Microsoft Windows Winsock 2 Service Provider Interface (SPI). A LSP is a DLL, or file extension, that uses Winsock APIs to attempt to insert itself into the TCP/IP protocol stack. Once in the stack, a Layered Service Provider can intercept and modify inbound and outbound Internet traffic. It allows processing of all the TCP/IP traffic taking place between the Internet and the applications that are accessing the Internet (such as a web browser, the email client, etc.). For example, it could be used by malware to redirect web browsers to rogue websites, or to block access to sites like Windows Update. Alternatively, a computer security program could scan network traffic for viruses or other threats. The Winsock Service Provider Interface (SPI) API provides a mechanism for layering providers on top of each other. Winsock LSPs are available for a range of useful purposes, including parental controls and Web content filtering. The parental controls web filter in Windows Vista is an LSP. The layering order of all providers is kept in the Winsock Catalog.
- **Botnet DDoS** – A botnet is a number of Internet-connected devices used by a botnet owner to perform various tasks. Botnets can be used to perform Distributed Denial of Service (DDoS), steal data, send spam, allow the attacker access to the device and its connection. The owner can control the botnet using command and control (C&C) software. The word botnet is a combination of the words robot and network. The term is usually used with a negative or malicious connotation.
- **DDoS** – Distribution Denial of Service (DDoS) is a cyber-attack where the perpetrator uses more than one unique IP address, often thousands of them. An advanced persistent DoS is more likely to be perpetrated by an APT.