Cybersecurity and Botnets

Kazi Sayeda Momtaz
Computer System Analyst, Roads and Highways Department

Cybersecurity

Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, security includes both cybersecurity and physical security.

Cybersecurity means protecting information and systems from major cyber terrorism, cyber warfare, and cyber espionage Cybersecurity is therefore a critical part of any governments' security strategy.

Ensuring cybersecurity requires coordinated efforts throughout an information system. Elements of cybersecurity include:

Application security
Information security
Network security
Disaster recovery / business continuity planning
Operational security
End-user education

Information security (infosec)

Information security (infosec) is a set of strategies for managing the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information. Infosec responsibilities include establishing a set of business processes that will protect information assets regardless of how the information is formatted or whether it is in transit, is being processed or is at rest in storage.

Computer security

Computer security, also known as cyber security or IT security, is the protection of computer systems from the theft or damage to the hardware, software or the information on them, as well as from disruption or misdirection of the services they provide.

Cyber Terrorism

Cyber terrorism is the disruptive use of information technology by terrorist groups to further their ideological or political agenda. This takes the form of attacks on networks, computer systems, and telecommunication infrastructures.

Cyber Warfare

Cyber warfare involves nation-states using information technology to penetrate another nation's networks to cause damage or disruption. Cyber warfare has been acknowledged as the fifth domain of warfare (following land, sea, air, and space). Cyber warfare attacks are primarily executed by hackers who are well trained in exploiting the intricacies of computer networks and operate under the auspices and support of the nation-states. Rather than "shutting down" a target's key networks, a cyber warfare attack may intrude networks for the purpose of compromising valuable data, degrading communications,impairing infrastructural services such as transportation and medical services, or interrupting commerce.

Cyber Espionage

Cyber espionage is the practice of using information technology to obtain secret information without permission from its owners or holders. Cyber espionage is most often used to gain strategic, economic, political, or military advantage. It is conducted through the use of cracking techniques and malware.

With cyber threats in a state of rapid and continuous evolution, keeping pace in cybersecurity strategy and operations is a major challenge to governments. Cybersecurity is a serious concern to private enterprise as well, given the threat to intellectual property and privately-held critical infrastructure. Advisory organizations such as The National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO) have recently updated guidelines to promote a more proactive and adaptive approach that prescribes continuous monitoring and real-time assessments. These guidelines are expatiated on in the NIST 800 and ISO 27002 publications.

Botnets

A bot is a piece of malware that infects a computer to carry out commands under the remote control of the attacker. Bots are difficult to detect and allow attackers to control the infected computer without the owner's knowledge or consent.

A **botnet** (short for "robot network") is a network of computers infected by malware that are under the control of a single attacking party, known as the "bot-herder." Each individual machine under the control of the bot-herder is known as a bot. From one central point, the attacking party can command every computer on its botnet to simultaneously carry out a coordinated criminal action. The scale of a botnet (many comprised of millions of bots) enable the attacker to perform large-scale actions that were previously impossible with malware. Since botnets remain under control of a remote attacker, infected machines can receive updates and change their behavior on the fly. As a result, bot-herders are often able to rent access to segments of their botnet on the black market for significant financial gain.

Common botnet actions include :

* Email
* Distributed denial-of-service (DDoS) attacks
* Financial breach
* Targeted intrusions

Botnets are created when the bot-herder sends the bot from his command and control servers to an unknowing recipient using file sharing, email, or social media application protocols or other bots as an intermediary. Once the recipient opens the malicious file on his computer, the bot reports back to command and control where the bot-herder can dictate commands infected computers. Below is a diagram illustrating these relationships:

A number of unique functional traits of bots and botnets make them well suited for long-term intrusions. Bots can be updated by the bot-herder to change their entire functionality based on what he/she would like for them to do and to adapt to changes and countermeasures by the target system. Bots can also utilize other infected computers on the botnet as communication channels, providing the bot-herder a near infinite number of communication paths to adapt to changing options and deliver updates. This highlights that infection is the most important step, because functionality and communication methods can always be changed later on as needed.

As one of the most sophisticated types of modern malware, botnets are an immense cyber security concern to governments, enterprises, and individuals. Whereas earlier malware were a swarm of independent agents that ▸

simply infected and replicated themselves, botnets are centrally coordinated, networked applications that leverage networks to gain power and resilience. Since infected computers are under the control of the remote bot-herder, a botnet is like having a malicious hacker inside your network as opposed to just a malicious executable program.

Malware (short for "malicious software") is a file or code, typically delivered over a network that infects, explores, steals or conducts virtually any behavior 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 * Worms
* Trojans * Rootkits
* Remote Access Tools (RATs)
* Botnets * Spyware
* Polymorphic malware
* SPYWARE

Spyware is a type of malware (or "malicious software") that collects and shares information about a computer or network without the user's consent. It can be installed as a hidden component of genuine software packages or via traditional malware vectors such as deceptive ads, websites, email, instant messages, as well as direct file-sharing connections. Unlike other types of malware, spyware is heavily used not only by criminal organizations, but also by unscrupulous advertisers and companies who use spyware to collect market data from users without their consent. Regardless of its source, spyware runs hidden from the user and is often difficult to detect, but can lead to symptoms such as degraded system performance and a high frequency of unwanted behavior (pop-ups, rerouted browser homepage, search results, et cetera).

Spyware is also notable for its networking capabilities. Using an infected system to find information is of little value if the spyware can't deliver that information back to the attacker. As a result, spyware employs a variety of techniques to communicate back to an attacker in a way that will not cause suspicion or generate attention from network security teams.

As a tool for advertising, spyware is used to collect and sell user information to interested advertisers or other interested parties. Spyware can collect almost any type of data including web browsing habits and download activity. Perhaps the greatest concern related to spyware is that—regardless of whether it's presence detectable or not—the user has neither any idea of what information is being captured, sent away, or used, nor any mechanism or technology for finding out.

Spyware can use keyloggers to obtain personal details such as the user's name, address, passwords, bank and credit information, and social security information. It can scan files onto the system's hard drive, snoop other applications, install additional spyware, read cookies and modify the system's internet settings and dynamically linked libraries (DLL). This can result in lowered security settings (to invite in more malware), and malfunctions on the Internet and computer varying from numerous pop-up advertisements, whether on or offline, to connectivity failures sourced deep in the Internet settings of the system. Many of these changes are difficult to reverse or recover from without reimaging the affected device.

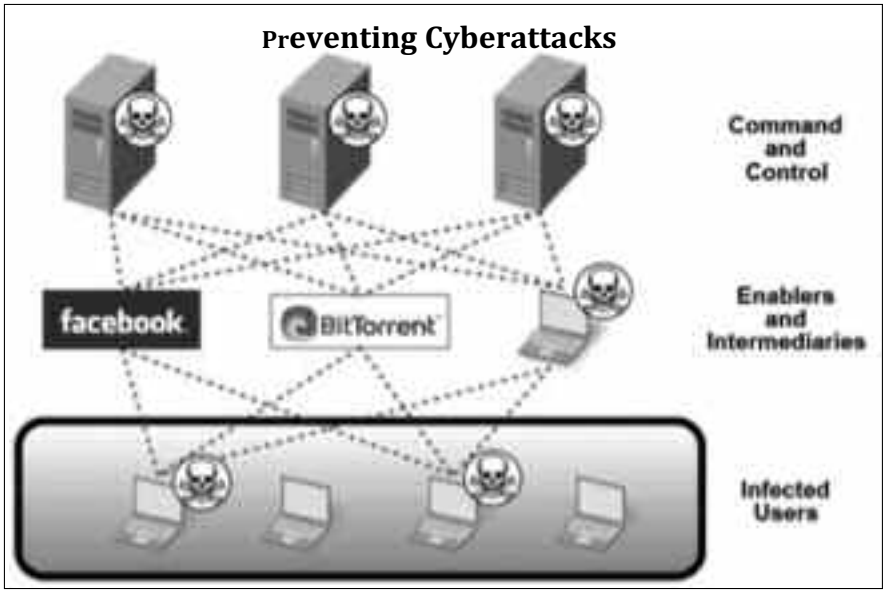
In addition to the stated threats that spyware pose to infected computers, it can also be a major consumer of system resources, often hogging up processor power, RAM, disks, and network traffic. The resulting performance degradation can lead to crashes or general system instability. Some spyware even disable or eliminate competing spyware programs, and can detect and intercept the user's attempts to remove it.

Spyware can be prevented through a combination of end-point and network security controls. Antispyware features are often integrated into modern antivirus software products that provide protection at the end-point. Given the need for spyware to communicate over the network, spyware is also increasingly being controlled at the network security layer, where spyware communications can be detected and blocked. Additionally, drive-by download protections can be enforced at the end-point by using the browser's pop-up blocker as well as via next-generation network controls that prevent the download of files without the user's consent Lastly, it is important to be monitor and validate which software components, plug-ins and services are allowed to run on a device as well as on the network; if the software is not recognizable or there is no specific reason to trust it, it is safer not to accept it until conducting further research.

Preventing Successful Cyberattacks

The downside of the ever-decreasing cost of computing power is the ability for cyber criminals and adversaries to launch automated and sophisticated attacks at lower and lower costs. It is now cheaper than ever to conduct successful cyberattacks, which has led to an onslaught of malicious activity against organizations, threatening the foundations of trust in digital systems critical to business operations and innovative advantage.

The end goal of security is to enable your operations to flourish and keep your organization out of the headlines associated with cyber breaches. This means reducing the likelihood of a successful attack. By focusing on prevention, the Palo Alto Networks Next-Generation Security Platform reduces cybersecurity risk to a manageable degree, allowing organizations to compartmentalize their most serious threats and focus on business operations ■



Reference: wikipedia