CYBERSECURITY

Information Sheet
Host Threats

Tags: Cybersecurity, Attack Vectors, Threats, Malware, Passwords

365 ARCHITECHS

Host threats are attack vectors that involve an attack a device, otherwise known as an endpoint. Other types of threats include network threats, application threats and social engineering.

This information sheet considers the different types of host threats that threat actors use to gain access to systems to steal information, harm reputations or disrupt operations.

Malware

Malware, or malicious software, is a program that seeks to take partial control of a computer or device. It can interfere with normal functioning by affecting the operation of, or data contained within the system.

Adware is software that attempts to disguise itself as legitimate software, that shows advertisements trying to entice the user into install a program, often from within a browser.

Spyware is software that observes activity without permission and reports it to others.

Viruses are types of malware that attach themselves to other software, that attempt to infect other software when executed.

Worms are similar to viruses, in that they seek to self-replicate over computer networks.

Trojans are designed to appear to be something useful in order to trick the user into running them. Once executed, trojans gain access to the infected device and can search for vulnerabilities or install other malware.

Ransomware encrypts data so that users are no longer able to access their files. This malware typically offers a way for a payment to be made to cybercriminals to provide an encryption key to decrypt and gain access to files again.

Rootkits infect the start up processes of the computer, attempting to provide attackers with administrator privileges on the infected system. This can effectively bypass many defences rendering devices open to other forms of attack.

Drive by Attacks occur when users access compromised websites. When opening an infected web page, browsers can download and execute malicious code that scans for vulnerabilities and infects devices. Users do not need to click on links for their systems to become infected.

Keyloggers

Keyloggers record user keystrokes and send them to attackers. Keystrokes can include usernames, passwords, credit card details and other highly personal and sensitive information.

Keyloggers may be hardware devices that are physically connected between a keyboard and a computer, devices that sniff the Bluetooth or Wifi traffic of a connected keyboard, or malware on an infected device.

Password Attacks

Once the standard way to protecting access to a system, passwords are little defence to cybercriminals of today.

Dictionary attacks attempt to guess easy passwords by trying common words and phrases.

Brute force attacks use speed to repeatedly guess passwords by way of an automated process of trying every combination of characters that can be used in a password.

About us
365 Architechs is a technology company based in Brisbane, Australia. We deliver solutions to support organisations on their digital transformation including cloud, modern applications, cybersecurity and artificial intelligence to drive profitability, growth and achievement of strategic objectives.
(07) 3393 1186 | www.365a.com.au | sales@365a.com.au