THE CYBER ECOSYSTEM + IP RESOURCES

A holistic view of the cyber ecosystem must be brought into the discussion

TOP 6 WAYS CYBER CRIMINALS ATTACK

HOW ADVERSARIES ENTER & EXPLOIT YOUR SYSTEM

ÄÁ A BROWSER

Web-based attack, A Browser serves as a heavily targeted segment and pathway of the attack surface and is often misused by the Abusers of Internet Protocol Resources to breach a system (examples: Crytojacking, XXS, plugins and Add-ons).

ÅÁ A LINK

A hyperlink is a unidirectional (moving or operating in a single direction) link connecting two different entities, meaning upon clicking a link the Users of Internet Protocol Resources, will leave their current website and travel to another location. An interface that links a source to a target, like a hypertext, URL, document, PDF, phrase, embedded image or even malicious code, that by clicking, the user triggers the operation. It is not the link itself that can infect your device, however it's the activity (content) that is downloaded and rendered from the link.

ÆÁ AN ATTACHMENT

An Attachment (file, program, or code) can be defined as an extra part or extension that is or can be attached to something to perform a particular function, while malware is software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system. Together, as a malicious attachment, a malware laced file, program or code can be used to deliver a dangerous payload (Malware) in multiple ways across the attack surface.

ÇÁ SOCIAL ENGINEERING

According Europol Social Engineering is a cross-cutting attack vector that remains a top threat to facilitate other types of cybercrime. Social engineering is an age-old threat, that has only expanded in the cyber world and continues to play a significant role in successful attacks against people, enterprises, and agencies.

ÈÁ AN INSIDER

According to NIST an Insider Threat (person or process) is the threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm or damage through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of departmental resources or capabilities.

ÉÁ SCANNING RECONNAISSANCE & EXPLOITATION

Web application/injection attacks. Scanning and Reconnaissance Exploitation (Triad), it's means, methods, ways, routes, processes or measures (how the attacker gains initial access) on how the Abusers of Internet Protocol Resources may use Scanning and Reconnaissance Exploitation to initially access your device, network, or enterprise system. Scanning can be defined as to look, sweep, search or cause a surface, object, or part to be traversed. While Reconnaissance is the observation of what you find, and Exploitation is gaining authority or taking advantage of a system.

Listcrime.com