The Logic Behind ACSIA XDR Plus and its Technology

"If they can't find you, they can't attack you"

"A thousand battles, a thousand victories. The supreme art of war is to subdue the enemy without fighting. Victorious warriors win first and then go to war, while defeated warriors go to war first and then seek to win. Invincibility lies in the defence; the possibility of victory in the attack"

- Sun Tzu

Preamble

There are as many perpetrators behind cyberattacks as there are reasons and objectives behind them. The diversity and implications of a successful cyberattack will vary depending on the data asset that is being illegally accessed, and the objective of the perpetrator. The following is a list of some of the most common commercial cyber exploits, the implication of which will vary considerably from organisation to organisation.

- Compromise a system to steal targeted data (Customer data, IPR, HR files ….etc)
- Compromise a system to change data or content
- Compromise a system to implant malware
- Compromise a system to encrypt data for a ransom payment
- Compromise a system to use as proxy to attack some other organisation
- Compromise a system to use compute resources such as Bitcoin miner
- Compromise a system to sleep and activate at another time
- And many more…

The time taken to identify and correct some of the larger and more sophisticated cyber attacks in an organisation is generally measured in Months to Years, so clearly the implication in terms of reputational damage, regulatory infringement, potential lawsuits and loss of shareholder value is enormous.

How do cyber criminals plan their attacks?

It is important to note that the proliferation of new tools and techniques available to cyber criminals over the past ten to fifteen years has vastly outpaced the response of the cybersecurity industry to provide strong, functional and cost effective solutions that protects the data assets of an organisation.

There are two broad methods used by cyber criminals to attack IT systems as follows:

- Cyber attacks manually performed by an actual human/individual
- Cyber attacks using automated software such as BotNet's

Some characteristics of manual cyber attack

Manually performed cyberattacks are extremely time consuming and require significant effort as well as expertise. These are often performed by rank amateurs who are learning cyberattack techniques, but also by professional and experienced cyber criminals who use the full range of tools and technologies to obfuscate and evade whatever security precautions have been implemented. These criminals can be highly motivated with specific motivational intent, making them a very serious security threat without a strong multi-dimensional defence capability.

A typical manual attack begins with information gathering and reconnaissance, so-called, pre-attack phase (see Mitre Att&ck framework for instance). It is a phase where the attacker is trying to get as familiar as possible with the targeted infrastructure, profiling weaknesses before moving onto the attack stage. The information gathering exercise collects what in isolation is a completely harmless piece of information that is publicly available from web servers and perimeter Network devices in every organisation. Many organisations rely on this type of publicly available information to conduct their legitimate business (a typical digital marketing organisation would query similar data for their lead generation and marketing ...), so in isolation this information does not represent an actual attack, but it is an essential step for a cyber attacker to complete before executing their attack strategy.

Once as much publicly available information has been collected and the attacker has enough information to get to know the targeted asset, the next step is to proceed with a vulnerability assessment where weaknesses can be revealed. To do this an attacker uses tools such as vulnerability scanners some of which can be very aggressive and noisy if used by inexperienced individuals, but if the attacker is experienced, they can be fairly silent and seamless.

Once vulnerabilities have been identified, the next phase is the exploitation phase where the attacker attempts to deliver payloads. The exploitation phase is very intrusive and for an experienced hacker who has identified vulnerabilities, there is a high possibility that they will succeed in compromising the data assets within an organisation.

Some characteristics of Botnet cyber attack

Automated cyberattacks using Botnets are performed pretty much the same way as manual attacks, except that the whole process is automated and can be launched instantaneously. This type of attack may not have the same motivational intent as that of an experienced cybercriminal manually targeting an organisation, but they do represent a real and present danger to all organisations with a digital presence. BotNets are sophisticated and smart, heavily weaponized and many of the newer deployments come with ML/AI capabilities to bypass cyber defence systems.

What do Manual and Botnet cyberattacks have in common?

It would be highly irregular for a cybercriminal to bypass the data gathering phase of an attack as it would be a very ineffective way of performing an attack (it would be the equivalent of driving a car in a new city whilst blindfolded). It is of paramount importance for cyber criminals to perform an information gathering process first, prior to planning their strategy and attack the Digital assets in an organisation.

ACSIA XDR Plus Core Logic

The core design and implementation of ACSIA XDR Plus incorporates a Threat Intelligence feed which will ban malicious sources of exploits (IP Addresses, URL, sources of malware..etc) from being able to access an environment as well as Pre-Attack technology which identifies and prevents whenever being gathered in a pre-attack (intelligence gathering) phase. This intelligence gathering phase is necessary for a successful attacker to plan and successfully exploit vulnerabilities. ACSIA XDR Plus is designed to capture all queries used during the intelligence gathering exercise before applying smart correlation and build patterns which enables ACSIA to predict and prevent the next steps that the cybercriminal is going to perform. Unlike other products in the market, ACSIA incorporates offensive armoury that will proactively stop a potential threat before they become an actual threat i.e. before it reaches the attack phase.

ACSIA also implements advanced defensive features which will detect exploits being performed in real-time where Predictive and Pre-attack technologies may have been bypassed (an example of which may be a compromised password being used to gain access ...etc).

Such exploits will attempt to access data which would be anomalous to the users typical behaviour or will attempt to inject or modify data through the use of malicious tools, both of which are rigorously monitored and detected by ACSIA. We also monitor Kernel activity for forensic analysis to detect and prevent zero-day compromise attacks.

More information on ACSIA can be found using the following link: ACSIA documentation
Contact us: email sales@dectar.com,