4SECURITAS

PROTECTING YOUR DATA ASSETS

Product Overview

ACSIA - SPOTTING & THWARTING ATTACKS

BEFORE YOUR ORGANISATION IS COMPROMISED

INTRODUCTION

Cyber attacks are carried out for many reasons, and have different objectives and purposes. A typical attack could compromise the system to:

- implant malware
- encrypt data and ask for a ransom
- steal relevant data
- use it as proxy to attack another organisation
- use it compute resources as bitcoin miner
- attack and access a partner's digital asset
- gather users' credentials and use them elsewhere.

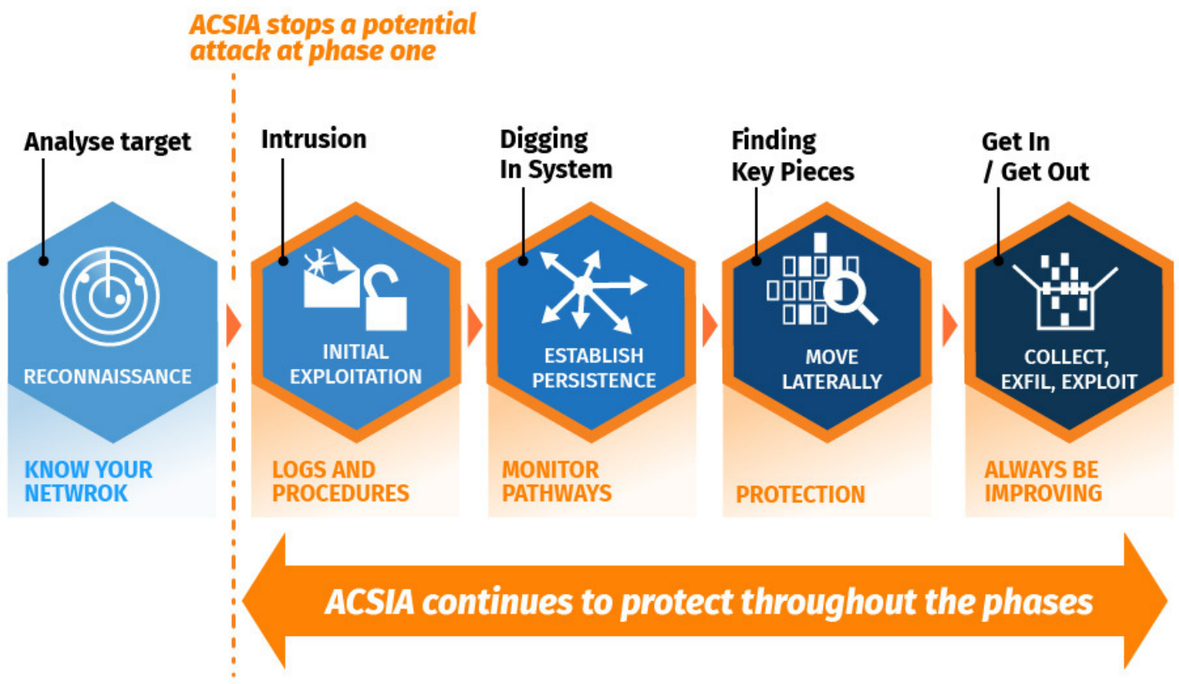
The list goes on....

THE CYBER ATTACK PROCESS

Hacking into a system is done either manually (performed by an **actual human/individual**) or by using automated software such as **BotNets.**

The process
Manually performed cyberattacks are extremely time consuming and require significant effort and expertise.

1. Typically attackers begin with information gathering and reconnaissance, the so-called **pre-attack phase** (see Mitre Att&ck framework, for instance). The attacker is trying to get as familiar as possible with the targeted infrastructure in order to identify weaknesses. The information gathering phase is completely harmless - it is just collecting data that is publicly available and provided by IT systems. It is NOT an actual attack. Even a typical digital marketing organisation would query similar data on businesses for their lead generation and marketing, etc..



2. Once the relevant information has been collected and the attacker knows the targeted asset, the next step is to proceed with a **vulnerability assessment** to reveal weaknesses. To do this an attacker avails of tools such as vulnerability scanners. These can be very aggressive and noisy but, if the attacker is experienced, they can be fairly silent and seamless.

3. Now the vulnerabilities are known, next is the **exploitation phase**. The attacker starts to perform *payloads (the component of the attack which causes harm to the victim).* This is the most dangerous stage - it is very intrusive and there is a high possibility that the attacker will succeed in breaking into a digital asset chosen as a target.

4. Finally, the payload is deployed, and **the system is compromised**.

Automated cyber attacks are performed much the same way as manual ones with the only exception that this whole process is automated and it can be done at a glance instantly. Recent BotNets are very sophisticated and fairly smart, heavily weaponised, and some come with Machine Learning/AI capabilities to bypass cyber defence systems.

Attacks (manual or automated) are highly unlikely to start at the exploitation phase, i.e., without preliminary study and information gathering. It would be a very ineffective way of performing an attack, which would likely be unsuccessful. The information gathering process is paramount for the attacker - it's how they collect relevant information to get to know the asset.

ACSIA'S CORE LOGIC

*ACSIA is designed and implemented in such a way that it will identify wherever and wherever data is being queried in the **information gathering phase** (when the attacker getting familiar with the target asset).*

*This is the type of information necessary for an attacker to break into a system, **but no harm has yet been done (it's literally "pre-attack").***

*ACSIA is a "smart solution". Once it spots data is being queried it **intelligently anticipates and predicts** the next steps the attacker is going to perform.*

The attacker will not be able to gather enough information to successfully reach the exploitation phase, and so attempts to deploy malware are thwarted.

Therefore ACSIA has the ability to proactively stop a potential threat before it becomes an actual attack.

It is simple as that.

ACSIA will never allow anyone to get close to the attack phase, stopping the potential attack in its preliminary phase. This is the very basic logic on which ACSIA is built and designed.