WHITE PAPER

KNOW HOW YOUR ADVERSARY THINKS

CYBERSECURITY.
EVOLVED.

SAPIEN

SAPIEN

THE EVOLVING THREAT

A new class of cyber threat has been evolving over the last decade or so to now represent a well-resourced and highly trained class of adversary. Dubbed "Advanced Persistent Threats" (APTs), these adversaries conduct long-term intrusion campaigns targeting highly valuable and nationally sensitive critical infrastructure with the intent to overcome most conventional computer network defence mechanisms.

Conventional network defence tools such as anti-virus pre-empt an attack and utilise information on known vulnerabilities to secure a network. Whilst these traditional approaches are important mechanisms to detect and prevent an attack, there are now certain adversaries armed with advanced tools, techniques and resources, which, when combined with intent, allow for a relentless and sophisticated attack on targets.

Understanding the "Kill Chain Model" that describes the phases of an intrusion enables a state of information superiority to be achieved by the defender which can reduce the likelihood of a successful intrusion. This includes mapping adversary kill chain indicators, linking the indicators to a course of action, identifying patterns to the intrusions, linking to broader campaigns and developing an iterative approach to intelligence gathering and interpretation.

TRADITIONAL SECURITY MEASURES ARE NOT ENOUGH

Many organisations are still relying on traditional IT protection technologies and processes to mitigate risks associated with automatic viruses or worms. These tools do not protect against a persistent threat actor who can manually adapt and respond in order to modify the behaviour of their intrusion mechanism.

THESE ATTACKS USED ADVANCED INTRUSION TECHNIQUES AND THE APTS DEMONSTRATED A LEVEL OF PATIENCE AND UNDERSTANDING ABOUT THEIR TARGETS TO HARVEST SENSITIVE INFORMATION.

Examples include various intrusions of US government agencies that were infiltrated prior to 2008 by APTs who were motivated by a desire to collect sensitive information. These attacks used advanced intrusion techniques and the APTs demonstrated a level of patience and understanding about their targets to harvest sensitive information. Such examples have shown that the typical approaches of anti-virus and patching are not sufficient protection mechanisms when the end user is targeted and threat actors are motivated to extract sensitive intellectual property.

ZERO-DAY VULNERABILITIES

A 'zero-day vulnerability' is a term used by security professionals to describe a vulnerability that is discovered by parties not invested in the protection of the network. These vulnerabilities present great threat to cyber security professionals as traditional pattern recognition detection systems are ineffective.

THE KILL CHAIN

A 'kill chain' model[1], developed by Lockheed Martin, is a systematic process used to target and engage an adversary to achieve a desired objective. It is defined within military doctrine as a process with the steps: find; fix; track; target; engage and assess. The steps allow an adversary to find targets, fix their location, track and observe, target with a suitable weapon, engage the adversary and assess the effects. A disruption in any one of the steps will break the chain and interrupt the entire process.

[1] Lockheed Martin, *The Cyber Kill Chain*, [online media], https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (accessed 7 August 2018).

SAPIEN

For computer network attacks or computer network espionage an intruder is attempting to develop a payload to breach a trusted boundary, establish a presence inside the trusted environment, move around within the environment or violate the confidentiality, integrity, or availability of a system within the environment. This cyber intrusion kill chain is defines as reconnaissance, weaponization, delivery, exploitation, installation, command and control and actions of objectives.

GAINING AN ADVANTAGE OVER AN AGGRESSOR

Sapien Cyber offers technology and experience that enables best practices of enterprise-wide patching and hardening to protect against any highlighted accessible vulnerabilities or existing insecurity indications. It's suite of cyber security technologies has been developed under the premise that an APT actor will continually adapt their capability in order to compromise a system using advanced tools, customised malware and 'zero-day' exploits that cannot be detected by simple defence mechanisms such as anti-virus. Sapien uses an intelligence-driven, threat-focused approach to analyse intrusions from an adversary's perspective. Each phase of the kill chain is deciphered for intrusions and actionable intelligence is delivered in accordance with the corresponding defence model.

SAPIEN USES AN INTELLIGENCE-DRIVEN, THREAT-FOCUSED APPROACH TO ANALYSE INTRUSIONS FROM AN ADVERSARY'S PERSPECTIVE.

The 'actionable intelligence' model provides organisations with a new defence mechanism that is constantly evolving to provide mitigations against intruders. It intelligently prioritises actions for new technology or processes to defeat an adversary. By using kill chain analysis the adversary can be defeated at any stage of the chain before they achieve their objectives. Just a single mitigation action in any phase of the kill chain is able to disrupt an adversary from moving through the entire chain which gives the defending organisation an advantage over the aggressor.

ACTIONABLE INTELLIGENCE

Enterprise defensive capabilities are enhanced by actionable intelligence that provides specific responses to an intruder that is taking discrete steps to target and infiltrate a network or system. Actionable intelligence allows cyber security defence that bases its security decisions and measurements on a deep understanding of adversary tools, tactics and behaviours.

The course of actions available to a defender during the various phases of the kill chain are broad. These include actions to detect, deny, disrupt, degrade, deceive and destroy. Sapien Cyber uses a system of systems approach to intrusion detection that provides actionable intelligence to passively detect exploits; provide patching recommendations to deny exploitation altogether and recommend data execution prevention to disrupt the exploit if it has initiated.

ZERO DAY ATTACKS

A defender's primary goal when facing persistent threats that continually adapt their operations over time is to have the highest level of resilience possible. The most notable 'adaptions' are events such as 'zero day attacks'. What is most notable about these so called 'zero day attacks' is that they all re-use observable tools or infrastructure in the various phases of the 'kill-chain'. Therefore, if an intruder deploys a zero-day exploit that uses an observable tool or infrastructure in the other phases, it can be detected by Sapien Cyber which renders any new improvement in the weapon as fruitless by deploying the actionable intelligence recommendations.

SAPIEN

DECONSTRUCTING INTRUSIONS

Most intrusions will provide a limited set of attributes that indicate the phase of the kill chain. Sapien Cyber uses experienced analysts to discover the other attributes for each phase to provide the maximum number of options for the defender to use. Traditional incident response occurs after the last exploit phase, highlighting that this approach leaves defenders at a significant disadvantage and responding too late. With actionable intelligence mapped to the kill chain and intrusions reconstructed at each phase of the kill chain, defenders are able to apply tools, technologies, and processes capable of responding to an intrusion before it is "too late".

SUMMARY

The prevalence of Advanced Persistent Threats necessitates the need for an intelligence driven network defence. Traditional, vulnerability focused approaches to these threats are now insufficient. Only by understanding the threat itself, its intent, its capability and patterns of operation can true resilience be created. This approach can spin the threat actor's persistence to now work against them. Turning their repeated actions into liabilities that decrease their likelihood of success with each intrusion attempt.

Sapien Cyber understands the nature of repetition used by threat actors. Be it out of convenience, preference or ignorance on the part of the adversary they will continue to re-use attack mechanisms. This allows threat intelligence to be gathered and used to gain information superiority for network defence.

CYBERSECURITY FOR OPERATIONAL TECHNOLOGY

INDUSTRIAL PLANTS /
PUBLIC INFRASTRUCTURE /
TRANSPORT SYSTEMS /
CRITICAL INFRASTRUCTURE NETWORKS /
UTILITIES /

EVOLVE WITH US | sapiencyber.com.au

SAPIEN CYBERSECURITY. EVOLVED.

Sapien Cyber Corporate Headquarters
Building 6, ECU, 270 Joondalup Drive
Joondalup, WA, Australia, 6027

1800 378 200
info@sapiencyber.com.au
sapiencyber.com.au