CYBER STASH

eclipse

The Case For Threat Intelligence To Defend Against Advanced Persistent Threats

An increasing number of organizations are being targeted by Advanced Persistent Threats (APTs). That is to say, stealthy, premeditated, methodical cyberattacks executed by well-funded, skilled and motivated threat actors who have capability and intent and utilize advanced attack techniques to maintain long-term access to their target's systems while pursuing their specific objective.

When failure is not an option for such motivated adversaries, do organizations really stand a chance of safeguarding their business and sensitive information?

Or is it now apparent that organizations must invest in defensive measures that utilize threat intelligence relating to APTs if they're going to have any hope at all?

If you're a decision maker, accountable or responsible for managing business risk and you believe that no level of defensive measures, or for that matter, threat intelligence, can prevent the inevitable, then you're 100% correct! What these countermeasures are supposed to do, however, is increase the likelihood of attacks being detected and therefore reduce risk to an acceptable level for your organization because they should be making it increasingly challenging for attackers to accomplish their objective. It's therefore less a matter of whether you will be hacked – because that's just a matter of time – but more about the number of times you will be hacked in a given period of time and your ability to detect and respond in time to prevent or reduce business impact.

As the decision maker, the questions you should be asking are:

1. What is the likelihood of my organization being targeted by an APT?

Symantec reports this to be roughly 4%. This number will vary, however, depending on your organization type and the type of organizations you conduct business with.

2. Does my organization need intelligence about APT groups?

Attributing the attack may not be important to many organizations, but we should remember that threat intelligence is foremost about providing the ability to detect threats and thereby reduce risk. Moreover, as APT techniques are likely to be adopted by conventional hackers, an organization can better defend itself by understanding them better.

When the stakes are so high, what matters is how we're able to inform risk management to disarm the instruments of power used against us to undermine our business credibility and resilience. Threat intelligence contributes to this. For cybersecurity defenses to be effective, they need to be layered and must therefore include threat intelligence. This, however, must be actionable and provide stakeholders with a high return on investment if they're going to maintain their level of relevance to business. Stakeholders should not be oversold, however. If threat intelligence cannot efficiently assist organizations to defend themselves against

To what extent, then, does threat intelligence provide information that informs our defensive capabilities against APTs and at what cost?

To accurately answer this, our security industry must drill-down and answer these four questions:

Accuracy of Attribution

How accurately does threat intelligence link threat actors to their operations?

Efficiency

How efficiently can threat intelligence related to APTs be operationalized?

Coverage

What percentage of current APTs and APT groups are likely to be discovered?

Value

What level of risk mitigation against APTs does threat intelligence provide and what's the Total Cost of Ownership (TOC) for the threat intelligence program?

Well-known APT groups and their preferred arsenal of Tactics, Techniques and Procedures (TTPs) provide us with a wealth of defensive information and the MITRE ATT&CK™ defines these in great detail. When we discover an APT, we not only learn about the TTPs they commonly use but can then use this information to predict how other attacks will form, whether these are APTs or simply opportunistic.

What then can be said about unknown APTs? Those that remain undiscovered? Can threat intelligence inform us about net-new attack-types if previous TTPs are not leveraged?

There are three cases to consider that we define in this paper as:

Mirror APTs

An APT group that leverages the exact TTPs as a well-known APT group and thus can continue to operate under a 'stolen' identity.

Deceptive APTs

A combination of Mirror and Undiscovered APTs where an APT group impersonates another APT group to cover its actual identity while using net-new tactics and techniques to accomplish its primary objective.

Undiscovered APTs

An APT group that leverages only attack types which are undiscovered. They use only net-new tactics and techniques.

When considering threat intelligence in its entirety, most of it, whether open-source or not, does not provide APT-related intelligence. Most of the IP addresses, hashes, URLs and domains that we associate with sources of threats, or the processes, registry changes and file paths that we use as Indicators of Compromise (IOCs) should in fact be classified as 'low-hanging-fruit' given they aren't strictly classified as being associated with APTs but are rather associated with opportunistic 'smash and grab' attacks without having a human adversary to meticulously coordinate the step-by-step actions and maintain long-term persistence.

We should, therefore, distinguish and separate the extent to which information we receive from threat intelligence sources informs us about APTs and to which extent about commodity attacks. While we must have defensive strategies for both categories, investment decisions should not be based on hype. Organizations should understand to what extent their organization is at a risk from each attack category and invest accordingly in defensive measures that are quantifiable so that threat intelligence maintains its relevance to risk management.

Application

It's important for organizations to understand the different use cases for threat intelligence and the cost-benefit of each. Depending on the organization's size and capability, threat intelligence can return cumulative degrees of value as organizations leverage it to deliver a greater number of use cases.

Organizations should tread carefully, however, and not try and implement all use cases as each one adds operational cost and resource overhead.

The table on the proceeding page shows the recommended use cases for threat intelligence, taking into consideration the likely capability and resources an organization would have based on the size of its security team and to what degree it's an APT target.

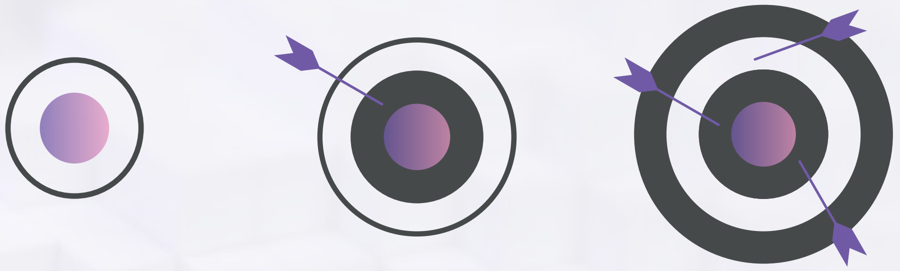
Organizations should consider their own business context, their ability to implement security orchestration and automation and the underlying technologies used, as these all play a large part in whether or not the use case can be implemented efficiently.

The assumption made for detective controls is that they are detective controls because they are prone to a greater number of false positives and would therefore not be suitable as a protective control. Furthermore, a higher level of resources and skills is going to be required to operationalize them because they need to be monitored, investigated and responded to in a timely manner.

.

EFFECTIVENESS/VALUE	Rating	Size of Organization’s Security Team					
	🟥 Low	Small to Medium Enterprise			Large Enterprise		
	🟪 Medium	Between 1 and 5 FTEs Dedicated to Security			With 6 or More FTEs Dedicated to Security		
	🟦 High						
	Considerations Degree of Risk Mitigation Control Prioritization Risk and Resource Optimization						
CATEGORY	Use Case	Low Risk Target	Medium Risk Target	High Risk Target	Low Risk Target	Medium Risk Target	High Risk Target
PROTECTIVE	🟦 Blocking IP Addresses, Domains and URLs at the Perimeter	🟦	🟦	🟦	🟦	🟦	🟦
	🟦 Blocking Processes, Files, DLLs on Endpoints			🟦		🟦	🟦
	🟪 Vulnerability Remediation Prioritization			🟪		🟪	🟪
	🟦 Using TTPs to Inform Protective Controls			🟦			🟦
DETECTIVE	🟪 Detecting IP Addresses, Domains and URLs at the Perimeter			🟪	🟪	🟪	🟪
	🟦 Detecting Processes, Files, DLLs on Endpoints			🟦		🟦	🟦
	🟦 Proactively Hunting for Indicators (Automated)		🟦	🟦		🟦	🟦
	🟥 Proactively Hunting for Indicators (Manual)						🟥
	🟪 Using TTPs to Inform Detective Controls					🟪	🟪
INVESTIGATION	🟪 Informing Incident Response			🟪	🟪	🟪	🟪
	🟥 Adding Context to Investigations				🟥	🟥	🟥
	🟥 Adding Context to Compromise Assessments			🟥		🟥	🟥
	🟪 Research to Informing Protective Controls (Predictive Intelligence)					🟪	🟪
	🟥 Research to Inform Detective Controls (Predictive Intelligence)						🟥
RESEARCH	🟥 Producing Trends and Reports to Inform Strategic Decisions			🟥		🟥	🟥
	🟪 Producing Trends and Reports to Inform Tactical & Operational Decisions					🟪	🟪
	🟥 Using Indicators to Track and Report on APT Campaigns						🟥
	🟦 Sharing Threat Intelligence on APTs					🟦	🟦
	🟥 Discovering New APTs (TTPs, Attribution and Motivation) and Following Existing Ones						🟥

Today, over 40 organization types are targeted by APT groups who are actively being tracked by several leading security research teams. The table below provides an indication of the level of risk your organiza-



Low-Risk Target	Medium-Risk Target	High-Risk Target
Trade and Commerce	Manufacturing Academic Research	Government Entities/
Software Companies	Activists	Defence/Military
IT Companies	Intelligence Agencies	Financial Institutions
Mass Media/Media	Private Companies	Healthcare
Critical Infrastructure	Organisations that form part of the supply chain or provide a service to High-Risk Targets such as MSPs.	Pharmaceuticals
Electronics Manufacturing		Geopolitical Diplomatic Entities
Construction Journalists		Telecommunication
		Higher Education
		High-Tech
		Energy/Utilities/ Petroleum Refining Chemicals Manufacturing/Mining
		Aerospace

Closing Remarks

Do organizations have adequate resiliency to survive an APT-based attack? An in-depth examination of the impact on the bottom line, brand and reputation of organizations hit by previous APT attacks is required to answer this question. These things, however, are certain:

Organizations should distinguish between APT and non-APT-based attacks and have a measurable risk mitigation strategy that defends against each type. If organizations are not a typical target of APTs, then investing in threat intelligence that helps detect APTs will not see a good return on their investment. Correspondingly, organizations that are a target, should study the actions of APTs and use this information to inform their defensive measures.

Threat intelligence should form part of the overall defense-in-depth strategy for all organizations, but for most organizations, the better value will be derived from threat intelligence that informs non-APT-based attacks. Government agencies, financial institutions and geopolitical diplomatic entities, are particularly targeted by APT groups and face the greatest risk.

No amount of threat intelligence can provide 100% coverage or attribution. We will increasingly see APT groups impersonating other APT groups because they understand only too well how our security industry leverages TTPs and other forms of threat intelligence to inform defensive measures. It's therefore expected that threat intelligence will provide a diminishing level of value to attribution. Nevertheless, organizations will continue to benefit from studying APTs, as their methods of attack will increasingly be leveraged by other forms of attack. Moreover, APT groups change constantly as their infrastructure and TTPs are discovered, and they develop new ones. In response, organizations with large security teams should follow APT groups and their campaigns in order to form an ongoing view of their profiles.

Whether or not your organization is at risk of an APT attack, the global average cost of all breaches for all attack types is what matters most and must be considered. Not being a typical target of an APT attack, does little to reduce the risk of a data breach to your organization. IBM estimates that 69% of all data breaches are executed by state actors or advanced criminal organizations and based on the Ponemon Institute's 2018 Cost of a Data Breach Study, the probability of an organization experiencing a data breach within a two-year period is 28%. That's 1 in 4 organizations being directly impacted with financial losses sustained as a result of a cyberattack. Organizations should therefore continue to establish business resilience regardless of their risk from APTs.

It's important to both effectively and efficiently operationalize threat intelligence as your organization looks to use it for its security practice. Bandura Cyber reports that 59% of organizations rate their threat intelligence effectiveness as only average or worse. To improve this position, threat intelligence should be used to prevent threats in-line and in real-time, and, proactive threat hunting should be automated. By doing so, your organization will simultaneously improve the program's effectiveness and greatly reduce the resource overhead necessary to maintain it and therefore reduce the total cost of ownership.

CYBER STASH

Explore

eclipse.xdr

To learn about how CyberStash operationalizes threat-intelligence to reduce risk for organizations, visit us at:

www.cyberstash.com

References:

- *https://www.symantec.com/*
- *https://www.fireeye.com/*
- *https://www.crowdstrike.com/*
- *https://enterprise.verizon.com/*
- *https://en.wikipedia.org/*
- *https://www.ibm.com/*
- *https://banduracyber.com/*