HITACHI
Inspire the Next

WHITE PAPER

Advanced Persistent Threats and the Case for a Security Intelligence and Response Program

Hitachi Systems Security Inc.

CONTENTS

INTRODUCTION

As the severity and sophistication of cyber attacks against Information and Communication Technology (ICT) infrastructure continues to impact business and government operations, new solutions are needed that will improve the ability to detect and respond. Computer Network Defence (CND) is the discipline of leveraging ICT capability to protect, monitor, analyze, detect, and respond to cyber attacks. Effective CND calls for decreasing the time from incident detection to response while preserving and providing sufficient information to human operators in order to review and influence automated defensive actions.

IT systems, including enterprise networks, are subject to an increased variety, volume, and sophistication of cyber-attacks from a variety of threat actors who benefit from unauthorized use, alteration, or intrusion into these networks. As threats have evolved, so too have the impetus and effort behind developing effective defenses and counter-measures.

> IT systems, including enterprise networks, are subject to an increased variety, volume, and sophistication of cyber-attacks from a variety of threat actors who benefit from unauthorized use, alteration, or intrusion into these networks.

Traditional IT security programs have often focused on threat avoidance rather than integrating technologies in the IT ecosystem to provide risk-driven decision-making and automated defence of critical assets. The failure to properly integrate operational scenarios and activities into security planning has left many organizations without a clear understanding of risk, and an inability to effectively mitigate observable activity in their IT domain. Through integration of leading edge cyber security assessment tools with advanced heuristics and algorithms, organizations can evaluate and prioritize mitigations. This security intelligence can be used to support automated or human driven response actions that take into account enterprise risk, vulnerabilities, threat activity, and operational or strategic business priorities.

The Treasury Board Secretariat's (TBS) Policy on Government Security (PGS) defines "situational awareness" as "having insight into one's environment and circumstances to understand how events

It is more and more important to understand and maintain accurate information about attack options that can allow entry into networks; which assets, information, and operations are most sensitive and the risks they expose; and overall knowledge of the technical environment.

and actions will affect business objectives, both now and in the near future". The PGS identifies that "Because incident management involves predictions and forecasts, situational awareness in the area of IT requires an understanding of the interrelationships between critical services and information, safeguards supporting IT infrastructure and processes, and evolving threats". Despite its importance, the increasing complexity of network environments makes it difficult to maintain situational awareness. It is more and more important to understand and maintain accurate information about attack options that can allow entry into networks; which assets, information, and operations are most sensitive and the risks they expose; and overall knowledge of the technical environment. Environment knowledge encompasses an awareness of systems or assets, and the vulnerabilities or threat events affecting these assets. When this information is combined with attack graph models, as well as organizational risk appetite and operational considerations, it becomes possible to move network defence from a purely reactive to a proactive stance.

ADVANCED PERSISTENT THREATS

APTs are differentiated from conventional IT security threats in their pervasiveness, sophistication, and motivation.

In order to develop mitigation strategies and approaches to counter advanced threat activity, it is first important to develop an understanding of advanced threats and what differentiates them from other more conventional threat actors. The definition of Advanced Persistent Threats (APTs) can be derived from an understanding of their name.

- Advanced: The attacker possesses skills and capabilities beyond those of other threat actors. In particular they have the necessary skills and resources to penetrate well defended networks and access very sensitive information. The advanced nature is partially related to the fact that they are well resourced and very adaptive.

- Persistent: The attacker upon successful penetration of a target's IT environment is capable of maintaining access despite actions taken by network defenders to secure and remediate security incidents. This persistence is generally made possible through propagation of malware to multiple systems within in the environment, such that multiple re-entry points exist to conduct operations against the target.

- Threats: Unlike many other threat actors, a key differentiation factor of an APT is the concept of intent. The attacker has very clear motives behind the attack and will utilize a prolonged campaign to realize the goal. These motives differ from traditional threat actors, as they are very specific to the target, for example intellectual property theft that will provide the attacker economic or industrial advantage over the target.

APTs are differentiated from conventional IT security threats in their pervasiveness, sophistication, and motivation. Several common motives typically associated with advanced actors includes:

- Economic or Industrial Espionage: Attackers will target specific information that can be used to provide economic or industrial benefits. This typically involves the theft of sensitive intellectual property that can provide a competitive organization or foreign state with an advantage. Recent examples of this espionage include the suspected prolonged cyber campaign against Nortel Networks[1]. Economic espionage is not limited to theft of intellectual property, but may also include theft of financial information, particularly as it related to contract negotiations, acquisitions, and mergers. Similar reporting surfaced relating to cyber attacks against legal and financial firms involved in the takeover attempt of Potash Corporation.[2]

> Attackers will target specific information that can be used to provide economic or industrial benefits. This typically involves the theft of sensitive intellectual property that can provide a competitive organization or foreign state with an advantage.

[1] http://www.cbc.ca/news/business/nortel-collapse-linked-to-chinese-hackers-1.1260591

[2] http://www.theglobeandmail.com/technology/tech-news/hackers-linked-to-china-sought-potash-deal-details-consultant/article534297/

- Military Operations: As countries critical infrastructures are increasingly dependent on the Internet to function, they become valuable targets in times of military aggression. In 2007, Estonia was victim to prolonged cyber attack campaigns that disrupted government operations, financial institutions, and the media. These illustrated the affect that can be felt at a national level when coordinated attacks are conducted against information infrastructure[3]. The recent stand-up of the United States Cyber Command shows the militarization of cyber space. The mission of Cyber Commands includes "full spectrum military cyberspace operations"[4], a clear indication that networks are a probable battlefield in future war scenarios.

In the pursuit of security and intelligence gathering requirements, many nation-states will utilize advanced capabilities to gain access to information infrastructure that contains valuable information.

- Covert Sabotage: The revelations about the STUXNET[5] worm in 2010 show how advanced capabilities can be used to disrupt operations and target control systems used in manufacturing and industrial systems. STUXNET was specifically designed to infect Microsoft computers and spread via a number of propagation techniques, including USB keys. The ultimate goal was to infect control systems within Iranian nuclear facilities and disrupt uranium enrichment operations.
- Security and Intelligence: Within the security and intelligence community, the term Computer Network Exploitation [6](CNE) refers to the actions taken to support the collection of intelligence from computer systems and networks. In the pursuit of security and intelligence gathering requirements, many nation-states will utilize advanced capabilities to gain access to information infrastructure that contains valuable information.

The nature of these attacks may support specific intelligence requirements related to national security.

[3] http://www.smh.com.au/news/Technology/Estonia-urges-firm-EU-NATO-response-to-new-form-of-warfarecyberattacks/2007/05/16/1178995207414.html
[4] http://www.stratcom.mil/factsheets/Cyber_Command
[5] http://www.virusbtn.com/conference/vb2010/abstracts/LastMinute7.xml
[6] http://www.virusbtn.com/conference/vb2010/abstracts/LastMinute7.xml

DIFFERENTIATING VICTIMS AND TARGETS

In order to understand who is likely to be attacked by an APT, it is important to consider two primary factors. The first is the motivation as described in the previous section, and the second is the advanced nature of the attacker. The attacker will have very specific goals that are the motivation for the cyber campaign, and he may realize these goals through unconventional tactics. In this section we introduce the concept of victims and targets to develop an understanding of who is likely to be impacted by an APT.

TARGETS

A target represents the end-goal of an APT. In the case of intellectual property theft from a technology company, it is the company from which the attacker wishes to harvest information. As such the most likely targets can be drawn from an understanding of critical infrastructure.

> Critical infrastructure providers are prime targets of attack originating from APT actors. This is due to the sensitive data they may possess, or the services that they provide.

Federal Governments in both the United States and Canada, have officially recognized several critical infrastructure sectors. Many other countries around the world have also adopted similar definitions, and while the lists may vary slightly, in general there is agreement on an international level about what is considered critical infrastructure. This list includes:

- Energy and Utilities
- Communications and Information Technology
- Finance
- Health Care
- Food
- Water
- Transportation
- Safety
- Government
- Manufacturing

If your organization is considered to be one of these critical infrastructures, then the probability that you are a target needs to be considered as a reality. For various reasons as outlined above, critical infrastructure providers are prime targets of attack originating from APT actors. This is due to the sensitive data they may possess, or the services that they provide.

A victim is defined as an organization that is compromised by an APT, however they are not the selected target of the operation. This is an important distinction to make because it touches on the advanced nature of these threat actors.

VICTIMS

In the context of this whitepaper, a victim is defined as an organization that is compromised by an APT, however they are not the selected target of the operation. This is an important distinction to make because it touches on the advanced nature of these threat actors. If we consider Internet Service Providers (ISPs) as an example, the distinction between target and victim can be understood. An ISP provides communication capacity and interconnectivity for their clients. Assuming one of these clients contains information of value to an APT, perhaps it is a technology company, or perhaps it is a customer that is of intelligence value to a foreign state, as was the suspected case with Belgacom[7] in 2013. The target would be the technology company or customer, then the ISP may be a victim of APT attack. The attacker would select the ISP as a possible victim given their business relationship with the target. An exploitation of the ISP can provide additional attack vectors that can be exploited to reach the intended target.

In this example, these victims can be considered as an enabler of the end goal because of business relationships with the target. They will typically serve as an intermediary that enables the APT to gain access and maintain persistence to the target. A second type of victim should also be considered, and these can be classified as infrastructure providers.

[7] http://grahamcluley.com/2013/09/belgacom-hack/

In order for an APT campaign to be successful attackers require the use of infrastructure, or basic systems and facilities to support the campaign. In the context of a cyber attacker, infrastructure refers to IT systems that are used to launch attacks, manage communications with victims, and receive, process and store the information that is taken from targets. The advanced nature of an APT requires that they go to great lengths to mask their presence and avoid using systems that can reveal their identity. Avoiding this attribution results in the use of multiple computer systems chained together using a covert network in order to route communications from the attacker to the target system or systems. Acquiring and maintaining this network of systems requires that the attacker control many systems around the globe. In order to achieve this, systems are compromised by the APT to serve as tools or components of his required infrastructure. The selection of these infrastructure victims is not focused on any industry or sector, instead they are opportunistic. Typically, any system connected to the Internet with exposed vulnerabilities can be a victim of APT attack in order to serve as the necessary infrastructure to support operations.

> Many in the information security industry have developed tailored recommendation and guidance to help organizations rapidly address the challenge of advanced threats operating against their information infrastructure.

The information presented in this section illustrates that APT actors will have very specific targets, however in order to achieve their established goal and complete the mission, they will victimize other organizations and systems that may not traditionally be considered as having information or services of value to the attacker.

THE DEFENSE

The advanced capabilities and indiscriminate nature of APT activity is cause for growing concern. Many in the information security industry have developed tailored recommendation and guidance to help organizations rapidly address the challenge of advanced threats operating against their information infrastructure. Two prime examples of this advice are the Defence Signals Directorate (DSD)

Top 35 Strategies to Mitigate Targeted Intrusions[8], and the SANS Top 20 Critical Security Controls for Effective Cyber Defence[9]. Both provide very specific recommendations on improvements to security controls that have been demonstrated to effectively mitigate the risk of APT activity. The tools provide valuable, concrete actions that can be taken to dramatically improve information security practices, and address many of the gaps and vulnerabilities that are most exploited by APT actors. Upon review of the advice however, it can be noted that the recommendations are not dissimilar from similar advice that has been provided by information security professionals for the last decade. Indeed, the advice is much more specific and provides implementation guidance, however lacks a critical element necessary to counter APTs.

As security practices are improved, it is important to remain cognizant of the fact that the aggressors are motivated, and for sufficiently valuable targets, this motivation is not likely to be outweighed by security measures.

As previously noted, APTs are extremely capable and motivated aggressors with access to cutting edge capability and resources. As security practices are improved, it is important to remain cognizant of the fact that the aggressors are motivated, and for sufficiently valuable targets, this motivation is not likely to be outweighed by security measures. Consider an organization that is the target of an advanced persistent threat. Once they have identified this capability they may implement a number of IT security control improvements to increase the security of their information infrastructure. While these improvements may successfully mitigate the current activity, the organization remains a target of interest to the aggressor. The initial motivation for the attacks has not been addressed, and as a result the APT is likely to continue their attacks.

In order to overcome the security improvements, new techniques and tools may be formulated and used. This is not inconceivable given the advanced nature of the attacker. Furthermore, past intrusions have given them internal knowledge about the target's information infrastructure that can be leveraged in future attempts

[8] http://www.asd.gov.au/infosec/top-mitigations/top35mitigationstrategies-list.htm
[9] https://www.sans.org/critical-security-controls/

to regain a foothold. Countering an adversary with this degree of capability requires situational awareness, a key enabler of security intelligence.

There exist many definitions for the term situational awareness, as it has been an area of extensive academic research. One such definition is that situational awareness is "knowing what is going on so you can figure out what to do". (Adam, 1983)[10] This definition, while simplistic in nature is an accurate description of what situational awareness provides. It requires an understanding of the environment, and the ability to make decisions based on perceived changes to this environment. The lifecycle of situational awareness is broken down into perception, comprehension, and projection.

- Perception relates to monitoring, detecting, and recognizing data from a variety of sources as they relate to your environment. The aggregation of these data sources enables basic insights related to the environment.

- Comprehension is the ability to process the individual data elements that you are able to perceive, and create knowledge. Knowledge is enabled by distilling valuable information from seemingly independent data elements through the recognition of patterns, relationships, and dependencies between various data elements.

- Projection maps to decision-making and action. Once data has been transformed into knowledge that should be used to assist in decision-making and action. Sufficient knowledge enables you to predict how your actions will affect the environment and act accordingly.

This cycle of situational awareness does not end, it is continuous as for each action within an environment, new data will be produced to support better understanding of the environment. This information

Past intrusions have given attackers internal knowledge about the target's information infrastructure that can be leveraged in future attempts to regain a foothold. Countering an adversary with this degree of capability requires situational awareness, a key enabler of security intelligence.

[10] Fighter cockpits of the future. Proceedings of 12th IEEE/AIAA Digital Avionics Systems Conference (DASC), 318–323.

lifecycle is applicable to mitigation of advanced threat activity, and is materialized through security intelligence. Understanding the environment, yourself and potential aggressors enables organizations to better position defenses, and take action when threat activity becomes active in the environment. Implementing controls without the ability to maintain situational awareness is a short-term strategy that addresses current aggressors and techniques, but does not provide the necessary tools to identify and react to changes in aggressor behavior over time.

Effective security intelligence relies, not only on technical information such as vulnerability details and threat activity from security monitoring technology, but also business information.

VISIBILITY OF THE ENVIRONMENT — PERCEPTION OF DATA

Security Intelligence begins with the collection of relevant data from the environment. Effective security intelligence relies, not only on technical information such as vulnerability details and threat activity from security monitoring technology, but also business information. In order to create a defensible network organizations need to understand what information is of most value to their overarching business strategy and what level of protection is required.

Technical data from security tools need to be identified and collected. This collection should include the normalization of data from a variety of tools into a standard security event format to support identification of relationships and enable higher order analytics. Common technologies to facilitate this collection are commercial SIEM products or cloud based threat management services. Data collection should cover data from intrusion detection and intrusion prevention platforms, malicious code defenses, enterprise networking equipment such as routers and firewalls, enterprise vulnerability management services, authentication services, corporate applications and databases, network flow details, and common enterprise services such as web proxies, domain name servers, and e-mail gateways. The ability to collect and process this technical information is essential in subsequent phases of situational awareness.

Business data needs to come from senior level executives and decision makers. In order for security to be effective, it must support the needs and goals of the business. A common tool for identifying this data is through a comprehensive enterprise security architecture. Hitachi Systems Security Inc. recommends the SABSA[11] methodology. An enterprise security architecture should identify the fundamental business drivers which are derived from the strategy and mission of the organization. Based on these drivers security practitioners can better understand how security services enable business objectives, and a clear understanding of what is important to the organization can be identified. Understanding what is important to a business is an important tool in combating APT activity, as information you deem critical is likely to be of interest to advanced attackers.

> In order for security to be effective, it must support the needs and goals of the business. A common tool for identifying this data is through a comprehensive enterprise security architecture.

UNDERSTANDING OF THE ENVIRONMENT — COMPREHENSION OF INFORMATION

Once data is available, knowledge can be created by distilling the data into valuable information. During this phase of the security intelligence cycle, organizations develop an understanding of the environment in which they operate. Through advanced analytics, advanced threats can be identified in the environment. Sufficient information is available to understand how these threats materialized, and what they are ultimately targeting. Understanding the environment includes the ability to view your network and your information in the same light as an attacker. Knowing what vulnerabilities you are exposing and which techniques can be used to penetrate your own network is an important tool in improving defenses.

Understanding the environment is enabled through data analytics and correlation based on the data that has been collected. It is

[11] http://www.sabsa.org/

imperative to understand not only the capabilities and intentions of APT actors, but also your own security posture and defensive capabilities. This awareness is only possible through constant evaluation of new data. To be accurate it must include both technology and business knowledge. Consider the ancient wisdom of Sun Tzu who stated that “if you do not know your enemies nor yourself, you will be imperiled in every single battle”[12]. In many ways APT aggressors can be considered as enemies or combatants. They seek to overpower or circumvent established defenses in order to cause damage, or personal benefit through adversarial actions against another. To successfully counter this type of threat requires knowledge.

Knowing what vulnerabilities you are exposing and which techniques can be used to penetrate your own network is an important tool in improving defenses.

TAKING DEFENSIVE ACTION — PROJECTION INTO THE ENVIRONMENT

The final aspect of mitigating threats through security intelligence is to take action based on the knowledge gained previously. Acting without knowledge creates additional risk. For example, consider an organization that has detected an APT and immediately counters the threat with control improvement addressing the perceived vulnerability that was exploited. If the organization does not understand what information the APT was after, or the complete capabilities of the adversary they may fail to appropriately safeguard the appropriate data. Furthermore, control improvement undertaken without consideration for continued surveillance and intelligence may simply drive an adversary to use capabilities that you have not yet conceived and therefore are not able to monitor and protect.

When responding to an APT, the knowledge of their intent and motives, coupled with detailed awareness of risk appetite and technical security posture, will enable defensive action.

When responding to an APT, the knowledge of their intent and motives, coupled with detailed awareness of risk appetite and technical security posture, will enable defensive action. These

[12] The Art of War, Sun Tzu - http://classics.mit.edu/Tzu/artwar.html

actions can vary from security control improvement to incident response and forensics and one end of the spectrum. For organizations with advanced security capabilities, this may also result in automated defensive actions being taken to contain and mitigate the threat activity in near real-time. Regardless of the action taken, the rationale for the decision needs to be captured and as well as the factors that contributed to the action being taken. Immediately following an action the behavior of the adversary and any changes to the environment need to be understood and integrated as new elements of the situational awareness. If an organization is incapable of observing their adversaries reaction, then the security intelligence cycle is incomplete.

CONCLUSION

This whitepaper has provided a general overview of advanced persistent threats and who needs to be concerned about their malicious activities. As a capable, motivated and well-resourced adversary, APTs are a growing concern for businesses and organizations dependent upon access to the Internet to achieve their objectives. Countering advanced threats requires not only technical capability, but also knowledge and understanding. There is no single technical solution that will eliminate advanced threats, however through constant evaluation of the environment, security intelligence services can be used to predict and take action based on real threat activity with an environment. Organizations acting without this intelligence picture inadvertently create additional risk that can be leveraged by APT attackers. Improving technical security controls is an important aspect of APT defence, however it cannot be undertaken in isolation. To fully realize the benefit of security improvement, situational awareness, or a security intelligence lifecycle, is necessary.

> There is no single technical solution that will eliminate advanced threats, however through constant evaluation of the environment, security intelligence services can be used to predict and take action based on real threat activity with an environment.

Hitachi Systems Security Inc.
955 boul. Michèle-Bohec, Suite 244, Blainville (Québec) J7C 5J6 Canada
Tel: +1 450-430-8166   Fax: +1 450-430-1858
www.hitachi-systems-security.com