Advanced Persistent Threats:

What Are They and Why Do I Care?

Bryant Rossil

East Carolina University

Abstract

My term paper will focus on the protection of the enterprise against the business directed cybercrimes, Advanced Persistent Threats (APT). This paper will define what an APT is and some of the behaviors and characteristics associated with this sophisticated attack which are unlike the attacks businesses face daily. Showing how an APT works will also be present in this paper which will detail some of the ways APTs find there way into corporate systems. I will then focus on the detection of APTs and how an information security team can monitor these stealth attacks that can last an indefinite amount of time depending on the attackers goal. Lastly, I will cover the methods in which the business can deter these cyber attacks and the multiple ways to protect the company's assets from these criminal operators.

With technology becoming one the forefront topics amongst consumers and media headlines, its no wonder that Information Security is becoming a growing concern for many companies and business professionals. Some of the rising risks are viruses, malware, spyware, Trojan horses, spam, phishing, botnet, and the list goes on. One threat in particular that has gotten a lot of attention from information security professionals is Advanced Persistent Threats (APT). An APT broken down gives us critical insight as to what it truly means. Advanced is a "criminal operator behind the threat utilizing the full spectrum of computer intrusion technologies and techniques" ("Advanced Persistent Threats (APT), (n.d.)). Persistent means, "Criminal operators give priority to a specific task, rather than opportunistically seeking immediate financial gain"("Advanced Persistent Threats (APT), (n.d.)). Threat, "means that there is a level of coordinated human involvement in the attack, rather than a mindless and automated piece of code ("Advanced Persistent Threats (APT), (n.d.)).

With that rising concern around Advanced Persistent Threats, this raises a lot of questions and concerns, such as: What are Advance Persistent Threats and why should we be concerned with them? What are the behaviors and characteristics of Advanced Persistent Threats that I should be concerned with? We need to understand how an APT works. How do these threats find their way into corporate systems and what initiatives can we take to ensure we can be prepared against these vicious attacks? All of these burning questions are raising security concerns around these attacks and there are many ways of understanding the risks

to be prepared for scenarios where this could affect you or the financial integrity of the company you currently work for.

WHAT ARE APTs?

As described by Nicho (2014) an "Advanced Persistent Threat (APT) is a term used for a new breed of insidious threats that use multiple attack techniques and vectors conducted by stealth to avoid detection so that hackers can retain control over target systems unnoticed, for long periods of time." But what does this really mean? Another description more simply put by Aurnou (2013) states that "Advanced Persistent threats (also known as APT's) are deliberately slow-moving electronic attacks used to quietly compromise a computer network without revealing themselves". Combining both of those descriptions we can conclude that Advanced Persistent Threats are a fairly new threat to security that use multiple techniques that attack slowly to remain undetected for extended periods of time gathering key information or data from the targeted company. The dilemma with advanced persistent attacks is that the "attacks are extremely difficult or even impossible to detect." (Kolochenko, 2015). As one can imagine, this is a nightmare for Information Technology (IT) staff within an enterprise. With a simple click you could potentially put yourself at risk to one of these attackers or even worse, the whole firm could be breached. The long-term effects of an Advanced Persistent Threat on your network could cause possible data loss, disruption of service to your applications, or complete system failure thereby causing devastating ramifications to a company's reputation and financial status. Kolochenko (2015)

stated, “93.6 percent of respondents consider APT’s to be a “very serious threat” for their companies.”

WHY DO WE CARE?

Why pay special attention to Advanced Persistent Threats? What makes them more of a threat and require higher attention than other cyber attacks? Some companies have been quick to educate their staff on how to mitigate everyday attacks and have preventive controls in place to ensure malicious content is not penetrating their networks (“Advanced”, 2013, p6). Advance Persistent Threats have been causing large-scale security breaches and are being classified as a new class of network intrusion threat (“Advanced”, 2013, p6). APT’s are being aimed directly towards “theft of intellectual property as opposed to achieving immediate financial gain and are prolonged, stealthy attacks” (“Advanced, 2013, p6). Often times they are not leveraged through external attacks but using trusted connections or insider threats to target compromised systems (“Advanced”, (n.d.)). With individuals already possessing the skills and the resources needed, the only pieces left are the motivation and the target organization to carry out the actions on.

WHERE DO APTs BEGIN?

Where do Advanced Persistent Threats come from? These threats stem from individuals with “sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors” such as “physical, cyber and deception” (“Advanced, 2013, p6). As you

could imagine we are dealing with stealthy criminals who are allowing time to pass while data is being collected from various methods, so how do we stop this? It's tricky because these individuals hold the skills to use construction kits and have access to more advanced tools as well as strategizing to use multiple attack methodologies and tools to compromise the target ("Advanced Persistent Threat (APT)", (n.d.)). They use these tools to breach even in the presence of properly designed and maintained depth strategies such as internet-based malware infection, physical malware infection, and external exploitation ("Advanced Persistent Threat (APT)", (n.d.)).

HOW DO APTs GET INTO MY SYSTEM?

How do these threats find their way into corporate systems and how do they work? Symantec describes an Advanced Persistent Threat as having "multiple phases to break into a network, avoid detection, and harvest valuable information over the long term." ("Advanced Persistent Threats: How", (n.d.)). There are a few steps that go into how APTs function within a system. First step is reconnaissance. During this process, the attacker attempts to leverage information from a variety of sources to get a blueprint of the specified target. The second step is incursion, where attackers use social engineering to break into a network to distribute the malware onto the vulnerable systems ("Advanced Persistent Threats: How", (n.d.)). The third step in the process is discovery, where the attackers remain in the shadows and create a map of the organization's defense system, in conjunction with creating a plan of action for when the real assault takes place. ("Advanced Persistent Threats:

How", (n.d.)). The fourth step is to capture information over an extended amount of time from those unprotected systems. During this step, attackers may install malware to interrupt corporate operations or to collect confidential data. Symantec describes an Advanced Persistent Threat as having "multiple phases to break into a network, avoid detection, and harvest valuable information over the long term." ("Advanced Persistent Threats: How", (n.d.)). See diagram below for a visual representation of an attack taken place:

Diagram from: ("Advanced Persistent Threats (APT): How", (n.d.))

HAVE MY SYSTEMS BEEN AFFECTED?

How do you know when you have been a victim of an Advanced Persistent Threat? There are a few signs to tell if you are being affected by Advanced Persistent Threats including: increase in log-ons, backdoor Trojans, unexpected information flows, unexpected data bundles, pass-the-hash hacking tools, and Adobe Acrobat

.pdf files. The first threat is an increase in elevated log-on times at various non-working hours (Grimes, 2012, p1). “Advanced Persistent Threats start to rapidly escalate from compromising a single computer to taking over the whole environment” (Grimes, 2012, p1). Hackers start by reading authentication databases, or compromising user credentials and understand which user or service accounts have elevated permissions or privileges (Grimes, 2012, p1). Hackers use these elevated credentials to compromise the assets within the targeted environment. A way to understand and track if you have been or are currently a victim of these advanced threats is to check the volume of log-ons at night. Typically, cyber criminals are on the opposite side of the world and will cause high volumes of elevated log-ons outside of the normal office hours (Grimes, 2012, p1). The second sign is finding widespread backdoor Trojans (Grimes, 2012, p1). Nefarious criminals will find backdoors, or vulnerabilities that have not been patched, and install rogue programs within the exploited environment to compromise the device. Hackers take these actions to ensure they will have access to the log-on credentials regardless if system administrators change the passcodes (Grimes, 2012, p1). The third sign are “unexpected information flows” which are “the single best way to detect APT activities” (Grimes, 2012, p1). These can easily be internally checked at all points interacting with internal and external computers to look for unexpected flows of data. This data can be transferred “server to server, server to client, or network to network” (Grimes, 2012, p1). To be able to interpret the data flows, you need a fundamental understanding of how the data flows within the targeted environment to track where the last user logged in (Grimes, 2012, p1). The fourth sign is

unexpected data bundles (Grimes, 2012, p2). With Advanced Persistent attacks, stolen data will be aggregated into a sole internal collection point before being transferred externally. To detect this form of threat by no means is a simple task. Administrators will need to review logs for large chunks of data appearing in places that the data normally shouldn't be (Grimes, 2012, p2). For example, if you have gigabyte chunks of data that are being compressed into an archive format that is not a company standard, this should immediately raise a red flag for concern. The fifth sign is detecting pass-the-hash hacking tools (Grimes, 2012, p2). Advanced Persistent Threats do not always use these types of tools but when used they will frequently pop up. It's typical that hackers forget to delete these after using them and leave the tools installed (Grimes, 2012, p2). The final indicator is that an employee of a company opened or used an adobe pdf file that contained malware. This is one of the most common and easiest forms of Advanced Persistent Threats (Grimes, 2012, p2).

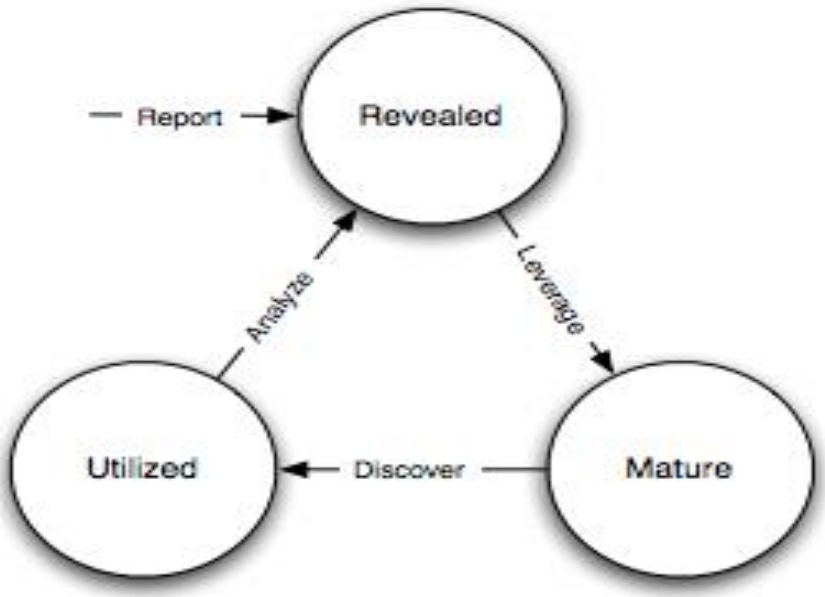
REAL WORLD SCENARIOS

In 2011, there were a high number of Advanced Persistent Threat attacks that affected organizations such as Sony, RSA, Lockheed Martin, Epsilon, NASA, PBS, FBI, and many more (Nicho, 2014, p1). An example of an attack was in 2009, when botnet armies that were sponsored by North Korea targeted the US governmental institutions (Bar-Yosef, 2010). The original mission failed but this attempt allowed North Korea to start targeting the United States' private sites. Another example is around a worm called Stuxnet. This worm targeted SCADA systems and the "worm

consisted of four different attack vectors, all separately exploiting different vulnerabilities" (Bar-Yosef, 2010). The code the hackers wrote took six months of development time and had a specific target – Iran. Soon, it was distributed to Iran, Germany, Russia, India, and many other countries. Stuxnet wasn't focused on obtaining any data, but to gain control of the Bushehr Nuclear Plant. The technique displayed from the worm was "target as many systems, and sooner or later, there will be a victim." (Bar-Yosef, 2010).

HOW CAN WE PROTECT OURSELVES?

How can an information security team monitor APTs? There are certain indicators we can be aware of around these advanced attacks. These indicators are "any piece of information that objectively describes an intrusion. Indicators can be subdivided into three types: Atomic, Computed, and Behavioral" (Hutchins, (n.d.), p3). Atomic are those that cannot be broken into smaller parts such as IP and email addresses (Hutchins, (n.d.), p3). Computed are those that are derived from an incident where data has been taken such as hash values. Behavioral are a combination of computed and atomic indicators. They are "often subject to qualification by quantity and possibly combinatorial logic" (Hutchins, (n.d.), p3). An example of this is that an attacker uses a backdoor to generate the network traffic that matches the same rate and IP addresses on the system and then replaces this with a matching MD5 hash value (Hutchins, (n.d.), p3). The diagram below shows the indicator life cycle:



Resource: (Hutchins, (n.d.), p4)

As explained by Virvillis, there are many technology limitations when it comes to combatting Advanced Persistent Threats (2014, p2). "Advance Persistent Threats make frequent use of zero-day exploits or modify/obfuscate known ones and, thus, are able to evade the majority of signature-based end points and network intrusion detection solutions" (Virvillis, 2014, p2). These attacks are spread across a large amount of time and do not give you a correlation or detection around when the systems are being intruded. The amount of time attackers will spend to explore all of the potential attack paths is significant; they will plan all paths with no time constraints to ensure their attacks will be successful. Some attackers are supported by nation-states that give them more power around manufacturing, physical access and intelligence collections around cyber attacks (Virvillis, 2014, p2). Another high-risk problem is cyber criminals target only a select few individuals and these tend to

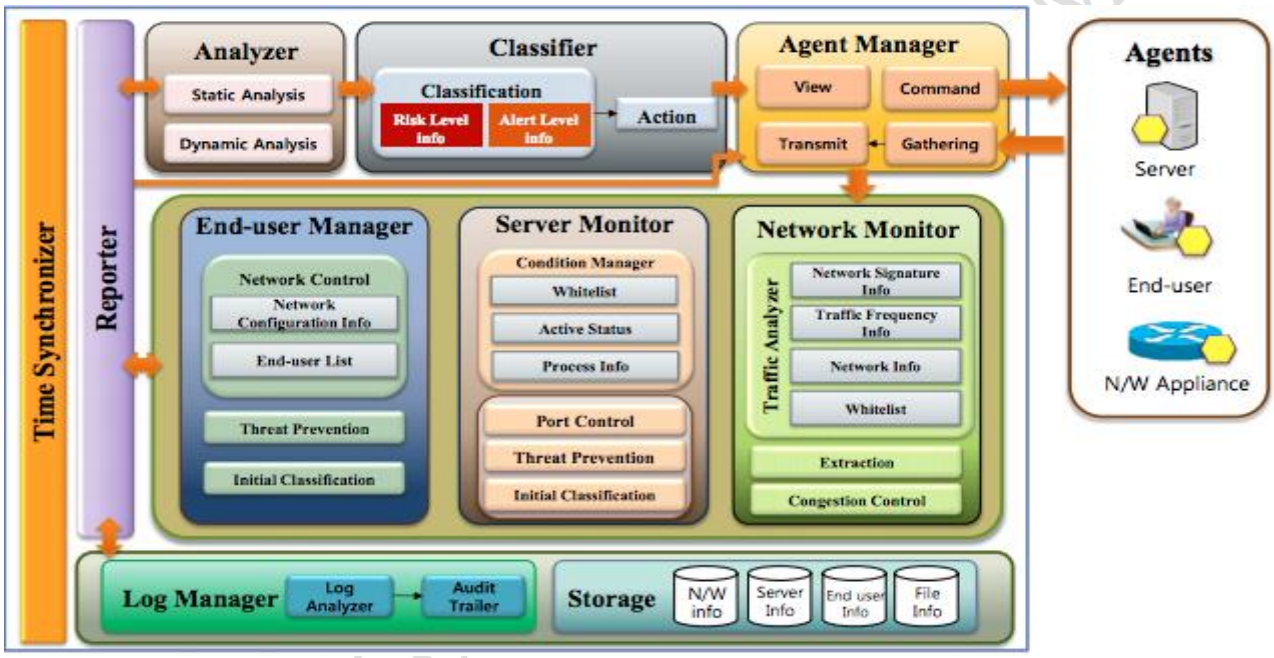
be individuals with nontechnical backgrounds so they will be less likely to identify the threat (Virvillis, 2014, p2). With the characteristics noted above it makes it hard for current cyber security solutions to prove effective.

METHODS TO DETER APTs

What are some methods to deter these cyber attacks and protect your network? First, you should ensure you have network security software in place to monitor the electronic traffic flowing through a system (Aurnou, 2013). Just having network security software will not work unless you are tracking both inbound and outbound network traffic to ensure there isn't any type of rogue-encrypted communications. In addition, a deployment of honeypots, in which they act as a tripwire to reveal when there is a hacker on the network, is also advisable (Aurnou, 2013). Implementation of access controls to keep users from being able to interact with network information that does not pertain to their job role is another countermeasure the enterprise can take. Access control helps to secure individuals from having accounts that can be compromised by attackers. A whitelisting of your programs is also advised to only allow them to communicate on the network only when the network administrator has approved the access (Aurnou, 2013).

A more sophisticated model would be a multi-layer defense system to prevent these Advanced Persistent Threats (Moon, 2014). By implementing a multi-layer defense system, this will defend against APT's. This system is also reinforced by "collecting and analyzing log information from devices and installing the agent on the network appliance, server and end-user" (Moon, 2014). This model creates an

eight-component model that consists of "classifier, analyzer, agent manager, server monitor, end user manager, network monitor, log manager and storage." (Moon, 2014). This Multi-Level Defense System is a more reliable setup to provide security against Advanced Persistent Threats. To understand the flow of data through this model, refer to the diagram below:



Resource: (Moon, 2014)

Websense also recommends being successful around a defense strategy for APT's, that you must have "a multi-layered approach in which multiple detection mechanisms work together to identify complex patterns of evasive behavior" ("Advanced", 2011)

Another key aspect around these threats is how to remediate the issue when the threat has been discovered? As shown by McAfee's Incident Response Plan diagram, you must first respond to the issue before you can prepare for the investigation phase. Responding to an incident and analyzing the cause in a

methodical way is critical because if you rush to fix the issue around the affected systems you could by alert the criminals that they have been discovered, and fast tracking yourself into further compromising your environment ("Combating", 2011). McAfee's diagram around creating an incident response plan gives insight around the correct actions to take to ensure the impact you receive from an Advanced Persistent Threat is minimal. See the figure below:

Plan Phases	Phase Categories	Detail
Preparation	Risk Assessment	• Identify and classify business assets and data stores • Conduct vulnerability assessment across critical infrastructure • Quantify risk with highest value assets and highest vulnerabilities atop the list • Recommended solutions: ◦ McAfee Risk and Compliance
	Security Assessment	• Review security measures protecting critical business assets • Recommended solutions for APT prevention: ◦ McAfee Email Security with message and sender reputation ◦ McAfee Web Security with URL reputation ◦ McAfee Firewall Enterprise with application awareness ◦ McAfee Network Security Platform for intrusion prevention with file, IP reputation, and behavior heuristics ◦ McAfee Application Control with whitelisting ◦ McAfee Data Loss Prevention
	Organizational Preparedness	• Identify key individuals most likely to be the target of social engineering attacks (due to high levels of access) • Implement aggressive access control by restricting network access of key individuals to 'business need to know' • Employee training: ◦ Prioritize high-risk individuals and work groups ◦ Examples: safe surfing practices, what to do with suspicious emails, social networking dos and don'ts
	Operational Preparedness	• Identify incident response team (including legal and business owners) • Communication plan, including law enforcement if necessary • Schedule/conduct incident response dry run

(continued)

Plan Phases	Phase Categories	Detail
Investigation and Initial Response	Detection	• Recommended detection technologies: ◦ McAfee Network Threat Response for malware detection, root cause analysis ◦ McAfee Network Threat Behavior Analysis to identify attack propagation, scope of attack ◦ Third-party network forensics to assist with log analysis, historical context ◦ McAfee Network Security Platform to detect unusual connection patterns and malware downloads ◦ McAfee Data Loss Prevention to identify data breaches
	Internal Stakeholder Notification	• Business owners • IT management • CEO, CTO • Board of directors (if necessary)
	External Response Strategy Notification	• Corporate/public relations • Law enforcement (if necessary) • Compromised users (if necessary) • Regulatory bodies (if necessary)
Containment	Countermeasures	• Custom intrusion prevention system signatures • Quarantine and clean infected devices • Update firewall rules, policies to block command and control channels

Reference from McAfee ("Combating", 2011)

CONCLUSION

As we've seen, Advanced Persistent threats can cause a lot of harm to companies. With the rising number of cyber incidents directly targeting any company, we have to be informed around these types of attacks and understand how to deal with these major challenges. The problem is that our employees are lacking the security knowledge it takes to decipher these signs and threats and without the knowledge to keep these attackers from compromising confidential data, how will we be prepared? We will need to ensure that the employees are trained to understand the warning signs and should be required to take security awareness training sessions for further learning. Once employees are concerned and prepared with security knowledge, the overall security of the firm increases.

Advanced Persistent Threats are harder for a company to prepare for since there is little to no detection of them existing on their network. However, if you have an incident response plan in place that will allow you to understand the measures you would need to take in case of emergency, then this is another method of mitigating risk to the company. This goes back to the topic of making sure employees are conscientious of the items they click on to not allow malware into their system that will eventually disrupt the network. Being proactive by making sure weak points has been identified can also to reduce risk to the firm. A majority of companies will see security training as a waste of resources and would rather spend budget allocations on hardening application security. In reality, while securing applications is necessary, training employees in the enterprise is another effort to companies should take to mitigate risk. Focusing on ensuring end users are aware of the grave danger they could face through Advanced Persistent Threats, how to detect them, and how to secure themselves from the threats will provide security awareness for all within the company.

Simply being aware of threats such as APTs provides a safeguard against the attackers who will do anything to get into your accounts. Protecting confidential information and even the reputation of your firm should be a top priority regardless of the size of the firm. A bad reputation or loss of data from a firm could highly impact your customer base and ultimately loss of trust in the services you provide. APT's are not going away any time soon. Companies should continue to provide the various mitigation strategies mentioned previously to avoid loss of reputation, information and monetary loss.

References

Advanced Persistent Threat Awareness. (2013). Retrieved December 5, 2015, from http://www.trendmicro.com/cloud-content/us/pdfs/business/datasheets/wp_apt-survey-report.pdf

Advanced Persistent Threats and Other Advanced Attacks: Threat Analysis and Defense Strategies for SMB, Mid-Size, and Enterprise Organizations. (2011). Retrieved December 5, 2015, from https://www.websense.com/assets/white-papers/whitepaper-websense-advanced-persistent-threats-and-other-advanced-attacks-en.pdf

Advanced Persistent Threats: How They Work | Symantec. (n.d.). Retrieved December 5, 2015, from http://www.symantec.com/theme.jsp?themeid=apt-infographic-1

Aurnou, S. (2013, October 21). Advanced Persistent Threats: What Are They & How Do They Work? Retrieved December 5, 2015, from http://www.thesecurityadvocate.com/2013/10/21/advanced-persistent-threats-what-are-they-how-do-they-work/

Bar-Yosef, N. (2010, November 16). When the Advanced Persistent Threat (APT) Meets Industrialization | SecurityWeek.Com. Retrieved December 5, 2015,

from http://www.securityweek.com/when-advanced-persistent-threat-apt-meets-industrialization

Combating Advanced Persistent Threats: How to Prevent, Detect, and Remediate APT's. (2011). Retrieved December 5, 2015, from http://www.mcafee.com/us/resources/white-papers/wp-combat-advanced-persist-threats.pdf

Grimes, R. (2012, October 16). 5 signs you've been hit with an advanced persistent threat. Retrieved December 5, 2015, from http://www.infoworld.com/article/2615666/security/5-signs-you-ve-been-hit-with-an-advanced-persistent-threat.html

Hutchins, E., Cloppert, M., & Amin, R. (n.d.). Intelligence-Drive Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Retrieved December 5, 2015, from http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Kolochenko, L. (2015, July 21). Modern APTs start at your corporate website. Retrieved December 5, 2015, from http://www.csoonline.com/article/2950049/advanced-persistent-threats/modern-apts-start-at-your-corporate-website.html

Moon, D., Im, H., & Dong Lee, J. (2014, December 3). MLDS: Multi-Layer Defense System for Preventing Advanced Persistent Threats. Retrieved December 5, 2015, from http://www.mdpi.com/journal/symmetry

Nicho, M., & Khan, S. (2014, March 1). Identifying Vulnerabilities of Advanced Persistent Threats: An Organizational Perspective. Retrieved December 5, 2015, from http://www.irma-international.org/viewtitle/111283/

Virvilis, N., Serrano, O., & Dandurand, L. (2014). Big Data Analytics for Sophisticated Attack Detection. Retrieved December 5, 2015, from http://www.isaca.org/Journal/archives/2014/Volume-3/Documents/Big-Data-Analytics-for-Sophisticated-Attack-Detection_joa_Eng_0514.pdf

What's an Advanced Persistent Threat (APT). (n.d.). Retrieved December 5, 2015, from https://www.damballa.com/paper/advanced-persistent-threats-a-brief-description/