BDO KNOWS:

CYBERSECURITY

CONTACTS:

DR. ERIC CHUANG
Managing Director
Cybersecurity Advisory
Services
echuang@bdo.com

GREGORY GARRETT
Head of U.S. and
International Cybersecurity
ggarrett@bdo.com

CYBER THREAT INTELLIGENCE

Whenever the subject of cyber threat intelligence comes up during conferences or discussions, it becomes readily apparent that few people really understand what "threat intelligence" means. Everybody has their own idea of what it is: many think threat intelligence is a synonym for dark web intelligence. While others believe every cybersecurity subscription they receive is some form of threat intelligence. The one universally shared belief is that people feel overwhelmed by either the sheer volume of threat intelligence, or the actual usefulness of threat intelligence to their specific organizations. Almost everyone agrees that threat intelligence of some sort is important. Most receive and review some type of threat intelligence, but things can quickly break down regarding which specific type of threat intelligence is actually useful, and what executives should do with the intelligence that they receive. The conversation often become even livelier, if the topic turns into how much each organization should pay for such intelligence, and if the intelligence is worth the price.

The same trends in the proffering of traditional human intelligence (HUMINT) and signal intelligence (SIGINT) are being adopted in the emerging field of cyber intelligence. Corporate consumers could fall for the same salesmanship and fallacies that plagued the government intelligence services. It is extremely difficult for consumers to effectively absorb or make use of the all the information intelligence purveyors generate. Every incoming piece of intelligence is buried by the next wave of intelligence and relegated to the huge pile of unprocessed data, or worse yet, only discovered after an incident had occurred. Unfortunately, this practice then restarts the cycle of finding new intelligence sources and vendors, not realizing the issue was never the lack of intelligence, but rather that the intelligence they have is not in the hands of the right people. This trend is also happening frequently in the corporate world as well.

Whenever there is a cyber incident, the easy answer is always to blame the person responsible for “reading” the intelligence and failing to do something about it. We have all seen companies after a major cyber breach blame the information technology (IT) person for not implementing a particular software security patch that was circulated by various intelligence reporting for months. Although there is always plenty of blame to go around in a cyber breach, firing the IT person generally will not improve the company’s ability to use the intelligence properly. Unless the company changes how intelligence is purchased, processed, and applied, the same problem will remain, and the true responsibility lies not with the IT staff, but with the higher level decision makers.

To understand how to make use of cyber intelligence effectively, or at least the ability to evaluate the applicability of an intelligence product for the company, the decision makers themselves need to know how cyber-attacks are actually conducted. Once the decision makers understand the components of the attack, they will have enough knowledge to challenge the vendors and know what components of the cyber-attack the cyber intelligence product actually focus on. Then the senior leadership can make truly informed decisions regarding which intelligence product they should be purchasing in order to fulfill their company’s specific needs. More importantly, senior leadership can then decide which department and associated individuals will be responsible for what intelligence; instead of assuming the CISO, CIO, or the IT Department Head will be responsible for processing all of the intelligence.

Cybersecurity Intelligence consumers, especially the senior executives and decision makers, need to know at least how to differentiate actionable versus information intelligence. Unlike the government who send intelligence analysts to months and years of training to be able to learn and practice the art of finding the thread of usable intelligence among an ocean of bulk data, this chapter is not meant to make the senior executives into intelligence analysts. Rather, it is meant to educate executives about the fundamentals in the day-to-day applications of cyber intelligence, thus enabling them to be better business decision makers.

CYBER ATTACK AND MYTHOLOGY

The fundamental principle of cybersecurity is that it is a defensive activity. One must first understand how our adversaries conduct their offensive activities. Cyber-attacks, or hacking, can be a subject of discussion that can last for days, if not months, by enthusiasts and subject matter experts. When explaining hacking to senior executives, law makers, counsels, judges and finance managers, this writer has learned that the best way to understand hacking is by breaking it down into components that can be explained in simple everyday and relatable concepts. Once the audience can grasp the concept of the components, hacking is no longer a dark art or black magic. Rather it is just a combination of everyday parts that the audience is already familiar with; then the technical details become much easier to absorb. Even if the senior executives do not fully understand all of the details, they can at least appreciate the overall concept.

A common myth is that cyber criminals are all-knowing computer geniuses who can hack into your computer as if they are using black magic. People do not typically understand how an attack actually works. This writer had the good fortune to lead the FBI’s cyber operations group for the latter part of his Bureau career, which required the end-to-end life cycle of conducting cyber operations that includes the development of all the components needed to perform such cyber operations. After many years in practicing both the offensive and the defensive art of cyber operations, this writer can categorically dispel the notion that cyber criminals are smarter than any of us. The fact is that almost all cybercriminals are simply users of hacking tools developed by others, and yes, that included those tools developed by our government that were leaked out to the world. Criminals use those tools just like we use Microsoft Office, but instead of building a spreadsheet or presentation, criminal hackers use their tools to steal information. Instead of using telephones or snail mail, they now have computers and emails. There are very few individuals who actually develop the software or discover the vulnerabilities themselves and use them for evil. Most criminals are simply re-purposing existing, commercially available software tools and using them for a malicious purpose.

Many cybersecurity professionals often feed into the myth by exaggerating the theoretical versus the practical reality. Some can over complicate the concepts and terminologies, when there are much easier ways to explain a cyber-attack.

COMPONENTS OF CYBER ATTACKS AND THE RELEVANT THREAT INTELLIGENCE

There are six components involved in every cyber-attack and every hacking.

1. **Attacker:** Cyber criminal/actor

2. **Victim:** Target

3. **Payload:** A general umbrella term that covers all software, also known as codes, which instruct the computer to perform specific functions after it is delivered onto the system

4. **Exploit:** A method or technique that can bypass security features so the computer will allow you to do the things you want it to do (but not what it was originally instructed to do)

5. **Delivery Vector:** How the attacker chooses to send the exploit and/or the payload onto the victim's system

6. **Command & Control:** Usually the most misunderstood and overlooked aspect in cybersecurity – the concept is straight forward: if someone wants to do something to your computer, there has to be a network connection from the attacker to the victim during all the aforementioned stages of exploitation, payload delivery, data exfiltration or any other payload objectives, where the attackers can perform all the functions they set out to accomplish, hence, commanding and controlling the various components and stages of the attack.

It does not matter whether the perpetrator uses low sophistication techniques to deliver a virus via a thumb drive, or a highly sophisticated nation-state level actor using zero-day exploits to remotely deliver seemingly undetectable payloads that are also known as Advanced Persistent Threat (APT). There are always six components involved in any attack.

LOOKING FORWARD

In a business that thrives on myth and fear, the threat intelligence industry is driven to perpetuate panic among the masses. Some hype the mythical super villainous attackers with magical powers, then espouse gratuitous technical terms to exaggerate the complexity unnecessarily. A lot of threat intelligence is generated simply for the sake of perpetuating this falsehood in order to drive business. This approach often confuses consumers.

Many organizations invest a significant amount of resources to meet compliance requirements, but are reluctant to spend just a little money to procure threat intelligence. Often decision makers do not fully appreciate the fact that compliance satisfies only regulatory and commercial requirements, and does very little in advising the decision maker of the actual state of information security. When an organization finds itself in a situation of non-compliance, the repercussions are fines and perhaps some lost business. However, if an organization fails to acquire the proper threat intelligence and suffers a cyber-attack, then the cost will be significantly higher. It is essential for decision makers to become better informed about cyber threats and the value of obtaining solid and actionable threat intelligence. Cyber threat intelligence is a wise investment. It is critical in order to design a cybersecurity solution which is customized to the threats that an organization is currently encountering, as well as those cyber threats they may face in the future. Organizational cybersecurity strategy should be threat-based cybersecurity tailored to the unique situation, rather than compliance-based cybersecurity solely aligned to generic government or industry information security standards.

This was an excerpt from ***Cybersecurity in the Digital Age.*** More information on this publication can be **obtained here**.

To learn more about threat intelligence, please contact the author, Eric Chuang (Managing Director, Cybersecurity Advisory Services) or Gregg Garrett (Head of U.S. and International Cybersecurity).

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.