Cyber Use Case

Adam Etches – April 2017

Background

Commoditization of advanced techniques.

Typically, when experts discuss the distribution of cyber threats, the 80/20 principle is brought up — meaning 80 percent of cyber actors are generally less sophisticated and the top 20 percent are so advanced that given enough time and resources they will break into any network. Historically, the top 20 percent of actors were mainly the concern of the defense and intelligence communities. Now, the emergence of commoditized threats has spread advanced techniques to a larger audience. For example, the 2006 emergence of the "Web Attacker" exploit kit introduced a packaged suite of tools that any user could operate.

Sophisticated developers who spent years honing their hacking techniques can now outsource their experience in a kit. The popular "BlackHole" exploit kit emerged in 2010, with more advanced techniques like zero-day exploits and social engineering modules to lure victims. These exploit kits are often sold on the dark web, some netting the developers nearly USD 50,000 per day. The widespread use of these kits has spread the tactics, techniques and procedures (TTPs) of top-tier actors to a much larger group.

Rise of the asymmetric threat.

The domain of cyber conflict has evolved into a state, wherein a hacker using a USD 500 laptop and some innovative techniques can penetrate a network where millions in USD are invested in security. Not even cyber industry leaders are free from the asymmetric threat:

A well-known security organization was infiltrated using a relatively unsophisticated technique of phishing employees with a malicious spreadsheet titled *2011 Recruitment Plan*. The ongoing conflict in the cyber domain has become a human problem with individual hackers continuously outwitting common security systems and the individuals responsible for security.

Too much data and too many tools.

Just obtaining the proper data for network visibility is an enormous task. Now, the modern network has massive amounts of tools and data storage recording every log, alert and heartbeat. There is so much data that a single analyst could spend a lifetime sifting through the disperate sources to discover relevant events. Compounding the issue of too much data is the confusing array of security tools, which must be constantly maintained and configured. According to the IBM Security Services 2014 Cyber Intelligence Security Index, over 95 percent of all investigated incidents may be caused by misconfiguration or lack of proper maintenance. The information security team may very well have the indicators and solutions about a cyber-attack, but the complexity of existing solutions makes it difficult to discover answers in real time.

Not enough experienced personnel.

Both the public and private sector are rapidly seeking to expand their cyber security ranks with qualified personnel. While demand for such positions in the last few years has risen dramatically, the training, experience and recruitment of such personnel will take time to catch up. According to a recent Rand Corporation study, between 2007 and 2012 listings for cyber security positions rose 73 percent, 3.5 times more than other computer-related postings. This demand has led to an average of 22,000 security jobs unfilled according to online career sites. Without an experienced team it is very difficult to keep up with the constant security operations.

Roles, responsibility and terminology.

To begin an intelligence-driven approach we must define the lexicon and outline specific roles. Cyber security must be thought of as a profession with formal training, qualifications and continuing education. The first such differentiation that must be drawn is between the *operational* aspects of security and the eventual product that is created. Thus, we should define the difference between *analysis*, *analytics* and *intelligence*:

Analysis is the examination, inspection and investigation of relevant data in order to reach a conclusion. Generally, this is a human-led and a manual process.

Analytics is the systematic and procedural computational analysis of data or statistics in order to produce a result. Generally, this process is automated and heavily assisted by a computer.

Intelligence is the ultimate result of the collection of valuable information, produced in a format that can aid a decision or conclusion.

Use case overview.

Using advanced analytics tools utilizing open source intelligence, data fusion, enrichment and multi-dimensional analysis this use case will examine traditional intelligence analysis tools and techniques applied to a cyber domain and how these may need to evolve. This use case will focus to two main functions of a cyber analyses which have similarities to traditional intelligence analysis.

Reactive Analysis

Given an event of a cyber nature, an event targeted at a computer network such as a malware or denial of service attack how can an analyst investigate this event to answer the following questions:

- Attribution - who perpetrated the attack?
- Extent - what is the extent of the attack and which systems have been affected?
- Data loss - has there been any breach of data?
- Remediation - what steps need to be taken to remediate this event and future events?

Proactive Analysis

Given the knowledge that many government and commercial networks are targets for cyber criminals, how would an organization defend and protect its network against attack? These activities have been given the name ‘Threat Hunting’ and many organizations are now engaged in this activity. From traditional intelligence analysis this is an ‘unknown unknowns’ analysis where both the threat and the actors are unknown. Here the analytical process will focus on open source datasets to assess specific and threats and actors who may be targeting the organization.