Security Intelligence: Information Sharing Strategies Using Trusted Collaboration

Executive Summary

Human-source intelligence (HUMINT) has been used for thousands of years by adversaries to thwart an enemy's intentions. The challenge for the recipient of raw intelligence is validating whether or not the information gathered is accurate and can be used effectively in a timely manner. The results of intelligence collection can be ambiguous at best and often lacks standards; therefore, raw intelligence must go through a number of steps to assess its value.

Where enterprise and network security is concerned, cyber Intelligence services began evolving over the last decade to provide an additional ad-hoc layer of "threat source" awareness to existing static security controls. These first forms of third party intelligence services were developed to increase threat space awareness in existing security controls but it lacked the in-depth analysis required and ultimately quality suffered.

The practice of using raw intelligence—without some form of human or machine-based analysis—creates a significant increase in false positive and negative alerts. Therefore, a lot of manual intervention is required to trim the block list to an acceptable size for a given security control, while also increasing the time and effort in forensic analysis to weed out misleading or non-relevant threats. To overcome these limitations, the next logical step for threat intelligence services is the ability to deliver greater accuracy and more effective protection against many different threat types—such as email attacks and Zero Day exploits—and not just potentially "bad" IP-addresses.

When researching security incidents, corporate IT staff often work in isolation and are reluctant to collaborate or share any information with untrusted external resources. Their main concern is centered on information control. Once released, there is no way to monitor or control who has subsequent access to that information. Unfortunately, there is little trust and collaboration between companies competing in the same marketplace. Often facing similar threats, the help and collaboration between companies is almost non-existent. To succeed in the long term, organizations must collaborate in the short term to achieve a common goal.

For organizations to break free from the continuous and unrelenting security and compliance treadmill, companies and their IT resources must band together and pool resources to become more effective against cyber threats. This fundamental shift away from the current behavior of many security practitioners and IT Staff can herald a new era in information dissemination and collaboration between trusted, third party entities. By leveraging some concepts of crowd sourcing, this new approach can immediately benefit a much wider audience, lessen the overall burden and workload, while at the same time reducing the concerns of sensitive data leakage that could lead to further compromise.

This white paper explores some of challenges faced and strategies that could be used to increase the effectiveness of security intelligence collection, analysis and the sharing of information to benefit trusted organizations or the information security community as a whole.

The Constantly Changing Threat Landscape

The Internet and network connectivity has become the lifeblood of financial, business and government operations requiring effective up-to-date intelligence to mitigate threats, safeguarding transactions, sensitive information and intellectual property from data theft and network compromise.

Ten years ago, cyber-threats were somewhat benign and noisy in nature—passive and consisting mainly of eavesdropping and brute force password guessing. Today, threats targeting organizations are much more inva- sive and crafted by organized crime using advanced malware and money laundering techniques. The threats facing organizations today include phishing, Trojan horses, Man-in-the-Browser, and Watering-hole attacks—many of which leverage technology to mask the source of an attack.

The most common threats include:

- Perimeter Security Control and Website Compromise. Attacks that typically target Internet facing IP addresses to exploit vulnerabilities in services or misconfigurations in perimeter security controls.
- Phishing. Phishing is masquerading as a trusted party in an electronic communication with links to a fake website in order to obtain account login information.
- Spear-Phishing. SpearPhishing is a targeted attack that attempts to compromise individuals within an organization using an apparently trusted element in an electronic communication.
- Watering-Hole Attack. An advanced attack relying on compromising and distributing malware and malicious code via trusted websites.

Attacks perpetrated against many organizations typically involve the penetration of websites and backend sys- tems to steal account data. Direct attacks against externally facing IP addresses of any Internet-based business continue to be a major concern and source of compromise. Even when best practices are followed and the necessary security controls are put in place, the network is too dynamic and requires a constant balancing act of changes to meet both business and security needs.

The Evolution of Threat Intelligence

In the days before the widespread adoption of firewalls and other security controls, the origins of threat intelligence began in the early days of SPAM filtering utilizing blocklists and allowlists. These lists were initially maintained by groups of individuals and focused on the IP addresses considered to be the source of SPAM attacks. The intelligence on the SPAM source IP's were accumulated from disparate system log files offered up by the user community. Unfortunately, the updates to these lists were sporadic, the intelligence inaccurate, and constantly increasing in size with heavy duplication—making them difficult to maintain.

Over the last decade, networks have become increasingly more complex due to the cumulative demands of user and connectivity requirements, business operations and regulatory compliance mandates. Companies spend billions of dollars on security controls to prevent unauthorized access to their network—and yet security breaches still occur. Breaches continue to happen due to the dynamism of attackers, the speed at which new threats circumvent existing security controls and the lack of up-to-date intelligence that realistically represents the true threat space.

Limited Threat Space Awareness and Raw Intelligence

Unfortunately, traditional point security vendor solutions have had limited threat space awareness due to product limitations and can only maintain an abbreviated list of the most common threats worldwide. Because of this limitation, third party security services have quickly evolved to focus on malicious IP blocking to help fill in the gaps left by vendors. This first iteration of security intelligence provided an important and previously untapped source of information to increase the effectiveness of existing perimeter defenses. However, while valuable, the IP centric intelligence typically provided by many of these services failed to identify the different types of threats being launched and rarely provided adequate information to the end-user on attack payloads and help with remediation strategies.

Raw intelligence data that focuses on purely malicious IP addresses has an increasingly limited shelf life and value to the defenses of the enterprise network. The next generation of threat Intelligence-based technology requires accurate, relevant, and actionable data as a means to identify and disrupt malicious activity before it can reach critical services and compromise the integrity of the network. The challenge is validating that intelligence within a time period that the resulting data can be acted upon. No company has the time, money or human/machine-based resources to adequately cover all known threats across the entire Internet, therefore an alternative, collaborative approach must be adopted in order to succeed. The same processes used in cyber intelligence collection must mirror that of real world intelligence to include the additional steps of analysis, classification, and sharing based on knowledge and levels of trust.

Sharing Incident Information Externally

The cultural challenge around security information sharing raises organizational concerns across many different industries. The thought that an internal employee may inadvertently reveal sensitive data externally about an incident—in which case the data may be used against them—is a valid concern. For many IT security specialists, working in a silo of isolation greatly lengthens the forensic and threat mitigation process. Many believe that the incident, corporate embarrassment and information leakage leading to subsequent attacks can be contained by their silence. Unfortunately, when a resolution to an attack is found, the information that could help other businesses or partners impacted by the very same threat is rarely shared outside of the organization. If logs are shared with an external entity, it is a very time consuming process to sanitize sensitive or potentially damaging information and mistakes can easily be made—so very few do.

The threat intelligence services have quickly evolved beyond the daily, inconsistent updates from a single vendor source into a trusted collaboration model with multiple levels of intelligence and payload validation. Adding raw multi-source threat feeds and customer logs as an intelligence foundation requires appropriate resources involved to validate the initial data sets of intelligence. To turn these raw threat feeds into finished Intelligence, the information must be carefully evaluated to determine if it came from a reliable, trusted source. Once each source is verified, the raw intelligence from the curated feeds must be scrubbed for duplicates then distributed to other human agents—or converted into a machine-readable format—to quickly validate the accuracy and verify facts before the intelligence can be deemed actionable. This greatly improves the intelligence sources' initial quality, but additional steps are needed in order to help make it actionable.

Trusted Collaboration and Shared Threat Intelligence

With the staggering number of threats and the dynamic nature of attack payloads, IT security staff are quickly overwhelmed with the enormity of the security problems they face. Many are now breaking down the barriers to collaborate and communicate with peers beyond their corporate boundaries to find the answers they need. One approach that is unique to security intelligence is the crowd source approach of "Trusted Collaboration". A trusted collaboration model applied to security intelligence provides organizations with greater

flexibility when implementing a defense strategy and helps to increase the accuracy and speed of threat information dissemination. Instead of being limited to the almost static capabilities of traditional security solutions, intelligence validated through trusted collaboration provides business with a more accurate assessment of risk, in addition to the faster mitigation of risk using higher quality, field validated information. This validated threat intelligence can then be applied to SIEM's and other security controls to increase accuracy and reduce false positive and negatives rates, while at the same time reducing the overall attack surface of the organization.

However, trusted collaboration and shared security intelligence—without the necessary human vetting and validation tools—is potentially open to manipulation by attackers using social engineering to masquerade as legitimate group members. To counter this type of infiltration, constant monitoring, controls and other data vetting procedures must be stringent enough to weed out any potential outliers or subversive "false flag" information to maintain the integrity of the data set.

The continued adoption of trusted collaboration will ultimately allow IT Departments to share information and validate data with trusted external entities without the need to obfuscate and share potentially sensitive log information. Working together, organizations can quickly create circles of trust to foster external group collaboration with trusted peers, in effect leveraging the security knowledge and resources of the organizations within a secure system to the benefit of circle.

Summary

New innovations in technology have not only increased the capabilities of legitimate organizations but also those of illegitimate cybercriminals and organized crime. With layers of security controls already in place, organizations continue to succumb to attacks that bypass traditional security measures due to the lack of timely and accurate intelligence that could have been used to mitigate the risk and reduce the attack surface further. With multiple vendor intelligence sources and disparate, non-validated data sets derived from customer event logs, security intelligence can be somewhat of a "hit and miss" technology without some form of human or machine-based vetting and validation. By automating the collection, risk ranking, de-duplication of threat intelligence, organizations can significantly save time and reduce overall cost by a large factor while strengthening their defense and response times.

In order for businesses to continue to leverage existing investments in their layered defenses, integrating security threat intelligence services such as OPTIC by Threat Stream can help minimize the attack surface of the network by using timely, accurate and validated sources of intelligence data to lower business risk.

Threat Stream's "Trusted Collaboration" model drives each "Circle of Trust"—an approach to external intelligence sharing that benefits the collective efforts of the group and leverages the previously siloed efforts of IT teams and security specialists without leaking sensitive data. Trusted collaboration can help ensure the control of incident information and who has access to it. Finally, trust and collaboration between companies competing in the same marketplace and often facing similar threats—can now work together to achieve a common goal without compromising the integrity of their network or their business as a whole.

About Anomali

Anomali is the leader in global intelligence-driven cybersecurity. Our customers rely on us to see and detect threats, stop breaches, and improve the productivity of security operations. Our solutions serve customers around the world in every major industry vertical, including many of the Global 1000. We are a SaaS company that offers native cloud, multi-cloud, on-premises, and hybrid technologies. As an early threat intelligence innovator, Anomali was founded in 2013 and is backed by leading venture firms including Google Ventures, IVP, General Catalyst, and several others. Learn more at www.anomali.com.