KNOW YOUR ENEMY:

THE ROLE OF BIG DATA, CROWDSOURCING AND MACHINE LEARNING IN CYBER-SECURITY

Today's cyber-security threat landscape is vast and expansive; so much so that organizations are becoming overwhelmed. IoT bonnets, DNS attacks, SSL-encrypted assaults, ransom DDoS, zero-day malware outbreaks…the sheer volume of today's attack landscape makes identifying these threats quick enough problematic to say the least. Yet the ability to ascertain them before they unleash their malevolent intentions has become crucial to successfully mitigating them. The key? Know your enemy.

To know your enemy requires access to real-time information, lots of data, the proper tools to correlate and process this information and the expertise to act on it. Just like law enforcement, security teams must develop "cyber fingerprints," or the attributes and characteristics that define a particular attack vector, so DDoS mitigation and network security solutions can be configured to stop cyber-attacks in their tracks.

Data is the key. The future of automated security will evolve into an ecosystem of virtual intelligence learning from big data, informing network perimeter defense, and then collecting big data from both perimeter and endpoint security and the network's traffic flow – in real time as well as over long trend lines.

WHAT'S STOPPING YOUR ORGANIZATION FROM USING HUGE VOLUMES OF DATA?

Large organizations already have huge volumes of data at their disposal. It flows from a diverse set of sources including intrusion detection systems, network infrastructure, server and application logs and more. The data can quickly add up, totaling petabytes in size.

In practice, this means having enough processing power to analyze billions of records within seconds, and more importantly, have the in-house expertise to digest, interpret and take the proper course of action.

Normally, Security Information and Event Management (SIEM) platforms are used to manage all this data. However, many of these solutions were not built with big data in mind. Threat detection devices can produce petabytes of log data that need to be contextualized and analyzed in real time, but processing it takes significant computing power. Similarly, most security teams only have access to a few weeks of historical data as storing all this information at scale can be expensive, limiting their ability to identify attacks over long periods of time and to conduct forensic reviews.

Lastly, problems occur when high volumes of false positives are produced by SIEM tools. With so much data captured, it's easy to identify hundreds of suspicious events each day. Some may signify a compromised network, however many do not. Relying on individuals to review hundreds of alerts, including a large number of false positives, results in alert fatigue.

This last issue highlights a final issue: human expertise. Due to the rise of easy-to-use attack tools and anonymous payment mechanisms, the motivation for attacks is expanding into new domains such as ransom and hacktivism; yet the growing need for security expertise necessary to protect an organization is in direct contrast to the shortage of expert security personnel available to handle the job. Even with the best protection devices and a knowledgeable staff, DoS attacks, IoT botnets, ransom attacks and malware outbreaks present a major challenge to your business.

What's an organization to do?

A CYBER SECURITY INTELLIGENCE AGENCY

The sheer volume and expansive nature of the cyber-security threat landscape combined with the difficulties associated with information overload denotes that organizations need assistance. Enter your DDoS mitigation vendor, which should serve as an "intelligence agency," providing unique, real-time intel on emerging DDoS threats for preemptive protection. This data should come from a variety of sources.

Scrub-a-Dub-Dub
Leading DDoS mitigation vendors provide a cloud-based security network. This global network of scrubbing centers, providing 24x7 DDoS attack mitigation to customers, is perfectly positioned to validate DDoS attackers actively engaged in cyber assaults and pass that information to customers.

Deception Is the Name of the Game
Leading DDoS mitigation vendors run deception networks – honeypots – to attract hundreds of thousands of malicious IPs and use analytics and Big Data to catalog and identify new and emerging threat actors, including botnets, DNS attackers, spoofing, etc.

The Power of the Crowd
Zero-day malware has become one of the biggest data-stealing threats. To safeguard their most prized digital assets, organizations need to rely on the power of the crowd. The power should be delivered via its DDoS mitigation vendor, which can leverage a global community of millions of users from which to collect live intelligence and analyze it via machine-learning algorithms to proactively detect previously unknown malware.

Battle-Proven Expertise
Lastly, any DDoS mitigation vendor should complement the organization's in-house security expertise with its own battle-proven security experts, which rely on machine learning and algorithmic research to discover new attack vectors and provide 24x7 support in the event of a DoS attack or malware outbreak.

DDoS services like these allow an organization to develop an ecosystem of virtual intel by learning from others, turn raw data into actionable intelligence via brain-busting Big Data processing and shield networks and digital assets before the attack hits. When partnering with a DDoS mitigation provider, ensure they can provide the aforementioned services to complement your security teams' in-house expertise and data-processing capabilities.

LEARN MORE ABOUT RADWARE'S ERT ACTIVE ATTACKS FEED AND CLOUD MALWARE PROTECTION SERVICES.