Datasheet

Blue Hexagon for Encrypted Traffic

Threat Detection For Encrypted Traffic Harnessing the Power of Deep Learning

Attackers Are Hiding In Encrypted Traffic

Analyst firm Gartner believes that, "Through 2019, more than 80 percent of enterprise web traffic will be encrypted."[1] While encryption addresses privacy and legal requirements, security teams now face a challenge where they are blind to a large influx of traffic. In fact, Gartner also predicts that "During 2019, more than fifty percent of new malware campaigns will use various forms of encryption and obfuscation to conceal delivery, and to conceal ongoing communications, including data exfiltration."[1]

Blue Hexagon offers a two-pronged approach to address threats in encrypted traffic:

1. Security teams can **decrypt the traffic** using Blue Hexagon partner firewall and switch solutions such as Palo Alto Networks, Gigamon, F5 Networks and A10 Networks before sending it to Blue Hexagon for inspection. This solution integrates and scales seamlessly with the network infrastructure architecture.
2. **Enable Blue Hexagon deep learning inspection for Encrypted Traffic.** Unlike JA3 signatures which can create false positives, or analysis of "anomalous" protocol header communications/ netflow, Blue Hexagon inspects encrypted traffic in real-time and provides definitive verdict on threats without negatively impacting network speed and performance, or requiring additional devices.

Blue Hexagon for Encrypted Traffic delivers threat protection powered by deep learning to detect threats in encrypted traffic.

Approach 1: Decrypt Traffic on Switch or Firewall

As shown in Figure 1, Blue Hexagon integrates with next-generation firewalls like Palo Alto Networks or switches such as Gigamon, Ixia, A10 Networks and F5 Networks to decrypt traffic before inspection by Blue Hexagon. This integration brings several benefits:

- Selected and relevant traffic can be sent to Blue Hexagon for inspection.
- Links with low-traffic volumes can be aggregated together before being sent to Blue Hexagon.
- Supports asymmetric routing architectures to maintain session information.

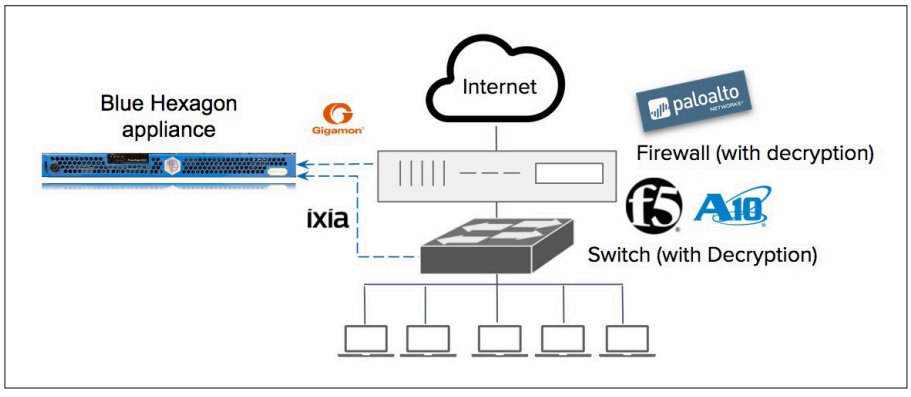

Figure 1: Traffic decryption by firewall or switch prior to Blue Hexagon deep learning inspection

[1]*Gartner, "Predicts 2017: Network and Gateway Security," Lawrence Orans et al, 13 December 2016.*

Approach 2: Blue Hexagon Deep Learning Inspection of Encrypted Traffic

For certain organizations with privacy and data confidentiality restrictions, decryption of encrypted traffic to perform threat inspection may not be possible for compliance reasons. For these organizations, Blue Hexagon offers deep learning-powered inspection of Encrypted Traffic.

The Blue Hexagon proprietary Deep Learning HexNet™ architecture detects suspicious patterns that can be observed in the SSL/TLS communications during different stages of the connection. The deep learning models are trained on thousands of observations and characteristics that are used to separate a malicious encrypted tunnel from benign communications channels. Such patterns are tightly bound to the core communication functionality of the client and server encryption process.

As a result, deep learning can identify and stop attacker mal-intent and threats in these communications channels even when the channel is encrypted. In contrast to slower analytics or hunting solutions that use correlations over large volumes of data or signature mechanisms like JA3 which can be fast but result in lots of alerts, the Deep Learning HexNet models provide instant and accurate verdicts as they observe the connection evolution over time. Blue Hexagon's payload analysis engine also uncovers new threats earlier than traditional engines, allowing the encrypted communication model to keep learning from new mal-intent communication patterns being used by adversaries.

Examples of use cases for Blue Hexagon encrypted traffic analysis using deep learning include the following:

- Download of a payload over an encrypted channel from a malicious or compromised website.
- Detection of encrypted command and control communications from a compromised endpoint from within the enterprise network.
- Download of a payload by a malicious entity already residing on an endpoint inside the enterprise network. This often happens in the later stages of the killchain following the initial delivery.

In a recent deployment at a software outsourcing company, Blue Hexagon **discovered 60,000 encrypted communications beaconing to the attacker domain in one day.**

Generations of Solutions For Detecting Threats In Encrypted Traffic

1st Generation: Signature-based

Inspection of ciphers and strengths, certificate signer, revocation list. No longer effective due to self-signed certificates.

2nd Generation: JA3, JA3S

Identifies malicious communications by fingerprinting TLS negotiation between client/server. Also correlates based on SSL library used by application, which is unfortunately also used by benign applications. Accuracy and overage shortfalls.

3rd Generation: Anomaly Detection

Identifies network protocol anomalies to predict threat propagation. Occurs post-compromise. Network patterns can be very complex and anomaly detection can create lots of false positives and be a burden on threat analysts.

4th Generation: Deep Learning

System pre-trained with millions of benign and malicious SSL transactions. No baselining or anomaly detection involved. Broad feature space enables detection of completely unique and new SSL obfuscation techniques.

With the introduction of this feature, Blue Hexagon becomes the first security vendor to offer a consistent deep learning-based threat detection platform for on-premises and cloud, to detect threats in all traffic including encrypted web and network communications. More importantly, the ability to inspect threats in less than a second at greater than 99.5% efficacy enables security teams to keep pace with the onslaught of attacks.

Blue Hexagon is a deep learning innovator focused on protecting organizations from cyberthreats. The company's real-time deep learning platform is proven to detect known and unknown network threats with speed, efficacy, and coverage that set a new standard for cyber defense. Blue Hexagon is headquartered in Sunnyvale, CA, and backed by Benchmark and Altimeter Capital. For more information, visit www.bluehexagon.ai or follow @bluehexagonai.

Headquarters
298 S. Sunnyvale Avenue, Suite 205
Sunnyvale, CA 94086
www.bluehexagon.ai
inquiries@bluehexagon.ai

BH-ET-DS-08-07-19

BLUEHEXAGON