FLASHPOINT

BUSINESS RISK INTELLIGENCE FOR

CYBERSECURITY

Cyber-threat actors' evolving skills and techniques continue to disrupt mitigation efforts, creating challenges for cybersecurity practitioners across all sectors. In response, more practitioners are incorporating Business Risk Intelligence (BRI) into their defense strategies.

Gleaned from high-value sources that include the underground communities where cyber-threat actors operate, Flashpoint's BRI helps organizations address cybersecurity threats and challenges, such as:

EMERGING MALWARE

Cybercriminals work continuously to develop malware capable of bypassing security controls. Since new malware strains are typically discussed and distributed on the DDW before being deployed in the wild, insight into this activity can enable cybersecurity teams to anticipate and defend against new and evolving malware threats.

In one instance, Flashpoint uncovered the early-stage development of an unreleased malware strain. Analysts provided critical details about the malware, such as how it was developed, its encryption, and associated indicators of compromise (IoCs), enabling customers to proactively deploy appropriate countermeasures.

RANSOMWARE & CYBER EXTORTION

Ransomware and cyber-extortion attacks can enable criminals to profit by holding critical data or systems for ransom. Organizations that fall victim to these attacks must quickly assess and mitigate the incident, because in many cases, the longer an infection or extortion threat lingers, the greater the damages and disruption.

Flashpoint's Threat Response & Readiness Subscription guides organizations through the proactive development of an incident-response plan. If a ransomware or cyber-extortion attack does occur, Flashpoint helps customers quickly assess and respond with appropriate countermeasures.

BREACH VERIFICATION

Many threat actors operating on the DDW have been known to make false claims regarding their capabilities, intentions, or activities, making it difficult for security teams to identify legitimate threats. Flashpoint's extensive linguistic, social, and cultural expertise helps customers cut through the noise of DDW chatter to confirm the validity of suspected cyber incidents.

In one situation, Flashpoint observed a well-known threat actor on a DDW marketplace claiming to have access to a global corporation's internal network. Flashpoint analysts conducted a thorough investigation to verify the breach, subsequently supporting the customer's incident-response efforts.

In another situation where an actor claimed to have access to a company's network and data, Flashpoint analysts determined the threat was not legitimate, because the actor had not obtained access to any of the company's assets. With this information, the company was able to avoid wasting security resources on a false alarm.

INSIDER THREAT

Since most organizations' security programs are devoted to defending against external attacks, insider-threat activity is a common security blind spot that many teams lack the resources and expertise to address.

The Flashpoint Professional Services (FPS) Insider Threat Program helps customers assess their existing capabilities, identify organizational requirements, and build an effective insider-threat function tailored to those requirements.

In the event of a cyber incident caused by an insider, FPS provides customers with impact-based engagement services, including but not limited to investigating and analyzing the event, identifying and procuring sensitive data, and evaluating the extent of a breach.

DDOS ATTACKS

Flashpoint's visibility into the DDW communities where adversaries congregate and conspire provides insights to help companies proactively address DDoS attacks, which can have a disastrous effect on business operations and continuity.
In one instance, Flashpoint identified the vulnerability that ultimately gave rise to the Mirai botnet and subsequent DDoS attacks.

Analysts traced the vulnerability to an upstream supplier contracted by many Internet-of-Things (IoT) manufacturers. Flashpoint immediately alerted customers, so they could patch the vulnerability, enforce stricter quality controls on suppliers and technology partners, and mitigate service outages appropriately.