FLASHPOINT

Extortion Monitoring Service

Threat actor collectives constantly evolve their methods of extorting information and payments from victims. Attacks like ransomware, distributed denial-of-service (DDoS), or executive targeting, often result in sensitive information and assets being posted to public repositories. This evolving attack landscape highlights the need for extortion victims, incident response teams, and digital forensics teams to have insight into illicit communities and websites to identify potential exposure via third-party vendors. Teams need to swiftly identify and access relevant breached data in order to adapt and optimize internal response plans.

Overview

Powered by our extensive, signal-rich collections and alerting engine, Flashpoint's Extortion Monitoring Service delivers real-time automated alerts of identified leaked assets as a result of an extortion incident, providing teams with the necessary insight into the extent of exposure and damage.

Key Benefits

✓ CONTINUOUS MONITORING

In the event of a breach, stolen data could end up on illicit markets months or years after the initial compromise has occurred—potentially leading to legal ramifications and reputation damage. Extortion Monitoring provides pre-and post-event keyword monitoring based on your requirements, to continuously assess reputation and legal obligations beyond the conclusion of an investigation or incident response.

✓ STRONG BENCH OF RESOURCES AND COLLECTIONS

Flashpoint's multidisciplinary intelligence analysts speak over 35 languages and drive our global collections engine which accounts for our extensive collection of illicit communities. Our data and collections cover more regions, countries, and types of threat actors than our industry peers.

✓ REAL TIME ALERTS

Flashpoint’s automated alerting matches conversations from illicit online communities with keywords associated with the team’s areas of concern and automatically provides these matches directly to the user.

✓ ACCESS TO ORIGINAL COLLECTIONS

Users can access the original collections in a safe environment if additional information is needed to research or analyze an incident.

Use Case

SUPPORT FOR INCIDENT RESPONSE TEAMS; IDENTIFYING AND PREVENTING THIRD-PARTY RISK

When an organization's critical network service falls victim to a ransomware or cyber extortion attack, incident response teams require immediate insight into the extent and damage caused. As part of their response plan and investigation, internal teams must understand if and where sensitive data and assets have been leaked. More often than not, the stolen information is sold in illicit communities, which leads to further damage extending beyond the organization, including third-party vendors. Incident response teams must consider the organization’s third-party vendors as part of their response plan to ensure the full protection of sensitive assets.

Extortion Monitoring supports incident response teams by providing immediate notification of identified leaked assets as a result of an extortion incident, thereby saving internal teams time and resources. Flashpoint sheds light on the extent of the exposure and damage, as well as the context surrounding the threats, in order to take immediate action and mitigate further risk. Our post-incident support ensures that internal teams have the tools and resources required to ensure extended protection that aligns with the organization's requirements.