Compromised Credentials Monitoring

Threat actors are continually targeting employee and customer credentials through various means, including phishing and brute-force attacks. As the methods used by threat actors to steal credentials evolve and leaked data is readily available online, defenders are at an ongoing disadvantage and increasingly vulnerable to account takeover, fraud, and misuse.

As the technology and tools to leverage stolen credentials advance, organizations must have awareness of their exposure to credential breaches, as well as exposed domains and passwords, to ensure their employees or customers are not at risk of having their accounts taken over.

Visibility into the illicit communities where credentials are leaked is another challenge. Flashpoint's unique access to compromised data—whether from closed forums, chat services platforms, publicly released data leaks, or via private threat actor groups—equips organizations with the data needed to mitigate risk to their business and customers.

Available Offerings

Flashpoint Compromised Credentials Monitoring (CCM) allows users to monitor exposure of compromised credentials for their enterprise domains and customer email addresses to take action after breaches to mitigate risk of account takeover (ATO). Flashpoint's advanced technology quickly collects and processes data and credentials, allowing for organizations to access the most up-to-date breach data and receive notification as soon as credentials have been identified.

Flashpoint intelligence analysts have spent years monitoring illicit communities, and are armed with the skill sets and accesses to obtain data when and where compromised databases and credentials are exposed. Their familiarity with threat actor tactics, techniques and procedures (TTPs) allows them to identify recycled data leaks claimed by actors as new leaks, and ensure customers are provided the most relevant and recent compromised credentials.

ENTERPRISE

Abuse of enterprise credentials allows attackers onto your network and exposes sensitive business and personal data. Compromised Credentials Monitoring - Enterprise enables organizations to search and monitor Flashpoint's unique collections for compromised enterprise accounts and passwords in order to flag accounts, reset employee passwords, and restrict permissions to prevent actors from accessing confidential or personally identifiable information (PII). Flashpoint's ability to filter out compromised email addresses that do not meet an organization's password requirements, or identify only data from recent and relevant breaches, allows users to receive alerts on actionable data, saving time and resources.

CUSTOMER

Flashpoint Compromised Credentials Monitoring for Customers (CCM-C) allows organizations to monitor exposure of compromised credentials for customer domains and email addresses, enabling them to preempt fraudulent activity and protect their client base. By identifying these compromised customer accounts, organizations gain deep insights into the the types of domains being targeted, as well as the most vulnerable passwords. This enables them to better analyze and predict future attacks.

Flashpoint CCM-C also provides cookies data, which gives organizations additional insights into exactly how threat actors are maliciously leveraging their customer accounts to access and infiltrate their systems. By leveraging CCM-C cookies data from Flashpoint's robust data sources, which provide further intelligence and context on threat actor's tactics and techniques, organizations can develop a better understanding of how their customers and organization are being targeted and proactively build a better defense against ATO.

Key Benefits

- ✓ Integrate data within client's existing business processes to make it immediately actionable
- ✓ Gain insight into the types of domains being targeted, as well as the most vulnerable passwords
- ✓ Gain insight into compromised credential breach landscape
- ✓ Access credential data leaked in breaches in near real-time
- ✓ Identify accounts which have been hacked on a consistent basis in order to provide ongoing fraud monitoring without impacting user experience

ABOUT FLASHPOINT

Trusted by governments, global commercial companies, and educational institutions, Flashpoint helps organizations protect their most critical assets, infrastructure, and stakeholders from security risks such as cyber threats, ransomware, fraud, physical threats, and more. Leading security practitioners—including cyber threat intelligence (CTI), vulnerability management, DevSecOps and vendor risk management teams—rely on the Flashpoint Intelligence Platform to proactively identify and mitigate risk and stay ahead of the evolving threat landscape.

For more information, visit flashpoint.io or follow us on Twitter at @FlashpointIntel