Use Case: Third-Party Risk Monitoring

THIRD-PARTY COMPROMISED CREDENTIALS MONITORING

PROBLEM:

DON'T GIVE THREAT ACTORS THE KEYS TO YOUR KINGDOM!

While facilitating innovation and efficiency, the third parties you employ can be sources of compromised credential risk. Threat actors can use compromised accounts within your trusted third parties as a gateway into your own organization, triggering cyber incidents, such as data breaches or ransomware attacks. When the consequences of compromised credentials blight both stakeholder trust and the bottom line, you must seek strategies for protecting yourself against this third-party risk.

INTEL 471 SOLUTION:

UNIQUE AND COMPREHENSIVE COVERAGE

Intel 471 continuously monitors for compromised credentials relevant to your third parties and instantly alerts upon any instance of them. Using sources exclusive to its intelligence capabilities, including sophisticated malware intelligence and covert communication with threat actors, Intel 471 provides insight into tens of millions of unique data points for enhanced visibility of compromised credentials for sale. Rather than simply listing credentials, Intel 471 paints a full picture of the threat they present and the actor behind them, so your organization can act decisively against the threat.

KEY FEATURES:

- **Near real-time monitoring and alerting** of the sale or leak of relevant third-party compromised credentials and pre-attack indicators.
- **Early detection** of third-party compromised credentials to prompt immediate escalation from security teams.
- **Unique visibility** into spaces, such as exclusive forums and instant messaging platforms, where compromised credentials are bought and sold.
- **Credentials dashboard** for pain-free monitoring and assessment of key information related to third-party compromised credentials, including date ranges, occurrence across other data sets, and links to related intelligence reports.

KEY BENEFITS:

- **Enable a proactive security response** to the threat of third-party compromised credentials, such as account takeover, to mitigate their potential impact early on.
- **Informed decision making and strategic deployment of resources** thanks to fully contextualized threats.
- **Improve risk management** by using cyber threat intelligence to evaluate third-party relationships and ascertain the actor's tactics and potential identity to remediate future incidents.
- **Stay ahead of the ever-evolving nature of cybercrime** by tracking threat actors wherever they go via Intel 471's continuously enhanced coverage of the dark web.

MONITOR THIRD-PARTY COMPROMISED CREDENTIALS WITH INTEL 471

Third-party compromised credentials monitoring is part of Intel 471's Third-Party Risk Monitoring set of capabilities. It is designed for organizations who want to reduce risks associated with third-party interactions, products, and services. Third-Party Risk Monitoring solutions provide customers with threat intelligence and information to assist with the identification and remediation of risks introduced by interconnected vendors, customers and other third-party entities, and includes:

- Third-party vulnerability monitoring
- Third-party breach monitoring
- Third-party compromised credentials monitoring
- Supply chain risk monitoring

ABOUT INTEL 471

Intel 471 arms enterprises and government agencies to win the cybersecurity war using real-time insights from the cyber underground. Organizations leverage our cyber intelligence platform to protect from costly security breaches and cyber incidents by solving real-world use cases, including third-party risk management, security operations, attack surface protection, fraud and more. Learn more at www.intel471.com.

Your Voice of Reason and Truth.

SALES@INTEL471.COM