DATASHEET

SpyCloud

FINANCIAL THREAT PROTECTION

PAYMENT CARD EXPOSURE INTELLIGENCE ACROSS YOUR ECOSYSTEM

THE PROBLEM

Criminal actors are financially motivated, and stealing consumer payment card data is one of the fastest and most reliable ways to monetize illicit activity. Payment card information is commonly harvested through company breaches, infostealer infections on desktops, and mobile malware on compromised phones.

These attacks result in the large-scale exposure of credit, gift, and loyalty card data, often including far more than just the card number. Stolen records frequently contain full account details and associated PII, such as email addresses, phone numbers, bank account and routing numbers, and other identity attributes – significantly increasing the value of the data and the downstream fraud risk.

THE SOLUTION

SpyCloud Financial Threat Protection delivers early visibility into compromised payment card data by recapturing intelligence from millions of infected devices, phishing sites, and breach sources every month.

This intelligence enables card issuers, payment processors, retailers, and other institutions across the payments ecosystem to identify exposed payment cards, disrupt criminal use of compromised financial data, and prioritize remediation before fraud occurs. By acting at the point of exposure, organizations can reduce losses, limit customer impact, and strengthen trust across payment and commerce workflows.

USE CASE EXAMPLES

Customer Identity Protection
Increase customer retention and provide added value by checking customers' issued credit, gift, and loyalty cards against breach data to mitigate exposure

Fraud Prevention
Leverage breached payment card data details for your anti-fraud initiatives

Exposure Management
Proactively handle client credit card exposures with a list of breached payment cards

SpyCloud

HOW IT WORKS

SpyCloud Financial Threat Protection enables automated identification and remediation of exposed payment cards across multiple integration models. Organizations can use the API in one of two primary ways, depending on their operational needs and data workflows.

TARGETED MONITORING – Query by BIN

Organizations can query the API using one or more Bank Identification Numbers (BINs) to retrieve exposed payment card records associated with specific card programs.

- Submit one or multiple BINs (up to 10 per request) via a RESTful API
- Receive all matching compromised card records linked to those BINs
- Card numbers are returned as SHA-1 hashes, enabling secure matching without exposing raw PANs
- Ideal for card issuers, processors, and program owners monitoring specific portfolios

Use cases

- Ongoing monitoring of issuer- or program-specific cards
- Automated card reissuance workflows
- Fraud prevention and exposure-based risk scoring

BROAD COVERAGE – Full Compromised Card Feed

Organizations can retrieve all compromised payment card records observed by SpyCloud – across credit, debit, gift, and loyalty cards – without limiting queries to specific BINs.

- Access comprehensive visibility into exposed payment cards across the ecosystem
- Enables bulk ingestion for large-scale analysis, enrichment, and remediation
- Designed for organizations that need broad exposure intelligence, not just issuer-specific views

Use cases

- Payment processors and acquirers monitoring cross-portfolio exposure
- Retailers identifying compromised store-issued cards
- Risk, fraud, and analytics teams correlating card exposure with downstream abuse

SpyCloud

API FIELDS

FIELD	VALUE EXAMPLE	DESCRIPTION
source_id	12322	Maps to a specific breach or source of data
log_id	sha256	For malware sourced data, the SpyCloud LogID value
document_id	alphanum	For non-malware sourced data, this value corresponds to the record that contained the data
infected_time	2023-01-01T00:00:00	The UTC ISO8601 formatted time string of the closest time we know to the time the data was stolen
spycloud_publish_date	2023-01-01T00:00:00	The UTC ISO8601 formatted time string of the closest time the data was published by SpyCloud
cc_number	62bf57c3250af4bed907b5091e034a83bd223d9a	Credit card numbers are stored and displayed using a SHA-1 hash by default. Customers can opt for SHA-256 or SHA-512 by contacting SpyCloud
cc_number_plaintext (optional field)	xxxxxxxxxxxxxxx	Credit card numbers delivered in plaintext
cc_bin	51051051	BIN / IIN of the card
cc_last_four	5100	Last four digits of card
cc_type	Visa	The type of card, when we know it
full_name	Bob Smith	Name directly associated with the card
cc_expiration	01/2001 (MM/YYYY)	Expiration of card, where day field is the last day of month if not otherwise known
cc_code	123	Credit verification value (CVV)
postal_code	100-01A5	Card postal code (international postal codes have a variety of formats)
cc_gateway	Stripe	The gateway used to check the validity of the credit card data

SpyCloud

API FIELDS CONT'D

FIELD	VALUE EXAMPLE	DESCRIPTION
ip_addresses	"ip1" , "ip2"	IP addresses corresponding to the victim machine
email	user@domain.com	Email addresses associated to this victim
infected_path	"c:\windows\system32\0wn4ge	Install path of the malware
phone	"+44 11 222 23232"	Phone number found on the victim machine
user_hostname	WIN232-1233	Computer name of the victim's computer
system_model	Android	Model of the system infected
user_sys_registered_owner	"George Lucas"	System owner information
infected_time	"2023-01-01T00:00:00"	The time when the user's system was infected with malware

ABOUT SPYCLOUD

SpyCloud transforms recaptured darknet data to disrupt cybercrime. Its automated identity threat protection solutions leverage advanced analytics to proactively prevent ransomware and account takeover, safeguard employee and consumer accounts, and accelerate cybercrime investigations. SpyCloud's data from breaches, malware-infected devices, and successful phishes also powers many popular dark web monitoring and identity theft protection offerings. Customers include seven of the Fortune 10, along with hundreds of global enterprises, mid-sized companies, and government agencies worldwide. Headquartered in Austin, TX, SpyCloud is home to more than 200 cybersecurity experts whose mission is to protect businesses and consumers from the stolen identity data criminals are using to target them now.

To learn more and see insights on your company's exposed data, visit **spycloud.com.**