DATASHEET

SpyCloud

COMPROMISED CREDIT CARD API

REMEDIATE EXPOSED CREDIT, GIFT, AND LOYALTY CARD DATA AND PROTECT YOUR CONSUMERS, YOUR TIME, & YOUR BRAND

THE PROBLEM

The main objective of criminal actors is to profit – and stealing consumer credit and store card information is an easy and preferred path for criminals looking to achieve their monetary-driven goals. Criminals obtain this data through breaching companies, infecting desktops with infostealers, or infecting cell phones with mobile malware. This results in the costly exposure of credit, gift, and loyalty card information that includes full account details, often beyond just the card number: email address, account and routing numbers, phone numbers, and other associated PII.

THE SOLUTION

SpyCloud researchers recapture data from millions of infected phones and computers, phishing sites, and breaches every month – delivering exposed credit, gift and loyalty card details to organizations that can disrupt criminal use of these financial details. This data enables card issuing financial institutions and retailers to prevent loss due to fraud and proactively protect their clients from becoming victims.

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 credit, gift, and loyalty card data details for your anti-fraud initiatives

EXPOSURE MANAGEMENT

Proactively handle client credit card exposures with a list of breached credit cards by issuing BIN

HOW IT WORKS

The SpyCloud Compromised Credit Card API helps to automate exposure remediation – returning exposed credit, gift, or loyalty card records from a query of 6 character BIN(s) via a RESTful API with JSON output. A customer system or user would query the endpoint with one or multiple (up to 10 at a time) BIN(s) and receive all matched card records (with credit card numbers returned as SHA1 hash).

NOTE FOR RETAILERS: Any credit, gift, and loyalty cards must exclusively contain digits only, not characters – with a minimum of 12 digits, and a maximum of 28 digits for all retail-issued cards.

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	5105105105105100	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_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

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 protect businesses from cyberattacks. Its products operationalize Cybercrime Analytics (C2A) to produce actionable insights that allow enterprises to proactively prevent ransomware and account takeover, safeguard employee and consumer identities, and investigate cybercrime incidents. Its unique data from breaches, malware-infected devices, and other underground sources also powers many popular dark web monitoring and identity theft protection offerings. SpyCloud customers include half of the ten largest global enterprises, mid-size companies, and government agencies around the world. Headquartered in Austin, TX, SpyCloud is home to more than 200 cybersecurity experts whose mission is to make the internet safer with automated solutions that help organizations combat cybercrime.

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