DATASHEET

SpyCloud

INVESTIGATIONS API

EMPOWERING ANALYSTS WITH DARKNET INTELLIGENCE

THE PROBLEM

Analysts and investigators increasingly recognize how OSINT data can support their work — that there is power in breached data made publicly available by bad actors. Often this underground data contains elements from attackers themselves. Those who perpetrate data breaches and online fraud or share stolen data with other criminals can be de-anonymized using this very data.

SpyCloud collects data circulating within criminal communities – not only breach data, but also malware logs and information from other covert sources. We make it actionable to protect organizations and their customers. Our researchers recover, on average, 12 billion assets per month. The result is a wealth of information investigators can put to use to protect users, discover information about adversaries, and shortcut their discovery of critical information.

PRODUCT OVERVIEW

SpyCloud Investigations API enables investigators to piece together decades-worth of criminals' digital breadcrumbs to reveal the identities of specific adversaries engaging in commercial compromise, online fraud, and other illegal activities. Simply put, SpyCloud Investigations makes it faster and more efficient to prevent adversary activity, protect users, understand tactics, techniques, and procedures (TTPs), and make informed decisions.

BENEFITS AT A GLANCE

GAIN SPEED & EFFICIENCY

Shorten the timeline of your investigations with deep results based on even limited information, including email address, domain, IP address, password, and more

CORRELATE MULTIPLE DATA SOURCES

Connect SpyCloud with disparate data sources, including internal data and OSINT data sources such as VirusTotal, Passive DNS, and Whois to add even more context to your investigation or analysis

DISCOVER THE UNDISCOVERABLE

Unmask specific threat actors and their alternate personas, research criminal campaigns and their infrastructure, and open up new angles of investigation by pivoting on known and newly discovered data points

INTEGRATE WITH YOUR PREFERRED TOOLS

The SpyCloud Investigations API is compatible with popular analysis tools including Maltego, Jupyter Notebook, Splunk, and others – delivering visualizations for a more robust understanding of complex digital personas

ANALYST SERVICES & TRAINING

Our analysts work with your team to perform high-level or detailed analyses, peer reviews, briefings on specific findings, and ad-hoc training to shorten the learning curve of analysts new to SpyCloud or OSINT investigations

KEY USE CASES


RANSOMWARE PREVENTION


FINANCIAL CRIMES RESEARCH


THREAT ACTOR ATTRIBUTION


INSIDER RISK ANALYSIS


CREDENTIAL STUFFING ANALYSIS


INFECTED HOST IDENTIFICATION

CYBERCRIME INVESTIGATIONS POWERED BY RECAPTURED DATA

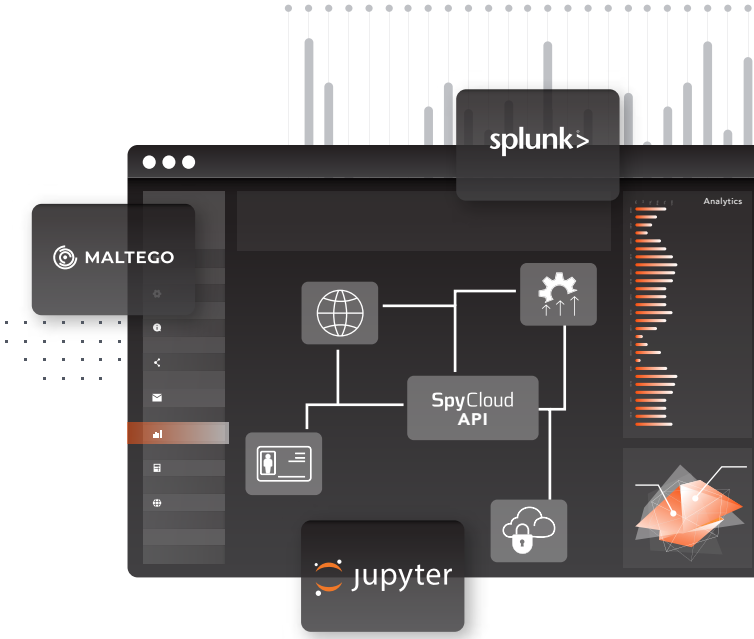
KEY CAPABILITIES

SpyCloud Investigations makes it faster and more efficient to take down those attempting to harm your organization. Draw on SpyCloud's rich dataset to help your team:

- **ATTRIBUTE CYBERCRIME** | Uncover the true identities of specific criminals and their personas
- **EVALUATE THREAT ACTORS** | Profile criminal targets, identifying where they have had accounts and where they are operating
- **UNDERSTAND ATTACKS** | Determine the origin of data used in credential stuffing attacks and identify the exposure of public applications to botnet credential stealers
- **INVESTIGATE CAMPAIGNS** | Research criminal campaigns and infrastructure, including the breadth and nature of malicious campaigns
- **ASSESS RISK** | Understand internal and external user risks, from reused credentials to malware infections
- **80+ MALTEGO TRANSFORMS** | In addition to querying the API in the SpyCloud portal, Investigations licenses come out-of-the-box with 80+ Maltego Transforms
- **ADVANCED JUPYTER NOTEBOOKS** | Pre-built, web-based Notebooks deliver query results in an easy-to-digest format that enables drill-downs, data exports, and flexible graphs

HOW IT WORKS

REST-based APIs enable analysts and investigators to combine breach data from SpyCloud with data from internal and other OSINT data sources via link analysis tools such as Maltego, Jupyter Notebook, and others. These interactive data mining tools render directed graphs for link analysis and are often used in investigations to find relationships between pieces of information collected from various sources located on the internet. With the SpyCloud API, investigators can pivot on data points like username, password, IP address, or email address and find a wealth of data.



THE INVESTIGATIONS API

- Feed SpyCloud data into third-party tools
- Write custom scripts to automate workflows
- Use data analysis and modeling tools to investigate large datasets of tens or hundreds of thousands of data elements at a time
- Combine SpyCloud-normalized OSINT with other valuable data from third parties in the same repository
- Perform macro-scale analysis on adversary community overlap
- Understand consumer impact of individual third-party breach sources or malware variants
- Perform large queries on high-volume result sets like domains
- Loop and batch queries for selectors based on high-value results

Looking for a SaaS-based solution for analysts of all skill levels? **Explore SpyCloud Investigations Portal >**

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 >**