Hudson Rock
Cybercrime Intelligence

Cybercrime Data Enrichment for Cybersecurity & Risk Assessment Use Cases

Among Our Customers: RAPID7 Malwarebytes bluevine Bridewell at bay Five9 Acronis HiBob eToro

Real-Time Actionable Data Sourced Directly from Threat Actors

30M+
Compromised Machines

10M+
Compromised Domains

4M+
Compromised Employees

Integrate Real-Time Compromised Credential Intelligence

In today's increasingly sophisticated cyber landscape, compromised credentials serve as the most popular entry point for many of the most devastating attacks, including ransomware and network infiltration.

At Hudson Rock, we provide companies — large and small — including cybersecurity & insurance firms, as well as MSSPs and governments, with real-time intelligence notifications on compromised credentials sourced directly from threat actors operating active global malware spreading campaigns.

This data allows product, security and IT teams to take proactive measures, preventing network breaches before they escalate into catastrophic events.

The Role of Credentials Compromised by Infostealers in Cyber Threats

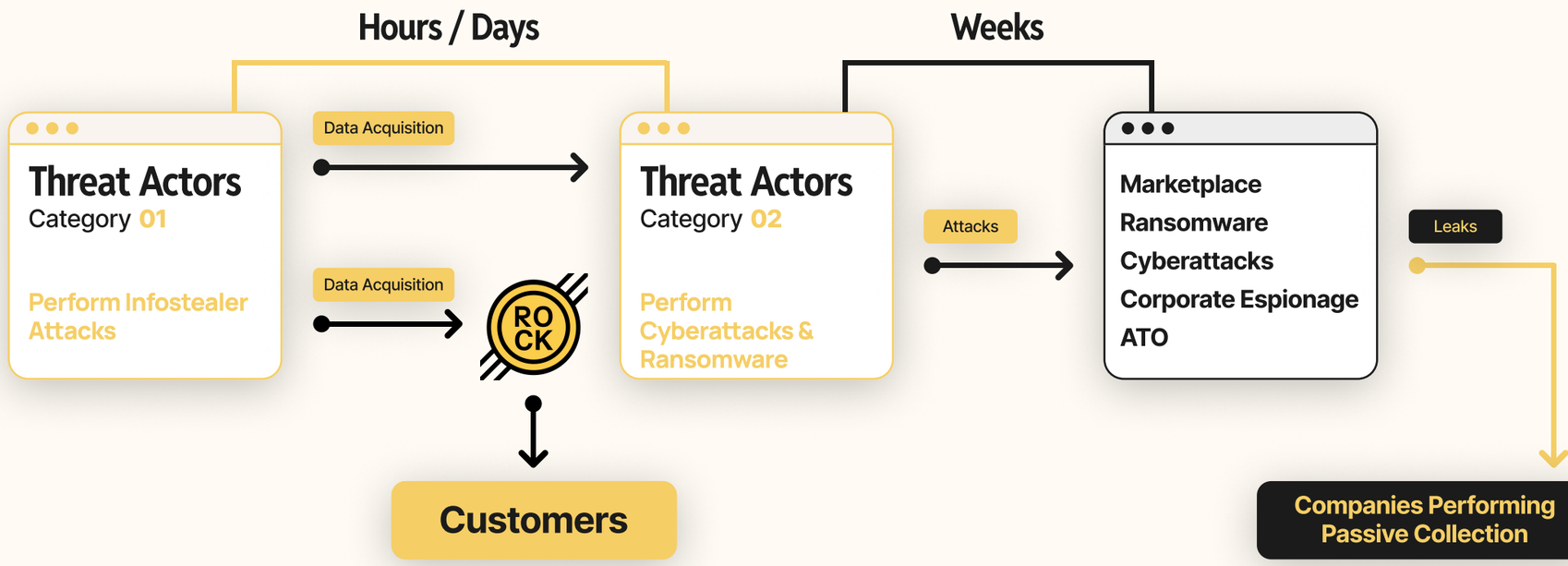
Designed to steal all critical information directly from victims' machines — corporate and personal computers — Infostealing malware became the most prominent attack vector for cybercriminals in recent years.

Threat Actors take advantage of compromised credentials and stolen cookies in order to bypass traditional security defenses such as 2FA, and gain initial access to sensitive network infrastructure. From there, they deploy ransomware, steal sensitive data, and perform fraud.

The compromised data from Infostealers is also used for conducting cyber attacks such as business email compromise (BEC), identity theft, cryptocurrency theft, hijacking application access tokens, social engineering and more.

Hudson Rock's unrivaled ability to provide real-time intelligence from Infostealer infections, as early as minutes after the infection, has helped prevent cyber attacks against some of the world's largest companies.

Based on Data Sourcing Techniques Pioneered at the 8200 Unit



Current Customers Integrate Hudson Rock's Compromised Credentials Data Enrichment For:

Early Detection of Threats: Leverage Hudson Rock's continuously collected and ingested compromised credentials data to alert customers before attackers use them to penetrate their network.

Proactive Defense Against Ransomware & ATO: Use Hudson Rock's cybercrime data feed to identify unauthorized access on customer infrastructure that often leads to ransomware attacks or financial fraud, paired with reputation damage.

Third-Party Credential Intelligence to Mitigate Supply Chain & Vendor Risks: Use Hudson Rock API to search for and identify compromised third-party credentials that frequently become supply-chain and attack surface exploitation for network and data infiltration.

AI-Powered Investigation Module: Delve deeper with Hudson Rock's Infostealer data for both advanced cybersecurity and general-purpose research, including accessing raw compromised data, threat actor deanonymization, illicit sources research, and extracting valuable intelligence for custom multi-sector investigation or academic publication.

Use Our Data to Protect Against

- Ransomware
- Data Breaches
- Corporate Espionage
- Account Takeover
- Session Hijacking
- Network Overtakes

Hudson Rock's cybercrime Data Enrichment provides actionable intelligence and alerts — based on data stolen via Infostealers — to Cyber Threat Intelligence and IT professionals, about compromised credentials belonging to Employees, Users, Customers & Vendors.

Data Delivery

- API
- JSON
- Data Lake

Supported Use Cases

- Cybersecurity Products & Services
- Third-Party Risk Assessment
- Supply Chain Vulnerabilities
- Post-Infection Analysis
- Cyber Insurance
- Threat Actor Attribution
- MSSP Solutions
- Penetration Testing

Compromised Data & Features Include

- Infected Machines
- Exposed Employee & Third-Party Credentials
- Vulnerable Users & Customers
- Exposed Cookies
- Mobile App Credentials
- AI-Driven Threat Analysis
- Web & API Access
- SOC & SOAR Integrations

Available Endpoints

1 End User Protection

- Search By Login
- Search By Login (Bulk)
- Search By IP
- Search By Stealer

2 Domain Intelligence

3 Assets Intelligence

4 Third Party Risk Assessment

5 External Attack Surface

API Schema | Request A Free API Key: hudsonrock.com/api

date_uploaded	ISO date string	The date in which the stealer was integrated into Hudson Rock's platform.
stealer	string	The unique ID of the stealer, typically indicating which stealer type it is, but often it is just random. Hudson Rock provides it as it was acquired from the threat actors.
ip	string	The IP of the infected computer at the time of the infection.
operating_system	string	Operating System of the compromised computer.
antiviruses	array/list	Anti-viruses installed on the victim's computer.
clientAT	array/list	An aggregation of all the companies (domains) that the retrieved computer is found to be a client at, based on the credentials from their computer.
employee_session_cookies	array/list	Cookies that were captured from the compromised computer, allowing threat actors to bypass traditional security measures such as 2FA by stealing the session of the victim.

date_compromised	ISO date string	The date in which the computer was infected.
stealer_family	string	Indicating which stealer type it is.
computer_name	string	The name of the compromised computer.
malware_path	string	The path in which the stealer malware was installed.
employeeAt	array/list	An aggregation of all the companies (domains) that the retrieved computer is found to be an employee at, based on the credentials from their computer.
credentials	array/list	Array of objects where each one contains the field type, url, domain, username and password.
installed_software	array/list	Array of installed software names and versions which were found on the compromised computer.

About Hudson Rock

At Hudson Rock, we specialize in delivering world-class cybercrime intelligence solutions that help businesses and security teams stay ahead of evolving threats. Powered by our ever-expanding cybercrime intelligence database of compromised machines, Hudson Rock provides actionable insights that empower organizations to protect their employees, customers, and infrastructure from cybercriminals. Whether you need protection against account takeovers, ransomware, or data breaches, Hudson Rock's intelligence platforms — Cavalier™ & Bayonet™ — offer the tools you need to secure your business.

hudsonrock.com