Infostealer Intelligence & Protection for Corporate Security

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

Real-Time Actionable Data Sourced Directly from Threat Actors

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 — with real-time intelligence notifications on compromised credentials sourced directly from threat actors operating active global malware spreading campaigns. This data allows security and IT teams to take proactive measures, preventing network breaches before they escalate into catastrophic events.

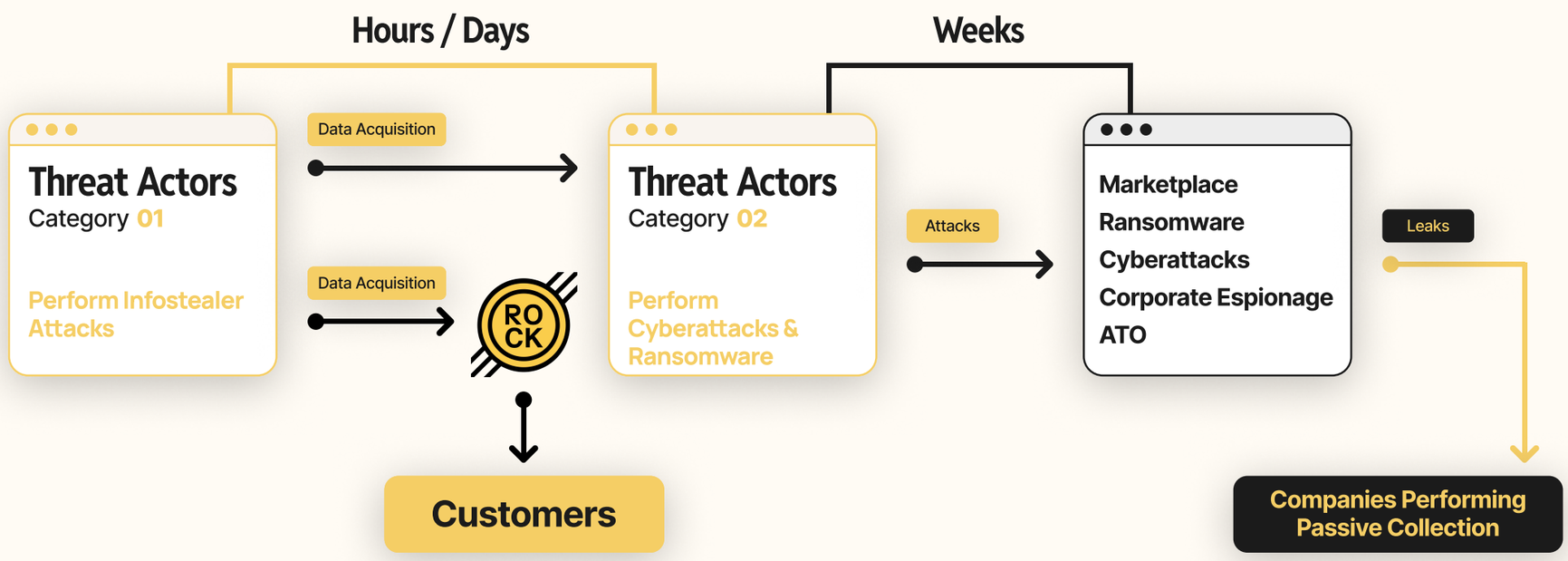
The Role of Credentials Compromised by Infostealers in Cyber Threats

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 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, or perform fraud.

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



Hudson Rock Provides Organizations

Early Detection of Threats: Our systems, powered by the industry's first Infostealer threat intelligence AI, continuously collect and ingest credentials data from active malware-spreading campaigns, alerting your security and IT teams before attackers use them to penetrate your network.

Proactive Defense Against Ransomware & ATO: By identifying and responding to Hudson Rock's intelligence, you will prevent unauthorized access that often leads to ransomware attacks.

Third-Party Credential Intelligence to Mitigate Supply Chain & Vendor Risks: In today's interconnected security landscape where third-party credentials frequently become weak links leading to significant breaches, Hudson Rock provides crucial protection for credentials used to access vendors and third-party providers, preventing their exploitation for network and data infiltration.

Protect Against

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

Sectors Served

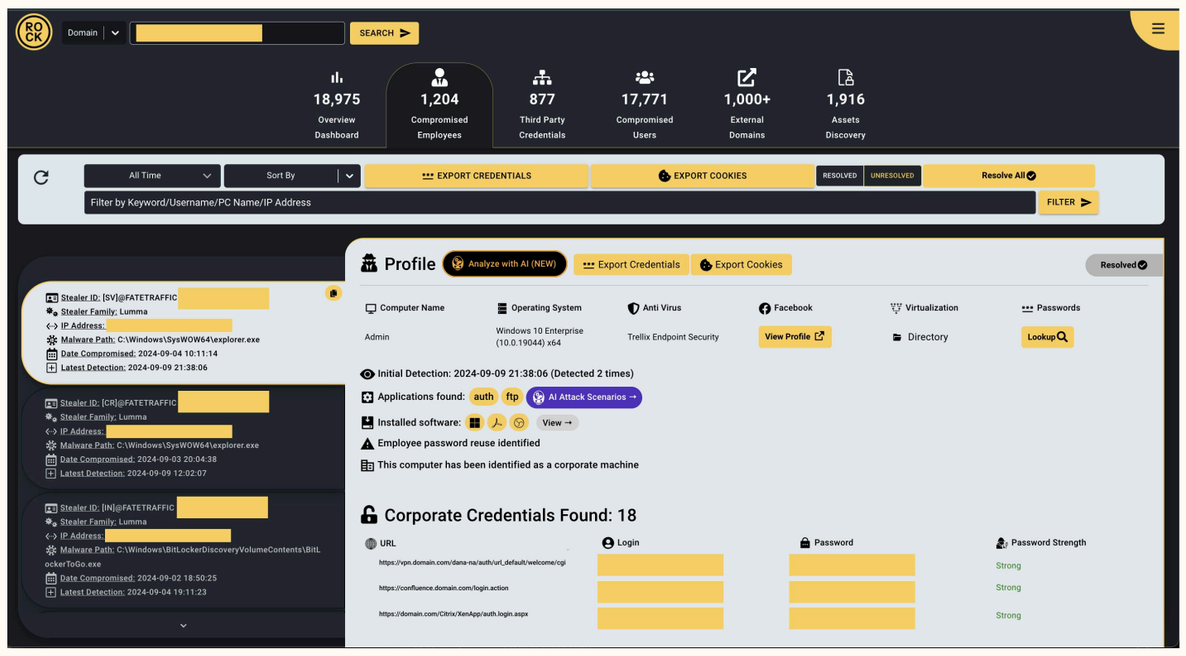
- Banking & Finance
- Cyber Insurance
- Crypto & FinTech
- Pharmaceutical
- Retail & eCommerce
- Healthcare
- Consumer Services
- Telecom
- Manufacturing
- Automotive
- Oil & Gas
- Legal
- Gaming & Leisure
- Aviation
- More...

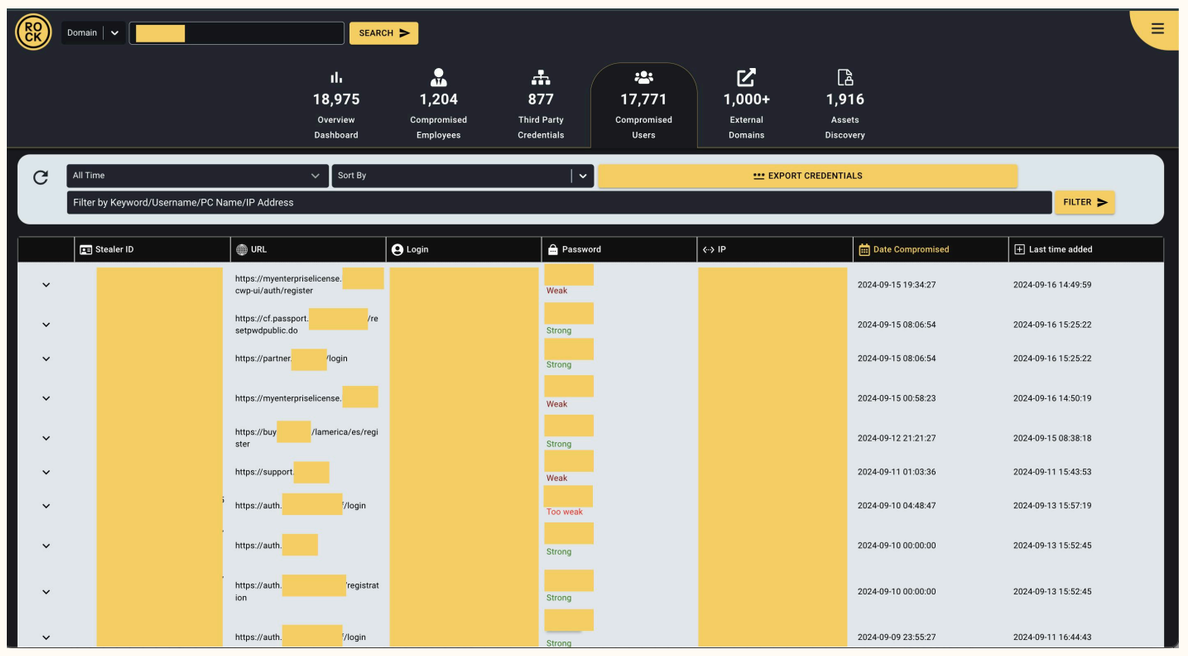
Cavalier™ is a cybercrime monitoring and notification platform which provides actionable intelligence and alerts — based on data stolen via Infostealers — to Cyber Threat Intelligence and IT professionals, about compromised credentials belonging to Employees, Users, Customers & Vendors.

Available Tiers

- Core
- Advanced
- Enterprise

> *CrowdStrike found that 62% of interactive cyber intrusions involved compromised identities, with a significant increase in attackers abusing legitimate credentials to bypass security measures and infiltrate sensitive systems.*
>
> *...research shows that identity-based attacks are becoming more prevalent, with adversaries leveraging credentials stolen via information stealers to bypass legacy security systems, making ransomware and data exfiltration more efficient."*





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**

Advanced Integration for Faster Response

Hudson Rock's compromised credential intelligence integrates directly with existing security infrastructure, enabling a faster, more efficient response to threats. Our data feeds integrate seamlessly into your SOC or threat intelligence platforms, helping your team prioritize responses based on the severity of the threat.

Data Delivery

- Web Interface
- API
- Email Notifications
- Integrations

Analysis Insights

- Post-Infection
- Penetration Testing
- Platform Integrity
- Threat Actor Attribution

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