SOCRadar®
Your Eyes Beyond

SOLUTION SHEET

Stealer Log Coverage & Defense

Monitor, investigate and analyze exposed data harvested by stealer malware and take action to prevent intrusion attacks.

The Growing Threat of Stealer Logs

As organizations navigate increasingly complex and dispersed IT environments, safeguarding user data and access credentials is more critical than ever. The rise of remote work, cloud services, and hybrid infrastructures has amplified the risks associated with stealer logs—i.e., collections of illegally obtained financial details, login credentials, browser cookies, personal data, etc.—harvested by stealer malware (also known as infostealers) covertly installed on infected user and corporate devices.

Stealer logs typically contain everything that opportunistic threat actors need to easily login, authenticate, and gain access to sensitive accounts, databases, systems, and digital corporate environments to conduct malicious activity. They can also contain stolen login cookies to bypass Multi-Factor Authentication (MFA).

Due to their convenience and ease-of-use, stealer logs are a hot commodity in the criminal economy, with thousands of transactions occurring daily across obfuscated dark web forums and marketplaces.

Risk Impact Of Stealer Logs

Organizational Risk:

- Ransomware
- Data Breaches/Leaks
- Compromising Third-Parties & Partners
- Business Email Compromise (BEC)
- Theft/Leaks of Intellectual Property (IP) & Trade Secrets
- Failing Security Compliance Audits/Requirements

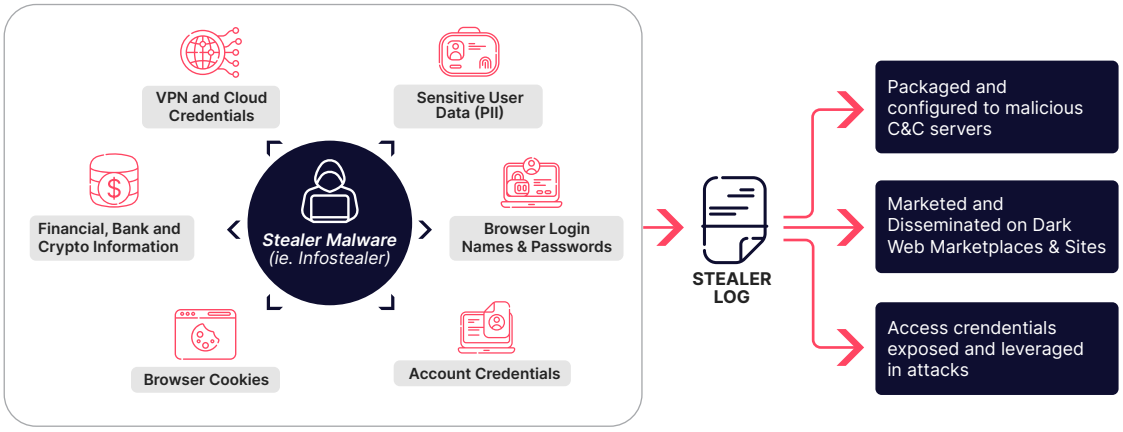
Individual Risk:

- Impersonation & Phishing Attacks
- Account & Email Takeovers
- Identity Theft
- Theft of Finances & Unauthorized Access into Financial Accounts
- Physical Threats & Doxxing

Notable Breaches Involving Stealer Logs:

The Snowflake breach (2024) was caused by stolen credentials and targeted customer accounts; impacting high-profile organizations such as Ticketmaster and Neiman Marcus.

The Okta breach (2024) was caused by exposed session tokens, which had been obtained in a past breach, allowing attackers to impersonate employees and infiltrate customer systems.



77%

Of all web application breaches involve stolen credentials*

$4.81M

Estimated average organizational cost of a data breach**

*https://www.verizon.com/business/en-au/resources/reports/2024/dbir/2024-dbir-data-breach-investigations-report.pdf
**https://table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf

SOCRadar Identifies Stealer Log Threats to Prevent Risk of Compromise

SOCRadar helps organizations find where they're compromised in stealer logs and proactively defends against the threats they present to their business and people. By actively monitoring thousands of hidden dark web sources and crawling for sensitive data shared by threat actors, SOCRadar automatically identifies and alerts on exposed credentials available for sale and distribution in stealer logs across illicit marketplaces and hacker communities. Additionally, SOCRadar goes beyond simply monitoring threat activity by delivering actionable insights gleaned from curated threat intelligence and stealer log analysis, helping security teams better investigate incidents and quickly remediate risk at its root level.

Get early warning of relevant compromised credentials and exposures in stealer logs so you can take immediate action to prevent risk.

Gain visibility into the criminal underground economy actively trading and monetizing stealer logs across dark web channels.

Easily search and access curated threat intelligence to find where stealer logs are exposing your employees, customers and business assets.

Gain insight from thorough stealer log analysis and stay informed of global identity and access threat trends to comprehensively assess risk.

Key Capabilities:

Dark Web Monitoring - Continuously scan over 6,000 (and growing) dark web forums, chats and marketplace sources to determine where organization-related credentials, VIP account login info, or sensitive data are being actively sold or distributed in a stealer log.

Stealer Log Alarms - Set up real-time and automated alerts with configurable rules, in-alert context with recommended actions, and employee domain tagging to inform and correlate intelligence about when and where stealer log exposures occur.

Threat Hunting - Empower security teams to search, filter, and investigate credentials across SOCRadar's massive pool of over 5 billion stealer logs from malware infected devices. This data is also available to integrate into your security stack via API integration.

Exposure Timeline Visualization - Get a clear picture of infostealer activity over the past month, helping you swiftly understand the distribution of potential compromises among your customers and employees.

Actionable Threat Intelligence - Correlate data from SOCRadar's Identity & Access module and stealer log analysis to pinpoint where infected devices and malware may reside in your organization to resolve embedded threats. Additionally, investigate malware variants using YARA and Sigma rules, as well as threat actor trends, tactics, and profiles, to stay up-to-date on the latest risks involving stealer logs.

"I've found [SOCRadar] to be indispensable in protecting our digital assets. The comprehensive Cyber Threat Intelligence it provides allows us to stay aware of emerging threats, giving us a proactive edge in our defense strategies."

Cyber Security Consultant | Gartner Peer Insights

How Stealer Logs Are Used For Attack

Threat actor obtains infostealer malware

Threat actor executes attack (ex. Phishing campaign)

Infostealer malware is secretly distributed to victim

Victim's credentials are exfiltrated and sent to criminal server

Stealer logs from victim are marketed, sold and distributed on the dark web

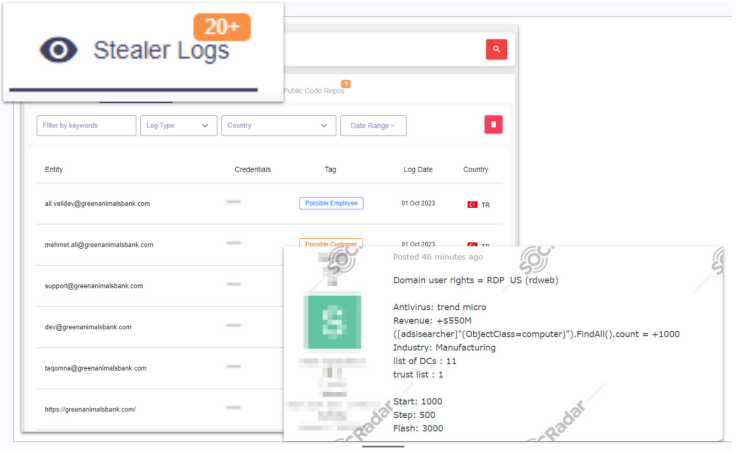
Initial Access Brokers (IABs) purchase stealer logs and pivot to selling direct access

Access is sold to criminal hackers who login to protected systems/environments

Compromise Incident (ex. Ransomware, Intrusion, etc.)

How Socradar Works To Defend Organizations From Stealer Logs

1. **MONITOR** thousands of dark web marketplaces and Telegram channels where hackers and Initial Access Brokers (IABs) engage in stealer log buying, selling and distribution.
2. **DETECT** in real-time instances of compromised credentials and exposures in stealer logs that mention your protected accounts, emails, passwords, etc.
3. **ENGAGE** threat actors via an experienced and embedded dark web task force that can conduct negotiations and transactions to acquire stealer logs on your behalf to eliminate further risk.
4. **INVESTIGATE** credential data from stealer logs with enriched intelligence across a massive, searchable database.
5. **TAKE PREVENTATIVE ACTION** by leveraging curated stealer log threat insights to inform security operations, address vulnerabilities, and engage threat actors before attacks occur.



See Where Your Data is Exposed in Stealer Logs!

Sign up for SOCRadar's Free Dark Web Report and get instant visibility into where your corporate, employee, and personal accounts are mentioned in stealer logs from compromised machines and third-party sites. Act now to identify exposed data across dark web channels and marketplaces—before it's too late.

Dark Web Report