



SOCRadar's mission is to inspire and enable the security community to identify threats before they turn into disruptive data breaches

# ADVANCED DARK WEB REPORT

yourdomain.com

Time Period: 2025/01/20 - 2026/01/20 | Report Date: 2026-01-20

Gartner  
Peer Insights™



SOCRadar HQ  
254 Chapman Rd, Ste 208 Newark  
Delaware 19702 USA

+1 (571) 249-4598  
info@socradar.io  
www.socradar.io



The following Dark Web Report presents security findings in the dark web detected by SOCRadar.

The report uncovers where/how your organization is exposed to deep and dark web threats. To find out the compromised credentials of your employees and possible sensitive data exposures, massive data collected from thousands of underground hacker forums, black markets, onion sites, Telegram channels, and Russian and English dark web marketplaces have been analyzed.

We highly recommend you request and run a free 14-day demo to see SOCRadar in action. The platform's alerts will be supported by certified Threat Intelligence analysts and the remediation actions will be provided instantly.

## SUMMARY



Threat Severity: **HIGH**



**Today**

Latest exposure finding



**7500**

Employee - Stealer Log  
at Third Party Websites



**7500**

Stealer Logs from  
Infected Machine



**1000+**

Stealer Logs for  
Sale in Blackmarket



**25**

Employee  
Credential Leak

In **758** Leak Sources



**16**

Dark Web & Hacker  
Channel Mentions

**8** Different Sources

# Stealer Logs from Infected Machine

For attackers, infecting computers or phones with malware is as easy as playing a game. Every day, in the emails we open, in the sites we visit, and in the links, we click, there could be malware that can infect our computers. We could give our credentials (username and password) and our documents into the hands of threat actors by clicking one link. SOCRadar collects stealer logs shared on the dark web.

**7500**  
Total Stealer Log

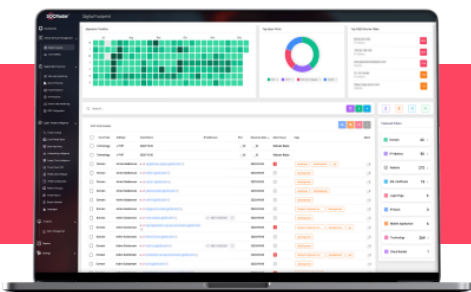
**10**  
Shown Stealer Log

## Stealer Logs from Infected Machine

Affected Assets	User	Password	Infection Date	Machine IP
yourdomain.com	d****@yourdomain.com	****M*****	2026-01-07	85.111.222.111
yourdomain.com	a****@yourdomain.com	****v*****	2025-12-25	85.111.222.111
yourdomain.com	a****@yourdomain.com	****s*****	2025-12-20	85.111.222.111
yourdomain.com	z****@yourdomain.com	****z*****	2025-07-14	85.111.222.111
yourdomain.com	j****@yourdomain.com	****d*****	2025-11-10	85.111.222.111
yourdomain.com	c****@yourdomain.com	****K*****	2025-09-08	85.111.222.111
yourdomain.com	j****@yourdomain.com	****H*****	2025-08-09	85.111.222.111
yourdomain.com	j****@yourdomain.com	****A*****	2025-05-01	85.111.222.111
yourdomain.com	b****@yourdomain.com	****P*****	2025-10-11	85.111.222.111
yourdomain.com	z****@yourdomain.com	****z*****	2025-06-19	85.111.222.111
yourdomain.com	z****@yourdomain.com	****z*****	2025-06-19	85.111.222.111
yourdomain.com	z****@yourdomain.com	****z*****	2025-06-19	85.111.222.111

+7490 Stealer Log

[View More](#)



Dare to look "what's more" on the Dark Web?  
Try ADWM's free trial now.

[I want to see more](#)

# Employee - Stealer Log at Third Party Websites

For attackers, infecting computers or phones with malware is as easy as playing a game. Every day, in the emails we open, in the sites we visit, and in the links, we click, there could be malware that can infect our computers. We could give our credentials (username and password) and our documents into the hands of threat actors by clicking one link. SOCRadar collects stealer logs shared on the dark web.

**7500**  
Total Employee

**10**  
Shown Stealer Log

## Company Employee - Stealer Log at Third Party Websites

Affected Assets	User	Password	Infection Date	Machine IP
yourdomain.com	d****@yourdomain.com	****M*****	2026-01-07	85.111.222.111
yourdomain.com	a****@yourdomain.com	****9*****	2026-01-06	85.111.222.111
yourdomain.com	g****@yourdomain.com	****S*****	2025-12-24	85.111.222.111
yourdomain.com	s****@yourdomain.com	****a*****	2025-12-24	85.111.222.111
yourdomain.com	t****@yourdomain.com	****1*****	2025-12-21	85.111.222.111
yourdomain.com	s****@yourdomain.com	****A*****	2025-12-12	85.111.222.111
yourdomain.com	j****@yourdomain.com	****A*****	2025-12-04	85.111.222.111
yourdomain.com	t****@yourdomain.com	****1*****	2025-11-23	85.111.222.111
yourdomain.com	j****@yourdomain.com	**** *****	2025-11-10	85.111.222.111
yourdomain.com	t****@yourdomain.com	****T*****	2025-10-01	85.111.222.111
yourdomain.com	*****@yourdomain.com	*****	*****	*****
yourdomain.com	*****@yourdomain.com	*****	*****	*****

+7490 Employee - Stealer Log at Third Party Websites

[View More](#)



Illuminate dark web threats with SOCRadar's Dark Web insights.

[See Free Trial in Action](#)

# Stealer Logs for Sale On Blackmarket

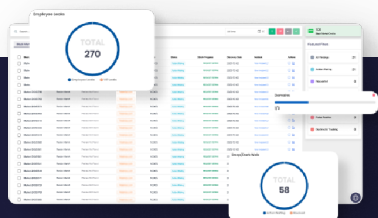
Stealer logs from malware-infected machines are very valuable. It provides actionable intelligence such as infected devices, affected users, and stolen data in the machine. This data is sold in Blackmarkets for only \$10 and falls into the hands of other threat actors. SOCRadar actively scans black markets and detects data for sale.

**1000+**  
Total Data for Sale

**7**  
Shown Data for Sale

## Stealer Logs for Sale

Affected Assets	Source	Price (\$)	Infection Date	Stealer
yourdomain.com <span>⚠</span>	RUSSIAN MARKET	10.00	2025-08-13	Sale
yourdomain.com	RUSSIAN MARKET	10.00	2026-01-12	Sale
yourdomain.com	RUSSIAN MARKET	10.00	2026-01-12	Sale
yourdomain.com	RUSSIAN MARKET	10.00	2026-01-05	Sale
yourdomain.com	RUSSIAN MARKET	10.00	2026-01-08	Sale
yourdomain.com	RUSSIAN MARKET	10.00	2026-01-06	Sale
yourdomain.com	RUSSIAN MARKET	10.00	2025-08-06	Sale



Don't let your data become a bargain. Stay ahead with SOCRadar.

See Free Trial in Action

Your company's internal data is one of its most valuable assets. To access that data threat actors and cybercriminals are continuously looking for credentials stolen from your employees including C-level people. SOCRadar detected breached credentials of 25 of your company employees in the last one year.

**25**  
Total Leak

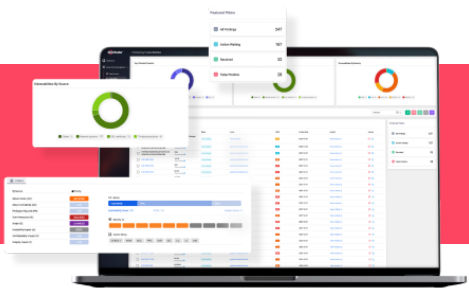
**15**  
Shown Leak

## Employee Credential Leaks

Breach Date	Credentials Data	Source
2026-01-05	j****@yourdomain.com	Combolist
2026-01-05	d****@yourdomain.com	Combolist
2026-01-04	g****@yourdomain.com	Combolist
2026-01-04	t****@yourdomain.com	Combolist
2026-01-04	d****@yourdomain.com	Combolist
2026-01-02	g****@yourdomain.com	Combolist
2026-01-02	m****@yourdomain.com	Combolist
2025-12-31	j****@yourdomain.com	Combolist
2025-12-31	j****@yourdomain.com	Combolist
2025-12-16	z****@yourdomain.com	Combolist
2025-12-12	c****@yourdomain.com	Combolist
2025-12-12	a****@yourdomain.com	Combolist
2025-12-12	d****@yourdomain.com	Combolist
2025-12-12	l****@yourdomain.com	Combolist
2025-12-12	j****@yourdomain.com	Combolist
2025-12-12	j****@yourdomain.com	Combolist
2025-12-12	j****@yourdomain.com	Combolist

+10 Leaks

[View More](#)



Know immediately if an employee account is being leaked

[See Free Trial in Action](#)



# ADVANCED DARK WEB MONITORING

Delivered from the best, the Dark Web Monitoring you need

Advanced Dark Web Monitoring makes you aware of your Dark Web Threats Minimizing room for catastrophic incidents.

## Dark Web Monitoring

Learn immediately if your sensitive information ends up on the dark web.

## Retrieve Sensitive Data from Black Market

Get your information out of Dark Web before it falls into wrong hands.

## Dark Web Search Engine

Search your threats through the dark web from your browser!

## Threat Actor Engagement

Learn what threat actors / ransomware groups up to?

## Dark Web Activity Monitoring

Learn what threat actors / ransomware groups up to?

## Stealer Logs

Detect your compromised accounts / machines before they turn into a breach!



Curious About What You Found Here? **Join 2-Weeks Free Trial** to learn more!

Trusted by 30,000 businesses and governmental organizations across 150+ Country

[I want to see what's more](#)

Gartner  
Peer Insights™



SOCradar HQ  
254 Chapman Rd, Ste 208 Newark  
Delaware 19702 USA

+1 (571) 249-4598  
info@socradar.io  
www.socradar.io

**SOCradar**®  
Your Eyes Beyond