SOCRadar® FREE TOOLS

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

DARK WEB REPORT

example.com

Time Period: 2023/01/04 - 2024/01/04 | **Report Date:** 2024-01-04

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

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

SOCRadar Dark Web Test Results

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.

HIGH
Threat Severity

Today
Latest exposure finding

500+
Stealer Logs from Infected Machine

1344
Stealer Logs for Sale in Blackmarket

320
Employee Credential Leak
In **2834** Leak Sources

326
Dark Web& Hacker Channel Mentions
8 Different Sources

Stealer Logs from Infected Machine

SOCRadar FREE TOOLS

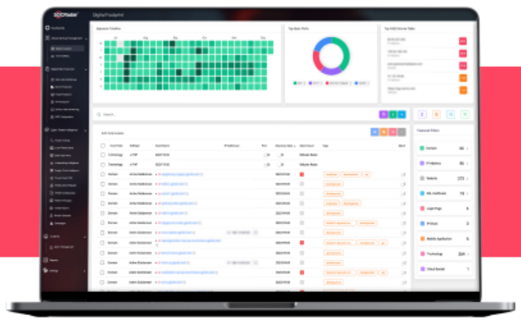
For attackers, infecting computers or phones with malware is as easy as playing a game. Every day, in the emails we open, in the sites we visit, and in the links, we click, there could be malware that can infect our computers. We could give our credentials (username and password) and our documents into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

500
Total Stealer Log

12
Shown Stealer Log

Stealer Logs from Infected Machine

URL	User	Password	Tag	Infection Date	Country	Machine IP
https://example.com/W	14015716566	147****	Possible Employee	2023-08-21	TR	85.100.192.190
https://example.com/W	;jsessionid=0000eKsIU 35cjWoFhVM3ela	147****	Possible Employee	2023-08-21	TR	85.100.192.190
https://example.com/W	14015716566	147****	Possible Employee	2023-08-21	TR	85.100.192.190
https://example.com/W	;jsessionid=0000eKsIU 35cjWoFhVM3ela	147****	Possible Employee	2023-08-21	TR	85.100.192.190
https://example.com/W	14015716566	147****	Possible Employee	2023-08-21	TR	85.100.192.190
https://example.com/W	;jsessionid=0000eKsIU 35cjWoFhVM3ela	147****	Possible Employee	2023-08-21	TR	85.100.192.190
https://example.com/W	14015716566	147****	Possible Employee	2023-08-21	TR	85.100.192.190
https://example.com/W	;jsessionid=0000eKsIU 35cjWoFhVM3ela	147****	Possible Employee	2023-08-21	TR	85.100.192.190
https://example.com/W	;jsessionid=0000eKsIU 35cjWoFhVM3ela	147****	Possible Employee	2023-08-21	TR	85.100.192.190
https://example.com/W	;jsessionid=0000eKsIU 35cjWoFhVM3ela	147****	Possible Employee	2023-08-21	TR	85.100.192.190
https://example.com/W	14015716566	147****	Possible Employee	2023-08-21	TR	85.100.192.190
https://example.com/W	;jsessionid=0000eKsIU 35cjWoFhVM3ela	147****	Possible Employee	2023-08-21	TR	85.100.192.190



One click, endless consequences.
Let SOCRadar secure your digital world.

Start for Free

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.

4692
Total Data for Sale

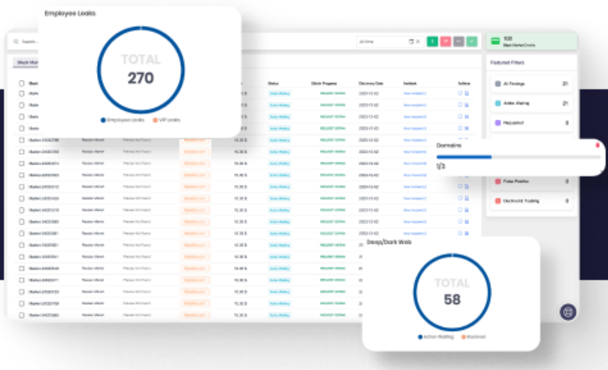
9
Shown Data for Sale

Stealer Logs for Sale

Affected Assets	Tag	Country	Source	Price	Malware Infection Date	Stealer
3dsecure.example.com.tr example.com.tr	Possible Employee	TR	RUSSIAN_MARKET_BOT	10.00 $	2023-08-19 00:00:00	Redline
internetsubesi.example.com example.com	Possible Employee	TR	RUSSIAN_MARKET_BOT	10.00 $	2023-08-19 00:00:00	Redline
internetsubesi.example.com 3dsecure.example.com.tr	Possible Employee	TR	RUSSIAN_MARKET_BOT	10.00 $	2023-08-19 00:00:00	Redline
3dsecure.example.com.tr example.com.tr	Possible Employee	TR	RUSSIAN_MARKET_BOT	10.00 $	2023-08-19 00:00:00	Redline
internetsubesi.example.com example.com	Possible Employee	TR	RUSSIAN_MARKET_BOT	10.00 $	2023-08-19 00:00:00	Redline
internetsubesi.example.com 3dsecure.example.com.tr	Possible Employee	TR	RUSSIAN_MARKET_BOT	10.00 $	2023-08-19 00:00:00	Redline
3dsecure.example.com.tr example.com.tr	Possible Employee	TR	RUSSIAN_MARKET_BOT	10.00 $	2023-08-19 00:00:00	Redline
internetsubesi.example.com example.com	Possible Employee	TR	RUSSIAN_MARKET_BOT	10.00 $	2023-08-19 00:00:00	Redline
internetsubesi.example.com 3dsecure.example.com.tr	Possible Employee	TR	RUSSIAN_MARKET_BOT	10.00 $	2023-08-19 00:00:00	Redline
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

+4367 Data for Sale

View More



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

Protect Your Data Now for Free

Employee Credential Leak

SOCRadar FREE TOOLS

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 5572 of your company employees in the last one year.

5572
Total Leak

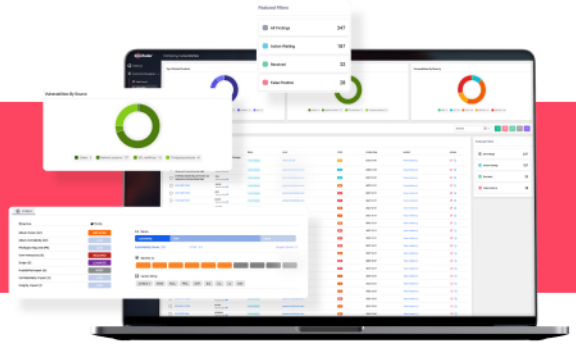
9
Shown Leak

Employee Credential Leak

Breach Date	Credentials Data	Source
2023-08-04	j****a@example.com | v****h	combolist_credential_stung
2023-08-04	d****h@example.com | s****h	combolist_credential_stung
2023-08-04	l****n@example.com | s****g	combolist_credential_stung
2023-08-04	a****r@example.com | d****f	combolist_credential_stung
2023-08-04	f****h@example.com | s****h	combolist_credential_stung
2023-08-04	m****n@example.com | j****g	combolist_credential_stung
2023-08-04	g****d@example.com |g****g	combolist_credential_stung
2023-08-04	b****h@example.com |c****h	combolist_credential_stung
2023-08-04	y***n@example.com | e****g	combolist_credential_stung
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

+5572 Leaks

View More



Empower your team with secure credentials.

Start for Free

Dark Web Mentions

SOCRadar FREE TOOLS

Threat actors do not hesitate to constantly share details about the companies they target and their cyber attacks. There are many meeting points for actors in dark web forums. SOCRadar constantly monitors these sources and receives information from the dark space.

1259
Total Mention

9
Shown Mention

Dark Web Mentions

Date	.	Content	Source
2023-08-04		Example.com:Diego_Men chachogamer1@hotmail.com:123456789 Nathan...	HACKER FORUM
2023-08-04		l supersaiyan_allen21@yahoo.com.ph:Xburner2110 nexxuzhd2016@gm...	HACKER FORUM
2023-08-04		example.com:Soychido slaymathers@example.com...	HACKER FORUM
2023-08-04		dandermanis@yahoo.com:Login <password> danielcrisp...	HACKER FORUM
2023-08-04		example.com:GurooruG chks24680@example.com...	HACKER FORUM
2023-08-04		example.com exampleExmple abc@example.com...	HACKER FORUM
2023-08-04		example.com:GurooruG chelseycrooasd@example.com...	HACKER FORUM
2023-08-04		loremipsum@example.com Lorem Ipsum...	HACKER FORUM
2023-08-04		yes@example.com : Example E....	HACKER FORUM
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]

+1250 Mentions

View More

Illuminate dark web threats with SOCRadar's insights.

Start for Free

Hacker Channel Mentions

SOCRadar FREE TOOLS

As messaging applications continue to evolve, threat actors nd it increasingly convenient to coordinate their activities through channels on these platforms. This ease of organization has amplied the signicance of closely monitoring these messaging applications. Notably, the proliferation of new channels is a constant challenge, with numerous channels being established daily. To address this, SOCRadar plays a pivotal role by actively incorporating these new channels into its resource repository, ensuring that organizations are well- equipped to stay vigilant and responsive to emerging threats.

3586
Total Mention

9
Shown Mention

Hacker Channel Mentions

Date	.	Content	Source
2023-08-04		| User : Duong Ngoc Phong | ID : 2128612759 | Command ...	TELEGRAM
2023-08-04		| User : MOON | ID : 5978972451 | Command : | FREE:.....	TELEGRAM
2023-08-04		| User : ZEUS | ID : 6222774746 | Command : | FREE: • Usage: /free me...	TELEGRAM
2023-08-04		| User : | ID : 6339384123 | Command : | FREE: • Usage: /free meth...	TELEGRAM
2023-08-04		| User : AMAN | ID : 6851536205 | Command : | FREE: • Usage: /free meth...	TELEGRAM
2023-08-04		| Attack Sent Successfully ... • User: Văn Đức • Host:..	TELEGRAM
2023-08-04		| User : CAT | ID : 62258547438 | Command : | FREE: • Usage: /free me...	TELEGRAM
2023-08-04		| Attack Sent Successfully ... • User: EXAMPLE • Host:..	TELEGRAM
2023-08-04		| User : EXAMPLE | ID : 62258 | Command : | FREE: • Usage: /free me...	TELEGRAM
[redacted]		[redacted]	[redacted]
[redacted]		[redacted]	[redacted]

+3577 Mentions

View More

Stay informed, stay protected.
Count on SOCRadar for real-time insights.

Start for Free

EXTENDED THREAT INTELLIGENCE (XTI)

Threat Intelligence enriched with External Attack Surface Management and Digital Risk Protection. Maximize the efficiency of your SOC team with false-positive free, actionable, and contextualized threat intelligence.

Sign Up For Free Edition

Trusted by more than 20.000 companies in more than 150 countries

Sign Up for Free

Gartner Peer Insights 4.8/5

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

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

SOCRadar® Your Eyes Beyond