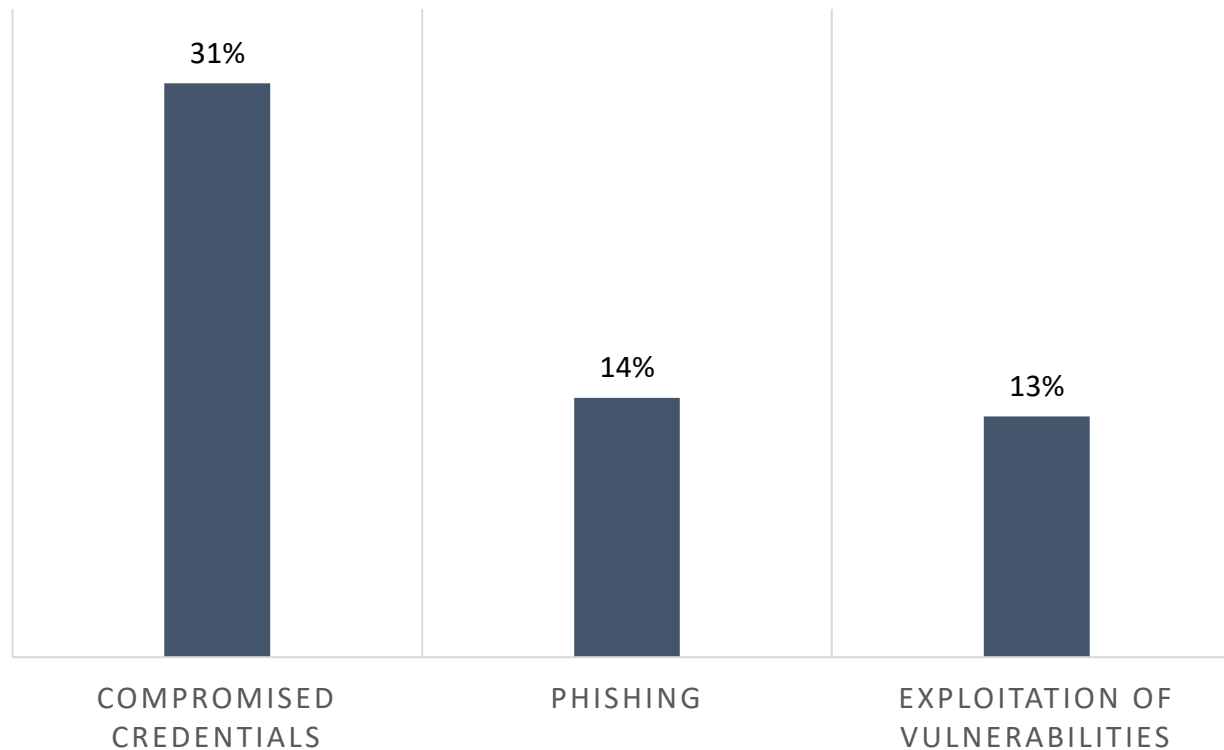# Prevent Cyber Attacks Before They Happen

ParanoidLab

Monitor your business on the Dark Web

ParanoidLab

Over **31%** of cyber-attacks involve using compromised credentials as an attack vector [1]

31%

14%

13%

COMPROMISED CREDENTIALS

PHISHING

EXPLOITATION OF VULNERABILITIES

1 – Verizon 2024 Data Breach Investigations Report

Vectors of attack

May 24, 2024

Hi! I will buy you accesses (Citrix, VPN and RDP) revenue from 10kk geo **US, CA, UK and EU.**

Привет! Я куплю ваши доступы (Citrix, VPN и RDP) доход от 10kk geo **США, Канады, Великобритании и ЕС.**

Contact/Контакт:
Tox: 54441████████████████████████████████████CB94A

n3on
Member
Nov 5, 2023
Messages   72
Reaction score   67
Points   18

A threat actor affiliated to Ransomware Hub ransomware group is buying
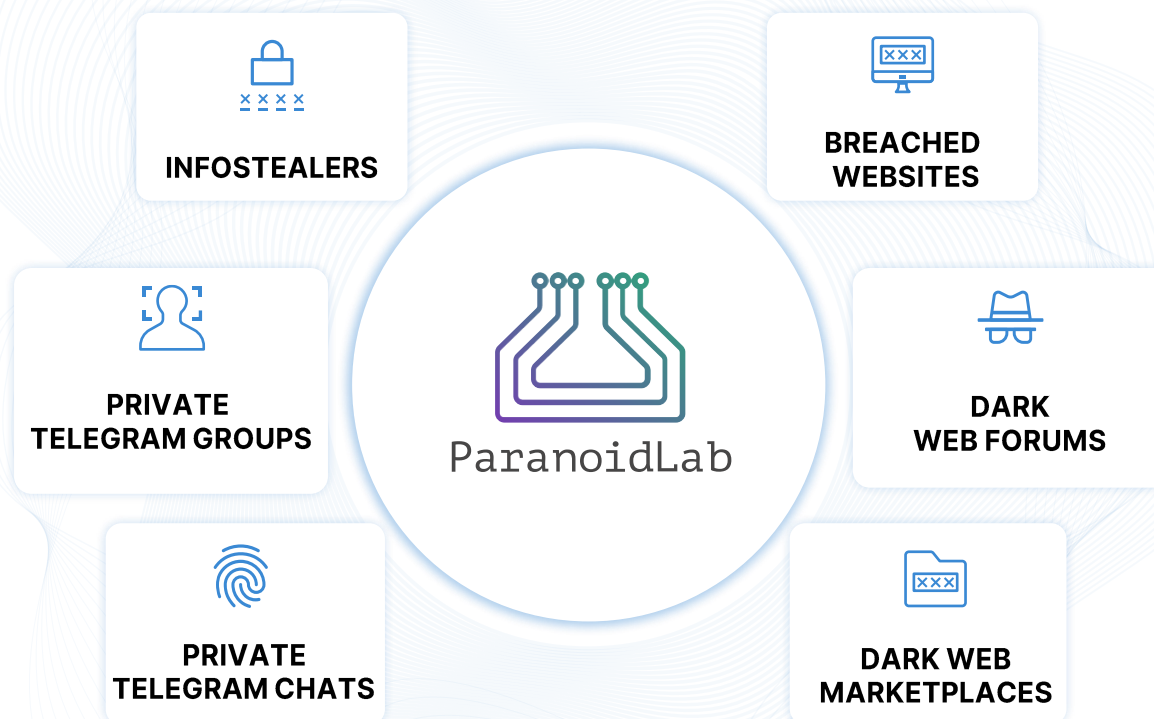
Compromised Credentials

Vectors of attack

qupi
байт
●

Q

Опубликовано: 17 августа 2021

куплю доступа, цена 10-50$
/vpn/index.html
/vpn/tmindex.html
/auth/login.aspx
/LogonPoint/tmindex.html
XenApp1/auth/login.aspx
auth/silentDetection.aspx
/citrix/
/+CSCOE+/
RDWeb
/dana/
/dana-na/
/global-protect/
/nf/auth/doAuthentication.do

Платная регистрация
● 0
7 публикаций
Регистрация
08/12/21 (ID: 119003)
Деятельность
вирусология / malware

A threat actor is buying Compromised Credentials to various companies by looking for specific keywords in URLs

Services offered by ParanoidLab

ParanoidLab

INFOSTEALERS

BREACHED WEBSITES

PRIVATE TELEGRAM GROUPS

ParanoidLab

DARK WEB FORUMS

PRIVATE TELEGRAM CHATS

DARK WEB MARKETPLACES

ParanoidLab empowers MSSPs, SOCs, and IT Security providers by continuously monitoring every hidden corner of the Dark Web - from Telegram channels and underground forums to Initial Access Brokers' databases, Infostealers, and marketplaces. It **detects Compromised Credentials** of employees, partners, and users, and mentions of **specific keywords in real-time**, and notifies you to **prevent ransomware and cyber-attacks**.

.

Services offered by ParanoidLab

Compromised Credentials Monitoring

☑ Infostealers

☑ Combo-lists

☑ Dark Web Marketplaces

Dark Web Monitoring

☐ Dark Web Forums

☑ Hacking Related Telegram Groups and Channels

Daily Updates

70M

50M

24 25 26 27 28 29 30

Monthly Updates

7B
6B
5B
4B
3B
2B
1B
0

50 million
records daily update

5 minutes
alert time

The value of **ParanoidLab**

Our achievement in the journey depicted in numbers

Up to 30x
Improvement In Threat Detection Time

According to the IBM Cost of a Data Breach Report 2024, detecting a breach takes 292 days on average.

ParanoidLab reduces this time to just 7 days, enabling organizations to quickly detect and respond to threats, significantly minimizing potential damage and associated costs.

Up to 3x
Reduced Likelihood Of A Company To Be Attacked

The likelihood of a company being attacked annually is 20% - 60%, depending on the industry and revenue.

ParanoidLab reduces this risk to 6% - 39% accordingly.

Up to 70%
Reduction In Ransomware Incidents

According to research by Zscaler, IBM, and Verizon, companies that implement Compromised Credentials Monitoring and Dark Web Monitoring experience **up to a 70% reduction in ransomware incidents** due to early detection of potential breaches and points of entry.

ParanoidLab Stops Cyber Attacks at the First Stage of the Cyber Kill Chain

ParanoidLab

1 RECONNAISSANCE $

2 WEAPONIZATION $$

3 DELIVERY

4 EXPLOITATION $$$

5 INSTALLATION

6 COMMAND & CONTROL (C2)

7 ACTIONS ON OBJECTIVES $$$$

*The Cyber Kill Chain outlines seven critical stages of a cyber attack, each representing an opportunity to stop attackers in their tracks. **ParanoidLab intervenes at the very first stage** - reconnaissance, where cybercriminals gather information about their targets.*

*By continuously monitoring the Dark Web for Compromised Credentials and mentions of specific keywords related to your clients, **ParanoidLab identifies** potential **threats before they materialize**. This early detection allows **MSSPs, SOCs, and IT Security providers** to **disrupt attacks at their inception**, when **intervention is most effective**, and **costs are lowest**.*

ParanoidLab hits the Top of the Pyramid of Pain
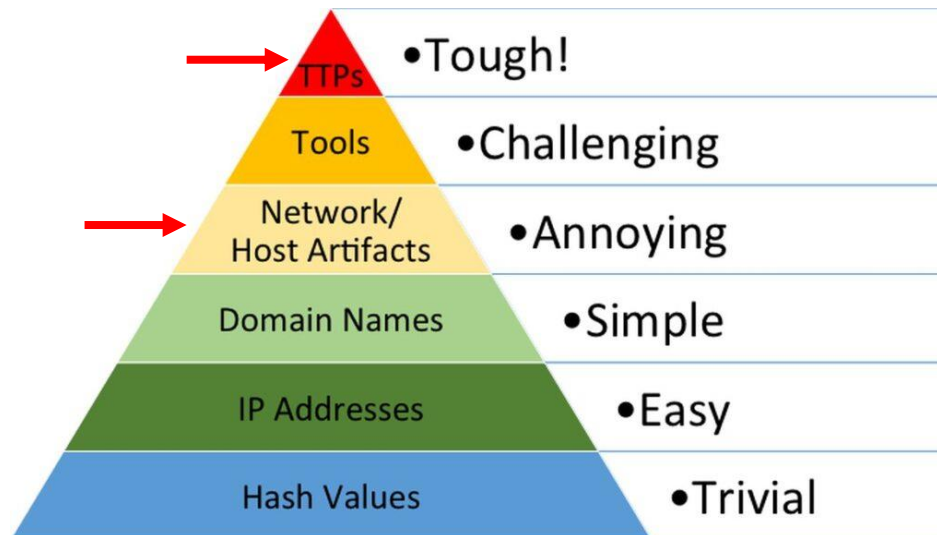
*ParanoidLab effectively **targets** critical cybersecurity pain points by disrupting the use of compromised credentials - a **primary initial access vector for threat actors**. Leveraging the MITRE ATT&CK® framework, **ParanoidLab** focuses on preventing unauthorized access to essential enterprise technologies like Active Directory, VPNs, and RDP through the "Valid Accounts" and "External Remote Services" techniques.*

*By monitoring and mitigating these threats, **ParanoidLab empowers MSSPs, SOCs, and IT Security providers to neutralize the most challenging tactics used by adversaries**, ensuring robust protection at the top of the Pyramid of Pain.*

Become a partner

ParanoidLab

Revenue Growth Opportunities

Expand *your* ***revenue streams*** *and* ***Attract new clients*** *by offering unique, high-value cybersecurity services.*

Enhanced Service Offerings

Provide *your* ***clients real-time alerts*** *and* ***comprehensive protection against*** *threats from* ***Initial Access Brokers*** *and* ***Infostealers****.*

Strengthen Client Trust & Compliance

Demonstrate *your* ***commitment*** *to* ***protecting clients****,* ***partners*** *and* ***employee's*** *data from cyber attacks.*

Partnership Models

MSSP / SOCs / IT Security providers

Partner with us *to* ***help your customers*** *and* ***grow your business*** *with easy-to-manage cybersecurity solutions.*

Integrate our proprietary data ***via API*** *to enhance Compromised Credential checks in any application.*

Resellers

Add a ***profitable****,* ***user-friendly solution*** *to your sales portfolio.*

Use ***ParanoidLab*** *to address the significant problem of Compromised Credentials and Infostealers, easing fears and protecting customers.*

Become a partner

ParanoidLab

Flexible Pricing Models

→ Choose from a variety of pricing options.

Pay-per-API request model for ultimate flexibility.

Easy-to-Setup Easy-to-Use

→ Designed for **rapid deployment** and user-friendly operation.

it's **easy to integrate** into your existing systems and begin protecting your clients right away.

White-Label Solutions

→ Offer our cybersecurity services under your own brand. Seamlessly integrate **ParanoidLab's** services into your existing platforms and workflows with our **custom API** solutions.

Pricing

ParanoidLab

	Free	Standard	Business					
Pricing monthly, USD	0	190	1 000	3 000	5 000	8 000	15 000	25 000
Pricing annually, USD	0	1900	11 000	32 000	54 000	86 000	160 000	260 000
Requests per month	10	100	3 000	10 000	25 000	50 000	100 000	200 000
Targets								
Domains	Unlimited							
Wildcard	+							
E-mails	Unlimited							
Keywords	-	-	Unlimited					
Sources								
InfoStealers	+							
Combo-lists	+							
Telegram	-	-	+					
Forums	-	-	+					
Marketplaces	-	-	+					
API	-	-	+					

Prevent Cyber Attacks Before They Happen

Become a Partner

Whether you're interested in reselling our cybersecurity solutions or integrating them into your existing services, we are here to help

Contact us via email, phone, or LinkedIn to discuss partnership opportunities

Calendly

Linked in