ParanoidLab

Inside the Mind of a Hacker:

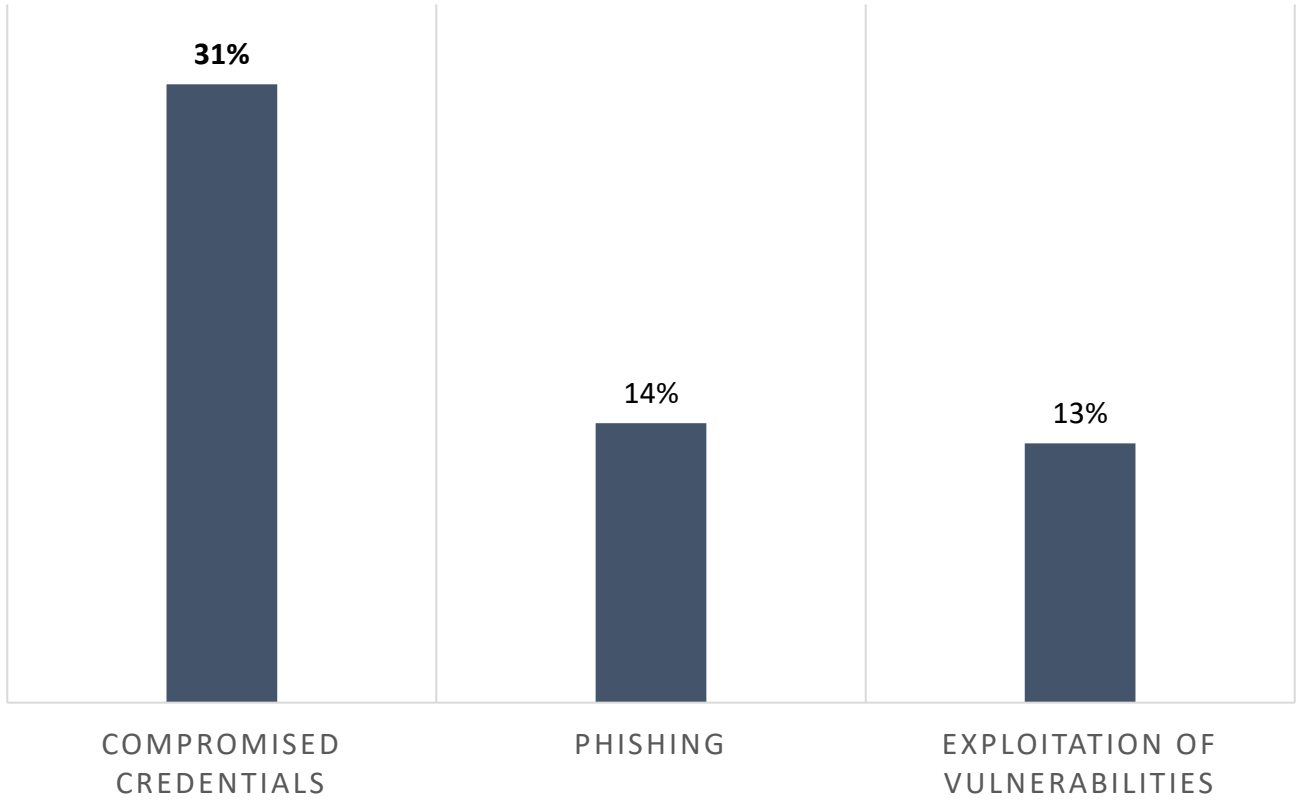
How do Cyber Criminals Find their Targets?

Ransomware

Vectors of attack

ParanoidLab

Over 31% of cyber-attacks involve using compromised credentials as an attack vector



Cyber Kill Chain

ParanoidLab

Reconnaissance on the Dark Web

ParanoidLab

Dark Web

ParanoidLab

Telegram

Weaponization

ParanoidLab

Weaponization

ParanoidLab

Delivery

ParanoidLab

Exploitation

ParanoidLab

Exploitation

ParanoidLab

TrudnyiVozrast

USA

Premium

Регистрация:	12.01.2022
Сообщения:	82
Реакции:	28
Гарант сделки:	3
Депозит:	5 ₿

16.03.2022

Куплю по хорошим ценам:
Быстрая проверка. Анонимно

0day/1day RCE (цена до 10.000.000$)
Windows
VPN
Citrix
Rdweb
Vmware
и другие...

Первый контакт в ПМ с описанием продукта и контактом (qTox)

Installation

Command and control

ParanoidLab

Actions on Objectives

ParanoidLab

Reconnaissance and Initial Access

ParanoidLab

Reconnaissance and Initial Access

ParanoidLab

qupi

байт

Платная регистрация

0

7 публикаций

Регистрация

08/12/21 (ID: 119003)

Деятельность

вирусология / malware

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

Reconnaissance and Initial Access

ParanoidLab

Reconnaissance and Initial Access

ParanoidLab

SYNLAB

[redacted].synlab.de/dana-na/[redacted]

Reconnaissance and Initial Access

ParanoidLab

Reconnaissance and Initial Access

ParanoidLab

[redacted]bayer.com/Citrix/[redacted]

Reconnaissance and Initial Access

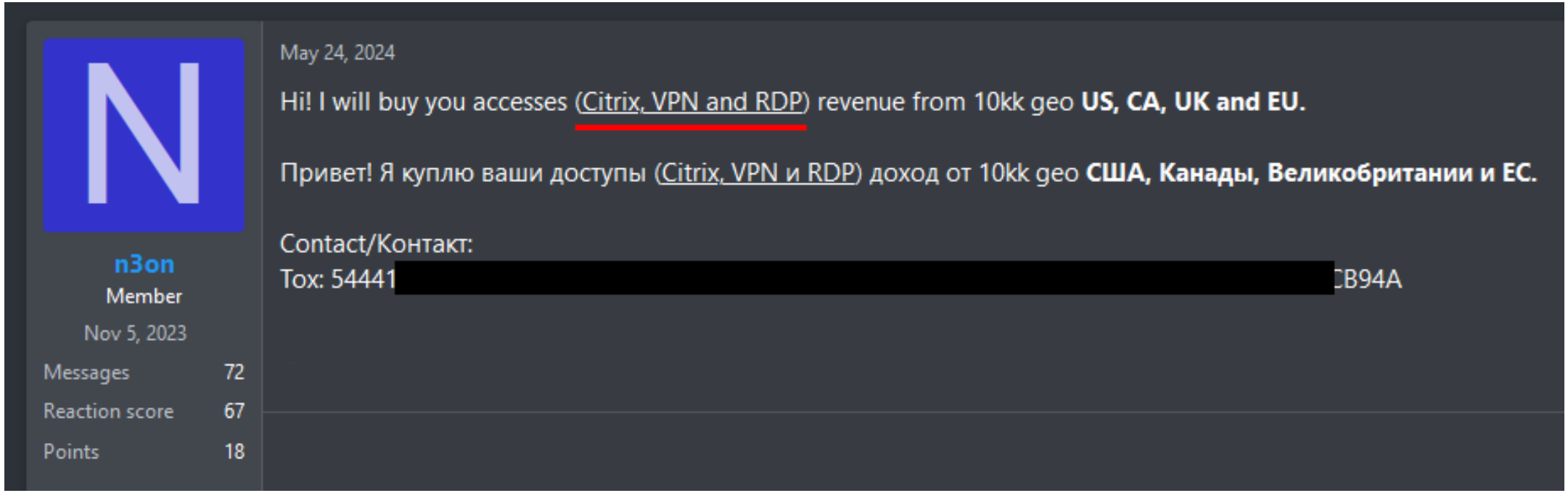
ParanoidLab

ENERCON
ENERGY FOR THE WORLD

[redacted].enercon.de/+CSCOE+/[redacted]

Reconnaissance and Initial Access

ParanoidLab



Lessons learned

ParanoidLab

Contact

ParanoidLab

Eugene Levytskyi

ParanoidLab Inc.

Booth 7A-615a

linkedin.com/in/eugene-levytskyi

https://paranoidlab.com