

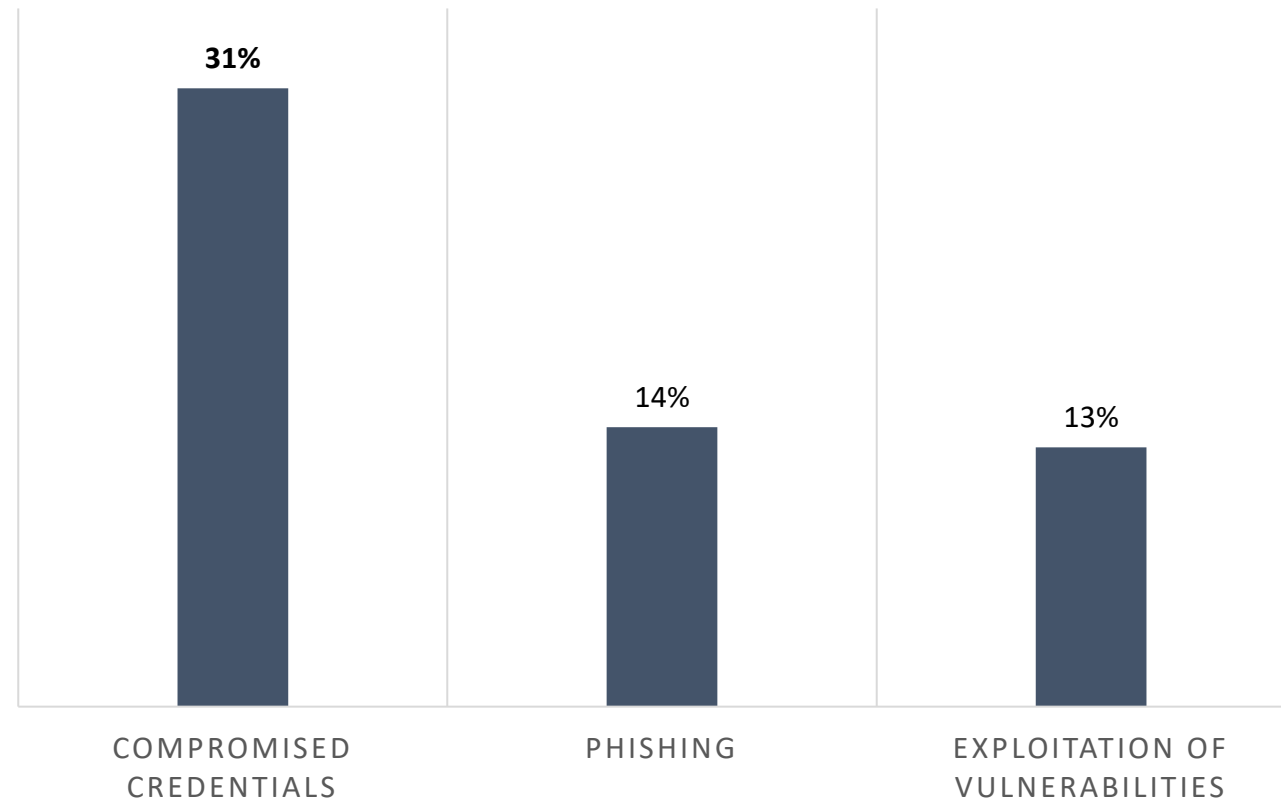


Inside the Mind of a Hacker:

How do Cyber Criminals Find their Targets?



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



Cyber Kill Chain



ParanoidLab



Reconnaissance on the Dark Web



ParanoidLab





~/ XSS.is



exploit.in



Telegram



BF BreachForums



RUSSIAN MARKET

Weaponization



ParanoidLab





REDLINE STEALER

Glade · 19 Фев 2020

16

17

18



Phoenix Native Stealer [C/C++ | 28 KB Build]

PhoenixSteal · 16 Map 2023



META Stealer

__META__ · 7 Map 2022

2







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



ParanoidLab





COMMAND & CONTROL (C2)



ACTIONS ON OBJECTIVES

Reconnaissance and Initial Access



ParanoidLab



Reconnaissance and Initial Access

cupi

байт



Платная регистрация



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

RUSSIAN MARKET



Country:

Germany (77066)

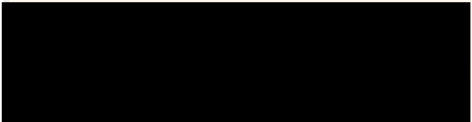
Zip:

The image shows a web form with a dark blue background and a repeating pattern of small, light blue icons. A red rectangular box highlights a dropdown menu for the 'Country:' field. The dropdown menu is open, showing 'Germany (77066)' as the selected option. Below the dropdown, there is a 'Zip:' label and an empty input field. To the left of the highlighted dropdown, there is another dropdown menu, partially visible, showing a small triangle icon.



```
[REDACTED].synlab.de/dana-na/[REDACTED]
```

e-on

 citrix.ssl.eon.com

Reconnaissance and Initial Access



ParanoidLab



bayer.com/Citrix/



 .enercon.de/+CSC0E+/

Reconnaissance and Initial Access



n3on
Member
Nov 5, 2023

Messages	72
Reaction score	67
Points	18

May 24, 2024

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

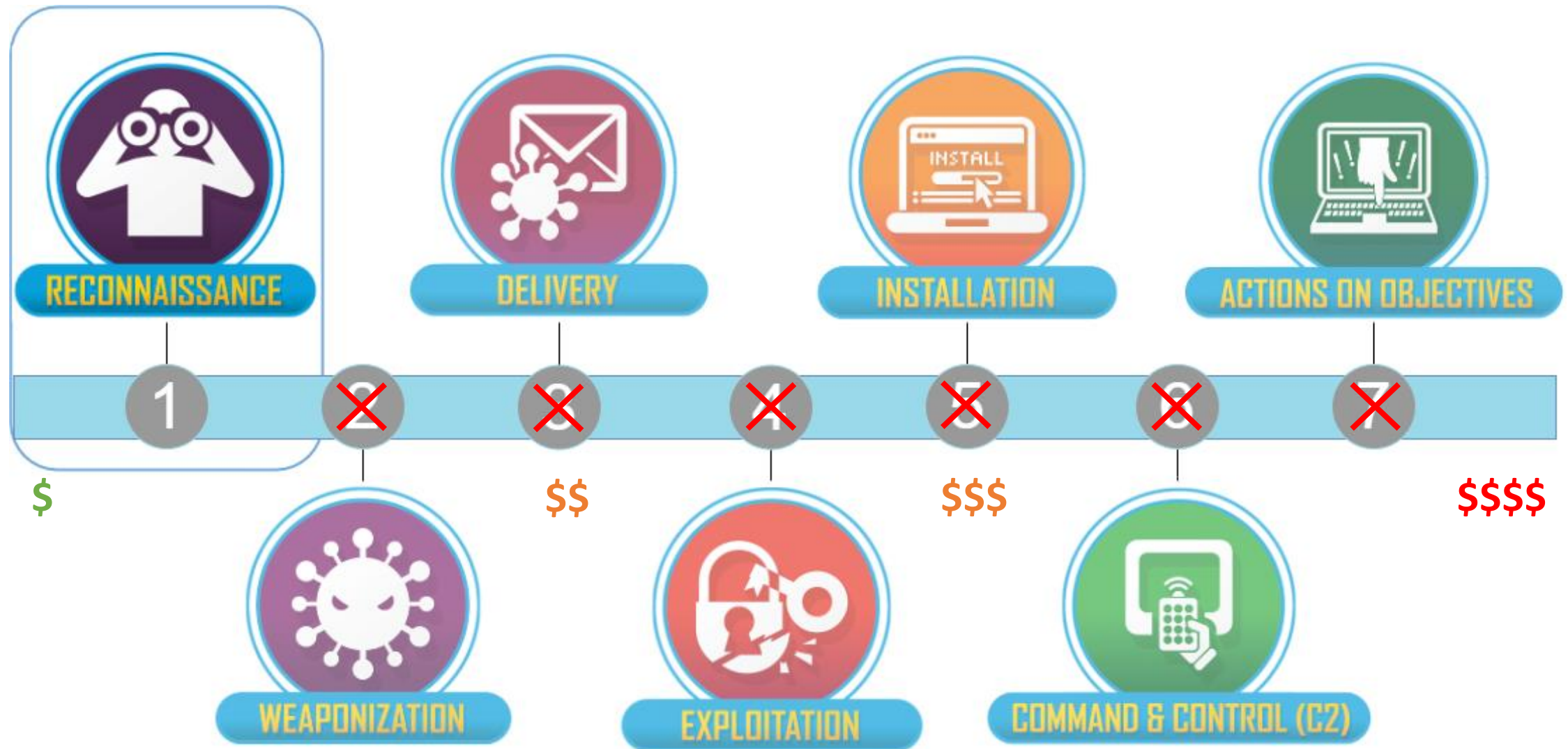
Привет! Я куплю ваши доступы (Citrix, VPN и RDP) доход от 10kk geo **США, Канады, Великобритании и ЕС.**

Contact/Контакт:
Tox: 54441 [REDACTED] B94A

Lessons learned



ParanoidLab





Eugene Levytskyi ParanoidLab Inc.

📍 **Booth 7A-615a**



[linkedin.com/in/eugene-levytskyi](https://www.linkedin.com/in/eugene-levytskyi)



<https://paranoidlab.com>