

Penetration Testers vs Initial Access Brokers

Helping the good guys win



Adrian Furtună
Pentest-Tools.com



> Agenda

- Intro
- Why this talk?
- What are Initial Access Brokers?
- Initial access techniques
- Live demo

> whoami

- Ex-fulltime pentester
 - 15+ years of experience in offensive security
 - Reformed programmer
- Founder @Pentest-Tools.com
- Associate professor @UPB
- Speaker at security events:
 - BlackHat UK
 - Hack.lu
 - Hacktivity
 - Defcamp, etc



> Why this talk?

- Shed a light on bad guys' attack techniques
 - We can reproduce them in attack simulations
 - Learn to better defend against them

- Offensive knowledge can be used for good or for bad
 - Don't go to the dark side



> What are Initial Access Brokers?



IAB



Gain access to corporate networks



Sell access info on Dark Web



Ransomware gang



Buy access to corporate networks



Install ransomware



> What are Initial Access Brokers?



LockBit
Conti
BlackMatter
Hive
Alphv, etc

IAB



Gain access to corporate networks



Sell access info on Dark Web



Ransomware gang



Buy access to corporate networks



Install ransomware



> Where do we find them?



Underground forums & marketplaces like:



- Exploit Forum
 - <https://exploitivzcm5dawzhe6c32bbylyggbjvh5dyvsvb5lkuz5ptmunkmqd.onion/register/>
 - <https://forum.exploit.in>

- XSS Forum
 - <http://xssforumv3isucukbxhdhwz67hoa5e2voakcfkuieq4ch257vsburuid.onion/>
 - <https://xss.is/>



- Breach Forum
 - <http://breached65xqh64s7xbkvqgg7bmj4nj7656hcb7x4g42x753r7zmejgd.onion/>
 - <https://breached.to/>

- and many more









> XSS.is - sneak peek

Обработка SEED фраз, логов и Privat key
AudiA6: Миксер + Обменник
Установка сниффа на ваши шопы

Торговая площадка

Прочитано!

 ДОСТУПЫ: сети, rdp, шеллы, ftp, sql-inj, DB's	Темы 2.9K	Сообщения 13.1K	 Продаю различные доступы. Sell ... Сегодня в 09:19 · Pirat-Networks
 MALWARE: вредоносы, крипт, инжекты, 0/1day экспы	Темы 2.6K	Сообщения 20.3K	 NEW Rhadamanthys Stealer Сегодня в 09:52 · freeide
 СПАМ: рассылки, отклики, базы, mail-дампы	Темы 2K	Сообщения 8.5K	 Gemini.com 5.7M Сегодня в 12:16 · blackedge

> XSS.is - sneak peek

Обработка SEED фраз, логов и Privat key
AudiA6: Миксер + Обменник
Установка сниффа на ваши

Trade platform

Торговая площадка

Прочитано!

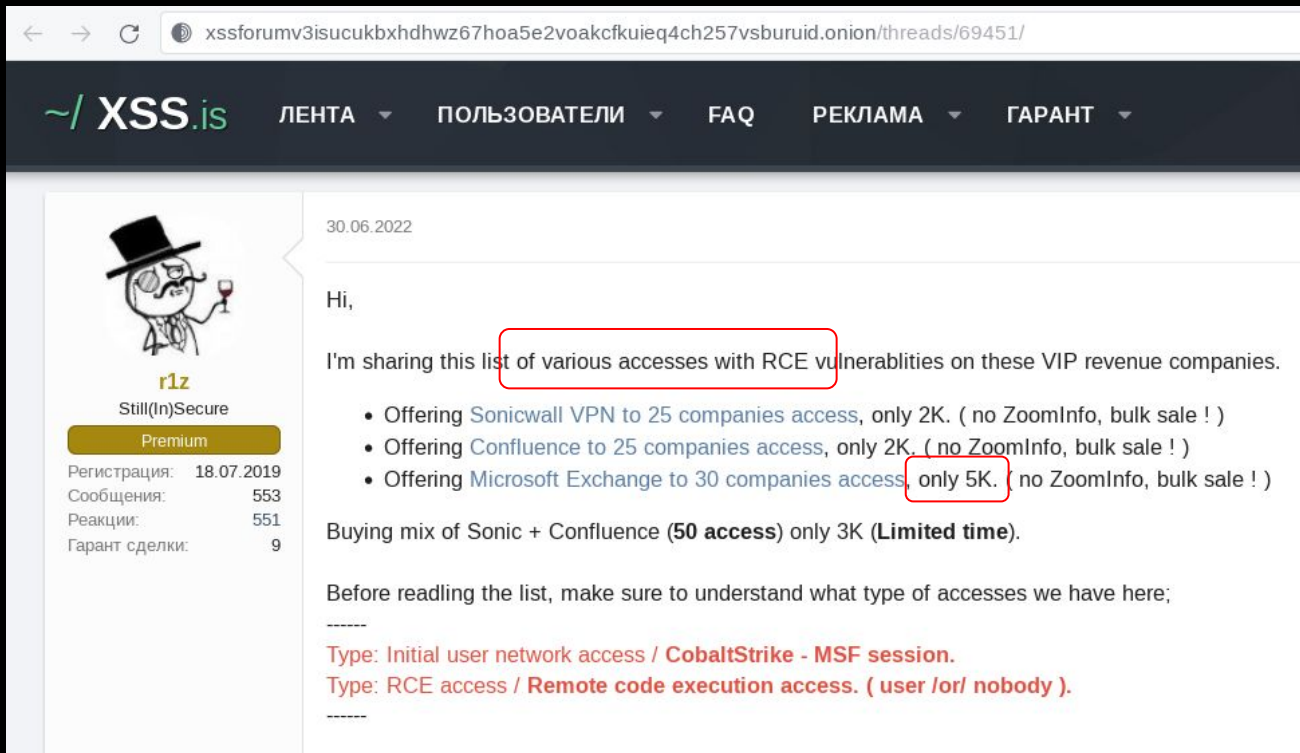
Темы	Сообщения	Пользователь	Тема
2.9K	13.1K	ALAN	Продаю различные доступы. Sell ... Сегодня в 09:19 · Pirat-Networks
2.6K	20.3K	ALAN	NEW Rhadamanthys Stealer Сегодня в 09:52 · freeide
2K	8.5K	ALAN	Gemini.com 5.7M Сегодня в 12:16 · blackedge

> XSS.is - sneak peek

The screenshot shows the XSS.is forum interface. At the top, there's a navigation bar with links for 'ЛЕНТА', 'ПОЛЬЗОВАТЕЛИ', 'FAQ', 'РЕКЛАМА', and 'ГАРАНТ'. Below this is a large banner for 'Brion's Club DUMPS & CARDS'. Underneath the banner, there's a section titled 'Торговая площадка' (Trade platform) with a list of services: 'Обработка SEED фраз, логов и Privat key', 'AudiA6: Миксер + Обменник', and 'Установка сниффа на ваши'. A blue callout box points to this section with the text 'Trade platform'. Below this is a list of forum topics. The first topic is 'ДОСТУПЫ: сети, rdp, шеллы, ftp, sql-inj, DB's' with 2.9K topics and 13.1K messages. A blue callout box points to this topic with the text 'Access: Networks, RDP, Shells, FTP, SQL-Inj, DB's'. Other topics include 'MALWARE: вредоносы, крипт, инжекты, 0/1day экспы' and 'СПАМ: рассылки, отклики, базы, mail-дампы'.

Тема	Сообщения	Последнее сообщение
ДОСТУПЫ: сети, rdp, шеллы, ftp, sql-inj, DB's	2.9K	13.1K
MALWARE: вредоносы, крипт, инжекты, 0/1day экспы	2.6K	20.3K
СПАМ: рассылки, отклики, базы, mail-дампы	2K	8.5K

> Access selling example (1)



The screenshot shows a forum thread on the website XSS.is. The browser address bar displays the URL: `xssforumv3isucukbxhdhwz67hoa5e2voackfkuieq4ch257vsburuid.onion/threads/69451/`. The forum header includes navigation links: ЛЕНТА, ПОЛЬЗОВАТЕЛИ, FAQ, РЕКЛАМА, and ГАРАНТ. The thread is dated 30.06.2022. The user profile for 'r1z' is visible, showing a registration date of 18.07.2019, 553 messages, 551 reactions, and 9 guaranteed deals. The main post content is as follows:

30.06.2022

Hi,

I'm sharing this list of various accesses with RCE vulnerabilities on these VIP revenue companies.

- Offering Sonicwall VPN to 25 companies access, only 2K. (no ZoomInfo, bulk sale !)
- Offering Confluence to 25 companies access, only 2K. (no ZoomInfo, bulk sale !)
- Offering Microsoft Exchange to 30 companies access, only 5K. (no ZoomInfo, bulk sale !)

Buying mix of Sonic + Confluence (50 access) only 3K (Limited time).

Before reading the list, make sure to understand what type of accesses we have here:

Type: Initial user network access / CobaltStrike - MSF session.

Type: RCE access / Remote code execution access. (user /or/ nobody).

> Access selling example (2)




← → ↻ xssforumv3isucukbxhdhwz67hoa5e2voakcfkuieq4ch257vsburuid.onion/threads/74052/

~/ XSS.is ЛЕНТА ▾ ПОЛЬЗОВАТЕЛИ ▾ FAQ РЕКЛАМА ▾ ГАРАНТ ▾

Торговая площадка > ДОСТУПЫ: сети, rdp, шеллы, ftp, sql-inj,... >

Citrix

👤 Salvador_Dali · 🕒 07.10.2022



Salvador_Dali
My life-my rules

Premium

Регистрация: 04.11.2019
Сообщения: 57
Реакции: 20
Гарант сделки: 6
Депозит: 0 ₪

07.10.2022

Свежак.Citrix,USA
AD
В сети 160 хостов.
Металлургия.
Ревеню 256кк

🔔 Жалоба

> Access selling example (2)




← → ↻ xssforumv3isucukbxhdhwz67hoa5e2voakcfkueiq4ch257vsburuid.onion/threads/74052/

~/ XSS.is ЛЕНТА ▾ ПОЛЬЗОВАТЕЛИ ▾ FAQ РЕКЛАМА ▾ ГАРАНТ ▾

Торговая площадка > ДОСТУПЫ: сети, rdp, шеллы, ftp, sql-inj,... >

Citrix

👤 Salvador_Dali · 🕒 07.10.2022



Salvador_Dali
My life-my rules

Premium

Регистрация: 04.11.2019
Сообщения: 57
Реакции: 20
Гарант сделки: 6
Депозит: 0 ₪

07.10.2022

Свежак.Citrix,USA
AD
В сети 160 хостов.
Металлургия.
Ревеню 256кк

🗨 Жалоба

Citrix, USA
AD
There are 160 hosts on the network.
Metallurgy.
Rhound 256kk

> Access selling example (3)



← → ↻ xssforumv3isucukbxhdhwz67hoa5e2voakcfkuieq4ch257vsburuid.onion/threads/74369/

~/ XSS.is ЛЕНТА ▾ ПОЛЬЗОВАТЕЛИ ▾ FAQ РЕКЛАМА ▾ ГАРАНТ ▾

Торговая площадка > ДОСТУПЫ: сети, rdp, шеллы, ftp, sql-inj,... >

blog.archive.org for Sale

1877te · 15.10.2022 · archive

15.10.2022

archive.org subdomain.

Price: \$750

Вложения

0.jpg

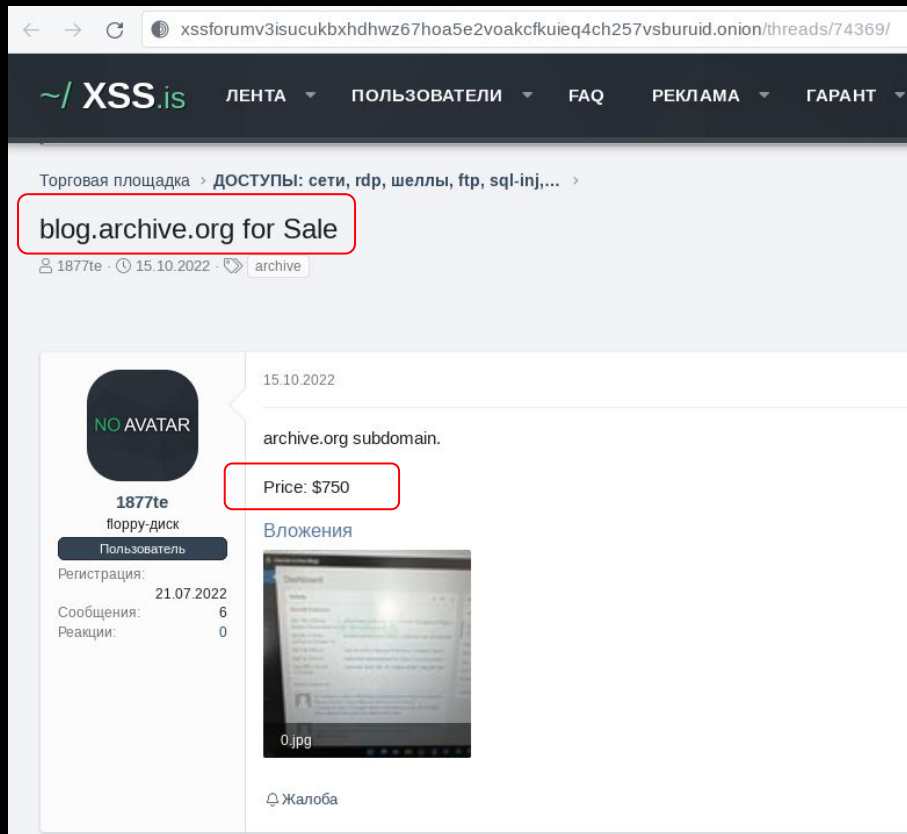
Жалоба

NO AVATAR

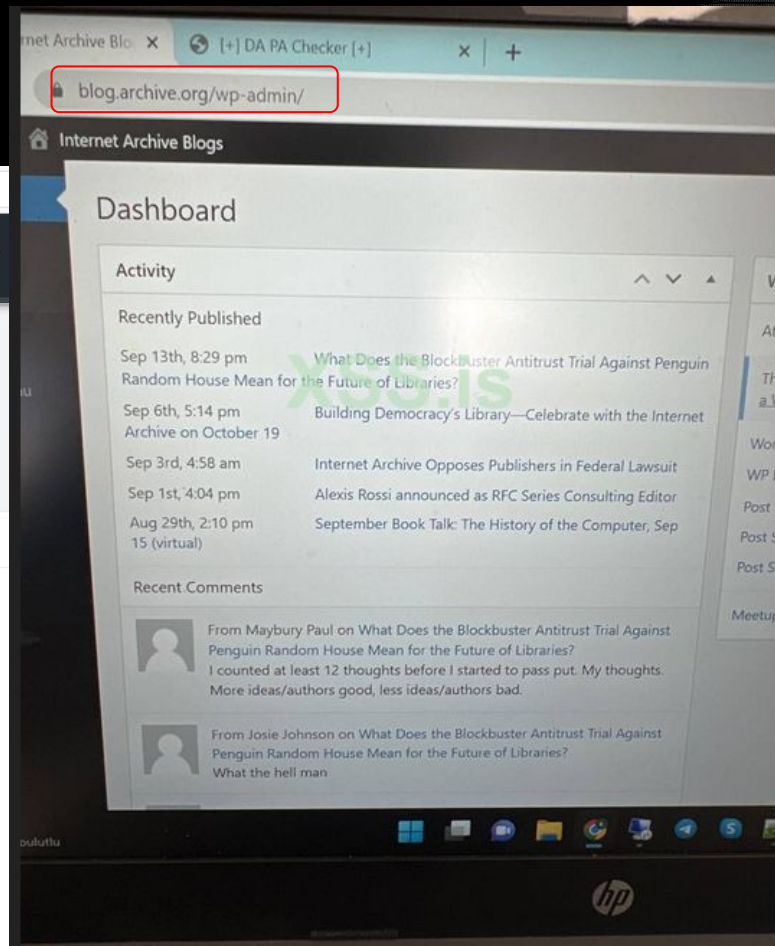
1877te
форру-диск
Пользователь

Регистрация: 21.07.2022
Сообщения: 6
Реакции: 0

> Access selling example (3)



The screenshot shows a forum post on the XSS.is website. The URL in the browser is `xssforumv3isucukbxdhzw67hoa5e2voakcfkuieq4ch257vsburuid.onion/threads/74369/`. The post title is `blog.archive.org for Sale`, which is highlighted with a red box. The post was made by user `1877te` on `15.10.2022`. The price is listed as `Price: $750`, also highlighted with a red box. The post content includes the text `archive.org subdomain.` and an image of a computer screen showing a webpage. The user's profile information shows a registration date of `21.07.2022`, 6 messages, and 0 reactions.



The screenshot shows a WordPress dashboard for the website `blog.archive.org`. The URL in the browser is `blog.archive.org/wp-admin/`, highlighted with a red box. The dashboard displays the `Internet Archive Blogs` site. The `Activity` section shows a list of recently published posts:

- Sep 13th, 8:29 pm: What Does the Blockbuster Antitrust Trial Against Penguin Random House Mean for the Future of Libraries?
- Sep 6th, 5:14 pm: Building Democracy's Library—Celebrate with the Internet Archive on October 19
- Sep 3rd, 4:58 am: Internet Archive Opposes Publishers in Federal Lawsuit
- Sep 1st, 4:04 pm: Alexis Rossi announced as RFC Series Consulting Editor
- Aug 29th, 2:10 pm: September Book Talk: The History of the Computer, Sep 15 (virtual)

The `Recent Comments` section shows two comments:

- From Maybury Paul on What Does the Blockbuster Antitrust Trial Against Penguin Random House Mean for the Future of Libraries? I counted at least 12 thoughts before I started to pass put. My thoughts. More ideas/authors good, less ideas/authors bad.
- From Josie Johnson on What Does the Blockbuster Antitrust Trial Against Penguin Random House Mean for the Future of Libraries? What the hell man



> Most interesting access types being sold

- RDP
- VPN
- Citrix
- Web admin panels & CMSs



> How do we know their methods?

- By studying ransomware gangs:
 - CISA Advisory on Conti ransomware - March 2022 (1)
 - Threat Intelligence reports
 - RecordedFuture - IAB Report - August 2022 (2)
 - KELA - Ransomware report - October 2022 (3)
 - Conti Leaks - February 2022 (4)
 - Public breach reports:
 - CISCO hack - August 2022 (5)
 - Colonial Pipeline attack - May 2021 (6)
- (1) https://www.cisa.gov/uscert/sites/default/files/publications/AA21-265A-Conti_Ransomware_TLP_WHITE.pdf
- (2) <https://g-recaptcha.com/enterprise/v2-0802.pdf>
- (3) https://ke-la.com/wp-content/uploads/2022/10/KELA-RESEARCH_Ransomware-Victims-and-Network-Access-Sales-in-Q3-2022.pdf
- (4) <https://www.cisecurity.org/insights/blog/the-conti-leaks-a-case-of-cybercrimes-commercialization>
- (5) <https://blog.talosintelligence.com/recent-cyber-attack/>
- (6) <https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know>



> Common techniques for initial access

Technique	Mitre Att@ck
Spear phishing: malicious attachments	T1566.001
Spear phishing: malicious links	T1566.002
Valid accounts - from leaked credentials	T1110.004
Valid accounts - from password brute-forcing	T1110.001
Fake software promoted via SEO	T1189
Exploit vulnerabilities in external assets	T1190
Malware distribution networks (e.g. ZLoader)	-

+ Installing infostealers like: RedLine, Vidar, Raccoon, etc

> Common techniques for initial access



Technique	Mitre Att@ck
Spear phishing: malicious attachments	T1566.001
Spear phishing: malicious links DEMO	T1566.002
Valid accounts - from leaked credentials	T1110.004
Valid accounts - from password brute-forcing DEMO	T1110.001
Fake software promoted via SEO	T1189
Exploit vulnerabilities in external assets DEMO	T1190
Malware distribution networks (e.g. ZLoader)	-

+ Installing infostealers like: RedLine, Vidar, Raccoon, etc



Live Demo

Simulate initial access attacks

with [Pentest-Tools.com](https://pentest-tools.com)



> Demo scenarios

1. RDP brute force
2. Exploit unpatched service
3. Spear phishing

> Spear phishing: malicious link



<https://pentest-tools.com>

1. Download
attack file (.doc)



8. Evidence of successful
attack is sent to PTT



2. Archive file + password
3. Upload file to G Drive
4. Send phishing email to
victim + link



4. User downloads file from link
5. User extracts archive
6. User opens document
7. User enables macros





> Conclusions

- Pentesters vs IABs
 - Same techniques
 - Very different intent: ethical vs malicious
- IABs are key to growth of ransomware attacks
- Don't go to the dark side



Pentest yourself, don't get hacked.

Thank you!

<https://pentest-tools.com>