Penetration Testers
vs
Initial Access Brokers

Helping the good guys win

Adrian Furtună
Pentest-Tools.com

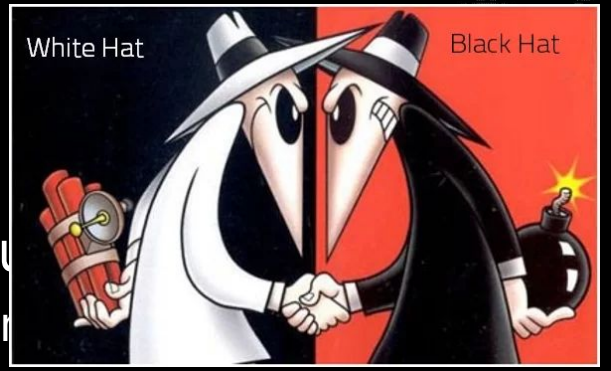
> Agenda

- 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 techniqu
  - We can reproduce them in attack simulatio
  - 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?

IAB

Gain access to corporate networks → **Sell access** info on Dark Web

Ransomware gang

Buy access to corporate networks → **Install** ransomware

LockBit
Conti
BlackMatter
Hive
Alphv, etc

> Where do we find them?

Underground forums & marketplaces like:

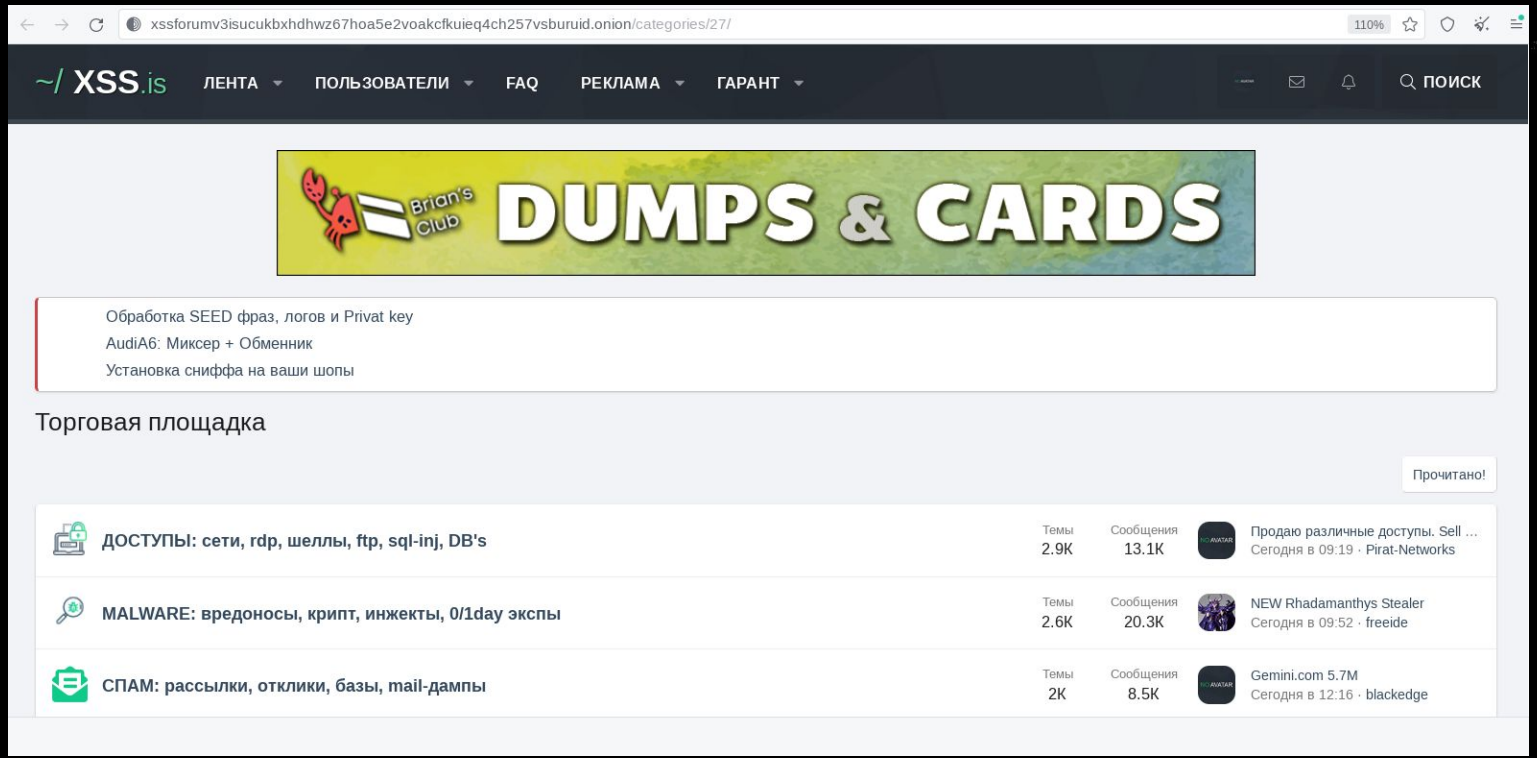
- Exploit Forum
  - https://exploitivzcm5dawzhe6c32bbylyggbjvh5dyvsvb5lkuz5ptmunkmqd.onion/register/
  - https://forum.exploit.in

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

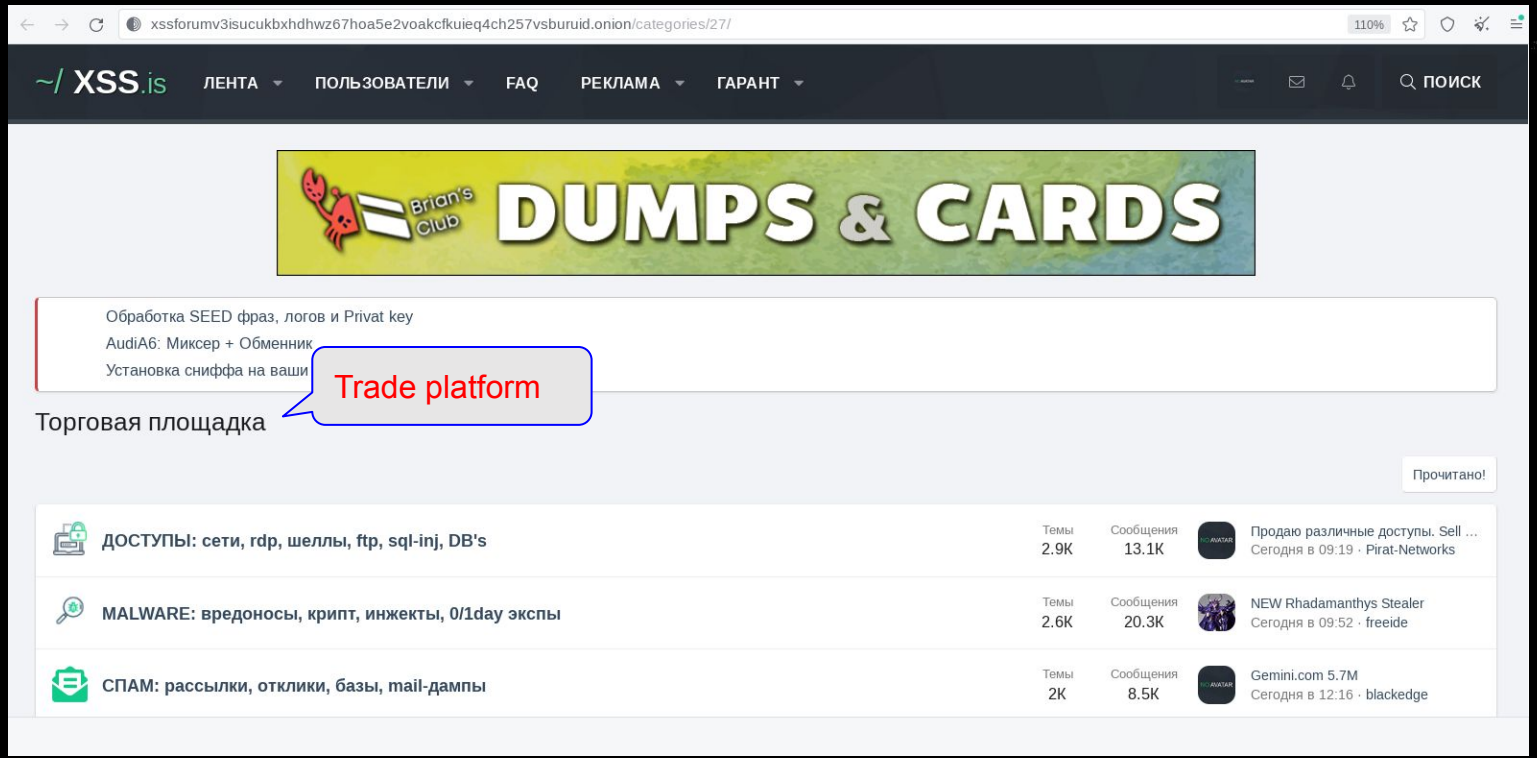
- Breach Forum
  - http://breached65xqh64s7xbkvqgg7bmj4nj7656hcb7x4g42x753r7zmejqd.onion/
  - https://breached.to/

- and many more

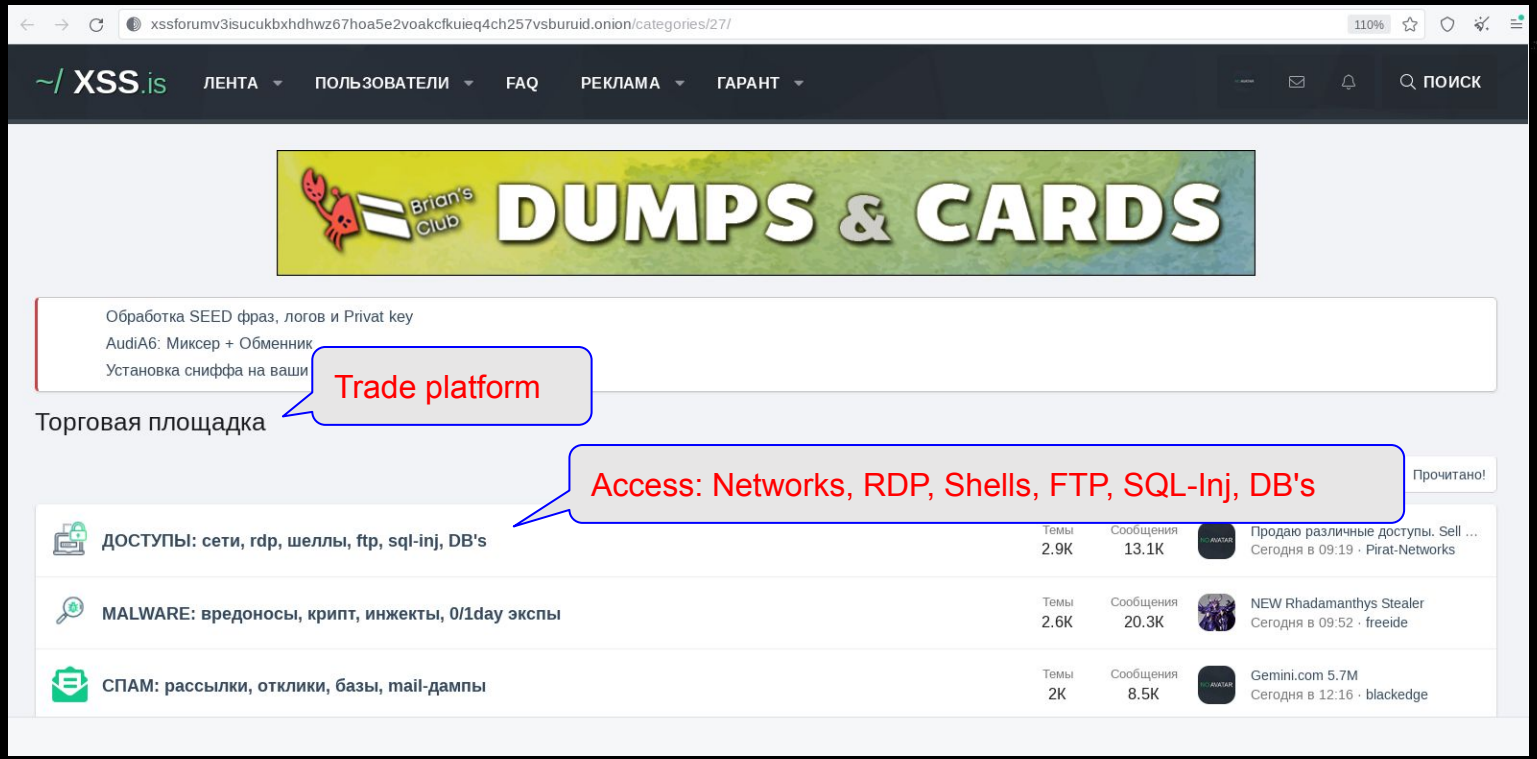
> XSS.is - sneak peek



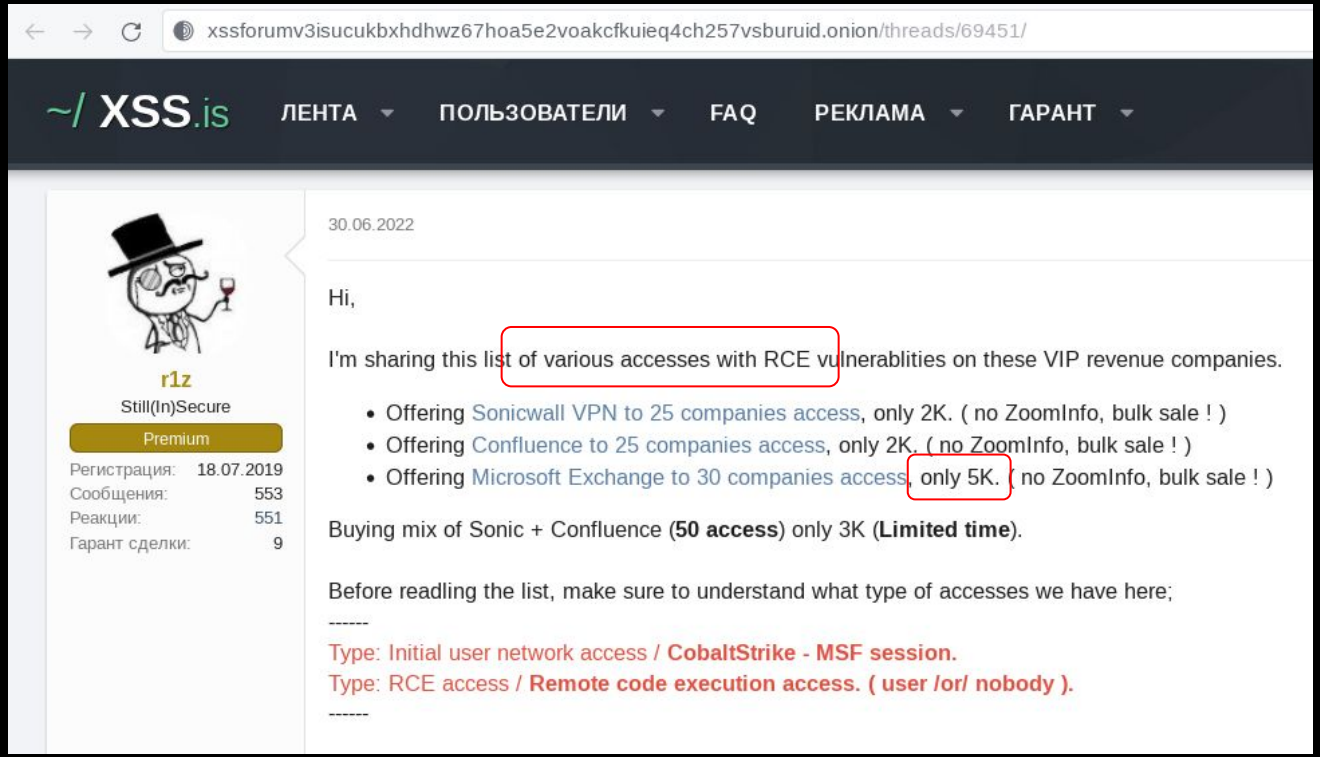
> XSS.is - sneak peek



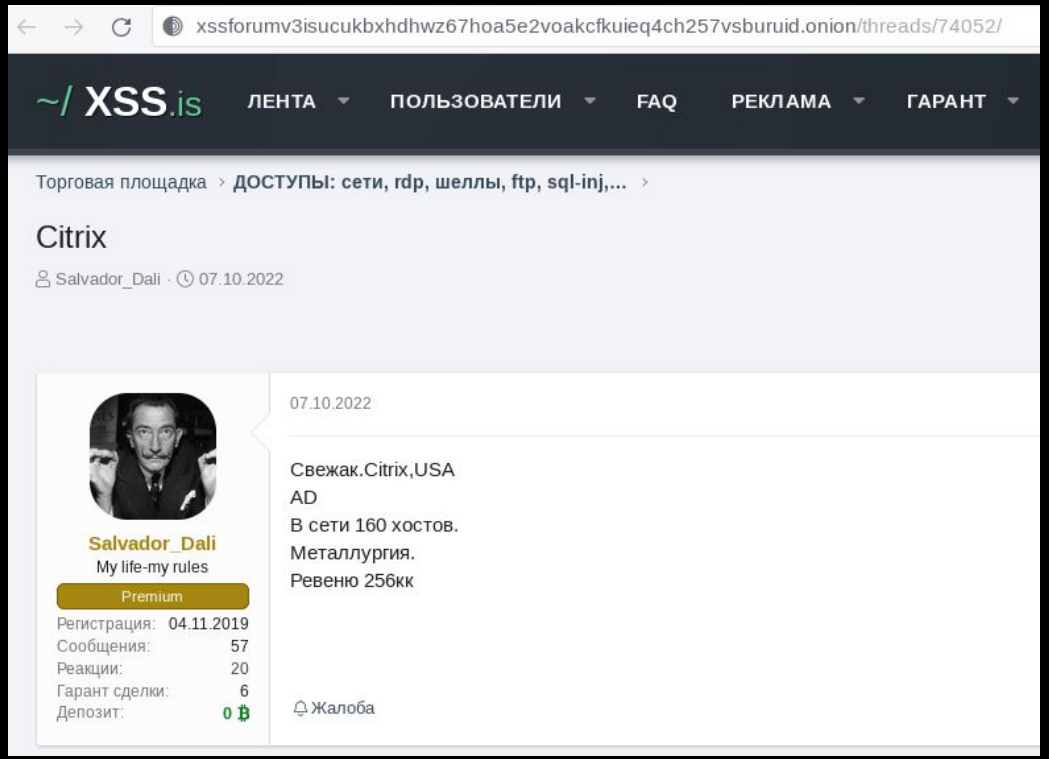
> XSS.is - sneak peek



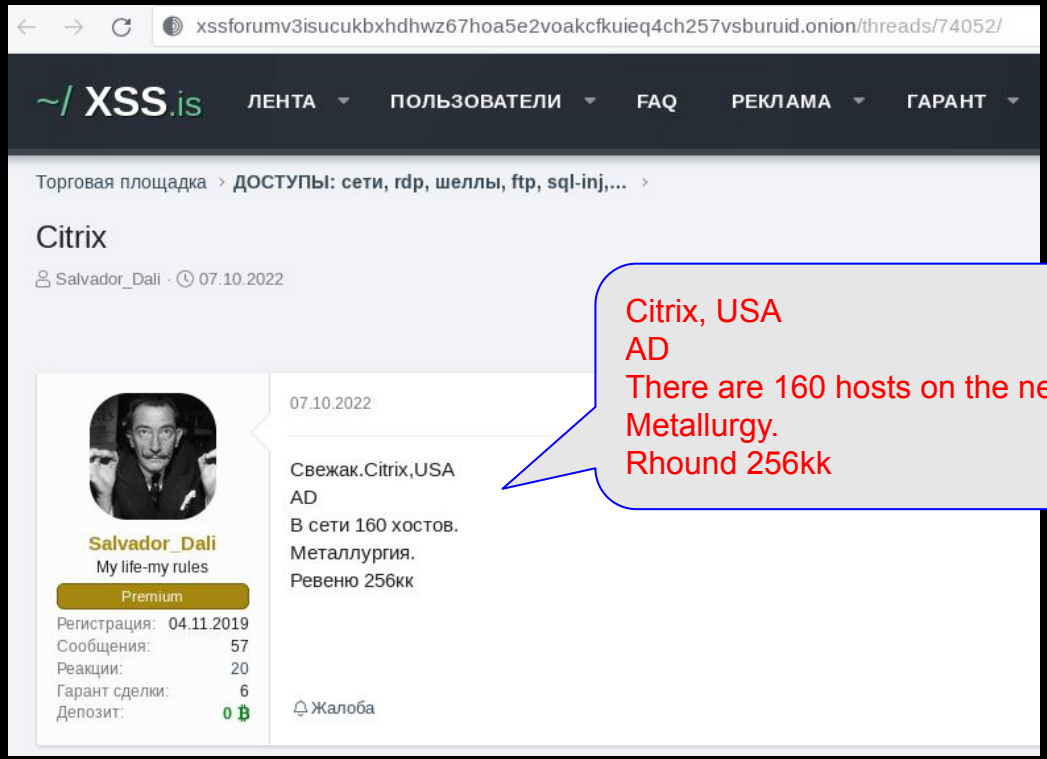
> Access selling example (1)



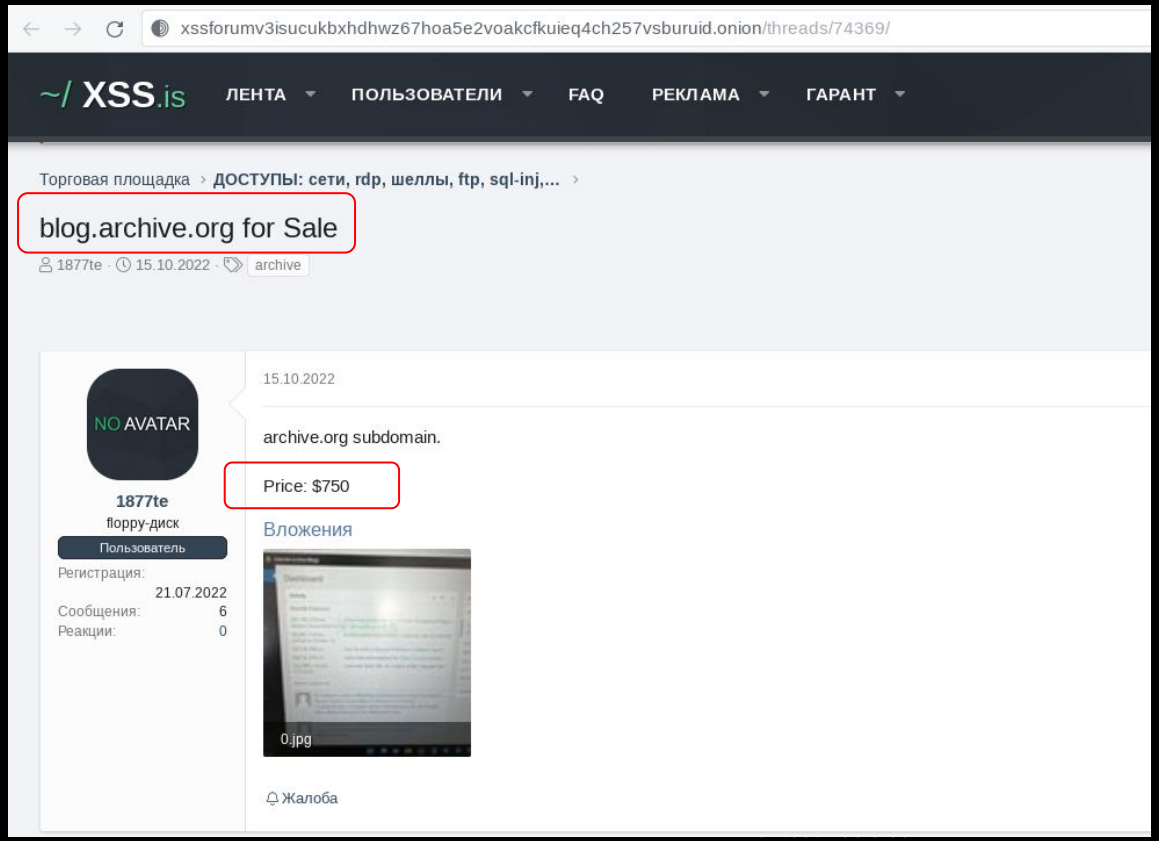
> Access selling example (2)



> Access selling example (2)



> Access selling example (3)



> 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

NO AVATAR

1877te

floppy-диск

Пользователь

Регистрация: 21.07.2022

Сообщения: 6

Реакции: 0

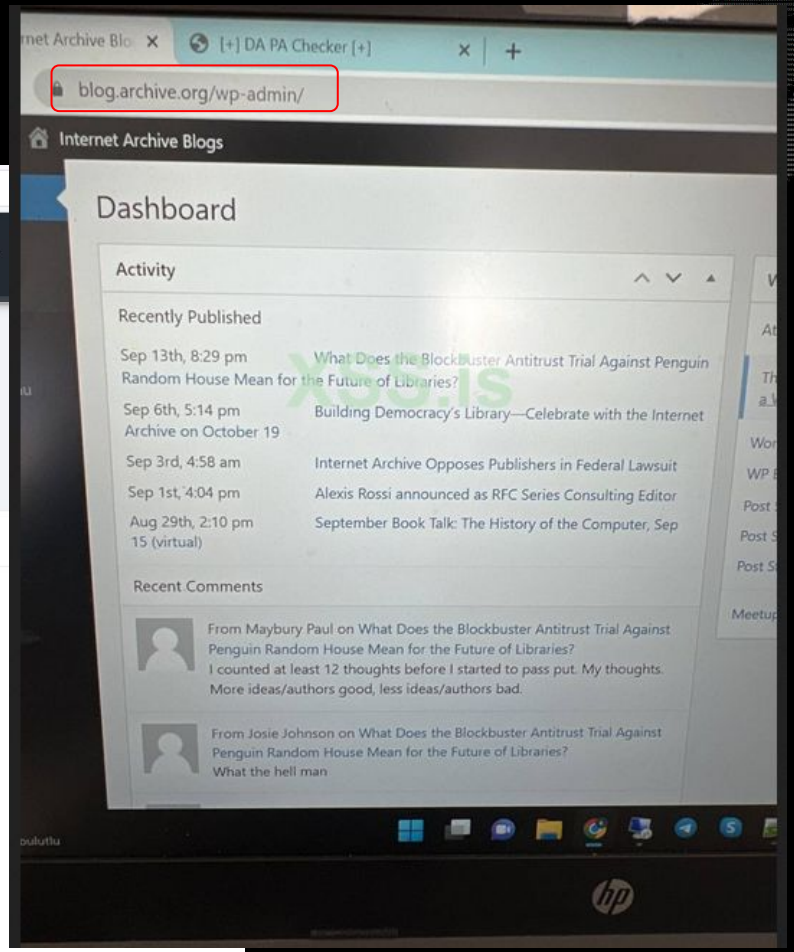
15.10.2022

archive.org subdomain.

Price: $750

Вложения

Жалоба



> 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://go.recordedfuture.com/hubfs/reports/cta-2022-0802.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

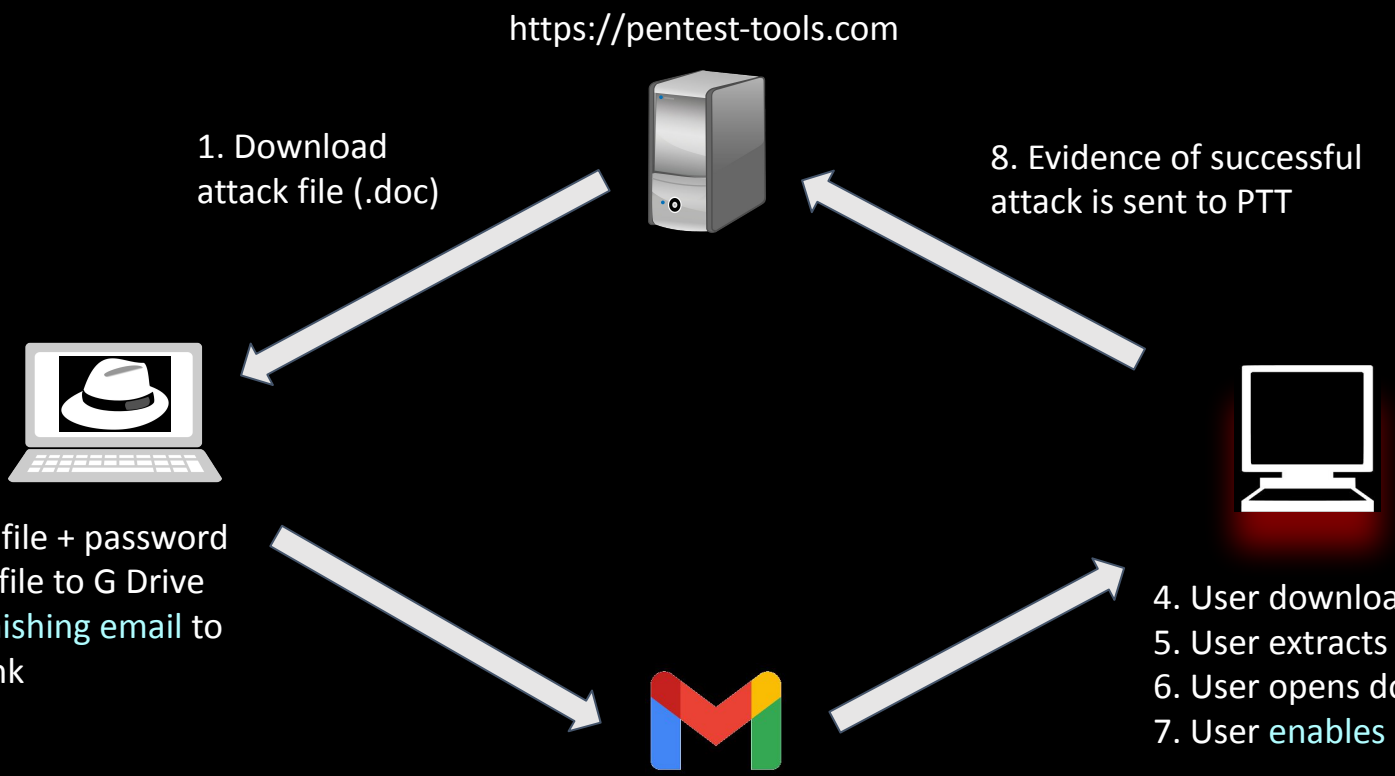
Simulate initial access attacks

with Pentest-Tools.com

> Demo scenarios

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

> Spear phishing: malicious link



> 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