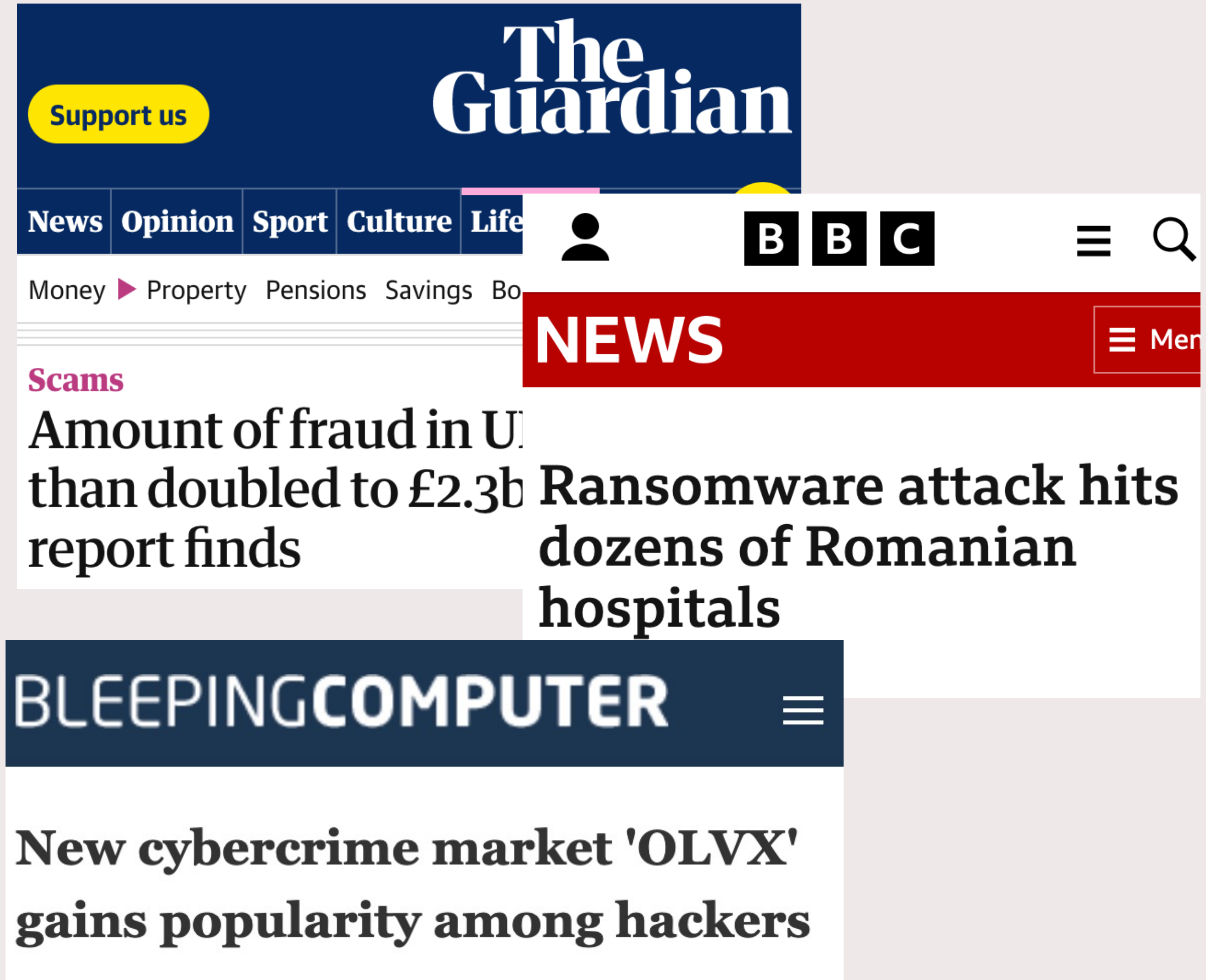
Understanding and Characterizing the Cybercriminal Ecosystem Enabling Attack Innovation at Scale

Michele Campobasso

Security Group, Mathematics and Computer Science

TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

Underground forums as criminal marketplaces



Support us

The Guardian

News Opinion Sport Culture Life

Money ▶ Property Pensions Savings Bo

Scams

Amount of fraud in U than doubled to £2.3b report finds

BBC

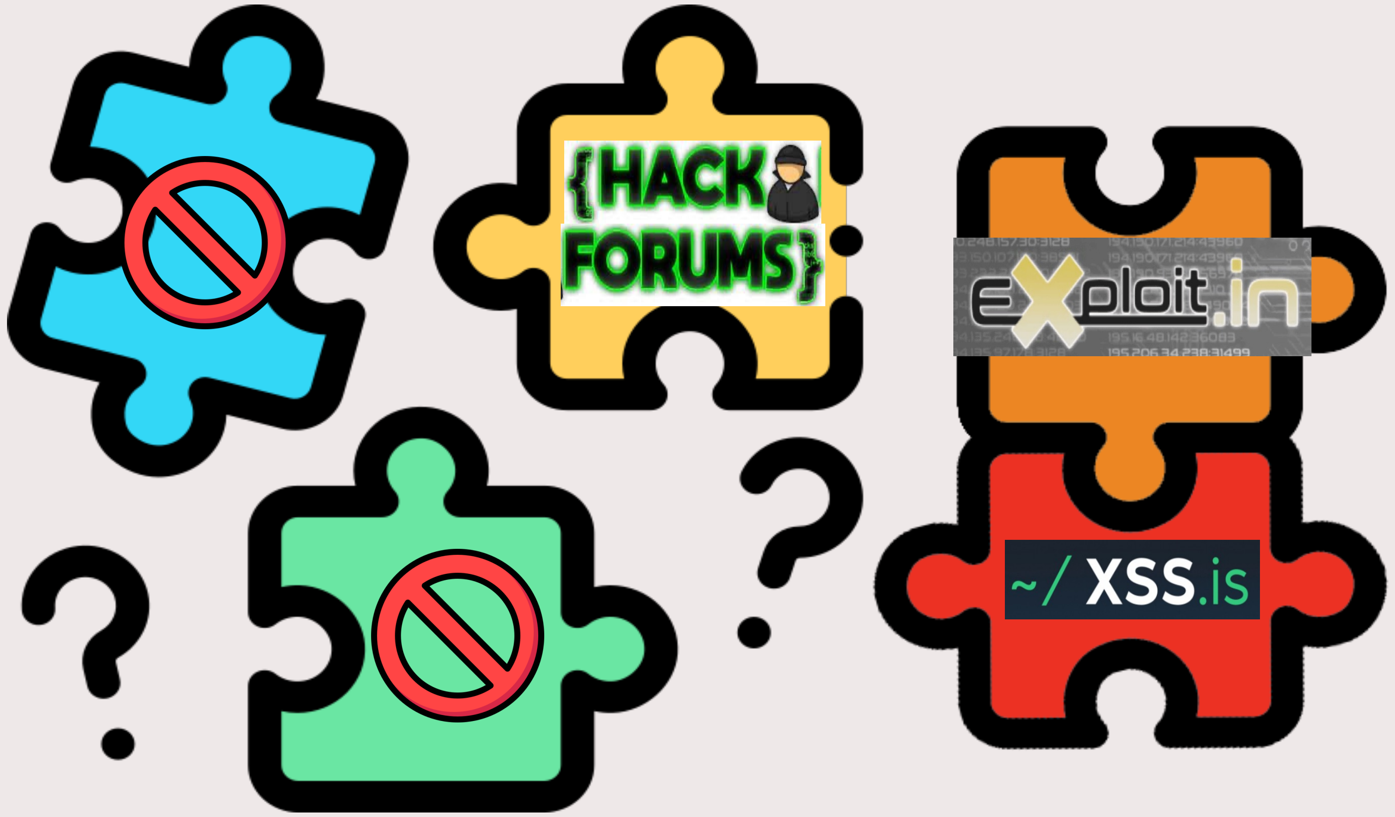
NEWS

☰ Men

Ransomware attack hits dozens of Romanian hospitals

BLEEPINGCOMPUTER

New cybercrime market 'OLVX' gains popularity among hackers



A large, fragmented ecosystem, hard to navigate

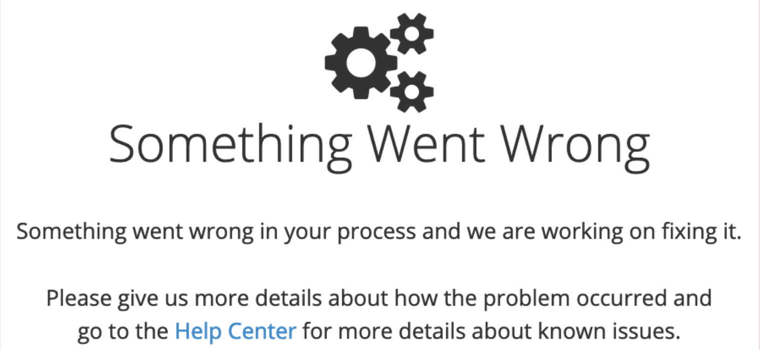
We need to better understand how it works

Open problems

Where do actual threats appear?

Market economy matters for product innovation!

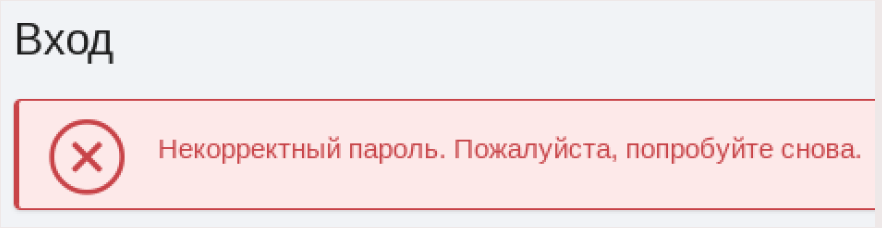
How to get the data?



Something Went Wrong

Something went wrong in your process and we are working on fixing it.

Please give us more details about how the problem occurred and go to the Help Center for more details about known issues.

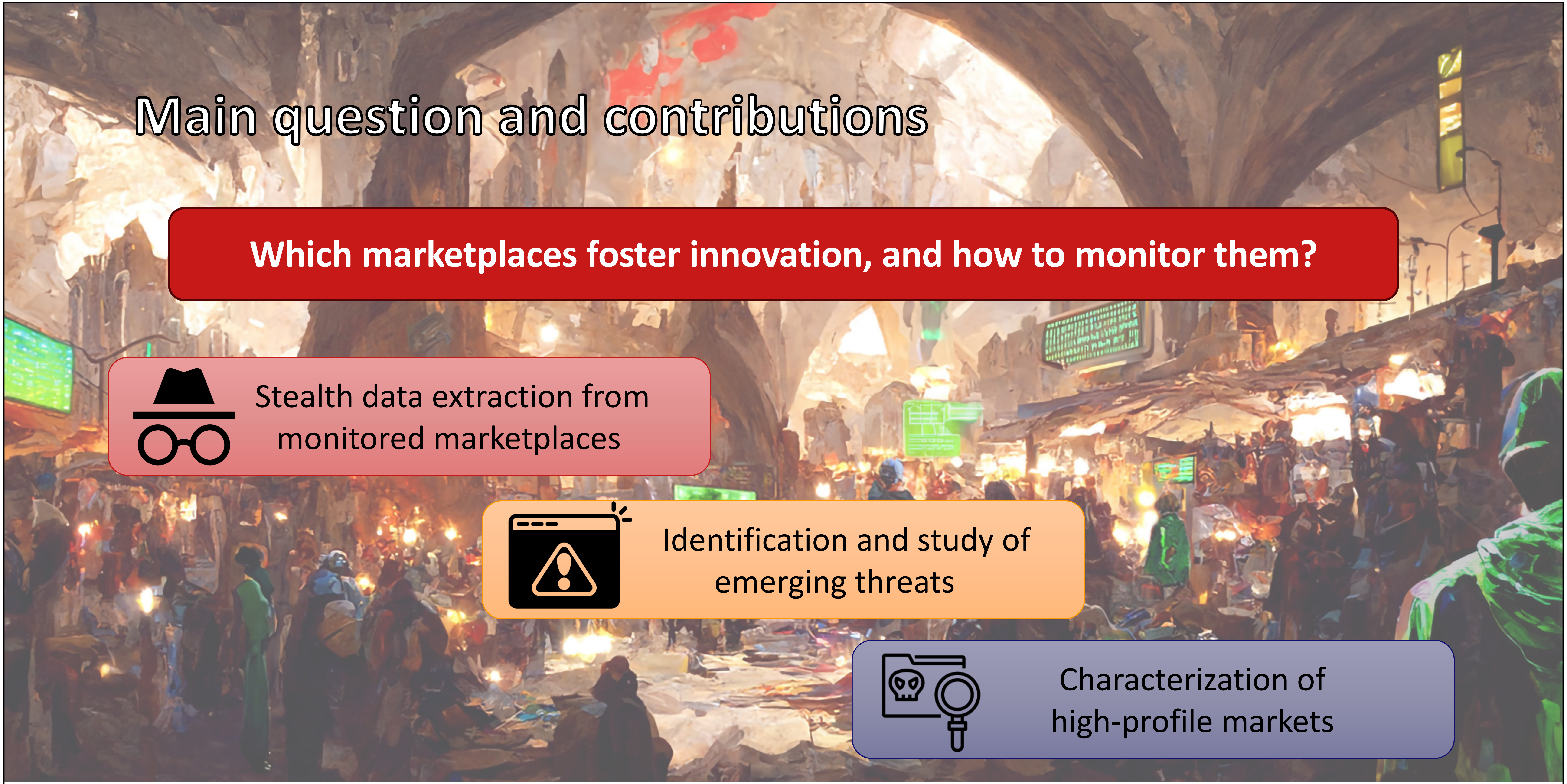


Вход

Некорректный пароль. Пожалуйста, попробуйте снова.

We need effective techniques and tools for the scientific community for stealth data extraction

Main question and contributions



Which marketplaces foster innovation, and how to monitor them?

Stealth data extraction from monitored marketplaces

Identification and study of emerging threats

Characterization of high-profile markets

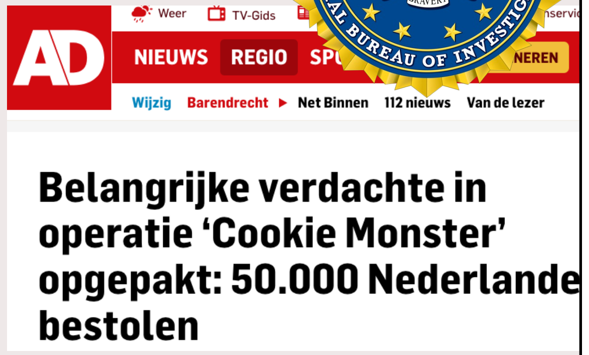
Overview of contributions

Part I:

Method for stealth data extraction
Open-source tool available

Part II:

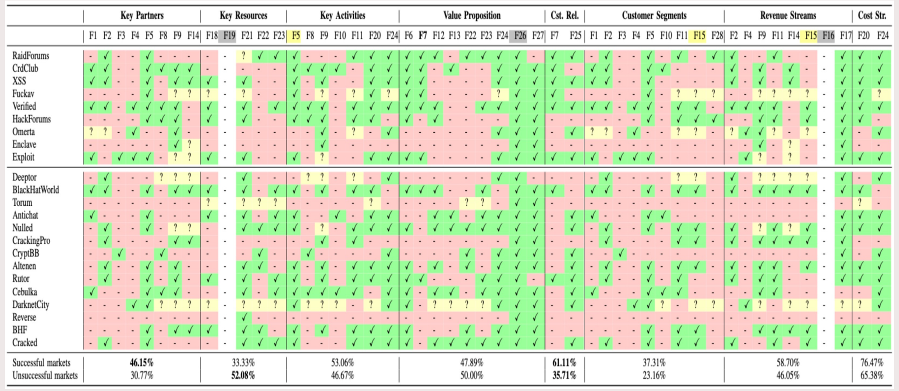
Characterization of novel IMPaaS threat model
Analysis of targets across the globe
Findings instrumetal to Genesis Market takedown



Belangrijke verdachte in operatie 'Cookie Monster' opgepakt: 50.000 Nederlande bestolen

Part III:

Identification of "successful" markets

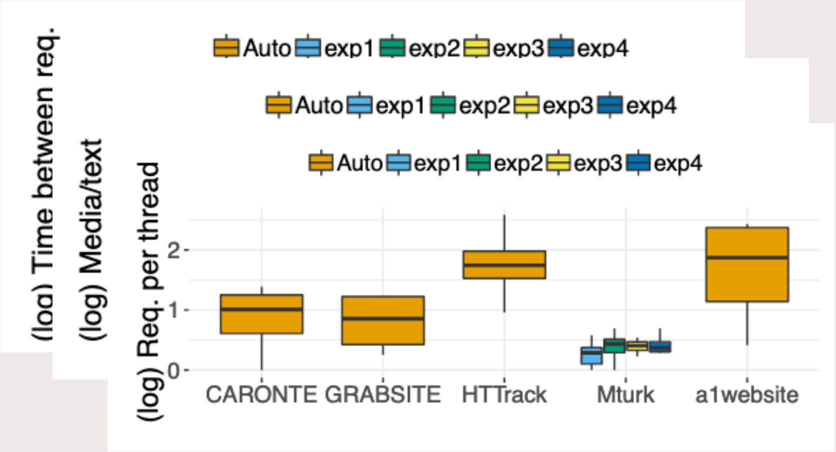


	Key Partners								Key Resources					Key Activities							Value Proposition									Cst. Rel.		Customer Segments									Revenue Streams								Cost Str.	
	F1	F2	F3	F4	F5	F8	F9	F14	F18	F19	F21	F22	F23	F5	F8	F9	F10	F11	F20	F24	F6	**F7**	F12	F13	F22	F23	F24	F26	F27	F7	F25	F1	F2	F3	F4	F5	F10	F11	F15	F28	F2	F4	F9	F11	F14	F15	F16	F17	F20	F24
RaidForums	-	✓	-	-	✓	-	-	-	-	-	?	✓	✓	✓	-	-	-	✓	✓	✓	✓	✓	✓	-	✓	✓	✓	✓	-	✓	✓	-	✓	-	-	✓	-	✓	-	✓	✓	-	-	✓	-	-	-	✓	✓	✓
CrdClub	✓	✓	-	-	✓	✓	✓	✓	-	-	-	-	-	✓	✓	✓	✓	-	✓	✓	✓	✓	-	✓	-	-	✓	✓	✓	✓	-	✓	✓	-	-	✓	✓	-	-	-	✓	-	✓	-	✓	-	-	✓	✓	✓
XSS	✓	✓	-	-	✓	-	✓	✓	✓	-	✓	-	-	✓	-	✓	-	-	✓	✓	✓	✓	-	-	-	-	✓	✓	✓	✓	✓	✓	✓	-	-	✓	-	-	-	-	✓	-	✓	-	✓	-	-	✓	✓	✓
Fuckav	-	-	-	-	✓	-	?	?	?	-	?	-	-	✓	-	?	-	?	✓	?	✓	✓	-	-	-	-	?	✓	✓	✓	-	-	-	-	-	✓	-	?	?	?	-	-	?	?	?	?	-	✓	✓	?
Verified	✓	✓	-	✓	✓	✓	✓	-	✓	-	✓	-	✓	✓	✓	✓	-	✓	✓	✓	✓	✓	✓	-	-	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	-	✓	✓	-	✓	✓	✓	✓	-	✓	-	✓	✓	✓
HackForums	-	-	-	-	✓	✓	✓	-	✓	-	✓	-	-	✓	✓	✓	-	✓	✓	-	✓	-	✓	-	-	-	-	✓	✓	-	-	-	-	-	-	✓	-	✓	✓	✓	-	-	✓	✓	-	✓	-	✓	✓	-
Omerta	?	?	-	✓	-	-	✓	-	-	-	-	-	-	-	-	✓	-	?	-	✓	-	-	-	-	-	-	✓	✓	✓	-	✓	?	?	-	✓	-	-	?	?	-	?	✓	✓	?	-	?	-	✓	-	✓
Enclave	-	-	-	-	-	-	✓	?	-	-	-	-	-	-	-	✓	-	-	-	-	-	-	-	-	-	-	-	✓	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	✓	-	?	-	-	✓	-	-
Exploit	✓	-	✓	✓	✓	-	?	?	✓	-	✓	-	-	✓	-	?	-	-	✓	✓	✓	✓	-	-	-	-	✓	✓	✓	✓	✓	✓	-	✓	✓	✓	-	-	-	-	-	✓	?	-	?	-	-	✓	✓	✓
Deeptor	-	✓	-	-	-	?	?	?	-	-	✓	-	-	-	?	?	-	?	-	✓	-	-	-	-	-	-	✓	✓	-	-	-	-	✓	-	-	-	-	?	?	-	✓	-	?	?	?	?	-	✓	-	✓
BlackHatWorld	✓	✓	-	-	✓	-	✓	✓	✓	-	✓	-	✓	✓	-	✓	-	✓	✓	-	✓	✓	✓	-	-	✓	-	✓	✓	✓	-	✓	✓	-	-	✓	-	✓	✓	-	✓	-	✓	✓	✓	✓	-	✓	✓	-
Torum	-	-	-	-	-	-	-	-	?	-	?	?	?	-	-	-	-	-	?	-	-	-	-	-	?	?	-	✓	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	?	-
Antichat	✓	-	-	-	✓	-	-	-	✓	-	✓	-	✓	✓	-	-	✓	-	✓	✓	-	-	✓	✓	-	✓	✓	✓	✓	-	✓	✓	-	-	-	✓	✓	-	-	-	-	-	-	-	-	-	-	✓	✓	✓
Nulled	-	✓	-	-	✓	-	?	?	-	-	✓	✓	✓	✓	-	?	-	✓	✓	✓	✓	-	✓	✓	✓	✓	✓	✓	✓	-	✓	-	✓	-	-	✓	-	✓	✓	-	✓	-	?	✓	?	✓	-	✓	✓	✓
CrackingPro	-	✓	-	-	-	-	✓	✓	-	-	-	-	-	-	-	✓	-	✓	-	-	-	-	-	-	-	-	-	✓	✓	-	-	-	✓	-	-	-	-	✓	✓	-	✓	-	✓	✓	✓	✓	-	✓	-	-
CryptBB	-	-	✓	-	-	✓	-	-	-	-	-	✓	-	-	✓	-	-	-	-	✓	-	-	-	-	✓	-	✓	✓	✓	-	✓	-	-	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	✓	-	✓
Altenen	-	✓	-	-	✓	-	✓	-	-	-	✓	✓	-	✓	-	✓	-	✓	✓	✓	✓	-	✓	-	✓	-	✓	✓	✓	-	✓	-	✓	-	-	✓	-	✓	✓	-	✓	-	✓	✓	-	✓	-	✓	✓	✓
Rutor	-	✓	-	-	✓	-	✓	-	✓	-	✓	-	✓	✓	-	✓	-	✓	✓	✓	✓	✓	-	-	-	✓	✓	✓	-	✓	✓	-	✓	-	-	✓	-	✓	-	-	✓	-	✓	✓	-	-	-	✓	✓	✓
Cebulka	✓	-	-	-	✓	✓	✓	-	-	-	✓	-	✓	✓	✓	✓	✓	✓	-	✓	✓	-	✓	✓	-	✓	✓	✓	✓	-	✓	✓	-	-	-	✓	✓	✓	-	-	-	-	✓	✓	-	-	-	-	-	✓
DarknetCity	-	-	-	✓	✓	?	?	?	?	-	?	?	?	✓	?	?	?	-	?	✓	✓	-	?	?	?	?	✓	✓	✓	-	✓	-	-	-	✓	✓	?	-	?	?	-	✓	?	-	?	?	-	?	?	✓
Reverse	-	-	-	-	-	-	-	-	-	-	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	✓	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
BHF	-	-	-	-	✓	-	✓	✓	✓	-	✓	✓	-	✓	-	✓	-	✓	✓	✓	✓	-	-	-	✓	-	✓	✓	✓	-	-	-	-	-	-	✓	-	✓	✓	-	-	-	✓	✓	✓	✓	-	✓	✓	✓
Cracked	-	✓	-	-	✓	-	-	-	-	-	✓	✓	✓	✓	-	-	-	✓	✓	✓	✓	-	✓	✓	✓	✓	✓	✓	✓	-	✓	-	✓	-	-	✓	-	✓	✓	-	✓	-	-	✓	-	✓	-	✓	✓	✓
Successful markets	**46.15%**								33.33%					53.06%							47.89%									**61.11%**		37.31%									58.70%								76.47%	
Unsuccessful markets	30.77%								**52.08%**					46.67%							50.00%									**35.71%**		23.16%									46.05%								65.38%	

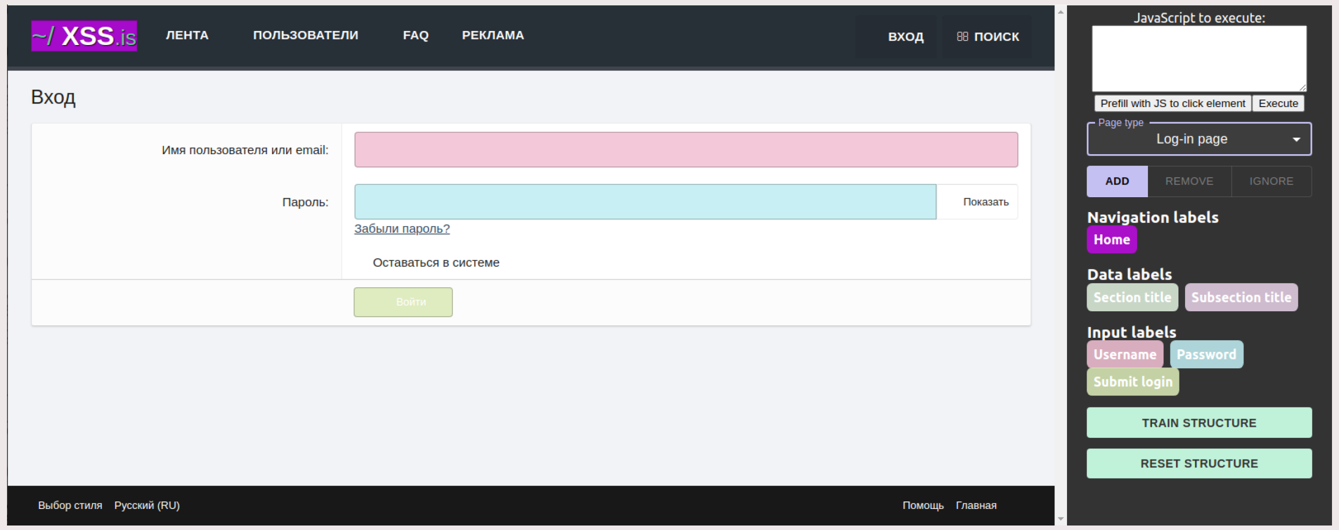
A stealth, trainable & extensible tool to extract data from cybercriminal markets: THREAT/crawl

Human-like behavior + browser

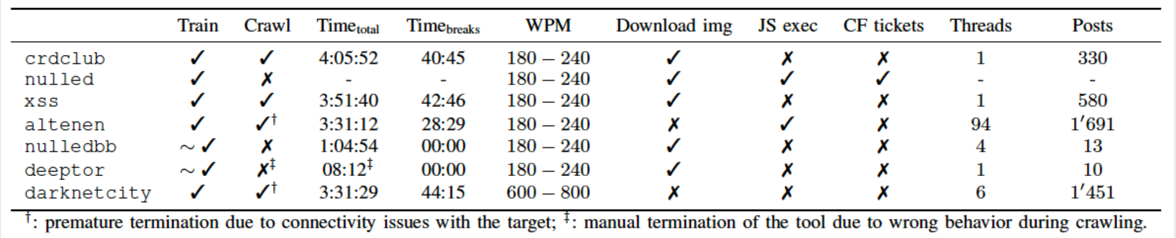
Promising stealth results via experiments against humans



Simple interface + learning + extensible



Encouraging results on learning, covering edge cases



	Train	Crawl	$\text{Time}_{\text{total}}$	$\text{Time}_{\text{breaks}}$	WPM	Download img	JS exec	CF tickets	Threads	Posts
crdclub	✓	✓	4:05:52	40:45	180 – 240	✓	✗	✗	1	330
nulled	✓	✗	-	-	180 – 240	✓	✓	✓	-	-
xss	✓	✓	3:51:40	42:46	180 – 240	✓	✗	✗	1	580
altenen	✓	✓[†]	3:31:12	28:29	180 – 240	✗	✓	✗	94	1′691
nulledbb	∼✓	✗	1:04:54	00:00	180 – 240	✓	✗	✗	4	13
deeptor	∼✓	✗[‡]	08:12[‡]	00:00	180 – 240	✓	✗	✗	1	10
darknetcity	✓	✓[†]	3:31:29	44:15	600 – 800	✗	✗	✗	6	1′451

[†]: premature termination due to connectivity issues with the target; [‡]: manual termination of the tool due to wrong behavior during crawling.

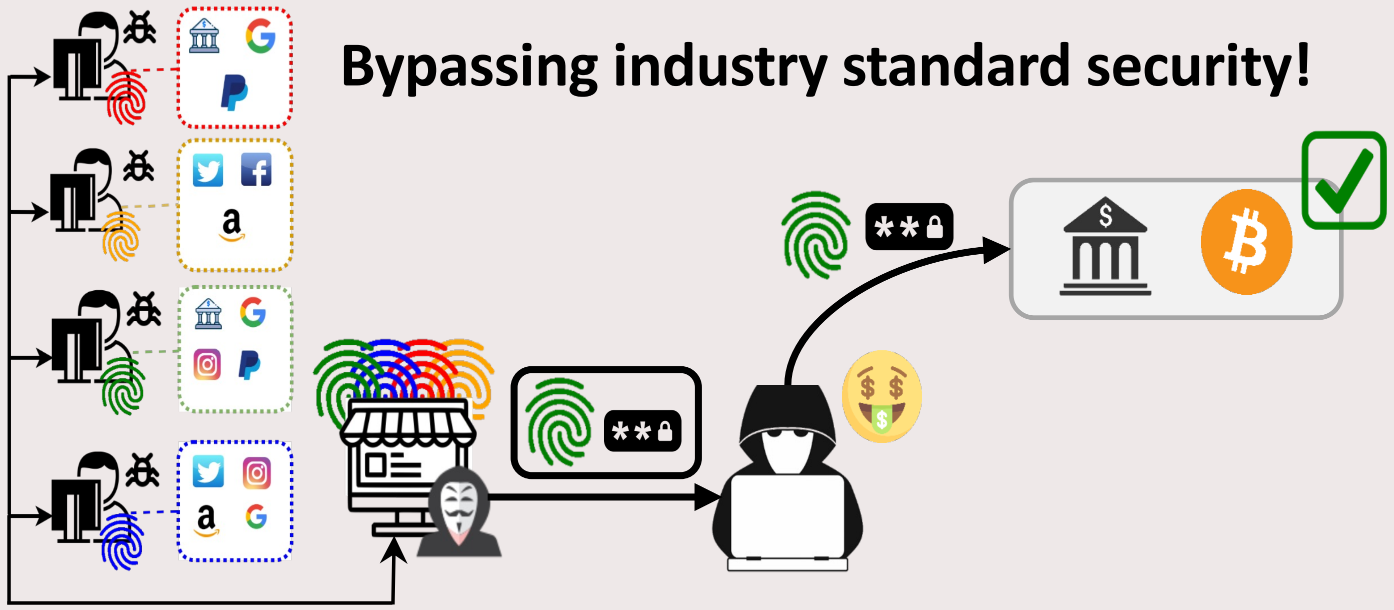
Prototype released

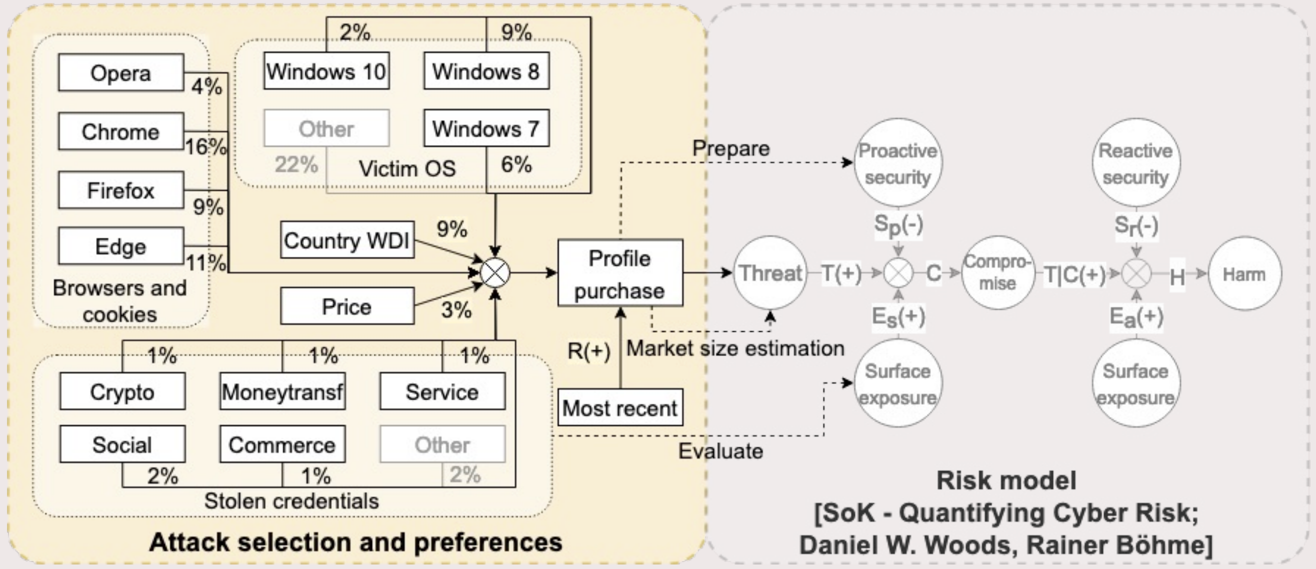
Method for stealth crawling overall valid

Studying attackers from global emergent threat:

The case of Genesis Market

Bypassing industry standard security!

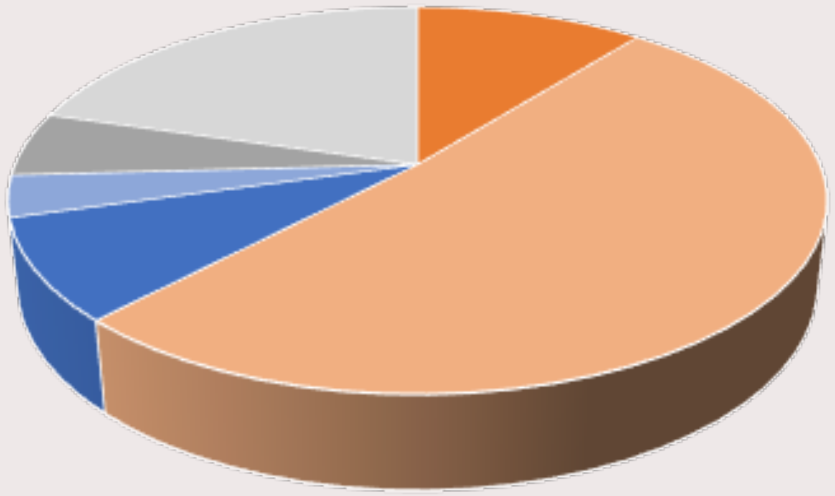




Attack selection and preferences

Risk model [SoK - Quantifying Cyber Risk; Daniel W. Woods, Rainer Böhme]

Attacker preferences to model cyber risk

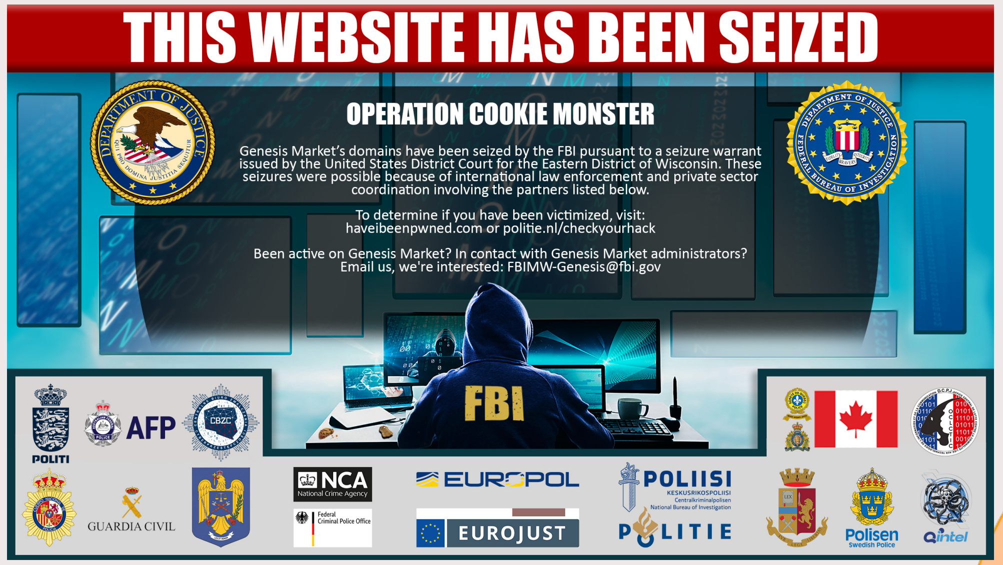


EU supply: 62% (!)
- 🟧 Sold EU: 17%
- 🟧 Unsold EU: 83%

NA supply: 12%
- 🟦 **Sold NA: 71% (!)**
- 🟦 Unsold NA: 29%

Other supply: 26%

Our estimate: 1.2–1.6M$ revenue per year ✓



THIS WEBSITE HAS BEEN SEIZED

OPERATION COOKIE MONSTER

Genesis Market's domains have been seized by the FBI pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Wisconsin. These seizures were possible because of international law enforcement and private sector coordination involving the partners listed below.

To determine if you have been victimized, visit:
haveibeenpwned.com or politie.nl/checkyourhack

Been active on Genesis Market? In contact with Genesis Market administrators?
Email us, we're interested: FBIMW-Genesis@fbi.gov

17 countries involved, 119 arrests worldwide
8M$ in revenues over ~5 years of activity

“Good” markets for a thriving economy

“Latest iPhone, 85% off, buy now!”
verylegitmarketplace.com

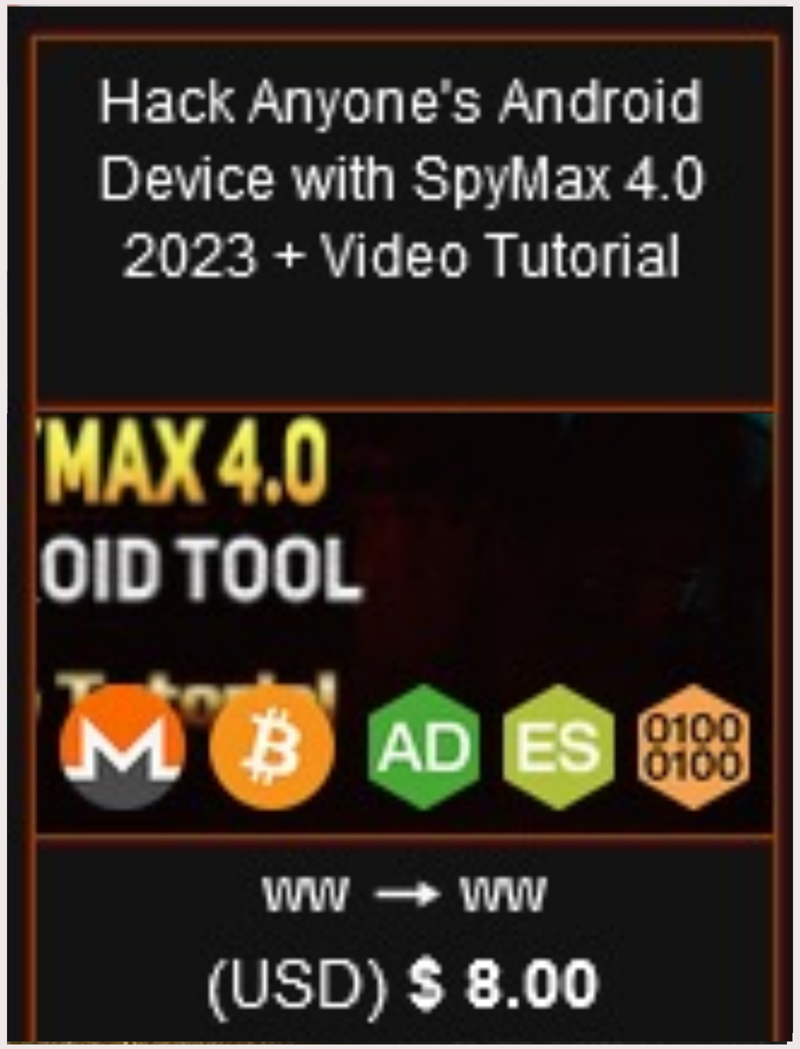
No refunds, seller unreachable

“Apple iPhone 15 256GB - Black”
bol.com

Seller rated 9.5/10, verifiable seller history, refunds possible, customer service

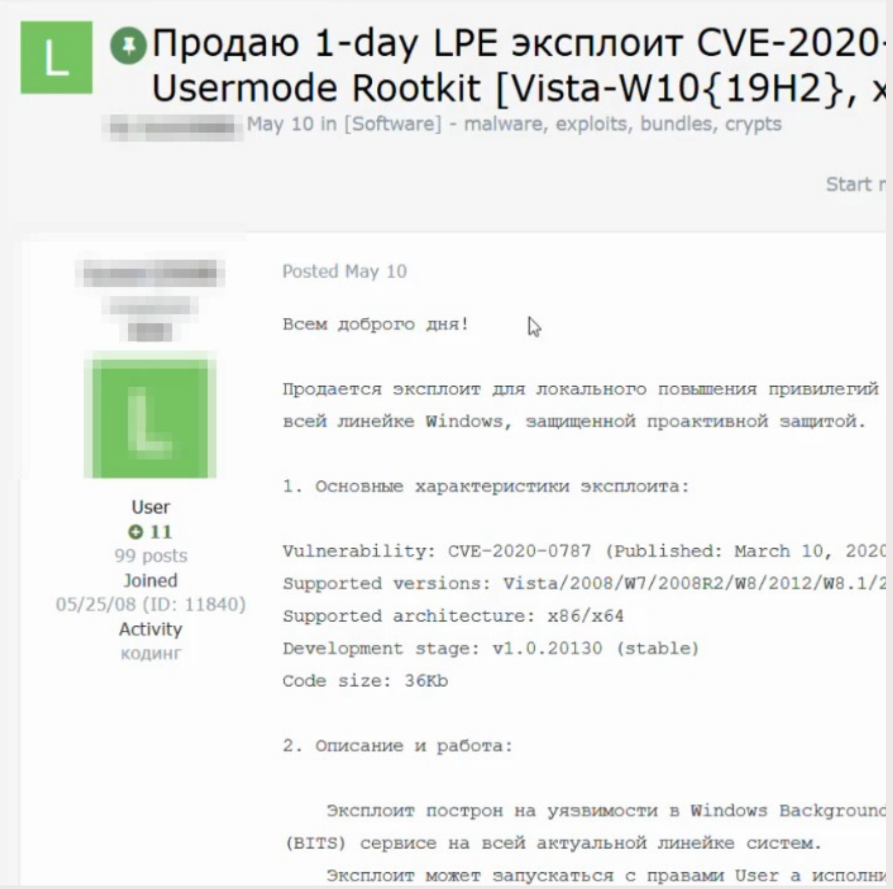
“Good” markets for a thriving economy

“Hack Anyone’s Device, 8$!”
anotherverylegitmarketplace.com


Hack Anyone's Android Device with SpyMax 4.0 2023 + Video Tutorial
MAX 4.0
OID TOOL
Tutorial
M
B
AD
ES
0100 0100
WW → WW
(USD) $ 8.00

No refunds, seller unreachable

1-day LPE exploit WIN10
exploit.in



Продаю 1-day LPE эксплоит CVE-2020-
Usermode Rootkit [Vista-W10{19H2}, x

[redacted] May 10 in [Software] - malware, exploits, bundles, crypts

Start r

[redacted]

User
11
99 posts
Joined
05/25/08 (ID: 11840)
Activity
кодинг

Posted May 10

Всем доброго дня!

Продается эксплоит для локального повышения привилегий
всей линейке Windows, защищенной проактивной защитой.

1. Основные характеристики эксплоита:

Vulnerability: CVE-2020-0787 (Published: March 10, 2020
Supported versions: Vista/2008/W7/2008R2/W8/2012/W8.1/2
Supported architecture: x86/x64
Development stage: v1.0.20130 (stable)
Code size: 36Kb

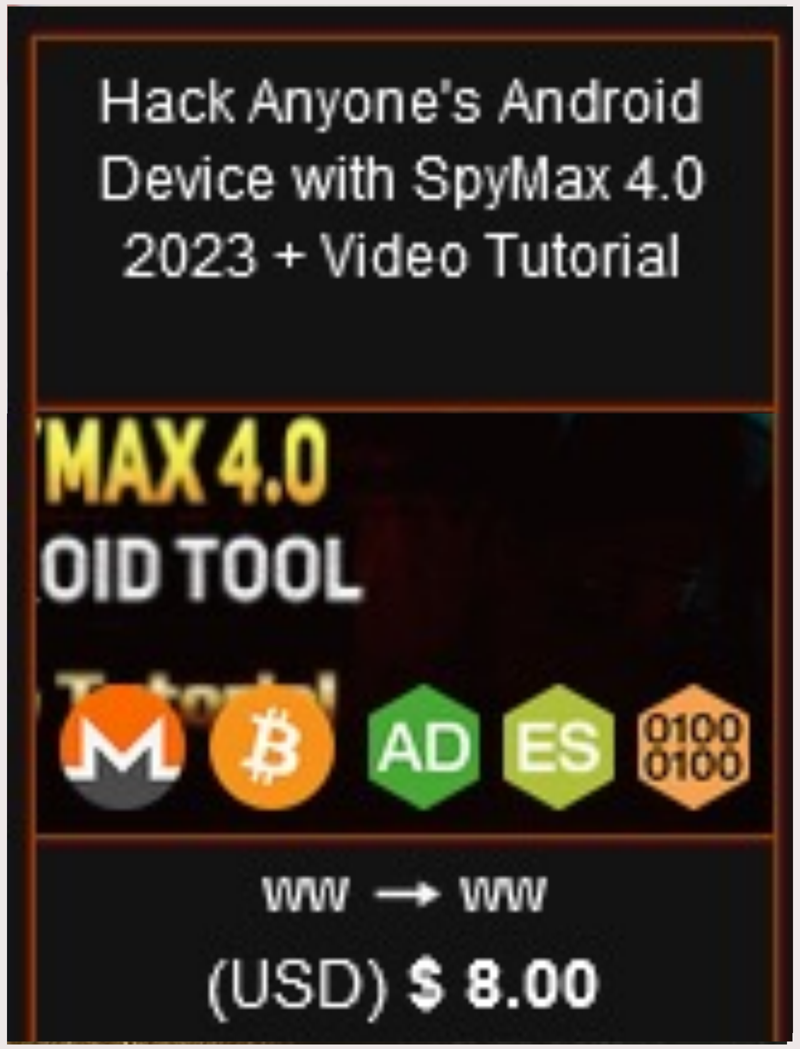
2. Описание и работа:

Эксплоит построн на уязвимости в Windows Background
(BITS) сервисе на всей актуальной линейке систем.
Эксплоит может запускаться с правами User а исполни

Seller rated 9.5/10, verifiable seller history, refunds possible, customer service

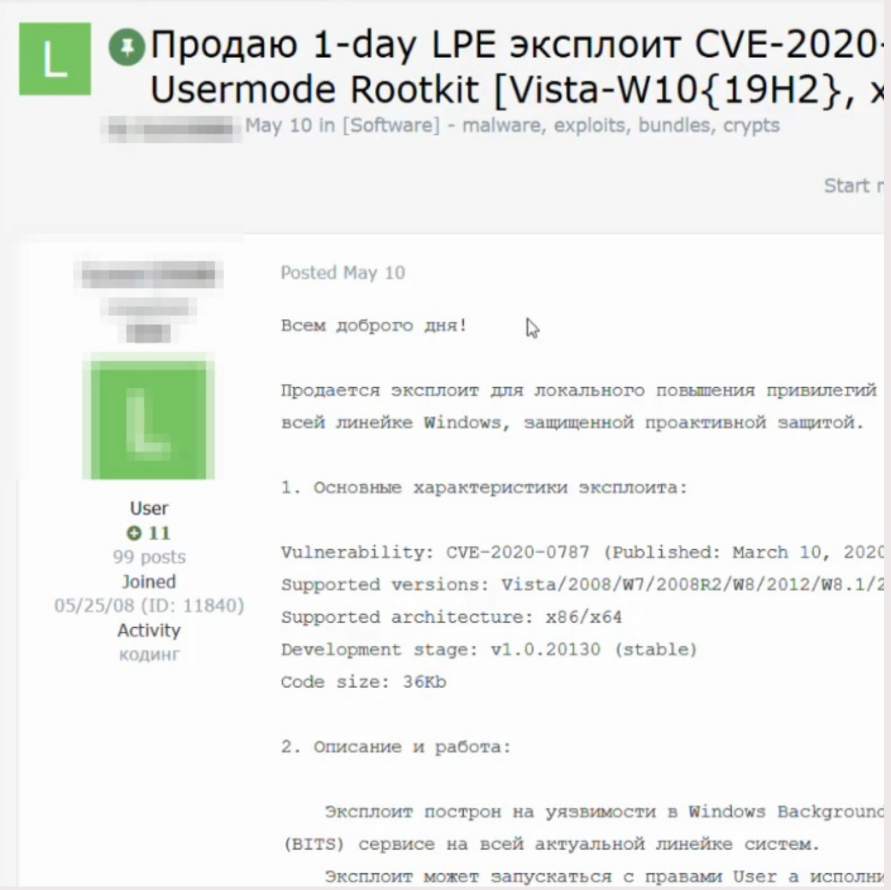
“Good” markets for a thriving economy

“Hack Anyone’s Device, 8$!”
anotherverylegitmarketplace.com



No refunds, seller unreachable

1-day LPE exploit WIN10
exploit.in



L Продаю 1-day LPE эксплоит CVE-2020-
Usermode Rootkit [Vista-W10{19H2}, x

[redacted] May 10 in [Software] - malware, exploits, bundles, crypts

Start r

[redacted]

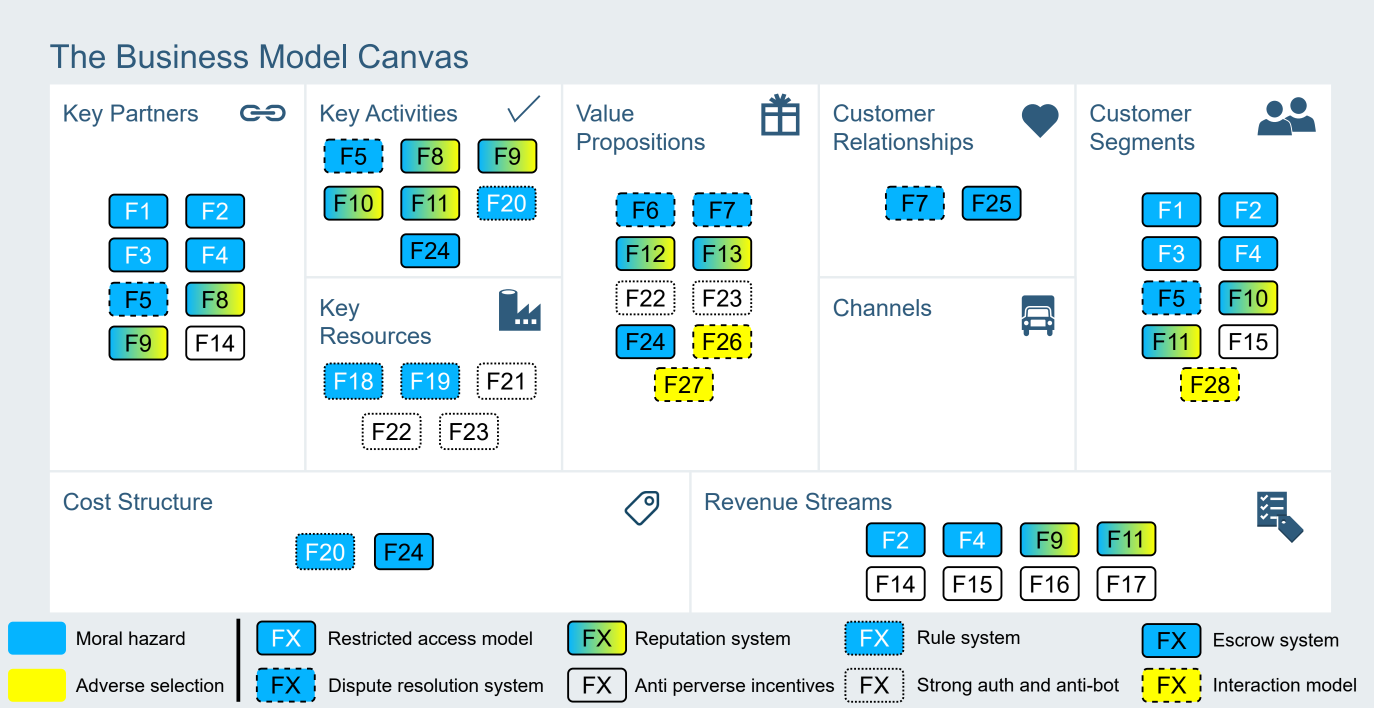
User
11
99 posts
Joined
05/25/08 (ID: 11840)
Activity
кодинг

Posted May 10

```
Всем доброго дня!

Продается эксплоит для локального повышения привилегий
всей линейке Windows, защищенной проактивной защитой.

1. Основные характеристики эксплоита:

Vulnerability: CVE-2020-0787 (Published: March 10, 2020
Supported versions: Vista/2008/W7/2008R2/W8/2012/W8.1/2
Supported architecture: x86/x64
Development stage: v1.0.20130 (stable)
Code size: 36Kb

2. Описание и работа:

    Эксплоит построн на уязвимости в Windows Backgrounc
(BITS) сервисе на всей актуальной линейке систем.
    Эксплоит может запускаться с правами User а исполни
```

Seller rated 9.5/10, verifiable seller history, refunds possible, customer service

Market features mitigating trade problems



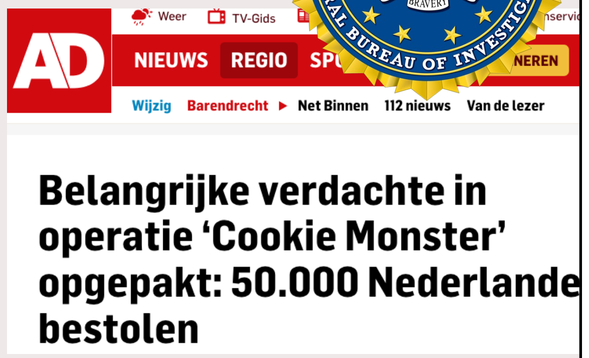
"Good" markets are more segregated, have stricter seller verification, admins are not involved in trade

A tool to identify the most damaging markets

Overview of contributions

Part I:

Method for stealth data extraction
Open-source tool available



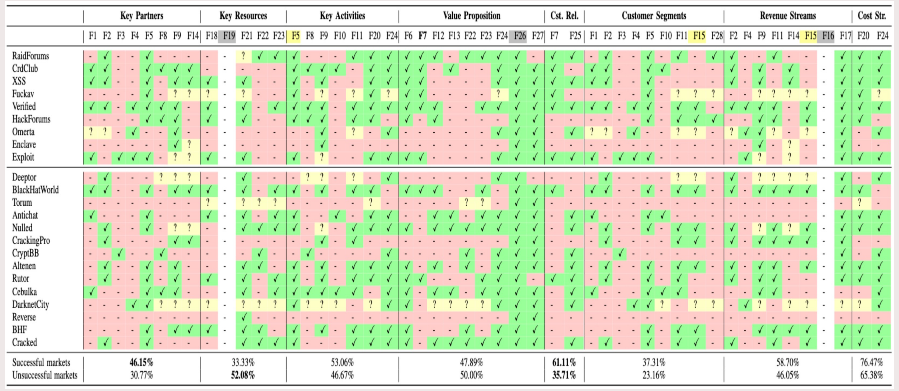
Belangrijke verdachte in operatie 'Cookie Monster' opgepakt: 50.000 Nederlande bestolen

Part II:

Characterization of novel IMPaaS threat model
Analysis of targets across the globe
Findings instrumetal to Genesis Market takedown

Part III:

Identification of "successful" markets



	Key Partners								Key Resources					Key Activities							Value Proposition									Cst. Rel.		Customer Segments									Revenue Streams								Cost Str.	
	F1	F2	F3	F4	F5	F8	F9	F14	F18	F19	F21	F22	F23	F5	F8	F9	F10	F11	F20	F24	F6	**F7**	F12	F13	F22	F23	F24	F26	F27	F7	F25	F1	F2	F3	F4	F5	F10	F11	F15	F28	F2	F4	F9	F11	F14	F15	F16	F17	F20	F24
RaidForums	-	✓	-	-	✓	-	-	-	-	-	?	✓	✓	✓	-	-	-	✓	✓	✓	✓	✓	✓	-	✓	✓	✓	✓	-	✓	✓	-	✓	-	-	✓	-	✓	-	✓	✓	-	-	✓	-	-	-	✓	✓	✓
CrdClub	✓	✓	-	-	✓	✓	✓	✓	-	-	-	-	-	✓	✓	✓	✓	-	✓	✓	✓	✓	-	✓	-	-	✓	✓	✓	✓	-	✓	✓	-	-	✓	✓	-	-	-	✓	-	✓	-	✓	-	-	✓	✓	✓
XSS	✓	✓	-	-	✓	-	✓	✓	✓	-	✓	-	-	✓	-	✓	-	-	✓	✓	✓	✓	-	-	-	-	✓	✓	✓	✓	✓	✓	✓	-	-	✓	-	-	-	-	✓	-	✓	-	✓	-	-	✓	✓	✓
Fuckav	-	-	-	-	✓	-	?	?	?	-	?	-	-	✓	-	?	-	?	✓	?	✓	✓	-	-	-	-	?	✓	✓	✓	-	-	-	-	-	✓	-	?	?	?	-	-	?	?	?	?	-	✓	✓	?
Verified	✓	✓	-	✓	✓	✓	✓	-	✓	-	✓	-	✓	✓	✓	✓	-	✓	✓	✓	✓	✓	✓	-	-	✓	✓	✓	✓	✓	✓	✓	✓	-	✓	✓	-	✓	✓	-	✓	✓	✓	✓	-	✓	-	✓	✓	✓
HackForums	-	-	-	-	✓	✓	✓	-	✓	-	✓	-	-	✓	✓	✓	-	✓	✓	-	✓	-	✓	-	-	-	-	✓	✓	-	-	-	-	-	-	✓	-	✓	✓	✓	-	-	✓	✓	-	✓	-	✓	✓	-
Omerta	?	?	-	✓	-	-	✓	-	-	-	-	-	-	-	-	✓	-	?	-	✓	-	-	-	-	-	-	✓	✓	✓	-	✓	?	?	-	✓	-	-	?	?	-	?	✓	✓	?	-	?	-	✓	-	✓
Enclave	-	-	-	-	-	-	✓	?	-	-	-	-	-	-	-	✓	-	-	-	-	-	-	-	-	-	-	-	✓	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	✓	-	?	-	-	✓	-	-
Exploit	✓	-	✓	✓	✓	-	?	?	✓	-	✓	-	-	✓	-	?	-	-	✓	✓	✓	✓	-	-	-	-	✓	✓	✓	✓	✓	✓	-	✓	✓	✓	-	-	-	-	-	✓	?	-	?	-	-	✓	✓	✓
Deeptor	-	✓	-	-	-	?	?	?	-	-	✓	-	-	-	?	?	-	?	-	✓	-	-	-	-	-	-	✓	✓	-	-	-	-	✓	-	-	-	-	?	?	-	✓	-	?	?	?	?	-	✓	-	✓
BlackHatWorld	✓	✓	-	-	✓	-	✓	✓	✓	-	✓	-	✓	✓	-	✓	-	✓	✓	-	✓	✓	✓	-	-	✓	-	✓	✓	✓	-	✓	✓	-	-	✓	-	✓	✓	-	✓	-	✓	✓	✓	✓	-	✓	✓	-
Torum	-	-	-	-	-	-	-	-	?	-	?	?	?	-	-	-	-	-	?	-	-	-	-	-	?	?	-	✓	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	?	-
Antichat	✓	-	-	-	✓	-	-	-	✓	-	✓	-	✓	✓	-	-	✓	-	✓	✓	-	-	✓	✓	-	✓	✓	✓	✓	-	✓	✓	-	-	-	✓	✓	-	-	-	-	-	-	-	-	-	-	✓	✓	✓
Nulled	-	✓	-	-	✓	-	?	?	-	-	✓	✓	✓	✓	-	?	-	✓	✓	✓	✓	-	✓	✓	✓	✓	✓	✓	✓	-	✓	-	✓	-	-	✓	-	✓	✓	-	✓	-	?	✓	?	✓	-	✓	✓	✓
CrackingPro	-	✓	-	-	-	-	✓	✓	-	-	-	-	-	-	-	✓	-	✓	-	-	-	-	-	-	-	-	-	✓	✓	-	-	-	✓	-	-	-	-	✓	✓	-	✓	-	✓	✓	✓	✓	-	✓	-	-
CryptBB	-	-	✓	-	-	✓	-	-	-	-	-	✓	-	-	✓	-	-	-	-	✓	-	-	-	-	✓	-	✓	✓	✓	-	✓	-	-	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	✓	-	✓
Altenen	-	✓	-	-	✓	-	✓	-	-	-	✓	✓	-	✓	-	✓	-	✓	✓	✓	✓	-	✓	-	✓	-	✓	✓	✓	-	✓	-	✓	-	-	✓	-	✓	✓	-	✓	-	✓	✓	-	✓	-	✓	✓	✓
Rutor	-	✓	-	-	✓	-	✓	-	✓	-	✓	-	✓	✓	-	✓	-	✓	✓	✓	✓	✓	-	-	-	✓	✓	✓	-	✓	✓	-	✓	-	-	✓	-	✓	-	-	✓	-	✓	✓	-	-	-	✓	✓	✓
Cebulka	✓	-	-	-	✓	✓	✓	-	-	-	✓	-	✓	✓	✓	✓	✓	✓	-	✓	✓	-	✓	✓	-	✓	✓	✓	✓	-	✓	✓	-	-	-	✓	✓	✓	-	-	-	-	✓	✓	-	-	-	-	-	✓
DarknetCity	-	-	-	✓	✓	?	?	?	?	-	?	?	?	✓	?	?	?	-	?	✓	✓	-	?	?	?	?	✓	✓	✓	-	✓	-	-	-	✓	✓	?	-	?	?	-	✓	?	-	?	?	-	?	?	✓
Reverse	-	-	-	-	-	-	-	-	-	-	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	✓	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
BHF	-	-	-	-	✓	-	✓	✓	✓	-	✓	✓	-	✓	-	✓	-	✓	✓	✓	✓	-	-	-	✓	-	✓	✓	✓	-	-	-	-	-	-	✓	-	✓	✓	-	-	-	✓	✓	✓	✓	-	✓	✓	✓
Cracked	-	✓	-	-	✓	-	-	-	-	-	✓	✓	✓	✓	-	-	-	✓	✓	✓	✓	-	✓	✓	✓	✓	✓	✓	✓	-	✓	-	✓	-	-	✓	-	✓	✓	-	✓	-	-	✓	-	✓	-	✓	✓	✓
Successful markets	**46.15%**								33.33%					53.06%							47.89%									**61.11%**		37.31%									58.70%								76.47%	
Unsuccessful markets	30.77%								**52.08%**					46.67%							50.00%									**35.71%**		23.16%									46.05%								65.38%	