Dark Deals:
unveiling the underground market of exploits

Anna Pavlovskaia

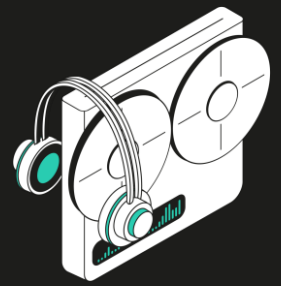
Senior Digital Footprint Intelligence Analyst

kaspersky

virus BULLETIN

- Senior Digital Footprint Intelligence Analyst, Kaspersky
- 8+ years in cybersecurity, CISSP
- OSINT enthusiast
- Dark Web researcher

- Forums
- Messengers
- Onion resources
- Private access forums



500 000+

messages daily

Compromised accounts

RDP accesses

Exploits

Malware-as-s-Service

XSS

Data leakages

Insiders

Banking cards

Targeted attacks

Malware logs

Exploits

Ransomware blogs

Date leakages

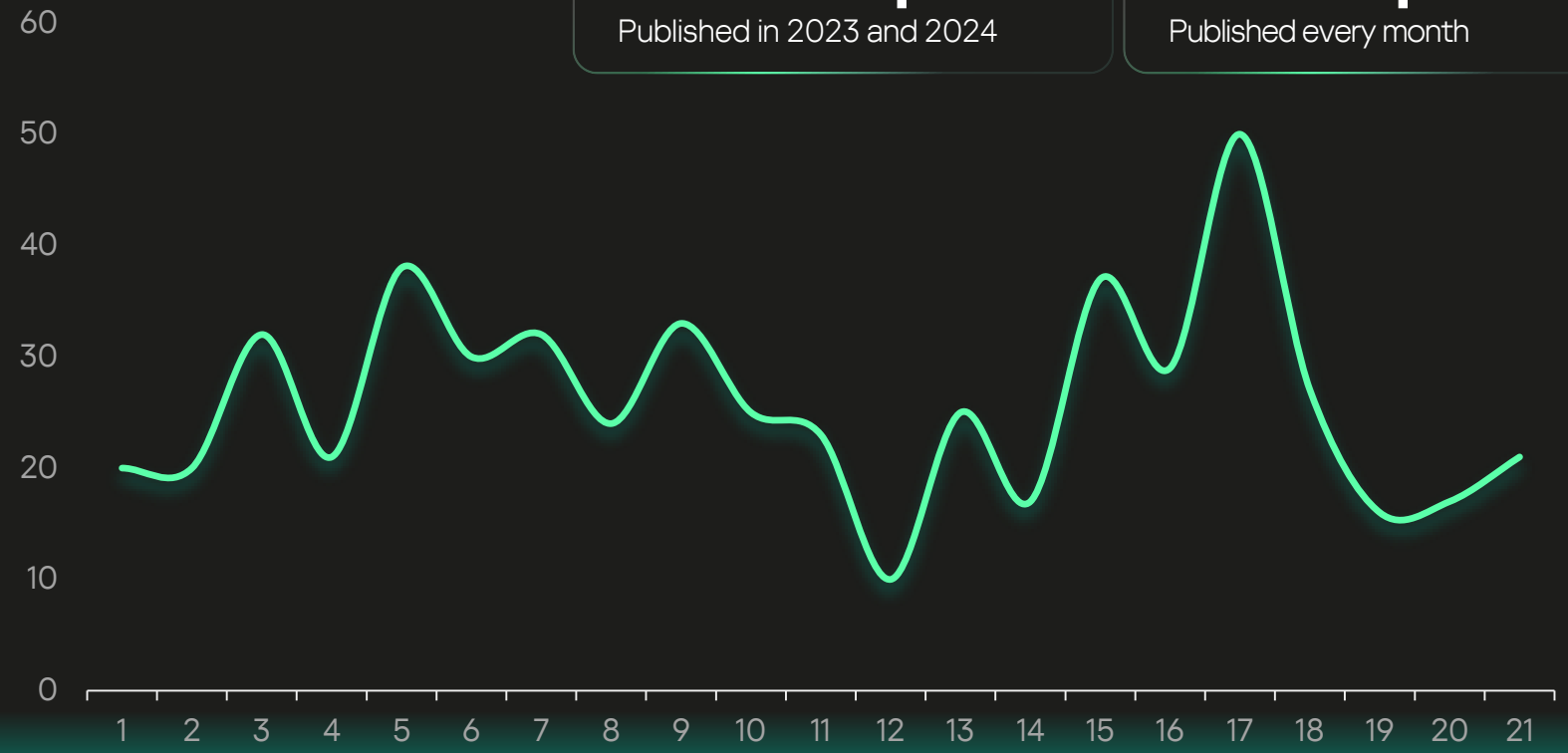
How many real exploits exist?

Does the exploit economy follow the same rules as other markets?

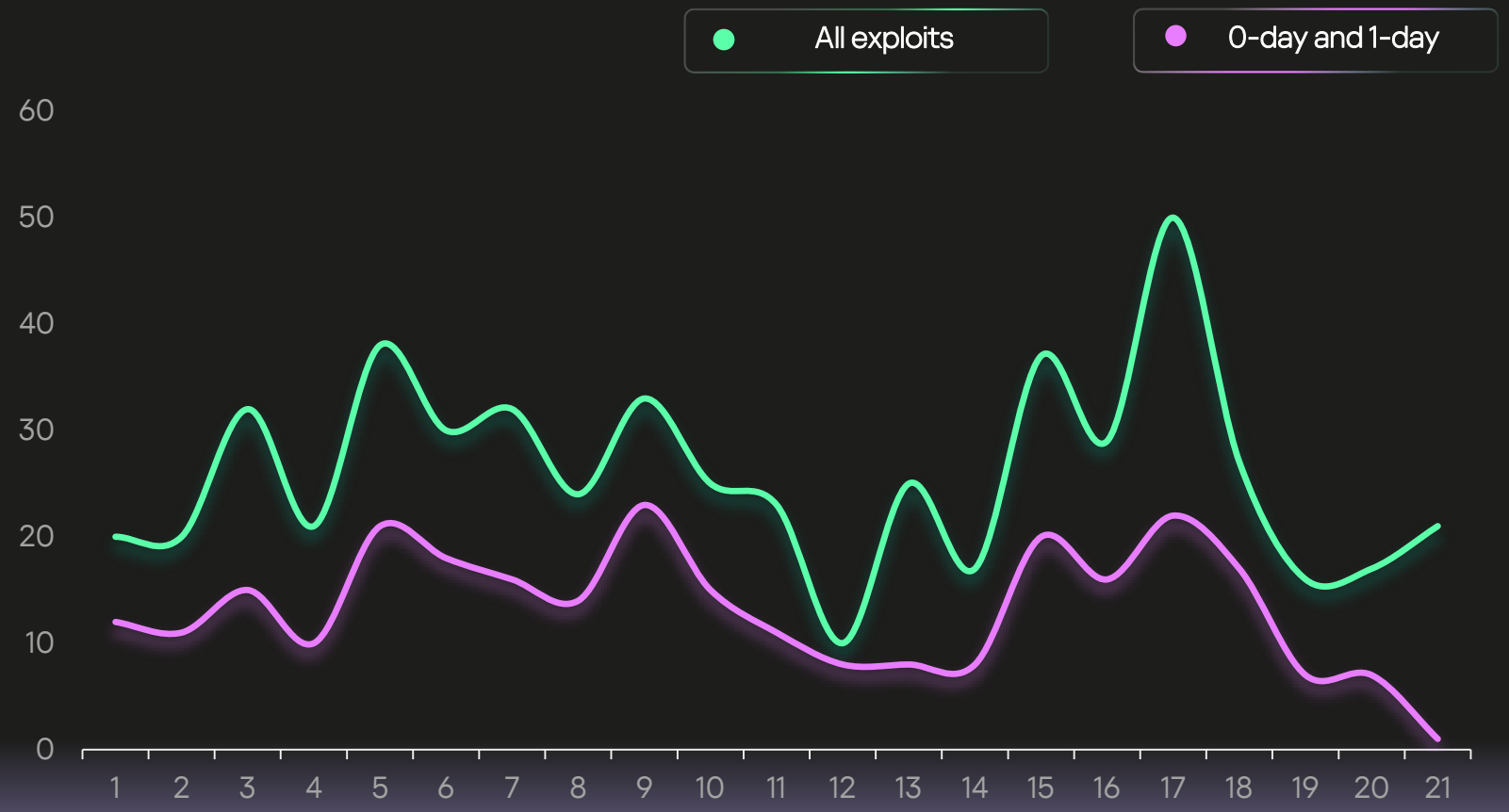
Number of exploits

~550 exploits
Published in 2023 and 2024

~26 exploits
Published every month



Number of exploits



Formation of prices

Type of exploit

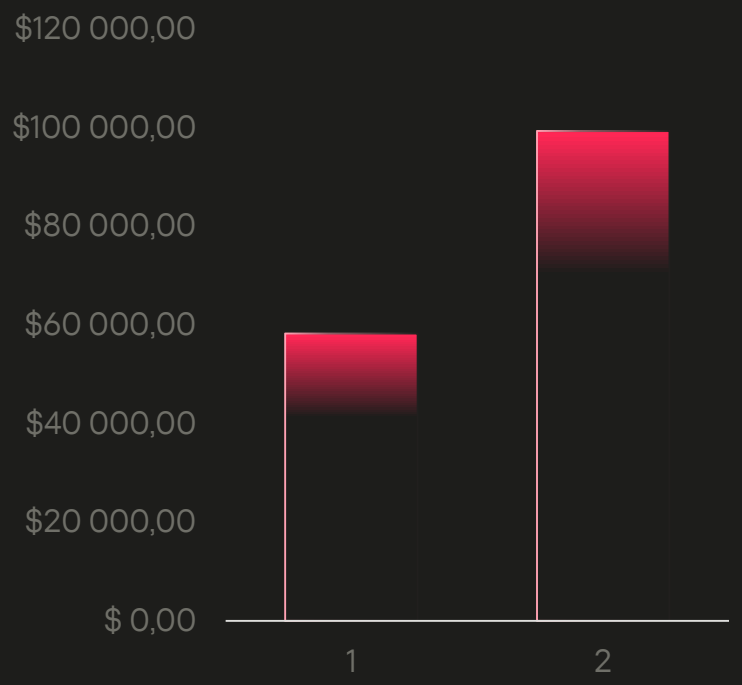
Number of sales

Criticality and Prevalence of the system

Uniqueness of the offer

Reputation of the seller

Price formation: Type of exploit



Average price for LPE exploits is around $60,000

Average price for RCE exploits is around $100,000

Price formation: Type of exploit

LPE 0-day

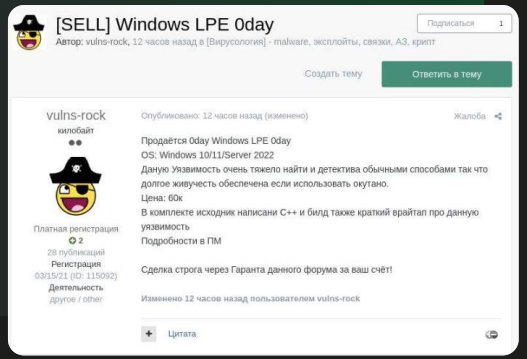
$60,000 – $250,000

For Sale 0-day Windows LPE

OS: Windows 10/11/Server 2022

This vulnerability is very hard to find and detect by normal means so long survivability is ensured if used shrouded.

Price: $60,000



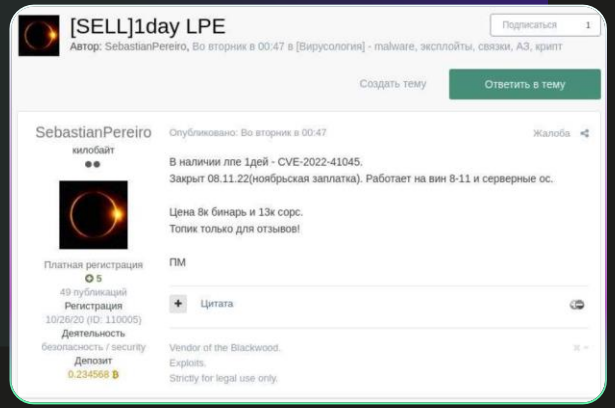
Price formation: Type of exploit

LPE 1-day

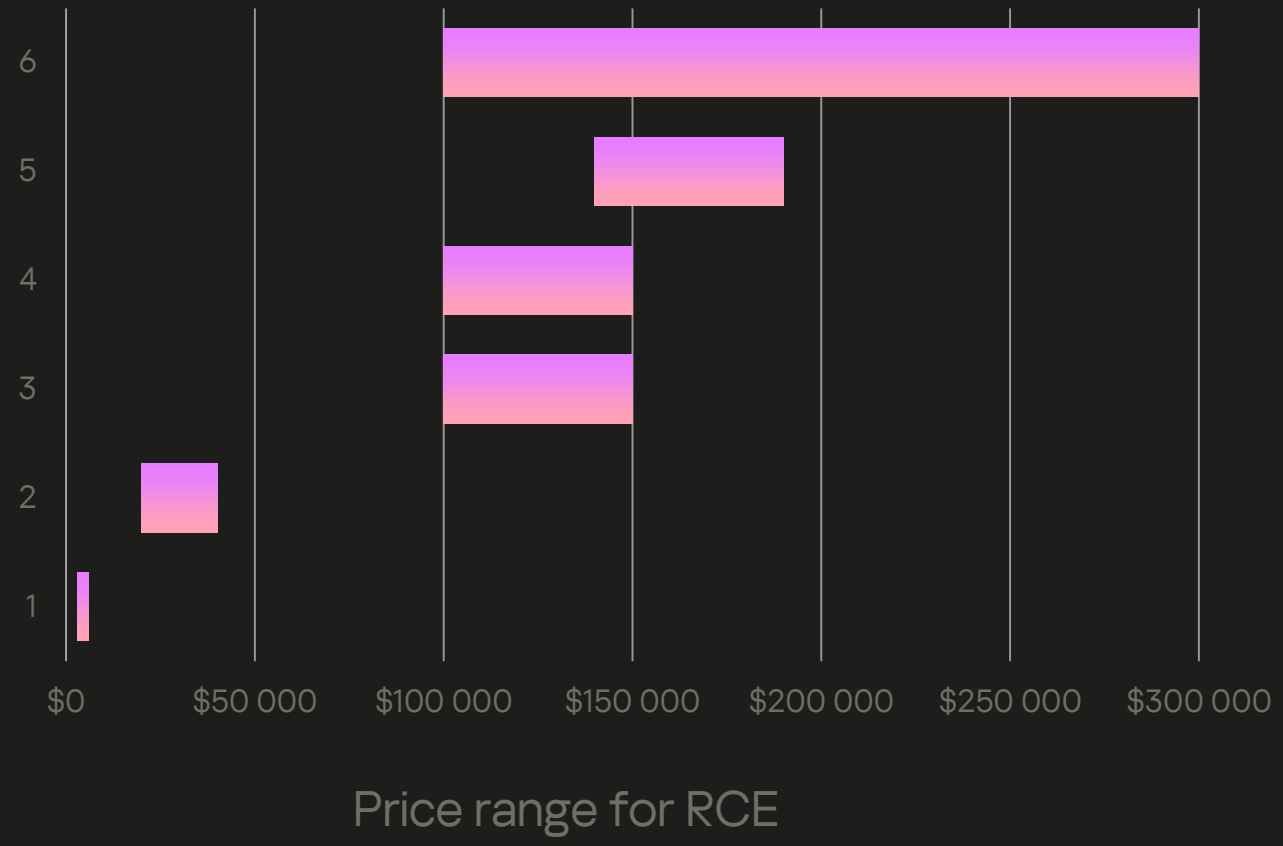
$500 to $10,000

For Sale LPE 1-day – CVE-2022-41045

Price:
$8,000 for the binary,
$13,000 for the source code



Price formation: Criticality and Prevalence of the System



Price formation: Criticality and Prevalence of the System

Outlook RCE 0day
by Cvsp - Tuesday May 14, 2024 at 05:07 AM

Cvsp

GOD User

GOD

Posts:	24
Threads:	4
Joined:	Sep 2023
Reputation:	126

Today, 05:07 AM (This post was last modified: Today, 05:54 AM by Cvsp.) #1

Outlook RCE Exploit 0-day

Tested versions x86/x64:

- Microsoft Office 2016
- Microsoft Office 2019
- Microsoft Office LTSC 2021
- Microsoft 365 Apps for Enterprise

Price: $1,700,000
Success rate: 100%
Exploit details in private

Message me on Telegram

Only dealing through escrow @[Owner] ShinyHunters

UPDATE: Don't message me without proof of funds. Stay away journalists.

Need a middleman? Try out our Escrow App!

PM Find Reply Quote Report

Price formation: Criticality and Prevalence of the System

MAGENTO 2.4.X REMOTE SHELL UPLOAD 0DAY \\ ESCROW

TOPIC
Magento 2.4.x Remote Shell Upload 0day \\ ESCROW

THREAD
Покупка/Продажа - [Вирусология] - malware, эксплойты, связки, АЗ, крипт

TOPIC URL

FORUM

USER
ring-0

байт
Платная регистрация
05 публикаций
Регистрация11/12/23 (ID: 156080)
Деятельностьдругое / other
Депозит0.000200

DATE
20231113062615

POST
ONLY working with GARANT
100 BTC
START in PM
Изменено 4 часа назад пользователем ring-0
0Оценить

Screenshot was obtained from internal Kaspersky monitoring system

Price formation: Number of sales

Most common case:
Sell to one buyer

WINDOWS TCP/IP RCE 0DAY

TOPIC
Windows TCP/IP RCE 0day

THREAD
Market - Others staff

TOPIC URL

FORUM

USER
anongod

7 Апр 2023

DATE
20240816151854

POST
I sell to one hand
Contact :

Sell several copies

[SELL]1DAY MAGENTO 2 RCE

TOPIC
[SELL]1day Magento 2 RCE

THREAD
Покупка/Продажа - [Вирусология] - malware, эксплойты, связки, АЗ, крипт

TOPIC URL

FORUM

USER
TylerDurden

мегабайт
Платная регистрация
14
85 публикаций
Регистрация03/29/22 (ID: 127978)
Деятельностьхакинг / hacking

DATE
20240925040156

POST
I am selling Magento 2 CVE-2024-34102 RCE
-Private implementation the process is automated you just have to input URL it auto exploits.
-It gets SSH shell
Price: 20k$
Only Selling 5 copies.
Garant Welcome
Contacts in PM

Screenshot was obtained from internal Kaspersky monitoring system

Who is buying?

- APTs
- Ransomware groups
- Experienced solo hackers
- Sponsored hacktivists

BUYING 0DAY. 100000$

TOPIC
Buying 0day. 100000$

THREAD
Покупка/Продажа - [Вирусология] - malware, эксплойты, связки, АЗ, крипт

TOPIC URL

FORUM

USER
h0stages

байт
Деактивирован
1
11 публикаций
Регистрация30.10.2020 (ID: 110151)
Деятельностьбезопасность / security

DATE
20201029221548

POST
Hello.
I'm currently looking to buy a 0day exploit for [Github, Gitlab, Twitter, Snapchat, Cisco VPN, Pulse VPN, etc] Basically any large site/software.
My budget is $100000 in BTC.
Person who directs me to someone will get $10000 BTC.
Reply to thread if you know anyone or anywhere selling this stuff.

Who is buying?

Any private or 1day/0day exploits for Fortinet, Cisco. Buy with escrow and have good budget

[BUY] 0DAY/1DAY RCE EXPLOITS

TOPIC	THREAD
[BUY] 0dAy/1dAy RCE Exploits	Market - Malware
TOPIC URL	**FORUM**

USER	DATE
1day	20240818005828
1 Апр 2024	**POST**

Any private or 1day/0day exploits for fortinet,fortiOS, fortiSSL, cisco. Buy with escrow and have good budget.
Also have 1btc deposit on xss.

Experienced team is looking for access broker.
VPNs of all types, Citrix, RDP, etc

ПАРТНЕРСТВО. ИЩЕМ ПОСТАВЩИКА КОРП ДОСТУПОВ. 1 БТК ДЕПОЗИТ

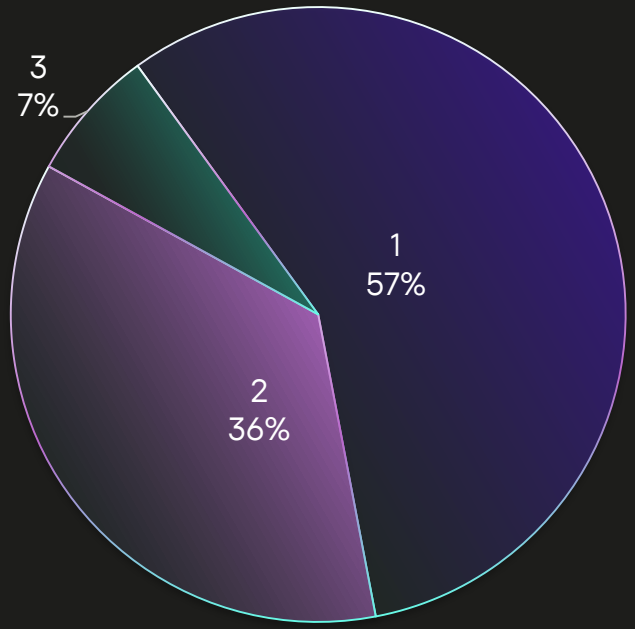
TOPIC	THREAD
Партнерство. Ищем поставщика Корп Доступов. 1 бтк депозит	Market - Access (SSH/RDP/VNC/Shell)
TOPIC URL	**FORUM**

USER	DATE
1day	20240703093453
1 Апр 2024	**POST**

Опытная команда пентестеров в теме более 4ти лет!! До этого работали в привате! Свои инструменты включая 0Day и 1Day!
Ищет поставщика Корпоративных Доступов
VPN'ы всех видов, Citrix, RDP Corp, HVNC, Shells, Боты, и тп

Screenshot was obtained from internal Kaspersky monitoring system

Statistics on sellers by numbers of offers



Who is selling? Persistent seller

User with 5+ offers in 2024:

- $200,000
- $30,000
- $150,000
- $60,000
- $100,000

The potential revenue

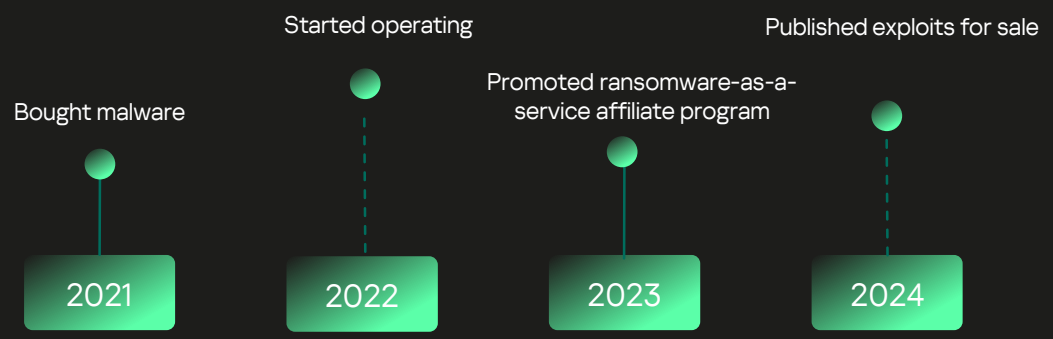
$540,000

Mallox ransomware

> 1000 victims*
Ransom from $ 1,000 to $60,000
10% from affiliate program

Initial access

Internet-facing MS SQL or PostgreSQL servers
RCE vulnerabilities, such as CVE-2019-1068 or CVE-2020-0618



*According to the interview Suspectfile.com

https://securelist.com/mallox-ransomware/113529/

Who is selling? Mallox

Sell RCE MS Office 0-day. Only with escrow service!

The price is $100,000
Possibly to sell only in one buyer depending on the price.
Possibly partial payment + % from the exploitation
Only in private messages

!

[ПРОДАЖА/SELL] RCE MS OFFICE ZERO DAY

TOPIC
[Продажа/Sell] RCE MS office zero day

THREAD
Market - Malware

TOPIC URL

FORUM

USER
Mallx

12 Ноя 2022

DATE
20240704154918

POST
[Продам] RCE MS office 0 дей
- Выполняется команда cmd/powershell
- Выполнение файлов exe, java, ps1, dll, другое... [ваши файлы должны быть чистыми, их можно и подписывать сертификатами в зависимости от файла, среднее выполнение пайлоада от 15 секунд до 1 минуты, все будет зависить от файла и его размера]
- Генератор уникальных хешей в документе [обеспечит долгую жизнь эксплоиту]
- Комплект: исходники, сборщик, описание уязвимости, мануал по установке и настройке этого "добра"
- Протестировано и работает на windows 7, 8, 10, 11.
- Уязвимые версии office: -> 2010 -> 2013 -> 2016 -> 2019 -> Office 365
- Скан AB: 0/26

Who is selling? Mallox

Is for sale! The last price in $75,000.
Only escrow services.
Have been waiting for the buyer for one month and no result

[ПРОДАЖА/SELL] RCE MS OFFICE ZERO DAY

TOPIC
[Продажа/Sell] RCE MS office zero day

THREAD
Market - Malware

TOPIC URL

FORUM

USER
Mallx

DATE
20240704154918

12 Ноя 2022

POST
Актуально, ждал покупателя 1 месяц, но в итоге человек на связь не вышел.
Продам! последняя цена 75.000 $ только гарант!

Who is selling? The seller of the most expensive exploit

Exploit is not mine, it is found by my partner I am just the face on the forum

PL+DE+USA SHOPS PACK

TOPIC
PL+DE+USA Shops Pack

THREAD
Аукционы

TOPIC URL

FORUM

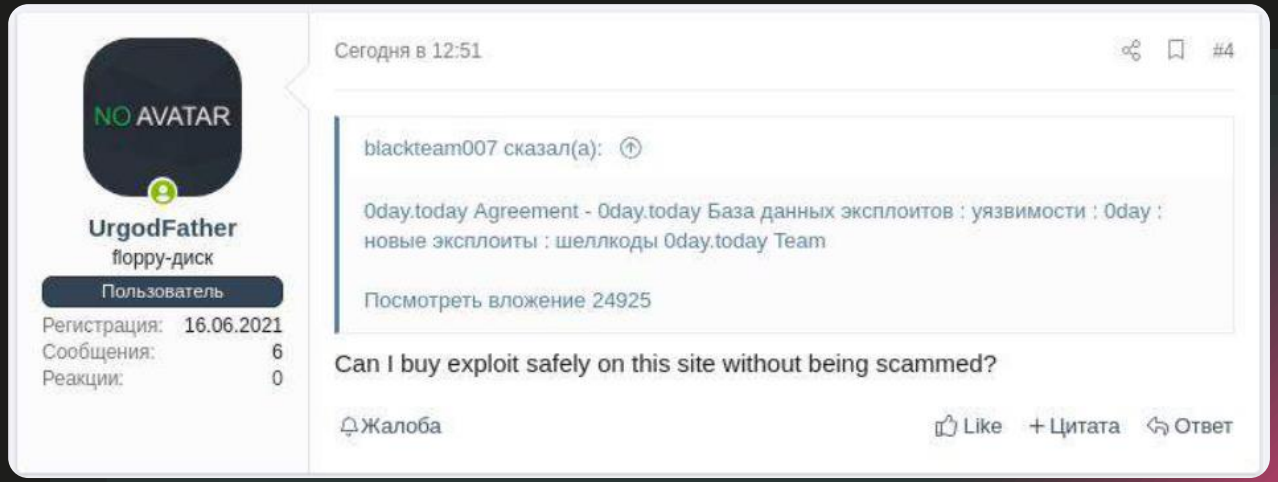
USER
ring-0

байт
Платная регистрация
2
13 публикаций
Регистрация11/12/23 (ID: 156080)
Деятельностьдругое / other
Депозит0.000200

DATE
20231230072023

POST
1 minute ago, God4father said:
You bid for shops, and you own 0day magento, and also you don't have money!
Weird....
Exploit is not mine, it is found by my partner i am just the face on the forum looking for people who have the sniffer to work with. Also, is it possible that not everyone is born with money in their pocket? I am trying to sell CC's 4000 on the forum if i sold there would be, but like this i need to transfer money from exchange

How to avoid scam?



Scam project earned more than $6,000,000

0DAY.TODAY

TOPIC	THREAD
0day.today	Offtopic. Случаи из жизни. Трёп
TOPIC URL	**FORUM**

USER	DATE
Shtang	20231016183500
Member Join Date: Sep 2023 Posts: 56 Balance: 0.00$	**POST** Originally Posted by mak Давно известно же - 0day.today RIPPER Я видел и на сайте не кидальном exploit-db что они рекламируются там через сплойты, прям в сплойтах написн

09.11.2018 16.2.2023

84,87967109 биткоинов равно $5772590,04 заработано за всё время, правда не забываем что раньше биток стоил меньше да и курс бакса тоже иной был

Regulation of deals

Deposit system

Escrow services

Arbitration

Deposit system – used to secure deals and provide proof of solvency

You will not find a real seller until you add at least 5 btc

BUYING 0DAY. 100000$

TOPIC
Buying 0day. 100000$

THREAD
Покупка/Продажа - [Вирусология] - malware, эксплойты, связки, АЗ, крипт

TOPIC URL

FORUM

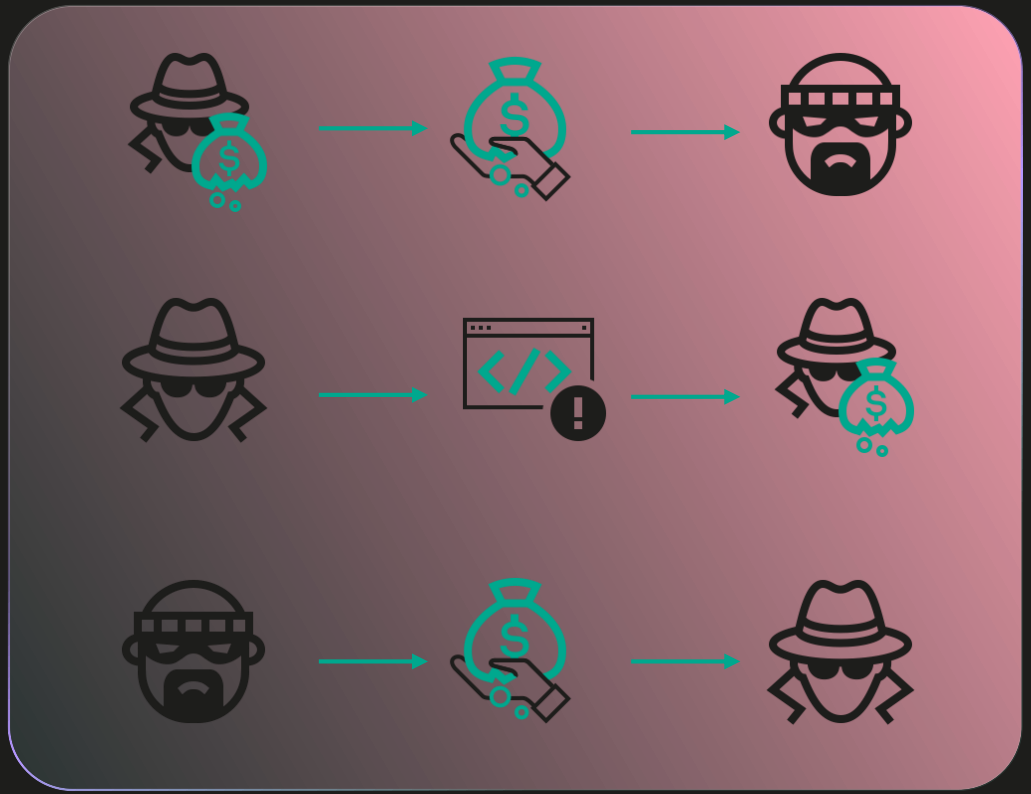
USER
ULT

байт
Платная регистрация
2
22 публикации
Регистрация19.05.2020 (ID: 104341)
Деятельностьдругое / other

DATE
20201031232649

POST
Цитата
incase i dont find seller
it works the other way around here. you will not find real seller until you add at least 5btc. a real seller 0day does not see you as a serious buyer and he is not interested in you. you can even offer 2 million and it won't change anything. btw deposit can be withdrawn at any minute.
0Оценить
Цитата

Escrow service



https://securelist.com/dark-web-deals-and-regulations/109034/

Arbitration

I am exploit seller, not a hacker. I do not penetrate networks and will not help to hack someone if buyer is not qualified enough

oxygen
Арбитр

Модератор
355
10620 публикаций
Регистрация

Опубликовано: 18 ноября 2020

Комментарий от модератора:
Вопрос по данному разбирательству решен.
Тема закрыта.

Conclusion

Every deal is a big risk for the both sides

KRENDEL - SCAM ON FORTINET RCE - RIPPER 750$

TOPIC
Krendel - Scam on Fortinet RCE - Ripper 750$

THREAD
Arbitrage - Abuse \ Rippers

TOPIC URL

FORUM

USER
Banderas
Banderas
Pwnstar
Krendel
Nowheretogo

DATE
20231122140915

POST
Hola damas y caballeros
Deal with caution with Krendel!!!!!! He did not deliver RCE & have multiple selling posts. We don't need this in Ramp. See chat screenshots below.

No test-drive – you buy “a pig in a poke”

The high possibility of scam hinders deals

Every 0-day published for sale on Darkweb resources publicly is LOUD

Such attention is undesirable for both the seller and the buyer

Exploit market is drastically smaller compared to eager buyers

0-day is like “strategic raw material”

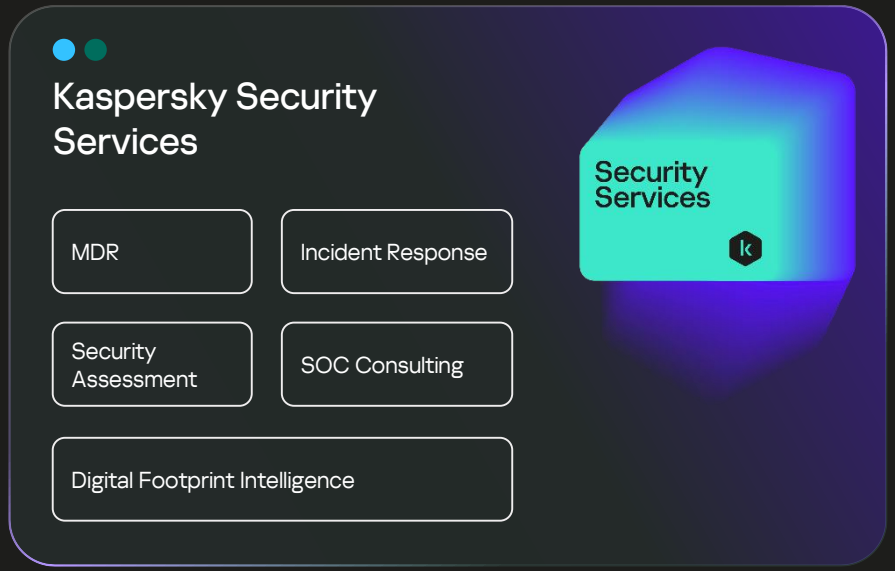
БРОКЕРЫ ЭКСПЛОЙТОВ

TOPIC Брокеры эксплойтов	**THREAD** Underground - Уязвимости в ПО / Эксплойтинг
TOPIC URL	**FORUM**

USER ShadowMan	**DATE** 20240819122641
Регистрация 30.09.2020 Сообщения	**POST** Нереально, если ты не арабский шейх, да и то.. 0-дэй это как стратегическое сырье, абы кому не продают

Screenshot was obtained from internal Kaspersky monitoring system

Thank you!



kaspersky