2EASY Marketplace

Presenter: Bujitha Ponsuge

Table of Content

- Summary
- What is an Dark Net Market
- What is 2EASY
- How Does it work
- Who is effected
- Why This is a Critical Issue
- Mitigation

Summary

- Online Marketplace running on the dark web.
- 600,000 Devices acting as bots to collect data
- Leading to hackers being given direct access to accounts and company networks.

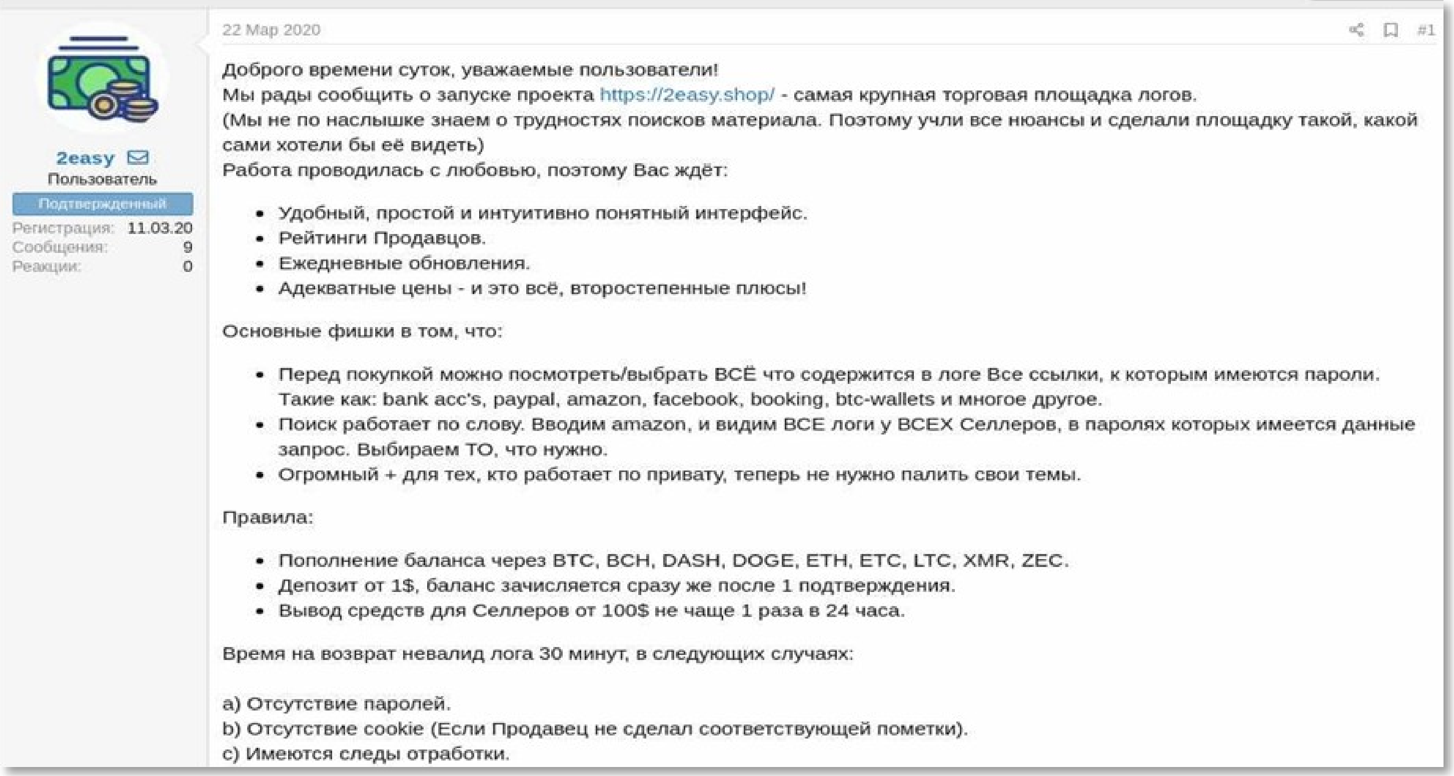
What is an Dark Net Market

- Cannot be accessed through standard web browsers
- Accessible through specific software, configuration or authorization
- Sell/Buy Variety of Illegal Materials and Items

What is 2EASY

- Dark Web Market Place
- Significant Player
- Data “Logs” from 600,000 Devices

2EASY Advert On Russian Forum



2easy

Пользователь

Подтвержденный

Регистрация:	11.03.20
Сообщения:	9
Реакции:	0

22 Мар 2020 #1

Доброго времени суток, уважаемые пользователи!
Мы рады сообщить о запуске проекта https://2easy.shop/ - самая крупная торговая площадка логов.
(Мы не по наслышке знаем о трудностях поисков материала. Поэтому учли все нюансы и сделали площадку такой, какой сами хотели бы её видеть)
Работа проводилась с любовью, поэтому Вас ждёт:

- Удобный, простой и интуитивно понятный интерфейс.
- Рейтинги Продавцов.
- Ежедневные обновления.
- Адекватные цены - и это всё, второстепенные плюсы!

Основные фишки в том, что:

- Перед покупкой можно посмотреть/выбрать ВСЁ что содержится в логе Все ссылки, к которым имеются пароли. Такие как: bank acc's, paypal, amazon, facebook, booking, btc-wallets и многое другое.
- Поиск работает по слову. Вводим amazon, и видим ВСЕ логи у ВСЕХ Селлеров, в паролях которых имеется данные запрос. Выбираем ТО, что нужно.
- Огромный + для тех, кто работает по привату, теперь не нужно палить свои темы.

Правила:

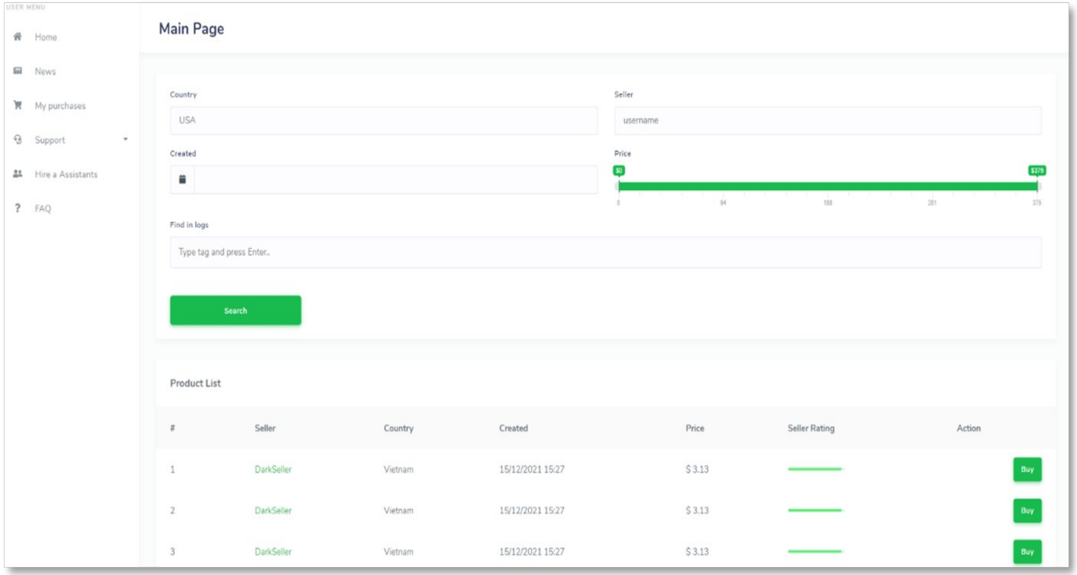
- Пополнение баланса через BTC, BCH, DASH, DOGE, ETH, ETC, LTC, XMR, ZEC.
- Депозит от 1$, баланс зачисляется сразу же после 1 подтверждения.
- Вывод средств для Селлеров от 100$ не чаще 1 раза в 24 часа.

Время на возврат невалид лога 30 минут, в следующих случаях:

a) Отсутствие паролей.
b) Отсутствие cookie (Если Продавец не сделал соответствующей пометки).
c) Имеются следы отработки.

“One of the first advertisements of 2EASY botnet market, posted on a Russian-speaking cybercrime forum Dublikat” – Source **Kela**

What is 2EASY



Main Page

Country: USA

Seller: username

Created:

Price

Find in logs: Type tag and press Enter..

Product List

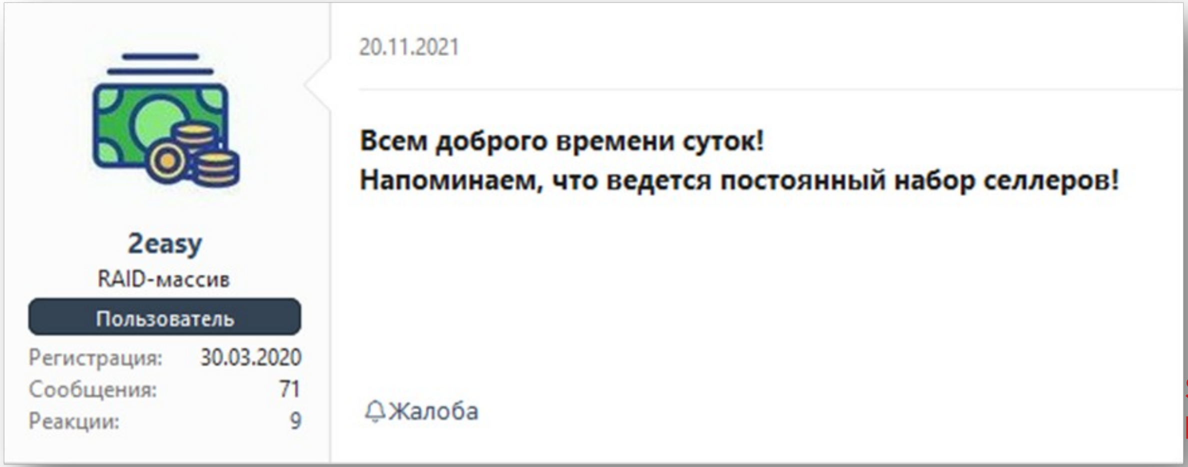
#	Seller	Country	Created	Price	Seller Rating	Action
1	DarkSeller	Vietnam	15/12/2021 15:27	$ 3.13	▬	Buy
2	DarkSeller	Vietnam	15/12/2021 15:27	$ 3.13	▬	Buy
3	DarkSeller	Vietnam	15/12/2021 15:27	$ 3.13	▬	Buy

- Logs = Archives of stolen data
- Compromised Web Browsers
- Systems Infected with malware
- Credentials, Cookies and Saved Credit Cards.

Source **Kela**
https://ke-la.com/2easy-logs-marketplace-on-the-rise/

How Does it work?

- Similar to sites like Ebay, Amazon etc..
- Operates fully automatically
- “Logs” sold for little as $5.00 USD ($7.00 AUD)
- 18 Known Sellers as of Decemeber 2021



2easy

RAID-массив

Пользователь

Регистрация:	30.03.2020
Сообщения:	71
Реакции:	9

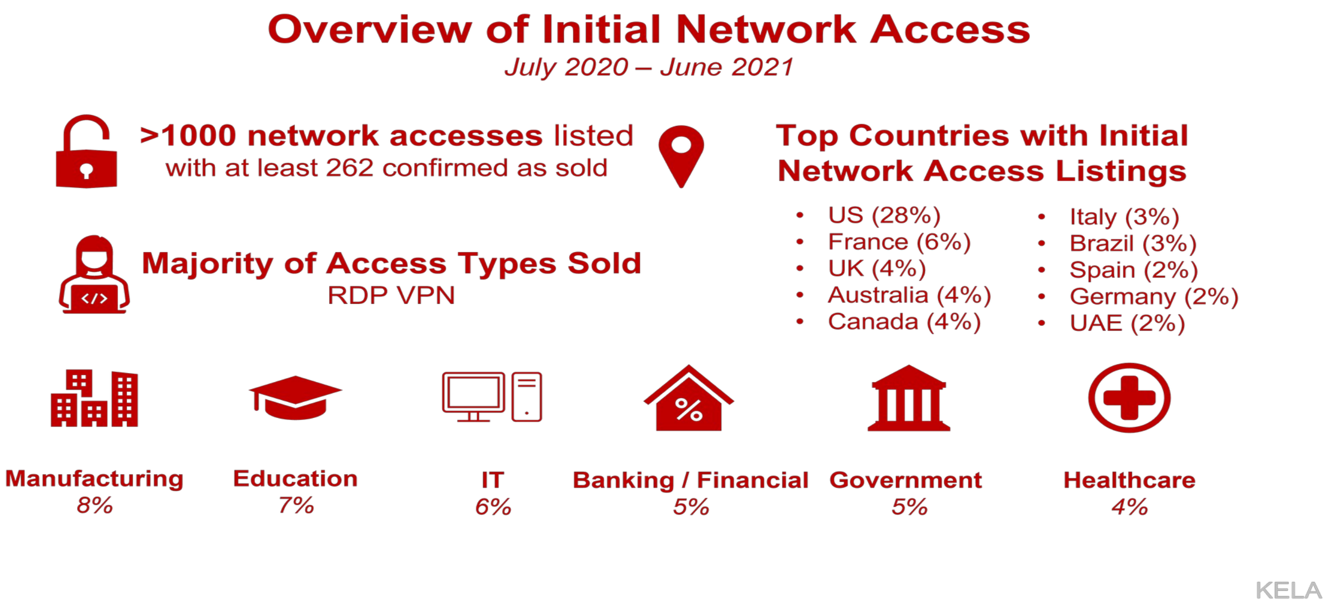
20.11.2021

Всем доброго времени суток!
Напоминаем, что ведется постоянный набор селлеров!

Source **Kela**
https://ke-la.com/2easy-logs-marketplace-on-the-rise/

Who is effected?

- Almost Everyone
  - Companies
  - End Users
  - Clients



Overview of Initial Network Access

July 2020 – June 2021

>1000 network accesses listed
with at least 262 confirmed as sold

Majority of Access Types Sold
RDP VPN

Top Countries with Initial Network Access Listings

US (28%)	Italy (3%)
France (6%)	Brazil (3%)
UK (4%)	Spain (2%)
Australia (4%)	Germany (2%)
Canada (4%)	UAE (2%)

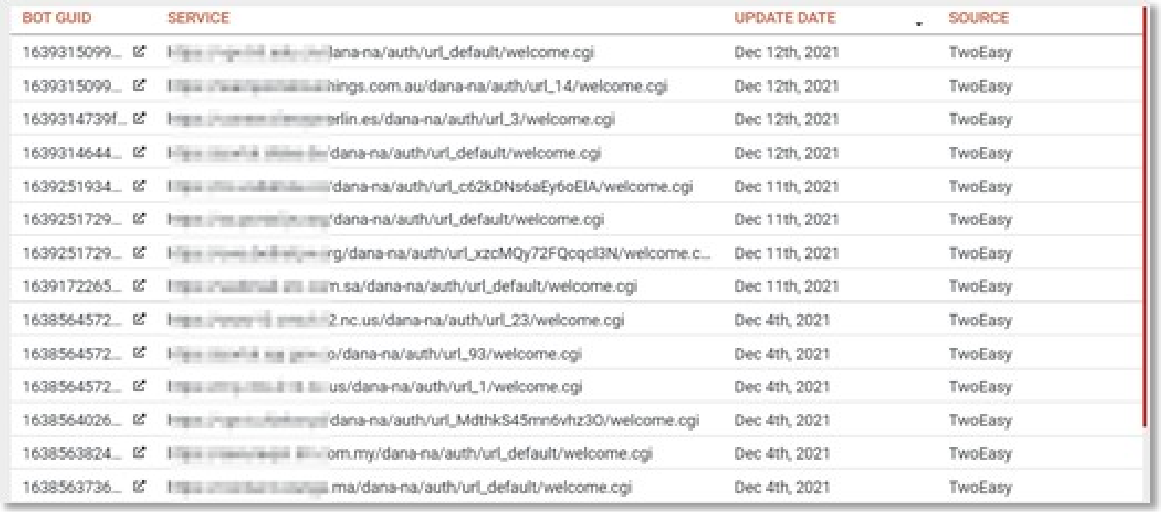
Manufacturing	Education	IT	Banking / Financial	Government	Healthcare
8%	*7%*	*6%*	*5%*	*5%*	*4%*

KELA

Source **Kela**
https://ke-la.com/2easy-logs-marketplace-on-the-rise/

Why this is critical

- Initial Access Broker Market.
- Lateral Movement Aginst Organizations.



BOT GUID	SERVICE	UPDATE DATE	SOURCE
1639315099...	[redacted]lana-na/auth/url_default/welcome.cgi	Dec 12th, 2021	TwoEasy
1639315099...	[redacted]hings.com.au/dana-na/auth/url_14/welcome.cgi	Dec 12th, 2021	TwoEasy
1639314739f...	[redacted]erlin.es/dana-na/auth/url_3/welcome.cgi	Dec 12th, 2021	TwoEasy
1639314644...	[redacted]/dana-na/auth/url_default/welcome.cgi	Dec 12th, 2021	TwoEasy
1639251934...	[redacted]/dana-na/auth/url_c62kDNs6aEy6oElA/welcome.cgi	Dec 11th, 2021	TwoEasy
1639251729...	[redacted]/dana-na/auth/url_default/welcome.cgi	Dec 11th, 2021	TwoEasy
1639251729...	[redacted]rg/dana-na/auth/url_xzcMQy72FQcqcl3N/welcome.c...	Dec 11th, 2021	TwoEasy
1639172265...	[redacted]n.sa/dana-na/auth/url_default/welcome.cgi	Dec 11th, 2021	TwoEasy
1638564572...	[redacted]2.nc.us/dana-na/auth/url_23/welcome.cgi	Dec 4th, 2021	TwoEasy
1638564572...	[redacted]o/dana-na/auth/url_93/welcome.cgi	Dec 4th, 2021	TwoEasy
1638564572...	[redacted]us/dana-na/auth/url_1/welcome.cgi	Dec 4th, 2021	TwoEasy
1638564026...	[redacted]dana-na/auth/url_MdthkS45mn6vhz3O/welcome.cgi	Dec 4th, 2021	TwoEasy
1638563824...	[redacted]om.my/dana-na/auth/url_default/welcome.cgi	Dec 4th, 2021	TwoEasy
1638563736...	[redacted]ma/dana-na/auth/url_default/welcome.cgi	Dec 4th, 2021	TwoEasy

Pulse Secure VPN Logins

Source **Kela**
https://ke-la.com/2easy-logs-marketplace-on-the-rise/

Mitigation

- **2FA/MFA**
  - Second Factor Authentication or Multi-Factor Authentciation for all user accounts and devices (if possible)
- **Anti-Virus**
  - Desktop,Laptops etc.
- **Firewall**
  - Edge Facing, Virtual Firewall
- **Training**
  - Awarness Training
  - Basic Security Training

THANK YOU