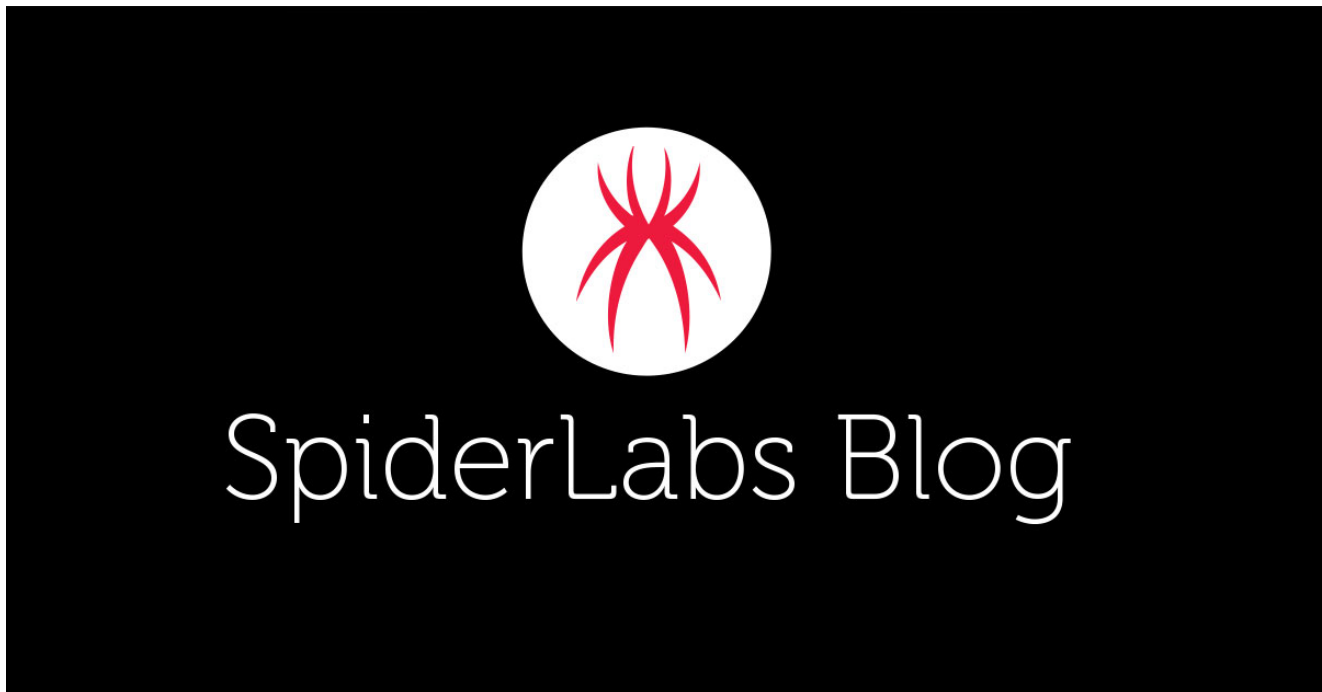


The Price Cybercriminals Charge for Stolen Data

 trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-price-cybercriminals-charge-for-stolen-data



Loading...

Blogs & Stories

SpiderLabs Blog

Attracting more than a half-million annual readers, this is the security community's go-to destination for technical breakdowns of the latest threats, critical vulnerability disclosures and cutting-edge research.

For the price of a Starbucks Caramel Frappuccino Grande and a cheese Danish, about \$8, a cybercriminal can obtain all the information needed to max out a person's stolen credit card and possibly steal their identity.

This is just one example dredged from the Dark Web by the elite Trustwave SpiderLabs team while it was conducting research for an exhaustive study into what cybercriminals charge for stolen records.

The team found repositories of financial and identity records along with VPN and remote desktop access credentials in various Darknet markets and uncovered a complicated pricing structure that sees threat actors pricing their information in the same manner as any seller on a legitimate retail site. Prices vary depending upon the country from which the information was stolen and the quality and depth of the content associated with the credential.

So, why are these records sold instead of used by the thieves? The answer is simple expediency. Criminals opt to sell credit card and driver's license information wholesale instead to quickly cash out and to avoid the time and trouble required to use the assets.

Generally, threat actors' activity is divided into business fields, someone is digging, attacking, and others are selling data or extracting user information and using it to obtain money. If the hacker or group does not know how to use the stolen information – they sell it. SpiderLabs found that in most cases, what is being sold on a forum was previously sold or used by a hacker. So, a buyer may not get first-hand hacked data.

And these threat actors do cash out. For example, the FBI's 2021 Internet Crime Report stated credit card fraud in the U.S. resulted in \$172,998,385 in losses, and this only takes into account reported incidents.

What's For Sale on the Dark Web?

The better question is – what is not for sale on the Dark Web, but let's focus on financial, identification and access data.

Here is a quick list of the items SpiderLabs found:

- Credit cards
- Bank account information
- Access to organizations through their VPNs and other means
- Social Security numbers
- Passports
- Driver's licenses
- And the ability to create the supporting documentation to prove these credentials belong to the purchaser.

Item name	Price range in USA	Price range in EU	Price range in Asia	Comments
-----------	--------------------	-------------------	---------------------	----------

Cloned Cards and Fullz	\$50 - \$1500	same	same	The price depends on how much credit would be provided for the card.
Common Credit Card, with Fullz	\$8 - \$70	\$25 - \$70	\$50 - \$90	This is a price for one card, in most cases it comes with full info
CC Track 1&2	\$30 - \$140	\$50 - \$100	\$50 - \$120	Price depends on CC class: Classic Gold Platinum Business Signature Purchase Corporate World
Bank account access	\$100 - \$3000	\$100 - \$3000	\$100 - \$3000	Price depends on account bank checking. And probable credit abilities.
Stealer Logs selling	\$1 - \$100			The logs from stealer could contain trash but could have your bank session. Depends on how many times info was extracted from logs, target.
FTP/RDP/SSH/VNC/VPN/ Organization access	\$50 - \$2000	\$50 - \$2000	\$50 - \$2000	The price could be much higher, depends on company revenue, targeted interest.
Social Security Numbers	\$0.20 - \$5			The logs from stealer could contain trash but could have your bank session. Depends on how many times info was extracted from logs, target.
ID, Passport, Driver's license	\$1 - \$50	\$1 - \$50	\$1 - \$50	The quality or uniqueness of the document has high role here
Selfie with your documents in hands	\$2 - \$10	\$2 - \$10	\$2 - \$10	The price could be higher if any specific photo with the documents should be taken

Each item is subdivided by the type of card being offered. For example, a common credit card with "Fullz" can cost between \$8 and \$70. Fullz means that for the posted price the buyer is also given additional information on the victim. This can include name, address,

Social Security number, driver's license, bank account credentials, and medical records, all wrapped up in one package and all of which enables the buyer to better utilize the stolen credential.

Trustwave SpiderLabs found three "classes" of credit card for sale. Cloned cards with fullz, common credit card with fullz and different classes of credit cards, such as gold, platinum, business, etc.

Cloned cards range in price from \$50 to \$1,500 with the cost depending upon the credit limit assigned to the card. The higher the limit, the pricier the card. Common cards, as previously noted, run from \$8 and \$70, per card and generally comes with fullz. The price for the final type varies slightly between regions, \$30 to \$140 in the U.S. and slightly less in the EU and Asia.

Hi guys! Call me Redseller94 Update 2022 LIST CREDIT CARD AND GIFT CARD

***** CREDIT CARD USA (Best Seller) UNITED KINGDOM (Best Seller) AUSTRALIA
CANADA FRANCE GERMANY CHILE TAIWAN SPAIN JAPAN ITALY BRAZIL

***** GIFT CARD AMAZON (Best Seller) ITUNES (Best Seller) BESTBUY STARBUCK
EBAY XBOX (Best Seller) WALMART TARGET

***** DEAD FULLZ INFORMATION US/UK FULLZ RANDOM BANK US/UK FULLZ WITH
ALL BANK (CHASE, HSBC, BARCLAYS, etc...) VALID PASSPORT – DRIVER'S
LICENSE – NATIONAL INSURANCE NUMBER – SSN – DOB UPDATED NEW YORK,
COLORADO, CALIFORNIA, TEXAS, RHODE ISLAND, ILLINOIS (DRIVER'S LICENSE,
SSN, DOB)

***** DUMPS WITH PIN + CLONE CARD

Selling Fraudulent Supporting Documentation

One class of documentation for sale in these marketplaces shows how much thought criminal actors will go to make their stolen data valuable.

Some sites will create false documentation to help a buyer prove to a bank or financial institution that they are in fact the true owner of the credentials they purchased.

HANZO
Drawing Documents

hanzo_hattori

Document Type	Price
Passport	10/15\$
ID card	10/15\$
Credit Cards	10/15\$
Driver License	10/15\$
Statement/Bill	10/15\$
Selfie	25\$

Scan/Photo

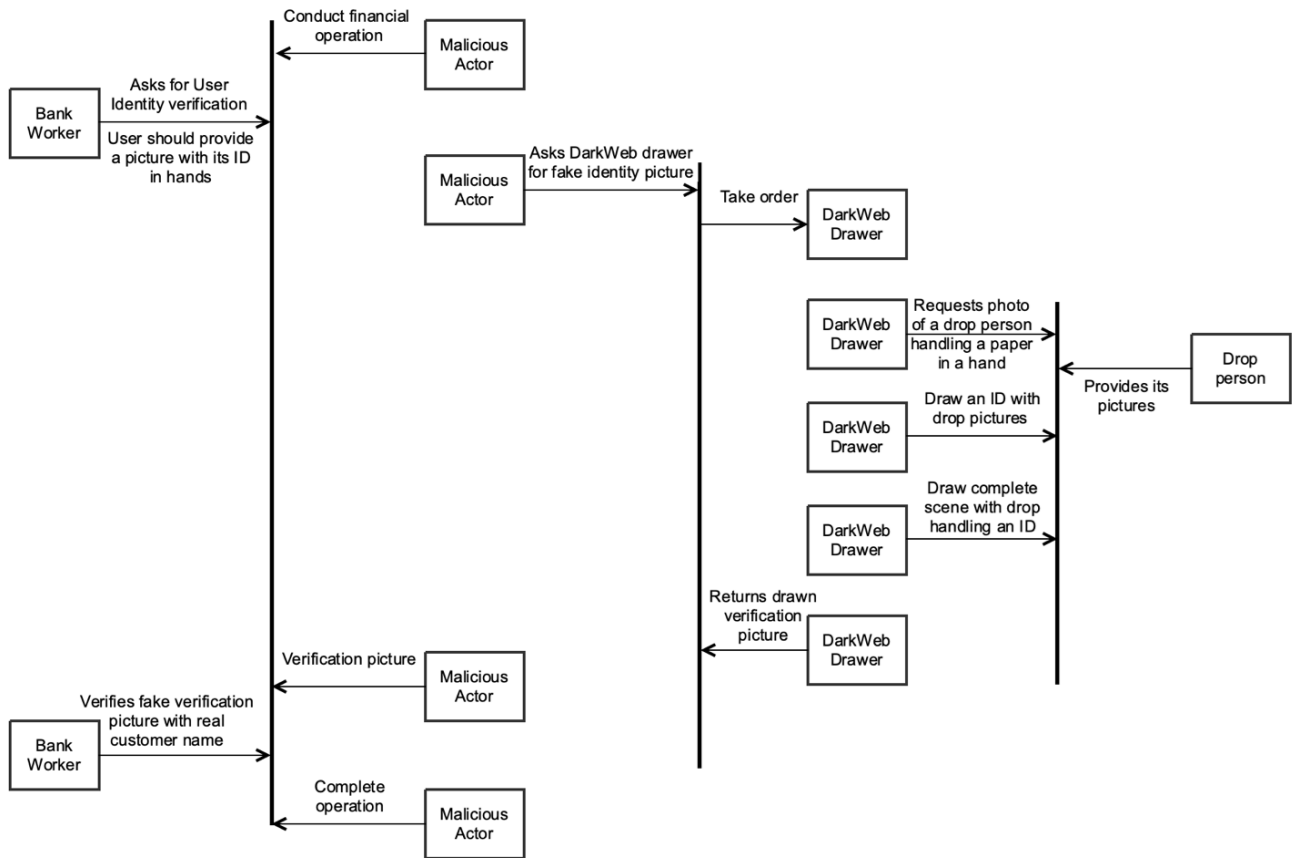
Оплата после проделанной работы

VALID BARCODES

The advertisements for these credit cards are brazen and full of details.

The common verification flow has the person who bought the stolen bank needing to confirm identity to the bank. So, the actor, to prove his identity, must provide a photo with himself holding an ID, like a passport or driver's license, along with the bank account information.

To provide such picture for verification, malicious attackers utilize the services of Drawer/Artist who can be found on a Dark Web market. The Dark Web artist creates the required ID using the photo a drop person. The drop person – is someone who will physically go to the bank to get the money or use the document as proof for an online withdrawal.



While this form of identification is not the norm in many countries, it can work at a bank with low security standards.



NEW MEXICO

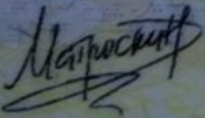
DRIVER'S LICENSE

License # **586204865** ISSUED **03/01/2018**
 Date of Birth **08/12/1970** EXPIRES **03/09/2026**

MATROSKIN
KOT

6104 PROSTOKVASHINO VIL
 NIZHNY NOVGOROD, NM 89129

SEX **M** HEIGHT **5'04"**
 WEIGHT **155** EYES **GRN**
 CLASS **D** ENDORSEMENTS **NONE**
 RESTRICTIONS **NONE**

UTAH **DRIVER LICENSE** 

573067384 ISS **11/02/2016**
 3 **DOB 09/02/1964** 4b **EXP 09/02/1964**

1 **WICK**
 2 **JOHN**

8 **221 PARK AVE**
PARK CITY, UT 84085

5 **DD 45385012**

9 **CLASS D** 9a **END MZ**
 15 **SEX M** 12 **BEST A**

16 **HGT 5'-07"**
 17 **WGT 90 lb**
 18 **EYES GRN** **09/02/64**
 19 **HAIR BRN Z**





DRIVING LICENCE

1. MATROSKIN
2. KOT

3. 14.06.1946 SCOTLAND
4a. 27.08.2016 4c. DVLA
4b. 02.10.2025

5. MATROSKIN406146K9NC 23

7. 

8. 31 STIRLING STREET, DUNDEE DD3 6PH

9. AM/A2/B1/C1/D/V/BE/CE/DE/I/K/q




UA ПОСВІДЧЕННЯ ЄДИНОГО РІВНЯ ЛІЦЕНЗІЇ ПЕРMIS DE CONDUIRE

1. 
2. 

3. **МІСЬК**
4. **ДІСКИ РОБАНОВИЧ**
5. **ІГОР ІВАНОВИЧ**
6. **ІГОР ІВАНОВИЧ РОБАНОВИЧ**
7. **26.08.2021** 8. **26.08.2023**
9. **TCU 7441** 10. **TCU 7441**
11. **04M 18841**

Клас	Категорія	Статус	Дата видачі	Дата закінчення
A1	A1	активний	26.08.2021	26.08.2023
A	A	активний	26.08.2021	26.08.2023
B1	B1	активний	26.08.2021	26.08.2023
B	B	активний	26.08.2021	26.08.2023
C1	C1	активний	26.08.2021	26.08.2023
C	C	активний	26.08.2021	26.08.2023
D	D	активний	26.08.2021	26.08.2023
E	E	активний	26.08.2021	26.08.2023
F	F	активний	26.08.2021	26.08.2023
G	G	активний	26.08.2021	26.08.2023
H	H	активний	26.08.2021	26.08.2023
I	I	активний	26.08.2021	26.08.2023
J	J	активний	26.08.2021	26.08.2023
K	K	активний	26.08.2021	26.08.2023
L	L	активний	26.08.2021	26.08.2023
M	M	активний	26.08.2021	26.08.2023
N	N	активний	26.08.2021	26.08.2023
O	O	активний	26.08.2021	26.08.2023
P	P	активний	26.08.2021	26.08.2023
Q	Q	активний	26.08.2021	26.08.2023
R	R	активний	26.08.2021	26.08.2023
S	S	активний	26.08.2021	26.08.2023
T	T	активний	26.08.2021	26.08.2023

12. **04M 18841**

South Carolina SC USA **DRIVER'S LICENSE** DL

4d DL#: **102864793**

1 MATROSKIN
2 KOT

8 6104 PROSTOKVASHINO VIL
NIZHNY NOVGOROD, SC 891209

3 DOB: **08/12/1970**



4a Issued: **07/16/2026**

4b Expires: **07/16/2028**

15 Sex: M 16 Hgt: 5'-01"
17 Wgt: 155 lb 18 Eyes: GRN
9 Class: D 9a End: None
12 Restrictions: None

5 DD 4257246708285754228

08/12/1970

Matroskin

Palmetto STATE

Governor

This artist group developed used high-end tools to create a quality finished product. The artists can even add the required holograms and mimic watermarks on the identification documents.



Fake documents. With this approach, even modern verification video calls could be easily passed by introducing such printed IDs.

Bank Accounts

Bank account pricing, \$100 to \$3,000 per account, is directly tied to the amount of money that can be accessed. The higher the amount that can be stolen, the more expensive the purchase. Additionally, the price correlates to how easy it is to access the bank account as some banks might not be easier for a criminal to fool.

The seller usually mentions the balance on that account along with the victim's physical address. This can be done to hint at the target's potential level of wealth, a toney address in Los Angeles or New York City might garner more interest from a buyer.

Typically, those buying a bank account gain online access, the account and routing number, any debit card and PIN information available, the owner's name and signature, phone number and billing address. The owner's IP address along with the operating system used to access the account might also be included.

While this information is generally used to digitally access an account, the criminal could go to the financial institution and use this information to simply withdraw the money in person. Stealing the money in this manner is one way to defeat any multifactor authentication that might protect the account, but it also opens up the possibility of the individual being caught and arrested.

Buying Virtual Private Network Credentials

VPN access credentials were the most expensive records SpiderLabs found being advertised. This is logical considering what a threat actor can do once inside an organization. Everything from stealing money, corporate espionage, IP theft, seeding malware and planting ransomware are all on the table once access is gained.

Our researchers found one ad asking \$5,000 for access to a corporate network, while another was priced at \$2,500 for VPN credentials purportedly to a Korean company with an estimated \$7 billion in revenue.

Ads for VPN access can offer a great deal of detail to help persuade a buyer. Sometimes they mention the businesses industry but the price for the access is generally determined by the company's revenue, as can be seen in this list of examples from the XSS forum. Note that the word 'jealousy' in the document is a bad translation for 'revenue.'

“Financial business, Taiwan. 627m of revenue. Palo Alto. 1500\$

Big business headquarters, manufacturing, finance, south korea. 7 billion jealous. Pulse. 2500\$

Working with insurance, Argentina. 171m revenue. Palo Alto. 500\$

Credit business, Indonesia. 99m of revenue. There is a stock symbol. Fortinet. 300\$

Headquarters, commodity business, dubai. 25m rope. Palo Alto. 400\$

Produce feed for livestock, leaders, myanmar. 227m revenue. Palo Alto. 900\$

Univer, UK. 274m jealous. Palo Alto. 300\$

Univer, Canada. 645m jealous. Cisco. 600\$

Univer, Australia. 635m of revenue. Palo Alto. 600\$

Business school, Denmark. 31m revenue. Palo Alto. 200\$

Yusa above 20m is relevant. There is Canada, bis on 20m. It's ok too. They are \$200 each.”

VPN access advertisements.

For this price, the seller provides administrator access to a server on the network. The ability to access other machines on the network depends on local permissions and the way the network is configured in that organization.

If a company has a solid cybersecurity defense in place even this level of access might not be enough to do severe damage. The ability to use that access for malicious purposes will be limited in environments that are fairly restricting, use network segmentation, and check for anomalies etc.

Trustwave

HOW MUCH IS YOUR
IDENTITY WORTH
ON THE **DARK WEB?**

01
The Dark Web is the digital equivalent of the black market—bank accounts, and data of unknowing consumers. This is how hackers gain access to personal data, and how much they sell it for on the Dark Web.

02
Faxes and snail mail are being used less often today, in favor of email and online identify verification services. The personal information provided to these services—driver's licenses, financial statements, utilities bills, and more—is often stored in databases on web servers.

03
Without proper security tools or encryption in place, hackers can gain access to the data.
Web servers

04
Hackers have turned this opportunity into a business, selling unsuspecting consumers' identities

05
The buyer—often another hacker—can use the stolen identity to authenticate

INFOGRAPHIC

How Much Is Your Identity Worth on the Dark Web?

The dark web is the digital equivalent of the black market, and there's no limit to the sensitive, personal information available for purchase in the dark underworld of hackers.

[Download Now](#)