



# DARK WEB

*Can you afford to be exposed?*



**Darryl Keys**  
PRESIDENT & CEO  
ZYPHA CORPORATION

# AGENDA

- 1 How **compromised credentials** can lead to a **data breach**, and what cybercriminals do with credentials once they've obtained them.
- 2 A tour of the Dark Web - the current landscape of **threats against small and medium sized businesses** and how your credentials can be exploited

## (SURFACE) WEB

The level where data is **PUBLIC**  
Only 4% of the web consists of indexed public websites that are visible to all web users through ordinary search engines such as Google and Bing.

## DEEP WEB

The level where data is **PRIVATE**  
The largest part of the internet is made of protected information and is only located and accessed by a direct URL or IP address, that may require a password or other security access to get past public pages. That includes: email, online banking, social media pages & profiles, services such as video on demand, etc. It's used for legit purposes. Most of us access the Deep Web every day.

## DARK WEB

The level where data is **ANONYMOUS**  
Within the Deep Web is the part of the internet called the Dark Web. A complex encrypted system not visible to traditional search engines that can only be accessed by a special browser called Tor. Transactions, IPs, profiles, locations, etc. are totally anonymous, making it the perfect place for many illegal activities to happen. It's not illegal by itself but that's where criminal sites live.



# DARK WEB

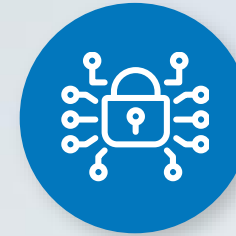
Estimated to be 550 times larger than the surface web and growing.

Because you can operate anonymously, the dark web holds a wealth of stolen data and illegal activity.

# HOW DO BREACHES HAPPEN?



**CREDENTIAL  
THEFT**



**BOTNETS**



**PHISHING**



**VULNERABILITY  
EXPLOITS**



# THE THREAT TO ALL BUSINESSES

*9 Ways Your Employees' Work Credentials Can Lead to a Breach. Your current and former employees often use their work email address and password to access common public sites. Many public sites have suffered data breaches, with data ending up on the Dark Web.*

## HR & PAYROLL

**PAYCHEX**  
**ADP**  
CERIDIAN

## EMAIL SERVICES

   
Office 365  
YAHOO!

## CRM

salesforce  
HubSpot  
ZOHIO

## TRAVEL SERVICES

Expedia  
travelocity  
ORBITZ  
FASTBOOKING

## COMMUNICATIONS

verizon  
AT&T  
Adobe  
T-Mobile

## E-COMMERCE

STAPLES  
ebay  
amazon  
Office DEPOT

## BANKING & FINANCE

intuit quickbooks.  
Bank of America  
freshdesk

## COLLABORATION

CITRIX  
box  
Dropbox

## SOCIAL MEDIA

# ALL IN ON ZERO TRUST

Compliance laws dictate that Security and Access Management are no longer optional. Data regulation is not just limited to Fortune 500 companies. Small and medium-sized organizations are also being held responsible.





# LET'S TOUR THE DARK WEB


## How you can purchase data about employees from various companies



### SNAPSHOTS FROM THE DARK WEB

Businesses are a common target for Dark Web criminals, because businesses tend to have money. It also allows the criminal to feel better about stealing from “Main Street Flowers” because they’re just “sticking it to the corporations.”

[AD] USA Business And Investor Database 8 Million Records + Add Listing

 Sold by Goldapple 7 5.00 Trust Level 1

FEATURES			
Product class	Digital Product	Quantity left	1
Views	276	Visibility	Public
Ends In	Never	Payment	Escrow

Unit price: 0.146306 XMR 0.00196914 BTC 0.11611036 LTC 0.03337236 BCH

USD 10.2897

Instant Delivery 1 Days - USD +0 / item

[Buy Now](#)

Maximum Quantity: 1

Product Description

USA Business And Investor Database 8 Million Records

All information in this database is in plaintext.

Included information: Employee Email Addresses, Company Name, Address, City, State, ZIP Code, Telephone Numbers, Company Website, Employee Numbers, Sale Volumes, Company Vocation, Fax Numbers, SIC.



## *Purchase voter databases with voter id's, addresses, dates of birth*



## SNAPSHOTS FROM THE DARK WEB

A screenshot of a web browser window with a white background and rounded corners. At the top, there are three colored window control buttons (red, yellow, green). Below them, there are three tabs: "Description", "Refund policy", and "Terms & Conditions". The "Description" tab is active. The main content area contains the following text:

**Product Description**

Kansas Voter Database 1.8 Million Voters

All information in this database is in plaintext.

Included information: Voter IDs, Full Names, Physical Addresses, Previous Addresses, Date of Birth, Genders, Voter Status, Phone Numbers.

We promise:

- Your order will be delivered instantly.
- If you are not satisfied with your order we will refund your order.

# Clone Card Crew Dark Web site - Credit card dumps



## SNAPSHOTS FROM THE DARK WEB

<a href="#">USFine DB.txt.gz</a>	22-May-2017 01:28	30331
<a href="#">Uefa Dump.sql.gz</a>	22-May-2017 01:28	1049846
<a href="#">VanquishRSPS.db.txt.gz</a>	22-May-2017 01:28	138269
<a href="#">Verizon Accounts Dump.txt.gz</a>	22-May-2017 01:28	1456
<a href="#">Viphf December 2014.sql.gz</a>	22-May-2017 01:28	6162092
<a href="#">Virtual credit cards.txt.gz</a>	22-May-2017 01:28	3052252
<a href="#">WAREHOUSE MAIN.sqlite3</a>	22-May-2017 01:29	87365632
<a href="#">WarnerBros.txt.gz</a>	22-May-2017 01:29	10272

**CLONE CARD CREW**  
Attack of the Clone

Welcome back! Thank you for giving us another chance to provide you with the best credit cards. Here you'll find cloned credit cards at discounted price and promised funds.

All cards are skimmed and cloned. Every card is written by high quality writer and come with working PIN. We have a large database of credit card - ranging from 0day to 90days. Every card is verified for funds and validity before shipment. They work worldwide.

We ship all of our cards 100% discrete via FedEx Standard Overnight within USA and FedEx International Priority for countries outside of USA. Shipping cost is included.

These cards are legit and safe to receive. Using them is another thing...

**Free CC dumps of April 2015. We also sell dump 1&2 tracks!**

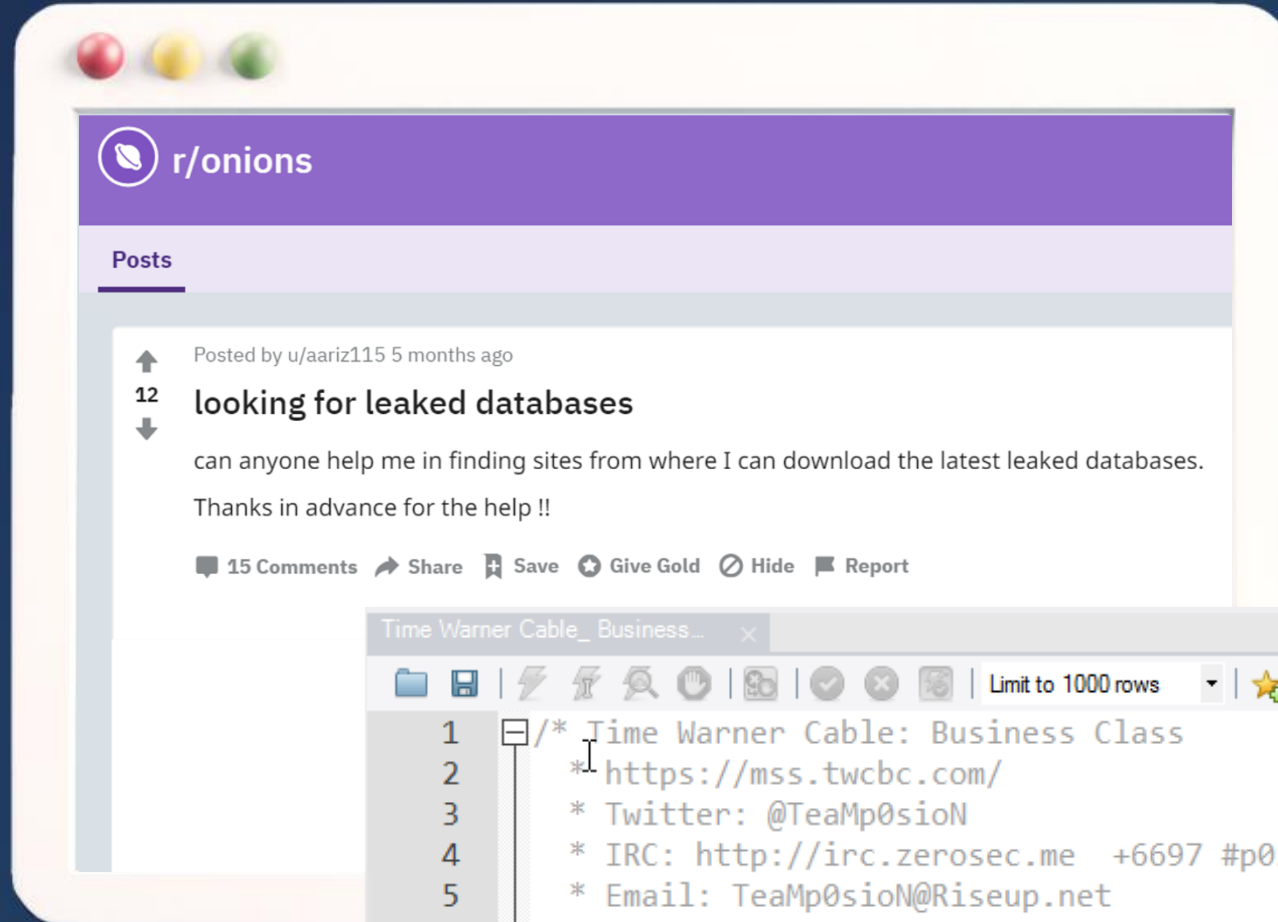
First Name : William  
Middle Name : K  
Last Name : Black  
Spouse Name :  
Father Name :  
Billing Address : 65 Autumn Creek Lane,Apt C  
City : East Amherst  
State : NY

Please choose card You wish to buy below and fill in the form. (Payment as always - Bitcoins.)

BALANCE \$2,000    USA VISA CREDIT CARD BALANCE \$5,000    EU VISA CREDIT CARD BALANCE €5,000




# SNAPSHOTS FROM THE DARK WEB



```
Time Warner Cable_Business... x
Limit to 1000 rows
1 /* Time Warner Cable: Business Class
2 * https://mss.twcbc.com/
3 * Twitter: @TeaMp0sioN
4 * IRC: http://irc.zerosec.me +6697 #p0ison
5 * Email: TeaMp0sioN@Riseup.net
6 * Greetz: Pseudo, Militis, Jimmy, MLT & The Rest of TeaMp0isoN
7 */
```



# SNAPSHOTS FROM THE DARK WEB



### USA Business Bank Account and Routing Numbers! Perfect for ACH Fraud

29.99 EUR 0.006477

**In stock**

**Vendor:** eucarder [+1]-0]

**Class:** Digital

**Escrow Type:** Full escrow

1 items sold since 2018-02-11 01:25:06

Favorite Question Report

Quantity: 1

Litecoin (LTC)

Bitcoin (BTC)

Monero (XMR)

**Buy Now**

#### Details

Business Bank Chequing and Routing Numbers!

What you get is a listing of a bank account that belongs to a U.S. business (routing and checking numbers, NOT login).

You will receive the exact following:  
Business name, Bank Account Account Name , Address, City, State, Zip, Tel, Bank Name, Routing Number, Account Number

Format may vary but recall that all routing numbers are 9 digits and start with a 0, 1, or 2 so if it is 8 digits then a 0 goes in front.

What can these be used for?  
Anything, but primarily ACH transfers would be best.  
Funds being available have never been an issue with these accounts.

Want to do more with them? Many of the listings have the bank account name as an individual. See if you can purchase their ssn online, and from their it is quite easy to gain access to their bank login.



## SNAPSHOTS FROM THE DARK WEB

This one is so popular that it's sold out. 'Fullz' typically means there is enough information to commit ID fraud

The screenshot shows a marketplace listing for '300 x Business Fullz Of Californian Business owners! Complete! High Credit score!'. The price is listed as 15 EUR (0.003231) and is marked as 'Out of stock'. The listing includes a vendor name 'BOOM [+2]-1', a class of 'Digital', and an escrow type of 'Full escrow'. It also shows '5 items sold since 2017-11-07 21:47:17'. The listing is currently unavailable for purchase, with a 'Buy Now' button that is disabled. The interface includes navigation tabs for 'Details', 'Terms & Conditions', and 'Feedback', and a 'Details' section that repeats the listing title.

300 x Business Fullz Of Californian Business owners! Complete! High Credit score!

15 EUR  $\text{B}$  0.003231  
Out of stock

Vendor BOOM [+2]-1  
Class Digital  
Escrow Type Full escrow  
5 items sold since 2017-11-07 21:47:17

Favorite Question Report

Quantity: 1  
 Litecoin (LTC)  
 Bitcoin (BTC)  
 Monero (XMR)

Buy Now

Details Terms & Conditions Feedback

Details  
300 x Business Fullz Of Californian Business owners! Complete! High Credit score!



## SNAPSHOTS FROM THE DARK WEB

Here's someone selling the "largest" known data dump for \$10. These markets are run largely the same as eBay or Etsy. Note that the seller even has "ratings."

The screenshot shows a marketplace listing for a database collection. The title is "Database Collection #1-5 + AntiPublic (2019) (+-1TB)". There are two tabs: "Description" (selected) and "Refund policy & Vendor information". The description text reads: "In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popular hacking forum. The data contained almost 2.7 billion records including 773 million unique email addresses alongside passwords those addresses had used on other breached services. Full details on the incident and how to search the breached passwords are provided in the following blog post: <https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/>". Below the description are two sections: "Details" and "Rating". The "Details" section lists: "Quantity in stock 8 Piece", "Minimum amount per order: 1 Piece", "Maximum amount per order: 1 Piece", "Category: Digital goods → Other", and "Views: > 200". The "Rating" section is highlighted with a red box and shows two categories: "Communication" with a 4-star rating (4 reviews) and "Quality" with a 5-star rating (5 reviews).

### Database Collection #1-5 + AntiPublic (2019) (+-1TB)

Description Refund policy & Vendor information

In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popular hacking forum. The data contained almost 2.7 billion records including 773 million unique email addresses alongside passwords those addresses had used on other breached services. Full details on the incident and how to search the breached passwords are provided in the following blog post: <https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/>

#### Details

**Quantity in stock** 8 Piece  
**Minimum amount per order:** 1 Piece  
**Maximum amount per order:** 1 Piece  
**Category:** Digital goods → Other  
**Views:** > 200

#### Rating

Communication	★★★★☆	(4)
Quality	★★★★★	(5)



## SNAPSHOTS FROM THE DARK WEB

Business credit card details are being sold with a holiday discount.

The screenshot shows a marketplace listing for 'Miami, Florida Centurion & Small Corporate 201 Credit Dumps'. The vendor is 'pikachupacket' with a rating of 3.91. The listing includes a 'HOLIDAY DISCOUNT' badge and a 'Buy' button. The interface also shows options for payment in Bitcoin or Monero and a 'Buy' button.

**Info**  
Vendor: pikachupacket (521) ★★★★★ (3.91)  
Any questions about the offer?  
 Digital goods  
Escrow

bitcoin MONERO  
★ Add to favorites  
Amount: 1  
Buy  
Scroll down for prices

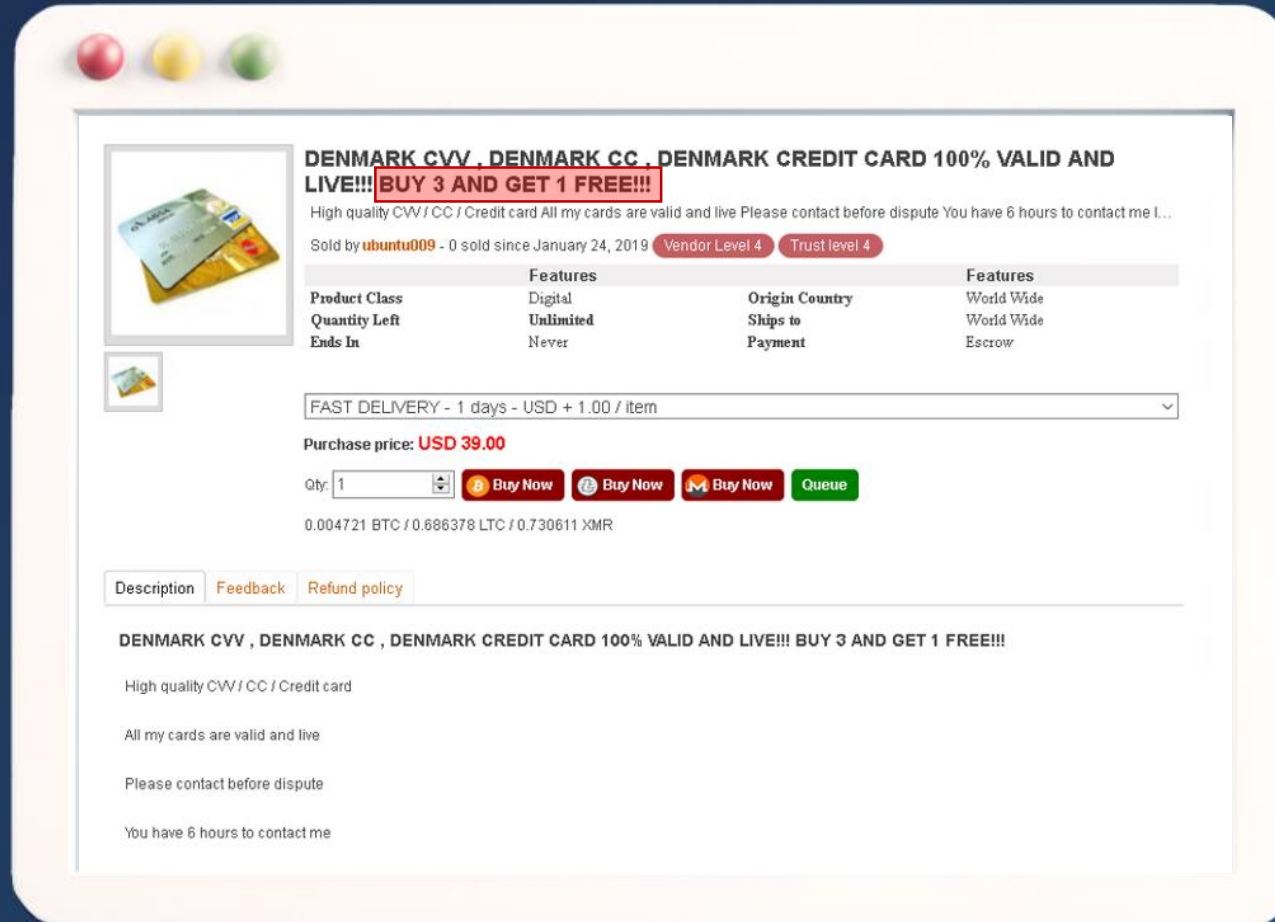
### Miami, Florida Centurion & Small Corporate 201 Credit Dumps

Description Refund policy & Vendor information

This listing is for Track1 & Track2 Platinum, Centurion, and Small Corporate 201 American Express Credit Dumps from Miami, Florida.

**HOLIDAY DISCOUNT**

# THIS ISN'T LIMITED TO THE U.S.



**DENMARK CVV , DENMARK CC , DENMARK CREDIT CARD 100% VALID AND LIVE!!! BUY 3 AND GET 1 FREE!!!**

High quality CVV / CC / Credit card All my cards are valid and live Please contact before dispute You have 6 hours to contact me I...

Sold by **ubuntu009** - 0 sold since January 24, 2019 **Vendor Level 4** **Trust level 4**

	Features		Features
Product Class	Digital	Origin Country	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

FAST DELIVERY - 1 days - USD + 1.00 / item

Purchase price: **USD 39.00**

Qty:  [Buy Now](#) [Buy Now](#) [Buy Now](#) [Queue](#)

0.004721 BTC / 0.686378 LTC / 0.730611 XMR

[Description](#) [Feedback](#) [Refund policy](#)

**DENMARK CVV , DENMARK CC , DENMARK CREDIT CARD 100% VALID AND LIVE!!! BUY 3 AND GET 1 FREE!!!**

High quality CW / CC / Credit card

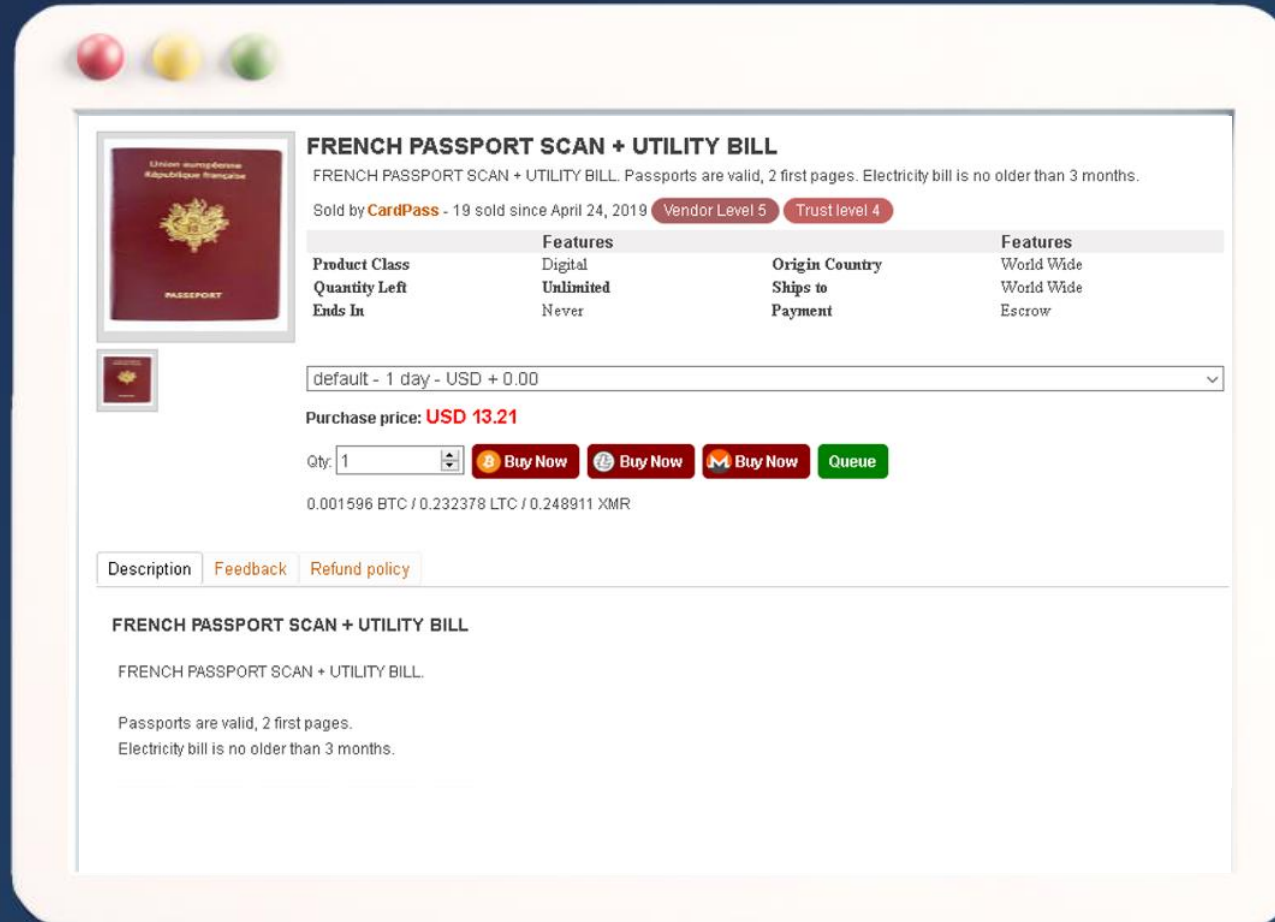
All my cards are valid and live

Please contact before dispute

You have 6 hours to contact me



# THIS ISN'T LIMITED TO THE U.S.



The screenshot shows a marketplace listing for a digital product. The product is titled "FRENCH PASSPORT SCAN + UTILITY BILL". It includes a small image of a French passport cover. The listing text states: "FRENCH PASSPORT SCAN + UTILITY BILL. Passports are valid, 2 first pages. Electricity bill is no older than 3 months." It is sold by "CardPass" and has been sold 19 times since April 24, 2019. The vendor has a level of 5 and a trust level of 4. A table of features is provided, and the purchase price is listed as USD 13.21. There are three "Buy Now" buttons with different payment icons (Bitcoin, Litecoin, Monero) and a "Queue" button. The quantity is set to 1. Below the purchase options, the prices in Bitcoin (0.001596 BTC), Litecoin (0.232378 LTC), and Monero (0.248911 XMR) are shown. At the bottom, there are tabs for "Description", "Feedback", and "Refund policy".

**FRENCH PASSPORT SCAN + UTILITY BILL**

FRENCH PASSPORT SCAN + UTILITY BILL. Passports are valid, 2 first pages. Electricity bill is no older than 3 months.

Sold by **CardPass** - 19 sold since April 24, 2019 **Vendor Level 5** **Trust level 4**

	Features		Features
<b>Product Class</b>	Digital	<b>Origin Country</b>	World Wide
<b>Quantity Left</b>	Unlimited	<b>Ships to</b>	World Wide
<b>Ends In</b>	Never	<b>Payment</b>	Escrow

default - 1 day - USD + 0.00

**Purchase price: USD 13.21**

Qty: 1

0.001596 BTC / 0.232378 LTC / 0.248911 XMR

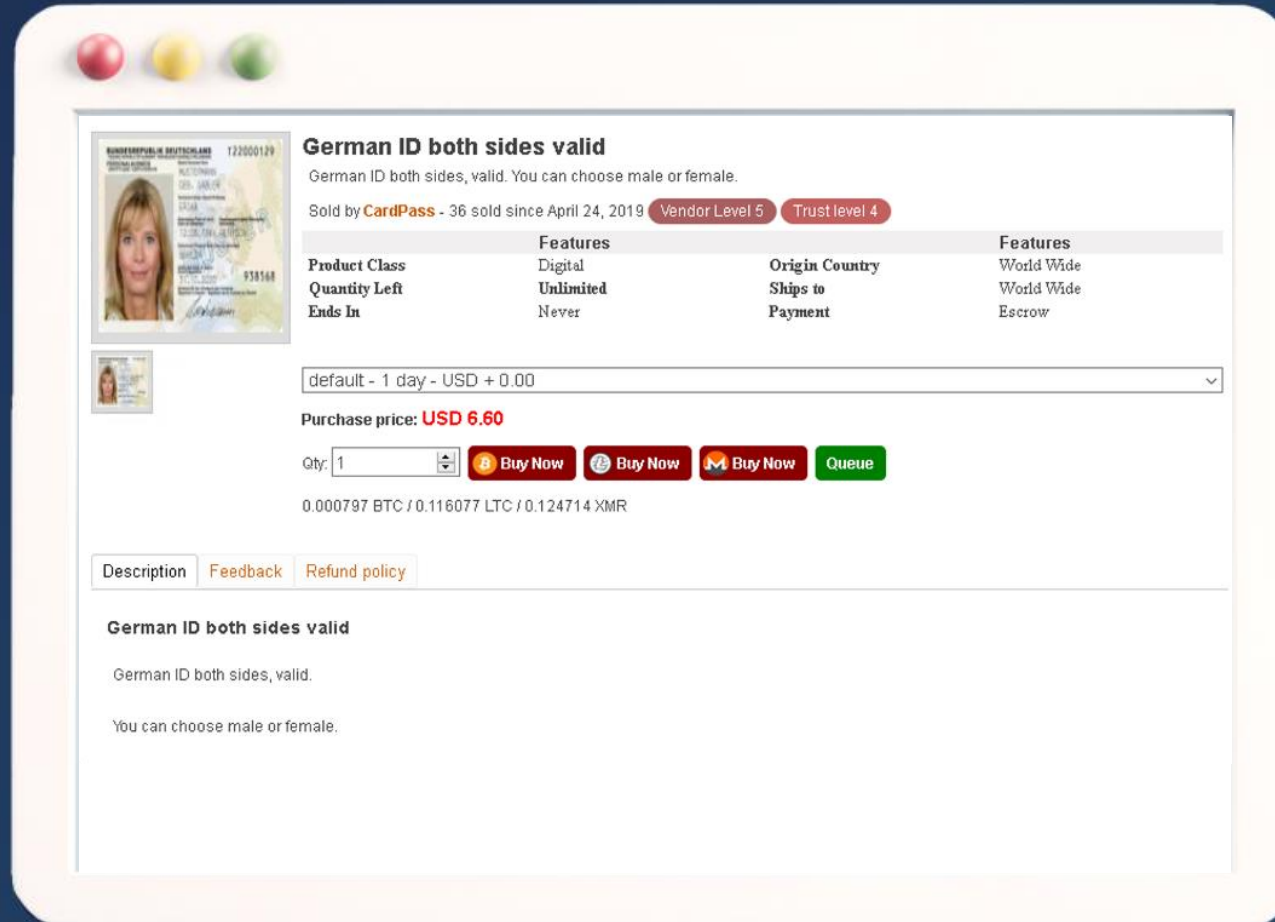
[Description](#) [Feedback](#) [Refund policy](#)

**FRENCH PASSPORT SCAN + UTILITY BILL**

FRENCH PASSPORT SCAN + UTILITY BILL.

Passports are valid, 2 first pages.  
Electricity bill is no older than 3 months.

# THIS ISN'T LIMITED TO THE U.S.



The screenshot shows a marketplace listing for a "German ID both sides valid". The listing includes a thumbnail image of the ID card, a title, a description, a table of features, a purchase price, and a quantity selector. The ID card image shows a woman's face and the text "BUNDESPUBLIK DEUTSCHLAND 722000129". The title is "German ID both sides valid". The description states "German ID both sides, valid. You can choose male or female." and "Sold by CardPass - 36 sold since April 24, 2019". The features table lists "Product Class" as Digital, "Quantity Left" as Unlimited, "Ends In" as Never, "Origin Country" as World Wide, "Ships to" as World Wide, and "Payment" as Escrow. The purchase price is "USD 6.60". The quantity selector is set to "1". The listing also shows conversion rates: "0.000797 BTC / 0.116077 LTC / 0.124714 XMR".

**German ID both sides valid**  
German ID both sides, valid. You can choose male or female.  
Sold by **CardPass** - 36 sold since April 24, 2019 **Vendor Level 5** **Trust level 4**

	Features	Features
<b>Product Class</b>	Digital	<b>Origin Country</b>
<b>Quantity Left</b>	Unlimited	World Wide
<b>Ends In</b>	Never	<b>Ships to</b>
		World Wide
		<b>Payment</b>
		Escrow

default - 1 day - USD + 0.00

Purchase price: **USD 6.60**

Qty: 1 **Buy Now** **Buy Now** **Buy Now** **Queue**

0.000797 BTC / 0.116077 LTC / 0.124714 XMR

[Description](#) [Feedback](#) [Refund policy](#)

**German ID both sides valid**

German ID both sides, valid.

You can choose male or female.

# THIS ISN'T LIMITED TO THE U.S.

The screenshot shows a marketplace listing for 'Worldwide CC & CVV from UK/US/DE/FR/CA/JP/AU/NL/IT/CH/DK/EU/Asia...'. The listing includes a product image with logos for VISA, MasterCard, and AMERICAN EXPRESS. The text describes the product as 'Fresh and High Quality CC & CVV from all countries in the world' and provides details on the seller's performance, including 'Vendor Level 7' and 'Trust level 7'. A table lists features such as 'Product Class: Digital', 'Quantity Left: Unlimited', and 'Ends In: Never'. The purchase price is listed as 'USD 10.99' with a quantity selector set to 1. Below the purchase options, there are tabs for 'Description', 'Feedback', and 'Refund policy'. The description section repeats the product title and provides a note: 'Note: All my cards are coming without address, most of them are non-AVS (Address Verification System), you can use any fake billing address when you make carding.'

**Worldwide CC & CVV from UK/US/DE/FR/CA/JP/AU/NL/IT/CH/DK/EU/Asia...**  
Fresh and High Quality CC & CVV from all countries in the world. Data Format: Card Number | Expire Month | Expire Year | CVW | ...  
Sold by **bluer** - 5939 sold since April 21, 2019 **Vendor Level 7** **Trust level 7**  
79 Items available for auto-dispatch

	Features		Features
Product Class	Digital	Origin Country	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

Bin Level Bank Request - 1 days - USD + 15.00 / item

Purchase price: **USD 10.99**

Qty:  **Buy Now** **Queue**

0.001330 BTC

[Description](#) [Feedback](#) [Refund policy](#)

**Worldwide CC & CVV from UK/US/DE/FR/CA/JP/AU/NL/IT/CH/DK/EU/Asia...**  
Fresh and High Quality CC & CVV from all countries in the world.  
Data Format: Card Number | Expire Month | Expire Year | CVW | Card Type | Holder Name | Card Level | Country | Email  
Note: All my cards are coming without address, most of them are non-AVS (Address Verification System), you can use any fake billing address when you make carding.

Our analysts pulled this job posting which looks exactly like something you might see on Indeed or LinkedIn.

## **LOOKING FOR A JOB?**

*The Dark Overlord is hiring 'goal-oriented' cybercriminals for \$63K per month*

*The Dark Overlord is hiring. Specifically, it's hiring software designers and systems engineers with at least "10 years of experience" to "bring innovative approaches to operations and think outside the box."*

*An annual salary of \$762K (payable after a 90-day probationary period, naturally) with an expected increase to \$1.068M after two years (contingent upon positive performance reviews, of course).*



# THE DARK WEB BUSINESSES ARE REAL

Hackers are posting verified  
Zoom accounts on the Dark Web.

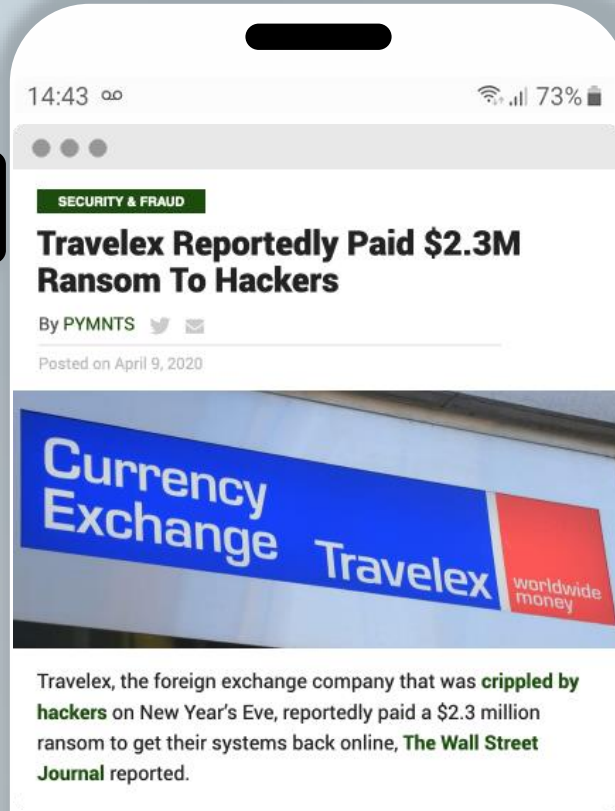


“On April 1st, an actor in a popular dark web forum posted a link to a collection of 352 compromised Zoom accounts,” a spokesperson for cybersecurity firm Sixgill wrote in an email. “In comments on this post, several actors thanked him for the post, and one revealed intentions to troll the meetings.”

Sixgill said these links included email addresses, passwords, meeting IDs, host keys and names, and the type of Zoom account. Most were personal, but not all.

zoom  
zoom  
zoom  
zoom  
zoom  
zoom  
zoom  
zoom

# FROM RANSOMWARE TO PUBLIC EXTORTION



A screenshot of a forum post. The title is 'Maze releases some of the Allied Universal files'. The text reads: 'Knowing that tomorrow was Maze's deadline, we were surprised tonight when they posted in our forums a description of the breach and a link to almost 700 MB of leaked files.' A quote box contains the text: 'We have already morning of Friday. Yes, it is friday in asia. Forgot to mention that deadline is a friday by our local time, and not US.' Below this, it says: 'This link was for a 7-zip archive containing files related to termination agreements, contracts, medical records, server directory listings, encryption certificates, and exported lists of users from their active directory servers.'

Name	Date modified	Type	Size
XXXXXXXXXXXXXXXXXXXX2.xlsx	8/25/2015 12:15 PM	Microsoft Excel W...	93 KB
XXXXXXXX Meeting.pdf	9/16/2015 9:52 AM	Chrome HTML Do...	27 KB
XXXXXXXX signed severance agreemen...	1/17/2016 12:32 PM	Chrome HTML Do...	11,290 KB
DRAFT - CONFIDENTIAL SEPARATION A...	11/16/2015 8:37 PM	Microsoft Word D...	41 KB
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX-CONFIDENTIAL SEPARATI...	8/24/2015 2:39 PM	Microsoft Word D...	43 KB
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX-CONFIDENTIAL SEPARATI...	8/24/2015 2:39 PM	Chrome HTML Do...	216 KB
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.docx	8/24/2015 10:03 AM	Microsoft Word D...	25 KB
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.pdf	8/24/2015 10:10 AM	Chrome HTML Do...	186 KB
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX-CONFIDENTIAL SEPARAT...	8/24/2015 2:24 PM	Microsoft Word D...	44 KB
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX-CONFIDENTIAL SEPARAT...	8/24/2015 2:25 PM	Chrome HTML Do...	215 KB
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.docx	8/24/2015 10:03 AM	Microsoft Word D...	25 KB
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.pdf	8/24/2015 2:26 PM	Chrome HTML Do...	186 KB

# THE DARK WEB IS DANGEROUS TERRITORY

But you are not alone. Let's design  
the right strategy and shield your  
business against Dark Web threats.

[dkeys@zypha.com](mailto:dkeys@zypha.com)

941.214.0150

[www.zyphausa.com/darkweb](http://www.zyphausa.com/darkweb)





# THANK YOU

DARRYL KEYS, PRESIDENT & CEO

[dkeys@zypha.com](mailto:dkeys@zypha.com)

941.214.0150

[www.zyphausa.com/darkweb](http://www.zyphausa.com/darkweb)