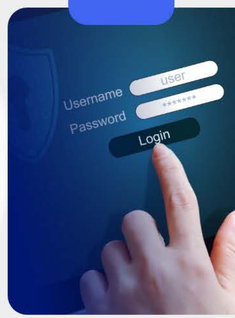
dARKWEBsteR

DARK WEB SLANG

CYBERSIXGILL GUIDE

JARGON OF THE DARK WEB

23 Must-Know Slang Terms for Cyberthreat Intel Professionals



cybersixgill

dARKWEBsteR
DARK WEB SLANG

TABLE OF CONTENTS

cybersixgill

dARKWEBsteR
DARK WEB SLANG

INTRODUCTION

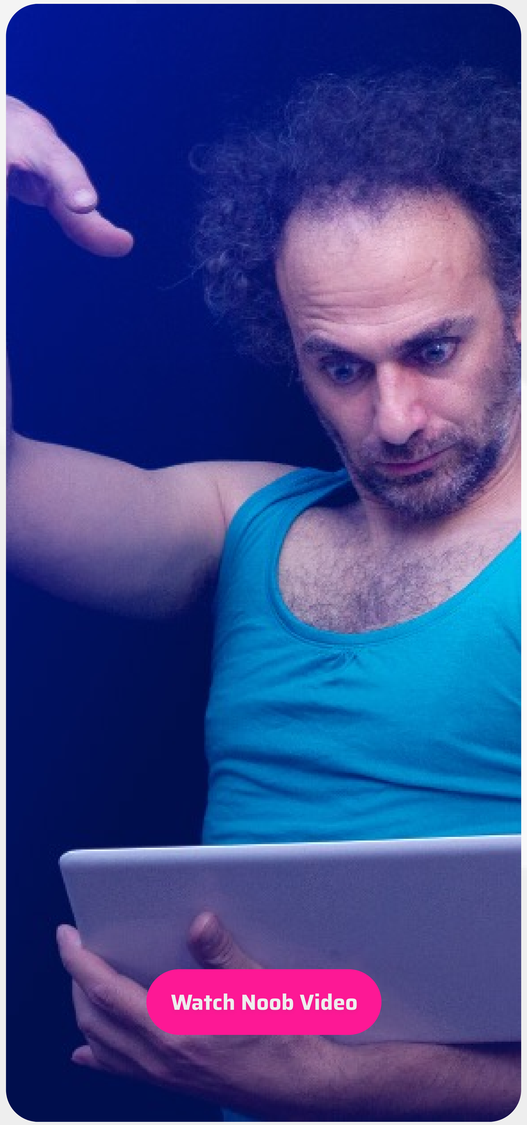
In the fast-moving field of cyberthreat intelligence, it is critical to keep up with the latest jargon. Content from the deep and dark web—sometimes referred to as **underground sources**—is a valuable source of information that companies and organizations can use to protect themselves from bad actors. By understanding the key slang and other vocabulary used within underground forums, cybersecurity professionals can empower themselves to understand who on the dark web is a threat actor, what messages they mean to convey, and how serious of a threat they pose.

But keeping track of these terms can be difficult and time-consuming. You don't really know which words to look for. And if you do come across an unfamiliar term, you need to see it used in several different contexts before you understand its true meaning and significance.

That's why we at Cybersixgill began running #DarkWebster, a weekly initiative to help our social media audience get up to speed with the latest terminology used frequently on the dark web. Now, we are happy to offer you this guide to 23 of the key terms we have featured since starting #DarkWebster.

We invite you to take a look at the terms covered in the following pages to test your own knowledge of the key terminology used on the dark web, fill in any gaps in your awareness, and make sense of the interactions taking place on underground forums.

Most importantly, we'd like to encourage you to use these brief and informative entries to acquire the vocabulary you need in order to search for, find, and understand relevant cyberthreat intelligence on the deep and dark web.



dARKWEBsteR
DARK WEB SLANG

NOOB

Short for newbie, a noob is simply a beginner, especially with regard to some aspect of computer technology – someone just starting to do something, such as frequenting the dark web's underground forums. Of course, whether we're novices or experts today, at one point each of us was a noob.

If you still consider yourself a noob when it comes to cybersecurity and the dark web, then #DarkWebster can help you get up to speed on the slang you need to know in order to follow the latest trends. And if your dark web background runs a little (or a lot) deeper, this new initiative offers you a chance to test your vocab knowledge, refresh your memory, and fill in any gaps.

dARKWEBsteR
DARK WEB SLANG

SKID

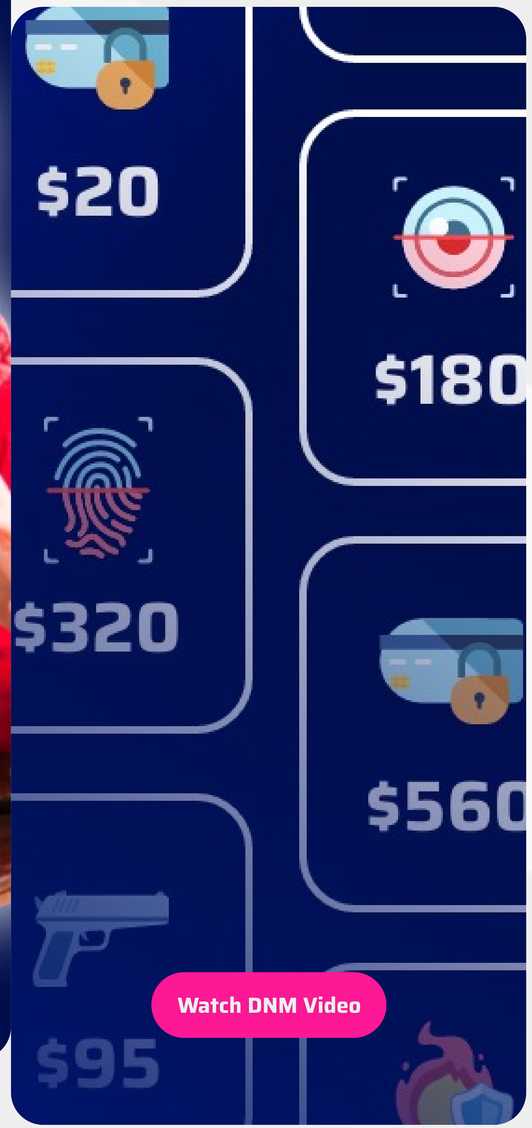
A *skid* (short for “script kiddie”) is someone who uses a malicious program without understanding how it works—a novice hacker.

Calling someone a *skid* in a forum is quite condescending. Whether or not they’d like to hear it, though, a majority of actors on the dark web could be considered script kiddies. Most of the people that we’re dealing with are not expert malware authors. So that sounds like a good thing for the defenders, right? Well, not exactly.

First, there is so much malware-as-a-service on the dark web, that skids can very simply amass a dangerous arsenal. You don’t really need to know how to create the weapon in order to buy it and use it.

Second, skids can be reckless. While state actors and expert hackers carry out attacks slowly and deliberately to avoid being detected, skids don’t really care. They just throw everything they’ve got until something works.

And finally, skids can grow up. Actors can begin their journey on the dark web as **noobs** and skids, but after immersing themselves in its many hacking tutorials and building relationships with more advanced actors, they can become far more skilled and dangerous.



dARKWEBsteR
DARK WEB SLANG

DNM

A *DNM* (which stands for “dark net market”) is an underground site devoted to buying and selling the kinds of goods and services for which the dark web is notorious.

Sites on the dark web fall into a few categories: You have forums, which are message boards based on specific topics and subtopics—think something like Reddit, but dedicated to hacking or malware or fraud. Then there are markets, which are product-oriented, with sellers and buyers.

Dark web markets sell just about anything, and these goods are mostly illegal. You’ll find plenty of narcotics and weapons, as well as compromised accounts and counterfeit items. You’ll also find exotic animals, as well as suddenly in-demand items: during the initial COVID outbreak, we saw some hospital ventilators and even a few alleged COVID vaccines for sale. Pro-tip: do not buy those vaccines.

Perhaps the most popular market type is credit card markets, which focus on selling stolen credit cards. In 2020, Sixgill found over 102 million stolen cards for sale on these markets.

Due to the illegal nature of these items, transactions take place in cryptocurrency, which is anonymous and harder to track, though not impossible.

dARKWEBstER
DARK WEB SLANG

RIPPER

A *ripper* is a scammer on a dark web market—someone who takes the money without delivering the goods, who rips people off.

Potential buyers are very concerned about rippers. They can't exactly file a police report that their crystal meth didn't show up as described. And they can't cancel the credit card charge, because they paid in bitcoin. So how do buyers know that they'll get what they purchase?

In order to instill confidence in potential buyers, dark web markets employ some of the same mechanisms that we're familiar with on ecommerce sites such as eBay, Amazon, and AliExpress. Sellers have ratings and feedback, so prospective buyers can check those before purchasing. And market administrators can be actively involved in dispute resolution. They have an interest in buyer satisfaction.

Finally, known and respected actors can also vouch for someone—I know this guy. Trust me to trust them.

Even so, it's not unheard of for someone to build up a solid, positive reputation in a market, and then one day stop delivering orders and vanish with the proceeds. So if you're considering buying something from a dark web market, buyer beware—it's against the law, and you might fall victim to a ripper.

dARKWEBstER
DARK WEB SLANG

ESCROW

Although the term *escrow* is far from new, it has been given a new meaning in the context of the zero-trust environment of the dark web, where it can help buyers maintain their confidence when purchasing goods and services.

According to the internet, the word "escrow" dates back to the 11th Century, from the Middle English term "escrowl," meaning, a "scroll," which was used to record the terms of a transaction. Nowadays, it refers to a third-party individual or account that receives and disburses money according to a contract between two parties. Usage of this financial mechanism goes back to the 1930s.

On the dark web, there are many escrow services that provide something quite basic. A buyer pays into an escrow account, and once the buyer confirms receipt of the goods, the escrow account transfers the payment to the seller. The buyer buys in confidence, the seller calms the fears of the buyer, and the escrow provider takes a fee.

Escrow services are offered by many dark web markets, and there are also many individual actors that claim to offer them as well. But be careful—an escrow provider can also run off with your money, so you still need to know who to trust.

dARKWEBstER
DARK WEB SLANG

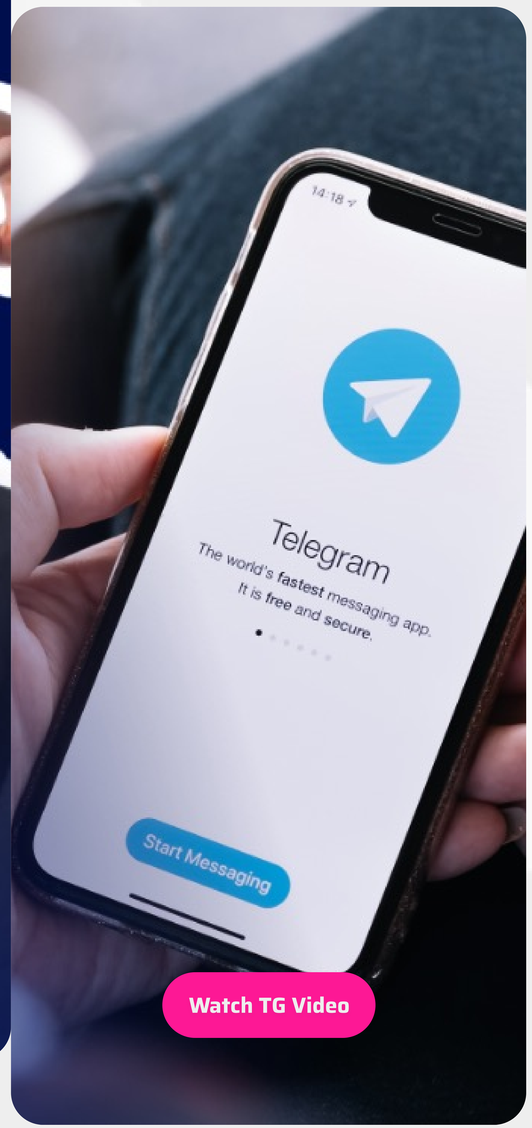
EXIT SCAM

An *exit scam* occurs when a dark web market simply vanishes, keeping all of the fees and payments in escrow. Actors can make quite a load of money in exit scams.

Dark web markets can exit scam for several reasons. The admins could have planned to do it all along, or maybe they just got tired of running the site and wanted to call it quits in a single supernova of scamming. Or maybe competing markets were biting into their sales, or law enforcement was about to seize them, and they wanted to pull out their proceeds before they went out of business.

Whatever the reason, we've seen some very high-profile markets exit scam over the last several years. Reports are that several of these have netted over $10 million each in cryptocurrency.

When a prominent market shuts down, we observe a noticeable dip in overall items for sale on the dark web, but soon after, other markets step in and fill the vacuum, so the volume of items for sale is restored.



dARKWEBstER
DARK WEB SLANG

TG

In the context of online threat intelligence, *TG* stands for Telegram, the popular messaging app.

In ancient times—like five years ago—most underground cybercrime took place on what's called the dark web—sites only accessible with the Tor browser, which have a .onion extension. This is because Tor has been considered the gold standard of an anonymous, secure platform.

However, cybercrime has spread out to all sorts of messaging platforms over the last few years. Many dark web posts conclude with "PM me on Telegram." And we see some massive groups on Telegram with topics such as financial fraud, narcotics, malware, and terrorism. Why has cybercrime spread beyond the dark web?

We'd argue that it's simply more convenient. Everyone has a smartphone, and these apps are optimized for them. Creating the infrastructure is easy—it's much simpler to open a new Telegram group than to build a new website. And there's built-in encryption, so it's fairly secure. However, there are drawbacks. There's a certain loss of control when setting up a shop on a messaging app. The app providers can shut it down instantly and without warning, banning all users and erasing chat history. Also, unlike dark web forums and markets, which are actively moderated, a Telegram chat can be more of a free-for-all, making it harder for users to follow and to trust other users.

DB

No surprises here: *DB* is short for “database.” You can also find databases referred to as “bases,” “leaks,” “dumps,” and “collections.”

Actors share all sorts of stolen databases on the dark web, and they can include personal details of millions of users, including names, contact information, dates of birth, and passwords. These databases are generally from websites, so we can presume that actors procure the data from servers that were misconfigured or improperly secured.

Sometimes these databases are sold, but very often they are just given out for free for anyone to download from an underground filesharing site. Once this happens, all of the personal information is out there, and any actor can use it for account cracking, social engineering, and identity theft.

How do you stay protected? If you’re an individual user, make sure to share your personal information selectively. And if you’re a cyber practitioner, please, please secure your customers’ data and make sure that you’re monitoring the dark web for leaks of your DB just in case something went wrong.

dARKWEBstER
DARK WEB SLANG

LE

Another key acronym of cyberthreat intel: *LE* stands for “law enforcement.”

Dark web actors are highly aware that their activities are illegal. They are concerned about being caught, and thus suspicious that their fellow forum users are actually undercover law enforcement agents. More advanced actors practice high levels of operational security, just to make sure that nobody will uncover their true identities.

A few months ago, I noticed a post on a forum related to money laundering, which concluded with an odd sort of disclaimer that if the FBI was investigating, the actor wasn’t actually involved with the scheme that they were posting about. Now, I’m a cybersecurity researcher, not a federal investigator, but I highly doubt that this type of language would remotely stand in a court of law. So why did they write it?

Digging deeper, I saw that this disclaimer became extremely popular on the forum. A lot of actors suddenly began to include it in their posts. I also found some chatter between actors fearing that the FBI had begun to investigate the forum. Turns out, someone started it all as a joke, but the suspicion about law enforcement turned into outright paranoia.

dARKWEBstER
DARK WEB SLANG

DOXING

Derived from the word “documents,” *doxing* is publicly exposing an adversary’s real-world personal details, which can include names, addresses, and contact information. It’s a significant form of harassment that really undermines why so many actors use the dark web—the ability to remain anonymous.

Doxing is a popular form of retaliation, and it’s used by gamers, hacking groups, and sellers on markets against their foes.

Once a target’s real-word details are exposed, they can be bullied by the internet mob, questioned by the media, or investigated by law enforcement. It can get very ugly. Because dark web actors are often engaged in highly illegal activities, being doxed can mean game over.

On the dark web, we find doxes of users, and we also find doxing-as-a-service offered by threat actors.

dARKWEBstER
DARK WEB SLANG

L33T

Dating back to the 1980s, *L33t* (also spelled 1337) is short for “elite,” as in an elite hacker.

This form of spelling is called L33tspeak, and it’s the pseudo-language in which these l33ts communicate. It basically involves replacing certain letters with numbers or symbols. For example, the letter O becomes the number 0, and the letters “and” (or other combinations of letters that sound like the word “and”) can be replaced with the ampersand symbol (&). So “banned” becomes “b&.”

It also involves new words, such as “pwned,” which is derived from the word “owned” and means taken over.

L33ts communicate in this way for two reasons. First, it’s to separate themselves from the *n00bs*, to show that they have *skillz* and expertise. Second, it’s to be able to articulate new concepts created by their internet, hacking, and gaming subcultures.

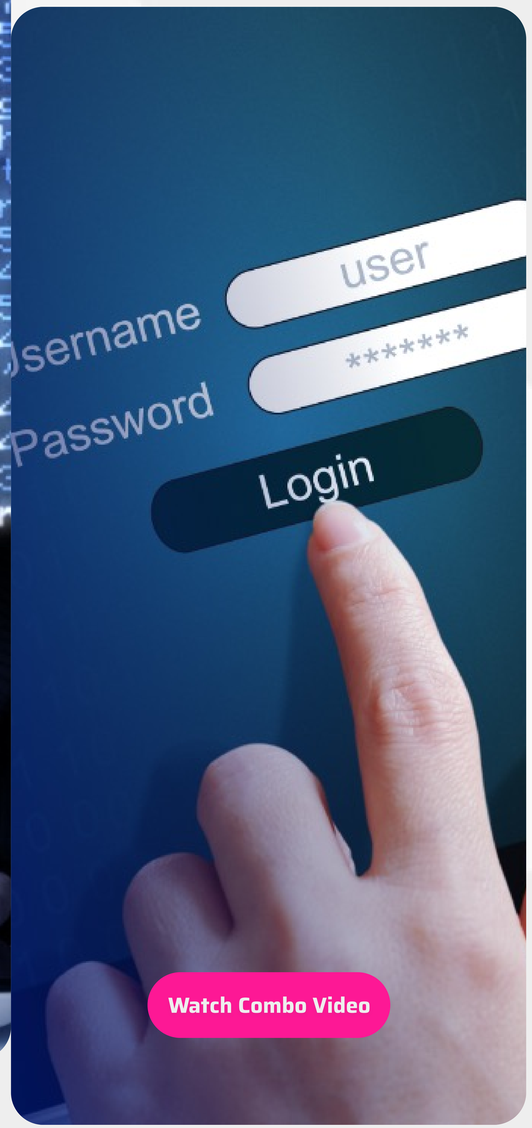
L33tspeak directly contributed to dark web slang, enabling those in the know both to distinguish themselves from everyone else and to explain new types of schemes and tools.

dARKWEBstER
DARK WEB SLANG

CRACKER

Simply put, a *cracker* is a program that cracks passwords. Crackers can use numerous techniques, from dictionary attacks to brute forcing to credential stuffing. Since many leaked credentials include passwords that are hashed, there are crackers that attempt to reverse hashes using rainbow tables. Anyone who logs in to the dark web has many options for crackers of all shapes and sizes.

Also worth noting: The term *cracked* is also more generally used on the dark web to refer to something that has its security bypassed. So a cracked password is one that's been figured out, and cracked software—also widely available on the dark web—is software stripped of DRM protection.



dARKWEBstER
DARK WEB SLANG

COMBO

Short for "combination," a *combo* is simply a leaked username and password. Dark web actors publish or sell massive combolists, sometimes containing tens of thousands of breached credentials.

Why is this so harmful? The primary tactic employed by dark web actors for account compromise is credential stuffing. This method involves taking previously breached credentials and testing them out against different services. Since people tend to recycle passwords, if I try someone's Yahoo address and password in Netflix, I just might be able to log in. I also might be able to get into their bank account.

The most important thing an attacker needs to attempt credential stuffing is usernames and passwords. Once the combos are out there, anyone can try them out against any service and possibly access private accounts.

How do you stay protected from credential stuffing attacks? The answer is straightforward and unexciting. Don't recycle your passwords. Use unique, complex passwords for everything. Use a good password manager to stay in control. Otherwise, once one of your accounts is compromised, that combo could be posted to the dark web, and then all of your other accounts may be cracked as well.

dARKWEBsteR
DARK WEB SLANG

CHECKER

How do attackers figure out which **combo** works with which service? How do they take a list of 10,000 usernames and passwords and determine which ones work on, for example, Disney+?

Most of these logins aren't valid. If attackers had to check those accounts one by one, they'd have to be pretty persistent until they got lucky.

Fortunately for the bad guys, this can be automated by a program called a *checker*. You simply load a checker with a combolist, and the checker checks all of the combos against the targeted service, and reports which ones generated an effective login.

Some checkers, like OpenBullet, are generic and can be used against any service of the user's choice with the proper *config*, or configuration file. Others are more specific, like several checkers that we found that target PayPal accounts.

Checkers have various levels of sophistication. Some can also scramble their traffic through proxies, so it doesn't look like all of the login attempts came from a single source.

dARKWEBsteR
DARK WEB SLANG

FULLZ

Derived from the word "full," *fullz* refers to a full stolen identity package. This will generally include the victim's name, address, date of birth, social security number, and phone number. It can also contain credit card information.

Unfortunately, there are quite a lot of fullz transacted on the dark web. Actors sometimes sell them in packages of hundreds of thousands. They can be general fullz, or specific to a country or US state.

Once an attacker acquires fullz, they can do a lot of damage. They can call any account provider while impersonating the victim. Using the victim's information to "prove" who they are, they can convince the account provider to reset the password or to transfer funds out of the account. In this way, an attacker can take over accounts and steal assets. The attacker can also open up new credit cards and withdraw loans in the victim's name. It's a real nightmare for the victim.

There are a lot of best practices out there to protect yourself from identity fraud. I recommend following them. **www.USA.gov/identity-theft** is a good place to start with an informative, practical checklist.

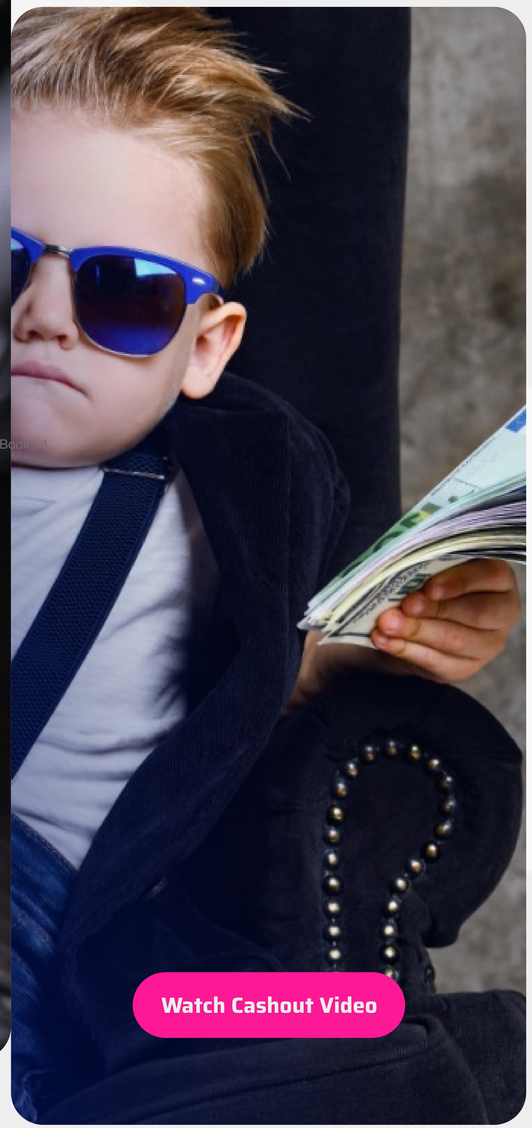
dARKWEBsteR
DARK WEB SLANG

GENERATOR

Let's say that you're a threat actor, and you want to open up some accounts on eBay, Facebook, Gmail, or any other service. If you're up to something fraudulent, then the accounts that you're using will likely be shut down quickly. So you need a lot of them.

That's where a *generator* comes in. A generator is a software tool, available on the dark web, which is used to automatically open accounts. With it, an actor can set up accounts in bulk and use them or even sell them. More advanced account providers have methods of preventing this type of activity, such as using CAPTCHA or requiring additional personal information to sign up.

There's another way that generators are used: to generate serial numbers. If something such as a gift card or software key uses a serial number that is enumerable, meaning, following a logical pattern that can be figured out, you can be sure that threat actors are using number generators to find valid codes. With them, they can unlock gift cards and use software without paying. So obviously, providers need to ensure that their serial numbers are harder to figure out.



dARKWEBsteR
DARK WEB SLANG

CASHOUT

Let's say that an actor manages to take over a financial account that contains some funds. How do they get that cash into their pockets?

Withdrawing or transferring money from a compromised account is known on the dark web as a *cashout*. Cashing out is not so simple. Financial accounts use advanced algorithms in order to detect and prevent fraudulent transactions.

Thus, it's a constant game of cat and mouse between the financial services and the fraudsters. The bad guys are always seeking new ways to circumvent the protective measures.

To these ends, there are actors on the dark web offering cashout services. For a cut of the proceeds, they offer to move funds out of a compromised account. Because cashing out requires advanced abilities, these services are at a premium. For example, one cashout service that I found demands a minimum amount of $10,000 and takes a 45% cut of the proceeds. So, for a threat actor, gaining access to an account doesn't necessarily mean that they'll pocket the total balance contained within.

dARKWEBsteR
DARK WEB SLANG

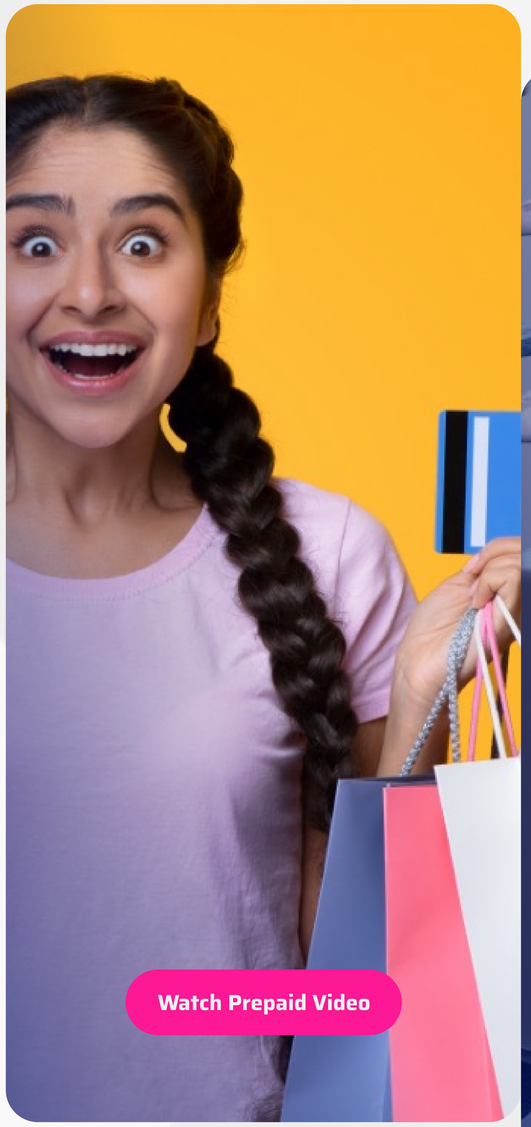
PREPAID

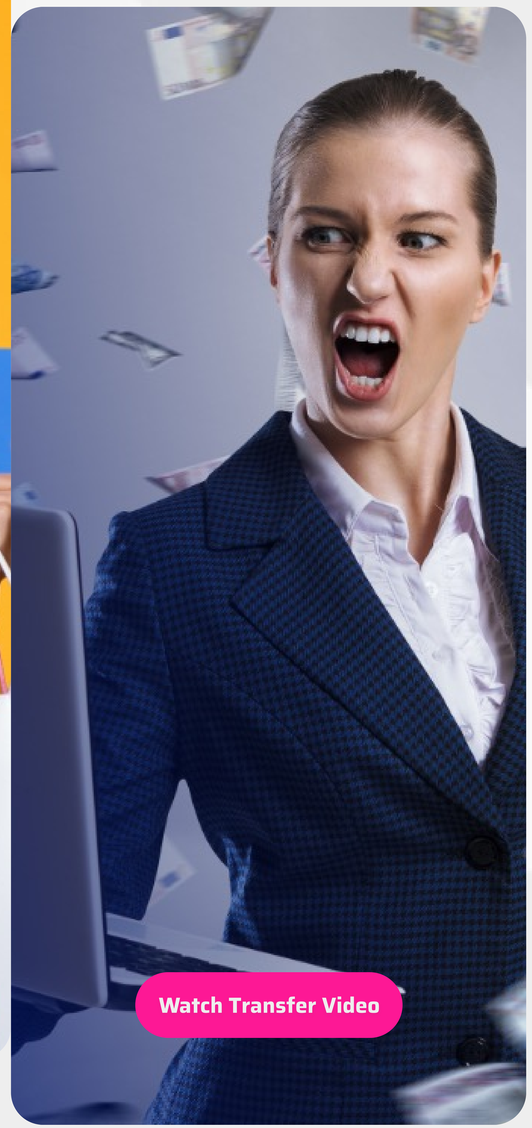
A *prepaid* is a gift card or a debit card with a fixed balance. Gift cards are an important tool used in money laundering, since they can be purchased with dirty money without much identification, and then are used to store funds and to make purchases that appear legitimate.

Because they are a physical product, like cash, it's harder to follow the money. They can be smuggled in suitcases without leaving an electronic trail.

Therefore, unsurprisingly, prepaids are important in the dark web economy, as they are one method used by actors to cash out accounts and move funds. Many actors sell and buy them in bulk.

Also, while credit cards have many security measures, including name, expiration date, CVV, and EMV chip, prepaids do not. This makes prepaids far more susceptible to cloning, in which a compromised point-of-sale terminal or ATM copies the magnetic strip, and then a new card is printed with the same data. There are, also unsurprisingly, tons of cloned prepaids for sale on the dark web.





dARKWEBsteR
DARK WEB SLANG

TRANSFERS

For many cybercriminals operating on the deep and dark web, executing a *transfer* (of funds) can be a major challenge. They often turn to transfer services, which receive funds from one account and transfer them to another account, allowing the criminal actors to obfuscate the origin of stolen funds and move them worldwide. These services operate specifically with regular currency, and each specializes in different payment platforms, such as PayPal or Cash App.

Operators of transfer services need to have intimate familiarity with antifraud mechanisms and the technical capabilities needed to avoid them. They channel money through aged, experienced accounts or compromised third-party accounts. They require patience, transferring smaller sums over time as opposed to a massive transfer that may be flagged and blocked.

And these services use remote-access tools to mask location. Some of them only operate within specific countries, indicating the importance of avoiding suspicion through maintaining a geographic presence, whether actual or virtual (enough to convince anti-fraud mechanisms).

With all of this complexity involved in executing transfers, dark web transfer services are premium, generally incurring fees of 33%.

dARKWEBsteR
DARK WEB SLANG

LOGS

Logs are valid, verified usernames and passwords, generally for financial accounts.

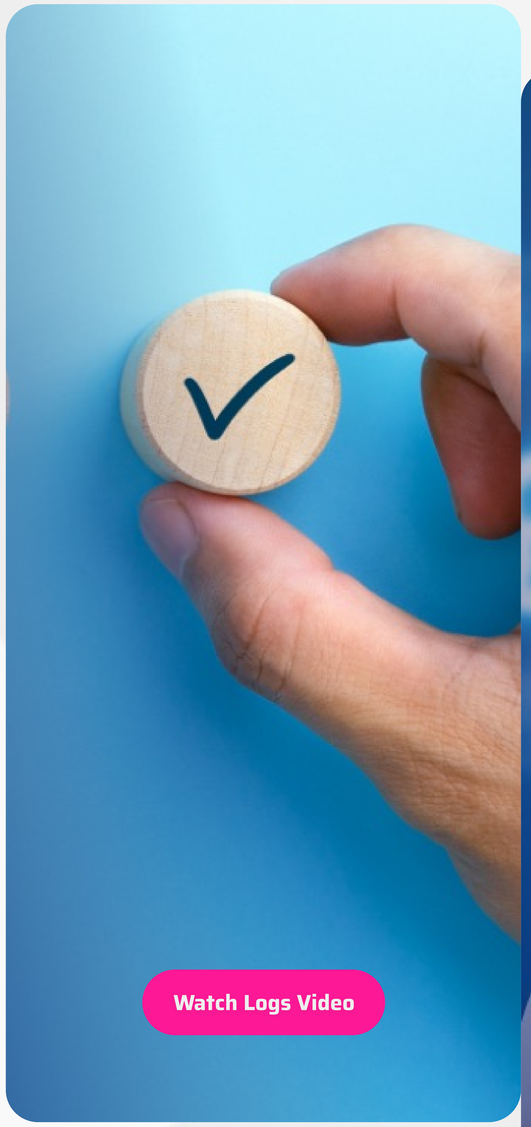
This is to distinguish them for combos, which are generic username and password combinations. An attacker needs to run combos through a credential stuffing tool until finding valid logs for specific accounts.

Since logs are verified and potentially contain access to funds, they are obviously more valuable than combos.

Credential stuffing is not the only way to discover logs. Attackers also get them through phishing or through banking trojans such as Trickbot.

If an actor discovers a log for a financial account, they can do a cashout. But if they find that to be too difficult or too risky for reasons that we've discussed over the last few weeks, they can still sell the logs on the dark web.

Logs sell on the dark web for single dollars into the hundreds, depending on the account type and level of verification. Sometimes they're sold one by one, and other times by the thousands. So there's quite a lot of money to be made just selling the logs.



dARKWEBsteR
DARK WEB SLANG

EXCHANGE

An *exchange* on the dark web is like a currency exchange in the real world. It allows actors to exchange currency from one form to another, or, more often, to exchange fiat into cryptocurrency.

Converting fiat into cryptocurrency is an essential step in money laundering. It allows actors to move money from a financial account, which is monitored and regulated, into cryptocurrency, which can be effortlessly moved across wallets and borders.

On the flipside, converting cryptocurrency back into fiat is a way for actors to actually buy something with their winnings. Until real estate agents and luxury car dealerships accept bitcoin as payment—and I know, many people say that will happen—actors will need to switch their crypto into their local currency so they can flaunt just how much money they stole.

dARKWEBstER
DARK WEB SLANG

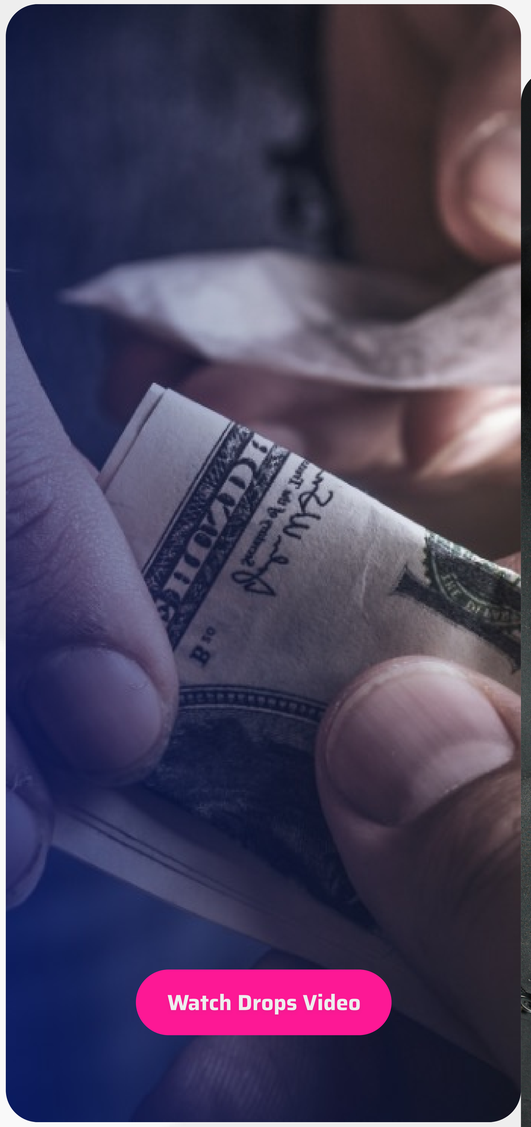
DROPS

When bad actors want to obscure the real origin of something specific (either a sum of money or a physical item), they often use *drops*.

An item drop is a physical location where contraband, such as narcotics, can be sent before it is distributed or forwarded somewhere else. Similarly, a drop account is a financial account to which money is transferred. The funds are physically withdrawn and then deposited into a new account. This way, there's no digital connection from one account to another.

By using these two types of drops to hide the origin of a certain object, threat actors can effectively remove the kingpin another step from the crime, complicating law enforcement efforts and increasing plausible deniability. Therefore, advanced financial crime groups have a wide network of drop accounts, enabling them to execute larger and more complex schemes.

Also worth noting: In dark web slang, a money mule—the pawn in this game who withdraws and moves the cash—is known as a *cashier*. Actors frequently post that they are looking for cashiers in specific locations, generally low-level operatives who are unaware of the larger schemes in which they are involved.



dARKWEBstER
DARK WEB SLANG

HOLDER

As we have seen, much dark web jargon surrounds the difficulties cybercriminals face when they want to move fraudulently obtained money into their own pockets. Cashing out an account is difficult—actors need to find transfers, exchanges, drops, and cashiers.

But there's one way threat actors can avoid those challenges entirely: by finding a *holder*. A holder is simply an account operated by someone else that first receives the fraudulent money. For example, let's say that you're running an eCommerce scam site in which you encourage payment for products that you simply don't ship. Instead of having to worry about how to open, for example, a PayPal account to accept the payments or deal with credit cards—all of which could involve complications—you simply have the site's proceeds paid directly into the holder's account. The holder takes a cut and transfers the rest to you, maybe even after they exchange it into bitcoin.

In this way, holder services further simplify the complex process of getting money from the victim to the attacker's pocket.

cybersixgill

ABOUT CYBERSIXGILL

Cybersixgill's fully automated threat intelligence solutions help organizations fight cyber crime, detect phishing, data leaks, fraud and vulnerabilities as well as amplify incident response – in real-time. The Cybersixgill Investigative Portal empowers security teams with contextual and actionable insights as well as the ability to conduct real-time investigations. Rich data feeds such as Darkfeed™ and DVE Score™ harness Cybersixgill's unmatched intelligence collection capabilities and deliver real-time intel into organizations' existing security systems. Most recently, Cybersixgill introduced agility to threat intel with their CI/CP methodology (Continuous Investigation/Continuous Protection). Current customers include enterprises, financial services, MSSPs, governments and law enforcement entities.

Learn More

For more info contact our marketing team
at marketing@cybersixgill.com

cybersixgill.com