
Illuminating the Dark Web - SMFS, Inc. dba GRIMM
GRIMM
HTTPS://GRIMM.RIP
DEMYSTIFYING
THE
DARK WEB
JOHNNY XMAS
SR. SECURITY RESEARCHER
&
SR .TRAINER
SMFS, INC. (GRIMM)

JOHNNY XMAS

GRIMM.rip

Sr. Security Researcher & Sr. Trainer

SMFS, Inc. d/b/a/ GRIMM

Illuminating the Dark Web - SMFS, Inc. dba GRIMM

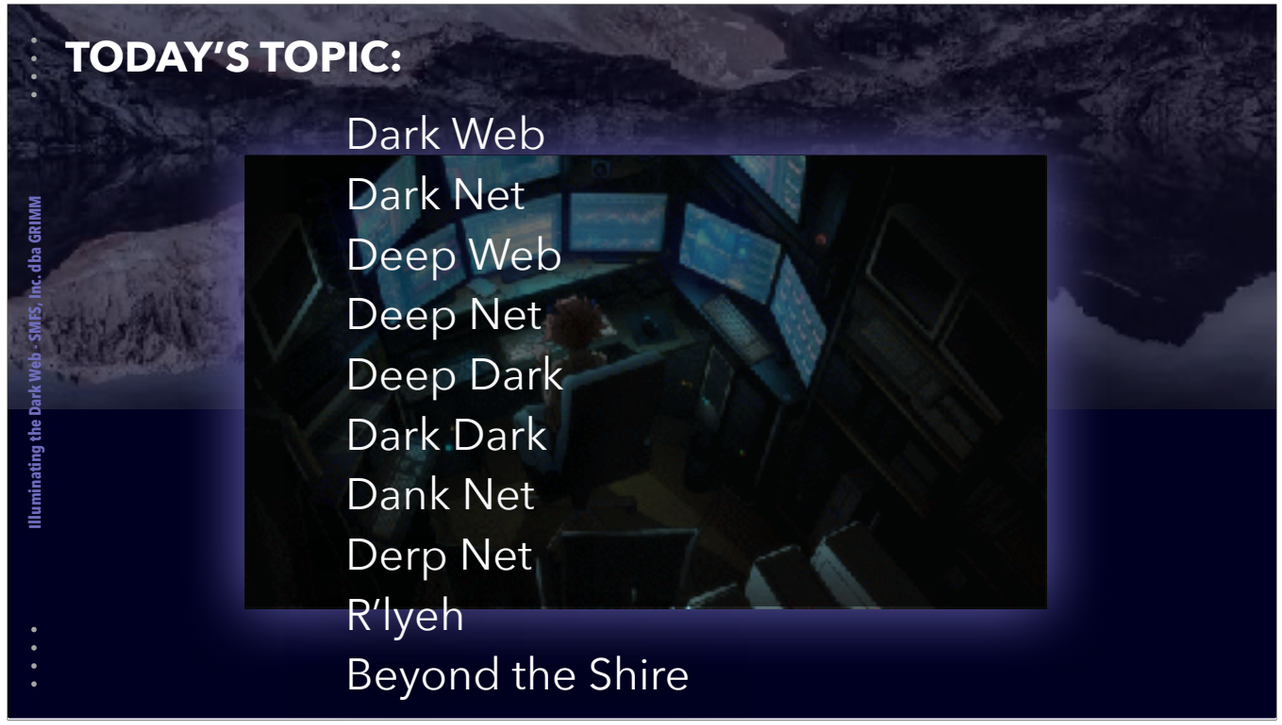
PREVIOUS PROFESSIONAL ROLES:

- Network Engineer
- Systems Engineer
- Information Security Engineer
- Information Security Consultant
- Penetration Tester
- OT Researcher
- Blade Runner (Bot Killer)

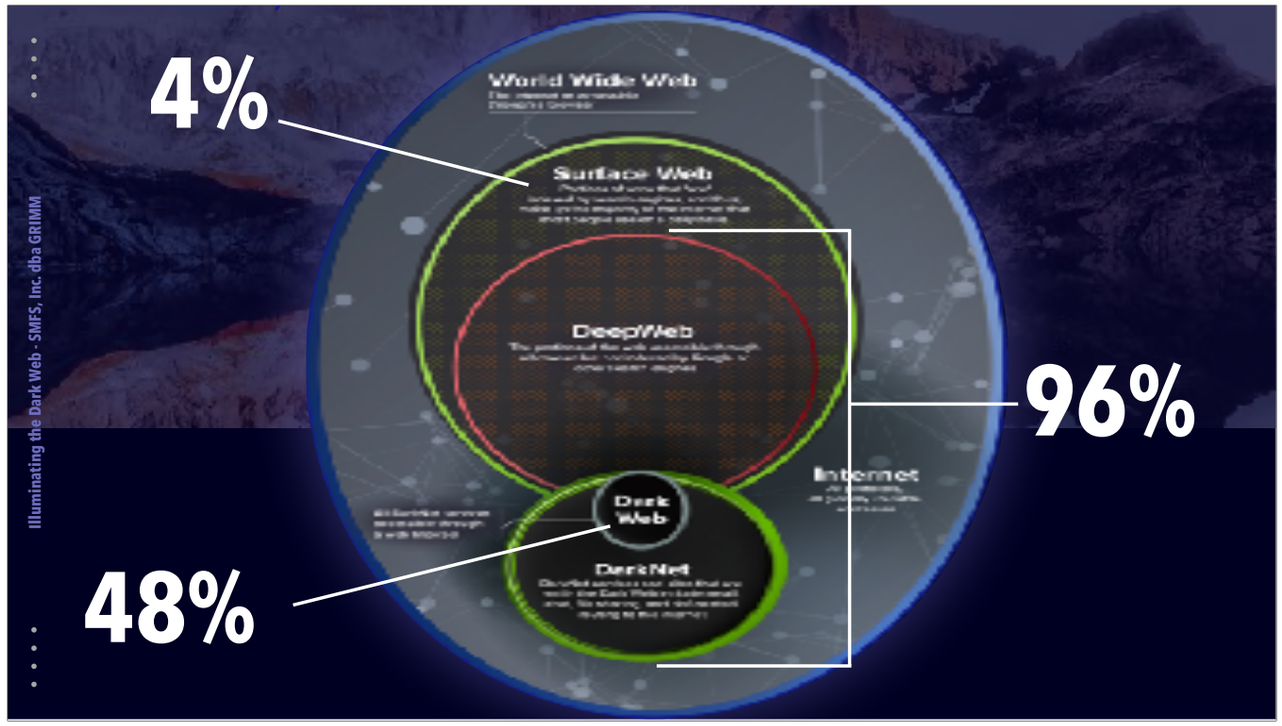
LINKS:

- https://grimm.rip
- https://github.com/johnnyxmas
- https://linktr.ee/johnnyxmas

JohnnyXmas@grimm.rip



Today we're going to talk about something that has been called a thousand names by a thousand media outlets: The Dark Web. Looking at this list scrolling by it's easy to think that many of these names are just someone misspeaking, or concurrently-generated titles for something which inherently has no real name. While that's certainly true for a small number of them, many of these terms actually refer to entirely different things, and we need to briefly cover what those things are in order to understand exactly what, and where, the Dark Web actually is.



Cover each circle starting with Internet and working inwards.

* Discuss how circles aren't proportional, as the Dark Web has grown MASSIVELY in recent years

The deep web which stores around 7,500 TB of data, the surface web stores a mere 19TB which is equivalent to around 980,000,000 websites. It's impossible to tell exactly what all of this data is attributed to, but given the simplicity of most dark web sites, we can imagine very scary answers to this not-very-fun thought exercise.

OK now we've got to go down the exceptionally-complex rabbit hole of connecting to the Dark Web and making sure we don't get caught. Here's an example of how the overly-cautious are going to recommend you do it:

*AFTER BRAVE, GO BACK TO VPN + TOR

Let's talk a little bit about the Tor protocol and how browsers leverage it.

If you're interested in online privacy and anonymity, you've probably heard of Tor. To many, Tor is the basis of true freedom on the internet. But what is Tor exactly? How does it work and why would you use it?

The Tor browser is one of the most important tools to guarantee anonymous and free browsing on the internet, and of course, the dark web. Tor gives you access to this dark part of the internet, but you shouldn't try to access it without knowing exactly what you're getting yourself into. That's why, before telling you more about Tor, I need to run you through some measures you can take to stay safe while using the Tor browser, especially when visiting the dark web.

First of all, make sure to check Tor's security settings. Tor uses a very effective and reliable system of data encryption, as we'll see in a bit. Even so, using Tor's security settings can make your online experience much safer. Secondly, even though this might be quite obvious to many, it's important to never visit websites and click on links you don't trust. Of course, this is something you should keep in mind regardless of the browser and safety measures you're using. Lastly, we recommend you use a good and secure VPN, or virtual private network.

Using a VPN at the same time as Tor ensures your data is encrypted beyond what Tor provides. Moreover, the VPN also hides your IP address by displaying the IP of the VPN server you're using rather than your "real", static IP-address. Using one of the many cheap anonymous VPN providers you've no doubt seen ads for then ads another layer of anonymity to everything, pending they are in fact truly anonymous.

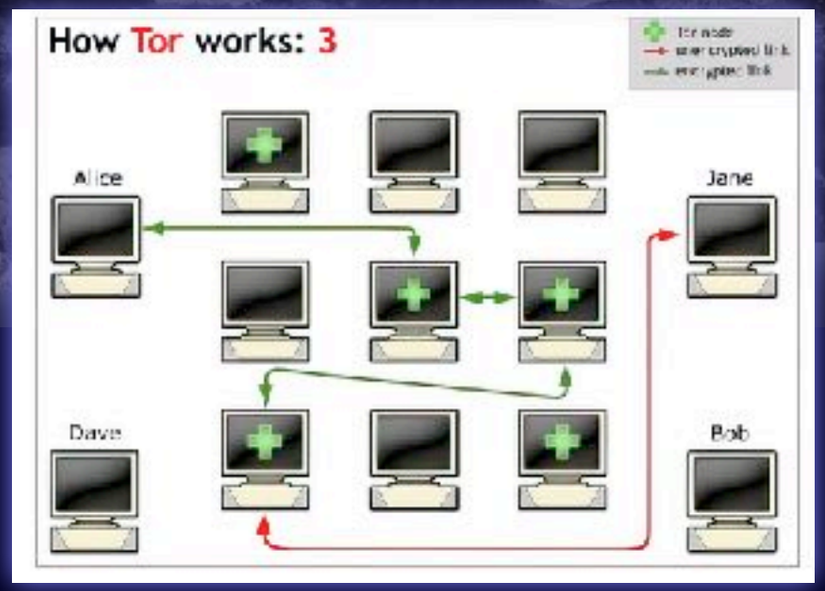
Though Tor's developers originally created the protocol for military purposes, it has developed into a tool that can be useful to all – especially to those who have something to hide or will otherwise benefit from online anonymity. Many political activists use it to avoid being prosecuted. Usually, these people live in countries where authorities might punish them for the thoughts and views they wish to share online.

Similarly, journalists use Tor to protect their sources. If a source does not want to risk being revealed, they can communicate sensitive information through the browser. Not just suppliers of information, but also consumers are to be found on Tor. Many people use it to access geo-restricted content, to bypass censorship and visit specific websites. After all, a lot of pages, such as those on the dark web, simply can't be accessed using a "normal browser" such as Chrome or Firefox.

Another well-known group of people who use Tor are whistle-blowers. For instance, one of Tor's most notable users and supporters is Edward Snowden, who revealed documents on classified surveillance programs in the US.

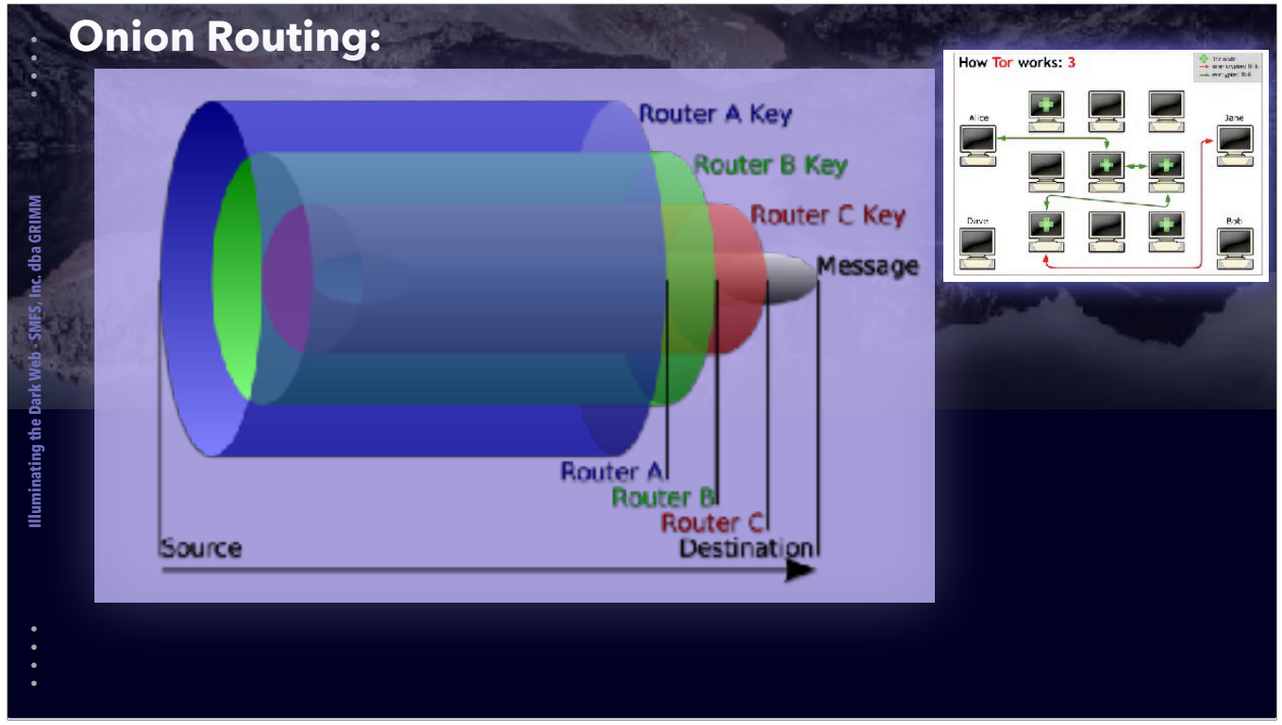
While all of this might seem very positive, not everyone uses Tor for what one might call "a noble cause". For instance, many hackers and cybercriminals use it to stay anonymous while conducting their illegal business. The anonymous browser is especially useful to criminals BECAUSE it provides access to the dark web. This dark part of the internet contains multiple illegal marketplaces such as the former Silk Road you may have heard about in the news long ago. I'm sure this is a primary topic you're concerned with, so we'll cover those marketplaces in depth later.

Tor Nodes \ “Routers”:



The team behind Tor (short for The Onion Router) provides free open-source software that helps you browse the internet anonymously. Originally the Tor network was developed with the help of the US navy. The network was developed to enable the US Navy and other military organizations to communicate anonymously online. These days, Tor mainly focuses its attention on its browser and the development of a few other privacy tools.

As we mentioned before, the Tor protocol greatly benefits your online privacy and, up to a point, your security. The browser makes use of the vast world-wide server network that the Tor network consists of. When using the browser, your data goes through different Tor Routers (or “nodes”), which are run by random individuals around the Internet who choose to host these nodes themselves; you too could even host one. The Tor protocol encrypts and routes your traffic as soon as you request a website by randomly selecting which nodes the traffic will pass through, exchanging a separate set of encryption keys with each one of those nodes, and then finally sending the request. The traffic is heavily encrypted and slowly decoded one layer at a time at the different nodes. The response from the remote server then does the same thing, including taking a different, randomly-selected set of nodes on the way back. This means that even if one of these nodes is compromised and the attacker is able to view the unencrypted traffic from inside the node, all they would see is that it cam from the previous node’s address, is heading to the next nodes address, and the actual request data is still encrypted with all of the nodes’ keys down the line so is unreadable. Unless the just happens to be on the first or last node in the random chain, they’ll just see a bunch of useless information. In fact, even if they ARE inside one of those nodes, they will still never even see the response to your request because it will take a different path back to you. In other words: this protocol makes it impossible, or at least very difficult, to identify its users.



Now I did gloss over the encryption mechanism earlier, but that's because I wanted to explain it a it more in depth, here. This diagram is an example of a message, say a request for Facebook.com, sent from your Tor browsers that will pass through 3 Tor routers we've called A, B and C. As I mentioned, your browser generates a unique set of encryption keys FOR EACH ROUTER, and then encrypts your message over and over again using each key in sequence, wrapping the message up like and onion. When your message gets to Router A, it decrypts that first layer, and all it gets from that is where to send the message next, and all the other information is still encrypted with Router B and C's keys, so not only can it not read your request, it doesn't even know about any future path beyond Router B. The message is sent off to Router B who does the same thing, peeling off the next layer of the onion. It then knows to send it to C, but can't read the encrypted request message, so it sends it. Finally Router C decrypts the message and sees you want to go to Facebook.com, and it says "OK," gets the site for you, and sends all of the site data back to your browser using this same method, but a totally different set of routers.

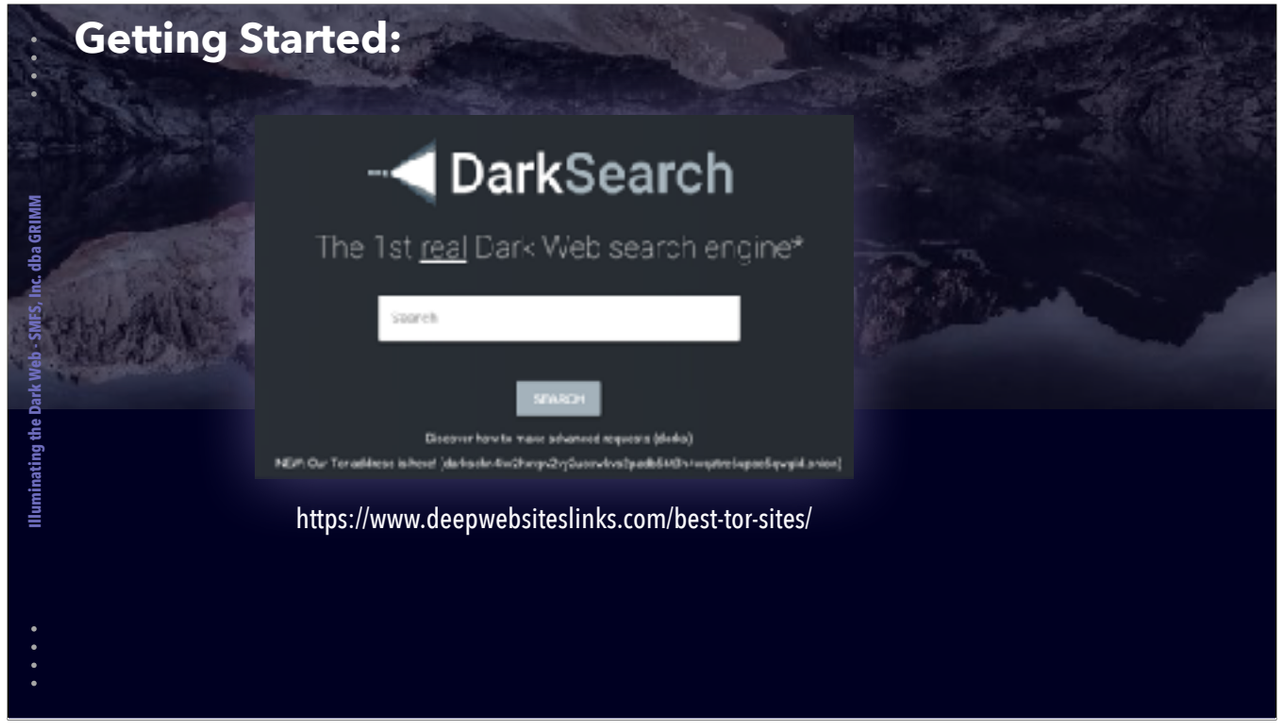
I realize this is a LOT to take in, and it can be hard for some to visualize this without perhaps seeing it in an animated form, but really it's not extremely important. All you need to know is the Tor protocol makes it nearly impossible for anyone to know who you are and what you're up to, at least as far as interception of the message on the fly goes.

NOW THAT we maybe sort of understand all THAT, and have everything we need to begin this dangerous journey, there is one extremely important thing we need to keep in mind as we begin:

Say it with me now.

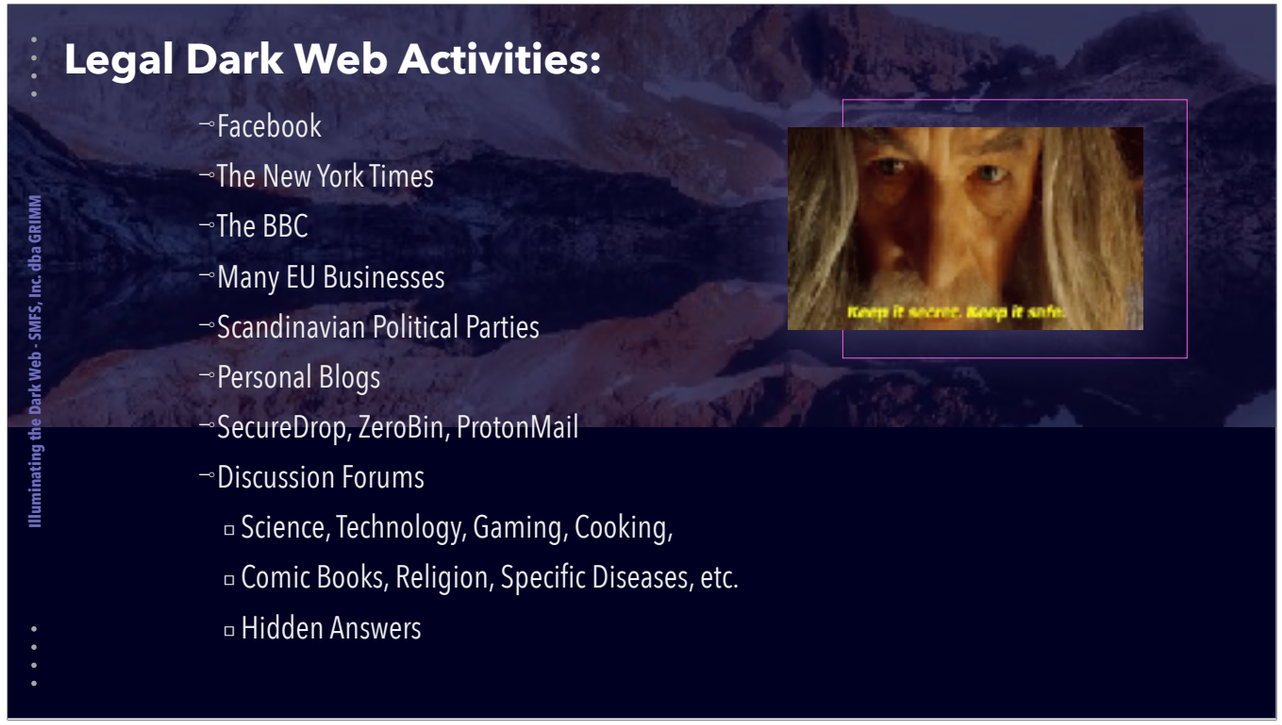
OK, cool so. . . .where do we start?

Getting Started:



https://www.deepwebsiteslinks.com/best-tor-sites/

DarkSearch.io is one of the better DarkWeb search engines out there, but there are many of them with varying degrees of accuracy, strengths and weaknesses. You're best bet for getting started my be just to throw down a Duck Duck Go search for "dark web site for (and whatever you're looking for), or even just look for some listicles like this link I've posted here.



Once you get going, you'll notice you'll actually find many major sites, especially major media outlets, have Onion sites you can visit. They do this to allow a means for those who are stuck in countries with oppressive regimes to still communicate and get access to information from the outside world.

Cicada 3301 is a nickname given to an alleged enigmatic organization that posted three sets of puzzles online between 2012 and 2014 to recruit codebreakers from the public. The first Internet puzzle started on January 4, 2012, on 4chan and ran for nearly a month. A second round began one year later on January 4, 2013, and then a third round following the confirmation of a fresh clue posted on Twitter on January 4, 2014. This may sound like I'm referencing ancient history, except that the third puzzle has yet to be solved. The stated intent was to recruit "intelligent individuals" by presenting a series of puzzles which were to be solved. No new puzzles were published on January 4, 2015. However, a new clue was posted on Twitter on January 5, 2016. Cicada 3301 posted their last verified PGP-signed message in April 2017, denying the validity of any unsigned puzzle.

The puzzles focused heavily on data security, cryptography, steganography, and internet anonymity.

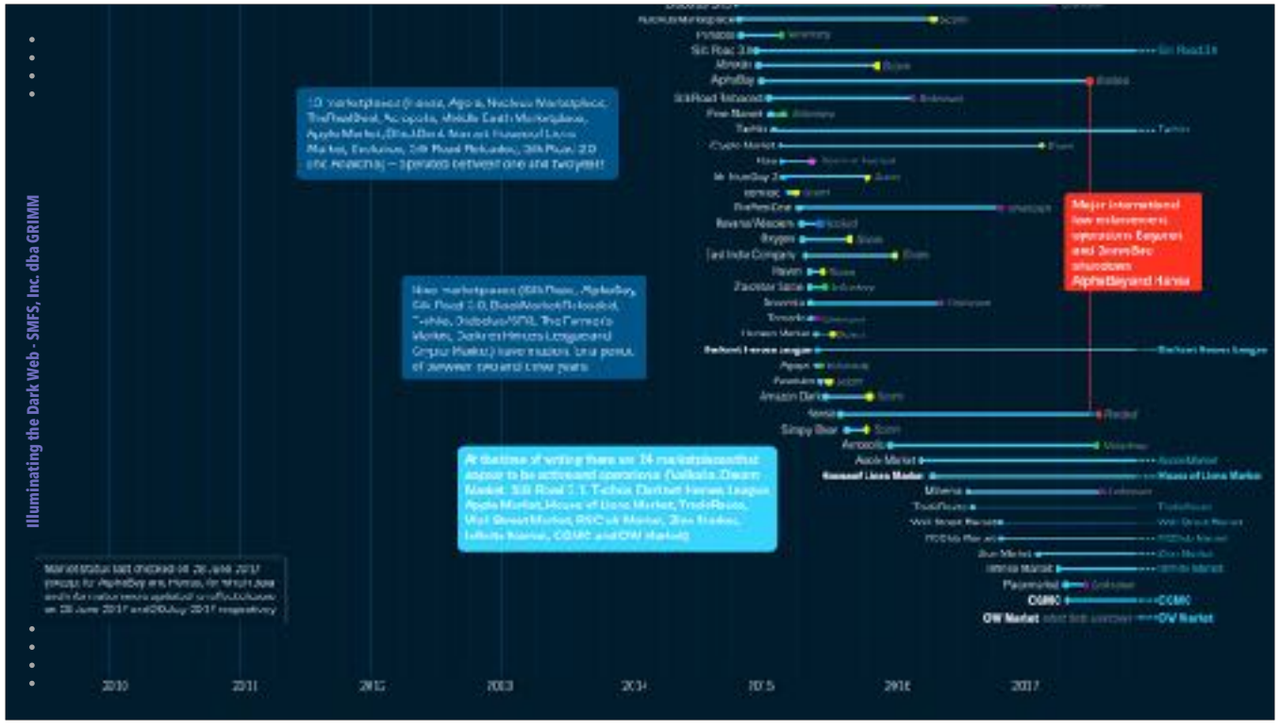
It has been called "the most elaborate and mysterious puzzle of the internet age" and is listed as one of the "top 5 eeriest, unsolved mysteries of the internet" by The Washington Post. Many have speculated that the puzzles are a recruitment tool for the NSA, CIA, MI6, a "Masonic conspiracy" or a cyber mercenary group.

The stated purpose of the puzzles each year was to recruit "highly intelligent individuals", although the ultimate purpose remains unknown. According to statements of several people who won the 2012 puzzle, 3301 typically uses non-puzzle-based recruiting methods, but created the Cicada puzzles because they were looking for potential members with cryptography and computer security skills, and many of the descriptions felt very cult-like. Either way it's a super cool puzzle some folks made that heavily leveraged the Dark Web.

Why Don’t we all Hang Out Here?

- Often slow
- Unreliable search engines and results
- Entire communities disappear overnight
- Scams / malware galore
- High risk of seeing things you didn’t want to
- Marketplaces are difficult to use

So with all this great, perfectly legal stuff, why does nobody we know actually hang out on the Dark Web?



Speaking of marketplaces:

This list I have here is a majority of the known Dark Web marketplaces along with the dates they were active and shut down. When we hear "the dark web" mentioned somewhere, most of the time its in the context of marketplaces and the purchasing of illegal goods. This is absolutely a massive aspect of the dark web, but accessing these markets is not without it's own challenges, not the least of which is actually finding one that is still functioning.

Some of these markets were shut down through joint government operations, and some were simply shut down by the teams who ran them. Because these marketplaces often offered escrow services for guaranteeing payment and product delivery, these shutdowns often meant any money users still had in limbo was immediately lost. In fact, sometimes these markets go down for that exact purpose, and the owners will split the money they stole. This is known as an "exit scam" Every yellow dot you see in this chart was an exit scam.

Marketplaces average a lifetime of only about 8 months, with the most enduring lasting up to 4 years, though that is extremely rare. Nearly all of the very largest marketplaces were gone within 2 years.

Anyway, At this point I'm sure you're saying "OK, great, whatever. . .but what's IN those marketplaces? Are all the things I hear really true? "

I don't know exactly what you've heard, but I can guarantee whatever it was the answer is "yes."

Marketplaces

- 67% of listings are for illegal physical contraband
- 17% are for Fraud / Counterfeiting (Mostly malware)
- “Empire” is the largest market currently
- Bitcoin, Litecoin & Monero are the common currencies
- Advances in online anonymity means more users
- Mystique has led to prices higher than the Clear Web.

Read first line, then:

Fraud and counterfeit listings were the next major category, accounting for 17% of marketplaces. It’s probably because of the fact that people give their personal information out so readily. Then, of course, there’s the wide availability of tools to allow data breaches as well. The dark web is a totally anonymous environment in which people can engage in illicit behavior without being caught.

Empire is currently one of the largest darknet marketplaces listing over 6,000 products.

Bitcoin, Monero, and Litecoin are accepted forms of payment. Once you pay, the money is held in Empire’s escrow and the goods are shipped to the buyer through a middle man who can be contacted by either party. Selling items on Empire actually requires a membership fee of $100.

The growth of anonymizing networks like tor (yes, there are others) has emboldened more people to go exploring, thus causing a boom in the dark web markets.

Dark web stats for 2021 show that Tor’s secured browser technology is the largest anonymizing network, with over 2 million active users connected directly to its service.

More than that, the bandwidth capacity of this network reaches over 300 gigabits per second. This indicates a massive growth, especially when compared to its 50 gigabits per second capacity in 2014.

Also, A hilarious side-effect of so many people figuring out how to access Dark Web markets is that sellers realize these folks think you can't buy their stuff on the clear web, so they jack the prices way up. With modern advances in anonymity and the easy of leveraging stolen servers to host your sites, the Clear Web has regained a ton of ground when it comes to selling illicit goods and services. However, most folks never think to go looking there, or assume it's a scam and yet blindly trust what they find on the Dark Web as legitimate and fair.

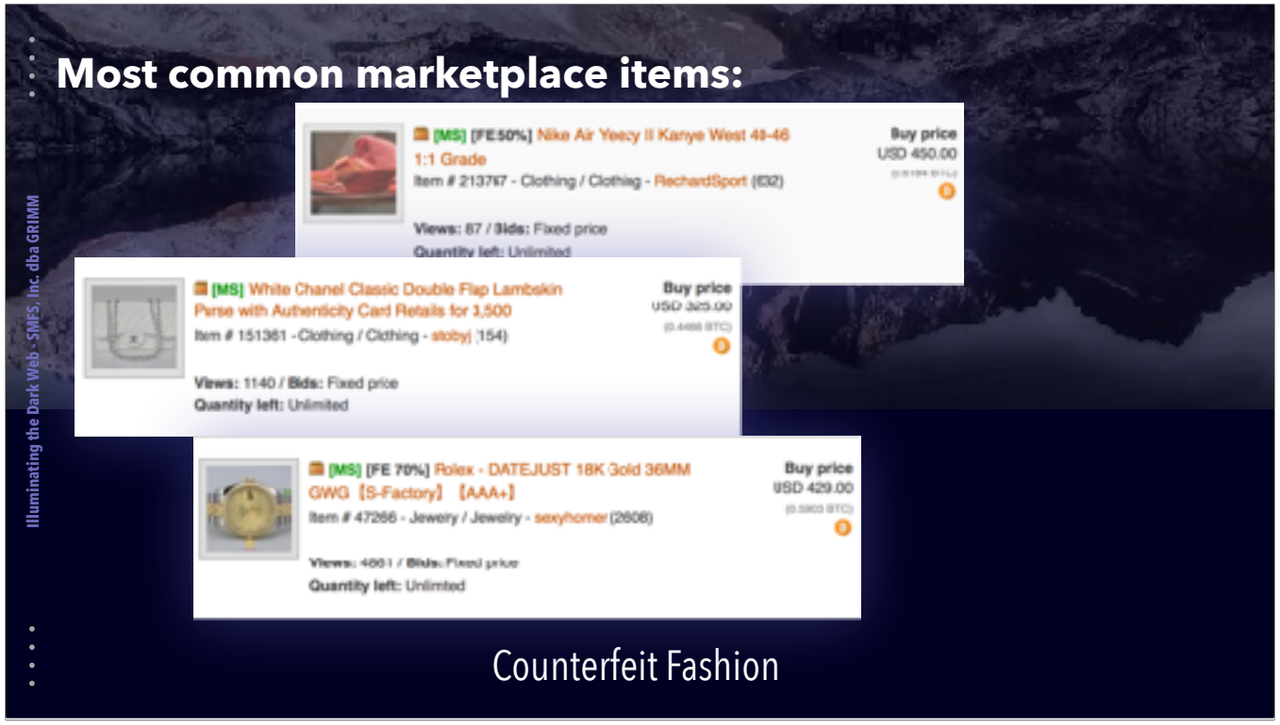
Let's dive in, anyway!

Most common marketplace items:

Prescription-Only Medication

Illuminating the Dark Web - SMFS, Inc. dba GRIMM

Over the next few slides I'm going to very briefly cover some of the more common things you may find on the Dark Web marketplaces


Most common marketplace items:
[MS] [FE50%] Nike Air Yeezy II Kanye West 48-46 1:1 Grade
Item # 213767 - Clothing / Clothing - RechardSport (632)
Views: 87 / Bids: Fixed price
Quantity left: Unlimited
Buy price
USD 450.00
[MS] White Chanel Classic Double Flap Lambskin Purse with Authenticity Card Retails for 3,500
Item # 151361 - Clothing / Clothing - stobyj (154)
Views: 1140 / Bids: Fixed price
Quantity left: Unlimited
Buy price
[MS] [FE 70%] Rolex - DATEJUST 18K Gold 36MM GWG 【S-Factory】 【AAA+】
Item # 47266 - Jewelry / Jewelry - sexyhomer (2608)
Quantity left: Unlimited
Buy price
USD 429.00
Illuminating the Dark Web - SMFS, Inc. dba GRIMM
Counterfeit Fashion

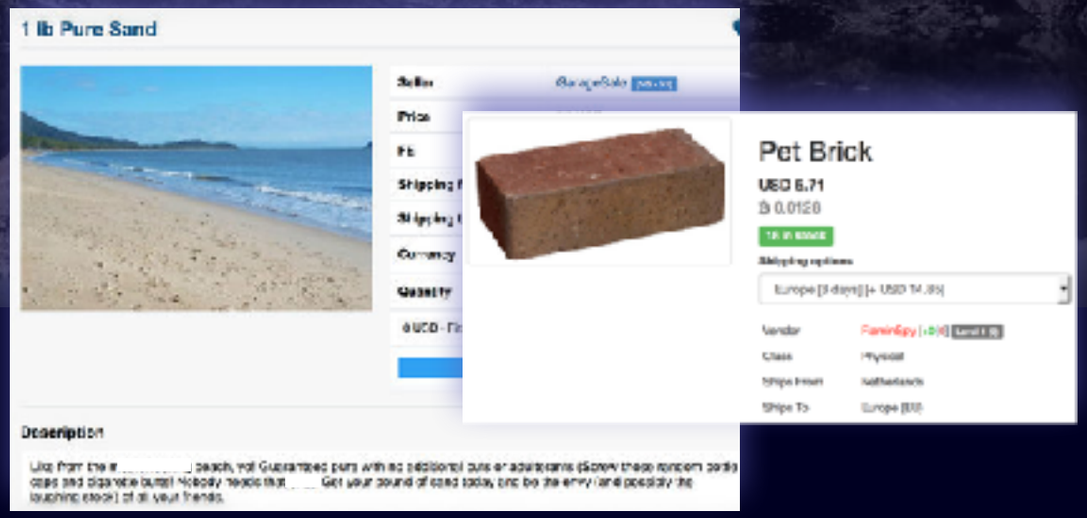
Most common marketplace items:

VERIFIABLE Degrees from Accredited Schools

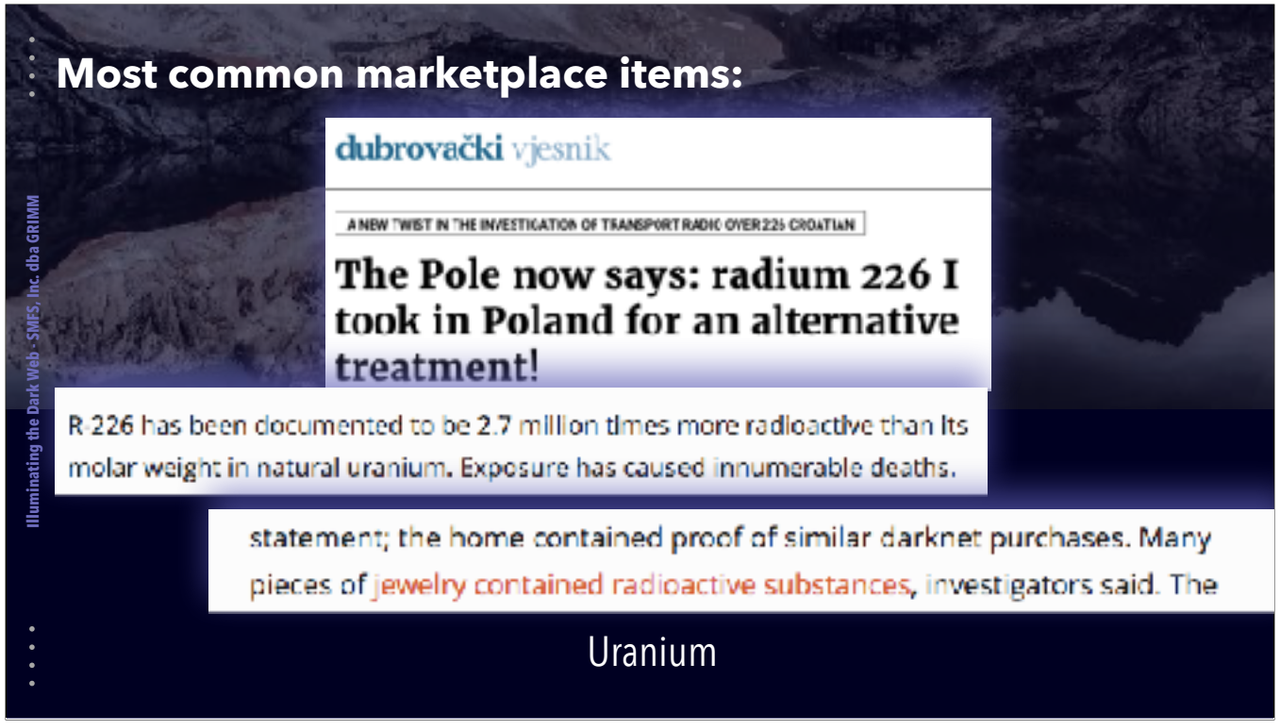
Most common marketplace items:

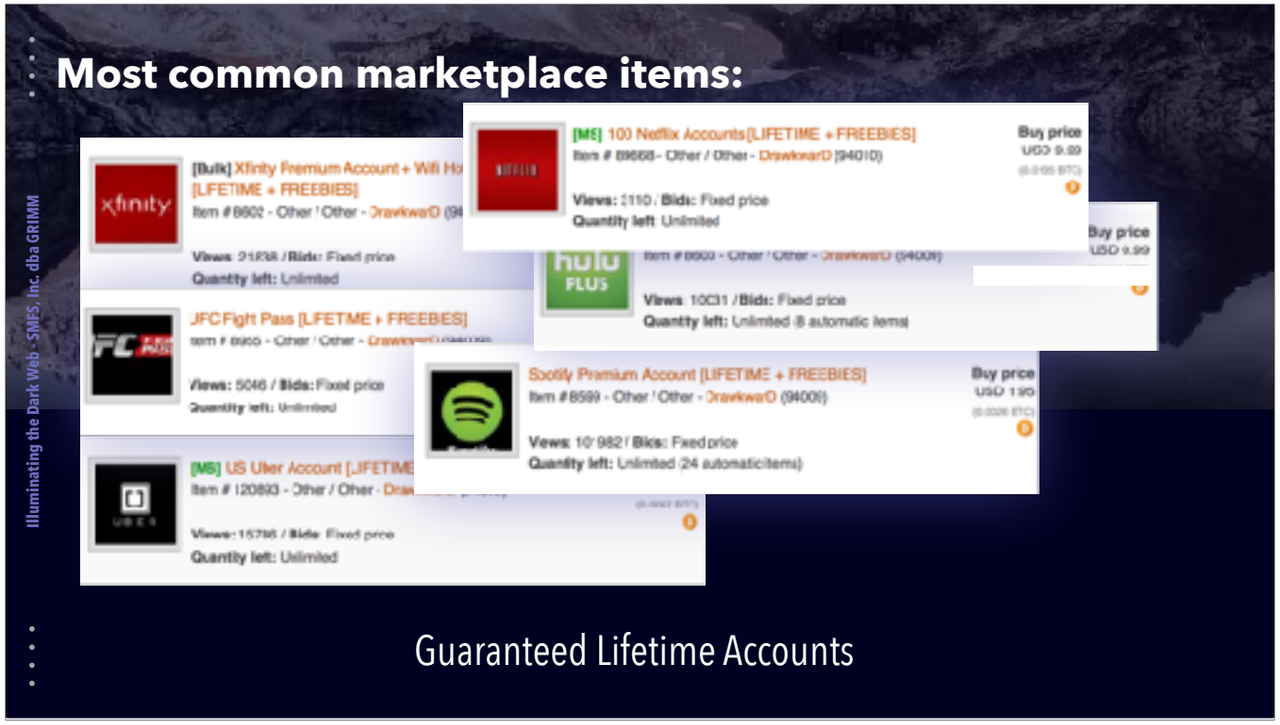
Passports \ Entire New Identities

Most common marketplace items:



"Other"


Most common marketplace items:
dubrovački vjesnik
A NEW TWIST IN THE INVESTIGATION OF TRANSPORT RADIC OVER 225 CROATIAN
The Pole now says: radium 226 I took in Poland for an alternative treatment!
R 226 has been documented to be 2.7 million times more radioactive than its molar weight in natural uranium. Exposure has caused innumerable deaths.
statement; the home contained proof of similar darknet purchases. Many pieces of jewelry contained radioactive substances, investigators said. The
Uranium
Illuminating the Dark Web - SMFS, Inc. dba GRIMM



(Briefly cover slide)

Additionally user accounts from all sorts of applications and breaches are found here. In May 2020 A hacker group known as “ShinyHunters” breached the security of ten companies in the Asian region and attempted to sell more than 73 million user records on the dark web.

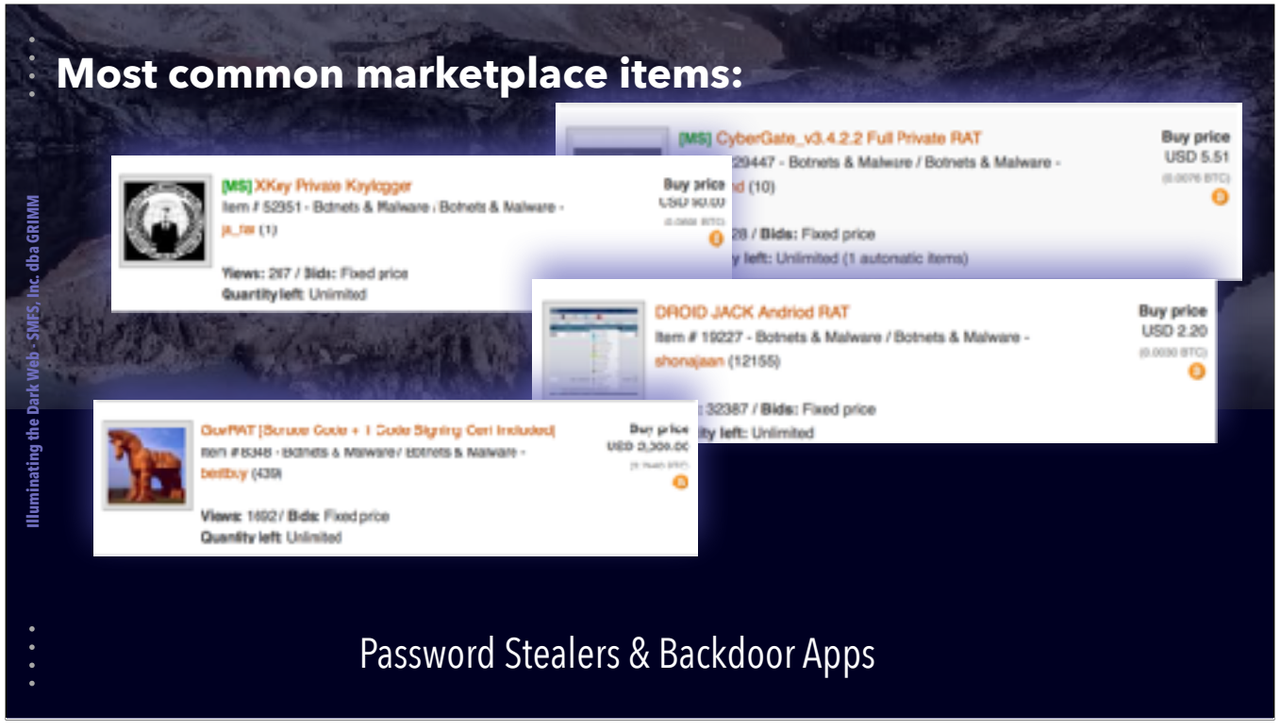
Dark web crime statistics indicate that his included user databases allegedly stolen from organizations such as Online dating app Zoosk (30 million user records), Printing service Chatbooks (15 million user records), and South Korean fashion platform SocialShare (6 million user records), to name a few.

The hackers attempted to sell each database separately, with each selling for around $18,000.

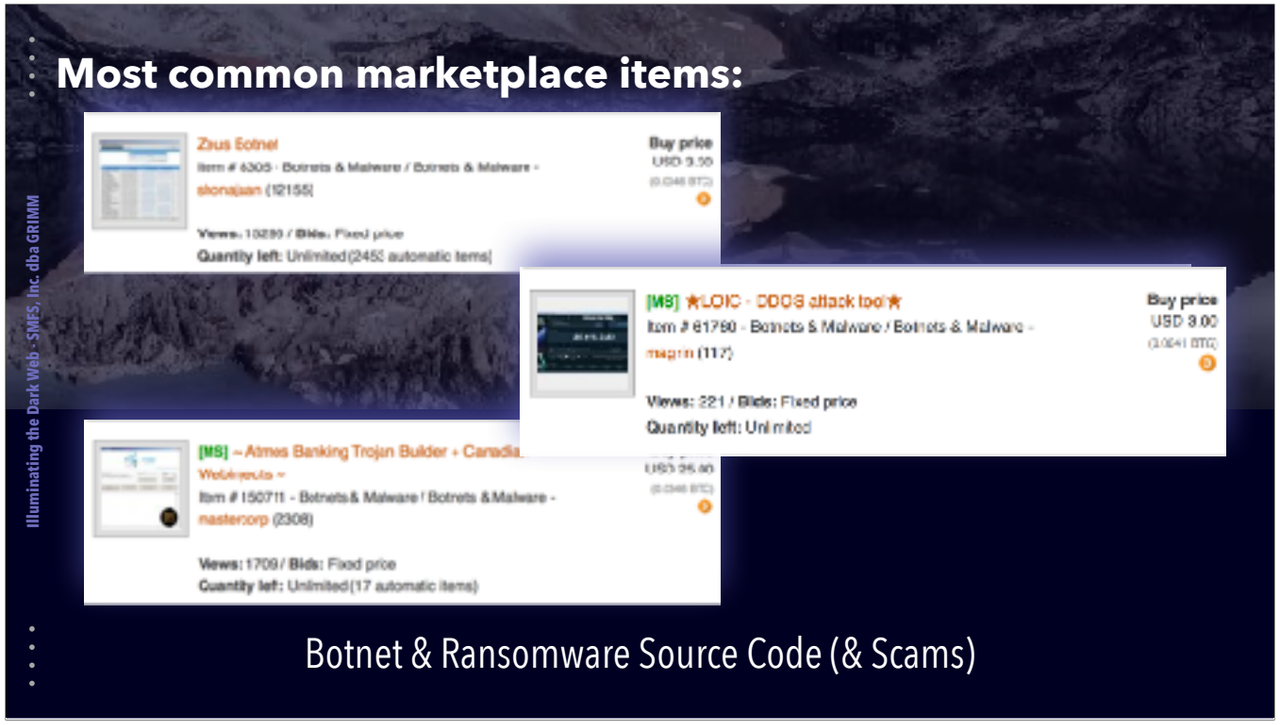
Half a million Zoom accounts were hacked in April 2020 and their data was sold. Some records were selling at less than one cent each. Others you could acquire free of charge. The data, some of which belonged to large, high-profile companies, included information like passwords, home addresses, and emails.

Most common marketplace items:

0-Days & Exploits

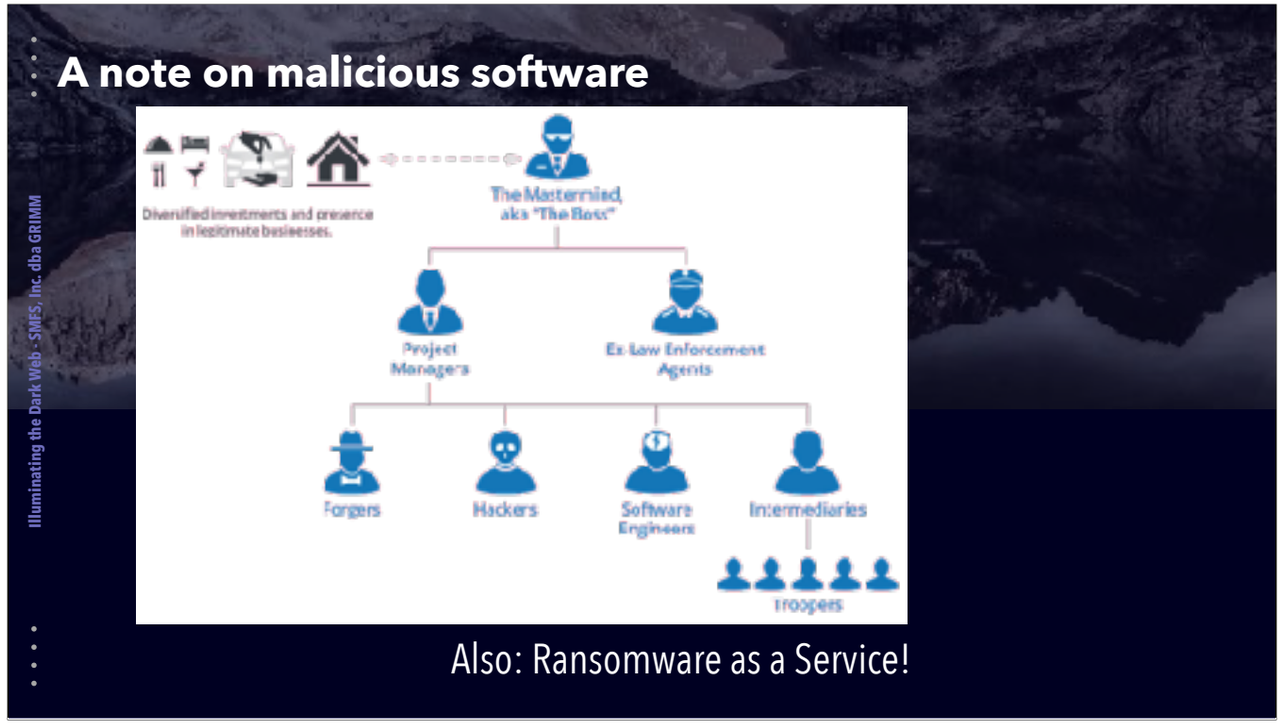


A stealer, costing around $10 can be used to steal your valuable passwords. There is also no end of RATs, or Remote Access Tools that allow access to your computer, microphone and webcam often without you ever being alerted. These tools are commonly used to capture video of victims which is later either directly sold, or held for ransom, very Black Mirror-style. A great reminder to get yourself a webcam cover.



I've chosen these screenshots because, while they are in fact for the sale of malicious code, this is all malicious code that is available for free on the Clear Web. The scams never end here on the Dark Web!

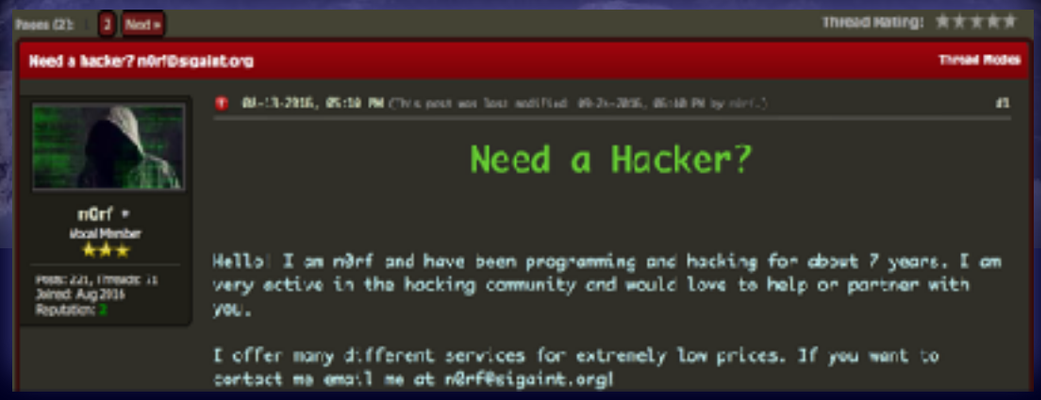
But in all seriousness, Botnets and ransomware pretty much go hand-in-hand these days, and are easily the #1 pieces of malicious software sold on the Dark Web. The competition between sellers has gotten so intense that many of them now even offer telephone tech support for setup and troubleshooting. You gotta wonder how they can handle something like that which definitely takes more than one person in a basement…



Well, The people distributing ransomware and collecting the revenue are almost never one or two scary criminals in a in some far-off country; they're usually members of a complex and well-managed criminal group. The Organized Crime groups that have operated all over the world for centuries haven't disappeared, they've simply adapted to a digital age. Realizing people are now leaving their digital homes open on the internet for all to pilfer, these organizations have added divisions which focus solely on cybercrime.

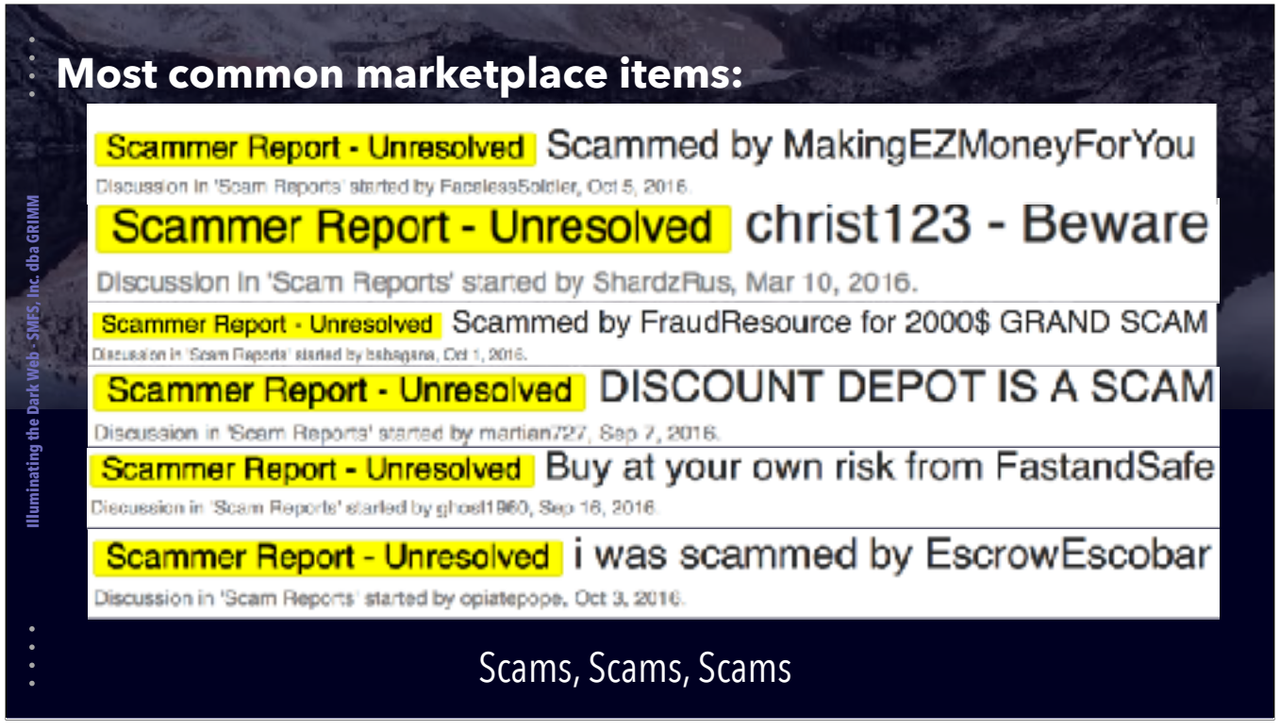
In fact, some of these organizations have gone so far as to create B2B, or business-to-business offerings in the way of "Ransomware-as-a-service." These offerings set up all the infrastructure an attacker needs in order to manage ransomware attacks: encryption keys, payment gateways, and even a tracking system to keep track of the hundreds or thousands of systems a single campaign my compromise. Given this, all an attacker now has to do is get a foot in the door, usually by way of a phishing email, and then simply direct the system to begin talking to their new fancy infrastructure. Practically point-and-click the entire way; it's never been easier.

Most common marketplace items:

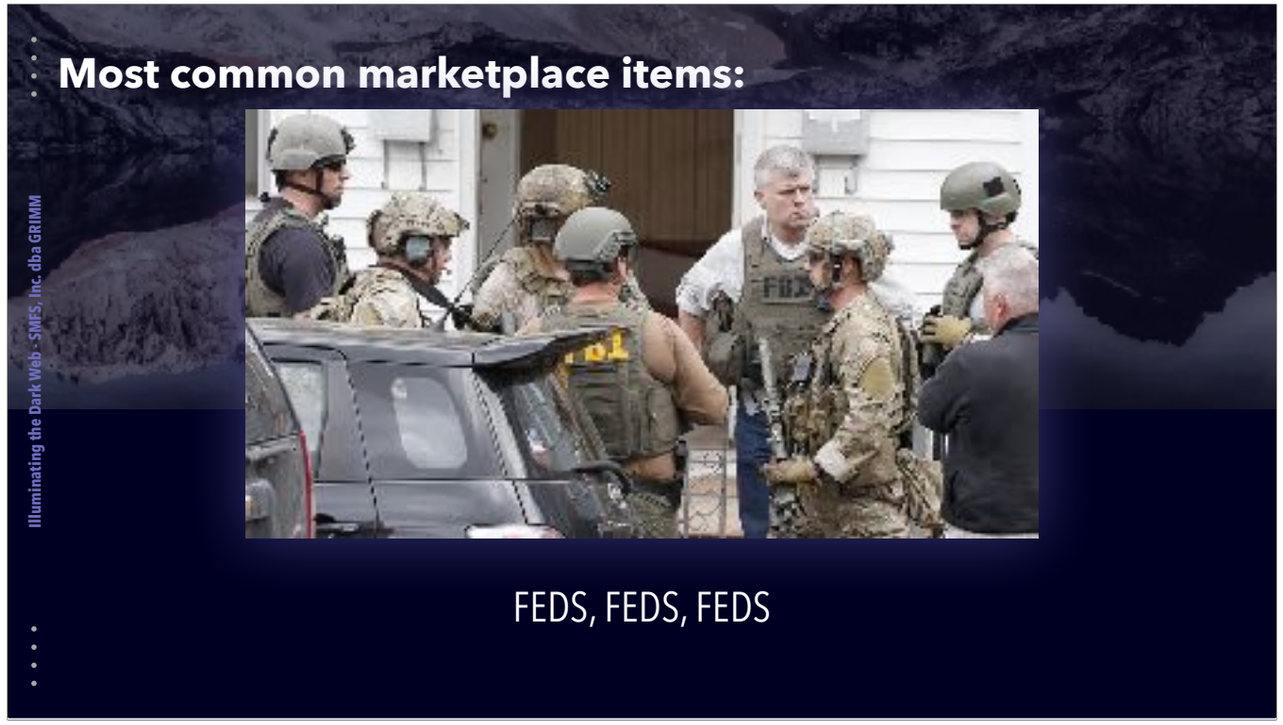


Hacking-as-as-Service

And if all that seems like too much work, you can always just hire a hacker directly to do it for you



Of course, and as we should all be well aware of by now, the scams don't end. Since these are anonymous marketplaces where neither party has any legal recourse due to the exchange of illegal goods, scamming rarely comes with a downside. Many marketplaces do having some systems in place to try to prevent this, such as Escrow and Amazon-style user and product ratings, but you never know when you're going to be dealing with someone who's on their way out and just wants to steal a bunch of money while they're shutting down. Heck, as we mentioned before, you never know when the entire marketplace you're using is going to just up and leave with everyone's escrow money!



Annnnnnd finally, the most important thing to be aware of if you're still even thinking of buying something off of here: pretty much every First-World country on Earth has perpetual sting operations running on every marketplace here. They're not just trying to take the markets down, but also those who buy and sell on them. It's just not worth the risk. It may be fun to surf around a little but, but under no circumstances should you ever, ever buy or sell anything. I wouldn't even risk the legal stuff.

So that's all I have for today. Be sure to check out our company at Grimm.rip in case you'd like to bring in some of the country's best experts in many security fields to train your teams, and we also offer and extended range of security assessment AND engineering services for both Information AND Operational Technologies. I've been Johnny Christmas, and thanks so much for having me. I'll hand it over now for some Q&A if there's time.