

Come a little closer

to

Funeral services Bergmann & Sohn

Jonasstraße 7, 10551 Berlin-Tiergarten, phone: (030) 200 10 15, www.bjg-berlin.de



DOWN THE RABBIT HOLE

A Comprehensive Tour of the Dark Web

Zahier Madhar | Security Engineer | Check Point evangelist @ the office of the CTO.

YOU DESERVE THE BEST SECURITY

DOWN THE RABBIT HOLE

Agenda

01.

A deeper look into the dark web architecture

02.

What is to be found on this platform

03.

Innovative technologies? The Dark Web & Blockchain

04.

Syndicates, collaboration and execution



“LIFE IS LIKE AN ONION...” BY CARL SANDBURG

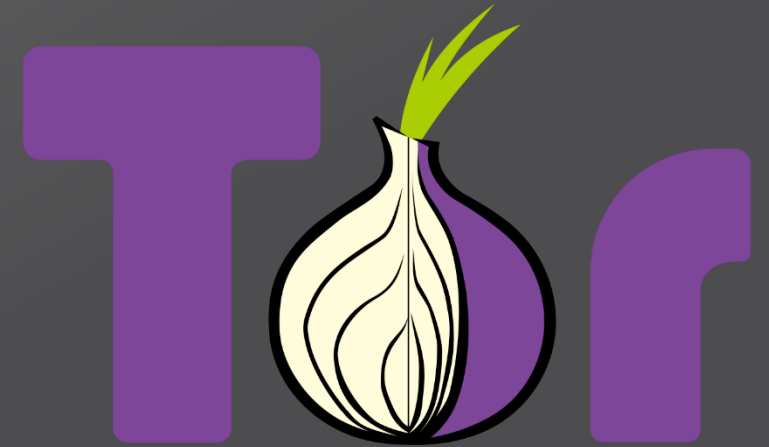
A deeper look at Check Point architecture

“BEGIN AT THE BEGINNING” LEWIS CARROLL

The Dark Web Evolution



Michael Reed

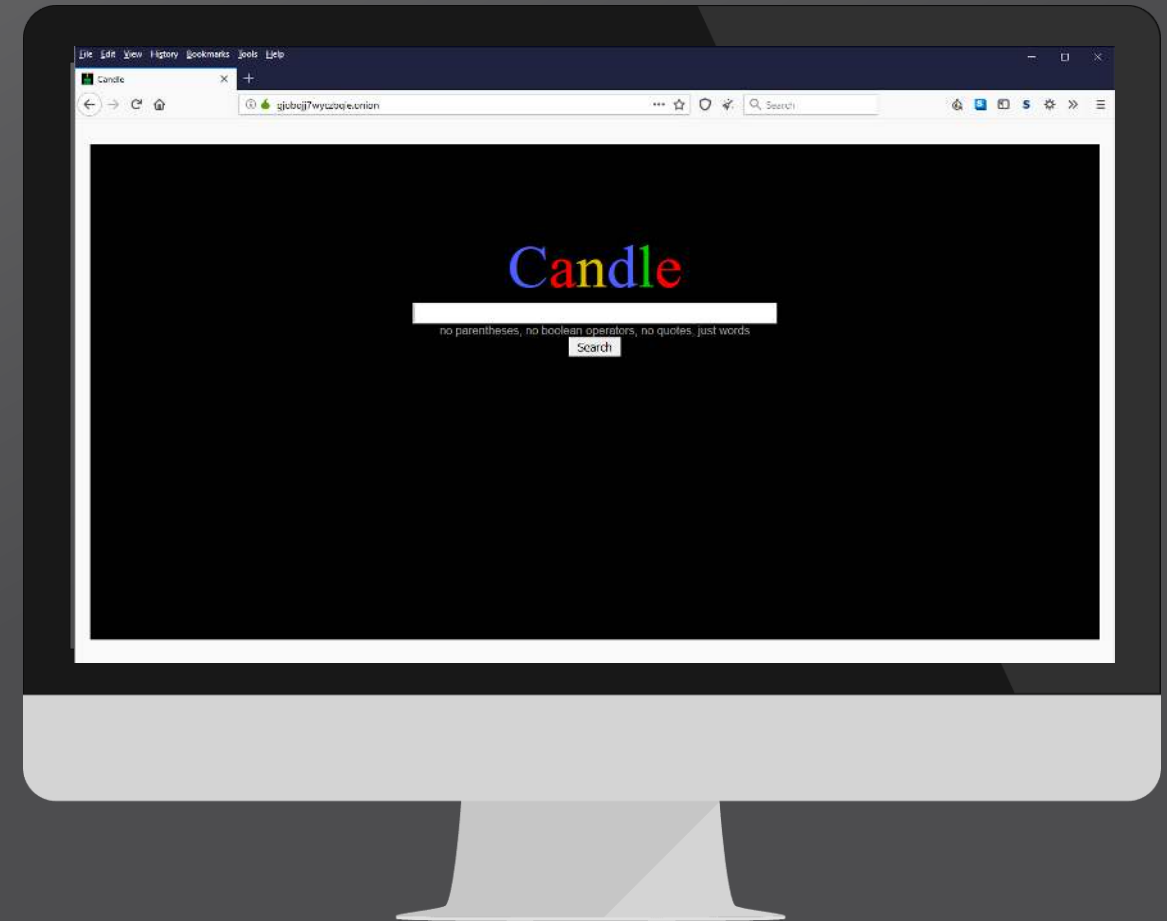
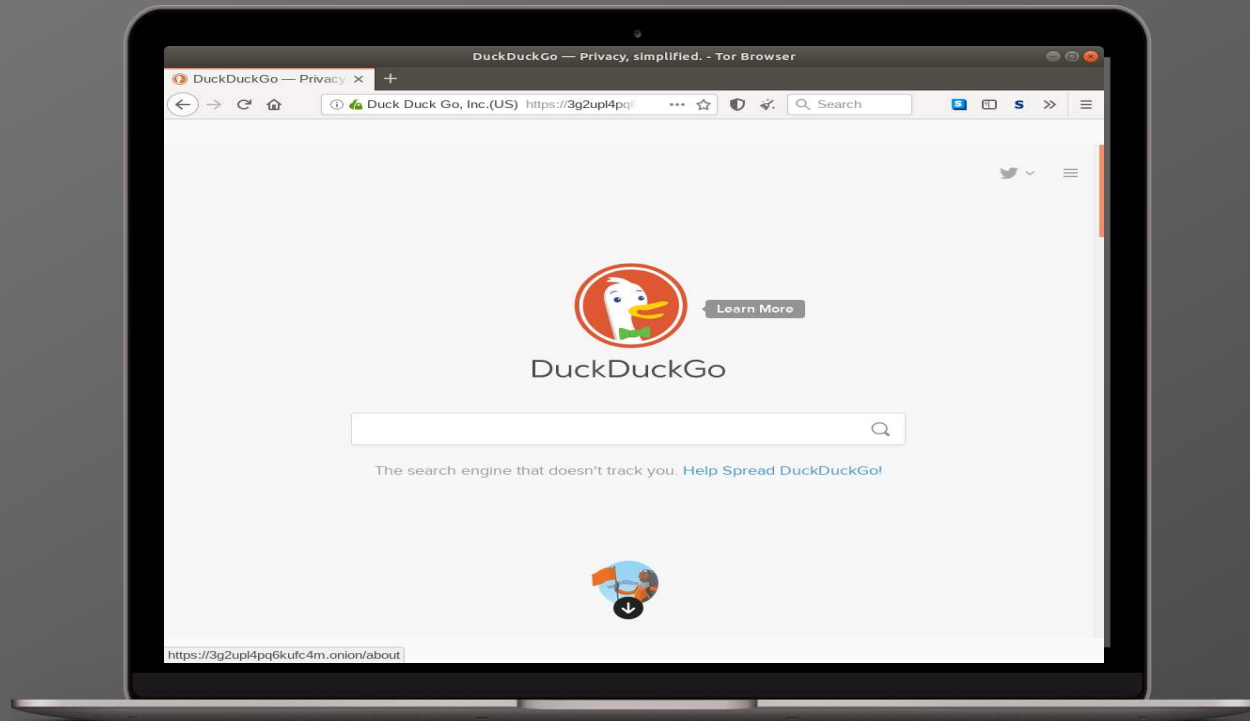


A brief capture of the Tor browser history and evolution

<https://www.torproject.org/about/history/>

“BEGIN AT THE BEGINNING”

What is TOR?



“BEGIN AT THE BEGINNING”

The Dark Web Evolution – Indexed & non Indexed pages

The screenshot shows a web browser window with the address bar containing the URL `wikitjerrta4ggz4.onion`, which is highlighted with a red rectangular box. The browser's address bar also shows navigation icons (back, forward, home, refresh) and a search field. The page content is titled "The Hidden Wiki" and includes a logo on the left. The main content area features a welcome message, "Editor's picks" with a list of links, "Volunteer TODO" with a list of tasks, and "Introduction Points" with a list of search engines and services. A "Contents" sidebar is visible on the right side of the page.

The Hidden Wiki

Hidden Wiki - Tor Wiki - Onion Links Directory [edit]

Welcome to the new Hidden Wiki, your Deep Web url list. Partly moderated and without spam links, now located at easy to remember url: **wikitjerrta4ggz4.onion**

Editor's picks [edit]

Bored? Pick a random page from the article index and replace one of the five slots with it.

1. [TORLINKS](#) - Directory for .onion sites, moderated.
2. [OnionWallet](#) - Anonymous Bitcoin Wallet and Bitcoin Laundry.
3. [EasyCoin](#) - Bitcoin Wallet with free Bitcoin Mixer.
4. [Bitcoin mixing guide](#) - Mixing/Cleaning bitcoins before using them on Silkroad.

Volunteer TODO [edit]

Bored? Here are five random things to help out with

1. Plunder other hidden service lists for links and place them here
2. File the [SnapBBIndex](#) links wherever they go.
3. Set external links to HTTPS where available, good certificate, and same content.
4. Care to start recording onionland's history? Check out [Onionland's Museum](#).
5. Perform Dead Services Duties.

Introduction Points [edit]

OnionLand link indexes and search engines

- [Ahmia.fi](#) - Clearnet search engine for Tor Hidden Services (allows you to add new sites to its database)
- [Core.onion](#) - Simple onion bootstrapping
- [Deepsearch](#) - Another search engine.
- [DuckDuckGo](#) - A Hidden Service that searches the clearnet.
- [Gateway](#) - Tor / I2p web proxy.

Contents [hide]

- 1 Policy Announcement
- 2 Editor's picks
- 3 Volunteer TODO
- 4 Introduction Points
- 5 Marketplace
 - 5.1 Financial Services
 - 5.2 Commercial Services
- 6 Hosting / Web / File / Image
- 7 Blogs / Essays
- 8 Forums / Boards / Chans
- 9 Email / Messaging
- 10 Political Advocacy
- 11 Whistleblowing
 - 11.1 WikiLeaks
 - 11.2 Operation AntiSec
 - 11.3 Other
- 12 HIP/AAW/C
- 13 Audio - Music / Streams
- 14 Video - Movies / TV
- 15 Books
- 16 Drugs
 - 16.1 Noncommercial (D)
 - 16.2 Commercial (D)
- 17 Erotica
 - 17.1 Adult
 - 17.1.1 Noncommercial (E)

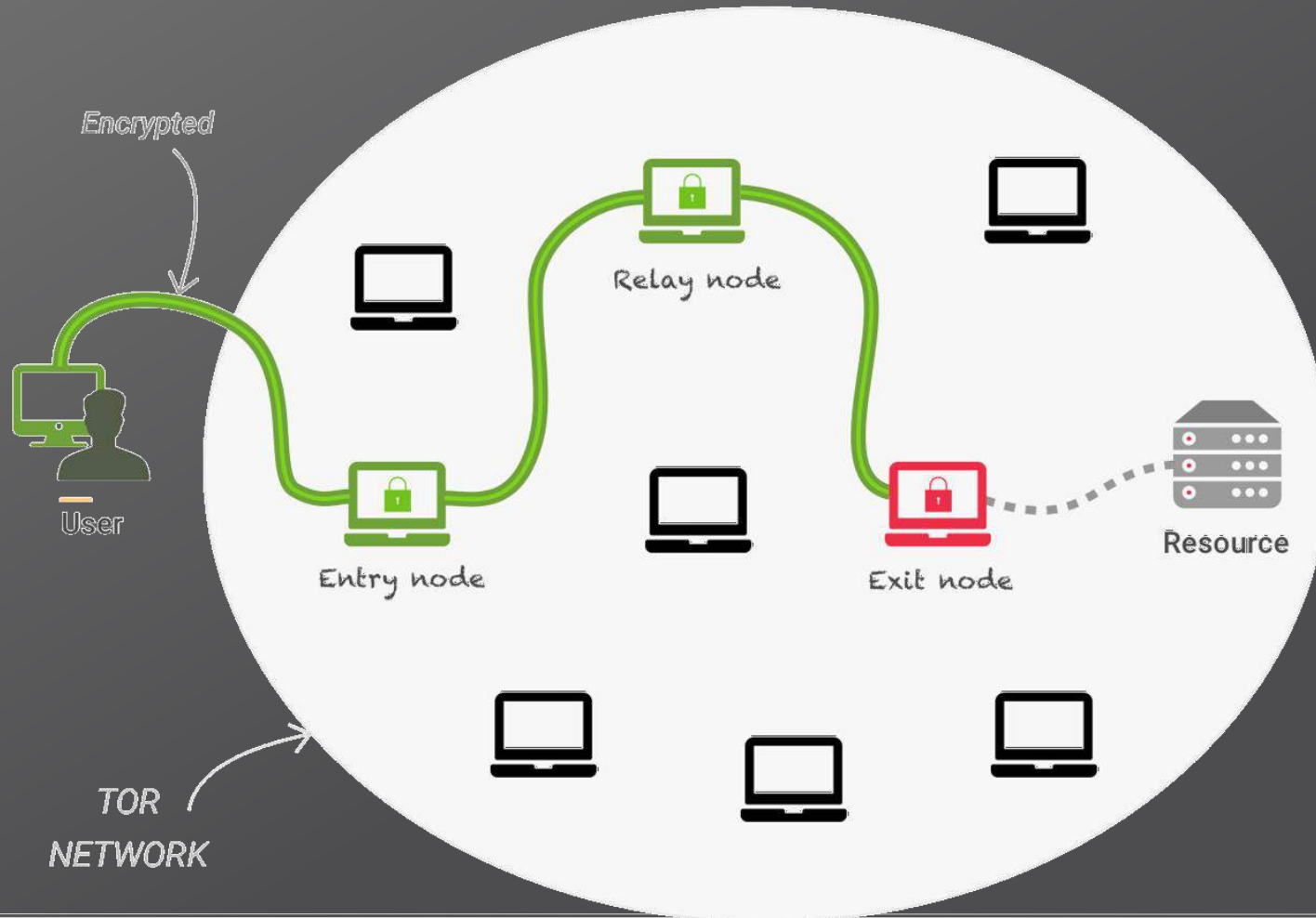
“IF YOU DON'T KNOW WHERE YOU ARE GOING
ANY ROAD CAN TAKE YOU THERE”

Network topology, VPN and encryption process



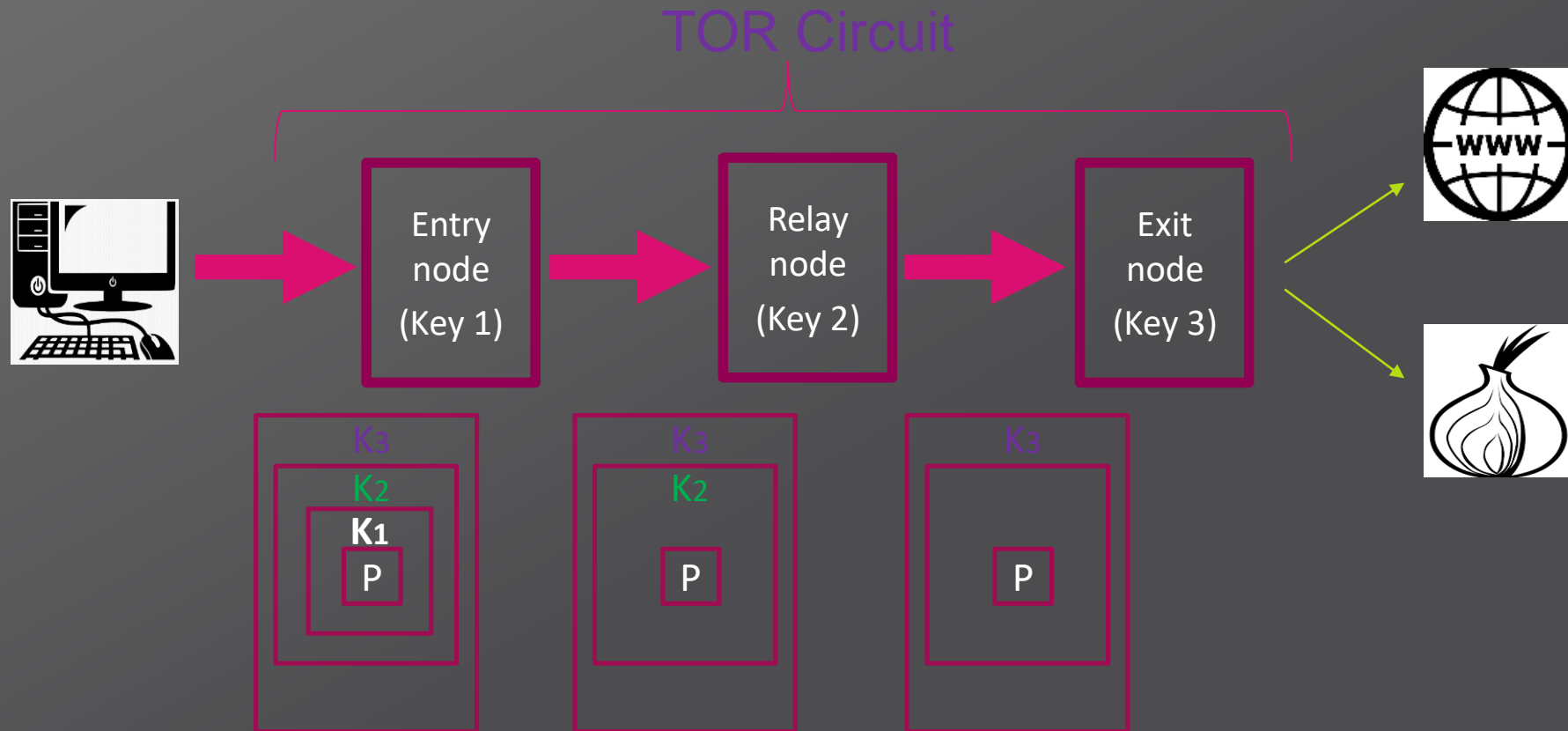
“IF YOU DON'T KNOW WHERE YOU ARE GOING ANY ROAD CAN TAKE YOU THERE”

Network topology, VPN and encryption process



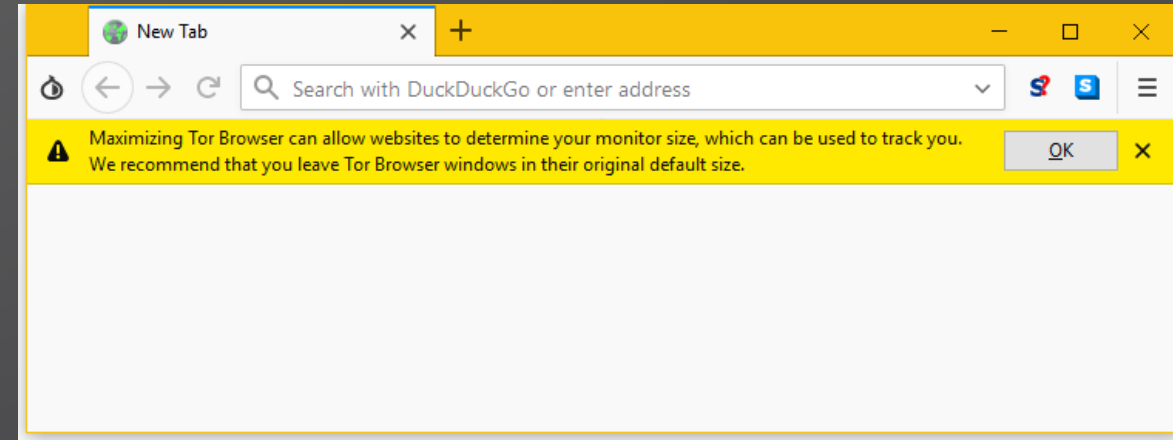
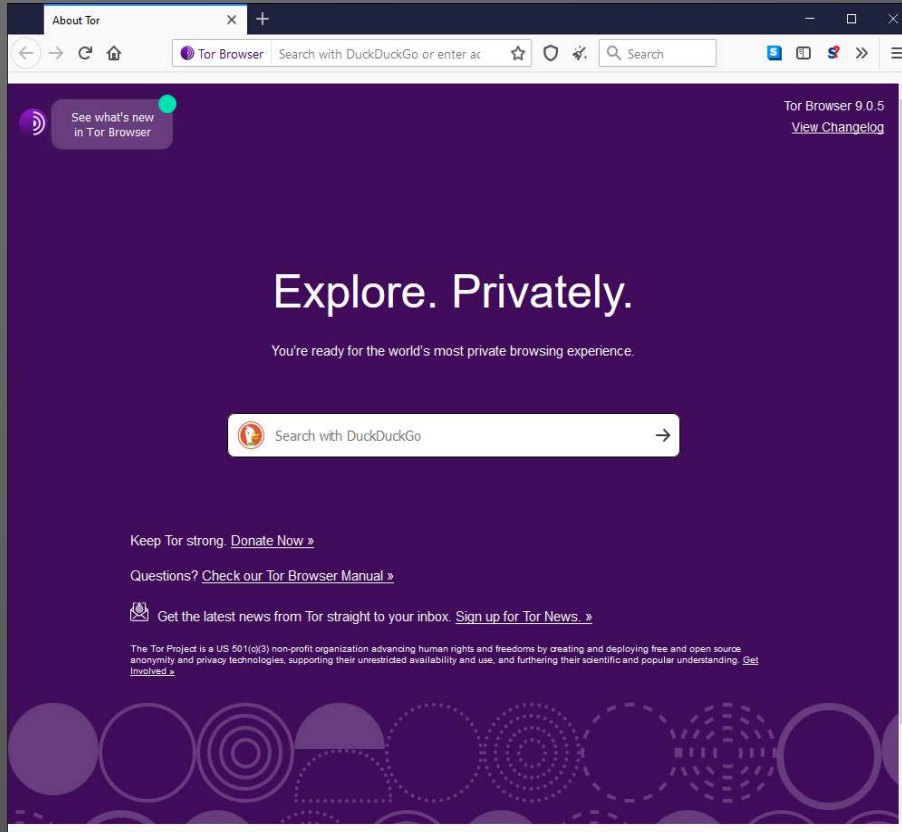
“IF YOU DON'T KNOW WHERE YOU ARE GOING ANY ROAD CAN TAKE YOU THERE”

Network topology, VPN and encryption process



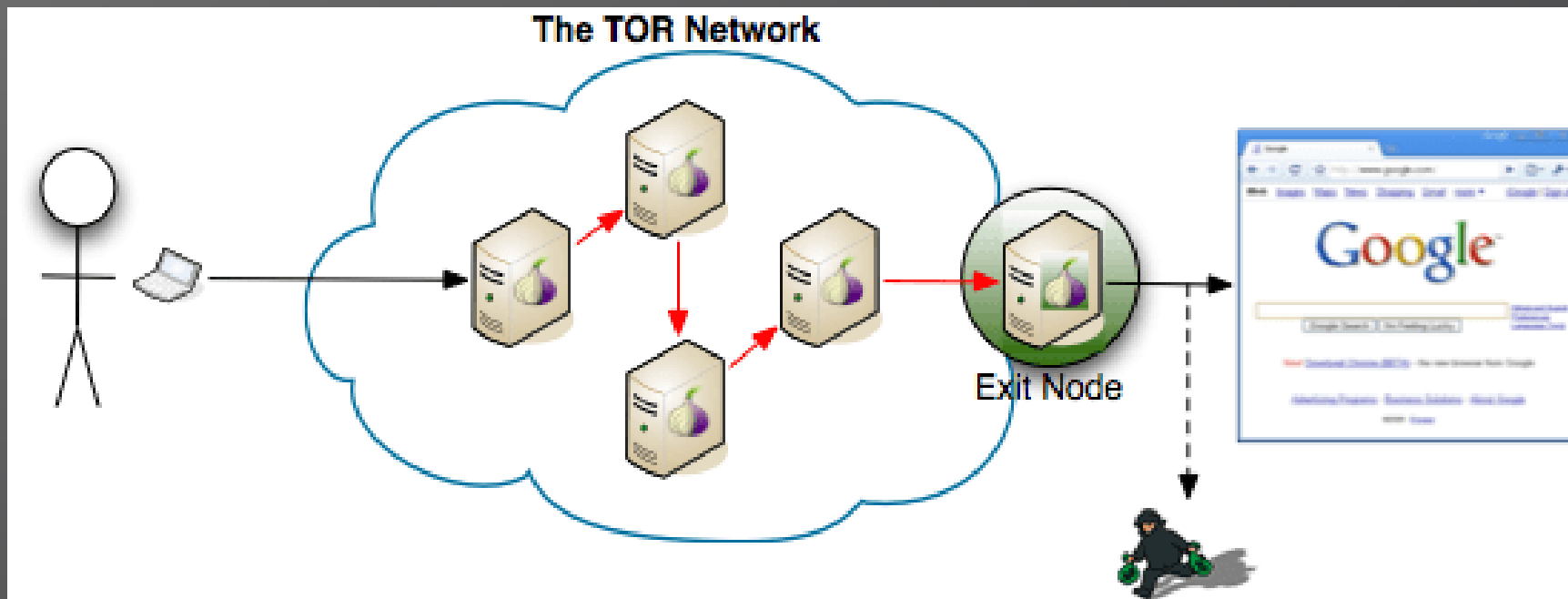
“WHO IN THE WORLD AM I?”

How does One keep Anonymous on the Dark Web?



“WHO IN THE WORLD AM I?”

Exit Relay – Exposure node



“THE MORE THERE IS OF MINE, THE LESS THERE IS OF YOURS”

Dark Net Nodes Paradigm – Reveal the Man Behind the Keyboard

TOP SECRET//COMINT// REL FVEY



Stinks ^(U)

██████████
CT SIGDEV
██████████
JUN 2012

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20370101

TOP SECRET//COMINT// REL FVEY

TOP SECRET//COMINT// REL FVEY

REMATION II ^(U)

- Joint NSA GCHQ counter-Tor workshop
- Week one at MHS focus on analytics
- Week two at GCHQ focus on exploitation

<https://wiki.gchq/index.php?title=REMATION>

TOP SECRET//COMINT// REL FVEY

TOP SECRET//COMINT// REL FVEY

Nodes: Baseline Our Nodes ^(TS//SI)

How many nodes do we have cooperative or direct access to? Can we deploy similar code to these nodes to aid with circuit reconstruction?

Can we do packet timing attacks using nodes?

Can we use the nodes to shape traffic flow?

Can we use the nodes to deny/degrade/disrupt comms to certain sites?

TOP SECRET//COMINT// REL FVEY

21

“THE MORE THERE IS OF MINE, THE LESS THERE IS OF YOURS”

Known Exploits, Reveal the Man Behind the Keyboard



“GCHQ has taps on 200 fiber-optic pipes, each transmitting on average **10 gigabits per second**.... That works as being **21.6 petabyte per day**”

“THE MORE THERE IS OF MINE,
THE LESS THERE IS OF YOURS”

Node and TOR Exploits – Real life example



REVEALING THE UNSEEN

What is the new platform

MORE THAN A MARKETPLACE

What is to be found on this platform

The screenshot shows the Silk Road anonymous marketplace website. The browser address bar displays 'silkroadvb5piz3r.onion'. The page header includes the Silk Road logo, a user greeting 'Welcome OzFreelancer!', and navigation links for 'messages(0)', 'orders(0)', 'account(\$0.00)', 'settings', and 'log out'. A search bar and a shopping cart icon with '(0)' items are also present.

Shop by category:

- Drugs(1582)
 - Cannabis(271)
 - Dissociatives(33)
 - Ecstasy(217)
 - Opioids(106)
 - Other(65)
 - Prescription(274)
 - Psychedelics(306)
 - Stimulants(190)
- Apparel(37)
- Art(1)
- Books(300)
- Computer equipment(9)
- Digital goods(218)
- Drug paraphernalia(33)
- Electronics(13)
- Erotica(165)
- Fireworks(1)
- Food(1)
- Forgeries(34)
- Hardware(1)
- Home & Garden(5)
- Lab Supplies(5)
- Medical(3)
- Money(89)
- Musical instruments(2)
- Packaging(1)

Product Listings:

- 10 Grams high grade MDMA 80+% **\$61.17**
- Amphetamines sulfate / Speed freebase... **\$28.59**
- 2g Jack Frost (weed) *420 SALE***** **\$8.54**
- 5 Grams of pure MDMA crystals **\$42.04**
- 100 red Y tablets 111mg (lab tested)... **\$97.77**
- Michael Jackson Discography 1971-2009... **\$2.52**
- 3.5g Albino Rhino (weed) **\$12.37**
- 10mg Flexeril (muscle relaxant)... **\$3.22**
- ***10gr. Amphetamine Sulphate... **\$33.19**

News:

- The gift that keeps on **giving**
- Who's your **favorite?**
- Acknowledging **Heroes**
- A new anonymous market **The Armory!**
- **State of the Road Address**

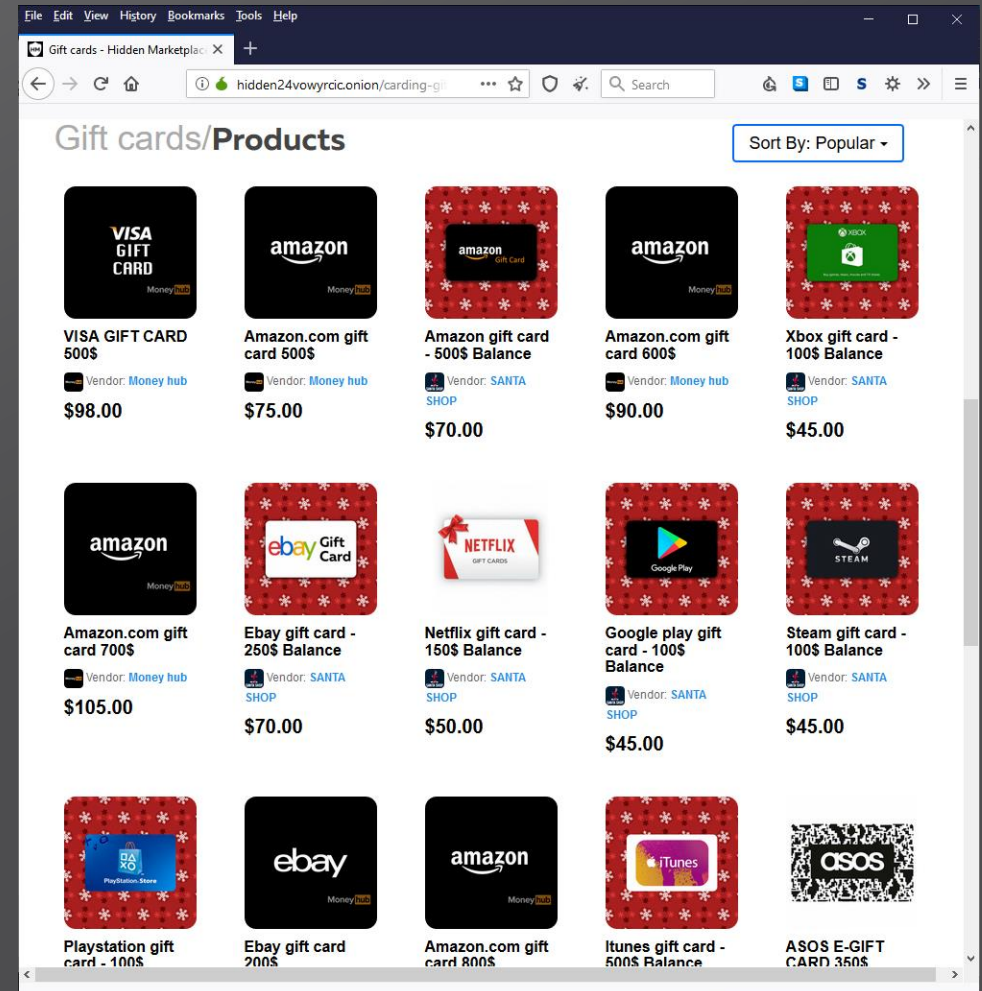
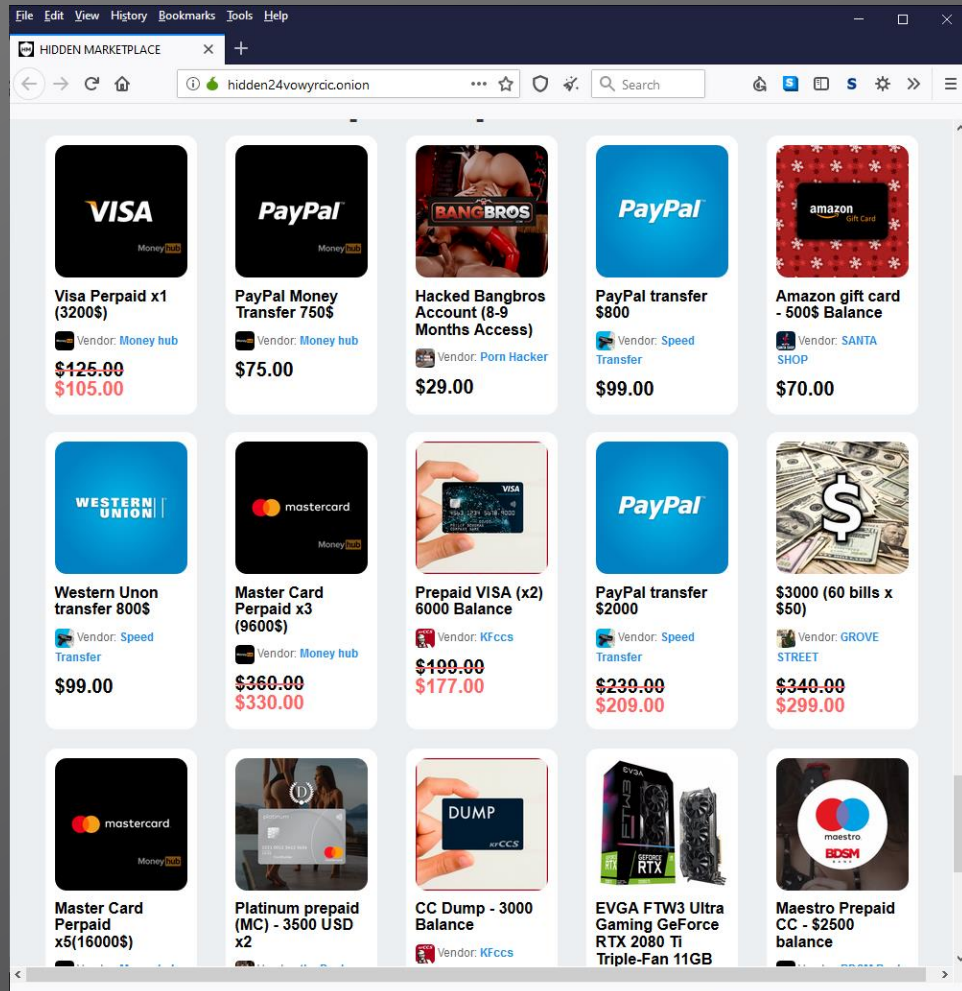
MORE THAN A MARKETPLACE

What is to be found on this platform



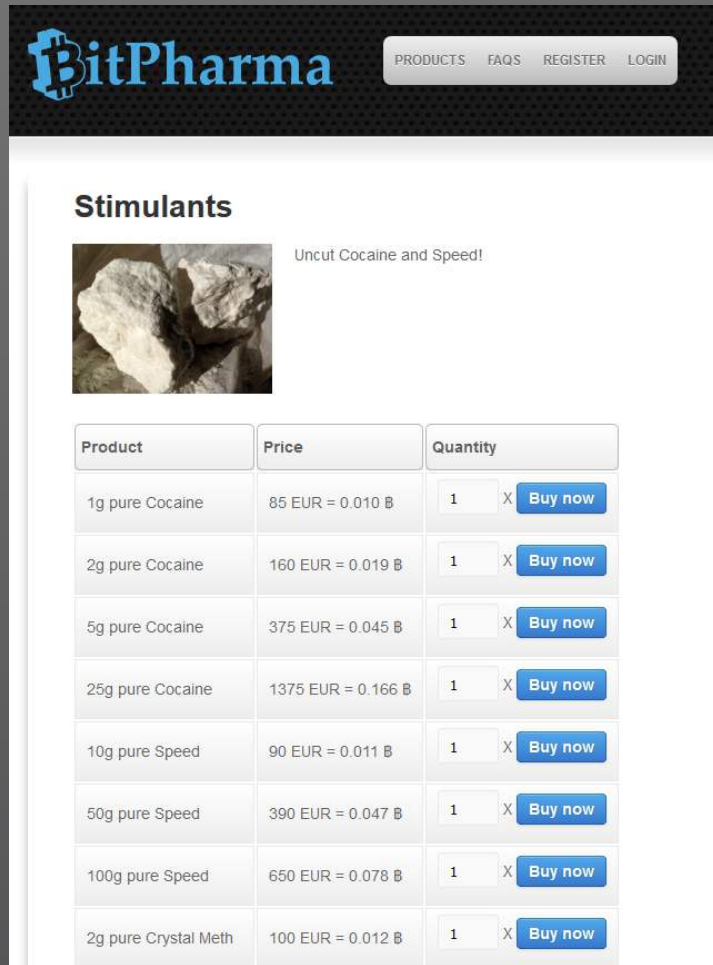
MORE THAN A MARKETPLACE

What is to be found on this platform




MORE THAN A MARKETPLACE

What is to be found on this platform

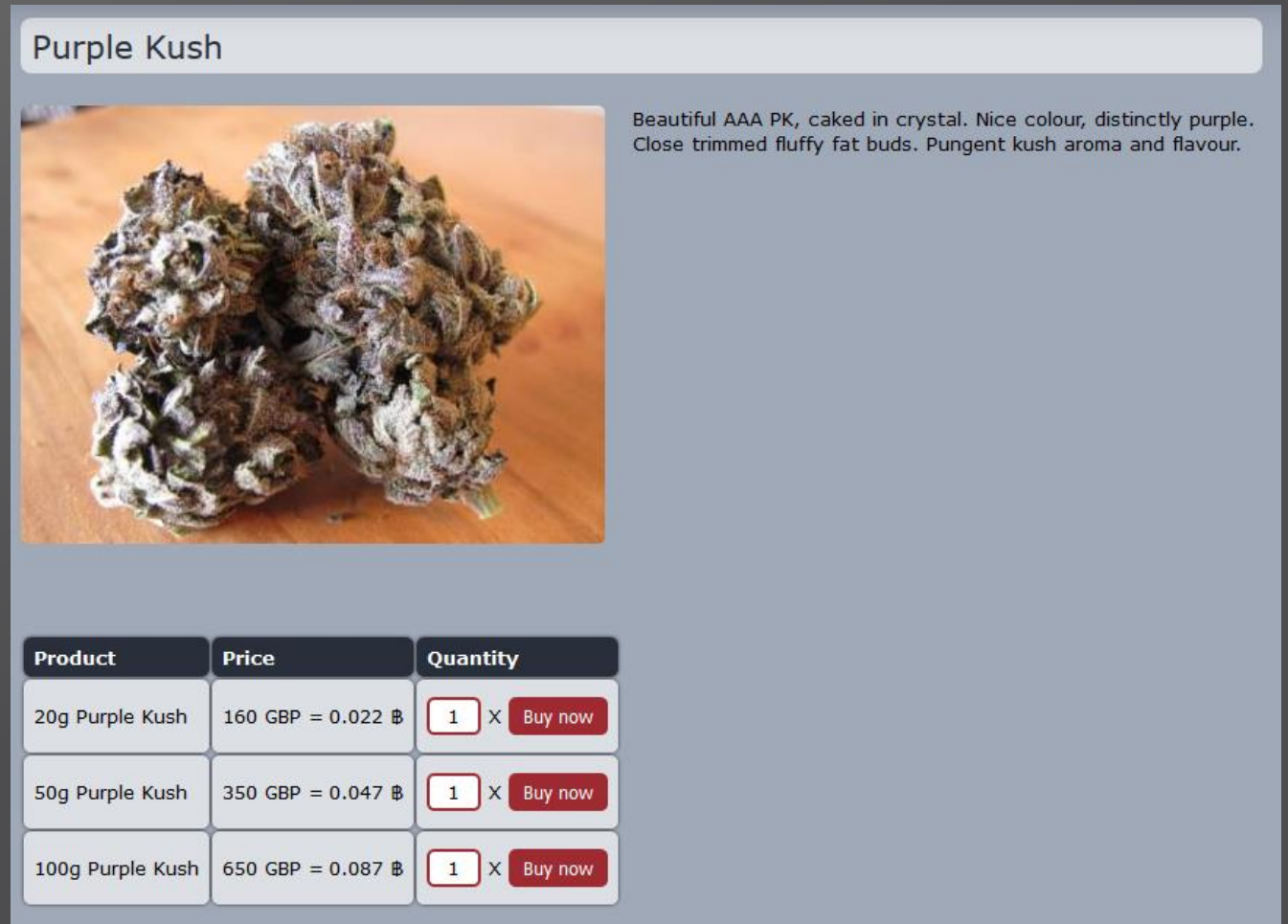


BitPharma PRODUCTS FAQS REGISTER LOGIN


Stimulants

 Uncut Cocaine and Speed!

Product	Price	Quantity
1g pure Cocaine	85 EUR = 0.010 ₿	1 X Buy now
2g pure Cocaine	160 EUR = 0.019 ₿	1 X Buy now
5g pure Cocaine	375 EUR = 0.045 ₿	1 X Buy now
25g pure Cocaine	1375 EUR = 0.166 ₿	1 X Buy now
10g pure Speed	90 EUR = 0.011 ₿	1 X Buy now
50g pure Speed	390 EUR = 0.047 ₿	1 X Buy now
100g pure Speed	650 EUR = 0.078 ₿	1 X Buy now
2g pure Crystal Meth	100 EUR = 0.012 ₿	1 X Buy now



Purple Kush



Beautiful AAA PK, caked in crystal. Nice colour, distinctly purple. Close trimmed fluffy fat buds. Pungent kush aroma and flavour.

Product	Price	Quantity
20g Purple Kush	160 GBP = 0.022 ₿	1 X Buy now
50g Purple Kush	350 GBP = 0.047 ₿	1 X Buy now
100g Purple Kush	650 GBP = 0.087 ₿	1 X Buy now

MORE THAN A MARKETPLACE

What is to be found on this platform

HOME DIRECTORY (DARK SITES LINKS LIST) MUST READ DARK WEB NEWS FREE VPN CONTRIBUTE DIRECTORY DASHBOARD

DARK WEB NEWS

Munich Gunman Allegedly Bought Gun from the Dark Web

By  admin  May 19, 2019  0  57 Views



David Ali Sonboly, **the Munich killer**, reportedly bought the Glock 17 pistol from the dark web.

The German police said that though the serial number of the reactivated gun with which the 18-year-old killed nine people was scratched off, it appeared as though it is of Slovakian origin.



MORE THAN A MARKETPLACE

What is to be found on this platform

ID Cards



Product	Price	Quantity
Czech ID Card	500 EUR = 0.060 ₿	<input type="text" value="1"/> X Buy now
Netherlands ID Card	550 EUR = 0.066 ₿	<input type="text" value="1"/> X Buy now
Denmark ID Card	550 EUR = 0.066 ₿	<input type="text" value="1"/> X Buy now
French ID Card	550 EUR = 0.066 ₿	<input type="text" value="1"/> X Buy now
Lithuanian ID Card	550 EUR = 0.066 ₿	<input type="text" value="1"/> X Buy now

USA Citizenship

[Products](#) [FAQs](#) [Register](#) [Login](#)

Become a citizen of the USA, real USA passport



We offer bulletproof USA passports + SSN + Drivers License and Birth Certificate and other papers making you an official citizen of the USA!
It will even work if you are not in the USA yet

How we do it? Trade secret! But we can assure you that you won't have any problems with our papers.

We are shipping documents from the USA, international shipping is no problem.

You can use your own name or a new name!

Information on how to send us required info (scanned signature, biometric picture etc) will be given after purchase.

The total price is 5000 USD, 1000 paid when you order and the other 4000 when we show you photo and video proof of your passport.

The first \$1000 are needed upfront to see you are serious about it. Once paid we will discuss details in our shop internal message system.

Product	Price	Quantity
Your USA citizenship first payment 20% 1000/5000	1000 USD = 0.108 ₿	<input type="text" value="1"/> X Buy now
US bank account with online banking and card. Great for cashing out bitcoin. Accounts will last at least 8 years.	1000 USD = 0.108 ₿	<input type="text" value="1"/> X Buy now

MORE THAN A MARKETPLACE

What is to be found on this platform

File Edit View History Bookmarks Tools Help

DN HACKING TEAM

hacknp5rq6sigjds.onion

DEEPWEB HACKERTEAM

INSTAGRAM HACK	\$199
HACK EMAIL ACCOUNT	\$239
SPY WHATSAPP	\$199
DESTROY SOMEBODYS LIFE	\$899
HACK VISA / Credit Card	\$199
HACK A OPERATING SYSTEM	\$299
PASSWORD SNIFFING	\$169
DDOS ATTACK	from \$99

MORE THAN A MARKETPLACE

What is to be found on this platform

The screenshot shows a web browser window displaying a product listing on DeepDotMarket. The product is titled "Hacking Facebook Account" and features a Facebook logo. The listing includes a quality rate of five stars, a price of 300.00 \$ per account, and a 15% discount with a COVID-19 code. The seller is identified as SSHacker, Level 1, with a reputation of +10 and 0 negative reviews. The listing is for 997 accounts out of 21 available. The purchase type is "Normal Escrow" and the amount is 1. The listing is for hacking into a Facebook account. The description states: "This listing is for hacking into an Facebook account. Hello. Welcome to SSHacker. We are a group of hackers dedicated to provide the best hacking services since 2005. SSHacker was founded in 2005 by Jonathan James when he decided to offer services for email hacking. In that years, internet was dominated by emails, because the social networks didn't exists yet and cell phones technologies were growing. Time has passed and the group increased gradually and we added new services like: Facebook, Twitter or Instagram. Now, our services are even more than then, including PC/Cellphone hacking, deface websites, grades change, custom ransomware, etc. We invite you to explore our Hacking Services and if you're interested in any of them, hire us! SSHacker, the best choice. Why should I hire a hacker? Why a hacker? Because if you really want any hacking service, either get a password, spy or track a

Coronavirus
discount

OPEN THE MYSTERY BOX

What is to be found on this platform



The screenshot shows a web browser window with the address bar displaying `hidden24vowyrdc.onion/index.php?route=product/manufacture/info&manu...`. The page header includes navigation links for 'Support', 'Login', and 'Register', along with a search bar and a shopping cart icon. The main content area features a product listing for 'Mystery Boxes Online' with a 'SEND MESSAGE' button. The product description includes details about the contents and seller information.

HiDDEN MARKETPLACE Search [MONEY BACK GUARANTEE](#) [HIDDEN FORUM](#) [CART](#)

[HOT SALE](#) [Credit cards](#) [Fake money](#) [Money transfers](#) [Gift cards](#) [Gadgets](#) [Porn and Erotic](#) [SELLERS LIST](#)

Mystery Boxes Online

Products: [Gift cards](#) [SEND MESSAGE](#)

If you want new emotions, an unexpected surprise or don't know what to present to your friend for his birthday, then our product is just for you!

In the box, can find anything, starting from toys adult entertainment, up to a new iPhone and MacBook Pro 16!
In any case, it will be something unusual and exciting. In our collection of 70 items of varying value (each item in 3-5 copies), which we chose by conducting anonymous surveys.
We have created 7 different thematic categories of products
In addition, our VIP product contains a collection of 7 unique handmade works of art by seven masters from different countries and continents.

We do not ship illegal products: weapons, drugs, cloned cards etc. We value our customers and will not send empty box or a box with bricks or dirty socks, used condoms etc. All our items have real value.

You won't what is there find out there until you open the box.
This gift will be remembered for a lifetime!

Our Mystery Boxes are perfect for YouTubers looking to create content.

For any inquiries please contact us!

Seller since **11.2019** | **331 Sales** | **7 Products** | **Rating** ★★★★★

Seller's Products:

OPEN THE MYSTERY BOX

What is to be found on this platform



PLAY THE GAME

Policies and reputation on the Dark Web

A screenshot of a dark web marketplace interface. The browser address bar shows 'gdaqpaukrkqwjop6.onion/?sessid=10465'. The page displays four vendor listings in a grid:

- PP Guru**: PayPal accounts. Member since Dec 2016, Sales: 79539, Status: Online, 9 stars.
- Click'n'Cash** (PROVIDOR): PayPal, Gift card and Credit cards cash out services. Member since Feb 2018, Sales: 74611, Status: Offline, 8.9 stars.
- eBay Store**: eBay virtual gift cards. Member since Dec 2016, Sales: 31601, Status: Offline, 7.8 stars.
- Amazon Gift Cards**: Digital Amazon gift cards. Member since Dec 2016, Sales: 85625, Status: Offline, 8.2 stars.

Each listing includes a 'View vendor' button and social media icons for Instagram and Telegram.

A screenshot of a dark web marketplace interface showing a 'Customer reviews' section. The browser address bar shows 'gdaqpaukrkqwjop6.onion/money-maker/'. The section includes a disclaimer and three reviews:

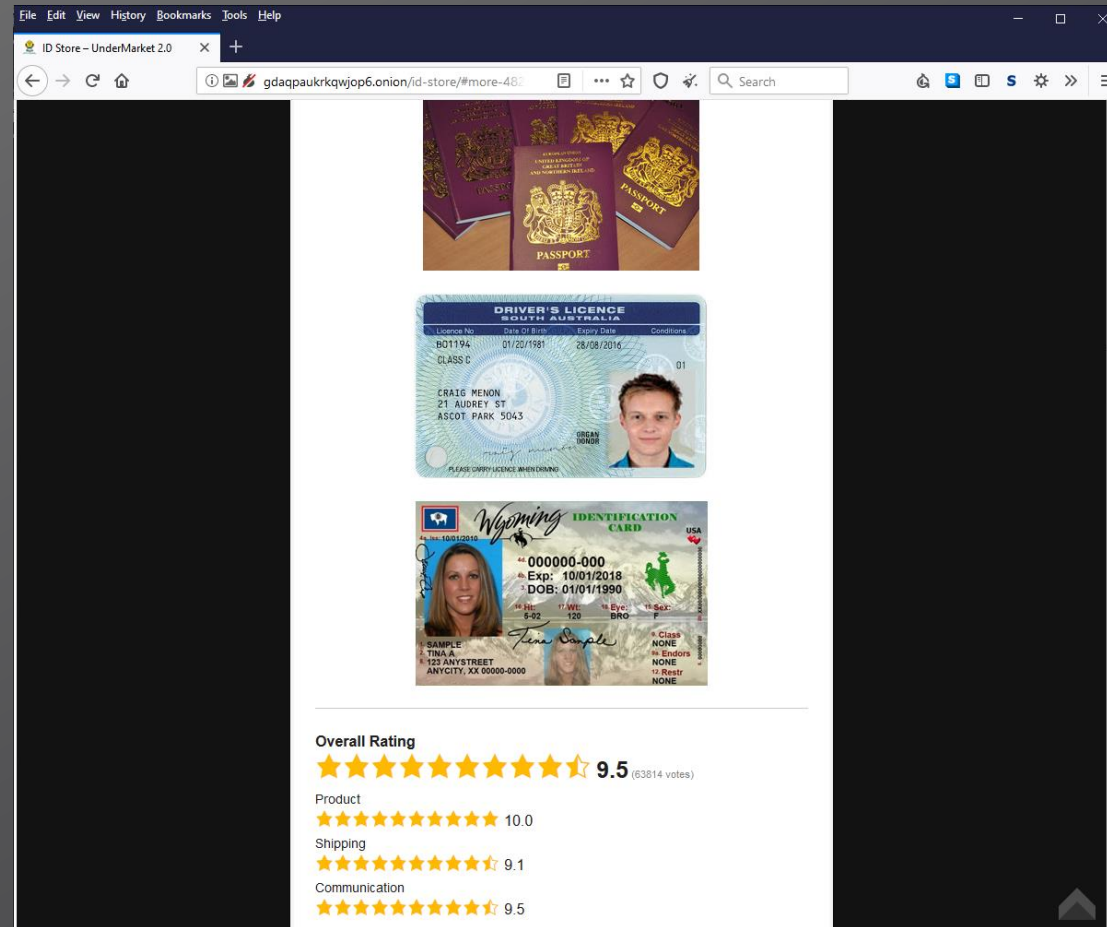
Customer reviews

This section is for customer reviews only. You will be able to leave a review on the order page once your order is finished. Before UnderMarket_2.0 engine this section was used for leaving normal comments as well. If you want to ask vendor an open question, feel free to ask it in [uChat](#).

- Mightfont** (Buyer): My overall rating: 6.7 (7 hours 28 minutes ago)
- Anarallador** (Buyer): no hustle. My overall rating: 7.3 (1 day 5 hours ago)
- NotAuthenticPat** (Crown Buyer): My overall rating: 7.5

PLAY THE GAME

- Policies and reputation on the Dark Web



THE PEOPLE BEHIND THE KEYBOARDS

Population on the platform



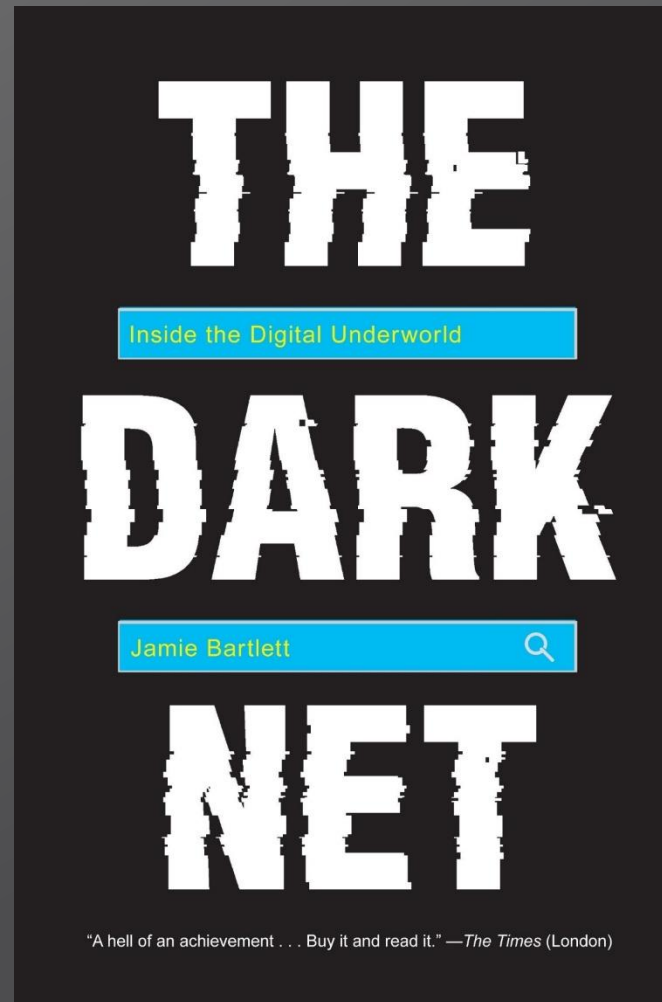
THE PEOPLE BEHIND THE KEYBOARDS

Professions on the platform



THE PEOPLE BEHIND THE KEYBOARDS

Population on the platform



Jamie Bartlett

GOODS TRANSFER - THE RISE OF CRYPTO'S

The Dark Web and Dark Web Technologies

GOODS TRANSFER - THE RISE OF CRYPTO'S

What is the payment process



GOODS TRANSFER - THE RISE OF CRYPTO'S

What is the payment process

The screenshot displays the WebMoney Transfer website interface. At the top, the WebMoney logo is on the left, followed by navigation links: 'About WebMoney', 'Personal', 'Business', and 'Help'. A search bar with the text 'Find information' is positioned to the right of these links. Further right are two buttons: 'Sign Up' (yellow) and 'Log In' (green). The main heading reads 'WebMoney Transfer' in a large blue font, with the subtitle 'universal payment system' below it. The page is organized into two main sections: 'Personal' and 'Business'. The 'Personal' section contains five icons with labels: 'Top-up' (green coins and globe), 'Pay' (orange TV, phone, lightbulb, and Wi-Fi), 'Withdraw' (red coins and arrow), 'Get a loan' (blue clock and hand), and 'Raise funds' (yellow people and coins). The 'Business' section contains five icons with labels: 'Accept payments' (green cash register), 'Make payments' (orange coins and arrows), 'Budget management' (red bar chart), 'Work management' (blue checkmarks and coins), and 'Secure transaction' (yellow handshake and shield).

GOODS TRANSFER - THE RISE OF CRYPTO'S

What is the payment process



Invisible Transactions

De Andrés said the dark web enables criminals to exploit three legitimate features of the modern internet: anonymization, encryption and virtual currencies. The latter has revolutionized money laundering and made cyber-enabled financial crime a top enforcement priority for investigators.

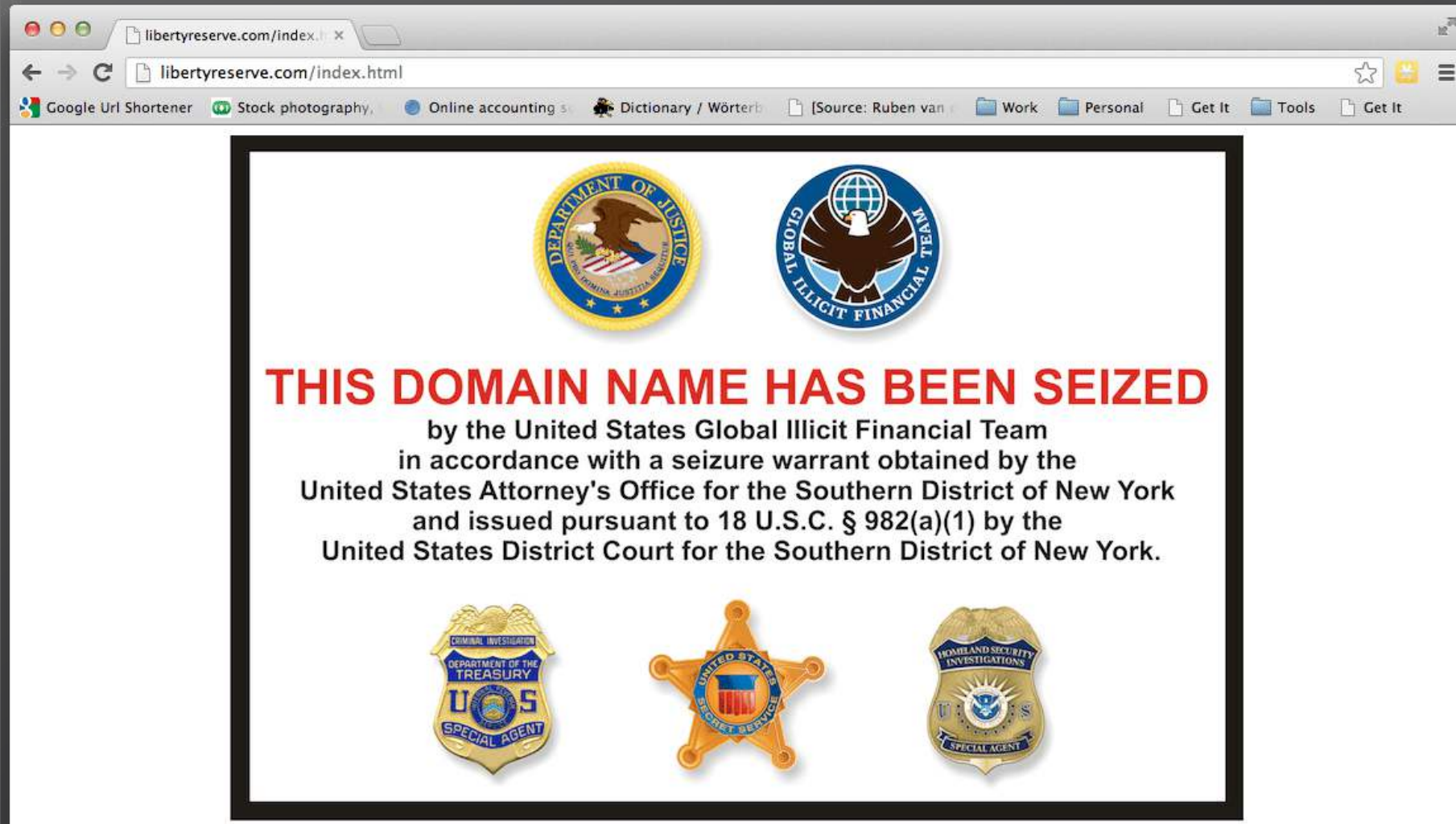
Organized crime groups are now using centralized virtual currencies like **WebMoney and Perfect Money** or decentralized cryptocurrencies like bitcoin to better cover their financial footprints.

Latin America and the Caribbean was home to the first major international virtual currency laundering scandal: the US government's takedown of underworld cyber banking system **Liberty Reserve** in 2013. Before its closure, authorities said the service laundered \$6 billion worth of illicit transactions tied to drug trafficking, investment fraud, credit card fraud, data theft and child pornography.

To further confound law enforcement, Latin American criminal organizations are employing "money-mule" networks, which structure virtual and conventional transactions into smaller and more innocuous-looking sums. De Andrés said each mule receives a commission of between 3 and 5 percent per transaction.

GOODS TRANSFER - THE RISE OF CRYPTO'S

What is the payment process



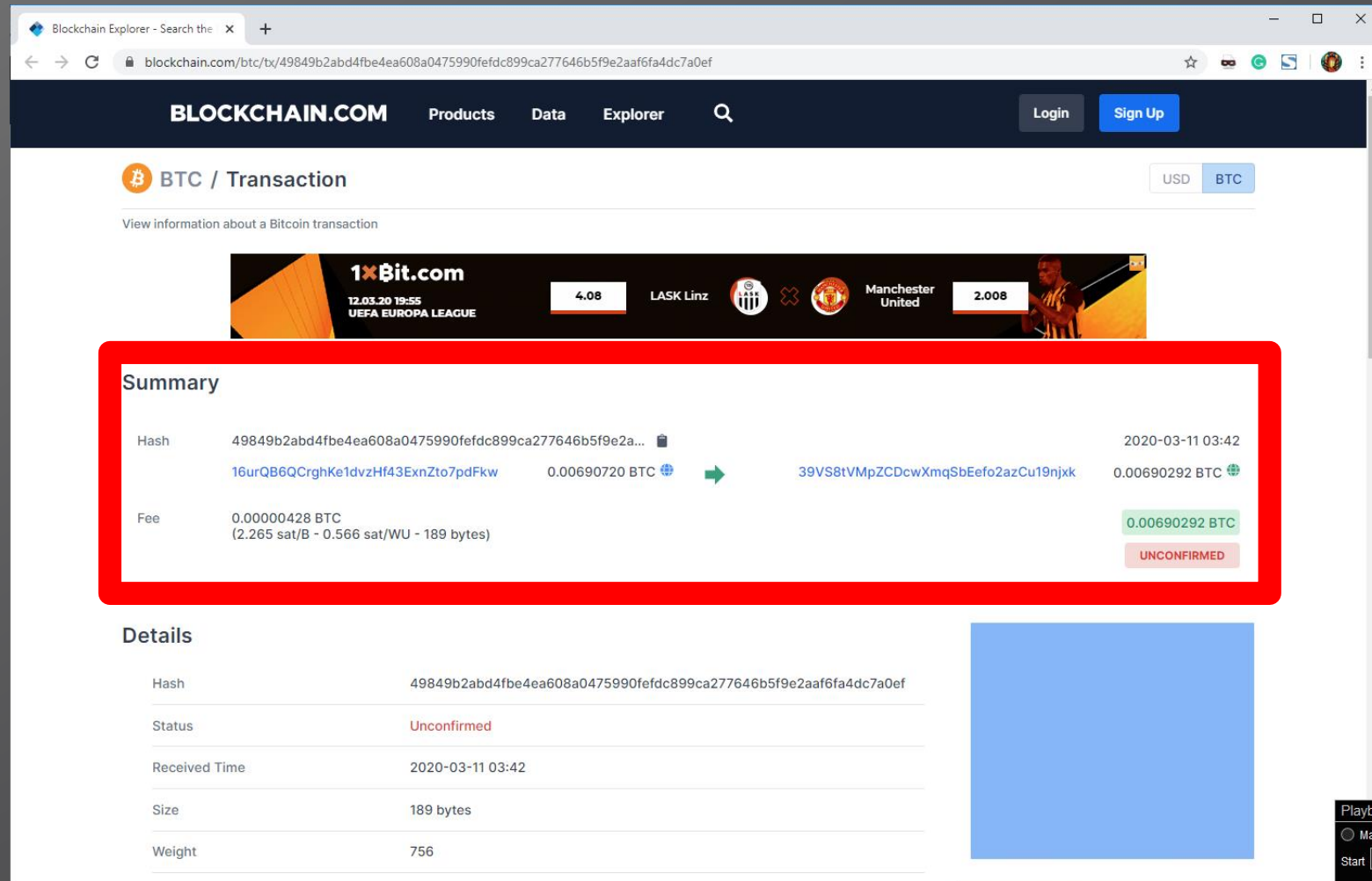
GOODS TRANSFER - THE RISE OF CRYPTO'S

The preferred methodology



GOODS TRANSFER - THE RISE OF CRYPTO'S

The preferred methodology



The screenshot displays the Blockchain Explorer interface for a Bitcoin transaction. The transaction is highlighted with a red border. The summary section shows the following details:

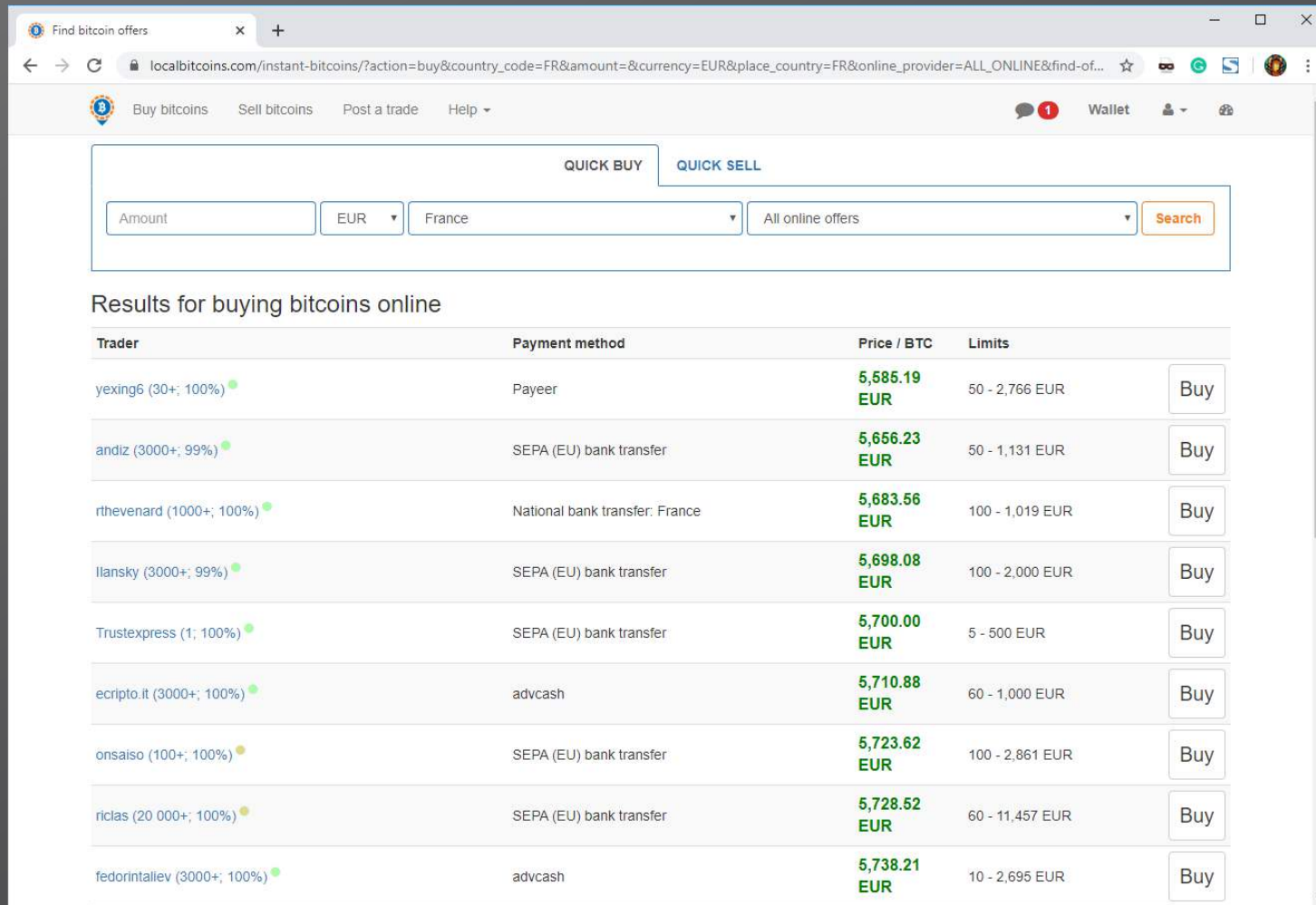
Field	Value
Hash	49849b2abd4fbe4ea608a0475990fefdc899ca277646b5f9e2a... 16urQB6QCrgHKe1dvzHf43ExnZto7pdFkw
Amount	0.00690720 BTC
Fee	0.00000428 BTC (2.265 sat/B - 0.566 sat/WU - 189 bytes)
Net Amount	0.00690292 BTC
Status	UNCONFIRMED

The transaction is dated 2020-03-11 03:42. The details section below the summary provides further information:

Field	Value
Hash	49849b2abd4fbe4ea608a0475990fefdc899ca277646b5f9e2aaf6fa4dc7a0ef
Status	Unconfirmed
Received Time	2020-03-11 03:42
Size	189 bytes
Weight	756

GOODS TRANSFER - THE RISE OF CRYPTO'S

The preferred methodology



The screenshot shows the localbitcoins.com website interface. At the top, there are navigation links: "Buy bitcoins", "Sell bitcoins", "Post a trade", and "Help". On the right, there is a "Wallet" section with a notification icon. The main content area features a search bar with the following fields: "Amount", "EUR", "France", and "All online offers", with a "Search" button. Below the search bar, the heading "Results for buying bitcoins online" is displayed. A table lists various trading offers with columns for "Trader", "Payment method", "Price / BTC", and "Limits". Each offer includes a "Buy" button.

Trader	Payment method	Price / BTC	Limits
yexing6 (30+; 100%)	Payeer	5,585.19 EUR	50 - 2,766 EUR
andiz (3000+; 99%)	SEPA (EU) bank transfer	5,656.23 EUR	50 - 1,131 EUR
rthevenard (1000+; 100%)	National bank transfer: France	5,683.56 EUR	100 - 1,019 EUR
iliansky (3000+; 99%)	SEPA (EU) bank transfer	5,698.08 EUR	100 - 2,000 EUR
Trustexpress (1; 100%)	SEPA (EU) bank transfer	5,700.00 EUR	5 - 500 EUR
cripto.it (3000+; 100%)	advcash	5,710.88 EUR	60 - 1,000 EUR
onsaiso (100+; 100%)	SEPA (EU) bank transfer	5,723.62 EUR	100 - 2,861 EUR
riclas (20 000+; 100%)	SEPA (EU) bank transfer	5,728.52 EUR	60 - 11,457 EUR
fedorintaliev (3000+; 100%)	advcash	5,738.21 EUR	10 - 2,695 EUR

GOODS TRANSFER - THE RISE OF CRYPTO'S

The preferred methodology

Enter BestMixer code: ?

optional

Enter your address: ⁱ

33.63%
2hr. 21min.

33.12%
4hr. 41min. ×

33.25%
6hr. 10min. ×

+ Add address

Service fee: ⁱ **1.0000%**

Reserves for mixing: ⁱ **Alpha Pool**

Percentage distribution: ⁱ

Transfer delay: ⁱ

Mixing strength meter: ?

Strong

GOODS TRANSFER - THE RISE OF CRYPTO'S

The preferred methodology – Monero Evolution

masterthecrypto

COMPARISON OF ANONYMOUS CRYPTOS

	PRIVATE	FUNGIBLE	DECENTRALIZED
MONERO	✓	✓	✓
bitcoin	✗	✗	✓
CASH	?	?	✗
DASH	✗	✗	✗
VERGE	✗	✗	✓

© 2020 Check Point Software Technologies Ltd.

BAD ACTORS SPACE

Syndicates

Execution

THE DARK NET FOOD CHAIN

Syndicates structure & Roles

Maze Team official press release. March 18 2020

Due to situation with incoming global economy crisis and virus pandemic, our Team decided to help commercial organizations as much as possible. We are starting exclusive discounts season for everyone who have faced our product. Discounts are offered for both decrypting files and deleting of the leaked data. To get the discounts our partners should contact us using the chat or our news resource.

In case of agreement all the info will be deleted and decryptors will be provided.

The offer applies to both new partners and the «archived» ones. We are always open for cooperation and communication.

We also stop all activity versus all kinds of medical organizations until the stabilization of the situation with virus

THE DARK NET FOOD CHAIN

Life of a hacker



THE DARK NET FOOD CHAIN

Syndicates structure & Roles



Ivan Viktorovich Klepikov
Aliases: “petr0vich”, “nowhere”

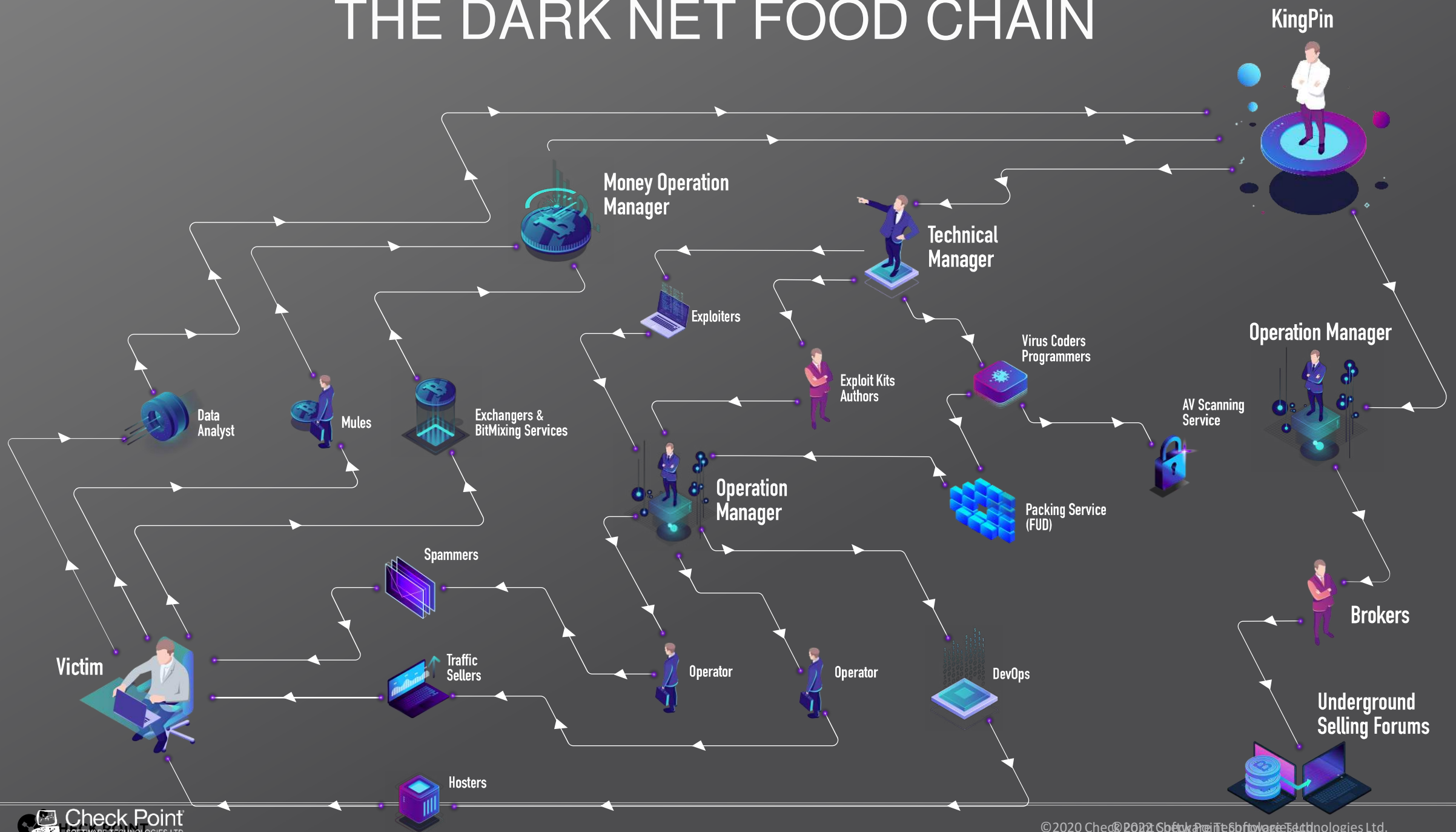


Alexey Dmitrievich Bron
Alias: “thehead”



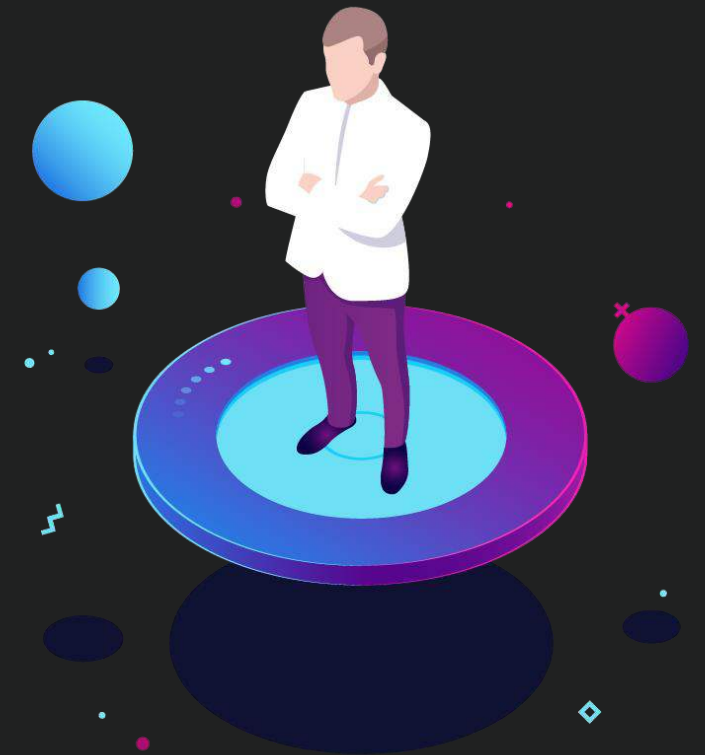
Vyacheslav Igorevich Penchukov
Aliases: “tank”, “father”

THE DARK NET FOOD CHAIN

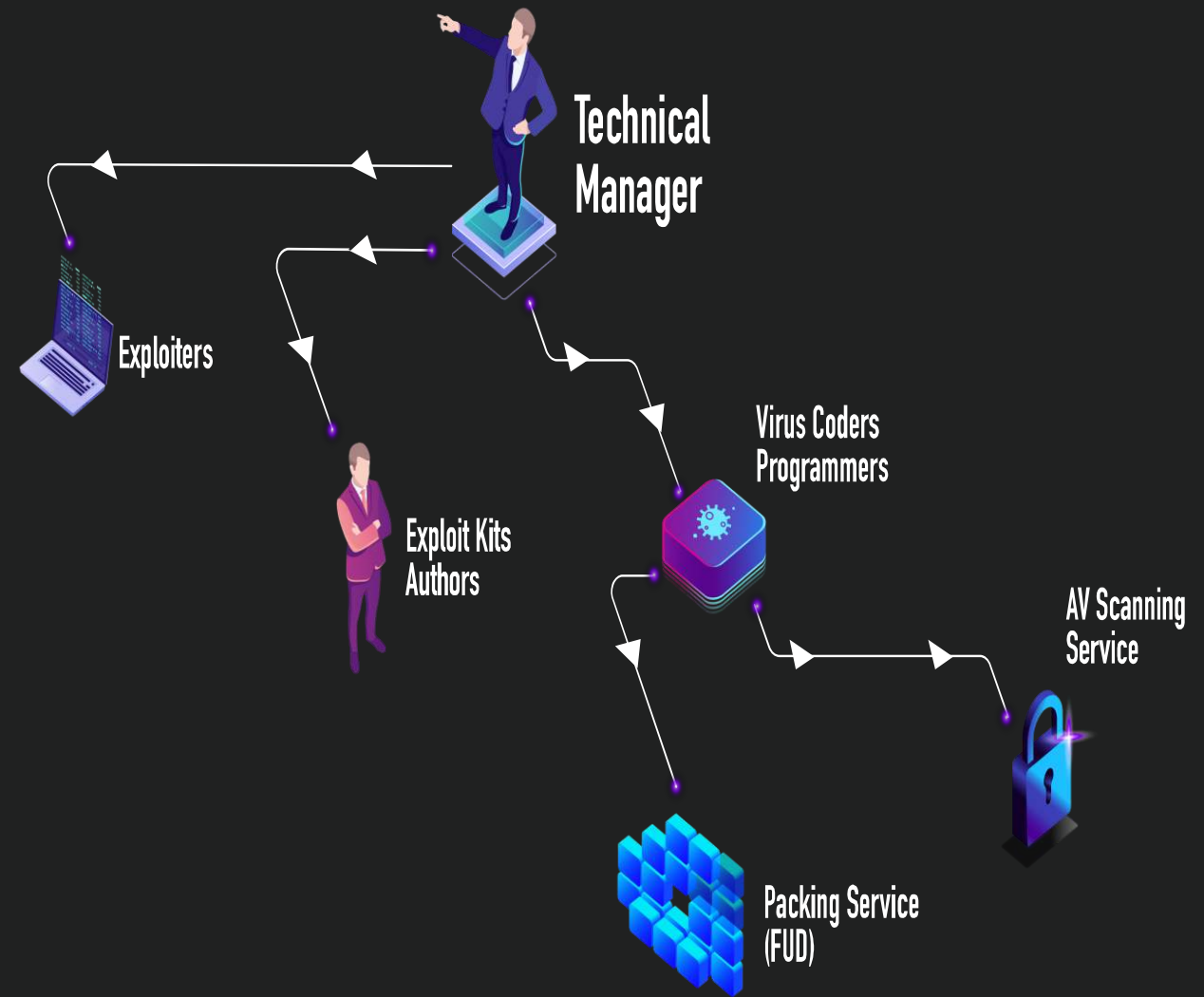


- The leader!
- Powerful criminal
- Well connected upside down in the crime scene
- And don't mess with him

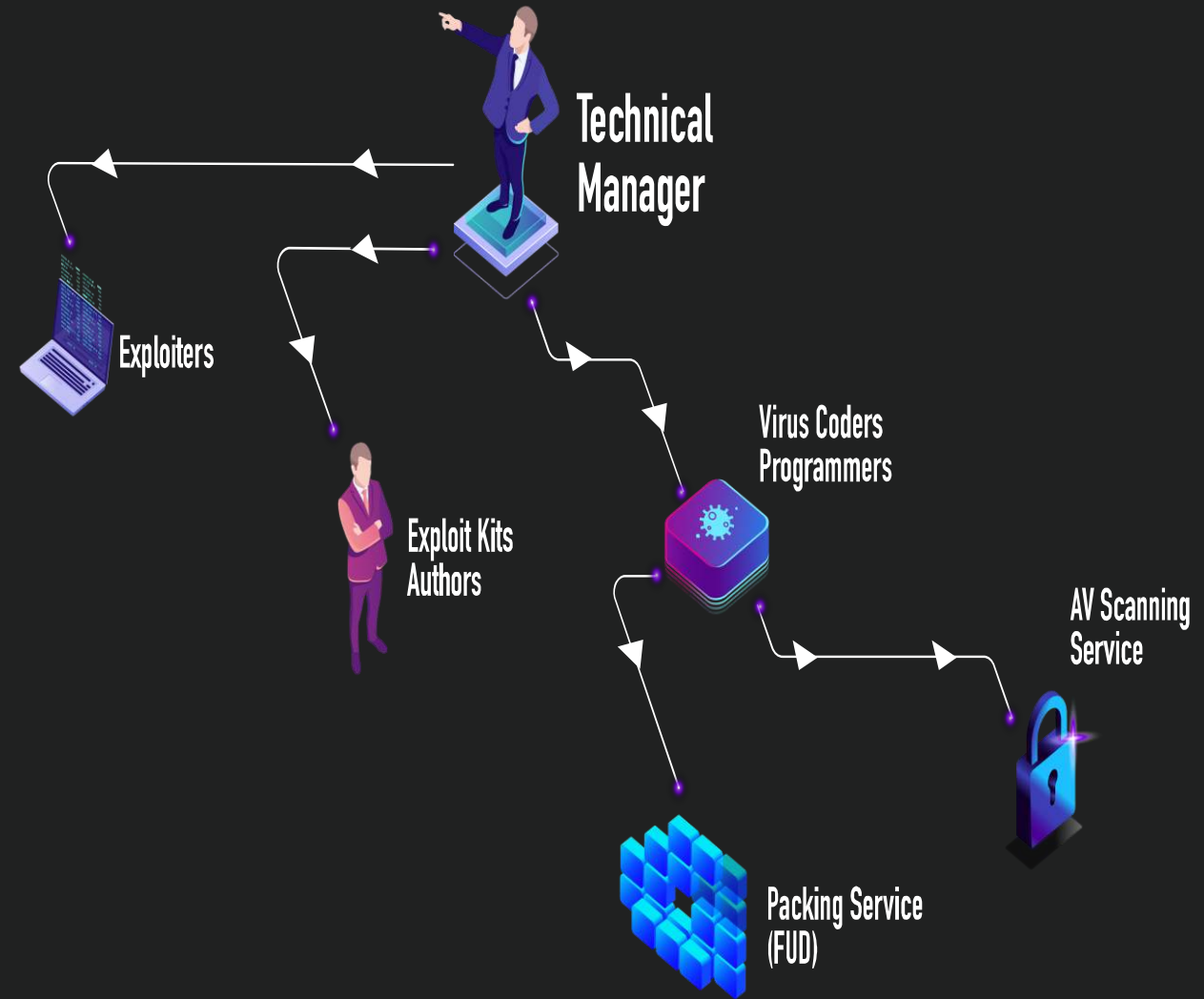
KingPin



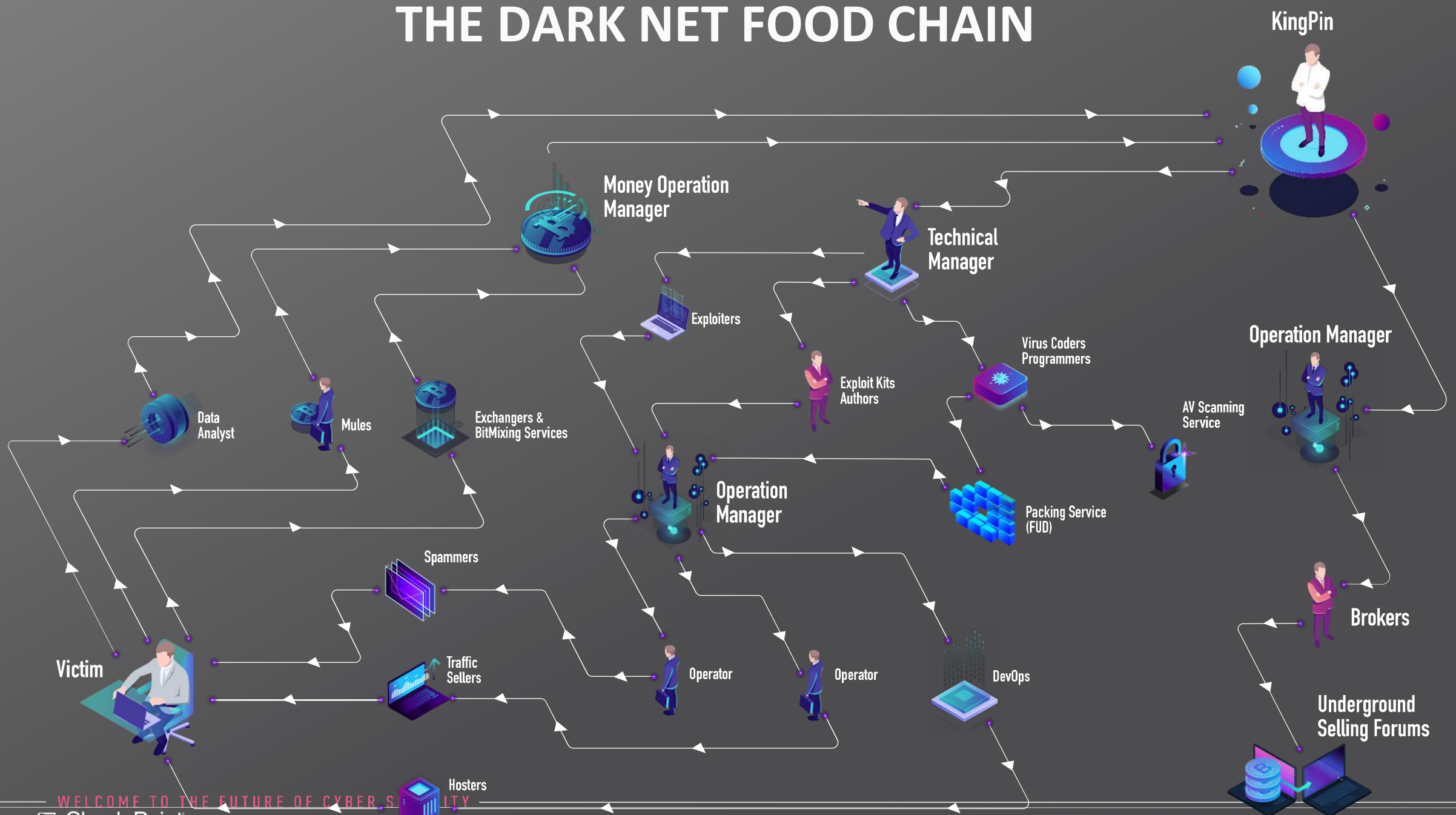
- Malware authors
- Exploit kit developers
- Phishing kit developers
- Hacking tools developers



- Developing 0-day exploits
- Weaponizing newly published exploits (1-days)
- Allowing malware authors to evade AV signatures
- Selling it as standalone exploit



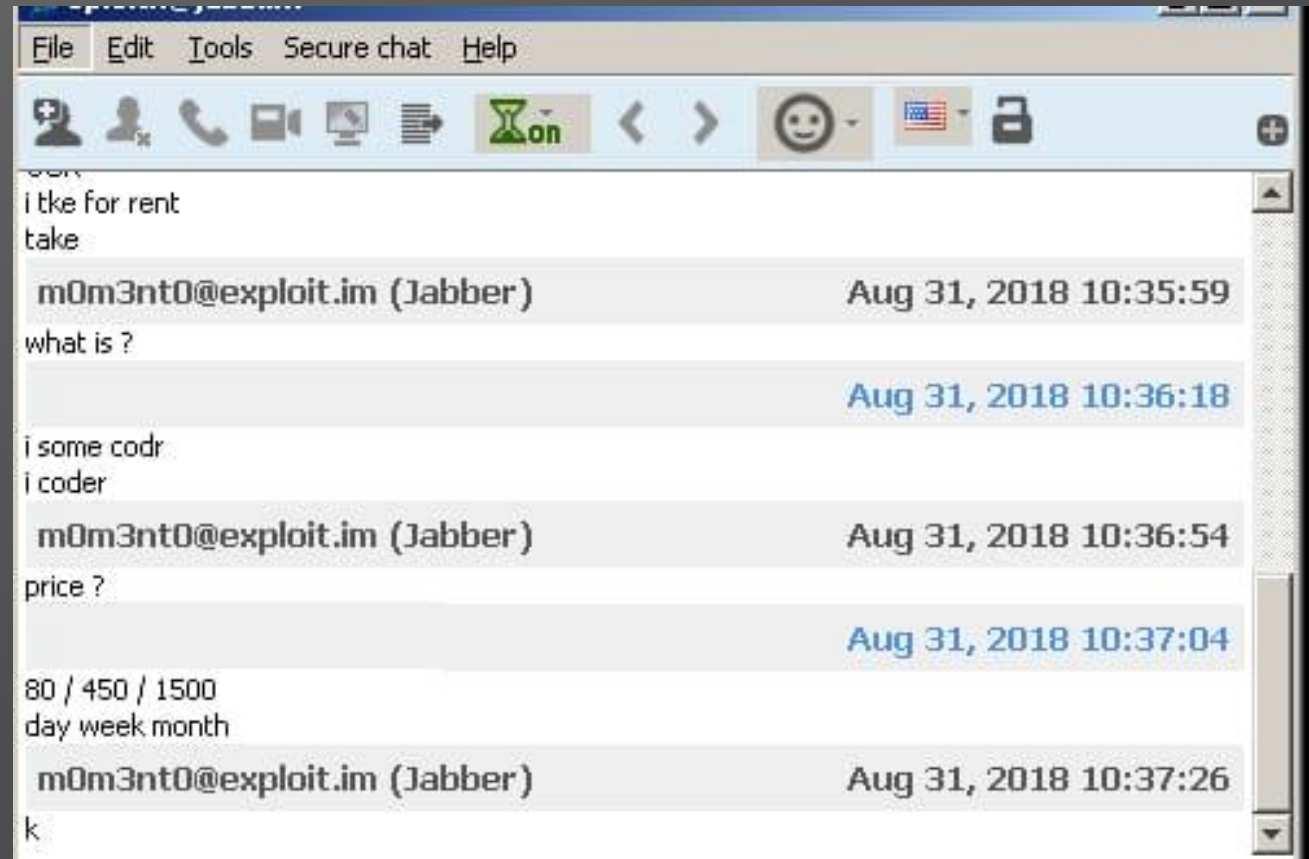
THE DARK NET FOOD CHAIN



WELCOME TO THE FUTURE OF CYBER SECURITY

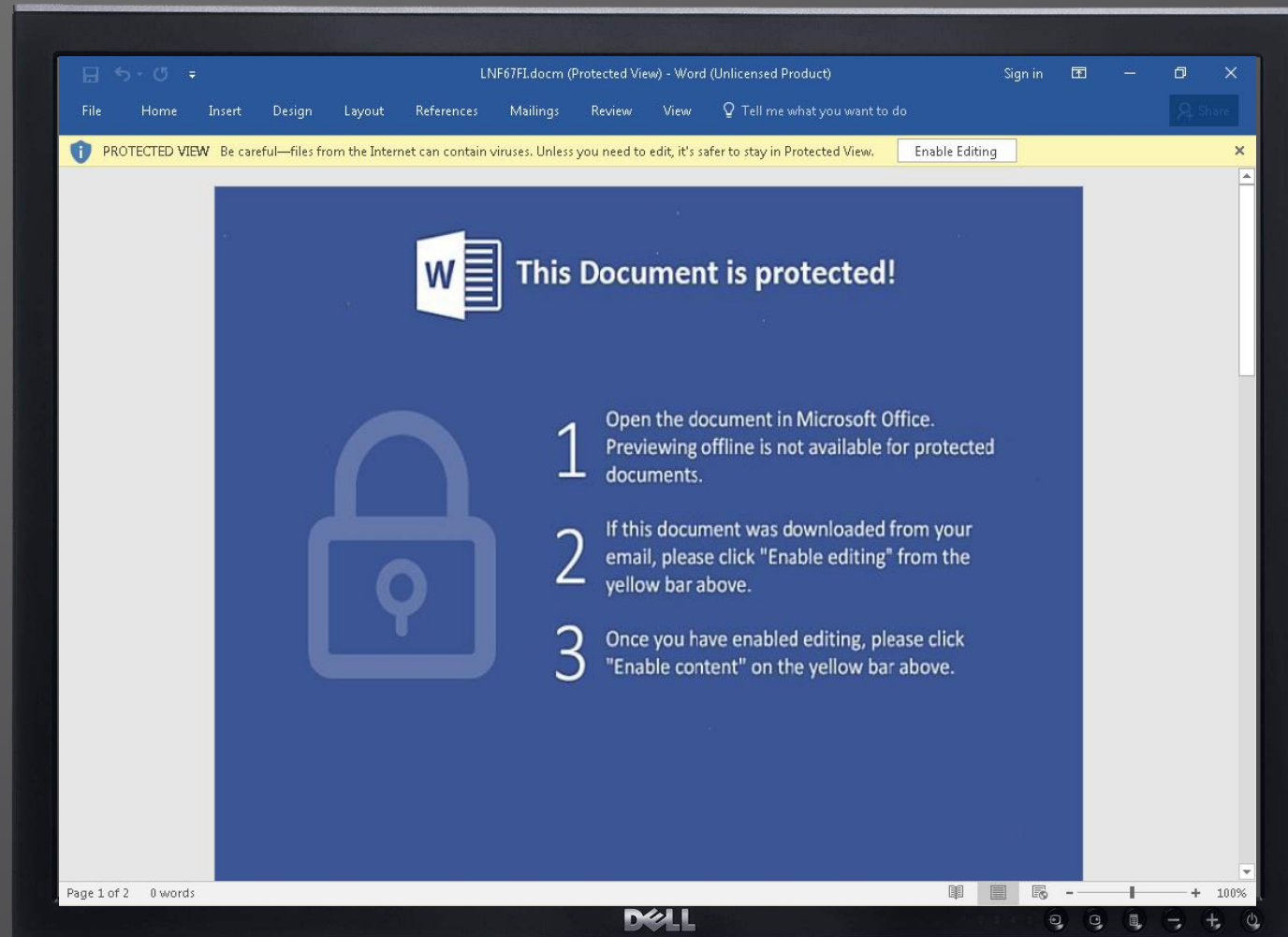
KNOWN ATTRIBUTED EXAMPLES

Collaboration and Execution – Locky Showcase



KNOWN ATTRIBUTED EXAMPLES

Collaboration and Execution – Locky Showcase



KNOWN ATTRIBUTED EXAMPLES

Collaboration and Execution – Locky Showcase

```
-*_=_+  
-$$$=-=._$$~.=.-+~  
.|.~_|-.*~--|=_-_=  
+_~$=-=
```

!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.

More information about the RSA and AES can be found here:

[http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.

To receive your private key follow one of the links:

If all of this addresses are not available, follow these steps:

1. Download and install Tor Browser: <https://www.torproject.org/download/download-easy.html>
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: g46mbrzpfsonuk.onion/9HQH9AYFTGQ0YZH6
4. Follow the instructions on the site.

!!! Your personal identification ID: 9HQH9AYFTGQ0YZH6 !!!

```
$__--~$.  
|_|==|
```

DELL



KNOWN ATTRIBUTED EXAMPLES

Collaboration and Execution



KNOWN ATTRIBUTED EXAMPLES

Collaboration and Execution

Problem loading page x Locky Decryptor Page x +

bvbers4hm6dx65f.onion/AA8F082137AA8933

Languages: English

Locky Decryptor™

We present a special software - Locky Decryptor™ - which allows to decrypt and return control to all your encrypted files.

How to buy Locky Decryptor™?

- 1 You can make a payment with BitCoins, there are many methods to get them.
- 2 You should register BitCoin wallet:
[Simplest online wallet](#) or [Some other methods of creating wallet](#)
- 3 Purchasing BitCoins, although it's not yet easy to buy bitcoins, it's getting simpler every day.
Here are our recommendations:
 - [localbitcoins.com \(WU\)](#) Buy Bitcoins with Western Union. Recommended for fast, simple service. Payment Methods: Western Union, Bank of America, Cash by FedEx, Moneygram, Money Order. In NYC: Bitcoin ATM, in person.
 - [localbitcoins.com](#) Service allows you to search for people in your community willing to sell bitcoins to you directly.
 - [cash.io](#) Buy Bitcoins with VISA/MASTERCARD or wire transfer.
 - [btcdirect.eu](#) The best for Europe.
 - [bitquick.co](#) Buy Bitcoins instantly for cash.
 - [howtobuybitcoins.info](#) An international directory of bitcoin exchanges.
 - [cashintocoins.com](#) Bitcoin for cash.
 - [coinjar.com](#) CoinJar allows direct bitcoin purchases on their site.
 - [anxpro.com](#)
 - [bitylicious.com](#)
- 4 Send 2.9997 BTC to Bitcoin address:
`1Mr2LVsyFkhaZVoxE6M2Lw9dzNjnttZ1z`
Note: Payment pending up to 30 mins or more for transaction confirmation, please be patient...

Date	Amount BTC	Transaction ID	Confirmations
2016-03-09 15:21:13	2.9997	f703fb422fa0c9c0e3fc0a0d702fb107048a8c5e1ea7f670b612ba0d974f1af	0
2016-03-09 01:37:39	0.0003	fe03047bc5587bf007b2928de506b4ae504e5d8716033c45681a25f70759157c	93
- 5 Refresh the page and download decryptor.
When Bitcoin transactions will receive one confirmation, you will be redirected to the page for downloading the decryptor.

DELL



“It’s a wonder you made your way out”

HOW TO STAY SAFE?

Tip for a secured journey on the Dark Net



Disable JS



Use VM's



Pseudonym



Jargon



THANK YOU

YOU DESERVE THE BEST SECURITY