

Come a little closer



Funeral services Bergmann & Sohn

Jonasstraße 7, 10551 Berlin-Tiergarten, phone: (030) 266 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....”

ARL SANDBURG

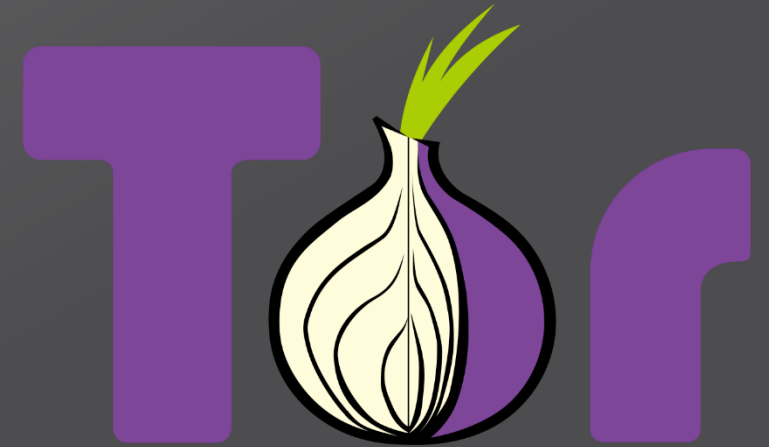
A deeper look at network architecture

“BEGIN AT THE BEGINNING” LEWIS CARROLL

The Dark Web Evolution



Michael Reed

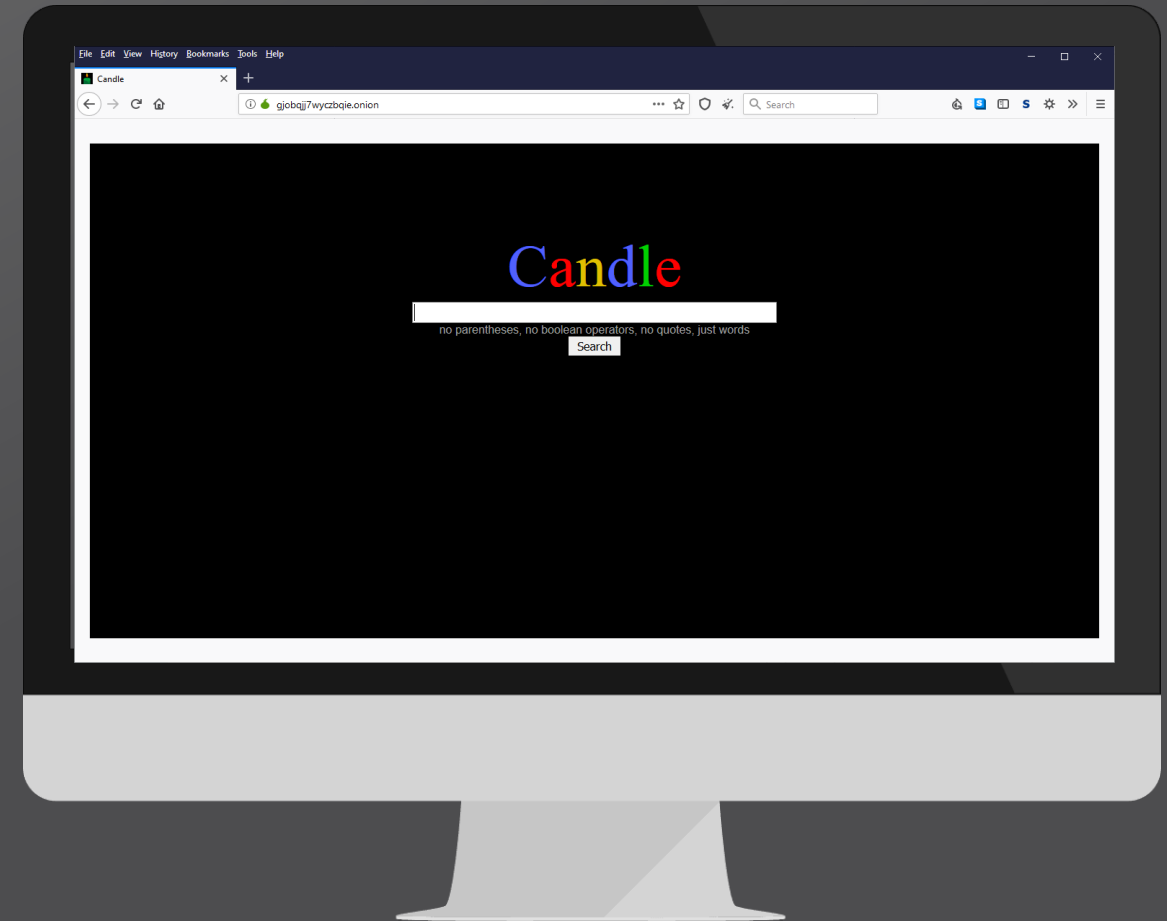
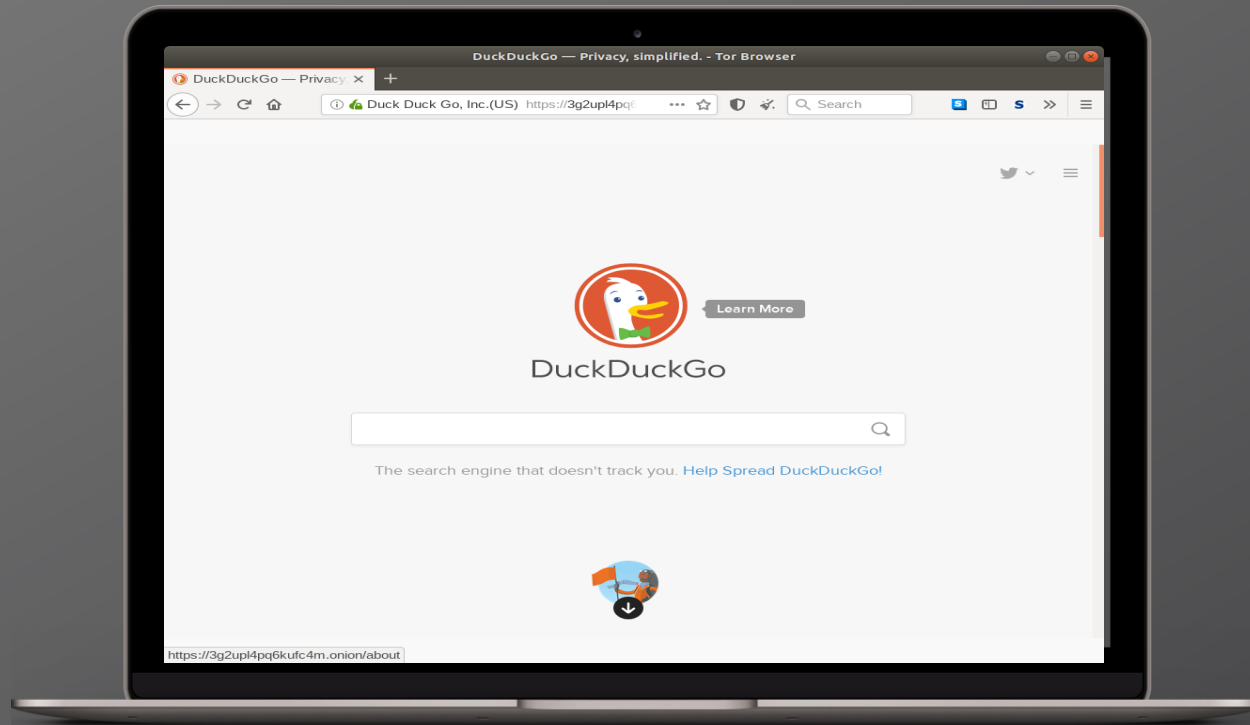


A brief capture of the Tor browser history and evolution

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

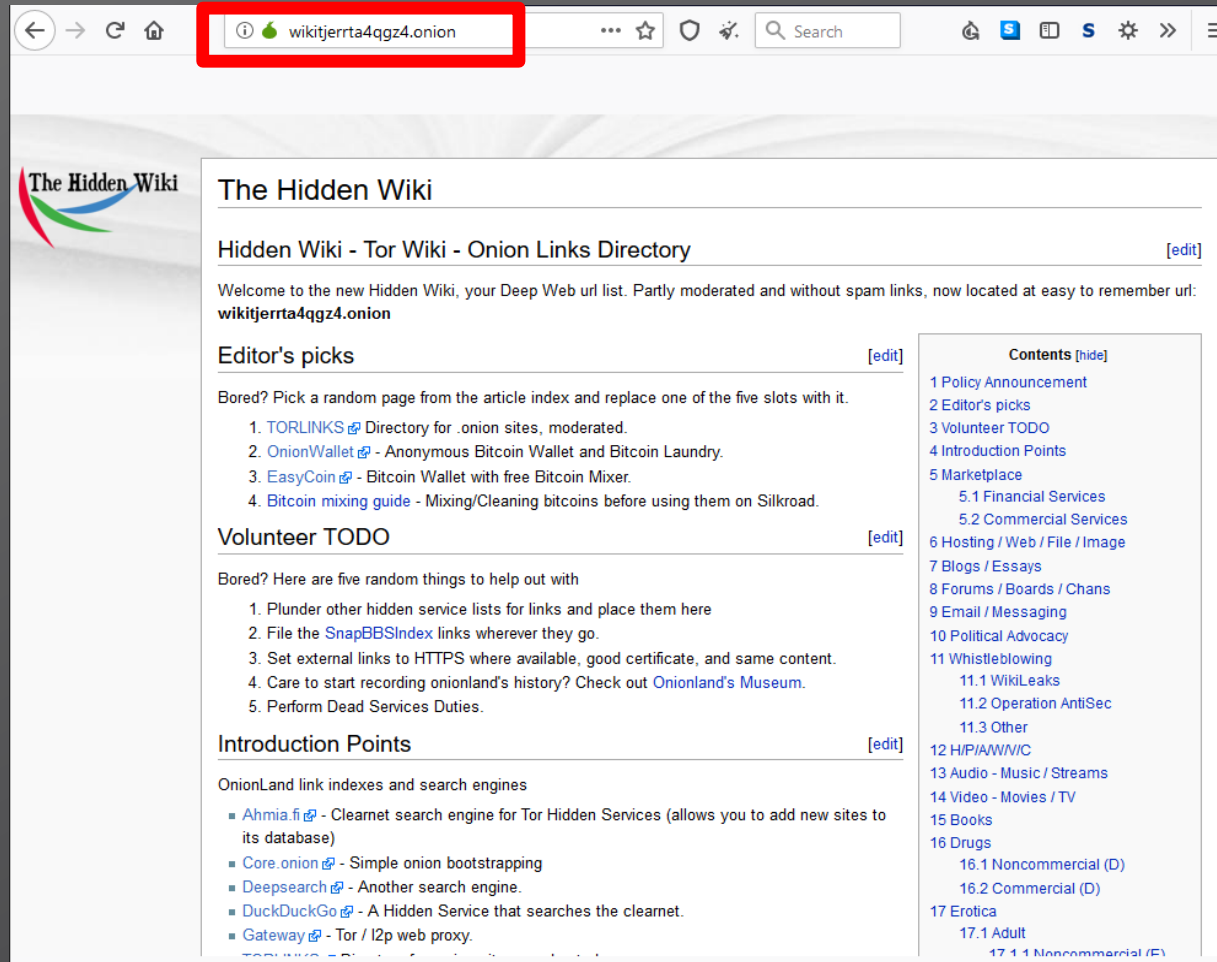
“BEGIN AT THE BEGINNING”

What is TOR?



“BEGIN AT THE BEGINNING”

The Dark Web Evolution – Indexed & non Indexed pages



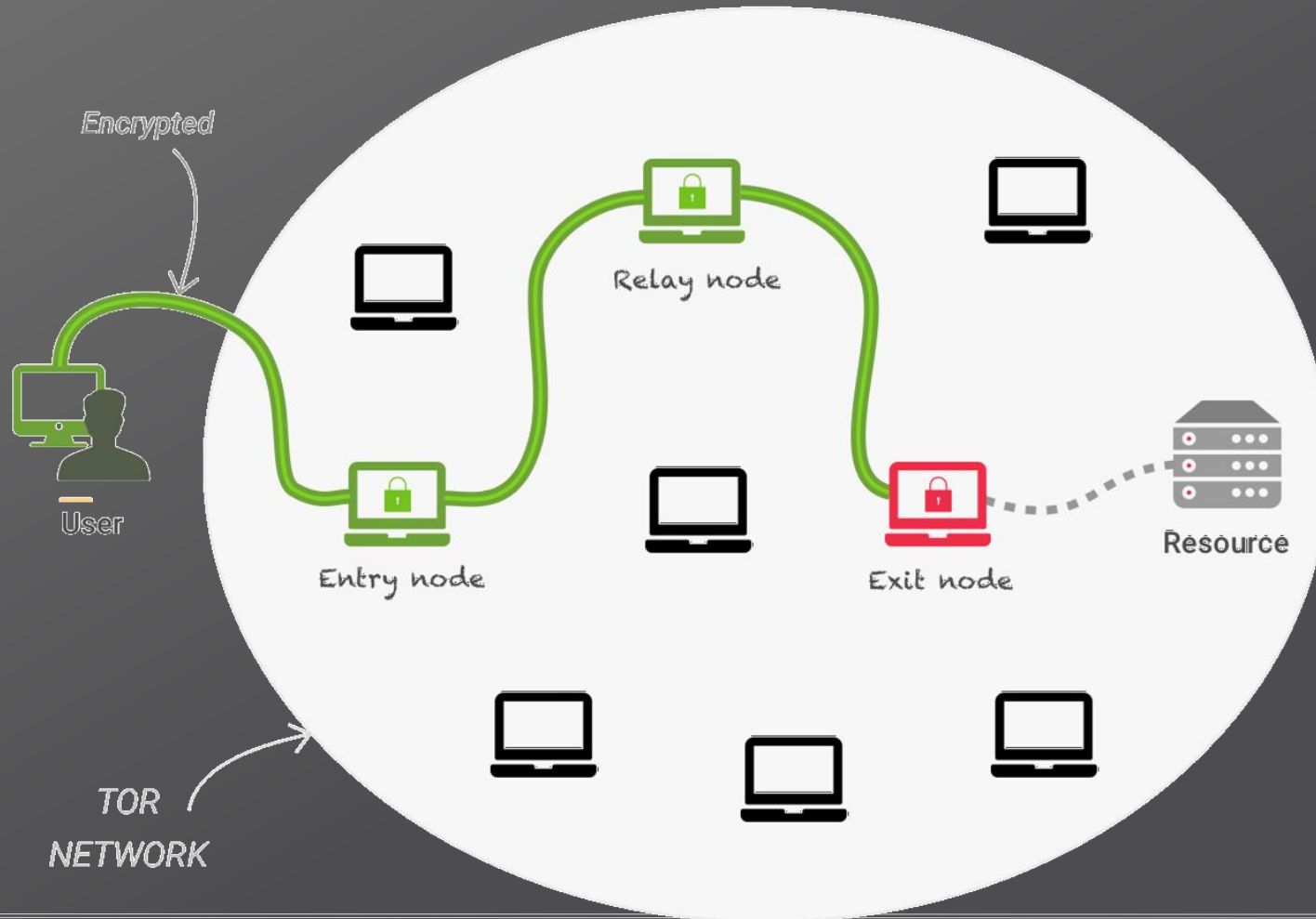
“IF YOU DON'T KNOW WHERE YOU ARE GOING ANY ROAD CAN TAKE YOU THERE”

Network topology, VPN and encryption process



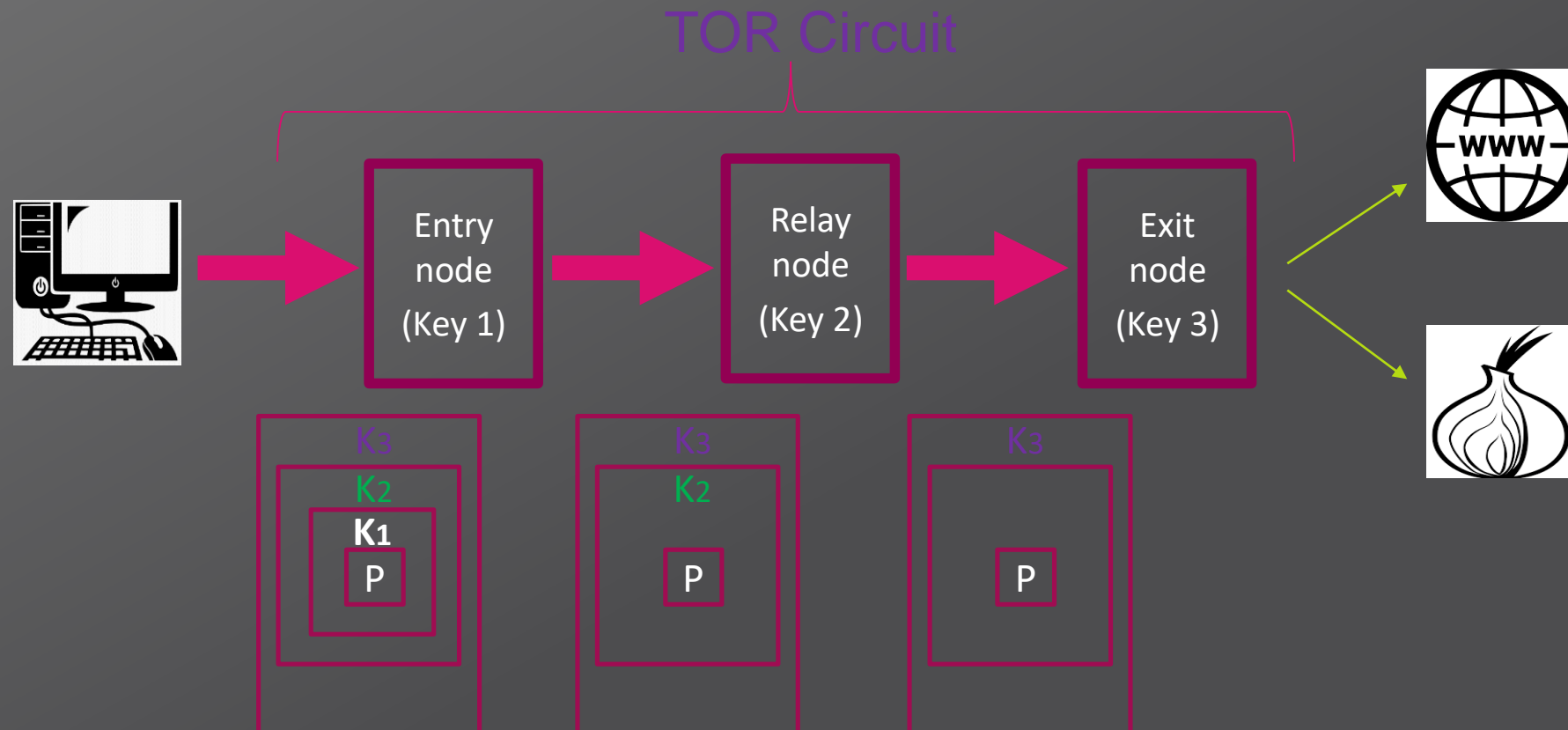
“IF YOU DON'T KNOW WHERE YOU ARE GOING ANY ROAD CAN TAKE YOU THERE”

Network topology, VPN and encryption process



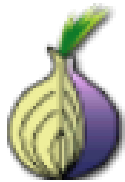
“IF YOU DON'T KNOW WHERE YOU ARE GOING ANY ROAD CAN TAKE YOU THERE”

Network topology, VPN and encryption process

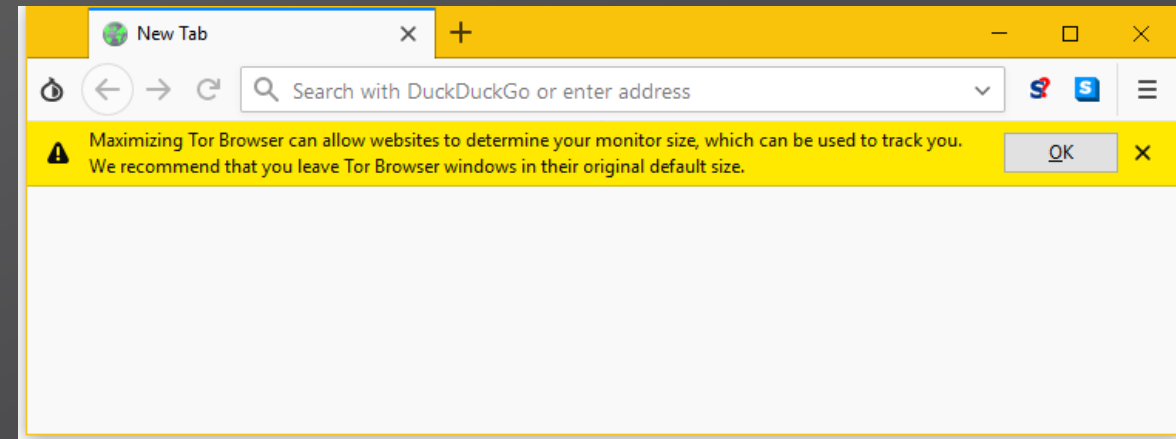
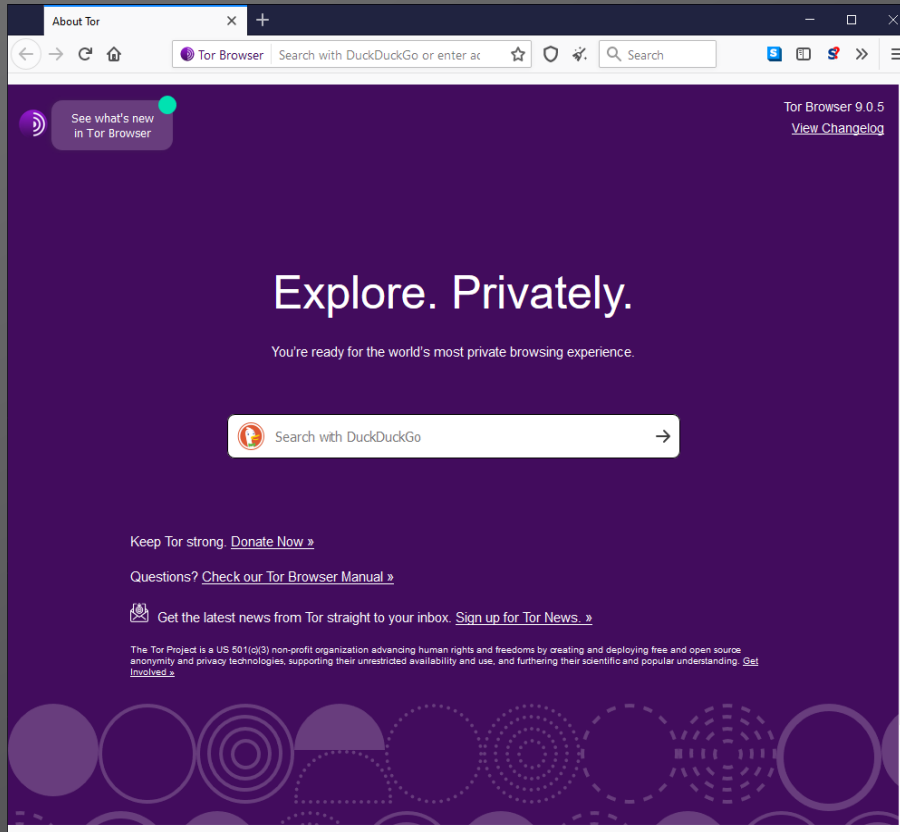


“WHO IN THE WORLD AM I?”

How does One keep Anonymous on the Dark Web?

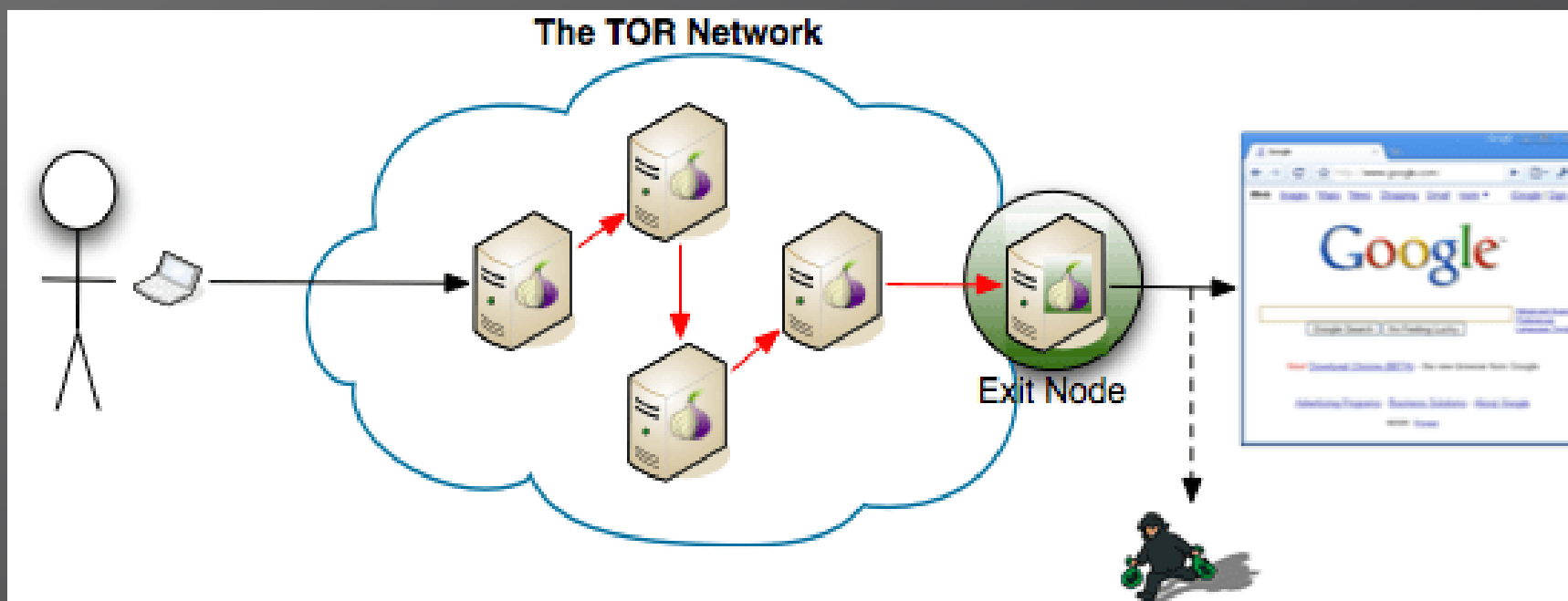


torbrowser-instal
l-win64-9.0.5_en-
US



“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)

[REDACTED]
CT SIGDEV
[REDACTED]
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

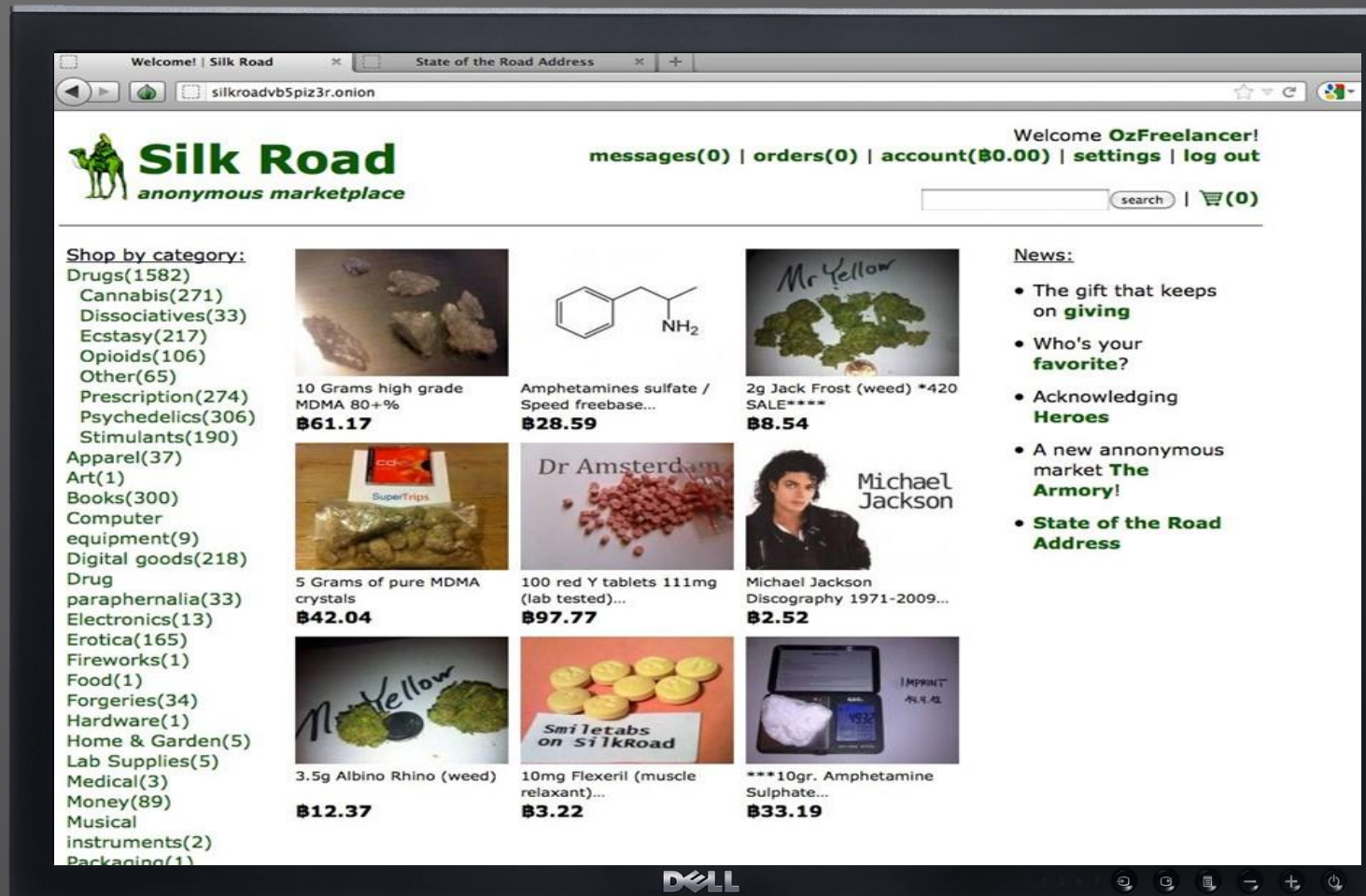


REVEALING THE UNSEEN

What is the new platform

MORE THAN A MARKETPLACE

What is to be found on this platform



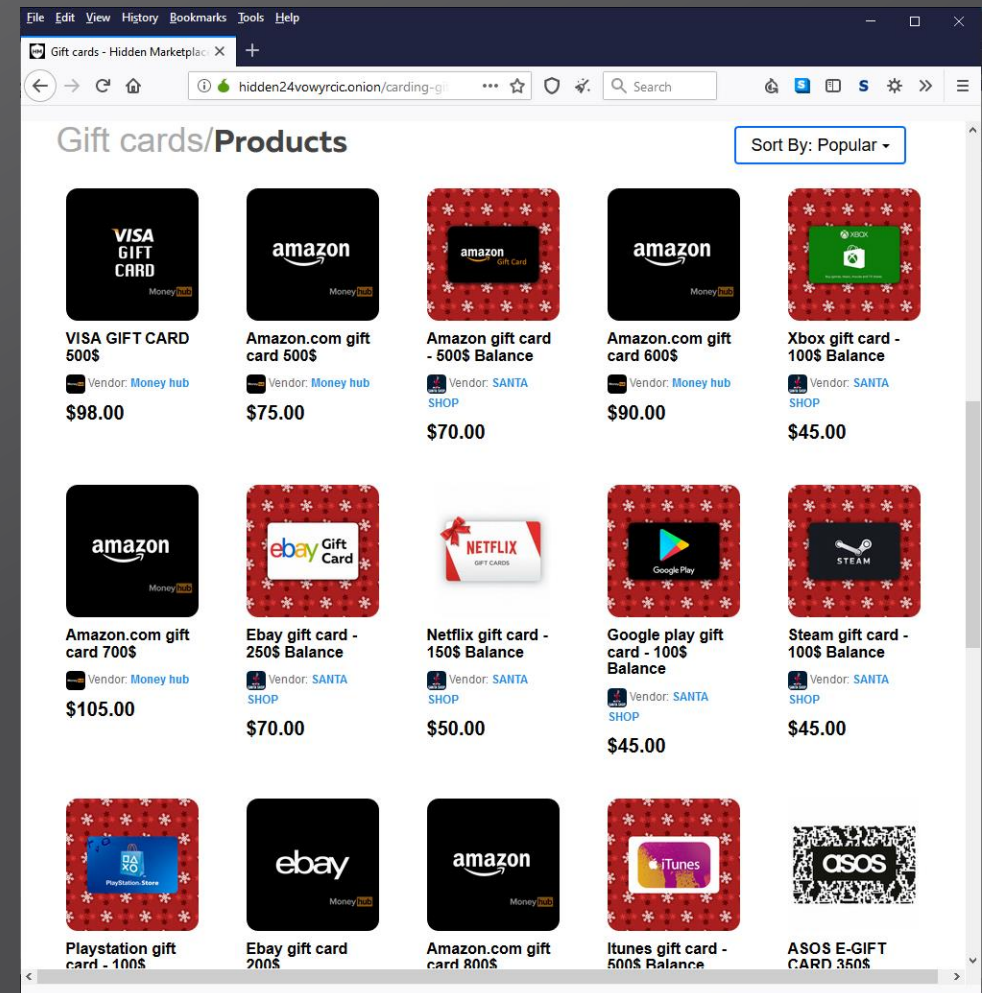
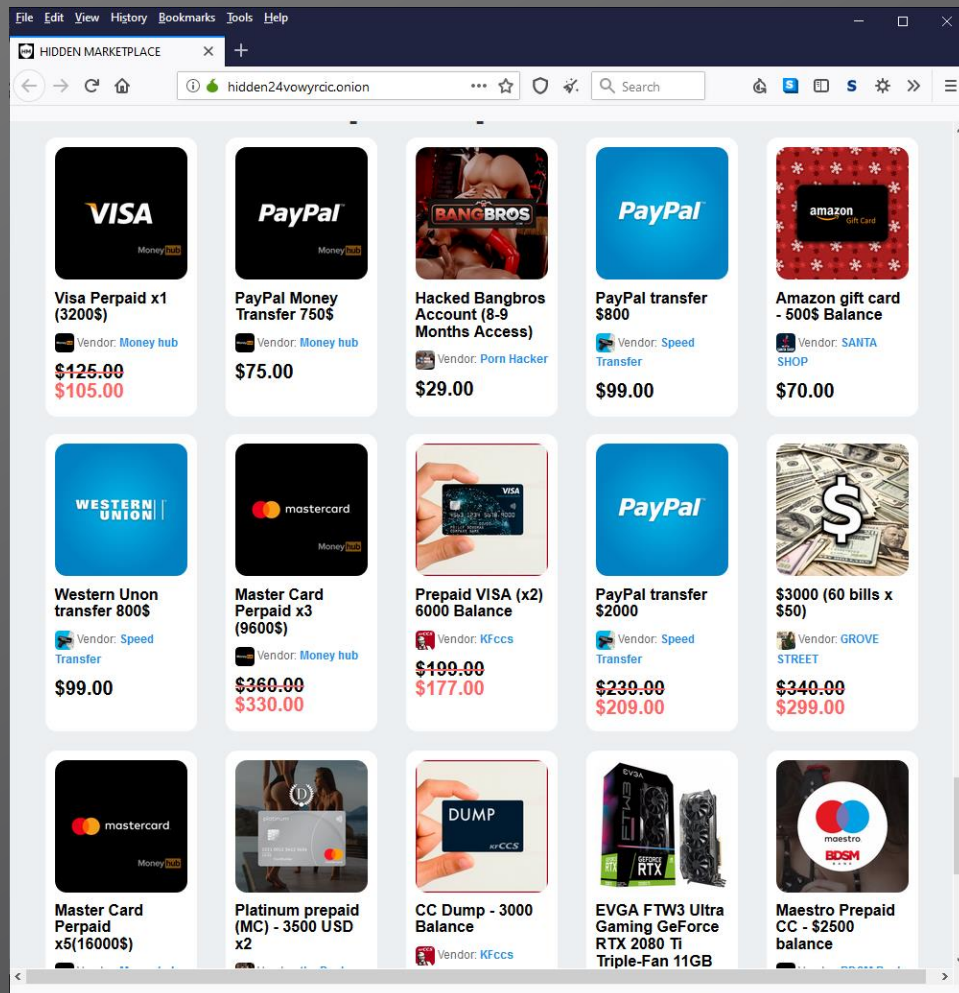
MORE THAN A MARKETPLACE

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



PRODUCTSFAQSREGISTERLOGIN


Stimulants



Uncut Cocaine and Speed!

Product	Price	Quantity
1g pure Cocaine	85 EUR = 0.010 ₿	<input type="text" value="1"/> X Buy now
2g pure Cocaine	160 EUR = 0.019 ₿	<input type="text" value="1"/> X Buy now
5g pure Cocaine	375 EUR = 0.045 ₿	<input type="text" value="1"/> X Buy now
25g pure Cocaine	1375 EUR = 0.166 ₿	<input type="text" value="1"/> X Buy now
10g pure Speed	90 EUR = 0.011 ₿	<input type="text" value="1"/> X Buy now
50g pure Speed	390 EUR = 0.047 ₿	<input type="text" value="1"/> X Buy now
100g pure Speed	650 EUR = 0.078 ₿	<input type="text" value="1"/> X Buy now
2g pure Crystal Meth	100 EUR = 0.012 ₿	<input type="text" value="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 ₿	<input type="text" value="1"/> X Buy now
50g Purple Kush	350 GBP = 0.047 ₿	<input type="text" value="1"/> X Buy now
100g Purple Kush	650 GBP = 0.087 ₿	<input type="text" value="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

DN HACKING TEAM

hacknp5rq6sigds.onion

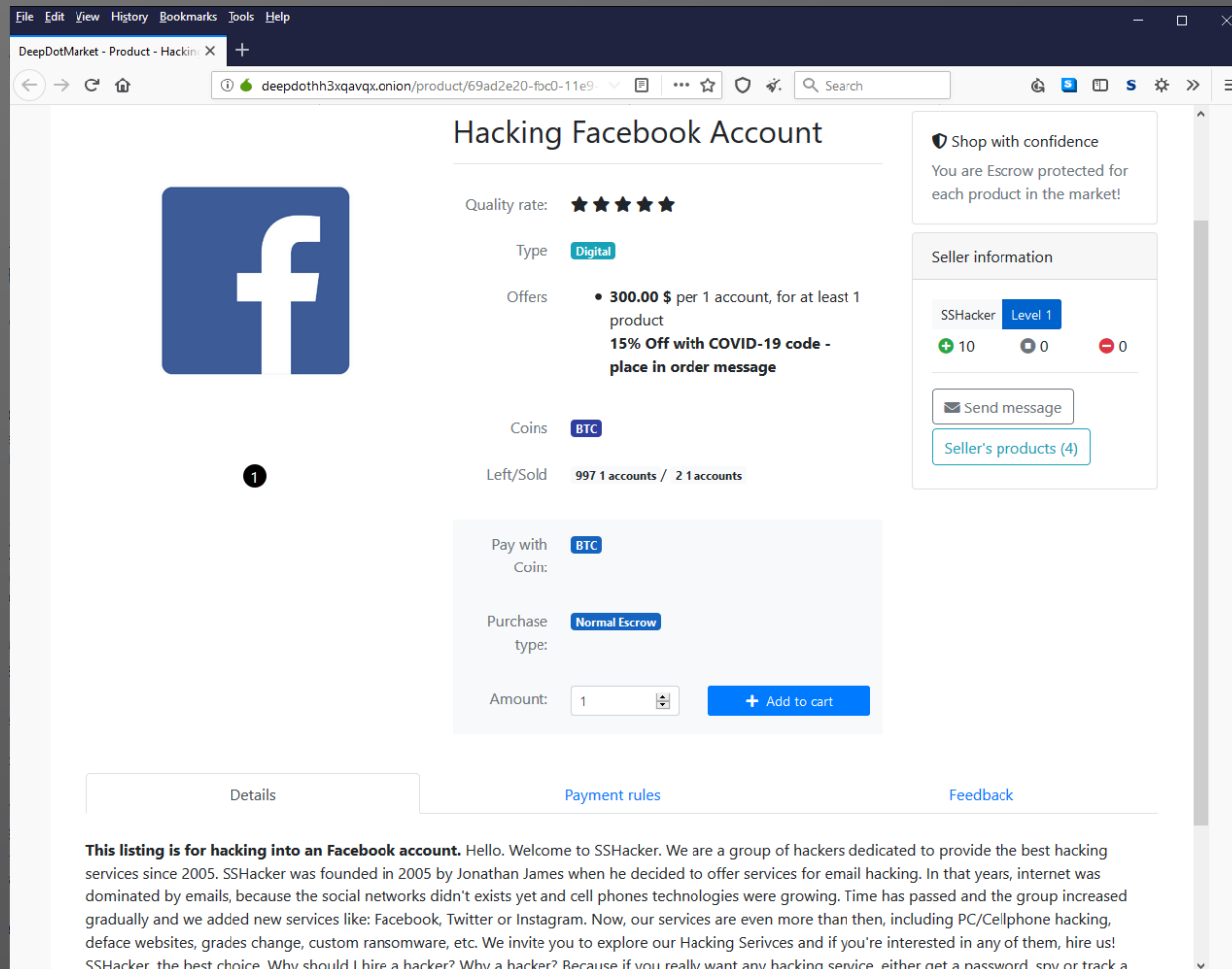
DEEPWEB HACKERTEAM



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



DeepDotMarket - Product - Hackin

deepdothh3xqavqx.onion/product/69ad2e20-fbc0-11e9-

Hacking Facebook Account

Quality rate: ★★★★★

Type: Digital

Offers: • 300.00 \$ per 1 account, for at least 1 product
15% Off with COVID-19 code - place in order message

Coins: BTC

Left/Sold: 997 1 accounts / 2 1 accounts

Pay with: BTC
Coin:

Purchase type: Normal Escrow

Amount: 1 + Add to cart

Shop with confidence
You are Escrow protected for each product in the market!

Seller information

SSHacker Level 1
+10 0 0

Send message

Seller's products (4)


Details Payment rules Feedback

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 displaying the 'Hidden24 Marketplace' website. The browser's address bar shows the URL 'hidden24vowyrdc.onion/index.php?route=product/manufacture/info&manu...'. The website's header includes a navigation bar with links for 'Support', 'Login', and 'Register', and a 'Bitcoin - \$7 868' status. The main content area features a product listing for 'Mystery Boxes Online'. The product is described as a surprise gift box containing various items, with a 'SEND MESSAGE' button. The seller's information is displayed at the bottom, including 'Seller since 11.2019', '331 Sales', '7 Products', and a 'Rating' of five stars.

File Edit View History Bookmarks Tools Help

Mystery Boxes

hidden24vowyrdc.onion/index.php?route=product/manufacture/info&manu...

Last 24h: Online - 1187 New users - 132 Guests - 1747 Bitcoin - \$7 868 www.coinbase.com Support Login Register

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

The screenshot shows a dark web marketplace interface with a dark background and white text. It features four vendor listings arranged in a 2x2 grid. Each listing includes a vendor name, a brief description of services, member statistics, status, and a star rating. A red 'PROVIDOR' badge is visible on the 'Click'n'Cash' listing.

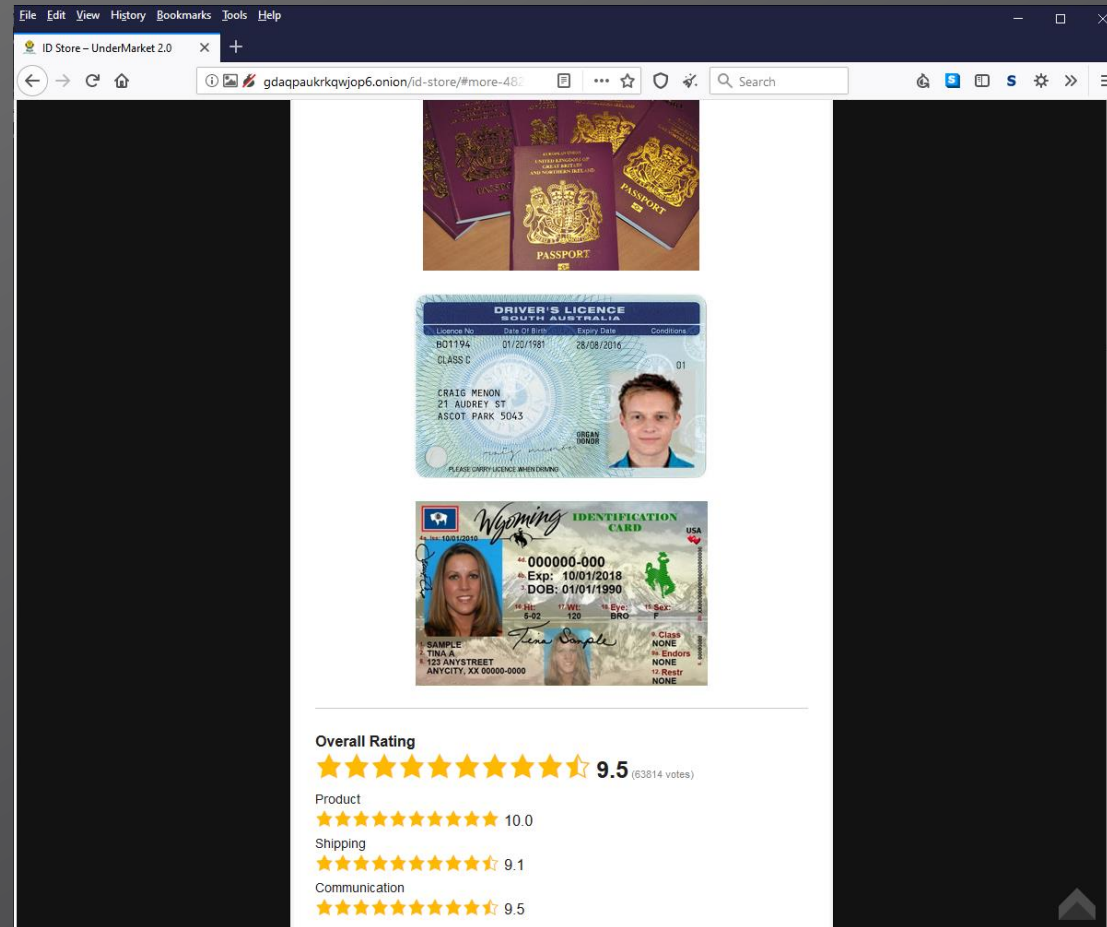
Vendor	Services	Member since	Sales	Status	Rating
PP Guru	PayPal accounts	Dec 2016	79539	Online	9
Click'n'Cash	PayPal, Gift card and Credit cards cash out services	Feb 2018	74611	Offline	8.9
eBay Store	eBay virtual gift cards	Dec 2016	31601	Offline	7.8
Amazon Gift Cards	Digital Amazon gift cards	Dec 2016	85625	Offline	8.2

The screenshot displays a 'Customer reviews' section on a dark web marketplace. It lists three buyers with their profile pictures, names, and overall ratings. Each review includes a star rating and a timestamp.

Buyer	Overall Rating	Time Ago
Mightfont	6.7	7 hours 28 minutes ago
Anarallador	7.3	1 day 5 hours ago
NotAuthenticPat	7.5	

PLAY THE GAME

- Policies and reputation on the Dark Web



THE PEOPLE BEHIND THE KEYBOARDS

Population on the platform



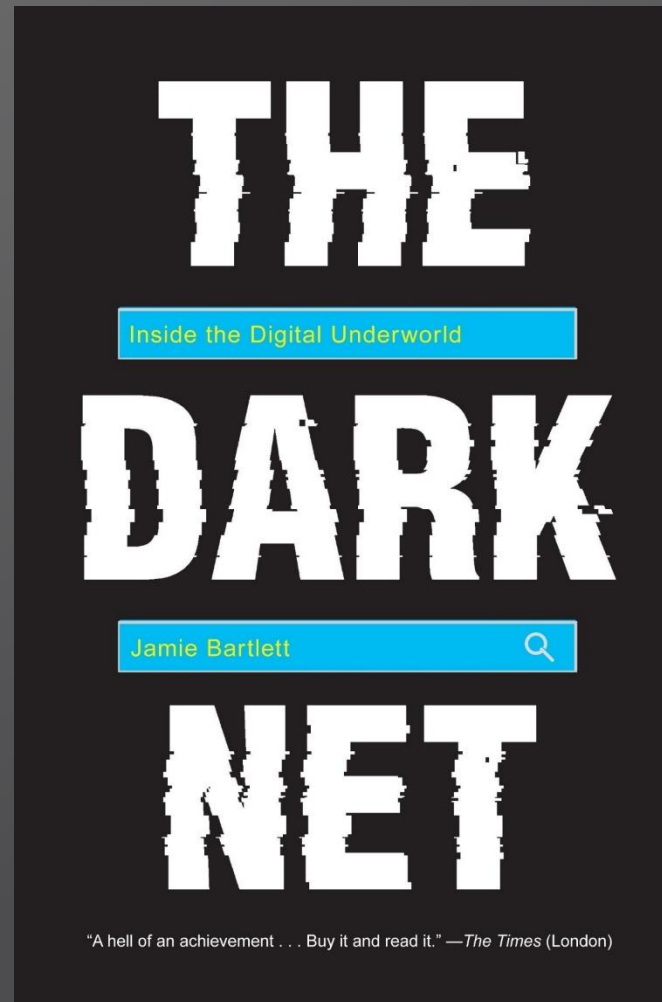
THE PEOPLE BEHIND THE KEYBOARDS

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 Blockchain 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



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.

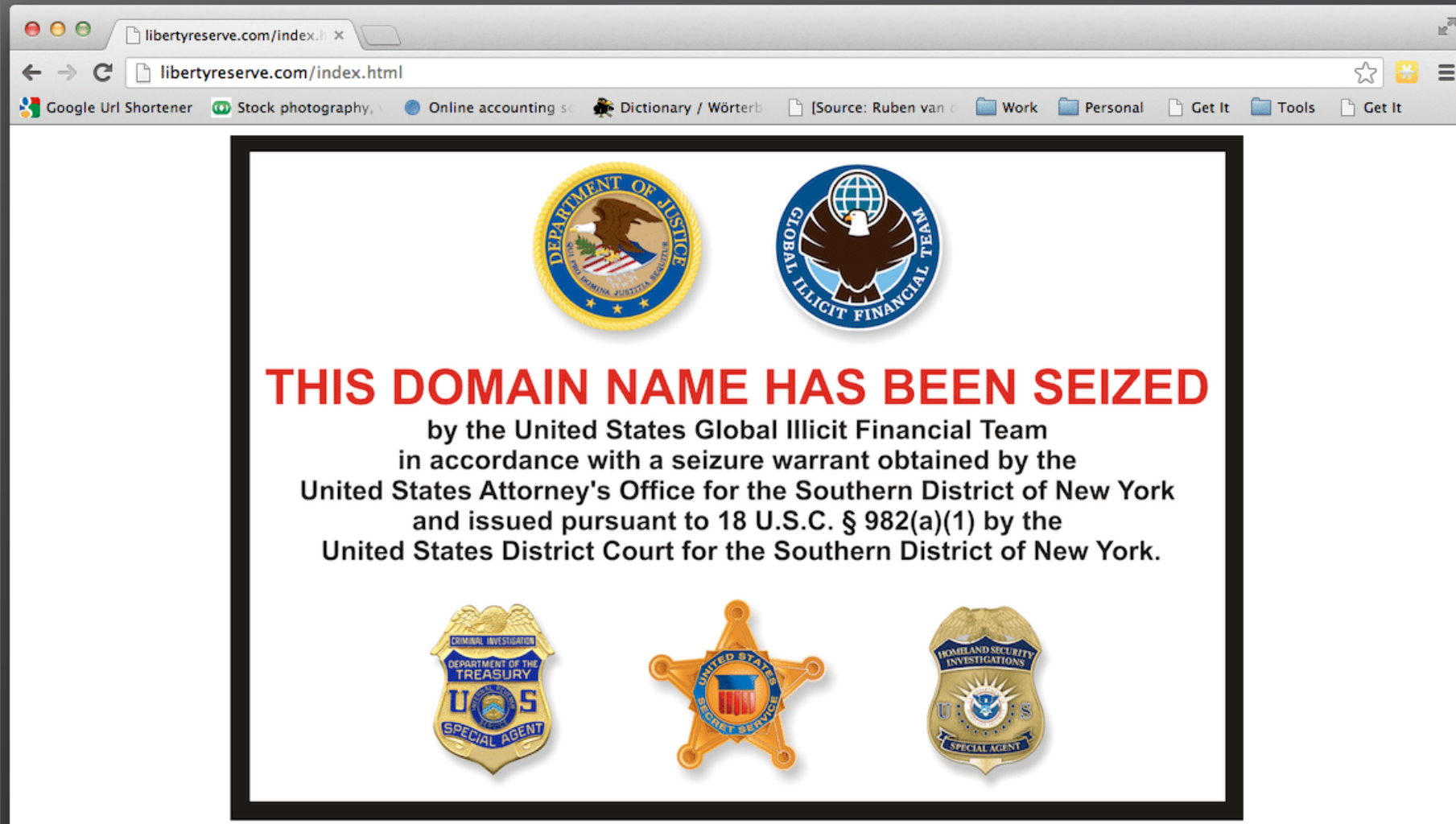
Organized crime groups are now using centralized **virtual currencies** like **WebMoney and Perfect Money** or decentralized cryptocurrencies like **bitcoin** to better cover their financial footprints.

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 shows the Blockchain.com interface for a Bitcoin transaction. A red rectangular box highlights the 'Summary' section, which contains the following information:

- Hash:** 49849b2abd4f4be4ea608a0475990fefdc899ca277646b5f9e2a... (with a copy icon)
- Date:** 2020-03-11 03:42
- From:** 16urQB6QCrghKe1dvzHf43ExnZto7pdFkw (0.00690720 BTC)
- To:** 39VS8tVMpZCDcwXmqSbEefo2azCu19njxk (0.00690292 BTC)
- Fee:** 0.00000428 BTC (2.265 sat/B - 0.566 sat/WU - 189 bytes)
- Status:** UNCONFIRMED

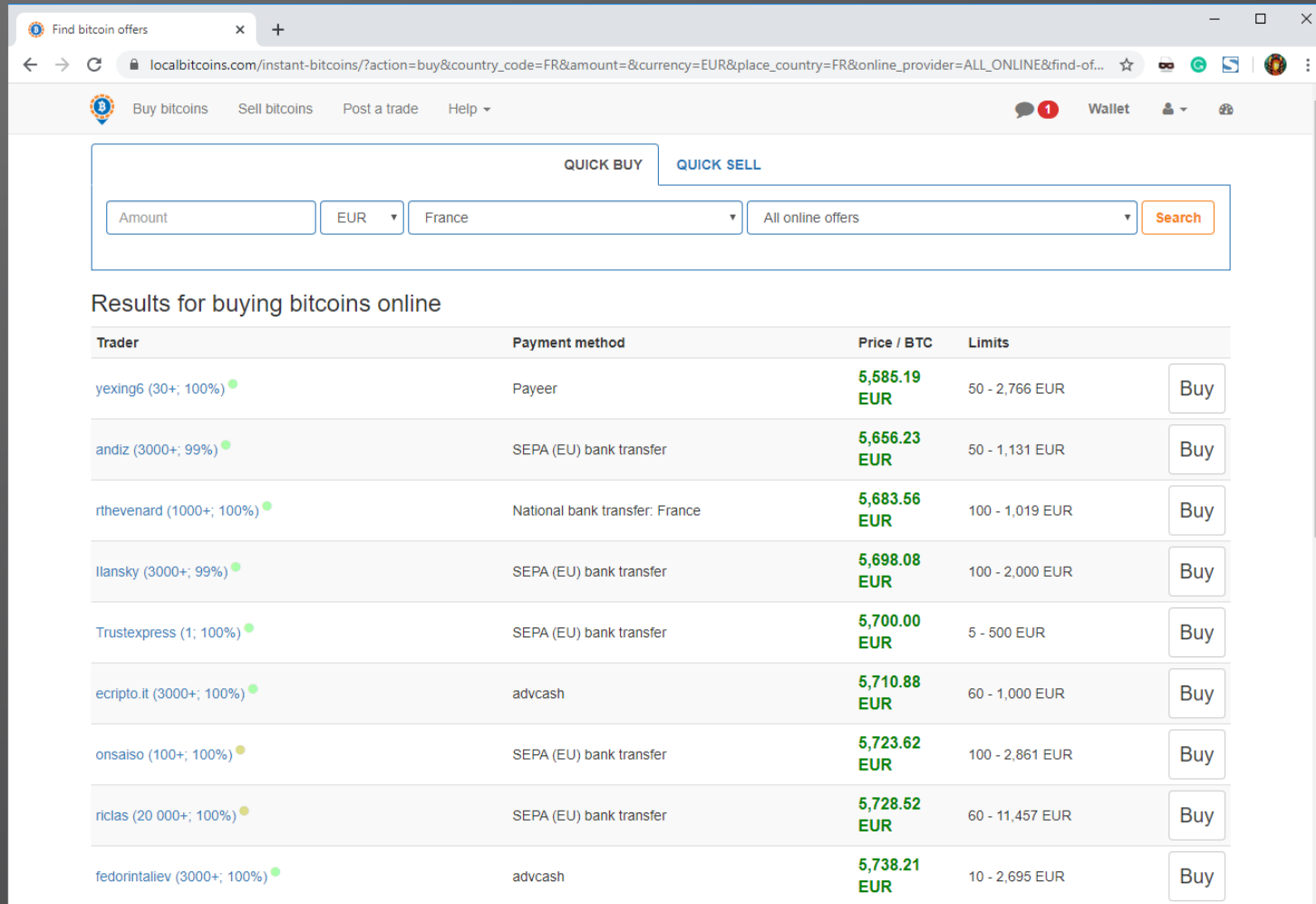
Below the summary, the 'Details' section provides further information:

Field	Value
Hash	49849b2abd4f4be4ea608a0475990fefdc899ca277646b5f9e2aaf6a4dc7a0ef
Status	Unconfirmed
Received Time	2020-03-11 03:42
Size	189 bytes
Weight	756

At the bottom right of the interface, there is a 'Playba' button and a 'Start' button with a '0' value.

GOODS TRANSFER - THE RISE OF CRYPTO'S

The preferred methodology



The screenshot shows the 'Find bitcoin offers' page on localbitcoins.com. The search parameters are set to 'EUR' and 'France'. The results are displayed as a table of offers from various traders, each with a 'Buy' button.

QUICK BUY **QUICK SELL**

Amount: EUR: France: All online offers:

Results for buying bitcoins online

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

GOODS TRANSFER - THE RISE OF CRYPTO'S

The preferred methodology

Enter BestMixer code: ?

optional

Enter your address: ⓘ

33.63%
2hr. 21min.

33.12%
4hr. 41min. X

33.25%
6hr. 10min. X

+ Add address

Service fee: ⓘ 1.0000%

Reserves for mixing: ⓘ Alpha Pool

Percentage distribution: ⓘ






Transfer delay: ⓘ

Mixing strength meter: ?

Strong

GOODS TRANSFER - THE RISE OF CRYPTO'S

The preferred methodology – Monero Evolution

COMPARISON OF ANONYMOUS CRYPTOS					
	PRIVATE		FUNGIBLE		DECENTRALIZED
 MONERO	✓	}	✓	}	✓
 bitcoin	✗		✗		✓
 CASH	?		?		✗
 DASH	✗		✗		✗
 VERGE	✗		✗		✓

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”

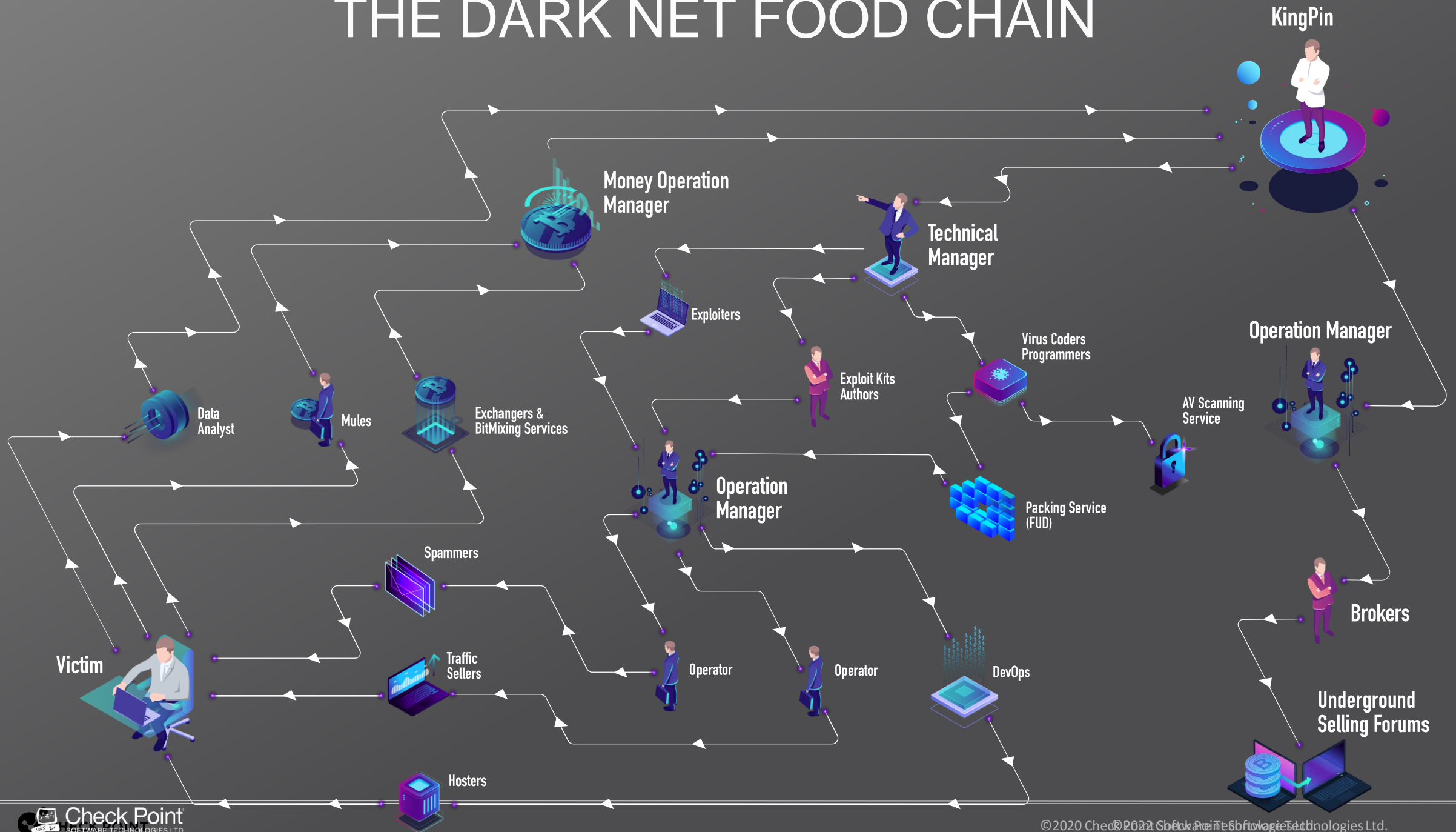


Alexey Dmitrievich Bron
Alias: “thehead”



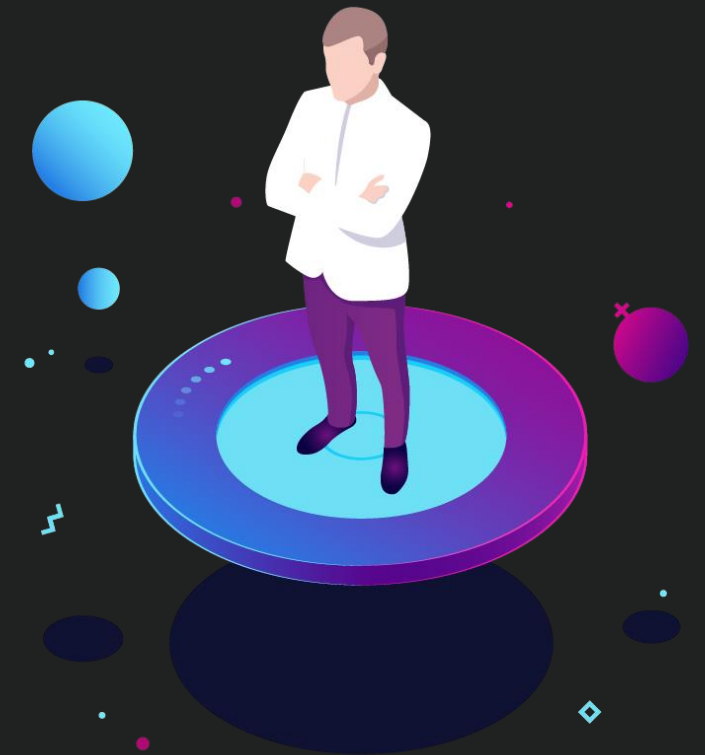
Vyacheslav Igorevich Penchukov
Aliases: “tank”, “father”

THE DARK NET FOOD CHAIN

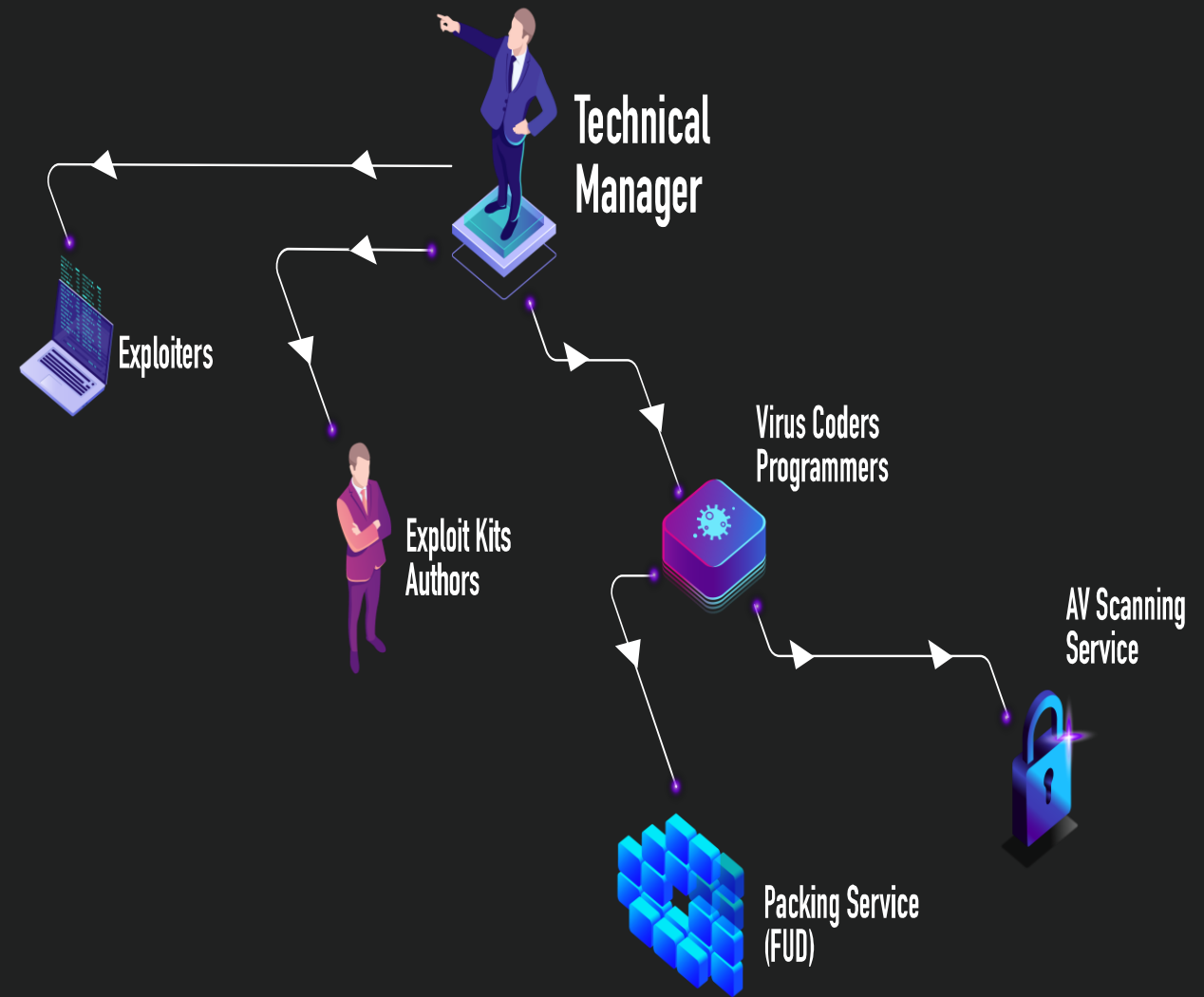


- The leader!
- Powerful criminal
- Well connected upside down in the crime scene
- And don't mess with him

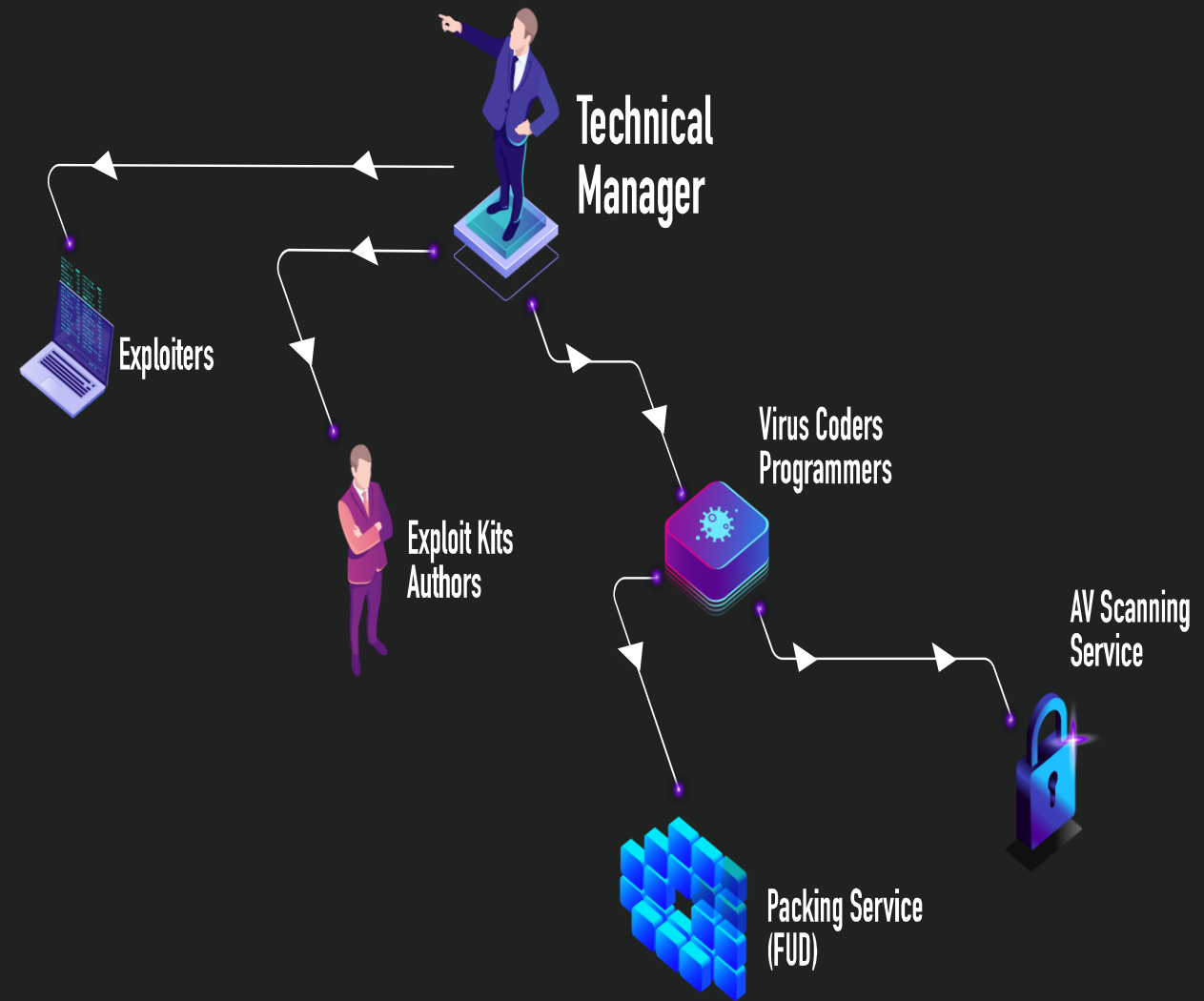
KingPin



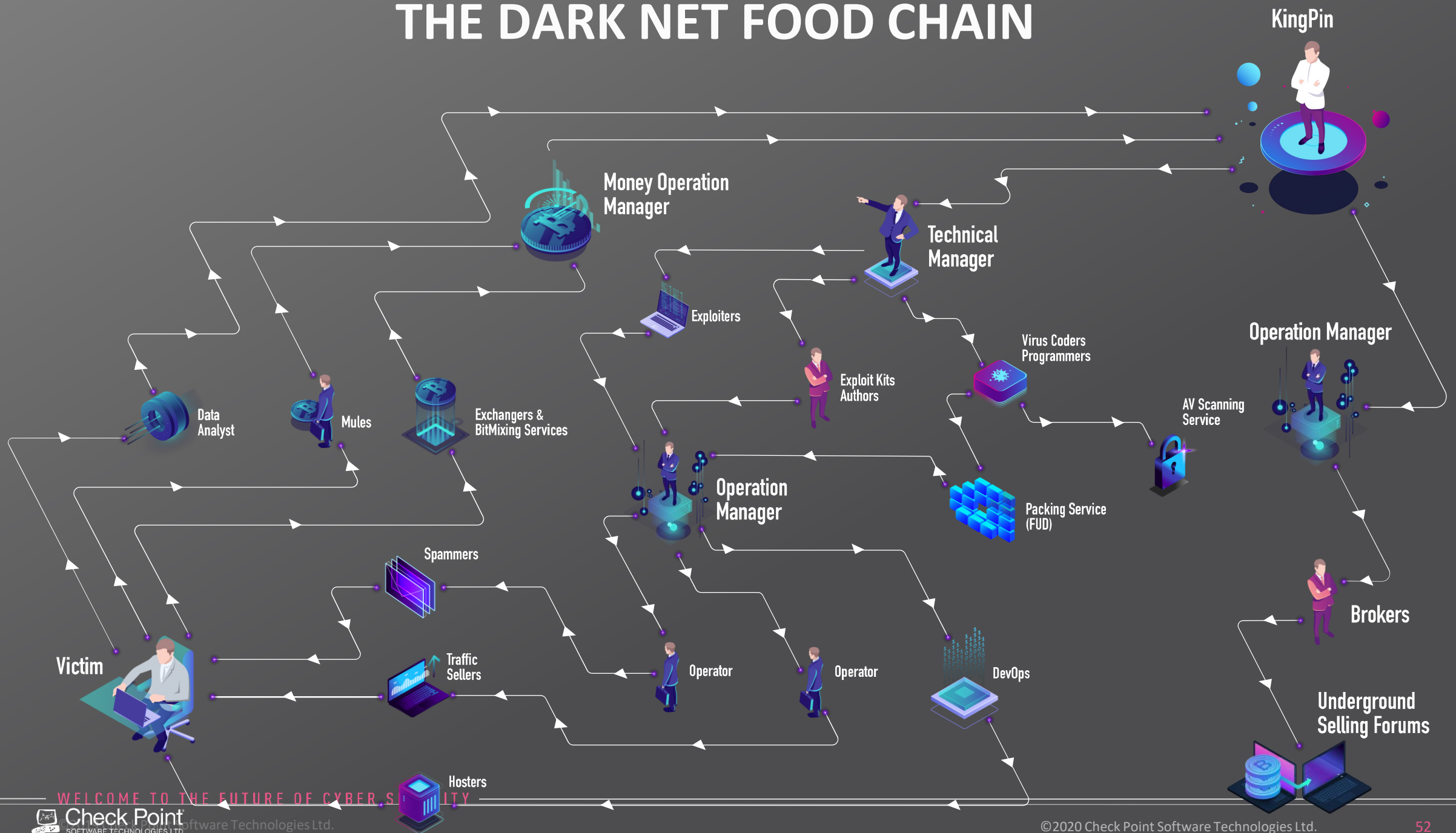
- Malware authors
- Exploit kit developers
- Phishing kit developers
- Hacking tools developers



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



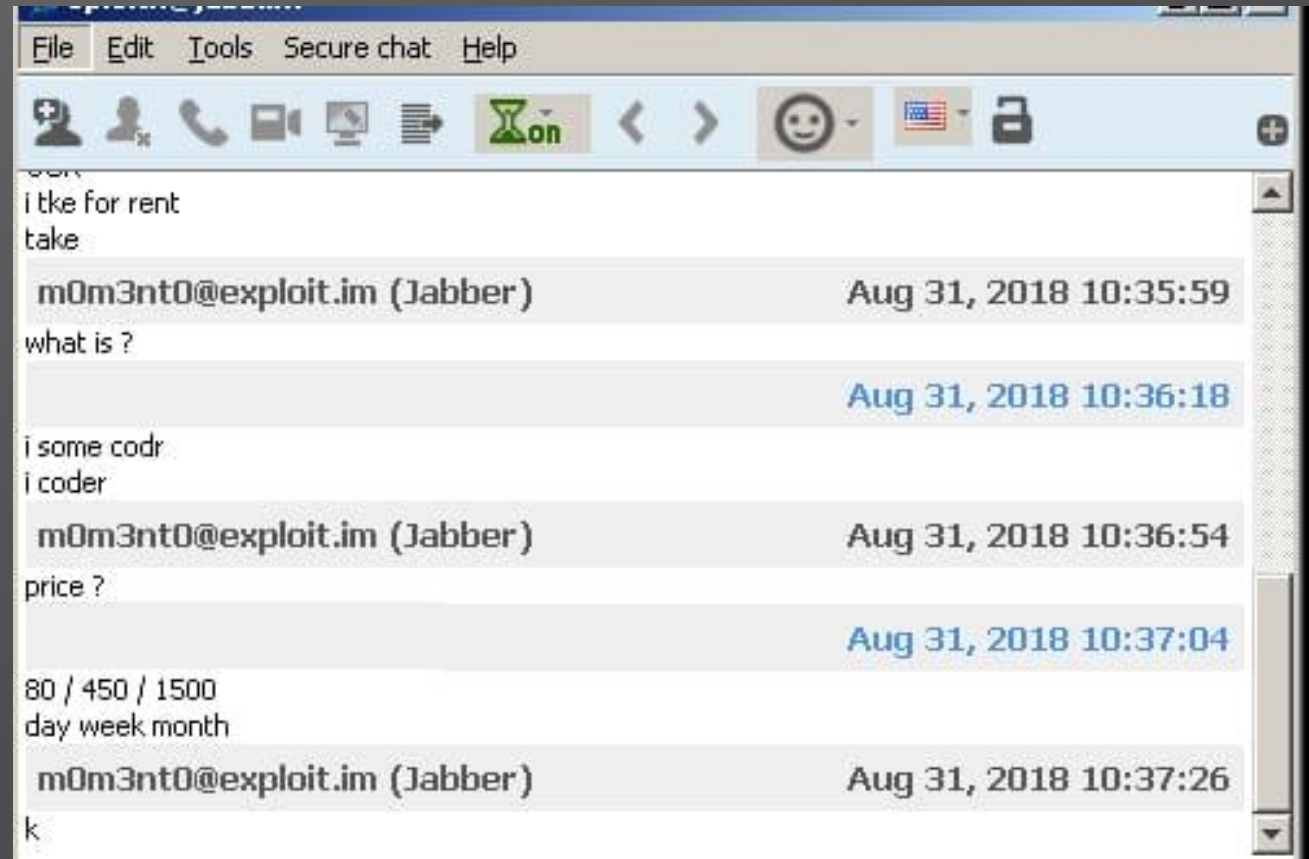
THE DARK NET FOOD CHAIN



WELCOME TO THE FUTURE OF CYBER SECURITY

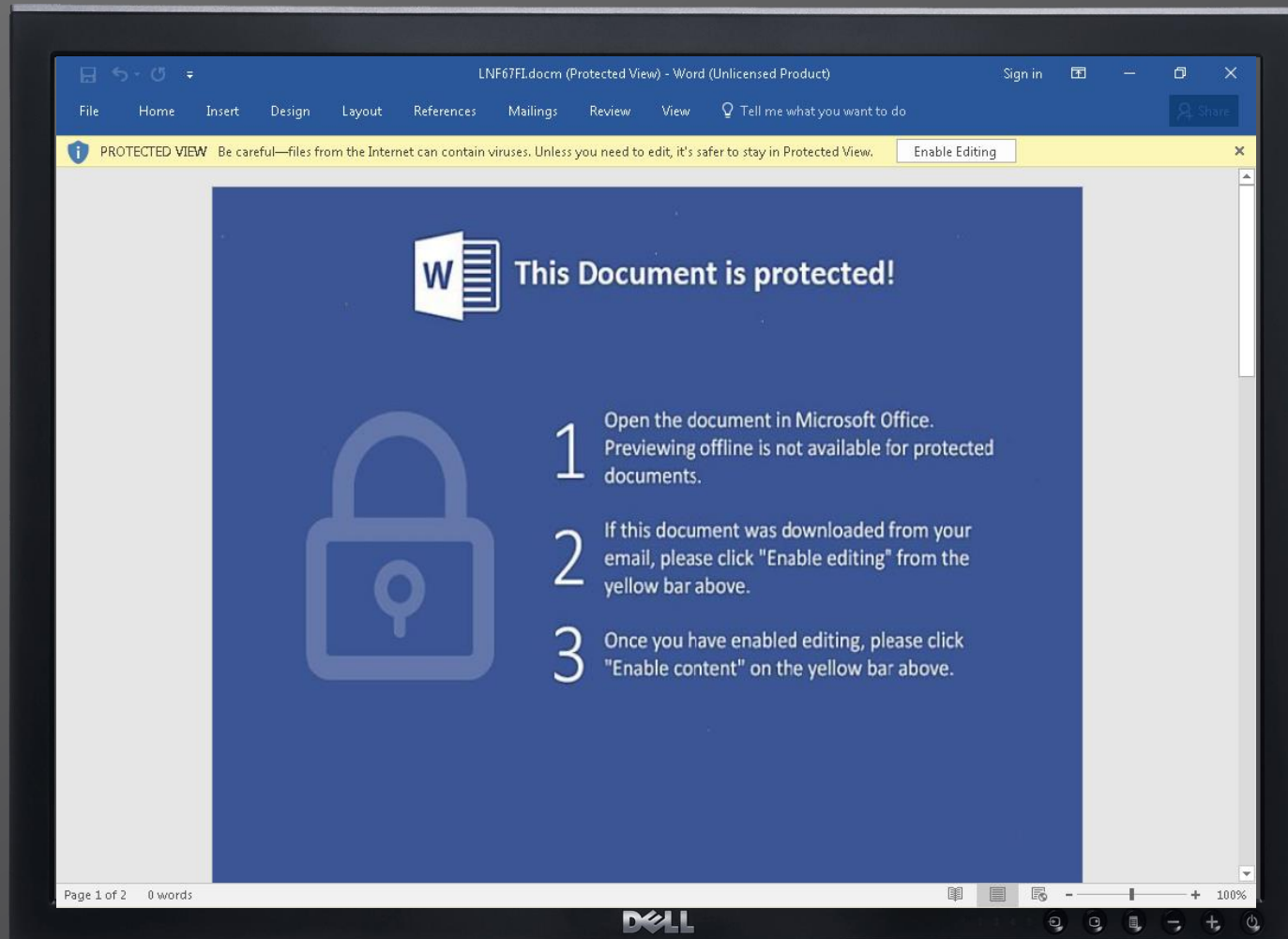
KNOWN ATTRIBUTED EXAMPLES

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: g46mbrrzpfsonuk.onion/9HQH9AYFTGQ0YZH6
4. Follow the instructions on the site.

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

\$__--~\$.

|-_|=|

DELL



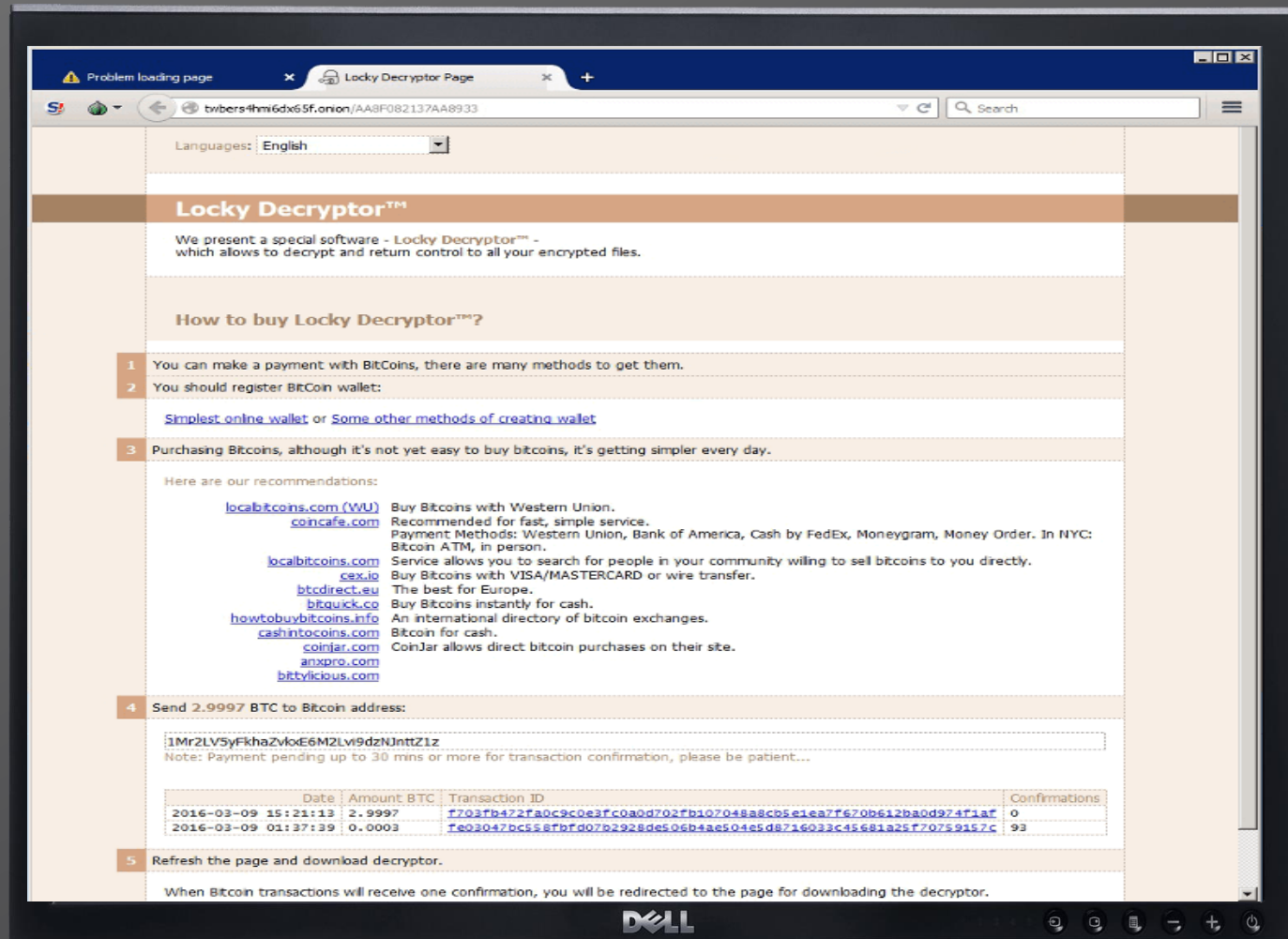
KNOWN ATTRIBUTED EXAMPLES

Collaboration and Execution



KNOWN ATTRIBUTED EXAMPLES

Collaboration and Execution





“It’s a wonder you made your way out”

HOW TO STAY SAFE?

Tip for a secured journey on the Dark Net





THANK YOU

YOU DESERVE THE BEST SECURITY