INTSIGHTS

Defend Forward™

CISO’s Guide To Shutting Down Attacks Using The Dark Web

October 25, 2019

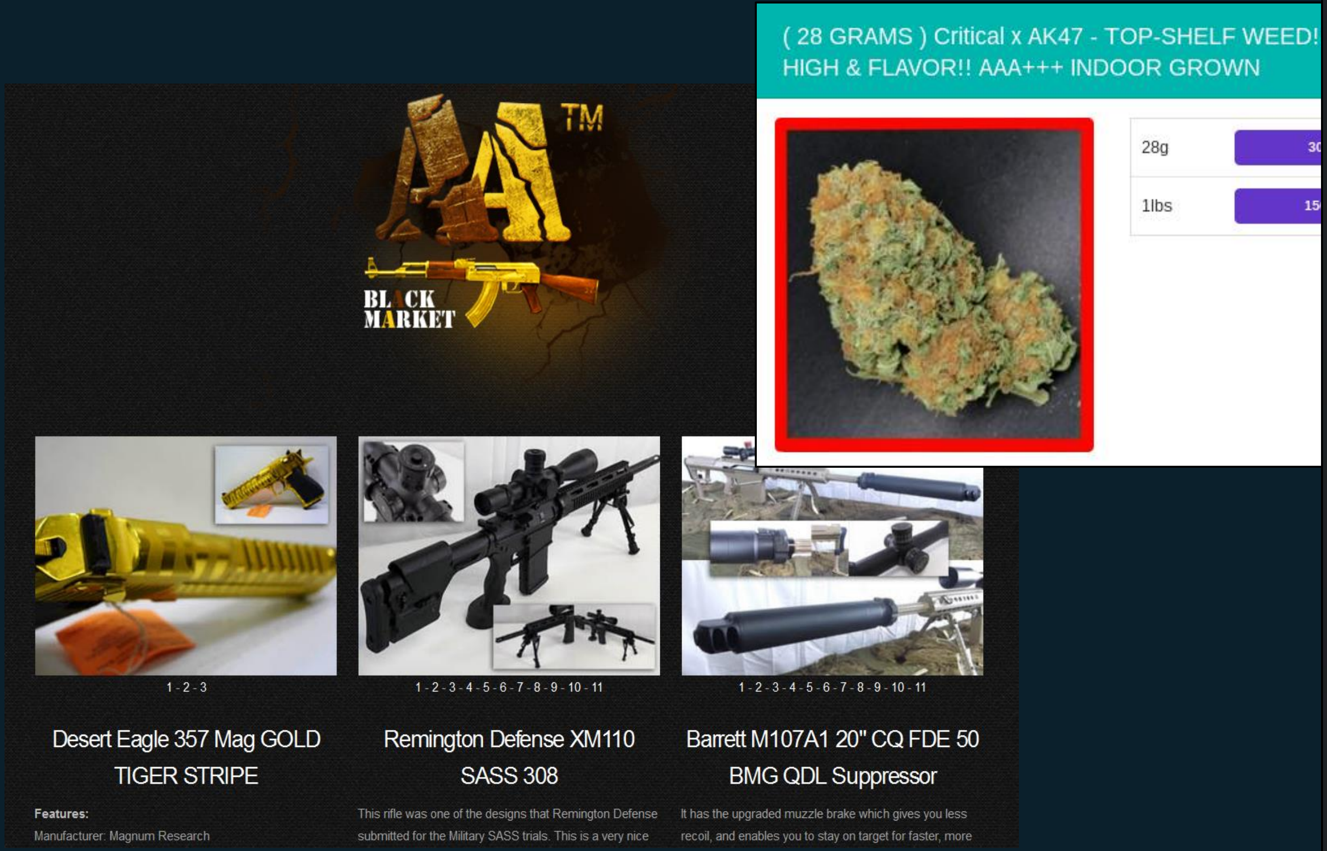
Agenda

- The Dark Web: What’s At Stake
- Gain Visibility, Take Control
- Live Dark Web Tour
- Key Recommendations

Agenda

- **The Dark Web: What's At Stake**
- Gain Visibility, Take Control
- Live Dark Web Tour
- Key Recommendations

What Do We Know About The Dark Web?



(28 GRAMS) Critical x AK47 - TOP-SHELF WEED! HIGH & FLAVOR!! AAA+++ INDOOR GROWN

28g	30
1lbs	15

1 - 2 - 3

Desert Eagle 357 Mag GOLD TIGER STRIPE

Features:

Manufacturer: Magnum Research

1 - 2 - 3 - 4 - 5 - 6 - 7 - 8 - 9 - 10 - 11

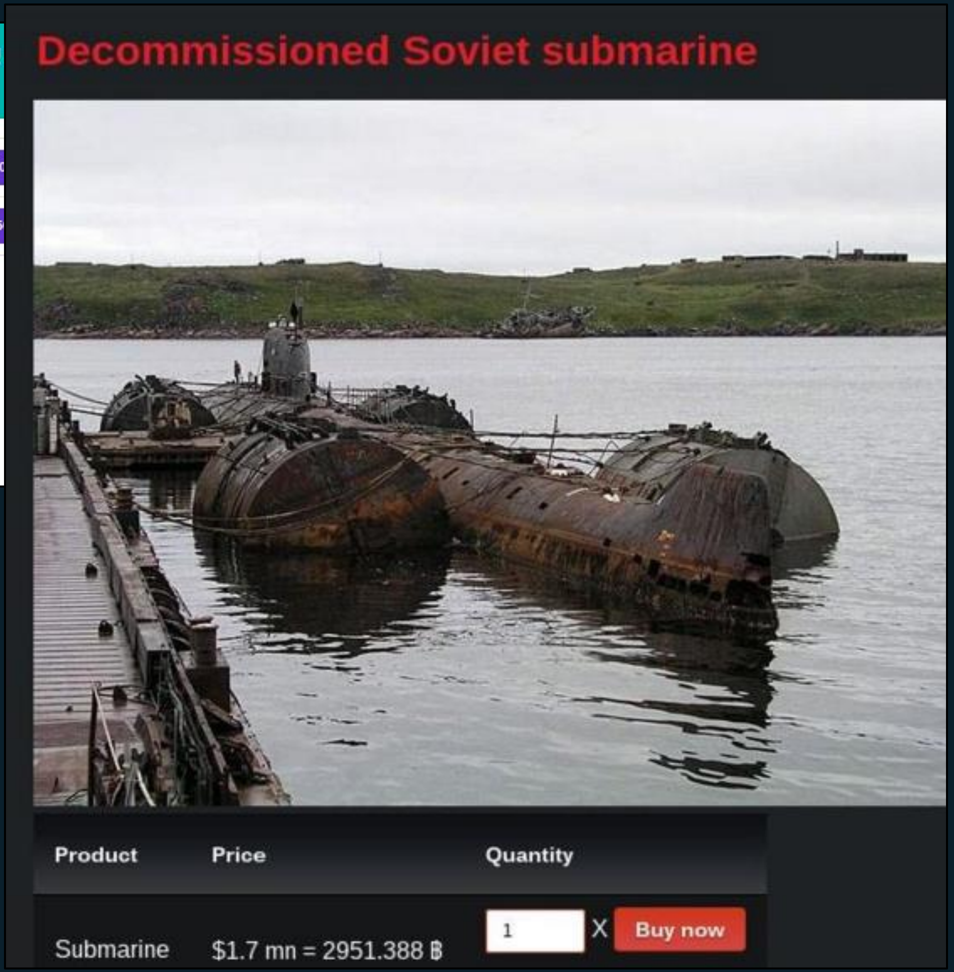
Remington Defense XM110 SASS 308

This rifle was one of the designs that Remington Defense submitted for the Military SASS trials. This is a very nice

1 - 2 - 3 - 4 - 5 - 6 - 7 - 8 - 9 - 10 - 11

Barrett M107A1 20" CQ FDE 50 BMG QDL Suppressor

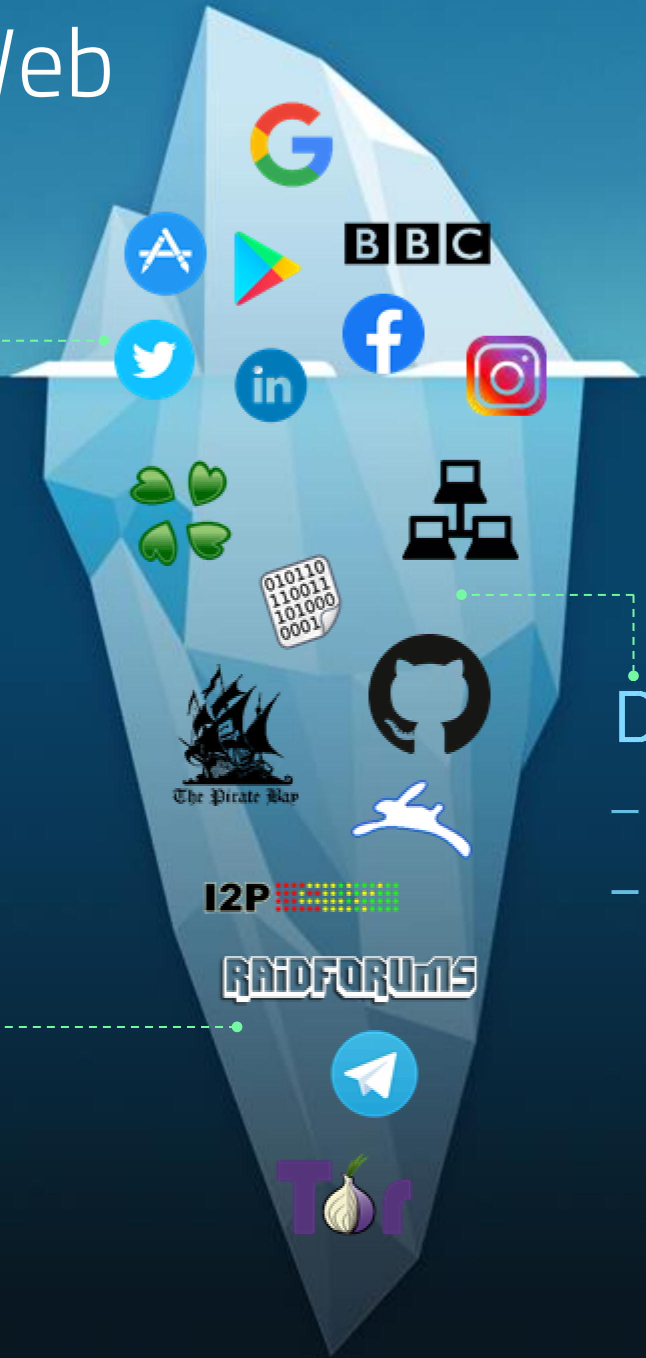
It has the upgraded muzzle brake which gives you less recoil, and enables you to stay on target for faster, more



Decommissioned Soviet submarine

Product	Price	Quantity
Submarine	$1.7 mn = 2951.388 ฿	1 X Buy now

The Clear, Deep, and Dark Web



Clear Web

- Search engines
- Media, blogs, etc.

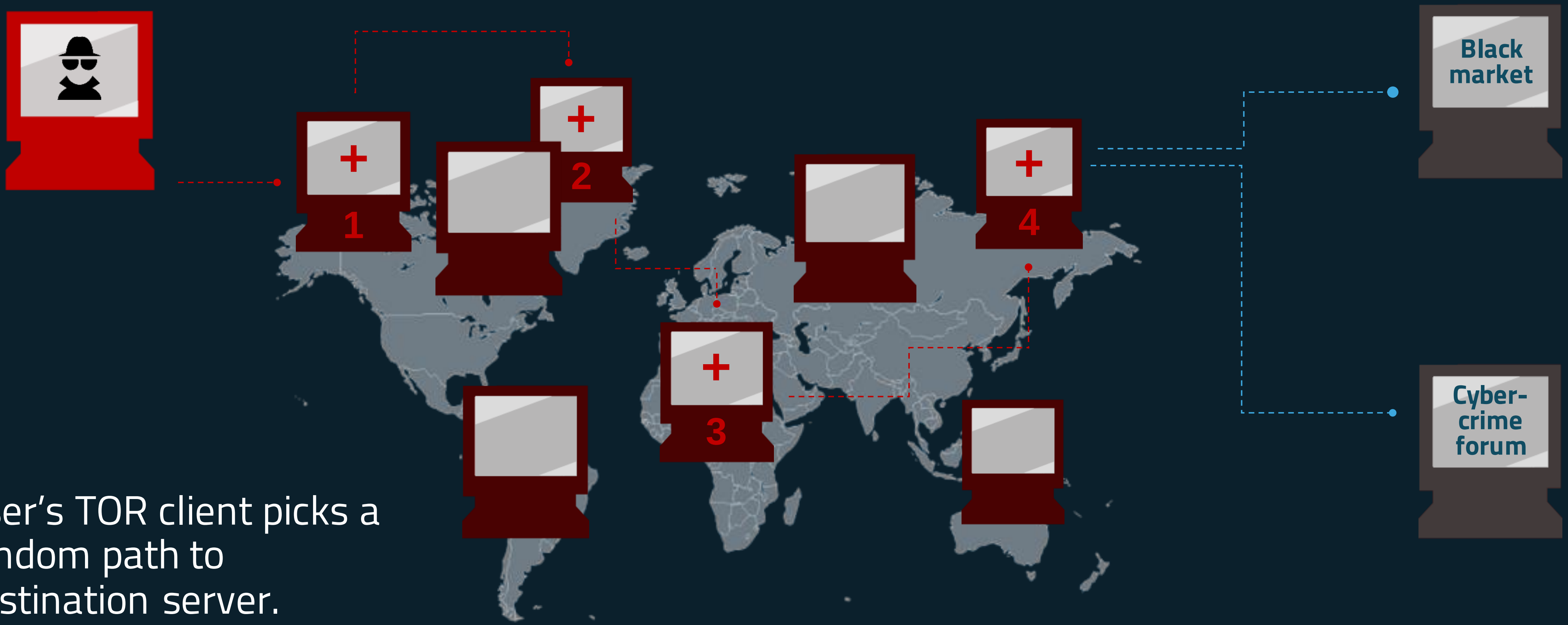
Deep Web

- Unindexed by search engines
- Webmail, online banking, corporate intranets, walled gardens, etc.

Dark Web

- Anonymous, closed sources, Telegram groups, invite-only (sometimes)
- Tor, P2P, hacker forums, criminal marketplaces, C2s, etc.

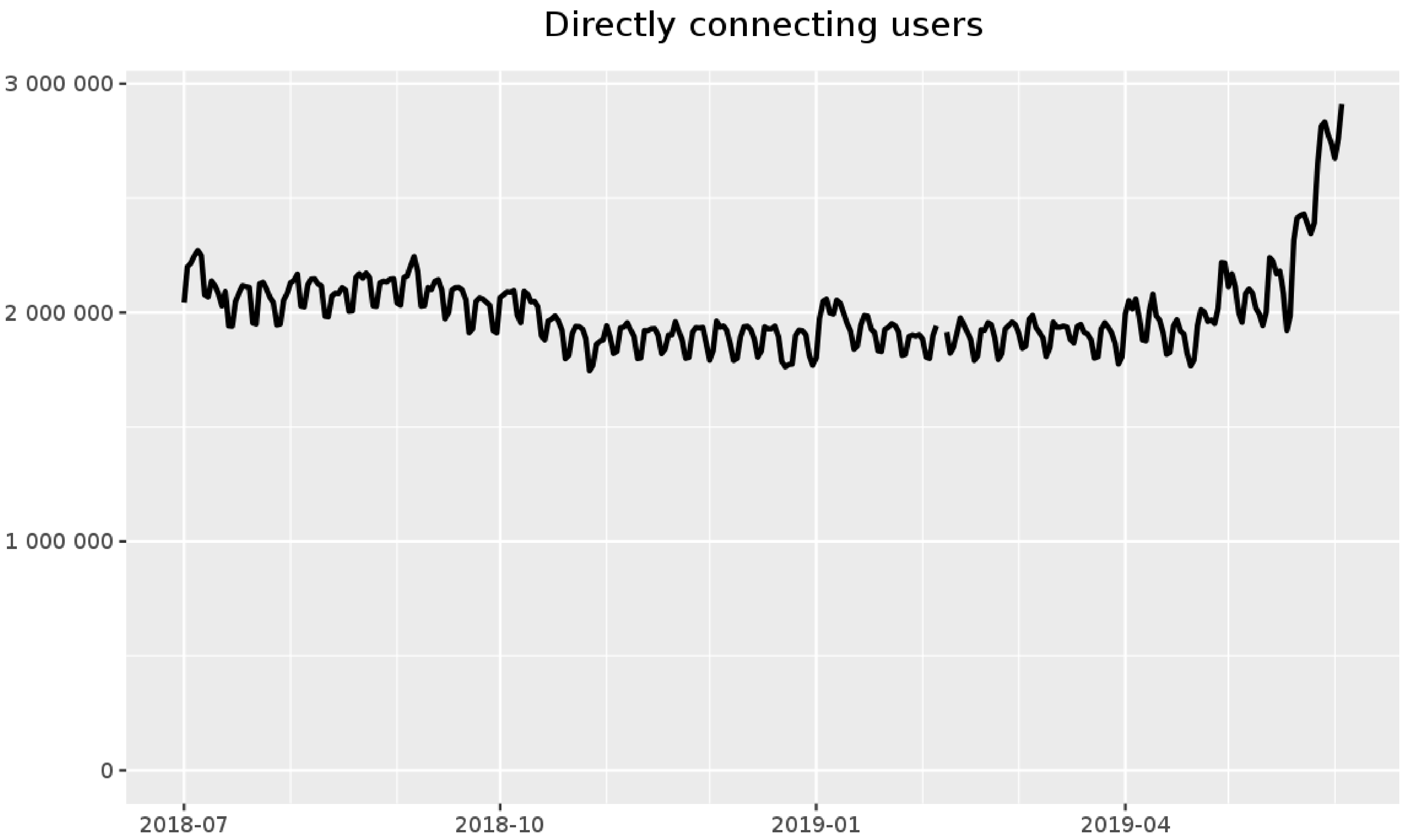
How Tor Works



User’s TOR client picks a random path to destination server.

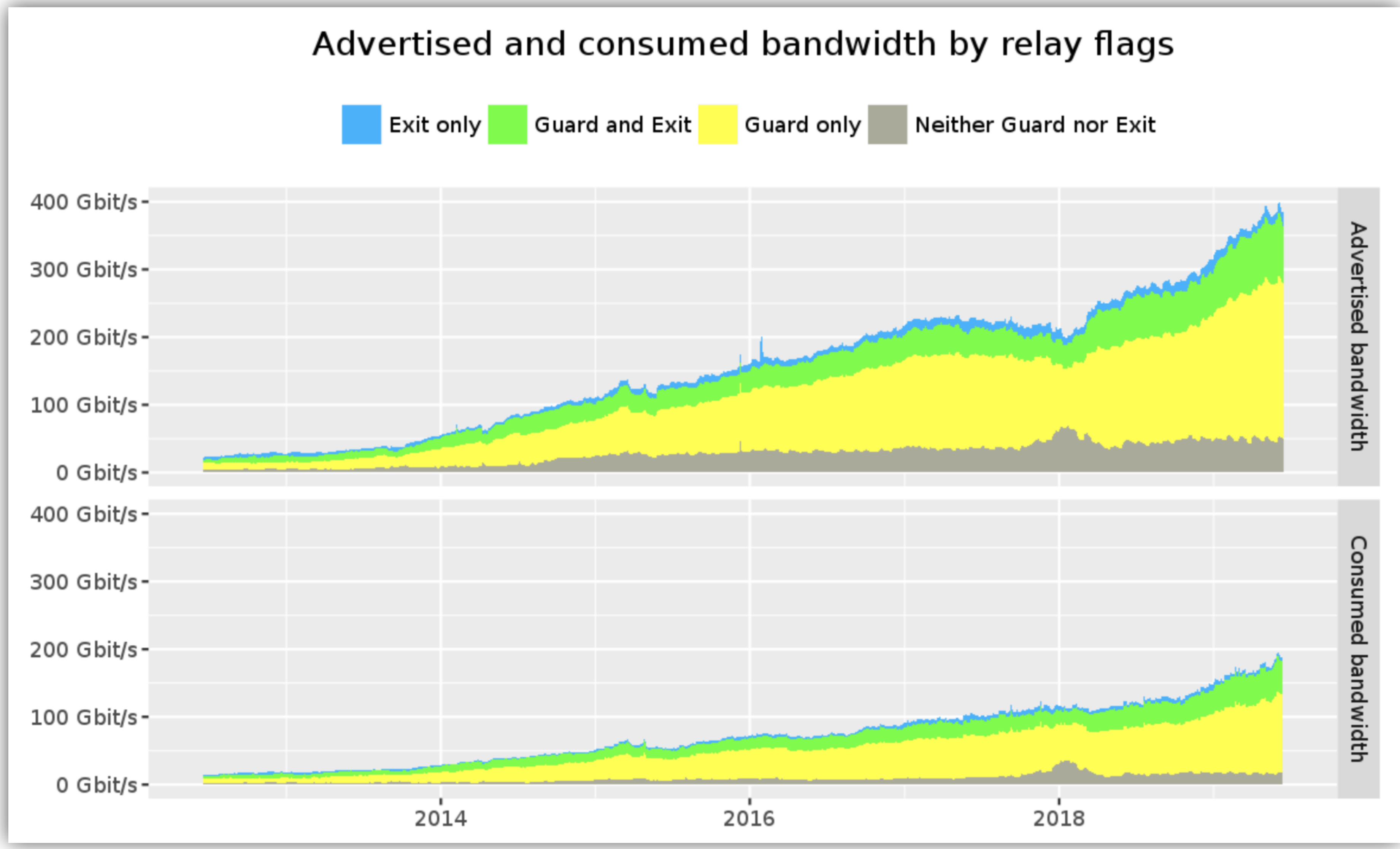
RED links are encrypted
BLUE links are in the clear.

Tor Usage Statistics



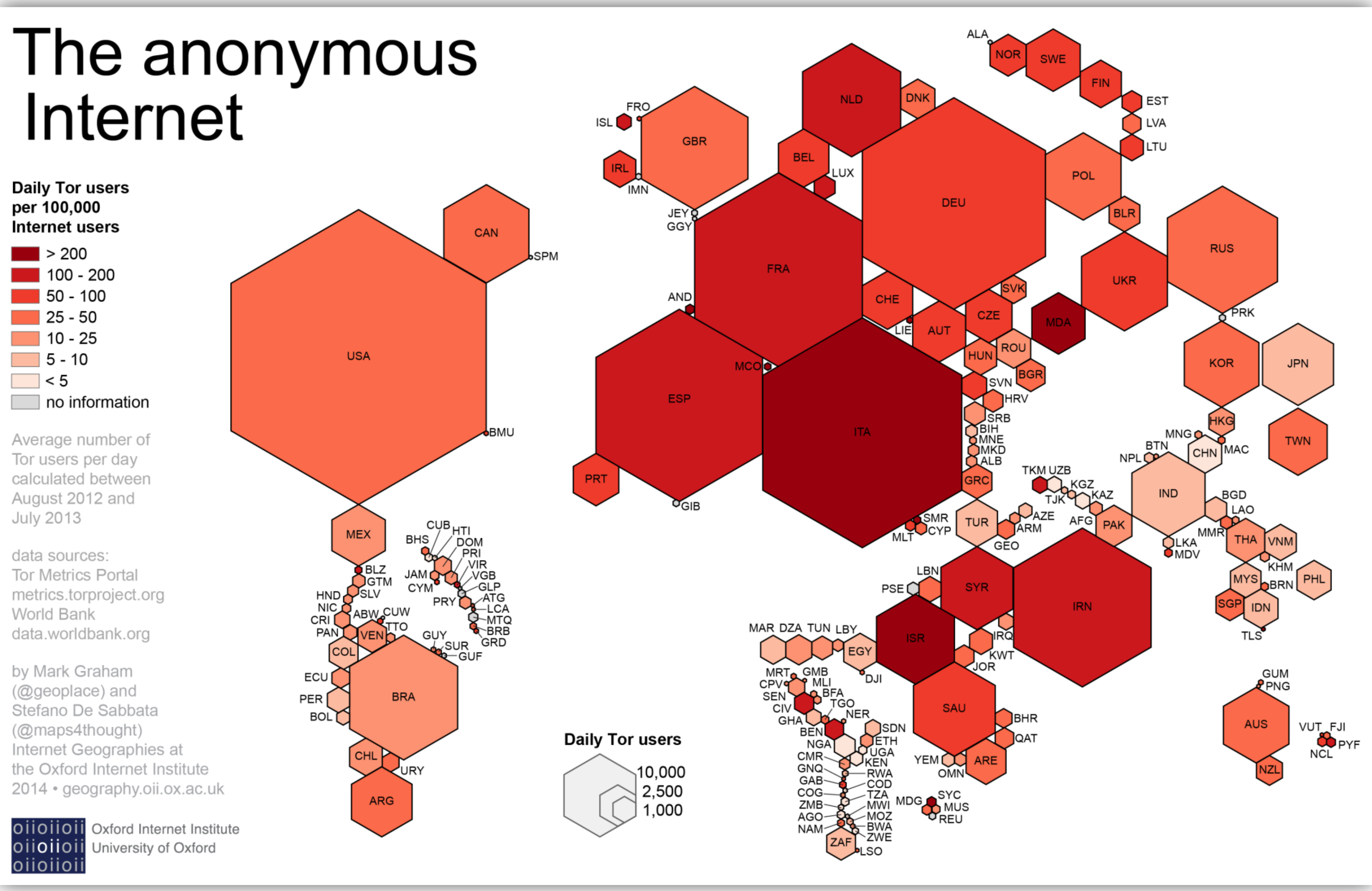
The Tor Project - https://metrics.torproject.org/

Tor Usage Statistics



Source: The Tor project – https://metrics.torproject.org/

Tor Usage Statistics



The anonymous Internet

Daily Tor users per 100,000 Internet users

- 🟥 > 200
- 🟥 100 - 200
- 🟥 50 - 100
- 🟥 25 - 50
- 🟥 10 - 25
- 🟥 5 - 10
- 🟥 < 5
- ⬜ no information

Average number of Tor users per day calculated between August 2012 and July 2013

data sources:
Tor Metrics Portal
metrics.torproject.org
World Bank
data.worldbank.org

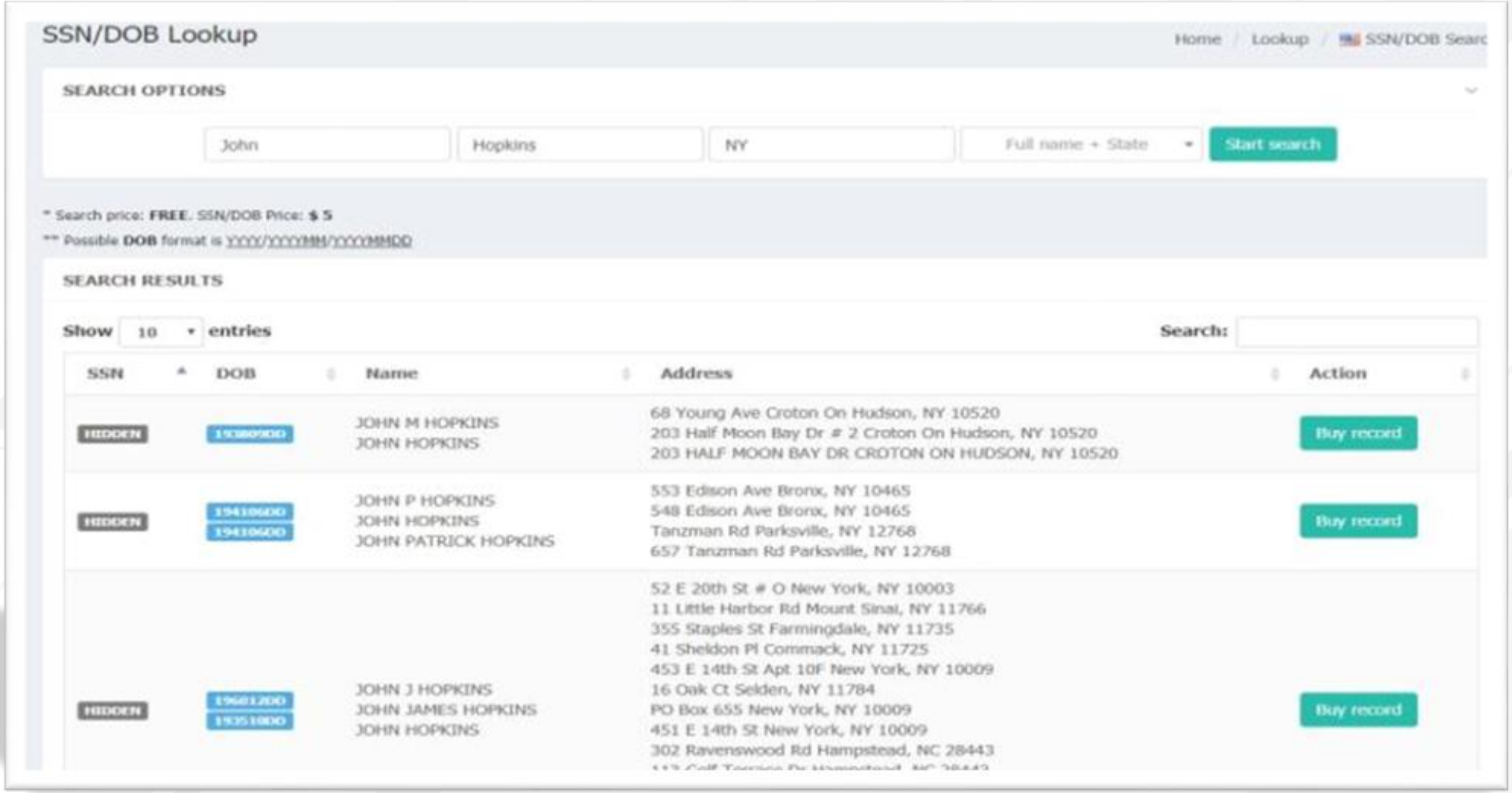
by Mark Graham (@geoplace) and Stefano De Sabbata (@maps4thought)
Internet Geographies at the Oxford Internet Institute
2014 • geography.oii.ox.ac.uk

Oxford Internet Institute
University of Oxford

Daily Tor users

10,000
2,500
1,000

The User Experience Can Match Legitimate Sites



SSN/DOB Lookup

Home / Lookup / SSN/DOB Searc

SEARCH OPTIONS

John | Hopkins | NY | Full name + State ▾ | Start search

* Search price: **FREE**. SSN/DOB Price: **$ 5**

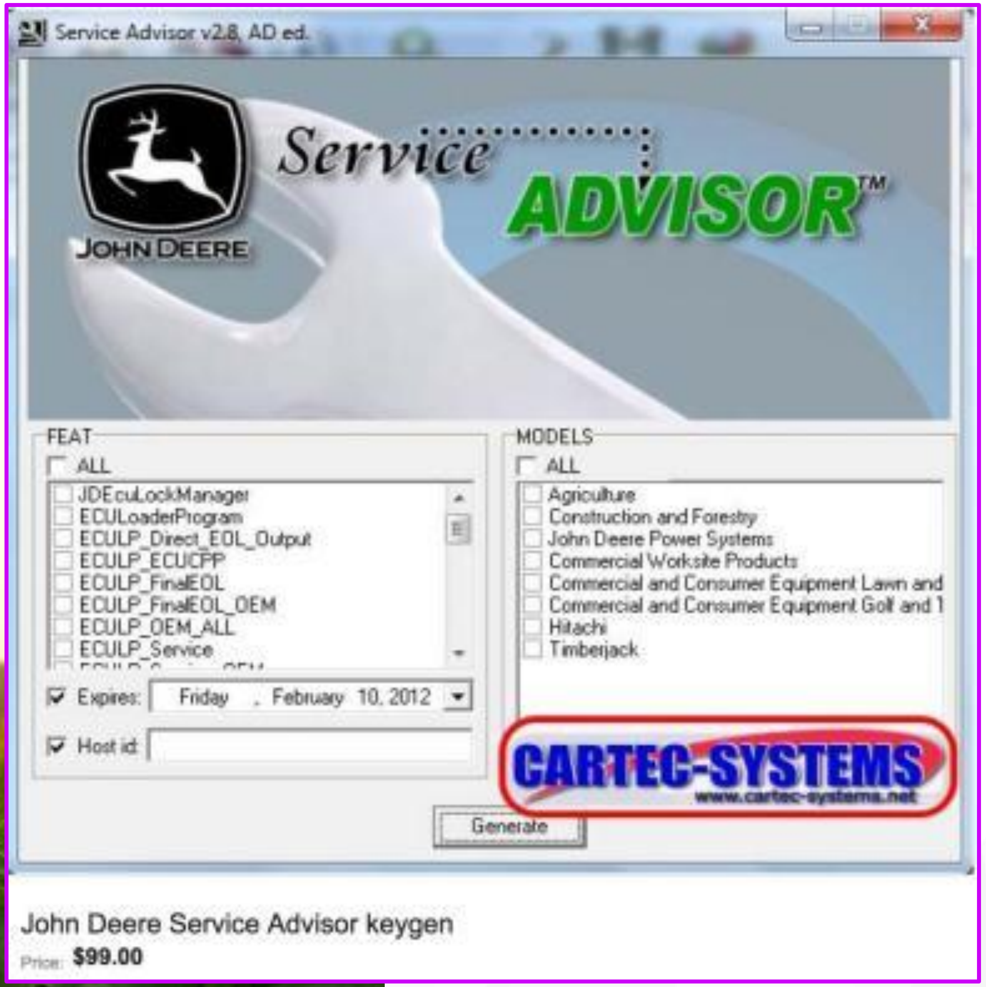
** Possible **DOB** format is YYYY/YYYYMM/YYYYMMDD

SEARCH RESULTS

Show 10 ▾ **entries** **Search:**

SSN	DOB	Name	Address	Action
HIDDEN	193809DD	JOHN M HOPKINS JOHN HOPKINS	68 Young Ave Croton On Hudson, NY 10520 203 Half Moon Bay Dr # 2 Croton On Hudson, NY 10520 203 HALF MOON BAY DR CROTON ON HUDSON, NY 10520	Buy record
HIDDEN	194106DD 194106DD	JOHN P HOPKINS JOHN HOPKINS JOHN PATRICK HOPKINS	553 Edison Ave Bronx, NY 10465 548 Edison Ave Bronx, NY 10465 Tanzman Rd Parksville, NY 12768 657 Tanzman Rd Parksville, NY 12768	Buy record
HIDDEN	196012DD 193510DD	JOHN J HOPKINS JOHN JAMES HOPKINS JOHN HOPKINS	52 E 20th St # O New York, NY 10003 11 Little Harbor Rd Mount Sinai, NY 11766 355 Staples St Farmingdale, NY 11735 41 Sheldon Pl Commack, NY 11725 453 E 14th St Apt 10F New York, NY 10009 16 Oak Ct Selden, NY 11784 PO Box 655 New York, NY 10009 451 E 14th St New York, NY 10009 302 Ravenswood Rd Hampstead, NC 28443 113 Golf Terrace Dr Hampstead, NC 28443	Buy record

Even Farmers Turn To The Dark Web



FEAT

□ ALL

- □ JDEcuLockManager
- □ ECULoaderProgram
- □ ECULP_Direct_EOL_Output
- □ ECULP_ECUCPP
- □ ECULP_FinalEOL
- □ ECULP_FinalEOL_OEM
- □ ECULP_OEM_ALL
- □ ECULP_Service

MODELS

□ ALL

- □ Agriculture
- □ Construction and Forestry
- □ John Deere Power Systems
- □ Commercial Worksite Products
- □ Commercial and Consumer Equipment Lawn and
- □ Commercial and Consumer Equipment Golf and 1
- □ Hitachi
- □ Timberjack

☑ Expires: Friday , February 10, 2012

☑ Host id:

John Deere Service Advisor keygen

Price: **$99.00**

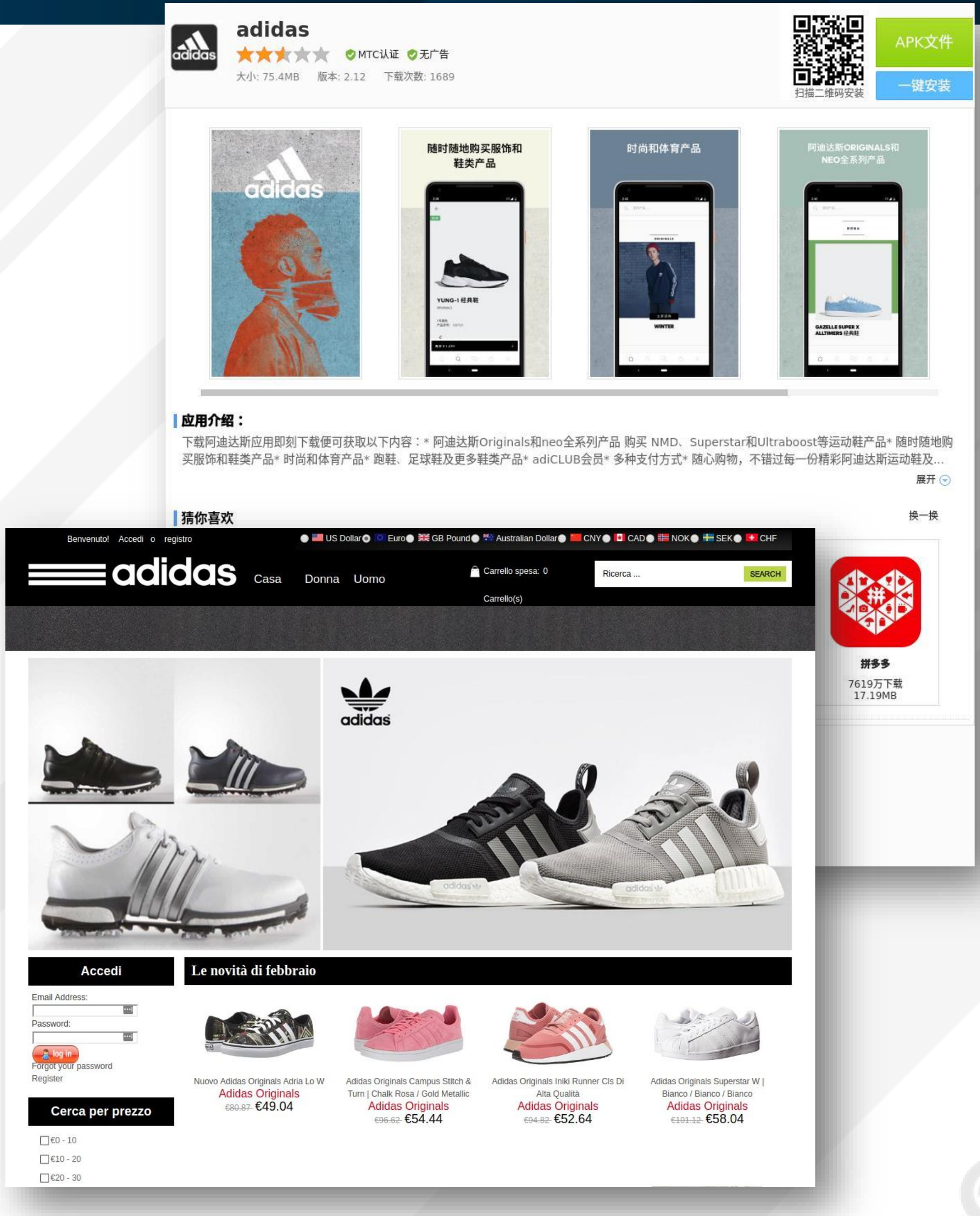
Threats are mounting

278% Products for sale on black markets

297% Phishing websites

171% Compromised employee credentials

149% Stolen credit cards for sale on dark web



adidas

MTC认证 无广告

大小: 75.4MB 版本: 2.12 下载次数: 1689

扫描二维码安装

应用介绍：

下载阿迪达斯应用即刻下载便可获取以下内容：* 阿迪达斯Originals和neo全系列产品 购买 NMD、Superstar和Ultraboost等运动鞋产品* 随时随地购买服饰和鞋类产品* 时尚和体育产品* 跑鞋、足球鞋及更多鞋类产品* adiCLUB会员* 多种支付方式* 随心购物，不错过每一份精彩阿迪达斯运动鞋及...

展开

猜你喜欢 换一换

拼多多

7619万下载

17.19MB

Benvenuto! Accedi o registro

○ US Dollar ● Euro ○ GB Pound ○ Australian Dollar ○ CNY ○ CAD ○ NOK ○ SEK ○ CHF

Carrello spesa: 0

Carrello(s)

Ricerca ... SEARCH

Accedi

Email Address:

Password:

log in

Forgot your password

Register

Cerca per prezzo

□ €0 - 10

□ €10 - 20

□ €20 - 30

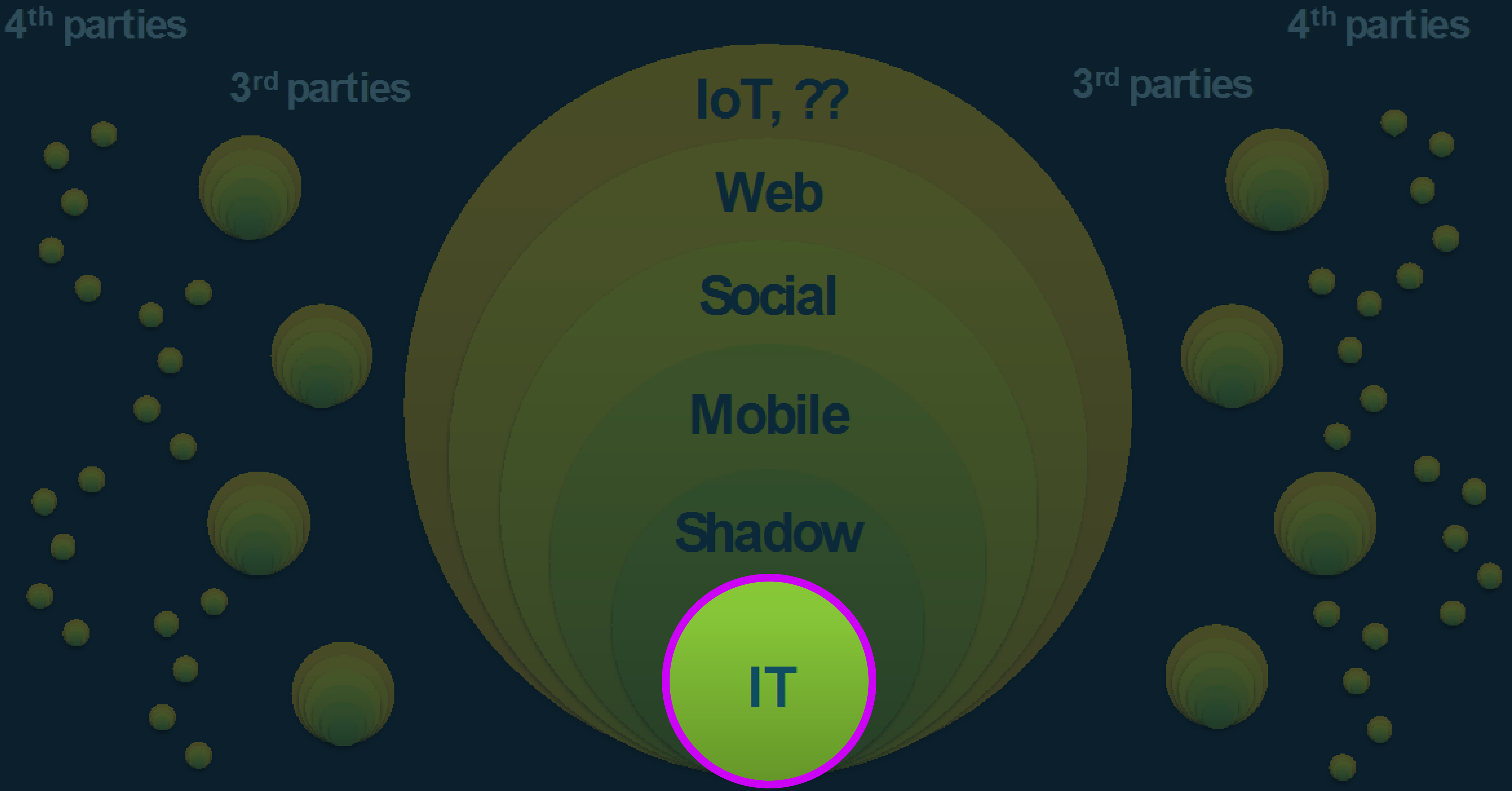
Le novità di febbraio

Nuovo Adidas Originals Adria Lo W	Adidas Originals Campus Stitch & Turn | Chalk Rosa / Gold Metallic	Adidas Originals Iniki Runner Cls Di Alta Qualità	Adidas Originals Superstar W | Bianco / Bianco / Bianco
Adidas Originals	Adidas Originals	Adidas Originals	Adidas Originals
~~€80.87~~ €49.04	~~€96.62~~ €54.44	~~€94.82~~ €52.64	~~€101.12~~ €58.04

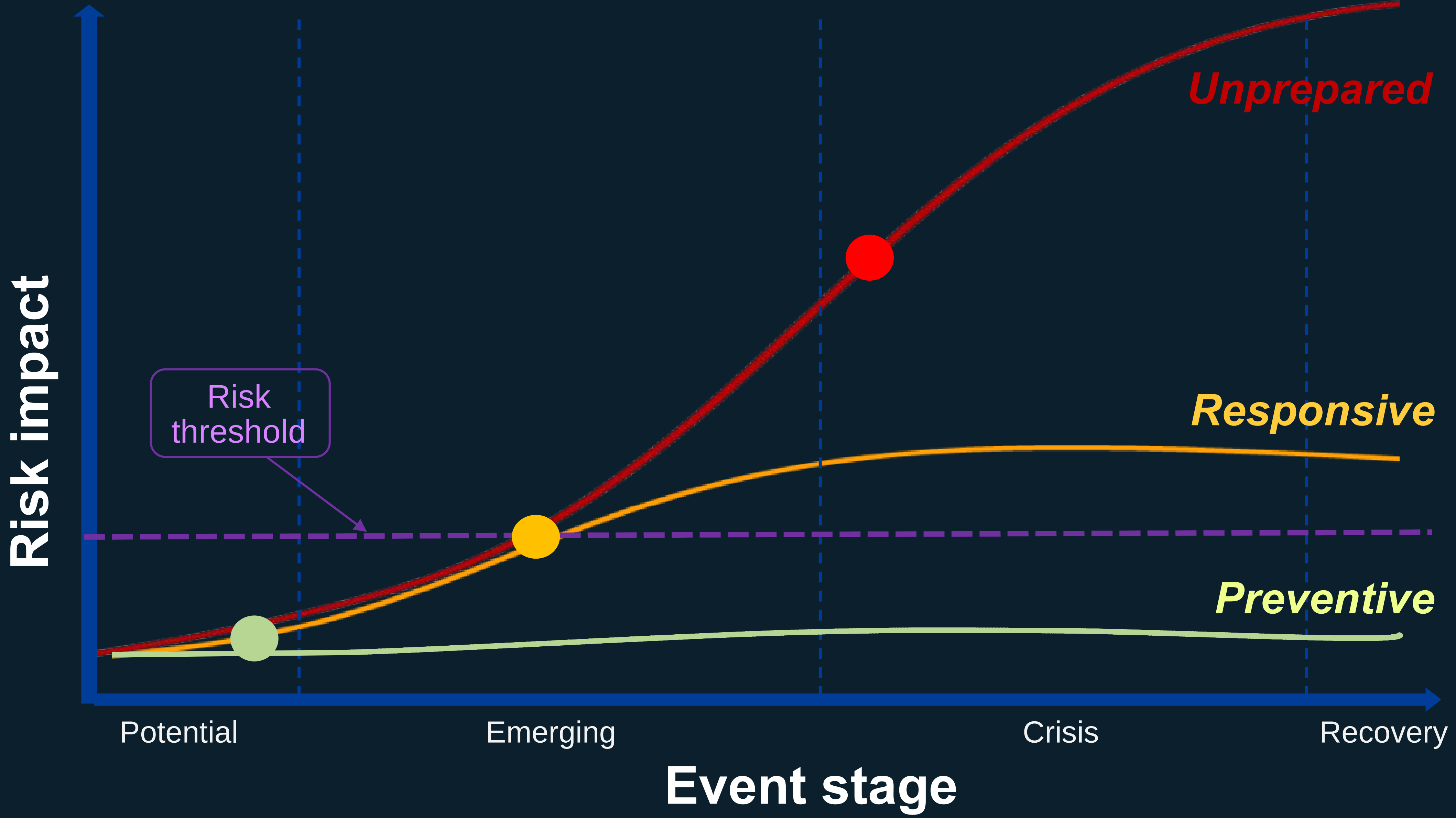
Agenda

- The Dark Web: What’s At Stake
- **Gain Visibility, Take Control**
- Live Dark Web Tour
- Key Recommendations

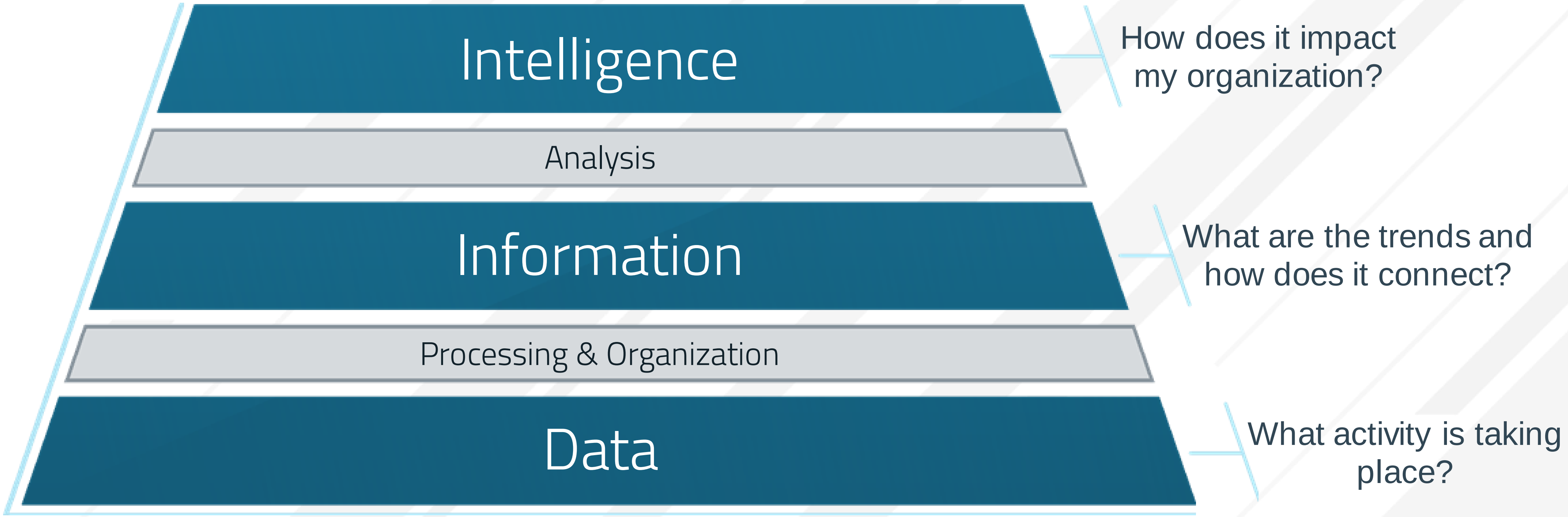
Lack Of ***Visibility***, Lack Of ***Control***



Reduce The *"Mean-time-to-Remediate"*



Turning External Data Into External "Intelligence"



Intelligence

Analysis

Information

Processing & Organization

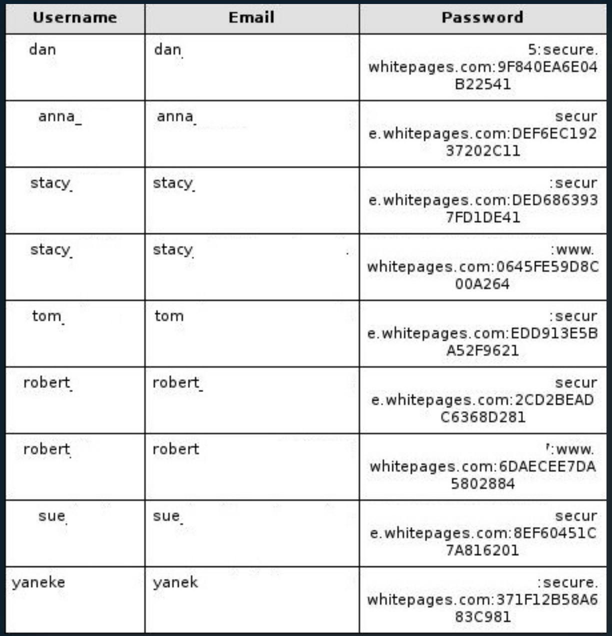
Data

How does it impact my organization?

What are the trends and how does it connect?

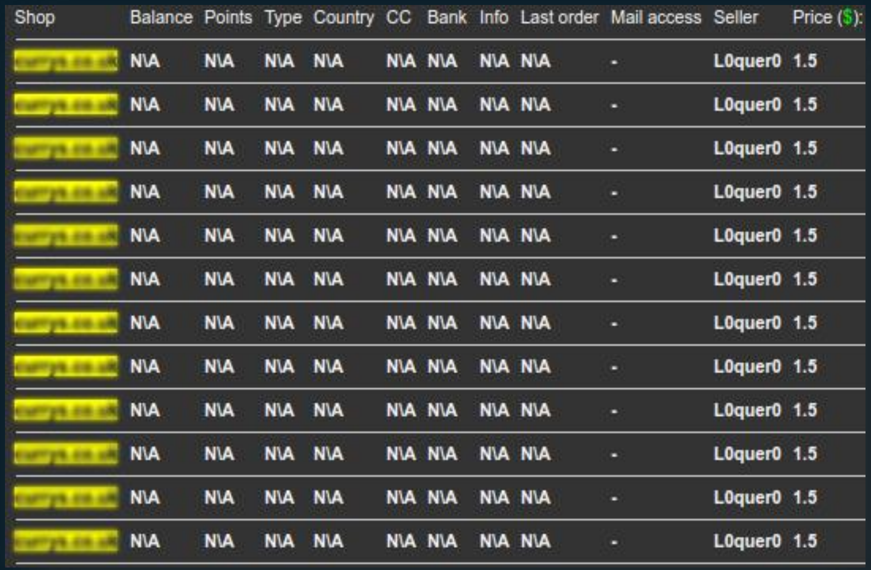
What activity is taking place?

What you’ll uncover: Compromised Credentials



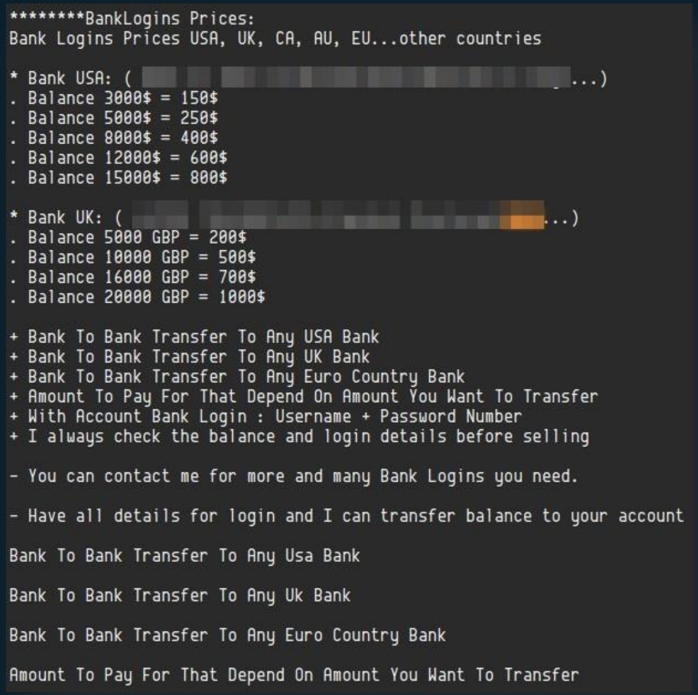
Username	Email	Password
dan	dan	5:secure.whitepages.com:9F840EA6E04B22541
anna_	anna	secure.whitepages.com:DEF6EC19237202C11
stacy	stacy	:secure.whitepages.com:DED6863937FD1DE41
stacy	stacy	:www.whitepages.com:0645FE59D8C00A264
tom	tom	:secure.whitepages.com:EDD913E5BA52F9621
robert	robert	secure.whitepages.com:2CD2BEADC6368D281
robert	robert	':www.whitepages.com:6DAECEE7DA5802884
sue	sue	secure.whitepages.com:8EF60451C7A816201
yaneke	yanek	:secure.whitepages.com:371F12B58A683C981

Employee credentials



Shop	Balance	Points	Type	Country	CC	Bank	Info	Last order	Mail access	Seller	Price ($):
[redacted]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5
[redacted]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5
[redacted]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5
[redacted]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5
[redacted]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5
[redacted]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5
[redacted]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5
[redacted]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5
[redacted]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5
[redacted]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5
[redacted]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5
[redacted]	N\A	N\A	N\A	N\A	N\A	N\A	N\A	N\A	-	L0quer0	1.5

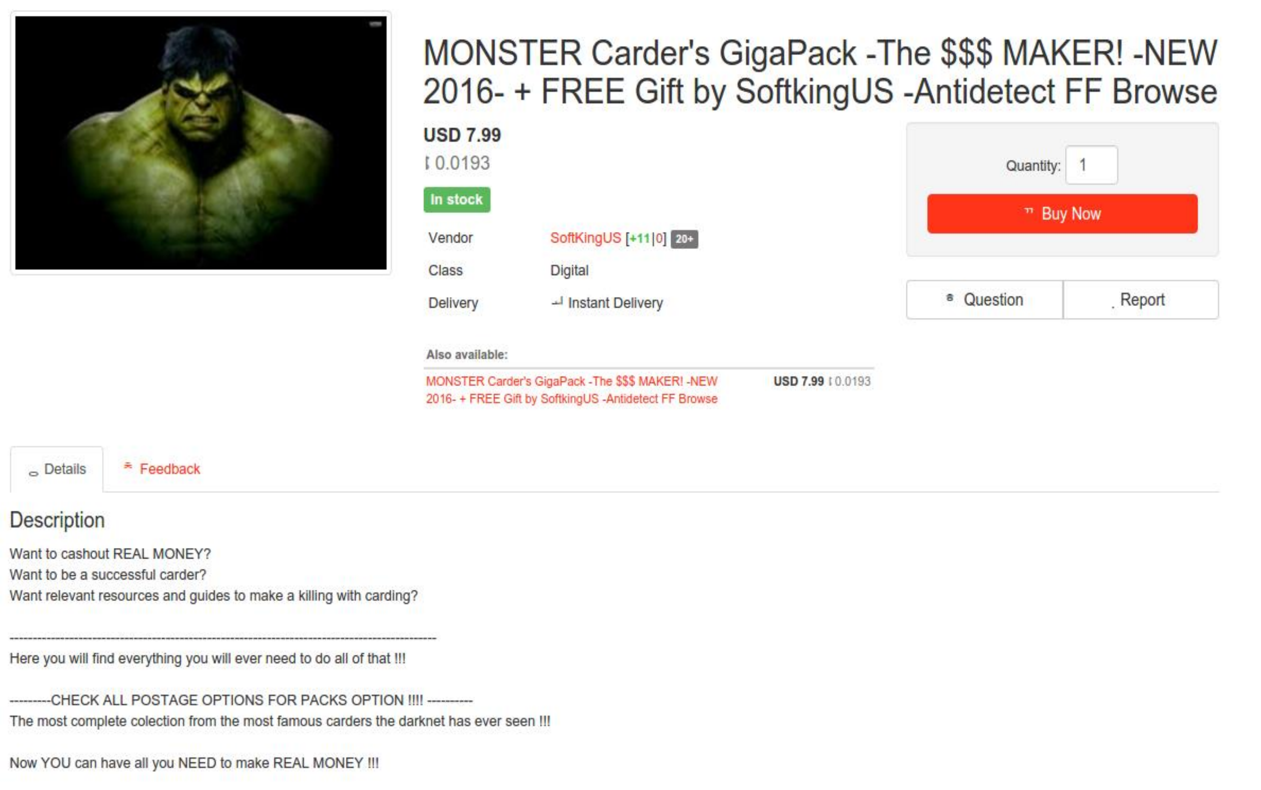
Customer logins



```
********BankLogins Prices:
Bank Logins Prices USA, UK, CA, AU, EU...other countries

* Bank USA: ( [redacted] ...)
. Balance 3000$ = 150$
. Balance 5000$ = 250$
. Balance 8000$ = 400$
. Balance 12000$ = 600$
. Balance 15000$ = 800$

* Bank UK: ( [redacted] ...)
. Balance 5000 GBP = 200$
. Balance 10000 GBP = 500$
. Balance 16000 GBP = 700$
. Balance 20000 GBP = 1000$

+ Bank To Bank Transfer To Any USA Bank
+ Bank To Bank Transfer To Any UK Bank
+ Bank To Bank Transfer To Any Euro Country Bank
+ Amount To Pay For That Depend On Amount You Want To Transfer
+ With Account Bank Login : Username + Password Number
+ I always check the balance and login details before selling

- You can contact me for more and many Bank Logins you need.

- Have all details for login and I can transfer balance to your account

Bank To Bank Transfer To Any Usa Bank

Bank To Bank Transfer To Any Uk Bank

Bank To Bank Transfer To Any Euro Country Bank

Amount To Pay For That Depend On Amount You Want To Transfer
```

Bank accounts

What you'll uncover: Stolen credit & gift cards



MONSTER Carder's GigaPack -The $$$ MAKER! -NEW 2016- + FREE Gift by SoftkingUS -Antidetect FF Browse

USD 7.99
₿ 0.0193

In stock

Vendor	SoftKingUS [+11|0] 20+
Class	Digital
Delivery	Instant Delivery

Quantity: 1

Buy Now

Question | Report

Also available:

MONSTER Carder's GigaPack -The $$$ MAKER! -NEW 2016- + FREE Gift by SoftkingUS -Antidetect FF Browse	**USD 7.99** ₿ 0.0193

Details | Feedback

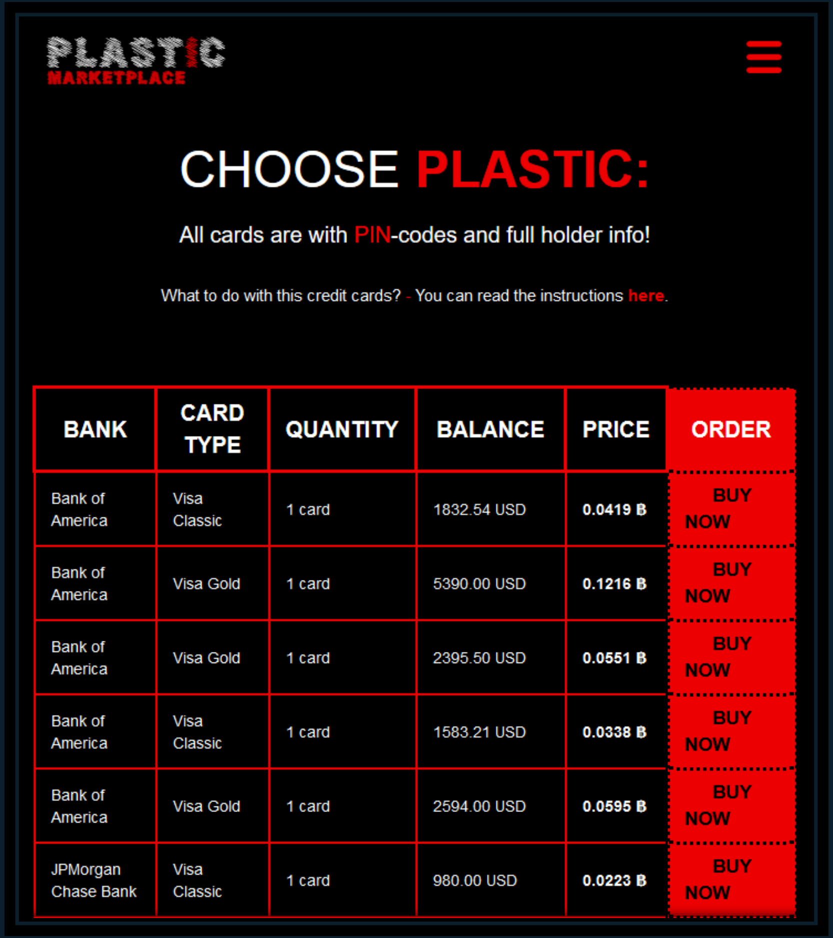
Description

Want to cashout REAL MONEY?
Want to be a successful carder?
Want relevant resources and guides to make a killing with carding?

Here you will find everything you will ever need to do all of that !!!

---------CHECK ALL POSTAGE OPTIONS FOR PACKS OPTION !!!! ----------
The most complete colection from the most famous carders the darknet has ever seen !!!

Now YOU can have all you NEED to make REAL MONEY !!!



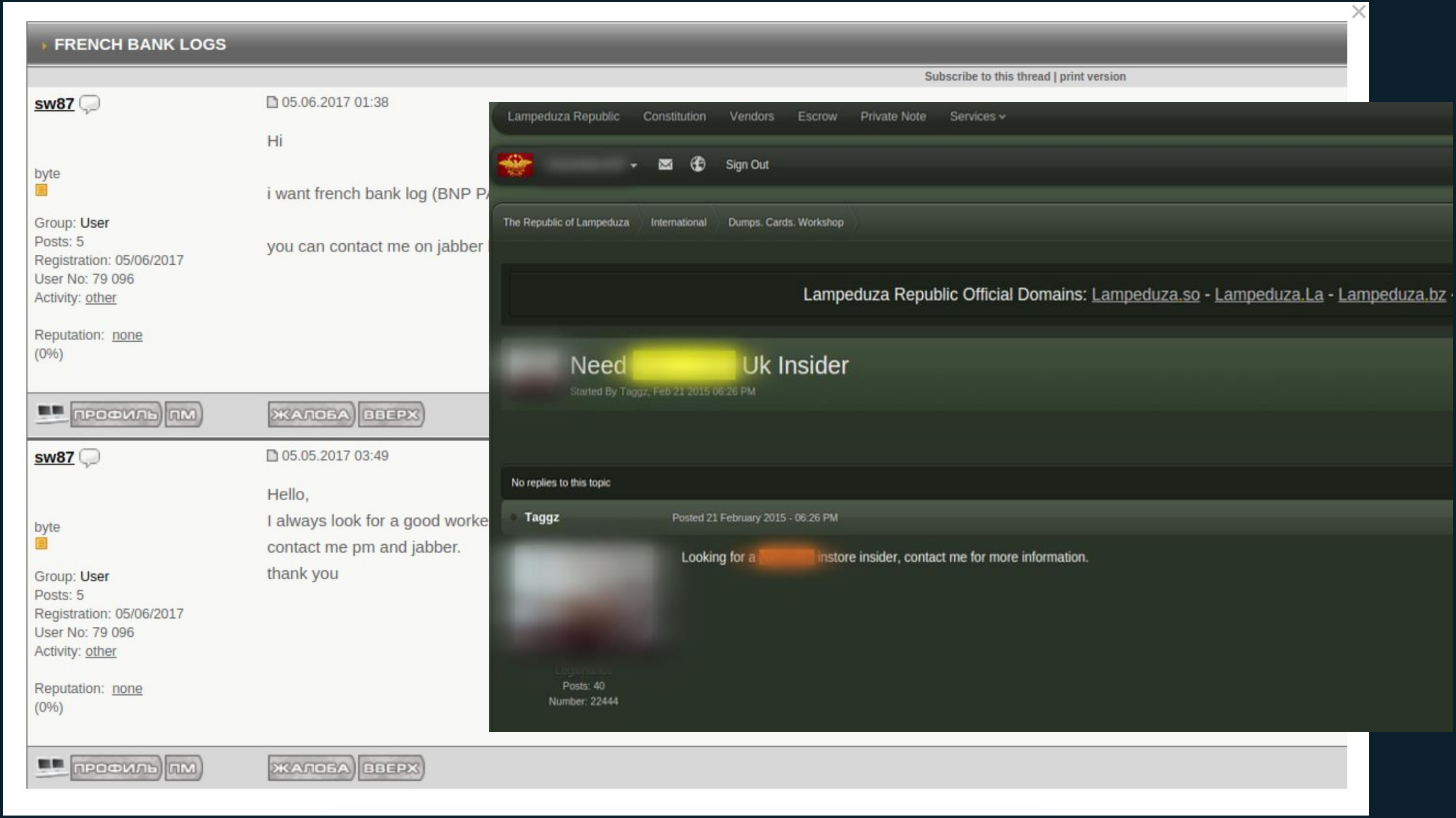
CHOOSE PLASTIC:

All cards are with PIN-codes and full holder info!

What to do with this credit cards? - You can read the instructions here.

BANK	CARD TYPE	QUANTITY	BALANCE	PRICE	ORDER
Bank of America	Visa Classic	1 card	1832.54 USD	**0.0419 ฿**	BUY NOW
Bank of America	Visa Gold	1 card	5390.00 USD	**0.1216 ฿**	BUY NOW
Bank of America	Visa Gold	1 card	2395.50 USD	**0.0551 ฿**	BUY NOW
Bank of America	Visa Classic	1 card	1583.21 USD	**0.0338 ฿**	BUY NOW
Bank of America	Visa Gold	1 card	2594.00 USD	**0.0595 ฿**	BUY NOW
JPMorgan Chase Bank	Visa Classic	1 card	980.00 USD	**0.0223 ฿**	BUY NOW

What You’ll Uncover: Insider Threats



FRENCH BANK LOGS

Subscribe to this thread | print version

sw87

byte

Group: User
Posts: 5
Registration: 05/06/2017
User No: 79 096
Activity: other

Reputation: none
(0%)

05.06.2017 01:38

Hi

i want french bank log (BNP P

you can contact me on jabber

sw87

byte

Group: User
Posts: 5
Registration: 05/06/2017
User No: 79 096
Activity: other

Reputation: none
(0%)

05.05.2017 03:49

Hello,
I always look for a good worke
contact me pm and jabber.
thank you

Lampeduza Republic Official Domains: Lampeduza.so - Lampeduza.La - Lampeduza.bz

Need [redacted] Uk Insider

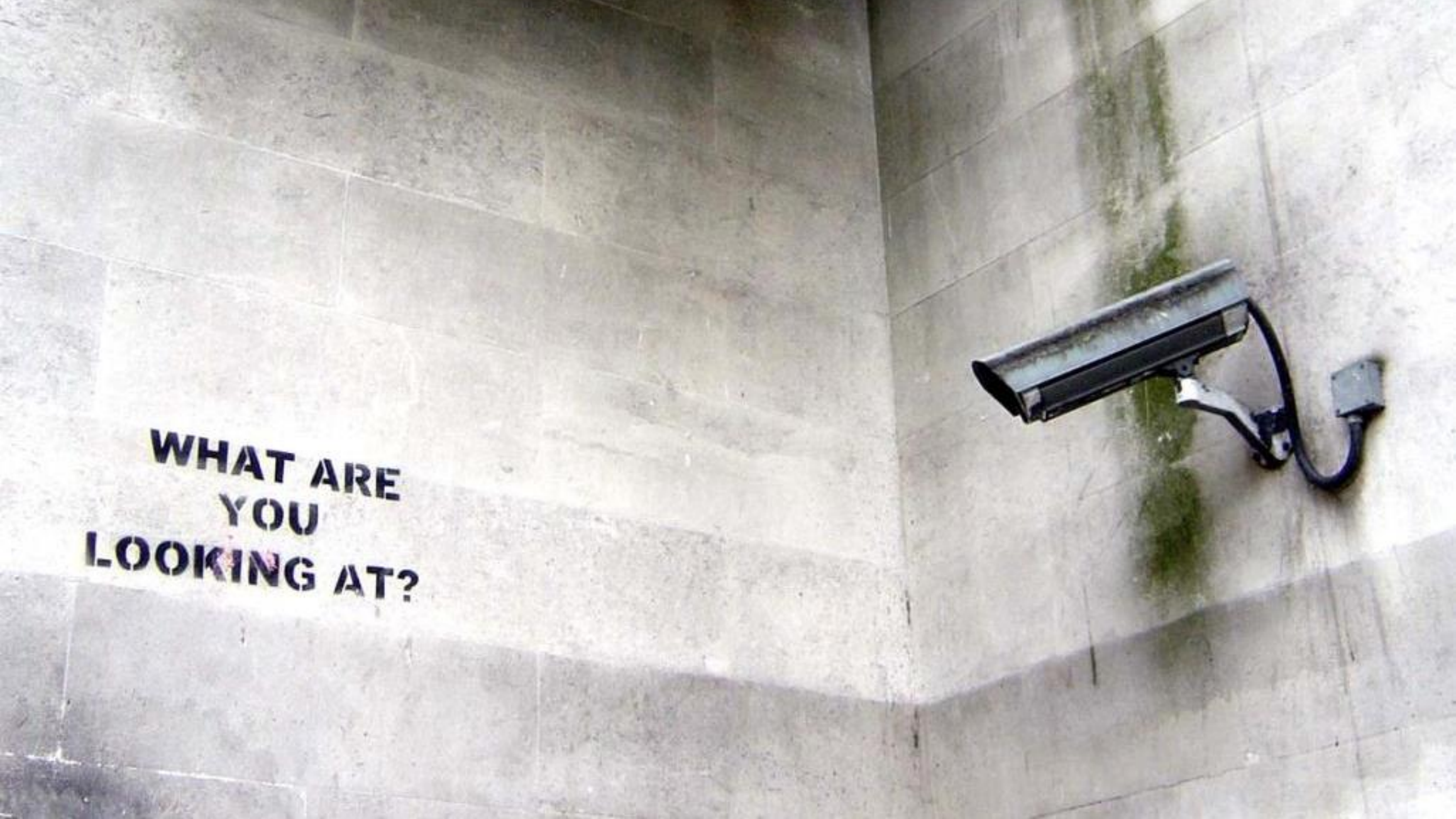
Started By Taggz, Feb 21 2015 06:26 PM

No replies to this topic

Taggz Posted 21 February 2015 - 06:26 PM

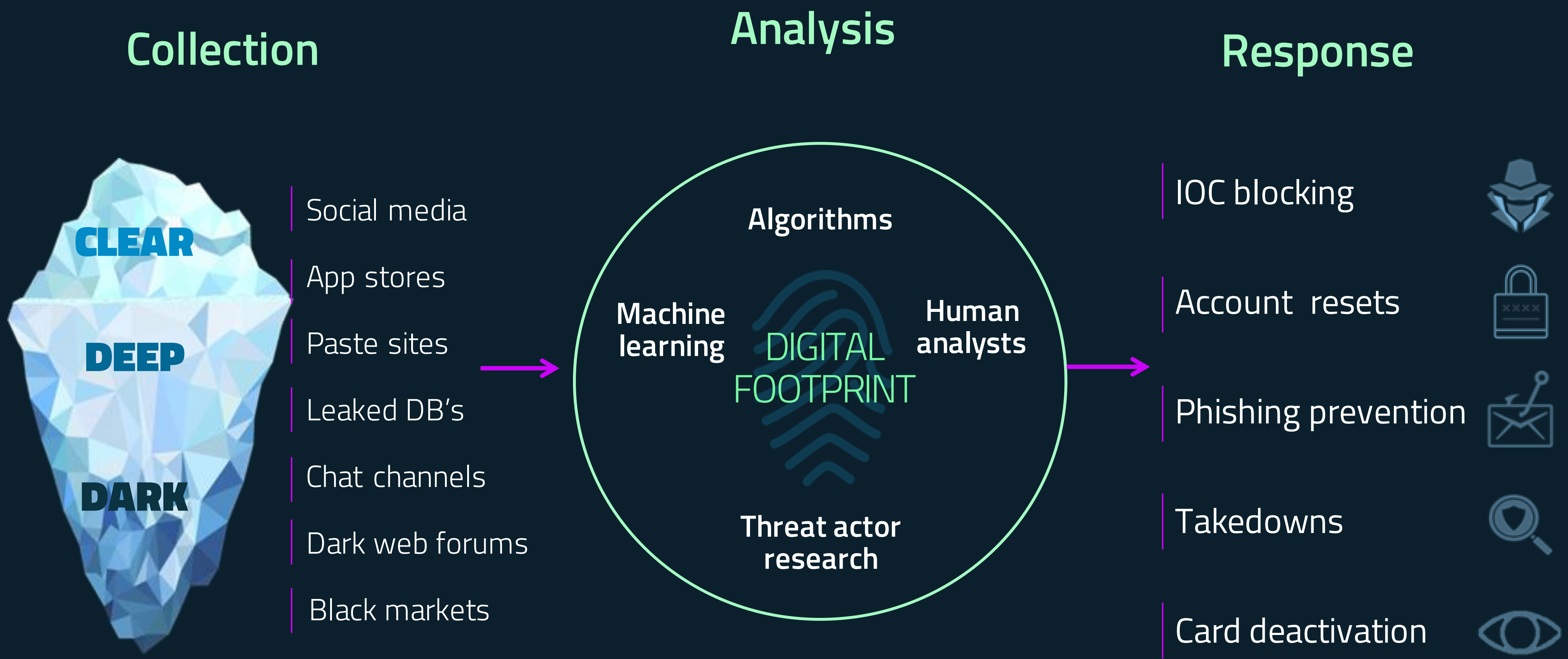
Looking for a [redacted] instore insider, contact me for more information.

Posts: 40
Number: 22444


WHAT ARE
YOU
LOOKING AT?

Tailor threat intelligence to *your business*.

Automate Your External Threat Defenses



Collection

CLEAR

DEEP

DARK

- Social media
- App stores
- Paste sites
- Leaked DB's
- Chat channels
- Dark web forums
- Black markets

Analysis

Algorithms

Machine learning

DIGITAL FOOTPRINT

Human analysts

Threat actor research

Response

- IOC blocking
- Account resets
- Phishing prevention
- Takedowns
- Card deactivation

The Emergence Of Phishing Kits

– **3)** Malware-as-A-Service & Phishing Kits

1) Website cloned

2) Credential-stealing script run from login page

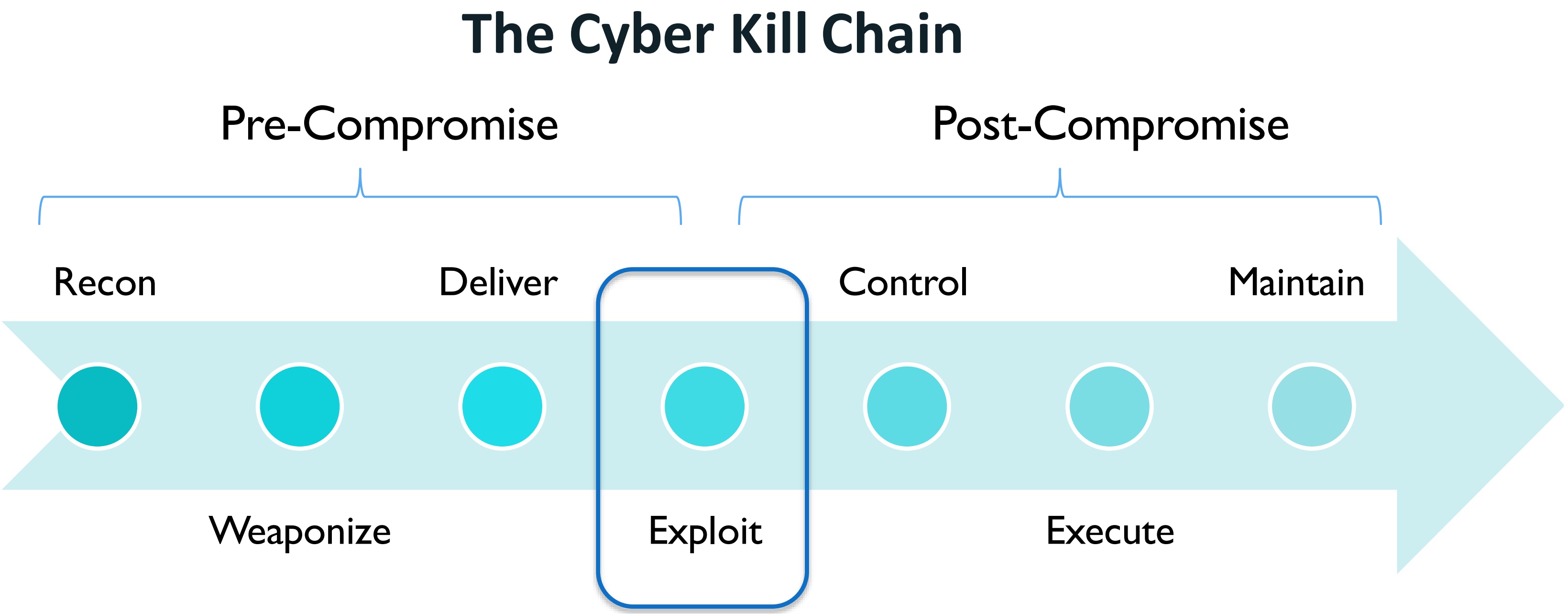
3) Credentials collected in bulk

4) Zip file uploaded and unpacked for reuse

5) New phishing campaign w/ spoofed website

Shutdown Phishing Early In Attack Chain, Pre-Exploit

- Monitor suspicious domains *before* they're activated.
- Automate the takedown process.



What External Exposures Are Threats To You?

1) Data leakage: strategic IP, customer & employee data, etc.

2) Malware-as-a-service, software exploits, phishing kits

3) Stolen and counterfeit products, gift cards, credit cards

4) Brand attacks: rogue apps, social media weaponization

5) Doxxing and digital extortion, Exec/VIP targeting

6) Compromised credentials, account takeover

7) Phishing attacks and domain squatting

8) Insider threats – hiring and coordination

9) Third-party and IT vendor risk

Embed Internal & External Remediation

- **Execute takedown processes**
  - Social networks
  - Mobile app stores
  - Registrars, domain hosting providers
- **Streamline card deactivations, password resets, reprovisioning**
- **Automate credential validation checks and protocols**
- **Integrate endpoint, gateway, and perimeter defenses**
- **Prepare digital extortion decision trees, run scenario analyses**

Agenda

- The Dark Web: What’s At Stake
- Gain Visibility, Take Control
- **Live Dark Web Tour**
- Key Recommendations

INTSIGHTS
Defend Forward.

Agenda

- The Dark Web: What’s At Stake
- Gain Visibility, Take Control
- Live Dark Web Tour
- **Key Recommendations**

INTSIGHTS
Defend Forward.

Embedding ETI Into Your Security Program

- What immediate challenges do we want to solve?
- Where are our assets & exposures? What do attackers see?
- What can we integrate or automate to improve our remediation? Internally and externally?
- How can we leverage threat intelligence in the long-term?
- What are expected outcomes in 6 months, 1 year, 3 years?

Recommendations

1) External threat intel improves SecOps – but only if it's actionable and contextualized to your organization.

2) Define use-cases upfront; start with one or two.

3) Neutralize threats on their territory; mitigate risk pre-exploit.

INTSIGHTS
Defend Forward™

Thank You!

Charity Wright
Cyber Threat Intelligence Analyst

Charity.wright@intsights.com
@CharityW4CTI

Rick Garza
Senior Sales Evan-gineer

Rick.garza@intsights.com