

# ALPHABAY MARKET: LESSONS FROM UNDERGROUND INTELLIGENCE ANALYSIS

**CHRISTY QUINN**

Threat Hunting, OSINT and Reconnaissance (THOR)



# BACKGROUND

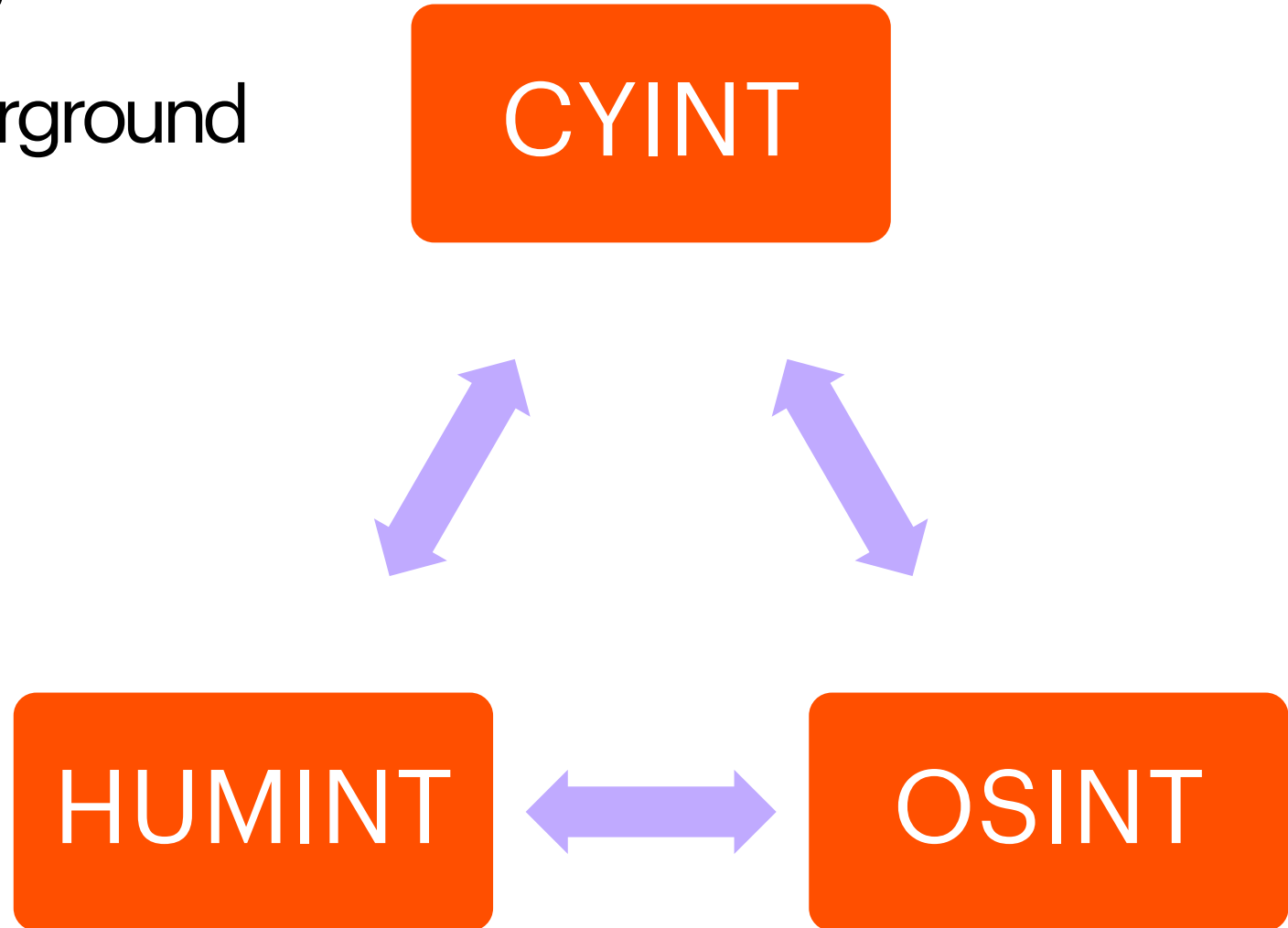
## Christy Quinn

- **South London, UK**
- **War Studies nerd**
- **Threat intel since 2015**
- **Organizations and networks...**



# BASELINE: WHAT'S UNDERGROUND INTELLIGENCE?

- Subset of threat intelligence
- Providing visibility into underground criminal activity



# PROS AND CONS...

- Get to know the people targeting you
- Identify clusters of criminal activity
- Optimal outcome- identify threat to org at target selection stage
- Suboptimal outcome- identify threat to org at post-attack exploitation stage
- High risk for average organization to homebrew- discovery and retaliation
- Technically and organizationally intensive- language, infra, opsec, etc

# CYBER CRIMINAL OPERATIONAL CYCLE

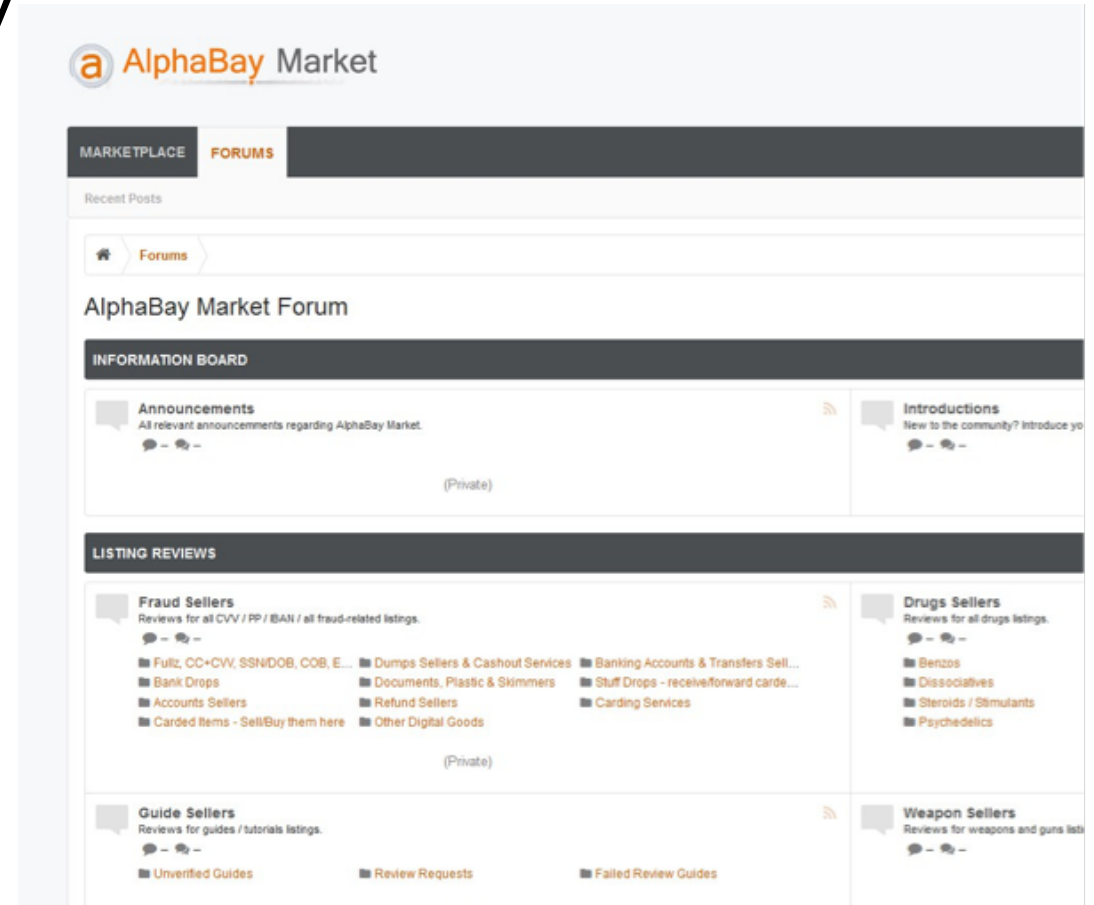


# HOW SHOULD MY ORG USE THIS?

- Global hotel and resort operator
- Identify clusters of TTPs within communities
- Interesting: employees offering insider access to customer payment systems of unspecified hotel company
- Engage with actor, ascertain threat
- Attempt to identify and mitigate planned attacks at the earliest possible stage


# DEEP DIVE: ALPHABAY MARKET

- Founded in December 2014 by Alpha02
- Combined “Silk Road” style marketplace with “Darkode” style criminal community
- By June 2017, approximately 190,000 registered members
- Target of strategic research project




# GUNS, CREDIT CARDS AND DRUGS, OH MY!

Search Results [\[Save Search\]](#)




**[MS] [Bulk] [Sticky]** 24/7 Layer 7 DDoS HTTP/Website (rent 25k botnet) (flat rate & guaranteed downtime) 2  
Item # 133745 - Botnets & Malware / Botnets & Malware - [vimproducts](#) (1762)  
Views: 20072 / Bids: Fixed price  
Quantity left: Unlimited

Buy price  
USD 25.00  
(0.0001 BTC)




**[BTC STEALER SETUP SERVICE™]** Jump From Noob to Pro Stealer In No Time - ♥ 100% POSITIVE FEEDBACK ♥  
Item # 42601 - Botnets & Malware / Botnets & Malware - [Creatine.exe](#) (6705)  
Views: 48472 / Bids: Fixed price  
Quantity left: Unlimited

Buy price  
USD 159.16  
(0.1279 BTC)



**BlackShades RAT 5.5.1 + User Guide**  
Item # 22902 - Botnets & Malware / Botnets & Malware - [shonajaan](#) (15029)  
Views: 49037 / Bids: Fixed price  
Quantity left: Unlimited (4623 automatic items)

Buy price  
USD 1.10  
(0.0009 BTC)



**[MS] Ableton Live Suite [WORKING 2017]**  
Item # 306261 - Botnets & Malware / Botnets & Malware - [lapscold](#) (12468)  
Views: 1481 / Bids: Fixed price  
Quantity left: Unlimited (24 automatic items)

Buy price  
USD 0.00  
(0.0000 BTC)

FORUMS

[Mark Forums Read](#) [Search Forums](#) [Watched Forums](#) [Watched Threads](#) [New Posts](#)

Member

Joined: Mar 19, 2015  
Messages: 350  
Likes Received: 75

[Report](#)


[Like](#) [Reply](#) #9

There's no secret in this. Its quite a simple trick. There are 3 ways to charge using CCs on stripe apart from apple pay, alipay etc.

- 1] You make a charge using ajax method on the payment form itself and your ip and useragent details will be submitted to stripe.
- 2] You submit the card details to a php file within your hosting server and your server's ip and useragent shows up on Stripe. You'll still be fingerprinted.
- 3] You have "customers" created and charge to them using any of one of the above method.

[Report](#) [Like](#) [Reply](#) #10

like this.



onionhood said: ↑

2] You submit the card details to a php file within your hosting server and your server's ip and useragent shows up on Stripe. You'll still be fingerprinted.

Pretty sure the no-charge panels are using number 2.  
But seems to be successful for a majority of people.

[Report](#) [Like](#) [Reply](#) #11



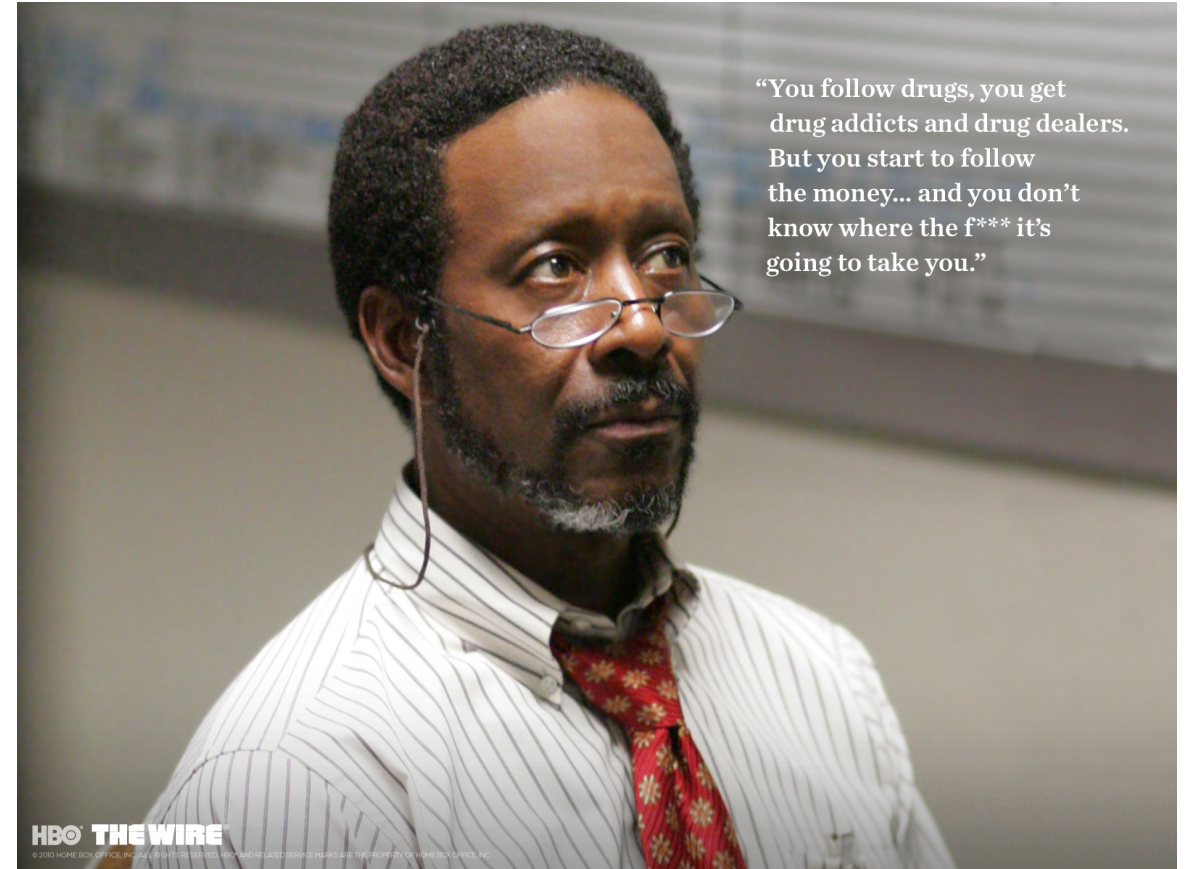
# IT WAS GREAT WHILE IT LASTED...

- Disappeared on July 5 2017
- DoJ announce joint AlphaBay – Hansa Market seizure on July 20 2017
- Some operational security mistakes...



# WHY ALPHABAY?

- Provided visibility into:
  - Operational planning of low-med tier cyber crime operators
  - Organizational relationships between Russian and English-language communities
  - Top tier criminals operating the market
  - Highly sophisticated financial model connecting AlphaBay with cryptocurrency manipulation



# "LIKE REDDIT, BUT FOR CRIMINALS"



# EXAMPLE: TACTICAL UNDERGROUND INTEL

- Contacted by criminal gang in Southern Europe on AlphaBay forum
- Had physical access to corporation's internal networks
- Needed specialist to provide malware to install using malicious insiders

\*Some details changed to protect victims

# THE RUSSIAN CONNECTION

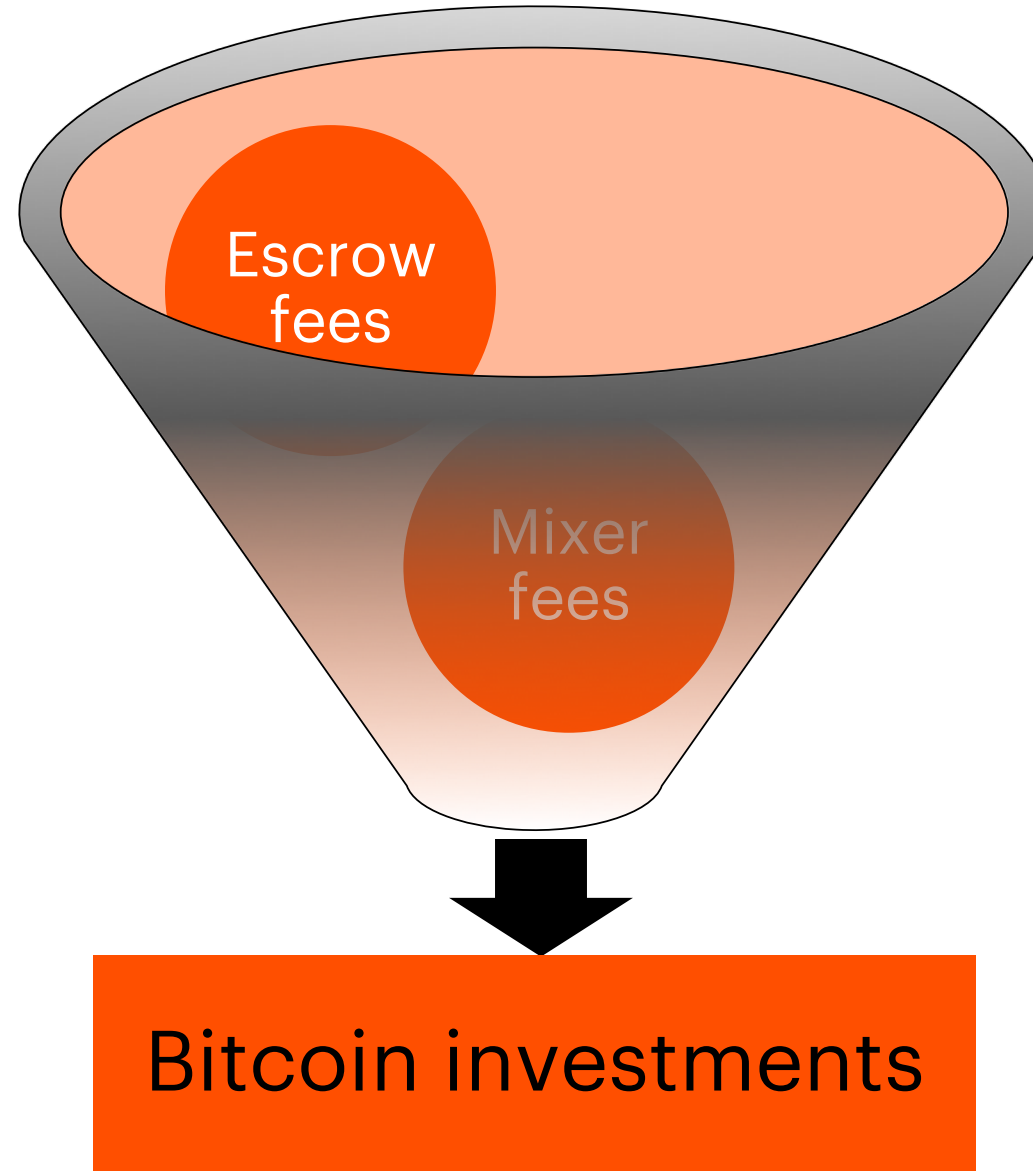
- Heavily leveraged connection to Russian underground
- Sale of Russian PII and financial data banned on market
- Cazes was Canadian and based in Thailand
- What do?



~ Будьте в безопасности, братья ~

--- Private messages from staff only. All support requests belong to the support ticket system. ---

# AB FINANCIAL MODEL





You can see Alphabay like a bank: while we allow people to deposit and withdraw at will, drugs are merely a product to attract customer. The cold wallet coins aren't just standing there: we invest in various things anonymously, make money with those investments, while always ensuring to run at 100% reserve. We won't go in the details, but there are thousands of ways to make money by investing Bitcoin online.

# HOW TO PUMP UP CRYPTO-CURRENCIES USING A MARKETPLACE

- Step 1: Buy a lot of a cryptocurrency not currently supported by marketplaces
- Step 2: Announce AB support for said-currency
- Step 3: Watch buyers flood into the market and pump up the coin's value
- Step 4: ???
- Step 5: PROFIT





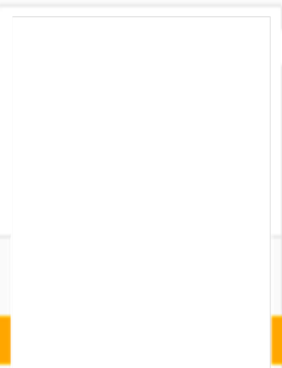
# MONERO



- Market cap:
- Aug. 18, 2016- 28,078 m USD
- Aug 21, 2016- 32,981 m Oasis Market announce support
- Aug. 22, 2016- 33,613 m AlphaBay announce support
- Sept. 1, 2016- 108,643 m AlphaBay complete integration

## Monero Charts






Joined: Mar 18, 2015  
Messages: 6,564  
Likes Received: 3,129


already very late. you should have bought the same day the AB announcement was made. there is NO excuse not to buy 5 figures worth of any crypto that AB announces it will accept

they announce they will accept dildos, you buy yourself a truckload of dildos. doesnt matter if you think it's stupid or disagree with the currency's mission, AB is nothing short of insider trading and price manipulation



, Yesterday at 5:49 PM

 Report

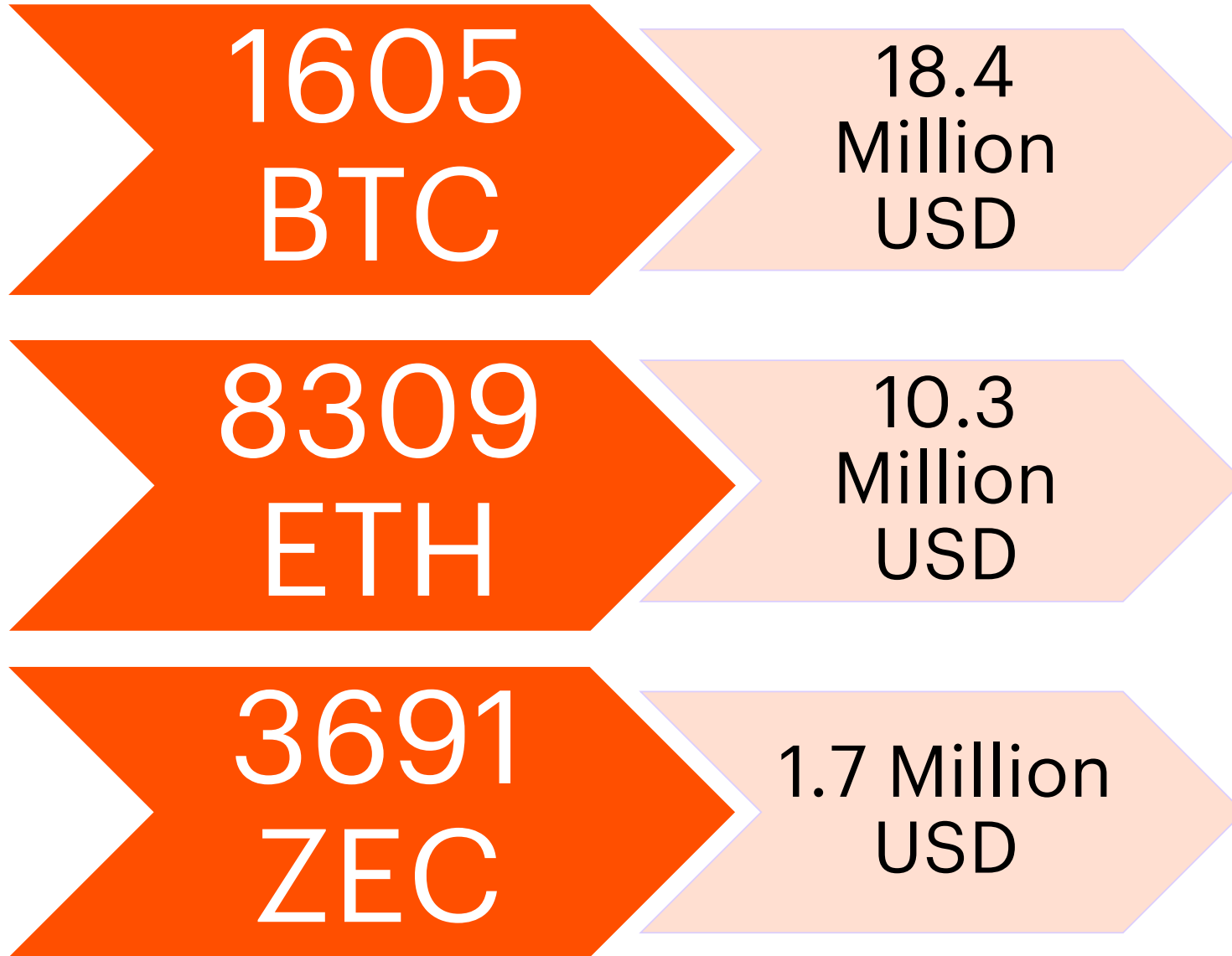
 Like

 Reply #4

[KingsX](#) likes this.

# ALEXANDRE CAZES ASSET FORFEITURE NOTICE

- 17 w. Approximately 1,605.0503851 Bitcoins seized from Alexandre CAZES and moved to  
18 secure government-controlled Bitcoin addresses:  
18 18yWFVddqNrGE966zwXTpyJgYJgr82SvMs (837.81699505 BTC) and  
19 1NXoCQLQqgaQU2cpBGtXTZ8NVmlcGnYD6p (721.76756789 BTC),
- 20 x. Approximately 8,309.271639 Ethereum seized from Alexandre CAZES and moved to  
21 secure government-controlled Ether address:  
21 0x41CC3B9213DE6FF4a8Ea85306326B00D18145E65,
- 22 y. Approximately 3,691.98 Zcash seized from Alexandre CAZES and moved to secure  
22 government-controlled address t1UAr3j9Hyt1oCMygsSLr7S3pLMuKBoNgLg,
- 23 z. Any and all Monero seized from Alexandre CAZES' personal computer and wallet  
24 addresses,



(As of Jan 28 2018)

# WHAT DOES ALPHABAY TELL US ABOUT UNDERGROUND INTEL?

- Powerful visibility into attacker intent and TTP development.
- Halt or mitigate attacks at target selection stage.
- Know your community!



# QUESTIONS?

Reach out:

@christyquinn

Christy.quinn@accenture.com