GDPO Situation Analysis

June 2018

Crypto-Market Enforcement - New Strategy and Tactics[1]

Alois Afilipoaie[2] and Patrick Shortis[3]

Subject

Between June and July 2017, two law enforcement actions targeted the cryptomarkets AlphaBay and Hansa Market, closed them, and arrested their operators, seizing millions of dollars in assets in the process. These operations, dubbed 'Operation Bayonet' (AlphaBay) and 'Operation GraveSac' (Hansa) saw a shift in the strategy and tactics that law enforcement agencies are using to target cryptomarket activity on the Tor network.[4] By deconstructing the operation, this situational analysis aims to provide pertinent lessons on how law enforcement agencies have adapted their approach towards tackling cryptomarkets.

History of the Operations

- On June 20th, 2017 the Netherlands National High Tech Crime Unit (NHTCU) infiltrated Hansa Market and took over the site's operations (Operation GraveSac), without alerting users or disrupting illicit sales.[5] This was done with the help of private cybersecurity company Bitdefender that supplied information that enabled the NHTCU to compromise a server in the Netherlands. This action led to German authorities arresting the two Hansa Market administrators, who provided information on another server in Germany and the main server's location in Lithuania. A link was then set up between the servers in Lithuania and the Netherlands that allowed law enforcement to create a real-time copy of the market database within NHTCU jurisdiction. They also obtained the cryptomarket

[1] This Situation Analysis was produced as part of a GDPO collaboration with Central European University's School of Public Policy (see http://gdpo.swan.ac.uk/?p=494 for more information)
[2] University of Bradford
[3] University of Manchester
[4] Europol Press Release. (2017). *Massive blow to criminal dark web activities after globally coordinated operation*. Available: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation
[5] Mihov, Dimitar. (2017) "Dutch police secretly ran a huge dark web drug marketplace for a month." *The Next Web*, 20 July 2017. Available: https://www.thenextweb.com/insider/2017/07/20/police-fbi-drug-dark-web-market/

source code that enabled them to modify the site and thus improve their intelligence collection capabilities.[6]

- A takedown operation on July 5th (Operation Bayonet) headed by U.S. law enforcement agencies closed AlphaBay and revealed 25-year-old Canadian Alexandre Cazes as the site's administrator 'alpha02'. He was arrested in Thailand pending extradition to the United States. Despite being the largest cryptomarket at the time, law enforcement made no official announcements of the arrest, leaving the user community to speculate about the market's downtime.[7] Initial reaction was that the administrators had performed an exit-scam, a theory that gained traction when members of the community noticed large bitcoin transactions they suspected as originating from the cryptomarket's wallet.[8]
- Following the shutdown of AlphaBay, Hansa Market saw an eight-fold increase in new registrations.[9] The administrators (NHTCU) announced they would temporarily close registration to cope with the influx and continue to fulfil orders.[10] This kind of action had been previously taken by cryptomarkets that experienced large jumps in their user base following rival market closures and therefore it did not raise the suspicions of Hansa's community.
- Cazes committed suicide in his Thai prison cell on July 12th and news broke out shortly afterwards that linked his arrest and subsequent death to a law enforcement operation that had taken down AlphaBay.[11] At this point the cryptomarket community was still unsure about law enforcement's involvement in AlphaBay's closure. Users were also unaware of any law enforcement links between AlphaBay and Hansa Market.
- On July 20th the US Federal Bureau of Investigations (FBI) and Europol released a joint statement confirming the operations and posted seizure notices on both Hansa and AlphaBay. Europol claimed that during the 27 days the NHTCU had control of Hansa as part of Operation GraveSac they monitored approximately 1,000 daily transactions. Additionally, they gathered 10,000 postal addresses along with thousands of messages from Hansa customers. Regarding Operation Bayonet the FBI estimated over 200,000 customers, 40,000 vendors and over 350,000 listings on AlphaBay.[12] This included 250,000 listings in illegal drugs plus over $1bn in total transactions since its inception in 2014, making it the largest cryptomarket to date.[13]

[6] Krebs, Brian. (2017) "Exclusive: Dutch Cops on Alphabay 'Refugees'". Krebs On Security. July 20, 2017. Available: https://krebsonsecurity.com/2017/07/exclusive-dutch-cops-on-alphabay-refugees/

[7] Fox-Brewster, Thomas. (2017) "How The Cops Took Down An Alleged $23 Million Dark Web Drug Kingpin." Forbes.com. 20 July 2017. Available: https://www.forbes.com/sites/thomasbrewster/2017/07/20/dark-web-drugs-to-suicide-accused-alexandre-cazes/#777e66361250

[8] Price, Rob. (2017) "One of the biggest dark web drug marketplaces went down, causing chaos for customers." Business Insider. July 06, 2017. Available: http://uk.businessinsider.com/dark-net-market-alphabay-down-exit-scam-accusations-2017-7

[9] Europol Press Release. (2017). *Massive blow to criminal dark web activities after globally coordinated operation*. Available: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

[10] Howell O'Neill, Patrick. (2017) "Fall of AlphaBay raises 'a different balance of power' on the dark web." CyberScoop. July 14, 2017. Available: https://www.cyberscoop.com/alpha-bay-closed-hamsa-dream-valhalla-dark-web/

[11] Keating, Fiona. (2017) "Co-founder of AlphaBay dark web for drugs and weapons found dead in cell." The Independent. July 16, 2017. Available: http://www.independent.co.uk/news/world/alphabay-alexandre-cazes-dark-web-dark-net-hanged-thailand-bangkok-narcotics-suicide-drug-a7843626.html

[12] These numbers have been disputed by findings from the academic community. See: Paquet-Clouston, Masarah, David Décary-Hétu, and Carlo Morselli. (2018) "Assessing market competition and vendors' size and scope on AlphaBay." *International Journal of Drug Policy* 54: 87-98. doi:10.1016/j.drugpo.2018.01.003.

[13] Europol Press Release. (2017). *Massive blow to criminal dark web activities after globally coordinated operation*. Available: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

Tactical Lessons

Operations GraveSac and Bayonet saw a combination of diverse operational tactics at play that made them markedly different from previous law enforcement actions aimed at taking down cryptomarkets.

1. The Honeypot

The use of Hansa Market as a compromised honeypot was a tactical shift that law enforcement had previously not used in cryptomarket operations and more closely mirrors operations aimed at Clearnet carding sites like Dark Market or Tor hidden services for child pornography like Playpen.[14] However as illicit e-commerce sites, cryptomarkets are more structurally complex and require specialised knowledge to manage the balance of customer service, disputes, and community engagement. The fact that the NHTCU were able to run the market and collect intelligence - without raising suspicion of the community - illustrates a developed level of understanding, technical ability, and capacity to engage in effective undercover operations targeting cryptomarkets.

2. Exploiting Technical Infrastructure

The NHTCU exploited several existing security features of the market's infrastructure to gather information on users. Login credentials were collected together with any unencrypted messages sent over the site. The system for removing photo metadata was also disabled, so that images would upload with the default Exchangeable Image File (EXIF) information that includes geolocation data. This allowed law enforcement to geotag users' images which gave them the coordinates of where each picture was taken.[15] They were also able to exploit the market's in-built PGP ('Pretty Good Privacy' software) system and decrypt all messages sent through it. The NHTCU also carried out a complex technical attack using Hansa's existing locktime file system. A newly-developed security feature, it created a '.txt' document that registers data about a vendor's transactions so that they can retrieve their funds from the market during downtime. The NHTCU turned these '.txt' files into an '.xlsx' file (spreadsheet) that forced the user's PC to ping a law enforcement server with its real IP address if it wasn't properly funnelling all its internet traffic through Tor or a VPN.[16]

3. Managing the Migration

Once a leading cryptomarket closes, many of its users will migrate to the largest remaining cryptomarkets shortly afterwards.[17] The honeypot operation hinged on this expectation and the NHTCU were careful to manage this process to maximise the information they could gain on large-scale orders of illegal drugs. To do this they temporarily closed registrations for new users to slow the amount of orders that came in and to log them effectively.[18] The tactic boosted their legitimacy as real administrators in the eyes of Hansa users as cryptomarkets have taken similar actions to mitigate against security problems posed by large migrations of

---

[14] Rumold, Mark. (2016) "Playpen: The Story of the FBI's Unprecedented and Illegal Hacking Operation." Electronic Frontier Foundation. September 28, 2016. Available: https://www.eff.org/deeplinks/2016/09/playpen-story-fbis-unprecedented-and-illegal-hacking-operation

[15] Greenberg, Andy. (2018) "Operation Bayonet: Inside the Sting that Hijacked and Entire Dark Web Drug Market". March 8, 2018. Available: https://www.wired.com/story/hansa-dutch-police-sting-operation/

[16] Cimpanu, Catalin. (2017) "Crooks Reused Passwords on the Dark Web, so Dutch Police Hijacked Their Accounts." BleepingComputer. July 26, 2017. Available: https://www.bleepingcomputer.com/news/security/crooks-reused-passwords-on-the-dark-web-so-dutch-police-hijacked-their-accounts/

[17] Martin, James. (2014) *Drugs on the dark net: how cryptomarkets are transforming the global trade in illicit drugs*. Basingstoke: Palgrave Macmillan. p23

[18] Krebs, Brian. (2017) "Exclusive: Dutch Cops on Alphabay 'Refugees'". Krebs On Security. July 20, 2017. Available: https://krebsonsecurity.com/2017/07/exclusive-dutch-cops-on-alphabay-refugees/

customers.[19] Rather than raising suspicions, the closure of new registrations was approved of by the community. This illustrates the NHTCU's advanced knowledge of the social behaviours and expectations of the Hansa user base, which they manipulated accordingly.

4. Targeting Trust

Both GraveSac and Bayonet used tactics designed to weaken the trust within the cryptomarket community during and after the operations were carried out. The FBI delayed their announcement of the AlphaBay takedown to give users the impression that an exit scam had taken place, creating instability within the environment. This was compounded by the later announcement that Hansa had been under law enforcement control for 27 days. The paranoia was then magnified once it emerged that the NHTCU had used customer login credentials to steal user funds from other markets and changed the PGP keys of vendors to their own. As a result, anyone who had sent a PGP message to a compromised vendor in that period had instead sent it to law enforcement.[20] Dutch authorities also posted the pseudonymised screen names of vendors and buyers under investigation to a hidden service they had previously created to deter users.[21] Finally, law enforcement followed up on these operations with a secondary joint action in February 2018. Users of Hansa in the United States and the Netherlands were visited by officers conducting a series of "knock-and-talk" actions. They were informed that their addresses had been compromised in the Hansa bust, and warned to stay away from cryptomarkets.[22] These actions dealt successive psychological blows to the community and shows a tactical shift away from takedowns and towards creating fear, uncertainty and doubt in the crypto-market trade.

5. Strategic Lessons

These tactics highlight a strategic shift in law enforcement approaches to international partnership and enforcement goals concerning cryptomarkets. They required close cooperation and coordination between government agencies, international organisations and the private sector. The level of success demonstrates that law enforcement agencies have consolidated their capacity and understanding of cryptomarkets. Support received from the private sector is indicative of a trend of collaboration between cybersecurity companies and government agencies in tracking activity on Tor.[23]

This multi-pronged approach was a step-change from previous law enforcement operations that aimed primarily at market closure. Law enforcement tactics demonstrate a strategic shift that focuses on breaking trust within the cryptomarket community. Several academic studies have shown that trust is integral to all aspects of cryptomarket operations as users are engaging in transactions in an anonymised space. Therefore feedback, community forums and the honesty of administrators in mediating disputes play a central role in the functionality of cryptomarkets.[24] By targeting these elements that underpin user trust rather than closing markets and arresting users immediately, law enforcement was able to deal more lasting damage to the

[19] Blackmarketreloaded.org. (2013) "Black Market Reloaded Closing". December 3, 2013. Available: https://blackmarketreloaded.org/black-market-reloaded-closing/

[20] Krebs, Brian. (2017) "Exclusive: Dutch Cops on Alphabay 'Refugees'". Krebs On Security. July 20, 2017. Available: https://krebsonsecurity.com/2017/07/exclusive-dutch-cops-on-alphabay-refugees/

[21] Dutch National Police. (2016) "Active At Dark Markets? You Have Our Attention." Dutch National Police Hidden Service. Available: http://politiepcvh42eav.onion. (Requires Tor Browser to access)

[22] Dutch National Police (2018) "Operation Mirum, darkweb is not anonymous". February 15, 2018. Available: https://www.politie.nl/nieuws/2018/februari/15/operation-mirum-darkweb-is-not-anonymous.html

[23] DividedBy0. (2018) "How the American Government Surveils the Blockchain." Deep Dot Web. January 16, 2018. Available: https://www.deepdotweb.com/2018/01/17/american-government-surveils-blockchain/ And: Williams-Grut, Oscar. (2016) "A startup that helps police track criminals using bitcoin just raised $5 million." Business Insider. March 21, 2016. Available: http://uk.businessinsider.com/bitcoin-tracking-company-elliptic-raises-5-million-series-a-2016-3

[24] Duxbury, Scott W., and Dana L. Haynie. (2017). "The Network Structure of Opioid Distribution on a Darknet Cryptomarket." *Journal of Quantitative Criminology*, 1-27. doi:10.1007/s10940-017-9359-4. And:
Tzanetakis, M., Kamphausen, G., Werse, B., & von Laufenberg, R. (2015). 'The transparency paradox. Building trust, resolving disputes and optimising logistics on conventional and online drugs markets'. *International Journal of Drug Policy*, 35, pp.58–68.

community. While this is the case, a good argument can be made that such action could possibly undermine the potentially beneficial characteristics of cryptomarkets, especially in regards to what has been called 'indigenous harm reduction'.[25]

Summary and Conclusions

- **Law enforcement has gained deeper knowledge of the cryptomarket environment**
  GraveSac and Bayonet present evidence that international law enforcement agencies have made significant gains in capabilities and tactics for targeting cryptomarkets. Lessons from previous operations have resulted in funding being channelled for the creation of dedicated teams to deal with this emergent form of crime.[26] The resulting improvements in knowledge and training have underpinned the enhanced cooperation, communication and methods which made these operations successful.

- **GraveSac and Bayonet highlight a change in cryptomarket enforcement**
  The operations illustrate a shift in strategy that refocuses on breaking trust in the community rather than merely closing markets. This approach signals that law enforcement understand the resilient nature of the cryptomarket trade and that targeting trust and maximising intelligence collection are more beneficial outcomes. It is likely we can expect to see more complex operations in future that will seek similar goals, using combinations of technical attacks, psychological manipulation and undercover operatives to achieve them.

- **The operations damaged trust but didn't break it**
  In the immediate aftermath users were cautious of the new market leader Dream Marketplace, with some voicing concerns that it could be another honeypot run by police.[27] This is highly unlikely given that the market recently implemented Monero as a payment system, a change that makes payments much more difficult to trace.[28] Overall there is evidence to suggest that cryptomarket sales are back to pre-bust levels, showing once again that law enforcement's impacts on sales are short-lived.[29]

- **Tactical displacement breeds tactical displacement**
  The immediate success of this operation is highly likely to drive advancements in security tradecraft among the community, making future investigations more difficult. Cryptomarket users are becoming wary of the busts, exit-scams and arrests that see markets closed and their bitcoins stolen. With OpenBazaar integrating Tor and the high transaction costs of Bitcoin pushing people to anonymised cryptocurrencies like Monero, we are now closer than ever before to a much more complex, decentralised and anonymous model for online illicit commerce.[30]

---

[25] Bancroft, Angus., and Reid, Peter Scott, (2016), 'Concepts of illicit drug quality among darknet market users: purity, embodied experience, craft and chemical knowledge,' *International Journal of Drug Policy,* 35, 42-29

[26] Cox, Joseph. (2015) "The UK Will Police the Dark Web with a New Task Force." Motherboard. November 08, 2015. Available: https://motherboard.vice.com/en_us/article/wnxeyn/the-uk-will-police-the-dark-web-with-a-new-task-force

[27] Mihov, Dimitar. (2017). "After AlphaBay and Hansa, Dream Market reportedly also seized by police." The Next Web. July 21, 2017. Available: https://thenextweb.com/insider/2017/07/21/dark-web-drug-market-alphabay-dream/

[28] Ista. (2018). "Dream Market Integrates Monero Payments." Dream Market Drugs. February 8, 2018. Available: https://dreammarketdrugs.com/dream-market-integrates-monero/

[29] Dittus, Martin. (2017) "A distributed resilience among darknet markets?" Oxford Internet Institute. November 9, 2017. Available: https://www.oii.ox.ac.uk/blog/a-distributed-resilience-among-darknet-markets/

[30] DividedBy0. (2017) "OpenBazaar Finally Integrates Tor." Deep Dot Web. February 28, 2017. Available: https://www.deepdotweb.com/2017/03/04/openbazaar-finally-integrates-tor/ And: Morse, Jack. "You know who's not loving Bitcoin's rise? Speed freaks." Mashable. December 19, 2017. Available: https://mashable.com/2017/12/19/bitcoin-fees-annoy-darkweb-buyers/#LgCpXGZ_zsqq

supported by

OPEN SOCIETY FOUNDATIONS

About the Global Drug Policy Observatory

The Global Drug Policy Observatory aims to promote evidence and human rights based drug policy through the comprehensive and rigorous reporting, monitoring and analysis of policy developments at national and international levels. Acting as a platform from which to reach out to and engage with broad and diverse audiences, the initiative aims to help improve the sophistication and horizons of the current policy debate among the media and elite opinion formers as well as within law enforcement and policy making communities. The Observatory engages in a range of research activities that explore not only the dynamics and implications of existing and emerging policy issues, but also the processes behind policy shifts at various levels of governance.

Global Drug Policy Observatory

Research Institute for Arts and Humanities

Room 201 James Callaghan Building

Swansea University

Singleton Park, Swansea SA2 8PP

Tel: +44 (0)1792 604293

www.swansea.ac.uk/gdpo

@gdpo_swan

GdPO Global Drug Policy Observatory

reportingmonitoringanalysis