https://doi.org/10.51483/IJCCR.5.2.2025.13-26

ISSN: 2790-1386

International Journal of Cryptocurrency Research

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper

Open Access

Dark Angels and the Largest Crypto Ransom Payment in History: Addressing Key Intelligence Gaps with Dark Angels

Shayiq Ahmed Shah[1*]

[1]Crypto Threat Intelligence Project, Middlebury Institute of International Studies, Monterey, CA 93940, United States. E-mail: shayiqahmeds@middlebury.edu

Article Info

Volume 5, Issue 2, December 2025
Received : 11 August 2025
Accepted : 22 November 2025
Published : 22 December 2025
doi: 10.51483/IJCCR.5.2.2025.13-26

Abstract

Dark Angels is a formidable cyber-criminal group that in the spring of 2024 received a record $75 million ransom payment. With their strategy of "big game hunting", they have emerged as one of the biggest threats to US corporations. Yet, there remains an intelligence gap with regards to the threat posed by Dark Angels. This project analyzes Dark Angels' patterns of crypto laundering and funds obfuscation techniques.

Keywords: *Dark angels, Cyber-criminal group, US corporations, Crypto laundering*

1. Introduction

Intelligence reports for the year 2024 suggest that there was a significant reduction in the total amount of ransomware payments made using virtual currency than those made in 2023. The 2024 annual report by Chainanalysis claimed a 35% year-on-year reduction in the total amount of ransom paid to ransomware attackers between 2023 to 2024.[1] However, the total amount of reported ransom payments, in 2024, still stood at approximately $813.55 million. The keyword here being: *reported*. As this study will showcase, through highlighting the dark cloud of uncertainty around the largest ransom payment in history, there are strong reasons to believe that many ransom payments are never reported to the relevant authorities. The continuing lack of mandated reporting requirements allows corporations to not disclose ransom payments made to cybercriminals. Therefore, a more accurate total of ransom payments made in cryptocurrency could well be much higher than the reported figure of $813.55 million.

US critical infrastructure is under grave attack, and we may not even know the true magnitude of the threat. Targeting of US critical infrastructure by ransomware attackers exposes a key national security vulnerability.

[1] 35% Year-Over-Year Decrease in Ransomware Payments, less than Half of Recorded Incidents Resulted in Victim Payments. *Chainalysis*, February 5, 2025.

* *Corresponding author: Shayiq Ahmed Shah, Crypto Threat Intelligence Project, Middlebury Institute of International Studies, Monterey, CA 93940, United States. E-mail: shayiqahmeds@middlebury.edu*

Presidential Policy Directive 21 established the 16 Critical Infrastructure sectors and placed them under the surveillance of the Cybersecurity and Infrastructure Security Agency (CISA).[2] In 2022, the Biden administration enacted the Cyber Incident Reporting for Critical Infrastructure Act, CIRCIA, which proposed mandatory reporting requirements for all "covered entities" that fell under one of the 16 US critical infrastructure sectors.[3] However, the CIRCIA act is yet to be passed and as it stands, corporations are not obligated to report to the US government any ransomware attacks or payments.

Public disclosures remain on a voluntary basis. Upon facing mass network or business disruptions, because of a cyberattack, many corporations have chosen to publicly disclose ransomware attacks and payments for the purposes of damage control. However, if they don't face public facing business disruptions, corporations have been hesitant to report attacks or ransom payments to law enforcement. Instead, they rely on the private sector to respond to such incidents, such as incident response firms. Such firms prioritize client privacy and treat their practices as trade secrets and therefore are de-incentivized to disclose attacks or ransom payments to the public or law enforcement.

The combination of these factors mentioned above helps explain the mystery behind the largest ransom payment made in history for a sum of about $75 million. In March of 2024, a $75 million ransom payment was made to operatives of a cybercriminal gang called Dark Angels by an unnamed victim following a ransomware attack.[4] This figure, reported in the Zscaler ThreatLabz ransomware report for 2024, is almost double the previous largest known ransom payout.[5] The previous largest payout stood at $40 million and was paid in 2021 by the insurance company CNA Financial. With a staggering sum of $75 million, Dark Angels now commands the highest known crypto ransom payout in history. Having said, we know very little of this attack or of the attackers.

We are unaware of what entity was the victim, what ransomware was deployed, and whether this entity experienced business disruptions, jeopardized data or both. Information on the attack could have assisted law enforcement and cybersecurity companies in studying the tactics, techniques, and procedures of Dark Angels and consequently, designing specific countermeasures. However, this case highlights the current lack of reporting requirements along with the emergence of a new competitive economy wherein incident response firms are de-incentivized to publicly disclose attack details.

With a lack of evidence available to the public, this report aims to fill in such scholarly and research gaps. It analyses the behaviour of Dark Angels, and their tactics, techniques, and practices used in their crypto laundering scheme. It begins with a literature review to compile known information on Dark Angels and the threat they pose. In doing so, it highlights the gap in such literature and identifies its research objectives to fill in those gaps.

2. Background: What Do We Know So Far?

Dark Angels ransomware surfaced with attacks beginning in April 2022. It operates out of Russian-speaking regions and targets entities mainly in the US and Europe. Dark Angels formulated their attack strategy in 2022 and is known as a "big game hunter", because of their history of targeting technically sophisticated and large organizations.[6] They are unique in their approach as they specialize in executing highly targeted and curated attacks.

Dark Angels not only encrypt the victim's data but also exfiltrate sensitive information before starting the encryption process. The group uses this stolen data as leverage, threatening to sell it publicly if the ransom is denied. Dark Angels operates a discreet site named DungHill for listing their data leaks online for sale should an entity refuse to pay.[7] Such an approach has grave consequences for public safety especially if the victim

---

[2] Executive Order 13636 and Presidential Policy Directive 21. *CISA*.

[3] Federal Register (2024). Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements. *The Daily Journal of the United States Government*, April 4.

[4] Winder, Davey (2024). Record-Breaking $75 Million Ransom Paid to Dark Angels Gang. *Forbes*, July 31.

[5] ThreatLabz 2024_Ransomware Report. *Zscaler ThreatLabz*, July 2024, 20.

[6] Barnett, Patrick (2024). Industry News 2024 DarkAngels Strikes Big Record-Breaking Ransom Secured. ISACA, October 10.

[7] An In-Depth Look at DarkAngels Ransomware. *Avertium*, August 5, 2024.

company is a covered entity under CISA's 16 critical infrastructure sectors. For example, were Dark Angels to target a hospital network and jeopardize their patient data, it could access patients' social security numbers, insurance details, addresses, birth dates and much more. Other malicious actors looking to commit identity fraud, insurance fraud, or any related crimes will be extremely interested in the purchase of such data. Therefore, not only does Dark Angels jeopardize the safety of corporations, but it also enables other criminals to commit fraudulent activities against the public. In the case of the $75 million ransom, it is rumoured that 100TB worth of data was stolen.[8]

Such an approach adds pressure on victims to comply with ransom demands. Moreover, certain high-profile takedowns in 2024 by law enforcement such as Operation Cronos[9] (LockBit) and Operation Endgame[10] (Initial Access Brokers) and the disappearance of Black Cat, following their exit scam against Change Healthcare[11] has left a market vacuum in the ransomware threat landscape. Dark Angels has emerged as one of the leading threat actors to fill that vacuum. They truly can grow into the biggest ransomware threat to US corporations. Therefore, countering them is imperative.

Some reports suggest that the victim in the $75 million payment was Cencora (formerly AmerisourceBergen Corporation), a pharmaceutical company that was ranked 10 on the 2024 Fortune 500 list.[12] Cencora did suffer a cyberattack in February 2024, not necessarily by Dark Angels. The corporation has not confirmed an attack by Dark Angels or if a payment was made to Dark Angels or any other ransomware group. Having said that, Cencora did report a security incident to the U.S. Securities and Exchange Commission (SEC) on 21 February 2024. Reports indicate that these incidents are inter-linked.[13] Therefore, Cencora could well be the victim that paid $75 million in ransom payments to Dark Angels. Whether or not Cencora is the victim in the Dark Angels ransomware attack, the threat to US critical infrastructure by Dark Angels is imminent.

3. Research Objectives

Considering the Dark Angels group is still a novel threat, crypto-intelligence and blockchain analytic firms have prioritized investigations into laundering techniques of more well-known ransomware groups. Therefore, there remains an intelligence gap regarding specific laundering techniques that Dark Angels use.

While this investigation wasn't able to pinpoint the $75 million transaction, it was able to analyze other illicit transactions by addresses attributed to Dark Angels by Crystal Intelligence. Using these addresses, this report aims to:

A) Analyze Dark Angels' patterns of money laundering. What exchanges do they tend to use? Are they using cross-bridges? Has any of their illicit income been off-ramped?

B) If so, what obfuscation methods did Dark Angels use? If not off ramped, what addresses is the crypto stored in? Are they using similar exchanges to any other actors?

4. Methodology

The bulk of the research project was conducted using the tracing tool developed by Crystal Intelligence. Crystal's tool has attributed certain addresses to Dark Angels and has recorded transactions involving these addresses. This report analyses a transaction from May 2022, tracing and mapping the flow of funds to study the laundering methods of Dark Angels in detail. The research also took assistance from open-source tracing tools such as Mempool, which were helpful in confirming transaction hashes, time stamps, and relevant entities (Figure 1).

---

[8] Kuhn, Daniel (2024). Hacking Group Dark Angels Received $75 Million in Bitcoin, Marking the Largest Known Ransomware Attack to Date. *The Block*, 18 September.

[9] DOJ (2024). US And U.K. Disrupt LockBit Ransomware Variant." *Justice.gov*, February 20.

[10] Europol (2024). Largest Ever Operation against Botnets Hits Dropper Malware Ecosystem. *Europol*, 30 May.

[11] Alder, Steve (2024). Blackcat Affiliate behind Change Healthcare Ransomware Claims Group Stole $22 Million Ransom. *The HIPAA Journal*, March 5.

[12] Wright, Rob (2025). The Mystery of the $75M Ransom Payment to Dark Angels. *Search Security, TechTarget,* 16 January.

[13] Manson, Katrina (2024). Gang Got $75 Million for Cencora Hack in Largest Known Ransom. *Bloomberg*, 18 September.

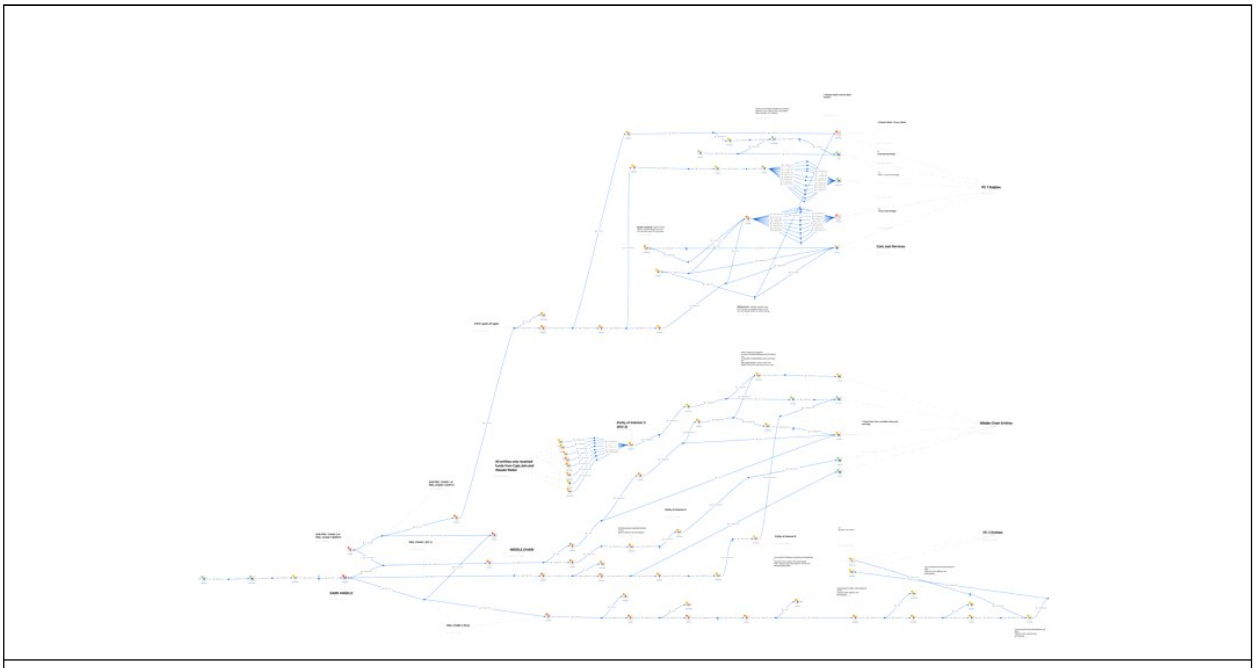

Figure 1: Tracing Chart of Dark Angels Obfuscation Techniques Produced Using Crystal Intelligence

5. Results

Our transaction of interest was completed on May 4th, 2022. The addresses associated with Dark Angels received 38.14 BTC. Upon receiving funds, Dark Angels peeled off the total amount into two primary Peel Chains (PC 1 and PC 2) and sent 31.78 BTC and 6.35 BTC respectively to each chain. Each of these peel chains continued to peel further as they broke off funds into smaller amounts. One of PC 1's subsidiary chains deposited 6.35 BTC back into the original Dark Angels address from which we started tracing the flow of funds. This original Dark Angels address proceeded to send this deposited 6.35 BTC into a new chain of addresses forming what we call the "Middle Chain." This is the third chain generated by Dark Angels and is sandwiched in between PC 1 and PC 2 (Figure 2). Having analyzed these three chains and how they interact with each other, the comprehensive and multi-faceted crypto laundering strategy of Dark Angels becomes clear.

6. Discussion

The report now follows each chain closely as each chain breaks off into subsidiary chains until we can trace the funds to illicit or licit entities.

6.1. PEEL CHAIN 1

PC 1 further breaks off into two sub chains: SC1PC1 and SC2PC1.

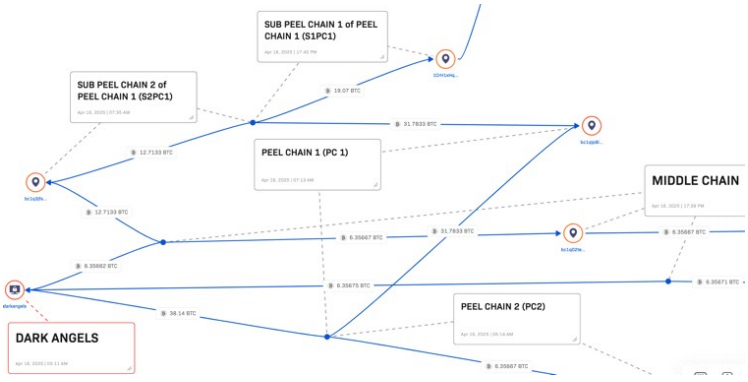

Figure 2: Initial Peeling from Main Dark Angels Address into PC 1, Middle Chain, and PC 2

6.1.1. SCPC1

The first sub chain of peel chain 1 (S1PC1) carries 19.07 BTC and passes through several address and continues peeling into smaller and smaller amounts of cryptocurrency. The funds are comingled with other addresses, seemingly legitimate, that serve as inputs in different transactions. These comingled funds go through certain BTC entities which have not been attributed but appear to be some form of conjoining services where other legitimate address have also sent funds to. Nonetheless, funds from Peel Chain 1 are traced to five different crypto entities (Figure 3). The five specific entities are: Wasabi Wallet, BTSE Licensed Exchange, MEXC Licensed Exchange, ThorChain bridge, and CoinJoin Participants coinjoin services.

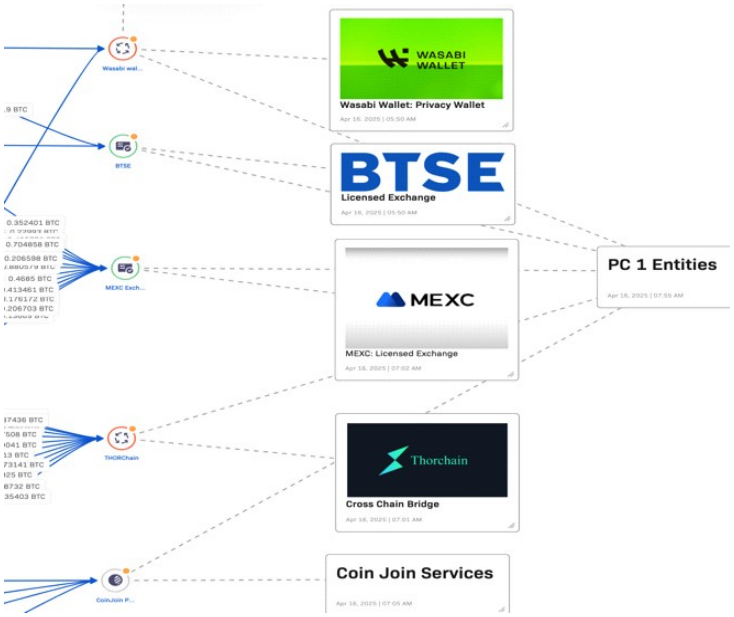

Figure 3: Endpoint Entities of Peel Chain 1

6.2. Wasabi Wallet

The Wasabi Wallet is a free and non-custodial "privacy wallet" that emphasizes privacy. The wallet's attributes such as Tor integration and BIP-158 block filtering, provide enhanced anonymity for users, making it ideal for intended obfuscation of funds.[14] Privacy wallets hold certain unique edges over other privacy strategies such as mixing services. Mixing services, at times, have proven to be unreliable as they hold significant drawbacks. A user must trust that a mixing service is not a law enforcement honeypot or that they are not malicious actors that will simply disappear with the deposited assets.[15] Since mixing services are externally handled, losing custodianship over your assets no longer remains a trust less undertaking.

Privacy wallets, such as Wasabi wallet, on the other hand are non-custodial in nature, or self-custodial, and ensure that users can maintain complete control of their assets. For such reasons, we have seen an increase in cybercriminal activity using privacy wallets. In fact, attackers responsible for the recent monumental Bybit hack, also used Wasabi Wallet for fund obfuscation.

Dark Angels' Peel Chain 1 (PC1) uses Wasabi in a complicated and cyclic manner. Not only do few of its subsidiary chains feed BTC directly into an address at Wasabi Wallet, but it also sends already mixed funds through CoinJoin Participants back into a Wasabi Wallet. Essentially, what appears to be happening is that PC 1 is making certain funds go through a "mixing cycle". Funds are deposited from PC 1 addresses into coinjoin services, only for different PC 1 addresses to receive these funds back from such coinjoin services. These different PC 1 addresses then deposit funds back into Wasabi Wallet, thus, creating a double jeopardy of funds obfuscation.

[14] S. Aaron (2025). Wasabi Wallet Review. *BitDegree*, January 24.

[15] Robinson, Dr Tom (2020). Crime Proceeds Being Laundered in Privacy Wallets. *Elliptic*, December 9.

Dark Angels' PC 1 shows complicated, nuanced, and thorough fund obfuscation strategies wherein attribution of illicit funds or their tracing from within a group of coinjoin transactions or privacy wallet addresses becomes extremely challenging. Moreover, as stated above, in some subsidiary chains, Dark Angels uses comingled funds with other seemingly legitimate transactions, that further complicates determination of illicit crypto flow.

6.3. BTSE Licensed Exchange

BTSE is an exchange that is licensed in Lithuania and Liechtenstein, both of which are considered as crypto-friendly jurisdictions.

Dark Angels' PC 1 interacts very carefully with the BTSE licensed exchange. It does not do so directly. Funds totalling 3.34 BTC, that can be directly traced back to the original Dark Angels address, are sent via subsidiary chains in PC 1 to a BTC entity (Entity of Interest 1 or EOI 1) that also received transactions from multiple other unrelated and seemingly legitimate addresses. EOI 1 is the entity that interacts with BTSE and sends almost 49 BTC to BTSE (Figure 4).

This transaction includes funds from the specific address within EOI 1 to which 3.34 BTC was sent to by PC 1. All addresses in EOI 1 are multi-signature addresses, but of a peculiar nature. Mempool data shows that these addresses are of "Multisig 1 of 2" in nature. Usually, multi-signature addresses have at least 3 registered signatures or require at least 2 signatures. It seems counterproductive to have a multi signature address when only one address is required to proceed with a transaction. Open-source research did not reveal any logical reasoning behind such a practice both for legitimate or illicit purposes. Regardless, 3.34 BTC from the original 38.14 BTC Dark Angels' funds end up at BTSE.

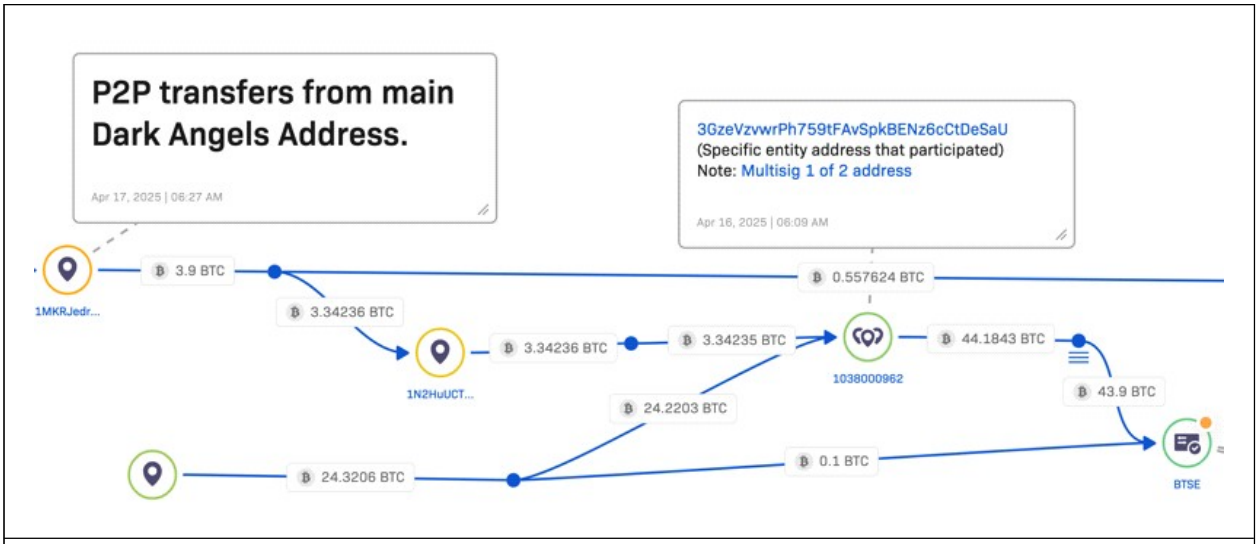

Figure 4: Funds from Dark Angels Addresses Flow through Multi-Signature BTC Entities Before Being Sent to BTSE Licensed Exchange

However, determining the specific addresses at BTSE remains complicated, given the comingling of seemingly legitimate funds by EOI 1. This report determines with low to moderate confidence that the relevant addresses at BTSE have been identified in our tracing and upon further investigation, a subpoena request into these addresses at BTSE will be appropriate. Such a request, if granted, will require BTSE to reveal their KYC information on control over these addresses. Being a centralized exchange, the custodial nature of their exchanges presents an opportunity for law enforcement to gather intelligence on associated Dark Angels addresses at BTSE.

6.4. MEXC Licensed Exchange

MEXC is a licensed exchange operating out of the Seychelles. However, it is not allowed to operate in the United States and US residents are barred from interacting with the exchange. Users circumvent such controls using private VPNs. The already suspicious nature of MEXC potentially explains why Dark Angels interacted

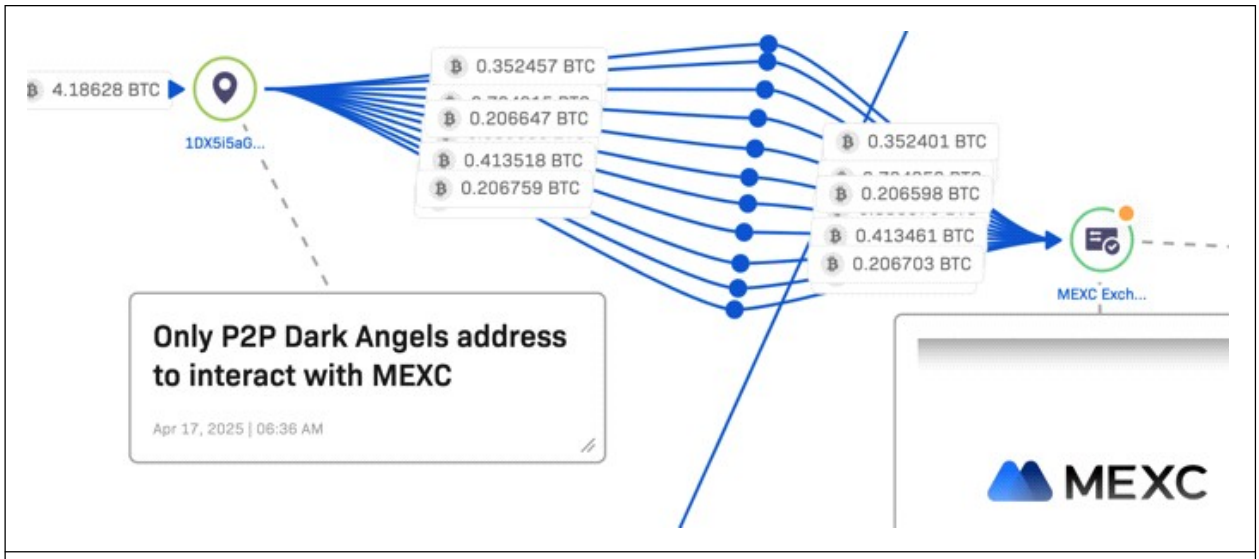

Figure 5: A Cluster of Transactions from a Singular Dark Angels Address (Attributed through Direct P2P) to Multiple Addresses in MEXC Licensed Exchanges

with it more directly than it did with BTSE exchange. In the case of MEXC, Dark Angels does not use any intermediary entities or addresses, rather its subsidiary chains directly send a cluster of funds to MEXC, albeit in very small quantities (Figure 5). Dark Angels send a cluster of funds to MEXC from one single address.

However, it uses multiple addresses to move these funds prior to sending it in a cluster of transactions to MEXC. The funds flowing through all these prior addresses can be traced directly back to Dark Angels and the transactions moving these funds follow a similar transactional pattern. All addresses only had one incoming and outgoing transaction, usually separated by a few weeks or a few months. Doing so, likely helped Dark Angels actors evade law enforcement or blockchain analysts as they look to focus elsewhere. This is evident in the low-risk scores given to these addresses, even though they have served as definitive agents in the one of the primary peel chains of Dark Angels. These addresses have only been used twice, once to receive funds directly linked to Dark Angels and once to move them.

Therefore, this report assesses with moderate to high confidence that all these addresses can be attributed to Dark Angels or at the very least are complicit entities in the group's crypto-laundering scheme.

The original transaction peeled off into PC 1 on May 4th, 2022, however, the last address, in one of the subsidiary chains, did not move its 4.18 BTC through a cluster of transactions to MEXC until September 18th and 19th of 2023. This laundering operation was a year and a half in the making. This last address uses multiple transactions to deposit low quantities of BTC, all under 1 BTC, into multiple addresses at the MEXC exchange. Given the lesser degree of separations between MEXC and Dark Angels, as opposed to with BTSE, there is more ground for a subpoena request. This report recommends law enforcement or blockchain firms to subpoena MEXC to reveal their KYC information on all addresses at the exchange that are associated with transactions originating from this address.

6.5. ThorChain Cross-Chain Bridge

ThorChain is a cross-chain bridges that allows users to swap native crypto currency between different blockchains such at the Bitcoin and Ethereum blockchains. This process has come to be called chain hopping.[16] They increase inter-chain operability but also present money laundering concerns as they are useful in the obfuscation of illicit funds. Decentralized cross-chain bridges are an unregulated alternative to exchanges for transferring of cryptocurrency in between different blockchains.[17] Such cross-chain bridges pose great challenge to anti-money laundering investigators and regulators, since there is no central service provider that facilitates

[16] Chain Hopping: The Future of Crypto Money Laundering. *Merkle Science*, July 10, 2023.
[17] Cross-Chain Crime: Over Half a Billion Dollars Laundered through a Cross-Chain Bridge. *Elliptic*, August 10, 2022.

these cross-chain transactions. Rather transactions are handled by a network of thousands of pseudonymous validators. Elliptic has reported that a single cross-bridge, RenBridge laundered $540 million.[18]

PC 1 interacts with ThorChain in a cluster like manner from a single address, much like its interactions the MEXC licensed exchange. However, the way it moves its funds to this address is slightly more complicated than the direct transactions that led to the MEXC off ramping. It moves funds to the address that interacts with ThorChain in two methods. The first method is like its methods of transactions with MEXC Licensed Exchange. Subsidiary chains of PC 1 use multiple address for just one incoming and outgoing transaction. These addresses move money, in a linear manner, after holding the funds for a few weeks or months at a time.

The second method involves the prior mixing of funds using CoinJoin participants. Coin joining transactions from CoinJoin participants sent funds to addresses that directly deposited additional funds to Dark Angels' only address that interacts through a cluster of transactions with ThorChain. One of these participating addresses lie within a BTC entity (Entity of Interest 2 or EOI 2) that only interacts with CoinJoin participants and Dark's Angels' ThorChain address (Figure 6). EOI 2 along with other addresses deposits close to 3.2 BTC to ThorChain, through one singular address.

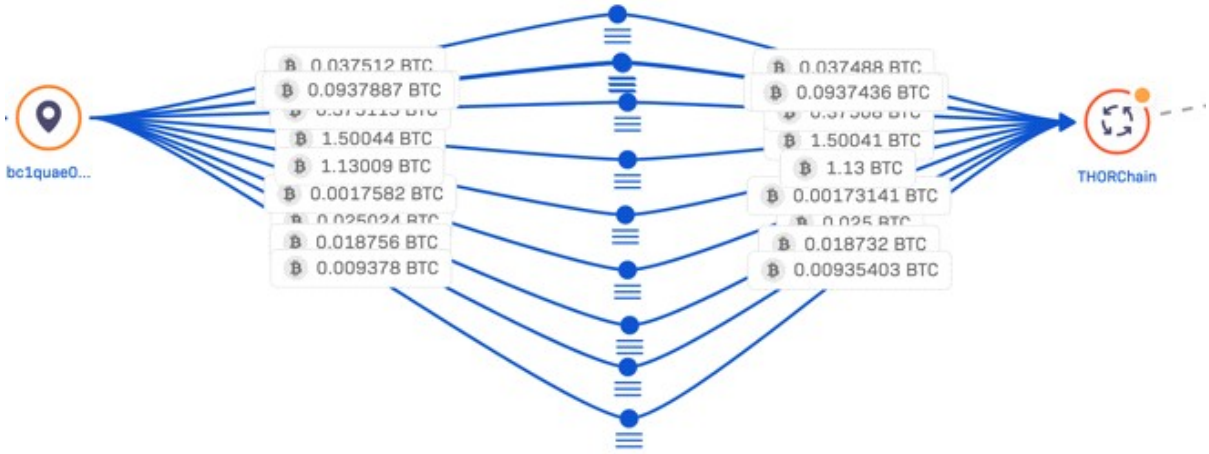

Figure 6: A Cluster of Transactions from a Singular Dark Angels Address (Attributed through Direct P2P) to ThorChain, a Cross Chain-Bridge

Given how well the funds have mixed before being sent to a cross-chain bridge, it is difficult to prove with certainty that all these entities are associated with Dark Angels. However, given they all interact closely with Dark Angels' only address that interacts with ThorChain, this report assesses with moderate confidence that these entities can be attributed to Dark Angels or at least are complicit in the crypto laundering scheme of Dark Angels.

6.6. CoinJoin Participants

CoinJoin Participants is a coinjoing service which takes input transactions from many different users and returns many output transactions of identical amounts, so that a blockchain analyst cannot easily determine which outputs belong to which of the participants.

PC 1 directly sends at least 9.6 BTC to CoinJoin Participants. It uses a similar strategy as it moves funds between addresses with single incoming and outgoing transactions separated by weeks or months. Having said that, it also deploys a "double jeopardy" approach where it receives mixed funds from CoinJoin participants only to send them for being mixed again either to CoinJoin Participants itself or to Wasabi Wallet. After double mixing, these funds feed the Dark Angels address that ThorChain exclusively interacts with. Thus, Dark Angels is mixing the same funds repeatedly only to move them to another chain using a bridge service, primarily ThorChain.

[18] Cross-Chain Crime: Over Half a Billion Dollars Laundered through a Cross-Chain Bridge. *Elliptic*, August 10, 2022.

6.6.1. SC2PC1

Sub peel chain 2 of PC 1 receives 12.71 BTC from the original 38.14 BTC. These funds are then divided almost equally into two separate transactions of 6.35 BTC each. The first transaction (T1) deposits these funds back into the original Dark Angels address from where these funds originated. The second transaction (T2) moves the remaining 6.35 BTC into addresses that keep peeling the funds off into addresses with lower and lower values of BTC. Once the primary Dark Angels address received funds from T1, it transferred all the funds into another address (Figure 7). This new address started peeling the funds just like the address that received funds from T2. Both transactions, T1 and T2 combine to produce the two subsidiary chains of the "Middle Chain" or MC. These two subsidiary chains interact close and hence have been grouped together, under the Middle Chain, to represent consistent laundering techniques used by Dark Angels in these two subsidiary peeled chains.

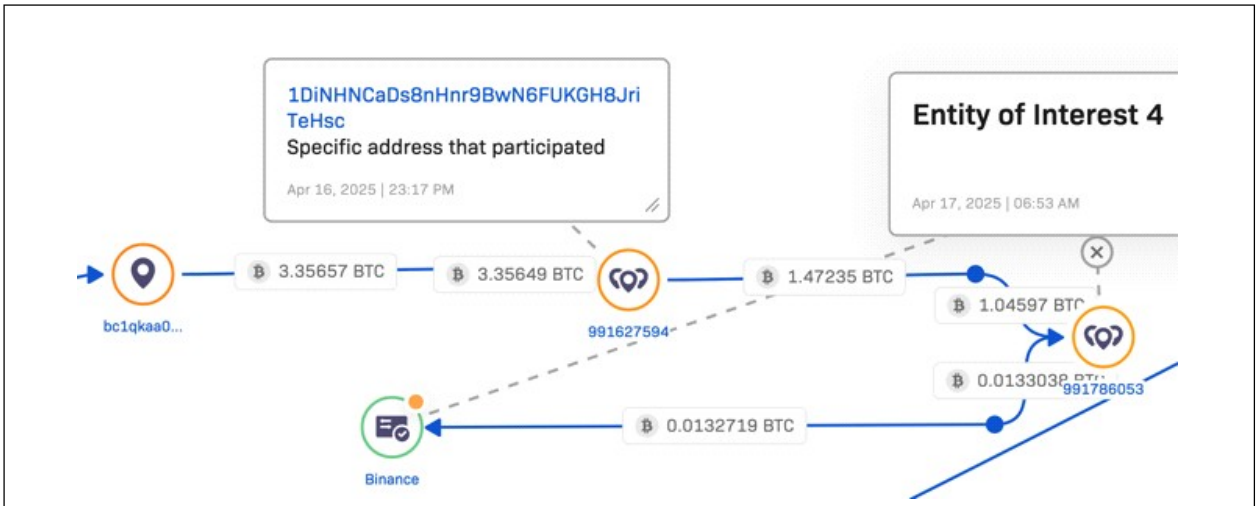

Figure 7: P2P Transactions End in Multi-Address Entities Before Sending Funds to Binance Centralized Exchange

6.7. Middle Chain

T1 and T2 form the middle chain as they both start the chain with a flow of almost equal funds, equalling 6.35 BTC each. These two subsidiary chains initially follow the same pattern of peeling wherein their BTC values are almost divided equally and peeled into two different addresses. This practice is repeated multiple times, approximately halving the BTC value with each transactional node. The Middle Chain, through its subsidiaries interacts with six different attributed entities. These include: Any Cash unlicensed exchange, HTX licensed exchange, FixedFloat unlicensed exchange, Binance licensed exchange, Kuna.io licensed exchange, and lastly privacy services in Wasabi Wallet and CoinJoin Participants.

The flow of crypto through Dark Angels addresses to these entities reveals two broad strategies that Dark Angels deploys in its middle chain for fund obfuscation: direct transfers and the use of intermediaries. We observed both strategies in Dark Angels' PC 1 as well, however, their intended use becomes clearer in the Middle Chain. The flow of funds directly flows from Dark Angels' addresses to these entities only if they are unlicensed exchanges. On the other hand, the funds consistently go through intermediary entities, before ending up in a licensed exchange.

Direct Deposits: In the case of Any Cash, the flow of funds can be traced through peer-to-peer transactions, with single addresses leading back to the primary Dark Angels address that split into PC 1 and PC 2. It also receives funds from our labelled entity of interest (EOI 3). More discussion about EOI 3 to follow under the section on the second strategy deployed by Dark Angels in the middle chain. Much like Any Cash, FixedFloat also receives funds directly from Dark Angels addresses. The obfuscation strategies differ from those in S1PC1 temporally. The timeline of the middle chain for these direct deposits to unlicensed exchanges is much quicker than the timeline of Peel Chain 1's cluster transactions into licensed exchanges. While the PC 1 operation ended in September 2023 and took a year and a half to fully launder funds, the middle chain directly deposits

BTC into Any Cash and FixedFloat unlicensed exchanges, on May 12th and May 14th respectively, only 10 days after the initial payment to Dark Angels' primary address.

This reveals that depending on whether they are using a licensed or unlicensed exchange, Dark Angels work on different timelines. They "wait and sit" on funds, destined to end at licensed exchanges, to evade early detection and hope that law enforcement has other critical matters at hand.

Use of Intermediaries: Three entities of interest EOI 3, EOI 4, and EOI 5 are used as intermediaries and prevents Dark Angels from directly interacting with the licensed exchanges of HTX, Binance, and Kuna.io (Figure 8).

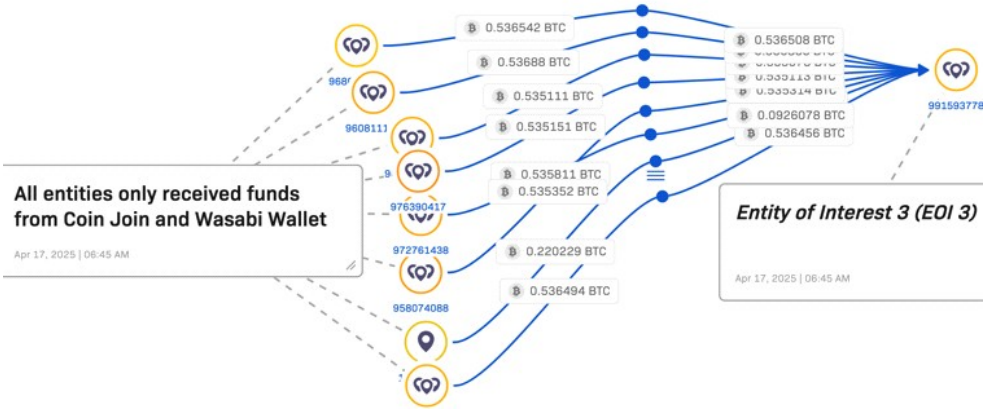

Figure 8: A Cluster of Entities Receive Funds from Wasabi Wallet and CoinJoin Participants and Exclusively Send them to EOI 3. EOI 3 Later Sends these Funds to Any Cash Unlicensed Exchange and HTX Licensed Exchange

Since these are largely complaint centralized exchanges, were Dark Angels to directly deposit funds to these exchanges, investigators can trace the funds easily and request a subpoena on the associated addresses. However, EOI 3, EOI 4, and EOI 5 all make attribution of illicit funds flow just complicated and uncertain enough for this report to only assess with low to moderate confidence that these funds have been rightfully traced all the way through to these exchanges. All the entities share upwards of 15-20 addresses each and have a complex web of transactions before finally sending funds to centralized exchanges.

Therefore, this report assesses with low confidence that these specific addresses can be attributed to Dark Angels or at least are complicit in their crypto launderings scheme. The last important caveat about the middle chain is the most fascinating. One of the subsidiary chains that flows into Any Cash unlicensed exchange and HTX licensed exchange, contains our Entity of Interest 3 (EOI 3). EOI 3 receives funds in a cluster of transaction from multiple entities. All these entities that send EOI 3 funds only received funds from CoinJoin Participants and Wasabi Wallet.

Considering the heavy reliance on CoinJoin Participants and Wasabi Wallet in PC 1, it is probable that these middle chain entities received the remaining mixed funds from PC 1, once they had been mixed by CoinJoin Participants and Wasabi Wallet. The time stamps on the transactions in both chains also align to support such a hypothesis. However, it remains difficult to provide a deterministic answer. Hence, this report assesses with moderate confidence that these entities in the Middle Chain are receiving the mixed funds from PC 1 after passing through Wasabi Wallet and CoinJoin Participants.

6.8. PEEL CHAIN 2

Peel Chain 2 or PC 2 starts with receiving 6.35 BTC from the primary Dark Angels address. The funds travel through single use accounts quickly however, small amounts keep deducting from the over 6BTC funds. These small amounts are consistently sent to BTC entities where small amounts are comingled with larger seemingly legitimate transactions. These subsidiary chains are unusually long with very low BTC values. The report decided to focus on the larger values of BTC and tracing their flow.

Furthermore, the small amounts when mixed into transactions with multiple folds more BTC make it harder to trace these subsidiary chains. After the initial instantaneous transfers through multiple accounts, PC 2 soon starts to mirror PC 1 with addresses only being used twice, at intervals of weeks or months between the incoming and outgoing transactions. Furthermore, the report did have success tracing these funds through P2P transactions to Blitzlato, a Hong-Kong based crypto currency exchange that was taken legal action against in early 2023. This seems to follow the general trend of cybercriminals preferring to use non-compliant exchanges based in South-East Asia.

The remaining funds end up in Entity of Interest 6, EOI 6, that can be seen as another multi-address entity. Here, the funds are mixed with very large seemingly legitimate transaction amounts, thus impeding our abilities to track our smaller quantities of funds further (Figure 9). These addresses, after back tracing, reveal associations with other cybercriminal groups or crypto scams. Therefore, it is probable that such entities serve as a hub for multiple ransomware actors to merge their criminal proceeds and obfuscate their flow of funds from law enforcement or blockchain investigators.

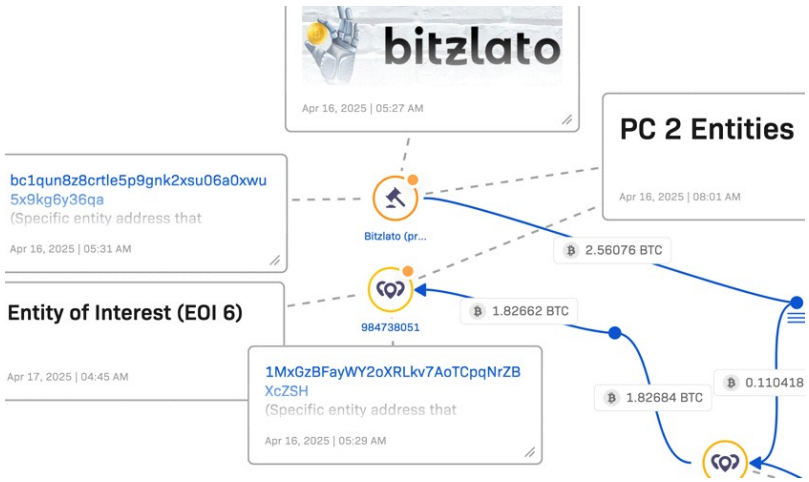

Figure 9: Tracing PC 2 Transactions Terminate at Blitzlato and EOI 6

7. Comparisons with Other Actors

If we compare this to the Change Healthcare hack that occurred in February of 2024 (Figure 10). The responsible entity, Black Cat/AlphaV seems to have exit scammed and left their co-conspirators without a share of their

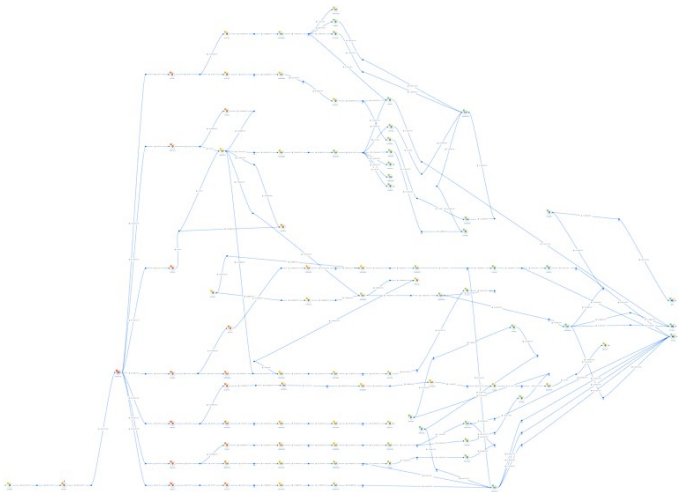

Figure 10: Traced Change Healthcare Hack for Use by Other Investigators to Conduct a Comparative Analysis with Dark Angels. Produced by Using Crystal Intelligence

spoils. An extension of this research project could be pursuing a comparative analysis between different ransomware attackers and their laundering schemes. Such an analysis will aid us in finding similarities in the tactics, techniques, and practices of Dark Angels with other threat actors to coordinate the most effective response. If certain strategies deployed by Dark Angels are similar to another threat group, we could source lessons learned from previous law enforcement.

8. Limitations

This research project is certainly not without limitations. There were many constraints in the execution of this project. The relatively small sample size is particularly problematic. Dark Angels is a relatively new threat group with only a few documented and uncontested ransomware attacks.

This project traced the transaction of interest solely using the Crystal tool and it was not uncommon to run into roadblocks with certain addresses, therefore making definitive attribution unlikely. Perhaps using multiple commercial tools could help improve the accuracy of attribution and provide more attributed transactions to Dark Angels.

9. Conclusion

Even though the study has added great insights into the laundering techniques used by Dark Angels, the report views its greatest contribution as highlighting the glaring gap in open-source intelligence available for researchers. To find an answer, we must turn our attention to the emergence of a new crypto market.

We have observed the emergence of a bustling licit economy that is driven by such ransomware attacks. Incident Response firms are at the centre of this new market. The global incident response market size stood at $25.67 billion in 2023. It is expected to grow at a Compound Annual Growth Rate (CAGR) of 19.9% from 2024 to 2030.[19]

The year 2024, the very first year of such projections, has already exceeded the projected CAGR of 19.9% with the estimated market size standing at $29.46 billion at the end of 2024.[20] Although these firms provide incident response expertise, they are incentivized to not publicize ransomware attacks to limit reputational loss for their clients. Their priority is and will always remain dollar paying customers and not public security. Moreover, with a growing market size, we have seen a tremendous growth in the number of incident response firms, thus making the market immensely competitive with more limited chances of collaboration between different competing firms.

Consequently, incident response firms are further de-incentivized from public disclosure to prevent giving their competitors an edge. Public disclosures will aid competing firms by providing them with case studies. Therefore, incident response firms are de-incentivized both because of their clients and rival competition from reporting attacks or disclosing payments. Thus, leaving law enforcement and the public in the dark.

As an industry, we must look to fix this. We should not aim to crush the incident response industry but look to find ways to allow public sharing of information to deepen collective security. Anonymous databases can be generated that include accounts of ransomware attacks, crypto addresses, exchanges used, cross-bridges utilized, and other information that can promote a public-private partnership in countering ransomware.

References

Aaron, S (2025). Wasabi Wallet Review. *BitDegree,* January 24. www.bitdegree.org/crypto/wasabi-wallet-review

Alder, Steve (2024). Blackcat Affiliate behind Change Healthcare Ransomware Claims Group Stole $22 Million Ransom. *The HIPAA Journal,* March 5. www.hipaajournal.com/blackcat-ransomware-affiliate-change-healthcare-scammed/

[19] Incident Response Market Size, Share & Growth Report 2030. *Grandviewresearch,* 2023.

[20] TRM (2024). Category Deep-Dive: Ransomware Demands Reached an All-Time High in 2024 | TRM Insights. *TRM Labs.*

Artis, Zelmenis (2025). Lithuania Company with Cryptocurrency License: Baltic Legal Incorporation. *Baltic Legal*. www.baltic-legal.com/lithuania-company-registration-cryptocurrency-licence-bank-account-eng.htm

Avertium (2024). An In-Depth Look at DarkAngels Ransomware. *Avertium*, August 5. www.avertium.com/resources/threat-reports/an-in-depth-look-at-darkangels-ransomware

Barnett, Patrick (2024). Industry News 2024 DarkAngels Strikes Big Record-Breaking Ransom Secured. *ISACA*, October 10. www.isaca.org/resources/news-and-trends/industry-news/2024/darkangels-strikes-big-record-breaking-ransom-secured#7

CISA (2013). Executive Order 13636 and Presidential Policy Directive 21 | CISA. *CISA.GOV*. www.cisa.gov/executive-order-13636-and-presidential-policy-directive-21

Chainalysis (2025). 35% Year-Over-Year Decrease in Ransomware Payments, Less than Half of Recorded Incidents Resulted in Victim Payments. *Chainalysis*, February 5. https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/

Chain Hopping (2023). The Future of Crypto Money Laundering. *Merkle Science*, July 10. www.merklescience.com/blog/chain-hopping-the-future-of-crypto-money-laundering

DOJ (2024). US and UK Disrupt LockBit Ransomware Variant. *Justice.gov,* February 20. www.justice.gov/archives/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant

Europol (2024). Largest Ever Operation against Botnets Hits Dropper Malware Ecosystem. *Europol*, 30 May. www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-dropper-malware-ecosystem

Federal Register (2024). Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements. *The Daily Journal of the United States Government*, 4 April. www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements

Kuhn, Daniel (2024). Hacking Group Dark Angels Received $75 Million in Bitcoin, Marking the Largest Known Ransomware Attack to Date. *The Block*, 18 September. www.theblock.co/post/317100/hacking-group-dark-angels-received-75-million-in-bitcoin-marking-the-largest-known-ransomware-attack-to-date

Manson, Katrina (2024). Gang Got $75 Million for Cencora Hack in Largest Known Ransom. *Bloomberg*, 18 September. www.bloomberg.com/news/articles/2024-09-18/gang-got-75-million-for-cencora-hack-in-largest-known-ransom

Robinson, Dr. Tom (2020). Crime Proceeds Being Laundered in Privacy Wallets. *Elliptic*, December 9. www.elliptic.co/blog/13-bitcoin-crime-laundered-through-privacy-wallet

ThreatLabz (2024). Ransomware Report.

ThreatLabz (2024). Dark Angels Exposed | ThreatLabz. *Zscaler*, 8 October. www.zscaler.com/blogs/security-research/shining-light-dark-angels-ransomware-group

TRM (2024). Category Deep-Dive: Ransomware Demands Reached an All-Time High in 2024 | TRM Insights. *TRM Labs*. www.trmlabs.com/resources/blog/category-deep-dive-ransomware-demands-reached-an-all-time-high-in-2024

Winder, Davey (2024). Record-Breaking $75 Million Ransom Paid to Dark Angels Gang. *Forbes*, 31 July. www.forbes.com/sites/daveywinder/2024/07/31/record-breaking-75-million-ransom-paid-to-dark-angels-gang/

Wright, Rob (2025). The Mystery of the $75M Ransom Payment to Dark Angels. *Search Security, TechTarget,* 16 January. www.techtarget.com/searchsecurity/feature/The-mystery-of-the-75M-ransom-payment-to-Dark-Angels

Cite this article as: Shayiq Ahmed Shah (2025). Dark Angels and the Largest Crypto Ransom Payment in History: Addressing Key Intelligence Gaps with Dark Angels. *International Journal of Cryptocurrency Research,* 5(2), 13-26. doi: 10.51483/IJCCR.5.2.2025.13-26.