

The Bitcoin Ransomware Detective Strikes Again: The UCSF Case

By Tal Be'ery

Published: 2020-09-03 · Archived: 2026-04-06 00:51:19 UTC

TL;DR: Hunting for real-world incidents in blockchain data sometimes leads to interesting insights and findings. In this case, we were able to find UCSF's \$1.14M ransom payment on the blockchain and correlate it to an additional \$700K transaction. This potentially increases the paid UCSF ransom to over \$1.8M.

Following our [recent article on the \\$4M Bitcoin CWT ransomware payment](#), we continued to hone our blockchain hunting skills. Usually, these skills are used to protect Zengo customers.

This time, however, we had a different focus. We managed to track down the \$1.14M ransom paid by the University of California San Francisco (UCSF).

You might remember this case.

It gained widespread exposure because ransom negotiations between UCSF's negotiator and hackers were made public and covered by popular media outlets like [BBC](#) and [Bloomberg](#).

In this article, we'll share our findings and some additional insights we were able to infer from the [Bitcoin](#) blockchain data. We'll also describe our methods so other security researchers can explore similar incidents in the future and possibly create a safer environment for all of us.

How to find a ransomware transaction

According to the [threatpost](#), UCSF paid a \$1.14 million ransom to recover data related to academic work. This data was encrypted after the [NetWalker ransomware](#) hit the medical school at the university.

Unlike the CWT case linked to above, public reports on UCSF ransomware did not include the attackers' Bitcoin address, supposedly preventing researchers from analyzing the money trail. This made our investigations a little more cumbersome. However, we did not give in.

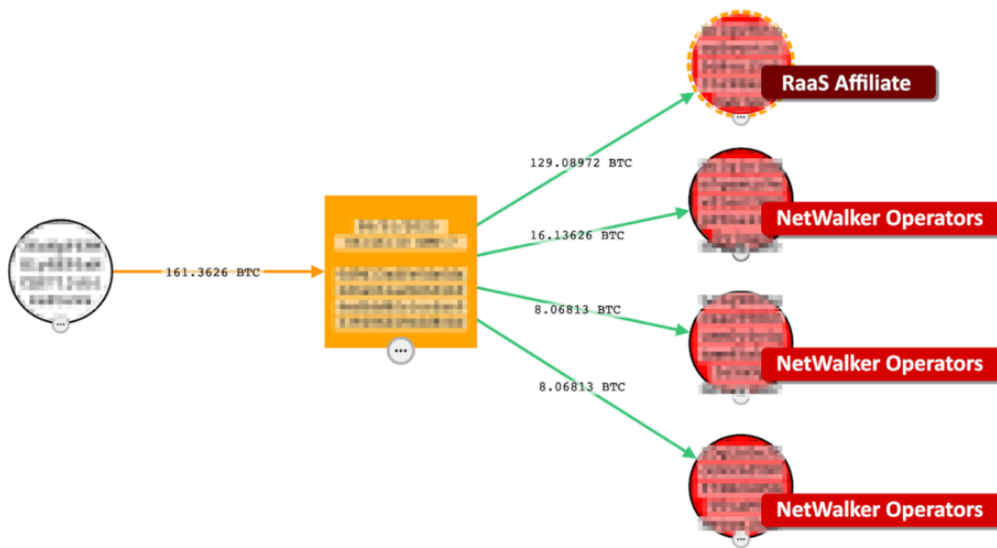
As we should all know by now, Bitcoin data is pseudonymous, not anonymous. Users are represented by mostly meaningless addresses, however all transactions between these addresses can be watched by anyone. With this in mind, we knew it would be possible to find the address if we could obtain enough information on the transaction details and money trail "pattern" (more on that below).

Diving into the media stories, we found two technical details that assisted in our investigation. The paid ransom sum was 116.4 BTC (\$1.14M at the time), and the payment took place on the 12th of June.

While sending such a large and specific amount of money in a particular time period may seem like enough to identify the transaction, we wanted to be sure. To have an even higher level of certainty, we required the transaction to be part of the following blockchain "pattern".

Ransomware payments usually follow a distinct pattern:

1. Negotiators buy the **exact** amount of Bitcoin requested by attackers, from a large liquidity provider. The negotiators use a “fresh” address, with no previous history to prevent any data leakage, for this transaction.
2. Negotiators then **immediately** transfer this **full amount** to the attackers’ fresh address. The transfer is done rapidly as negotiators don’t want to keep so much money in their possession for a long time. (Sometimes, negotiators will send a small transaction first to make sure they have the right address and then send the full amount.)
3. Once the payout lands in the attackers’ initial address, the attackers split the loot. In the case of the NetWalker ransomware, this split is very distinct. The NetWalker gang worked in a “Ransomware-as-a-service” (RaaS) model. The gang operates the infrastructure, while the affiliate drives the operation and infects the victim. Thanks to [ciphertrace](#) research, we know that this model creates a “four arms” pattern, depicted below. The NetWalker gang operators get 20% of the loot, split into 10%, 5%, and 5% payments to known addresses. The remaining 80% goes to the RaaS affiliate.



Source: CipherTrace Cryptocurrency Intelligence

NetWalker’s “four arms” Bitcoin payment pattern (source: [ciphertrace](#))

Finding the transaction

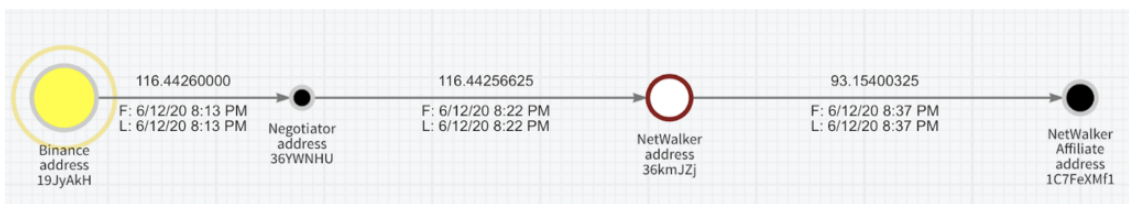
Using [BlockChair](#)’s interface, we could query the Bitcoin blockchain for transactions on the date and the reported sum. We provided a slightly bigger range for both dates and sums to allow some flexibility in case the details in the story were not exact. We created a query to retrieve transactions where the sum is between 116 and 117 Bitcoin, and the date is between the 12th and 13th of June:

[https://blockchair.com/bitcoin/outputs?s=spending_time\(desc\)&q=value\(11600000000..11700000000\),spending_time\(2020-06-12..2020-06-13\)#](https://blockchair.com/bitcoin/outputs?s=spending_time(desc)&q=value(11600000000..11700000000),spending_time(2020-06-12..2020-06-13)#)

	Value (BTC) ▼	Value (USD)	Recipient	S?	Spending tx hash	#	Times ▼	Spending value	Coindays
20:49	116.00979958	1,079,120.00	1Kr6QSydW9bFQG1mXiPNu6WpJGmUs91lg	YES	9c8b3c	0	2020-06-12 21:13	1,079,120.00	
20:45	116.61073030	1,084,710.00	bc1q3fn00jykvhnfsz2q2rh5z20exk4tvdzvnus40e2lasntsws46cg3h	YES	ec69	0	2020-06-12 21:13	1,084,710.00	
20:22	116.44256625	1,083,150.00	36kmJZjqcLdJ77KWUeFFCGm8Cys4rHuHej	YES	cb6e	0	2020-06-12 20:37	1,083,150.00	
20:13	116.44260000	1,083,150.00	36YWNHUPJZ48dshHcQsY6nHucVRezpRd6y	YES	4c	0	2020-06-12 20:22	1,083,150.00	
15:41	116.79857818	1,086,460.00	3QB7864heEKDdpX9yTc3Qf6drkHmarT4XG	YES	ae51	0	2020-06-12 20:13	1,086,460.00	
11:42	116.11950714	1,080,140.00	1LpDxrCGtbb85s53es28p3nkFPLcvb7Pa5	YES	4d16	0	2020-06-12 11:42	1,080,140.00	

Blockchair [query](#) results

Results returned six possible candidates, but it was easy to identify the relevant ransom transaction, as it followed our assumptions detailed above.



The ransom money trail: Binance → Negotiator → NetWalker → NetWalker Affiliate (all times UTC)

As we had expected, we found the Negotiators (address [36YWNH](#), shortened for readability) buying 116.4 BTC from [Binance exchange](#) (address [19JyAkHKh](#), associated with Binance according to [Clank](#)) into a fresh address on the 12th of June at 20:13 (All times UTC), then paying immediately to a fresh NetWalker address (address [36kmJZj](#)).

Transactions involving address		USD	BTC
Hash: 4f0336a499643ef203cd882144f72604adf93d7ccb08248a6528a8adbad390c	2020-06-12 20:22		11559 confirmations
Senders	Recipients		
← 116.44260000 BTC	36YWNHUPJZ48dshHcQsY6nHucVRezpRd6y	→	36kmJZjqcLdJ77KWUeFFCGm8Cys4rHuHej
			116.44256625 BTC
Hash: 614ae0a877f0ccaf601ca0a4df538191153b93e1f2645928ba8a25ff72dd65b	2020-06-12 20:13		11560 confirmations
Senders	Recipients		
← 647.85613234 BTC	19JyAkHKh36sFduqK4hMsMZhU6ZDoLotW	→	36YWNHUPJZ48dshHcQsY6nHucVRezpRd6y
			116.44260000 BTC
			19JyAkHKh36sFduqK4hMsMZhU6ZDoLotW
			531.41347432 BTC

Negotiators (address [36YWNH](#)) purchasing 116.4 BTC from Binance (address [19JyAkHKh](#)) then paying to NetWalker (address [36kmJZj](#))

The NetWalker address immediately split the ransom money, sending 20% to the known NetWalker address in the usual split (5%, 5%,10%) and 80% to the NetWalker affiliate (address [1C7FeXMf1](#)).

Senders		Recipients	
116.44256625 BTC	36kmJZjqcLdJ77KWUeFFCGm8Cys4rHuhej	bc1q98z5gxcan998h0uem0y4y4qtm45xk4r2e5m9p	5.82212826 BTC Unspent
		1DgLhGeJfoUkkXdyNV75NckX5ST5taPVo	5.82212826 BTC
		1C7FeXMf18mGrCF59DJTkmxRfkKeG1KFZ	93.15400325 BTC
		bc1q8r398v5v4aw0a6cah3ddd8nngq2nfr40xpg3q	11.64425753 BTC

The “four arms” payment: 80% goes to the NetWalker affiliate (address [1C7FeXMf1](#))

The additional “four arms” transaction

We discovered the ransom money trail, and verified the media story by cross-checking it with Bitcoin blockchain data.

However, we weren’t done yet.

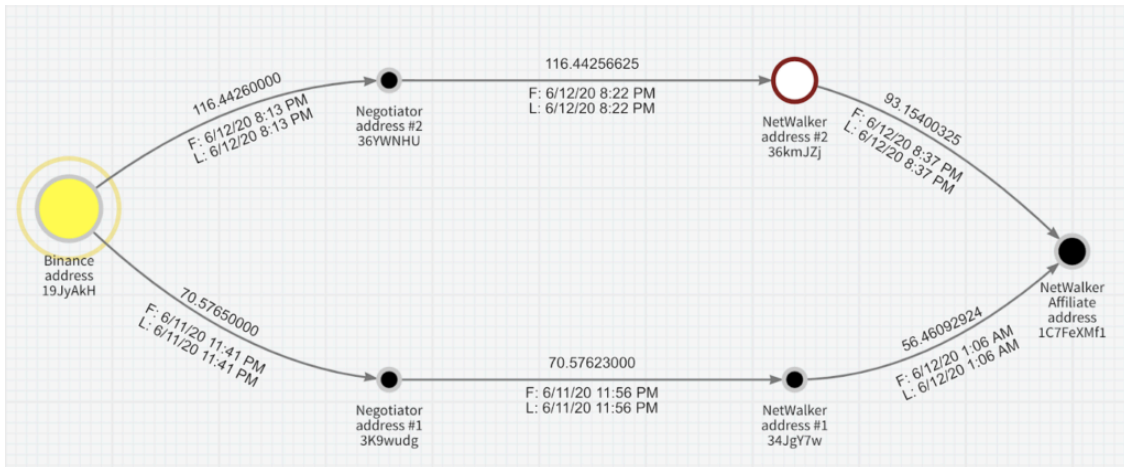
We discovered a similar “four arms” payment to the same affiliate address, made only 19 hours before the UCSF payment.

Senders		Recipients	
116.44256625 BTC	36kmJZjqcLdJ77KWUeFFCGm8Cys4rHuhej	bc1q98z5gxcan998h0uem0y4y4qtm45xk4r2e5m9p	5.82212826 BTC Unspent
		1DgLhGeJfoUkkXdyNV75NckX5ST5taPVo	5.82212826 BTC
		1C7FeXMf18mGrCF59DJTkmxRfkKeG1KFZ	93.15400325 BTC
		bc1q8r398v5v4aw0a6cah3ddd8nngq2nfr40xpg3q	11.64425753 BTC

Senders		Recipients	
70.57623000 BTC	34JgY7wwfEJgYeoTKcDb47zFWSA4Td4iyb	bc1q98z5gxcan998h0uem0y4y4qtm45xk4r2e5m9p	3.52881145 BTC Unspent
		bc1q8r398v5v4aw0a6cah3ddd8nngq2nfr40xpg3q	7.05762390 BTC
		1C7FeXMf18mGrCF59DJTkmxRfkKeG1KFZ	56.46092924 BTC
		1DgLhGeJfoUkkXdyNV75NckX5ST5taPVo	3.52881145 BTC

The two payments to the NetWalker affiliate, with only 19 hours between them (source: [blockchair](#))

Oddly enough, the money trail followed a similar path from the same Binance address to the same NetWalker affiliate. The Negotiators bought 70.5 BTC (about \$700K) from the **same** provider (Binance, address [19JyAkHKh](#)) and put it into a fresh address on the 11th of June at 23:41. They then transferred it immediately to a fresh NetWalker address, that was split to the **same** NetWalker affiliate (address [1C7FeXMf1](#)).



The two ransom paths: On the top side the known UCSF payment (addresses denoted as #2), on the bottom side the unknown payment (addresses denoted as #1)

This extra payment to the same attacker could be related to the UCSF incident or another unrelated ransomware incident. However, after talking to ransom negotiation experts, the former option is much more likely. This **puts the total ransom paid by UCSF to the attackers closer to \$2M** (187 BTC, or \$187K at the time).

According to these experts, in many cases, payments are not paid at once but tranced in return for certain “milestones” to build rapport between parties—for example, one payment to delete exfiltrated information or get more information on the penetration method used by attackers and a second to receive a decryption key.

Having the same liquidity provider (Binance), the same negotiator wallet “technology” (type of address and other technical optional fields) together with the payment to the same affiliate, which was conducted only 19 hours before the UCSF payment provides a strong, albeit circumstantial, support to this theory too. .

Additionally, the alternative explanation, that connects the first payment to another unrelated ransomware incident by the same NetWalker affiliate happening in parallel is unlikely. These two ransom transactions are the **only** NetWalker “four arms” transactions for this NetWalker affiliate. It doesn’t seem likely this NetWalker affiliate would have conducted two independent ransomware campaigns in parallel with the same address, and then completely disappeared.

Summing up

“Big game hunting” ransomware incidents [targeting large enterprises](#) are all over the financial news. However, in many cases, the details are often left in the shadows, as both attackers and victims want to keep the incidents from public view. Using Bitcoin blockchain research can help fill this information gap and reveal vital information on ransomware incidents.

At Zengo, our customers’ security is our top priority. That’s why we try to learn from every crypto-related security incident. In our experience, we’ve found that observing incidents is always useful and often leads to some interesting insights. We believe understanding this incident may increase the awareness of law enforcement and help them detect and stop such underworld payments in the future.

Source: <https://zengo.com/bitcoin-ransomware-detective-ucsf/>