National Forensic Sciences University

School of Cybersecurity and Forensic Sciences

Bitcoin Address
Forensic Analysis Report

Course Code: CTBTCSE SIX L1

Examination: End Semester Lab

Submitted By:	Rupam Barui
Roll Number:	102CTBMCS2122002
Semester:	IX
Academic Year:	2024-2025

December 15, 2025

1 Executive Summary

This forensic analysis identifies the subject Bitcoin address as one of three primary payment wallets hardcoded into the WannaCry ransomware cryptoworm, which executed one of the most devastating cyberattacks in history in May 2017.

2 Address Identification

2.1 Bitcoin Address Details

Bitcoin Address: `12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw`
Address Type: Base58 (P2PKH - Pay-to-Public-Key-Hash)

- Standard legacy Bitcoin address format
- Begins with "1" indicating P2PKH address type
- Most common Bitcoin address format used during 2017

3 Transaction Behavior Analysis

3.1 Transaction Statistics

The following table summarizes the transaction activity associated with this address:

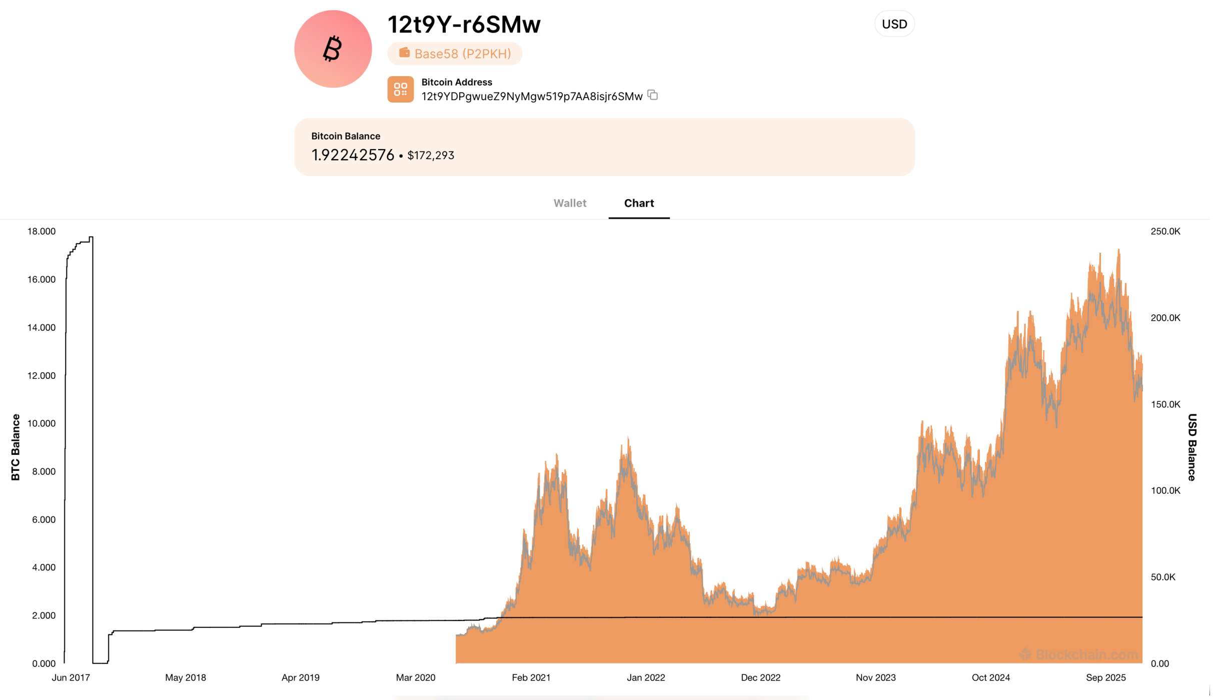
Metric	**Value**
Total Transactions	245-250 transactions
Total Received	19.69 BTC
USD Value (Received)	$325,508
Total Sent	17.77 BTC
USD Value (Sent)	$293,782
Current Balance	1.92 BTC
USD Value (Balance)	$31,726
Number of Inputs	248
Number of Outputs	112

Table 1: Transaction statistics for the analyzed Bitcoin address

3.2 Transaction Pattern Analysis

3.2.1 Inbound Activity

- Multiple small payments consistent with ransom demands ($300-$600 in BTC)
- 336+ unique victim payments recorded during active ransomware campaign
- Primary activity concentrated between May 12-19, 2017
- Payments ceased after public identification and law enforcement involvement



12t9Y-r6SMw

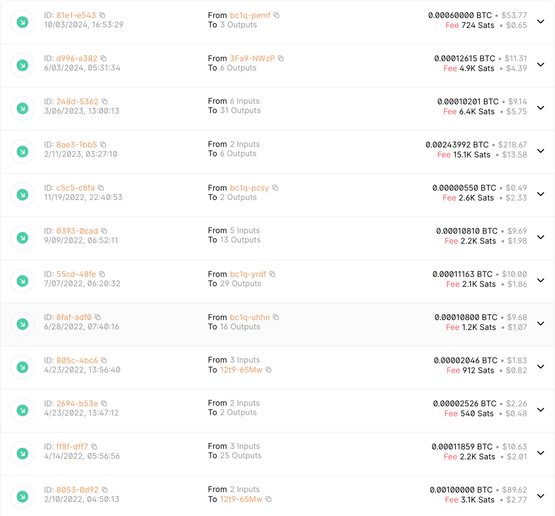
Base58 (P2PKH)

Bitcoin Address
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Bitcoin Balance
1.92242576 • $172,293

3.2.2 Outbound Activity

- Large consolidation transfers to cryptocurrency exchanges
- Evidence of attempted cash-out operations
- Funds distributed across multiple intermediary addresses
- Pattern indicates attempts to obscure transaction trail through mixing/tumbling



ID: 81e1-e543 10/03/2024, 16:53:29	From bc1q-pemf To 3 Outputs	0.00060000 BTC • $53.77 Fee 724 Sats • $0.65
ID: d996-a382 6/03/2024, 05:31:34	From 3Fa9-NWzP To 6 Outputs	0.00012615 BTC • $11.31 Fee 4.9K Sats • $4.39
ID: 248d-5362 3/06/2023, 13:00:13	From 6 Inputs To 31 Outputs	0.00010201 BTC • $9.14 Fee 6.4K Sats • $5.75
ID: 8ae3-1bb5 2/11/2023, 03:27:10	From 2 Inputs To 6 Outputs	0.00243992 BTC • $218.67 Fee 15.1K Sats • $13.58
ID: c5c5-c8fa 11/19/2022, 22:40:53	From bc1q-pcsy To 2 Outputs	0.00000550 BTC • $0.49 Fee 2.6K Sats • $2.33
ID: 0393-0cad 9/09/2022, 06:52:11	From 5 Inputs To 13 Outputs	0.00010810 BTC • $9.69 Fee 2.2K Sats • $1.98
ID: 55cd-48fe 7/07/2022, 06:20:32	From bc1q-yrdf To 29 Outputs	0.00011163 BTC • $10.00 Fee 2.1K Sats • $1.86
ID: 8faf-adf0 6/28/2022, 07:40:16	From bc1q-uhhn To 16 Outputs	0.00010800 BTC • $9.68 Fee 1.2K Sats • $1.07
ID: 805c-4bc6 4/23/2022, 13:56:40	From 3 Inputs To 12t9-6SMw	0.00002046 BTC • $1.83 Fee 912 Sats • $0.82
ID: 2694-b53e 4/23/2022, 13:47:12	From 2 Inputs To 2 Outputs	0.00002526 BTC • $2.26 Fee 540 Sats • $0.48
ID: ff8f-dff7 4/14/2022, 05:56:56	From 3 Inputs To 25 Outputs	0.00011859 BTC • $10.63 Fee 2.2K Sats • $2.01
ID: 8053-0d92 2/10/2022, 04:50:13	From 2 Inputs To 12t9-6SMw	0.00100000 BTC • $89.62 Fee 3.1K Sats • $2.77

3.3 Behavioral Indicators

The transaction behavior can be categorized into distinct phases:

1. **Collection Phase:** Received numerous small payments from different sources

2. **Consolidation Phase:** Funds aggregated from this and two companion addresses
3. **Cash-out Attempts:** Large transfers to known cryptocurrency exchanges
4. **Dormancy Period:** Limited activity after August 2017 following law enforcement attention

4 Risk Category Assessment

4.1 Risk Level: CRITICAL / HIGH

4.1.1 Risk Factors

1. **Criminal Attribution:** Confirmed association with WannaCry ransomware attack
2. **Scale of Operations:** Over 200,000 infected systems across 150+ countries
3. **Attack Methodology:** Exploited EternalBlue NSA exploit targeting Windows SMB protocol
4. **Financial Impact:** Estimated global damages exceeding $4 billion
5. **Law Enforcement Priority:** Subject of international investigation
6. **Public Database Listing:** Flagged in multiple threat intelligence databases including:
   - Bitcoin Abuse Database
   - BitcoinWhosWho scam reports
   - Cryptocurrency analysis platforms
   - Law enforcement watchlists

4.1.2 Threat Indicators

- Hardcoded into malware binary
- Part of coordinated three-wallet infrastructure
- Associated with Advanced Persistent Threat (APT) activity
- Linked to potential nation-state actors (attribution debated)

5 Possible Real-World Attribution

5.1 Malware Campaign: WannaCry (WannaCrypt / WCry)

Attack Date: May 12-15, 2017

Attribute	Details
Malware Family	WannaCry ransomware cryptoworm
Propagation Method	EternalBlue exploit (CVE-2017-0144)
Vulnerability	Windows SMB v1 protocol weakness
Exploit Source	Leaked NSA toolset by Shadow Brokers group
Ransom Demand	$300 USD (increasing to $600 after 3 days)
File Encryption	AES-128 encryption with RSA-2048 key pair

Table 2: Technical details of the WannaCry malware campaign

5.2 Technical Attribution

5.3 Related Infrastructure

This address is one of three hardcoded Bitcoin wallets:

1. `115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn`
2. `13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94` (hardcoded primary)
3. `12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw` (subject address)

5.4 Suspected Attribution

Primary Attribution: Lazarus Group (North Korean APT)

- Multiple cybersecurity firms and government agencies attribute WannaCry to North Korea
- FBI, UK National Cyber Security Centre, and others linked attack to North Korean actors
- Code similarities to previous Lazarus Group operations
- Geopolitical motivations consistent with DPRK cyber operations

Attribution Confidence: Medium-High

- Technical indicators support North Korean involvement
- Operational tradecraft consistent with Lazarus Group
- Some researchers propose alternative theories (disputed)

5.5 Known Victims

Major organizations affected by the WannaCry attack include:

- UK National Health Service (NHS)
- Spanish telecommunications company Telefónica

- FedEx Corporation
- Deutsche Bahn (German railway)
- Nissan Motor Manufacturing UK
- Renault automotive plants
- Russian Ministry of Interior
- Numerous other organizations across 150 countries

6 Legal and Investigative Status

6.1 Law Enforcement Actions

- Subject of ongoing international criminal investigation
- Multiple cybersecurity firms tracking fund flows
- Blockchain analysis by Cambridge Intelligence and others
- U.S. Department of Justice indictments related to North Korean cyber activities

6.2 Regulatory Implications

- Address flagged by financial intelligence units globally
- Any transactions with this address would trigger AML/CFT alerts
- Cryptocurrency exchanges blacklist this address
- Subject to asset seizure if identified on regulated platforms

7 Forensic Conclusions

This Bitcoin address represents a confirmed criminal payment infrastructure used in one of history's most significant ransomware attacks. The address:

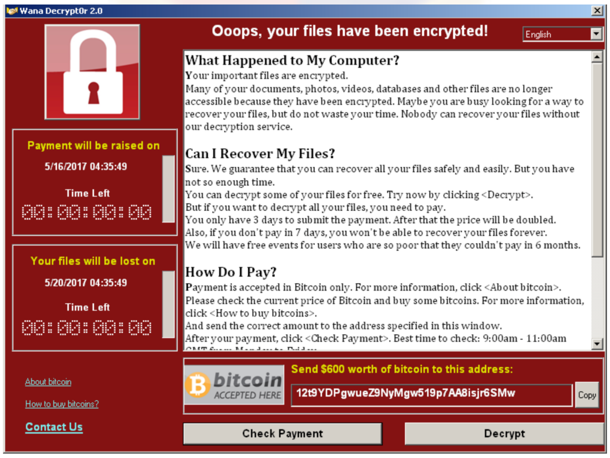
1. **Is definitively linked** to the WannaCry ransomware campaign
2. **Received ransom payments** from hundreds of victims worldwide
3. **Shows evidence of professional operation** with attempted fund obfuscation
4. **Represents critical risk** for any legitimate entity or individual
5. **Remains under active monitoring** by law enforcement and security researchers

7.1 Recommendations

1. **DO NOT** transact with this address under any circumstances
2. Report any observed activity to relevant authorities
3. Flag in threat intelligence databases
4. Monitor for fund movement indicating operator activity
5. Any connection to this address should trigger immediate investigation

8 References and Sources

1. Blockchain.com address explorer data
2. BitcoinWhosWho scam database reports
3. Cambridge Intelligence cryptocurrency analysis
4. US-CERT/CISA malware analysis reports
5. Multiple cybersecurity vendor technical analyses (Secureworks, Symantec, McAfee, etc.)
6. Academic research on WannaCry attack vectors
7. Law enforcement public statements and indictments



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 04:35:49
Time Left
00:00:00:00

Your files will be lost on
5/20/2017 04:35:49
Time Left
00:00:00:00

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $600 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Report Generated: December 15, 2025
Analysis Status: Confirmed Criminal Infrastructure
Recommended Action: Avoid all interaction, report if encountered