Bitcoin Battle: Burning Bitcoin for Geopolitical Fun and Profit

Kris Oosthoek
Delft University of Technology
Delft, The Netherlands
k.oosthoek@tudelft.nl

Kelvin Lubbertsen
Delft University of Technology
Delft, The Netherlands
k.j.m.lubbertsen@tudelft.nl

Georgios Smaragdakis
Delft University of Technology
Delft, The Netherlands
g.smaragdakis@tudelft.nl

***Abstract*—This study empirically analyzes the transaction activity of Bitcoin addresses linked to Russian intelligence services, which have liquidated over 7 Bitcoin (BTC), i.e., equivalent to approximately US$300,000 based on the exchange rate at the time. Our investigation begins with an observed anomaly in transaction outputs featuring the Bitcoin Script OP_RETURN operation code, tied to input addresses identified by cyber threat intelligence sources and court documents as belonging to Russian intelligence agencies. We explore how an unauthorized entity appears to have gained control of the associated private keys, with messages embedded in the OP_RETURN outputs confirming the seizure. Tracing the funds' origins, we connect them to cryptocurrency mixers and establish a link to the Russian ransomware group Conti, implicating intelligence service involvement. This analysis represents one of the first empirical studies of large-scale Bitcoin misuse by nation-state cyber actors.**

***Index Terms*—Bitcoin, Cybercrime forensics, FSB, SVR, GRU**

I. Introduction

Bitcoin has emerged as a significant instrument of state power in cyber-conflicts, with state actors and their affiliates leveraging the cryptocurrency for strategic advantage. Multiple sources confirm that governments and associated entities exploit Bitcoin's decentralized nature to circumvent traditional financial systems. For instance, media reports indicate that Iran's Islamic Revolutionary Guard Corps (IRGC) has engaged in Bitcoin mining to mitigate the impact of international sanctions [1] and has utilized Bitcoin transactions to fund proxy groups in the Middle East, such as Hamas and Hezbollah [2]. North Korea has been involved in numerous hacks of cryptocurrency exchanges, amassing approximately US$3 billion over a six-year span [3]. In 2024, Russia legalized crypto mining [4], employing it as a tool to sustain international trade amid economic sanctions [5], and Russian ransomware groups have been linked to co-opting with intelligence services. The Conti group, which has generated US$300 million in ransomware profits, is reportedly connected to the Federal Security Service of the Russian Federation (FSB) [6]. Likewise, members of Evil Corp, associated with the LockBit and BitPaymer ransomware strains, have FSB links either through prior employment [7] or familial connections [8].

In addition to its use by adversarial states, Bitcoin has drawn the attention of the United States as a target for surveillance. Leaked documents reveal that, as early as 2013, the U.S. employed signals intelligence to track Bitcoin senders and receivers [9]. Conversely, Russia's use of Bitcoin in cyber-espionage campaigns is also well-documented. During the 2016 hack of the Democratic National Committee, attackers linked to Russian intelligence leveraged Bitcoin to purchase servers and domains [10]. Similarly, in the SolarWinds supply-chain attack in 2020, alleged Russian state-sponsored actors used Bitcoin to purchase infrastructure [11]. In both instances, Bitcoin's pseudonymity enabled these actors to obscure their operations, hindering law enforcement efforts to trace activities through traditional financial channels. However, academic work on nation-state actors' use of cryptocurrency is limited compared to cybercriminal Bitcoin usage.

Beyond analyzing financial transactions, which has become commonplace through blockchain analysis, investigating other blockchain events can yield interesting results. One of these is *burning*, which can manifest itself in three ways. First, Bitcoin (BTC) is forever lost, that is, burned, if a miner fails to claim the block reward in the *coinbase* transaction. Second, BTC is removed from circulation when sent to a non-existing address as it distorts the cryptographic rule in which each address is a public key controlled with a secret key. Third, a non-existing or fabricated address is essentially a public key for which no private key exists, making the BTC unspendable.

Our analysis focuses on the third burn option named OP_RETURN an operation code (opcode) within the Bitcoin blockchain script to mark a transaction output as invalid. Also called *nulldata* field, it can add up to 80 bytes of arbitrary data to the transaction stored permanently on the blockchain. Sending to OP_RETURN creates an unspendable output, removing funds from circulation [12]. The OP_RETURN opcode was added to Bitcoin in March 2014 as part of the Bitcoin Core version 0.9.0 release [13]. It was originally introduced to provide a way for developers to store small amounts of data on the blockchain to minimize network impact and avoid known downsides of previous data storage methods in Bitcoin transactions. With its introduction, Bitcoin Core developers did not endorse storing data on the blockchain, as it would bloat the *unspent transaction output* (UTXO) database. Speculatively, this is why the feature was designed to render any amount of BTC unspendable when used.

Technically, an OP_RETURN output with a zero value can be included in a larger transaction with multiple outputs. There

is no requirement to attach a meaningful amount of *satoshis* (one one-hundred-millionth of a BTC, the smallest unit of account) to the OP_RETURN output, but it is used rarely; the mean value of BTC sent daily to OP_RETURN from January 1, 2023, until August 1, 2024, was 0.00805 BTC.

OP_RETURN allows users to store small amounts of data on the Bitcoin blockchain, taking advantage of the irreversible and immutable nature of the blockchain. Once the data are included in a block, it becomes a permanent tamper-resistant record that is accessible to anyone inspecting the blockchain. As an example, El Salvador's announcement of accepting Bitcoin [14] as legal tender was recorded on the blockchain using OP_RETURN.[1] The introduction of Taproot in 2021 significantly improved Bitcoin's scripting capabilities, allowing more efficient use of transaction space and greater data storage flexibility [15]. This inadvertently facilitated the creation of the Ordinals protocol, which uses Taproot's expanded data storage features to inscribe arbitrary data, such as text or images, onto individual satoshis, without relying on OP_RETURN.

Hence accounts of usage of OP_RETURN instructions are scarce, let alone coverage of their use in the context of nation-state actors' cyber operations. The only coverage we are aware of is by Sophos and Google, which in 2020 [16] and 2022 [17] reported on malware being controlled through OP_RETURN outputs. In addition to analysis by cybersecurity firms, this is the first academic account of nation-state actors' usage of OP_RETURN outputs in order to indefinitely burn a record amount of Bitcoin.

The contributions of this paper are as follows:

- We analyze the largest event of rendering BTC unspendable in the history of Bitcoin.
- We characterize the events in a geopolitical and cyber context, linking them to cyber espionage.
- We link wallets to cyber espionage, ransomware and hacking based on open and semi-open sources.
- We analyze significant simultaneous activity in over 60,000 automated fractional payment transactions between these wallets.
- We release 1,011 labeled wallet addresses to the community based on the analysis of this work [18].

The remainder of this paper is structured as follows. Section 2 provides an overview of the related work on the OP_RETURN instruction and exploits thereof. Section 3 provides an overview of Russian Cyber Operations. Section 4 describes the methodology of our analysis, including our initial findings. Section 5 attributes the wallets observed in the dataset to Russian intelligence services based on open sources. Section 6 explores simultaneous fractional payment activity. Section 7 summarizes our findings.

[1]Transaction hash: `cb01ea705494ce66d7e5b7cb51bb5b39b8e8ce31e168d1bd7dda253af359cc77`

II. Related Work

For the related work for our analysis, we consider academic contributions examining the OP_RETURN instruction, its associated exploits, and pertinent discussions in popular Bitcoin blogs and media.

Bartoletti and Pompianu [19] conducted a comprehensive study of the types and volumes of metadata embedded in OP_RETURN outputs, identifying their use in applications such as timestamping, asset tracking, and data anchoring. Other research has focused specifically on exploitation of the opcode for illicit purposes. Böck et al. [20] reported on blockchain-based botnets, where botmasters leverage blockchains' decentralized and censorship-resistant nature to establish command and control (C&C) channels. The authors assessed that the adversary's benefit of using blockchains for C&C is primarily resistance to law enforcement take-down but that its adoption is tempered by financial costs and technical limitations. Similarly, Matzutt et al. [21] examined how the metadata in Bitcoin is used to store potentially harmful or illegal content. Their analysis uncovered more than 1,600 embedded files, some containing objectionable material such as links to illegal content, which could make possession of the blockchain illegal in certain jurisdictions. Lastly, Narula and Narula [22] analyzed the Deadbolt ransomware, which, upon receiving payment, releases decryption keys on the blockchain through OP_RETURN transactions.

Coverage of OP_RETURN is scarce in popular media. The OP_RETURN lemma of the official Bitcoin Wiki is relatively short [12]. As discussed earlier, the coverage of the Glupteba malware by Sophos in 2020 [16] and Google's Threat Analysis Group in 2022 [17] described its use of OP_RETURN outputs. Both described Glupteba as a backdoor capable of stealing sensitive information, mining cryptocurrency, and enrolling infected devices in a botnet. The malware's operators embed encrypted data within OP_RETURN outputs, pointing to new C&C servers. This allows the malware to recover quickly even if one set of C&C servers is compromised or taken offline. The malware continuously monitors the blockchain for new transactions containing specific OP_RETURN data, ensuring that it can update its C&C addresses dynamically and autonomously. By not relying on a fixed domain name or a centralized server for C&C, the malware authors mitigate the risk of traditional C&C infrastructure being blocked by defenders or taken down by law enforcement.

Certain elements of our analysis concerning the evaporation (or "burning") of BTC align with observations in a blog post published in April 2023 by blockchain analysis firm Chainalysis [23]. The post offers a visual overview of transaction activity and references the OP_RETURN messages. However it provides only a cursory examination of the associated campaign. In contrast, this paper conducts a detailed investigation into BTC burning by nation-state cyber actors. Drawing on a diverse array of sources, we correlate these activities with geopolitical events over time, providing a comprehensive analysis of their strategic significance.

III. Russian Cyber Operations

Our research investigates a specific class of Bitcoin transaction metadata, with particular emphasis on references to the GRU, FSB, and SVR. The SVR (Foreign Intelligence Service), FSB (Federal Security Service), and GRU (Main Intelligence Directorate) are Russian Federation government's intelligence agencies that have become focal points in cyber security, espionage, and cyber warfare in a broader sense. This section explains their role in cyber operations, not self-evident to the blockchain and cryptocurrency community.

A. SVR

The *SVR* focuses on long-term intelligence collection and offensive operations. Its targets include diplomatic organizations, technology companies, international organizations, and defense contractors [24]. A cyber-espionage campaign attributed to the SVR is the attack on the software company *SolarWinds* in 2020, where an SVR cyber group, *APT29*, compromised SolarWind's software. The attack impacted several U.S. government agencies and tech companies using SolarWind's software. The breach allowed the SVR to monitor internal communications and exfiltrate sensitive information for months before being detected [11].

The ongoing operations of SVR-attributed actors APT29, Midnight Blizzard, Dukes, and Cozy Bear have a wider range of targets. With evolving TTPs, the actor has been observed to transform the operation from compromising on-premises networks to cloud infrastructure [25]. SVR operations focus on stealth and persistence, with long-term intelligence gain techniques aimed at political and economic advantages.

B. FSB

The *FSB* is primarily responsible for domestic security and counterintelligence, which extends to the cyber domain. In 2016, FSB-linked hackers launched *Armageddon*, a long-running cyber-espionage operation targeting Ukraine [26]. The operation carried out amidst the ongoing conflict between Russia and Ukraine, involved spear-phishing attacks and malware designed to steal military and government secrets.

In 2017, the *NotPetya* attack, attributed to the FSB and GRU, targeted Ukraine but caused global disruption [27]. NotPetya exploited a leaked backdoor developed by the US National Security Agency (NSA), causing damage to companies including Maersk, FedEx, and Merck. Disguised as ransomware, it was intended to erase data and disrupt operations, causing an estimated US$10 billion in damages worldwide.

Two *FSB* agents have been charged by the FBI for conducting a data breach of Yahoo! in 2016, in which more than 500 million Yahoo! accounts were compromised [28]. The attack, in collaboration with cybercriminals, exposed user data and demonstrated the FSB's reliance on criminal proxies to carry out large-scale cyber operations. More recently, the National Crime Agency (NCA) has described how the FSB has been co-opting *Evil Corp*, a cybercrime group for its own malicious cyber activity [29]. The FSB tasked Evil Corp with conducting cyber attacks and espionage operations against NATO allies.

Date	OP_RETURN Value
2022-02-18	*4.167737*
2022-02-12	*3.691136*
2021-02-14	3.548904
2021-02-13	2.591002
2020-10-11	2.405650
2021-02-18	2.345250
2020-10-23	1.988000
2021-02-15	1.873764
2020-10-12	1.746181
2015-09-11	1.565100

TABLE I: Top Days with BTC expenditures to OP_RETURN (dates relevant to this analysis in italic).

C. GRU

The *GRU* has been implicated in disruptive and aggressive cyber attacks. In the lead-up to the 2016 US presidential election, GRU cyber units *Unit 26165* and *Unit 74455* orchestrated a series of hacks targeting the Democratic National Committee (DNC) and the Democratic Congressional Campaign Committee (DCCC) [10]. Emails stolen during these hacks were later leaked through WikiLeaks, allegedly with the intention of influencing the US election outcome.

In the same year, the GRU conducted *Ghostwriter*, a disinformation operation targeting Eastern European countries. It involved hacking news outlets and altering articles to spread pro-Russian narratives, particularly in countries like Lithuania, Latvia, and Poland [30]. The GRU has also been held responsible for a cyber operation called *Olympic Destroyer*, targeting the 2018 Winter Olympics in South Korea. The attackers intended to disrupt the IT systems that support the event, including Wi-Fi networks and ticketing services [31]. Although the attack was designed to seem like it originated in North Korea, forensic analysis linked the operation to GRU's Unit 74455 (Sandworm), which targets critical infrastructure.

In 2015 and 2016, the GRU breached Ukraine's power grid, causing blackouts in several regions. The *Industroyer malware* (or *CrashOverride*) was designed to disrupt industrial control systems (ICS) used in power grids [32]. Together with Stuxnet [33], this is one of the few instances in which a cyber operation caused physical disruption of critical infrastructure.

IV. An OP_RETURN Anomaly

To facilitate an exploratory investigation of transactions containing OP_RETURN opcodes (from here called OP_RETURN), we parsed all historical transactions from a Bitcoin full node up until August 1, 2024. Bitcoin transactions can be appended with small script operations. Bitcoin Script is a stack-based programming language that defines the conditions under which Bitcoin transactions can be spent, enabling features such as multi-signature and time-locks through a set of operation codes (opcodes), instructing the blockchain what to do. If the script starts with the hexadecimal equivalent of OP_RETURN (i.e., `6a`), the opcode for OP_RETURN is identified as an OP_RETURN output. The use of OP_RETURN does not necessarily burn the bitcoin transacted. It is possible

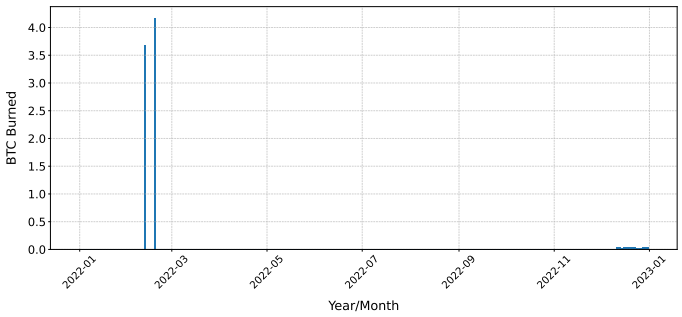

Fig. 1: Time series of BTC Burned on OP_RETURN in 2022.

to assign a zero value to the output. Any value other than null indicates that the corresponding amount of satoshi (one hundred millionth of a Bitcoin) will be burned.

A. Methodology

To gather the OP_RETURN binary metadata central to this analysis, we used a full node running Bitcoin Core version 26.2, synchronized with the blockchain until July 2024. To facilitate a quick analysis of transactions containing OP_RETURN opcodes (from here called OP_RETURN), we parsed all historical transactions until August 1, 2024. We used the *blockchain-parser* library [34] to convert Bitcoin-native raw blk*****.dat files, based on the `getrawtransaction` RPC command to plain text. The resulting text files were parsed on the fly for transactions containing OP_RETURN opcodes using regular expressions, the output of which was pushed to a DataFrame object for efficient query and data manipulation, run in memory on a workstation with significant (128 GB) RAM.

Upon obtaining the initial set of suspicious transaction hashes, the parsed Bitcoin data was crawled to discover associated inputs, outputs, and additional transactions. Data was obtained from the free Blockchain.com API [35] for a sample of transaction hashes. This allowed for the verification of the results from our parser, serving as a double check. We were provided access to, and we used the Graphsense API [36] maintained by Iknaio for its address clustering capabilities, based on the co-spend heuristic [37] to discover joint address ownership. We were also provided access to address labels by Scorechain [38] under an academic license to identify links with counterparties. A full list of the addresses in our dataset and their derived labels (GRU, SVR, FSB) is available online on GitHub [18].

With a feature that potentially renders funds irrecoverable, the use of OP_RETURN is relatively limited. The mean value of BTC sent daily with OP_RETURN from January 1, 2023, to August 1, 2024, is 0.00805 BTC. Only on a few historical dates does the total value peak above a single Bitcoin. Table I provides an overview of the historical daily top spending with OP_RETURN, based on aggregated daily non-zero outputs containing the OP_RETURN opcode. This overview made us decide to dig deeper into the two top dates, as these were also the most recent.

We found that on February 12, 2022, i.e., twelve days before Russia's invasion of Ukraine (on February 24, 2022) after months of military preparations, a total of 583 OP_RETURN transactions took place. A couple of days later, on February 18, another batch of 210 transactions followed. All transactions had either of three OP_RETURN messages attached. The fact that the OP_RETURN campaign took place less than two weeks before the actual invasion should not be regarded in isolation. We argue that it rather must be understood as part of a broader socio-political and technological context that includes the intersection of cryptocurrency adoption and hacking by state actors and geopolitical instability.

Figure 1 provides a visual impression of the significance of the amount of BTC burned on these two dates, relative to OP_RETURN disbursement during the rest of the year 2022. We queried the output of our custom parser to discover additional transactions from the addresses involved in the initial set of transactions that took place on February 12 and 18. Based on that, we identified 11 additional transactions on March 14th (i.e., after the Russian invasion of Ukraine) with a different OP_RETURN message, sending funds to the official Bitcoin donation address of the Ukrainian Armed Forces [39]. However, the OP_RETURN outputs on this date had 0 BTC attached, as shown in Table II.

As shown in Table II, the transactions included OP_RETURN instructions that with hexadecimal values representing Cyrillic characters, which can be translated into four distinct callouts: (i) GRU to SVR, (ii) GRU to FSB, (iii) GRU to GRU, and (iv) Helping Ukraine with money from GRU hackers.

Table II provides an overview of the Cyrillic and English versions of the messages and their count of appearances within blockchain transactions. Furthermore, the table shows timestamps for the first and last transactions per message, the cumulative amount of (fractional) Bitcoin burned by the different messages, and the number of unique addresses that participated in sending each message. Not all identified wallet addresses have engaged in burning Bitcoin. Our data set consists of 986 addresses that were either inputs or outputs in at least one OP_RETURN transaction. Of these 986 addresses, 275 were used as input addresses in the OP_RETURN transactions, burning 7.06 BTC in total. However, as will be discussed in the next section, all of the 986 addresses in our dataset engaged in sending and receiving small payment transactions.

To check the attribution of each address, we took the first sentence of each message, splitting it based on the word "to". As an example, for "GRU to SVR", we assumed the inputs are GRU wallets and the outputs SVR wallets. We only considered outputs, as observed in Table 2, the inputs are always GRU. For example, in transactions labeled *GRU to FSB*, the supposed GRU address will appear both as input and output due to it being a change address. Judging from the messages summarized in Table II, only addresses attributed to the GRU were used as transaction output, and the SVR and FSB were used as outputs. Although, based on the outputs, SVR and FSB addresses do indeed appear in the transactions,

TABLE II: Summary of Transactions containing OP_RETURN Outputs

OP_RETURN Message	English Translation	TXs	First TX	Last TX	Cuml. BTC Burn	Unique Addr.
ГРУ к ГРУ. Использованы для хакинга!	GRU to GRU. Used for hacking!	505	2022-02-12 15:56:34	2022-02-18 23:25:24	6.15219839	222
ГРУ к СВР. Использованы для хакинга!	GRU to SVR. Used for hacking!	309	2022-02-12 15:56:34	2022-02-18 21:41:59	0.90929650	196
ГРУ к ФСБ. ИспользоЂаны для хакинга!	GRU to FSB. Used for hacking!	248	2022-02-12 15:56:34	2022-02-18 23:25:24	0.00006946	161
Помощь Украину с деньгами от ГРУ хакиров	Helping Ukraine with money from GRU hackers	54	2022-03-14 18:14:13	2022-03-14 19:25:15	0	54

these rather engage in payment activity during the campaign, but not OP_RETURN outputs.

As shown in Table II and further discussed in the next section, the 14 March, 2022 OP_RETURN outputs referring to helping Ukraine did not burn any Bitcoin but were accompanied by the transfer of money to Ukraine's donation address [39]. For this reason, they are not represented in Table II. The difference in the total burned per date in Figure 1 and Table II can be explained by the OP_RETURN transactions that took place on these dates but were not associated with this campaign.

V. Address Ownership

In order to empirically assess ownership of the addresses, we have been looking for evidence of this in reliable sources, open to the public. Hence, we queried for sources reporting on usage of Bitcoin in Russian cyber operations. Of the addresses in the dataset, three have been publicly attributed by reliable sources to Russian intelligence agencies. This section considers these findings.

A. Democratic National Committee Breach

According to various sources, the Democratic National Committee (DNC) was hacked by Russian actors in 2018. The official indictment by a US court assesses that the actors have used Bitcoin to purchase VPN accounts, server infrastructure, and domain names [40]. Specifically, the indictment mentioned that newly mined Bitcoin were used to fund the attack infrastructure. This is consistent with the hypothesis that the Kremlin uses the fruits of Bitcoin mining for subversion [41]. Although the indictment does not mention any Bitcoin address, an industry media blog post includes the address `18N9jzCDsV9ekiLW8jJSA1rXDXw1Yx4hDh` [23].

The DNC hack is widely attributed to Fancy Bear and Cozy Bear [42], [43]. While Fancy Bear is linked to GRU Unit 26165, Cozy Bear is linked to the SVR [40]. In the OP_RETURN messages, the aforementioned public wallet address is linked to the GRU.

B. SolarWinds Breach

We found an archived blog by cyber incident response company HYAS, reporting on its forensic investigation of the SolarWinds hack in 2020, which mentioned two hashes of Bitcoin transactions to procure attack infrastructure [44]. On inspection of the transaction data, we found the source addresses `1DLA46sXYps3PdS3HpGfdt9MbQpo6FytPm` and `1L5QKvh2Fc86j947rZt12rX1EFrCGb2uPf` also occurred in our dataset. We labeled these addresses as SolarWinds for further analysis.

The SolarWinds breach is publicly linked to the SVR, specifically to a group known as APT29 (Advanced Persistent Threat 29), also referred to as Cozy Bear [45]. The OP_RETURN callouts in our dataset do also link the two wallet addresses to the SVR.

Furthermore, according to a report by Western intelligence agencies, Unit 29155 of the GRU, the 161st Specialist Training Center, has employed the WhisperGate malware against Ukranian and other NATO targets [46]. According to the report, the actors used Discord for the distribution and control of malware hidden as ransomware. The fake ransom note displayed by the malware listed the Bitcoin address `1AVNM68gj6PGPFcJuftKATa4WLnzg8fpfv`. Although this address does not appear in our cluster of GRU addresses, we mention it here as this Bitcoin link to GRU cyber operations.

The transaction activity of the DNC and SolarWinds addresses prior to the callouts is typical of a sophisticated cyber actor. Exactly as reported for ransomware syndicates [47], the addresses were only used once, i.e., a deposit, followed by a payment for infrastructure. They only become active again during the OP_RETURN campaign reported in this analysis.

Inherent to Bitcoin's asymmetric cryptography, the OP_RETURN transactions must have been initiated by an actor in possession of the private keys. The one-way hash function used to generate the public-private key pair cannot be reversed. As an example, this means that the private key of the addresses implicated in the DNC and SolarWinds hacks, used to purchase the attack infrastructure, was also used for OP_RETURN transactions. This can be compared to a password being obtained from a password manager and then being used to act as if one is the legitimate owner.

C. Address Characteristics

As shown in Table III, we found only three addresses in our dataset labeled as belonging to SVR. As discussed earlier in this section, two of these have been publicly linked to the attack on SolarWinds by the SVR. In addition, only four addresses were labeled as FSB. This means that most addresses belong to the GRU, at least according to the callouts. Furthermore, six addresses belonging to GRU start with *bc1* and thus are Bech32/SegWit addresses. All other addresses in the dataset start with '1' or '3' and thus are considered legacy

TABLE III: General statistics of clusters

Entity	# addresses	# clusters	Cluster size (avg)	Cluster size (std)	# transactions (avg)	# transactions (std)
SVR	3	3	1.000000	0.000000	1.666667	0.471405
GRU	15,856	872	16.196118	57.489070	13.371560	31.313955
FSB	13	4	3.250000	2.277608	204.250000	2.277608

addresses. Going with the hypothesis that the private keys were seized, using legacy addresses might suggest something about the software wallet type used to store the private keys.

D. Label-Based Address Clustering

With address ownership confirmed as far as possible, we applied clustering to the addresses using the co-spending heuristic first described by [37]. This heuristic merges all input addresses in an outgoing transaction to the same entity under the assumption that all inputs have to be signed. We argue that even though a third party allegedly compromised the private key, this still gives it access to only the funds of one group, GRU, as the descriptions in the OP_RETURN metadata only mention GRU as the sender.

All transactions, 984 addresses, can be labeled as associated with the GRU, SVR, or FSB. When applying co-spending, we learn that these fall into 879 clusters (see Figure 3). By clustering, we associate new addresses with those in the initial dataset. We learn that none of the clusters overlap between agencies; for instance, no addresses related to the GRU are also used by the FSB.

In Table III, we describe the statistics for the cluster. We must note that to be able to observe nation-state actor's activity, we must delete transactions done by wallet hackers. We assume they have included an OP_RETURN output in every transaction since their motive appears to have been doxxing. That way, we can analyze transactions associated with the original owner of the wallets and, for the first time, analyze the behavior of these nation-state actors. With three addresses being linked to Russian cyber actors by official sources, which appear in the co-spend address clusters in Table III, we can confidently establish that Russian actors indeed controlled these at one point.

VI. Financial Analysis

We distinguish between financial transactions that took place as part of the OP_RETURN campaign, but that did not burn money. We call these payment transactions. As the actor behind the campaign also put some externally sourced funds into it, we will focus on these transaction first, which we will call funding transactions.

A. Funding Transactions

On February 1st, 2022, the likely actor behind the campaign put 1 BTC into a wallet associated with Cryptomixer.io, a well-known centralized cryptocurrency mixing service.[2] Cryptomixer.io applies a series of transactions similar to a peel chain, a sequence of transactions where a large input is progressively split into smaller outputs across multiple transactions to obscure the origin of the funds and to withdraw money associated to other users of the service. This address served to load the addresses with sufficient funds to participate in the campaign. This was necessary, as some wallets were empty and some amount of funds is of course necessary to transact. These transactions did not include an OP_RETURN output and thus did not show up in our initial batch of transactions. The attribution of this address to Cryptomixer.io is based on labels obtained from ScoreChain [38].

B. Payment Transactions

Along the OP_RETURN outputs, the actor also sent small amounts to outputs which in our dataset are all identified as either GRU, SVR, or FSB wallet addresses. The outputs contain fractional amounts of Bitcoin below US$1. It has a parallel with *dusting attacks*, where tiny amounts of BTC, called *dust*, are sent to trace and analyze transactions, aiming to de-anonymize users. By analyzing transactions that include the dust, attackers can then identify which addresses are likely controlled by the same user.

Inpection of individual transactions reveals an interesting feature, suggesting that a scripted scheme. When inspecting the individual transactions, two things stand out. First, all transactions have a single input address, but multiple output addresses. One transaction even counts one input and 880 outputs of 0.00000547 BTC or US$0.23 each, with an aggregate total value of US$1,424.09.[3]

Figure 2 provides a force-clustered overview of the interaction of different GRU, FSB and SVR-labeled wallets during the February 12-18 timeframe. One wallet[4] is responsible for 100 OP_RETURN transactions, burning 96,658,067 satoshi, equivalent to 0.966 BTC.

We queried GraphSense [36], [48], a blockchain analysis tool hosted by Iknaio, to discover additional transactions of the addresses involved in the initial transactions between February 12 and 18. Based on that, we identified 11 additional transactions on March 14th with a different OP_RETURN message, sending funds to the official Bitcoin donation address of the Armed Forces of Ukraine [39], hosted by Ukrainian cryptocurrency exchange Kuna.io. On March 14th, in 11 transactions with a *Helping Ukraine with money from GRU hackers*

[2]Initial transaction hash: `96e8c84dfa9dcbe5b161c345877381f2c2e83a464c1db1e149c9b0071da9ced8`

[3]`2deb61815c8aff5fe89c39bd8ab632b1110f70be3b9fba52b1f77d68e3bbc622`

[4]`1594on5HBqWgpxLsvGKdijccdEpxJ5pjZV`

TABLE IV: Summary of Payment Transactions by Address Attribution

Label	Total Transactions	Total Value (USD)	Mean Value (USD)	Median Value (USD)	Min Value (USD)	Max Value (USD)	Outlier Count	Outlier Mean (USD)	Outlier Min (USD)	Outlier Max (USD)
FSB	308	129.20	0.42	0.43	0.22	0.43	16	0.23	0.22	0.25
GRU	59,855	2,065,728.28	34.51	0.43	0.22	8,353.29	864	1,995.44	835.53	8,353.29
SVR	1,083	336.72	0.31	0.22	0.22	0.43	0	0.00	0.00	0.00

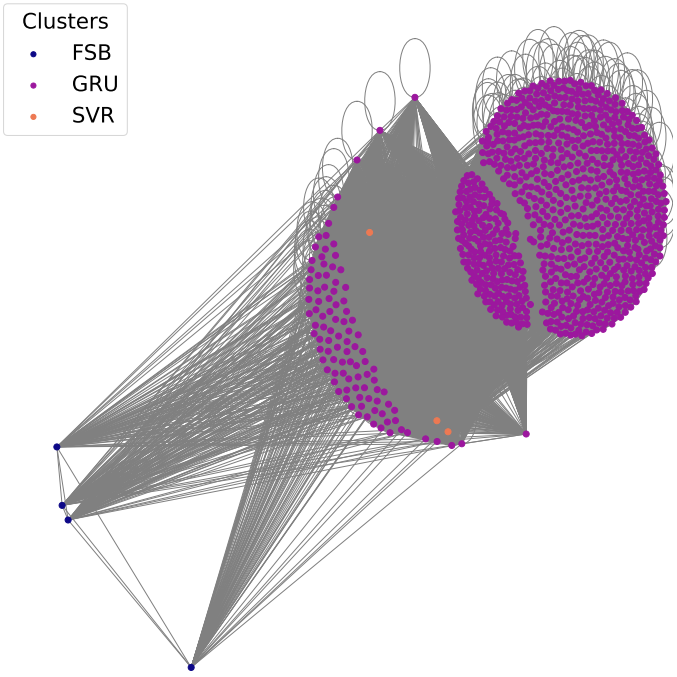

Fig. 2. Force-clustered payment transaction activity.

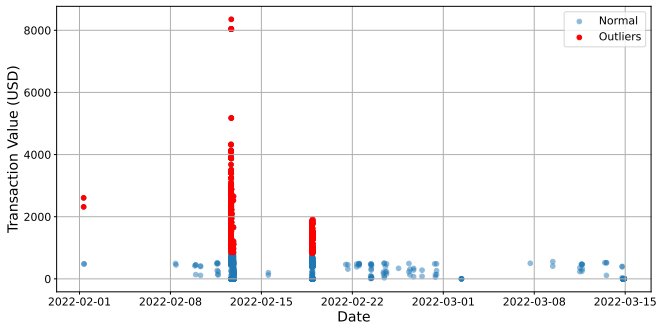

Fig. 3. Timeline of Payment Transactions in the OP_RETURN Campaign, highlighting normal (blue) and outlier (red) values.

OP_RETURN output, in total US$975,92 was sent to the official donation address. Of these 11 transactions, which had 637 outputs in total, 11 outputs went to the Ukrainian donation address. The average value of an output was US$3,22 and the minimum value US$0.23, again highlighting the circulation of small funds to generate transaction traffic and noise.

C. Ransomware and Breach Activity

Most addresses in our dataset have never seen activity after the campaign covered in this analysis. However the wallet address `1EWr1L7BSzFGjk5sZz3zkq5US2x7aiQSJQ`, attributed to the GRU, has been active after 2022. On 24 February 2022, it was observed interacting with a wallet associated with the Conti ransomware group according to labels obtained from Ransomwhe.re [47]. In one transaction,[5] 0.012485 BTC, worth US$466.59 at the time, was sent to the group. Notably, the now closed down group has become known for its connection to the FSB [6]. In a transaction[6] on May 28th, 2024, the same wallet was observed sending 0.003302 BTC, worth US$229.05 to an address associated with the exploit of the Rain.com cryptocurrency exchange. Finally, on June 26th, 2024 the wallet interacted with Reisbet, a Turkish gambling platform.[7] The Rain.com and Reisbet labels were provided by ScoreChain [38].

VII. Conclusion

Within the broader conflict known as the Russo-Ukrainian War, the dates of February 12 and 18, 2022, may appear anomalous, given that Russia's invasion of eastern Ukraine commenced on February 24, 2022. However, numerous events in the preceding months and days foreshadowed this escalation. As demonstrated in our article, it was in this time frame that the OP_RETURN actor deliberately generated significant activity on the blockchain by creating a spike and record in both OP_RETURN outputs and small dust-like transactions. Regarding the "6 D's" of cyber warfare (deterrence, deception, disruption, destruction, disinformation, denial), the OP_RETURN campaign can be classified as an act of denial and destruction. It exemplifies denial by depriving the original owner of access to their financial resources, while the use of the burn opcode in Bitcoin Script effectively destroys those resources.

Building on evidence embedded in the OP_RETURN binary code suggesting that these are indeed Bitcoin wallets once controlled by Russian intelligence agencies, two primary scenarios emerge regarding the attribution of this campaign. The OP_RETURN transactions could have been initiated either by a disgruntled insider with direct access or by an outsider who illicitly obtained the private keys. Given that few entities possess the capability, motive, and opportunity to penetrate

[5] `f79284691b73c2c667da69a36f648faf4be189a08acadaab054124b9a2fd23cf`

[6] `68a2d5cc511cf08f94b70b774eb11973fd80adf7cae1bdb353b5b304d9853792`

[7] `3372f4688cd4bd8207ffceb0a28c54cb7d5b16c1599d000aa43c803ce7a8c741`

the security of intelligence agencies such as the FSB, SVR, or GRU, it seems implausible that a low-level attacker (such as a script kiddie) could have acquired the keys and executed this campaign.

Alternative hypotheses regarding the campaign's origins warrant consideration. One possibility is an inside job, wherein an individual within the GRU, FSB, or SVR, perhaps a disgruntled operator or an IT employee with access to critical systems, misappropriated the Bitcoin. Such an act could stem from motives including financial gain, personal vendettas, or participation in a broader scheme orchestrated by external actors. Another scenario involves a rogue insider collaborating with a third party, providing essential access to systems or expertise in circumventing security protocols, thereby enabling an external hacker to execute the theft.

From a technical perspective, the GRU's Bitcoin wallet may have been compromised due to a vulnerability, such as a software flaw or an error in cryptographic protocol implementation, allowing an attacker to access and siphon funds. This would indicate a significant oversight on the part of the GRU. Alternatively, a more sophisticated method, such as a man-in-the-middle attack, could have been employed. In this case, the attacker might have intercepted communications during a transaction or wallet transfer process, compromising the GRU's assets without their immediate awareness.

This is further underscored by the actor's decision to burn over US$300,000 worth of Bitcoin against the prevailing exchange rate at the time. The choice not to monetize the acquired funds implies the presence of a robust ethical framework. Additionally, it seems highly improbable that Russian actors would voluntarily donate Bitcoin to the Ukrainian cause. The initiator's apparent ability to afford the destruction of over US$300,000 worth of seized Bitcoin suggests a level of sophistication, simultaneously deterring the original owner from reusing the associated addresses. Consequently, we assess that both the original owner and the actor who appropriated the funds are likely highly skilled actors. However, determining which of the two is more sophisticated, given the potential compromise of the private keys, is a matter for further debate and lies beyond the scope of this paper.

Acknowledgment

The authors would like to express their gratitude to Bernhard Haslhofer of Iknaio for providing access to the GraphSense API, which allowed Bitcoin address clustering and also to Scorechain, which facilitated the identification of potential ownership of addresses. This work was supported by the European Commission under the Horizon Europe Programme as part of the project SafeHorizon (Grant Agreement #101168562). The content of this article does not reflect the official opinion of the European Union. Responsibility for the information and views expressed therein lies entirely with the authors.

References

[1] Elliptic, "How terrorist groups are exploiting crypto to raise funds and evade detection," 8 2023. [Online]. Available: https://www.elliptic.co/blog/how-terrorist-organizations-are-exploiting-crypto-to-raise-funds-and-evade-detection

[2] Congressional Research Service, "Terrorist Financing: Hamas and Cryptocurrency Fundraising," 11 2023. [Online]. Available: https://crsreports.congress.gov/product/pdf/IF/IF12537/2

[3] J. Greig, "UN probing 58 alleged crypto heists by North Korea worth $3 billion," The Record, March 2024. [Online]. Available: https://therecord.media/north-korea-cryptocurrency-hacks-un-experts

[4] R. Waggaman, "Russia legalizes crypto for cross-border trade amid sanctions," CNBC, 7 2024. [Online]. Available: https://www.cnbc.com/2024/07/30/russia-considers-legalizing-crypto-as-a-form-of-payment-amid-sanctions.html

[5] G. Bryanski, "Russia is using bitcoin in foreign trade, finance minister says," Reuters, 2024. [Online]. Available: https://www.reuters.com/markets/currencies/russia-is-using-bitcoin-foreign-trade-finance-minister-says-2024-12-25/

[6] M. Burgess, "Conti Leaks Reveal the Ransomware Group's Links to Russia," Wired, March 2022. [Online]. Available: https://www.wired.com/story/conti-ransomware-russia/

[7] U.S. Department of Treasury, "Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware," December 2019. [Online]. Available: https://home.treasury.gov/news/press-releases/sm845

[8] ——, "Treasury Sanctions Members of the Russia-Based Cybercriminal Group Evil Corp in Tri-Lateral Action with the United Kingdom and Australia," October 2024. [Online]. Available: https://home.treasury.gov/news/press-releases/jy2623

[9] S. Biddle, "The NSA Worked to "Track Down" Bitcoin Users," March 2018. [Online]. Available: https://theintercept.com/2018/03/20/the-nsa-worked-to-track-down-bitcoin-users-snowden-documents-reveal/

[10] United States District Court for the Southern District of New York, "Complaint - Democratic National Committee v. Russian Federation et al." January 2019. [Online]. Available: https://storage.courtlistener.com/recap/gov.uscourts.nysd.492363/gov.uscourts.nysd.492363.1.0.pdf

[11] Cybersecurity and Infrastructure Security Agency, "Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations," 4 2021. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a

[12] Bitcoin Wiki, "OP_RETURN - Bitcoin Wiki." [Online]. Available: https://en.bitcoin.it/wiki/OP_RETURN

[13] Bitcoin.org, "Bitcoin Core version 0.9.0 released," March 2014. [Online]. Available: https://bitcoin.org/en/release/v0.9.0

[14] L. Alfaro, "El Salvador: Launching Bitcoin as Legal Tender," Harvard Business School, 2022. [Online]. Available: https://www.hbs.edu/faculty/Pages/item.aspx?num=62068

[15] Bitcoincore.org, "Bitcoin Core :: Bitcoin Core 0.21.1." [Online]. Available: https://bitcoincore.org/en/releases/0.21.1/

[16] L. Nagy, "Glupteba: Hidden Malware Delivery in Plain Sight Inside a self-concealing malware distribution framework with a security-resistant ecosystem," SophosLabs, June 2020. [Online]. Available: https://news.sophos.com/wp-content/uploads/2020/06/glupteba_final-1.pdf

[17] S. Huntley and L. Nagy, "Updates from Threat Analysis Group (TAG)," Google, 12 2021. [Online]. Available: https://blog.google/threat-analysis-group/disrupting-glupteba-operation/

[18] ksthk, "Bitcoin battle address dataset," Github. [Online]. Available: https://github.com/ksthk/btc-battle

[19] M. Bartoletti and L. Pompianu, "An Analysis of Bitcoin OP_RETURN Metadata," *Lecture Notes in Computer Science*, vol. 10323, pp. 218–230, 2017. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-70278-0_14

[20] L. Böck, N. Alexopoulos, E. Saracoglu, M. Mühlhäuser, and E. Vasilomanolakis, "Assessing the Threat of Blockchain-based Botnets," in *2019 APWG Symposium on Electronic Crime Research (eCrime)*, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/9037600

[21] R. Matzutt, J. Hiller, M. Henze, J. H. Ziegeldorf, D. Müllmann, O. Hohlfeld, and K. Wehrle, "A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin," *Lecture Notes in Computer Science*, vol. 10957, pp. 420–438, 2018. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-662-58387-6_23

[22] J. Narula and A. Narula, *Breaking Ransomware: Explore ways to find and exploit flaws in a ransomware attack (English Edition)*. BPB Publications, 2023.

[23] Chainalysis, "Bitcoin in War: OP_RETURN Callouts of Russian Military Bitcoin Addresses Point to Blockchains' Growing Role in Geopolitical Conflict," April 2023. [Online]. Available: https://www.chainalysis.com/blog/russia-bitcoin-op-return-messages/

[24] Federal Bureau of Investigation (FBI), National Security Agency (NSA), Cyber National Mission Force (CNMF), and National Cyber Security Centre (GCHQ), "Update on SVR Cyber Operations and Vulnerability Exploitation," Joint Cybersecurity Advisory, October 2024. [Online]. Available: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3931959/nsa-issues-updated-guidance-on-russian-svr-cyber-operations/

[25] National Cyber Security Centre (GCHQ), "SVR cyber actors adapt tactics for initial cloud access," February 2024. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a

[26] D. Antoniuk, "Russian hacking group Armageddon increasingly targets Ukrainian state services," 7 2023. [Online]. Available: https://therecord.media/armageddon-gamaredon-russian-hacking-group-increasingly-targeting-ukraine-government

[27] European Repository of Cyber Incidents (EUREPOC), "Major Cyber Incidents - NotPetya," March 2023. [Online]. Available: https://eurepoc.eu/publication/major-cyber-incident-notpetya

[28] US Office of Public Affairs, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts," March 2017. [Online]. Available: https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions

[29] National Crime Agency (NCA) and Federal Bureau of Investigation (FBI), "Evil Corp: Behind the Screens," October 2024. [Online]. Available: https://www.nationalcrimeagency.gov.uk/who-we-are/publications/732-evil-corp-behind-the-screens/file

[30] C. Page, "EU warns Russia over 'Ghostwriter' hacking ahead of German elections," TechCrunch, September 2021. [Online]. Available: https://techcrunch.com/2021/09/24/european-council-russia-ghostwriter/

[31] Office of Public Affairs, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," October 2020. [Online]. Available: https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

[32] Cybersecurity & Infrastructure Security Agency, "CrashOverride Malware," July 2021. [Online]. Available: https://www.cisa.gov/news-events/alerts/2017/06/12/crashoverride-malware

[33] D. Kushner, "The Real Story of Stuxnet," *IEEE Spectrum*, vol. 50, no. 3, pp. 48–53, 2013.

[34] ragestack, "Blockchain-parser," Github. [Online]. Available: https://github.com/ragestack/blockchain-parser

[35] "Blockchain.com." [Online]. Available: https://www.blockchain.com

[36] GraphSense, "GraphSense Cryptoasset Analytics Platform." [Online]. Available: https://graphsense.org/

[37] Sarah, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. M. Savage, "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names," pp. 127–140, 2013.

[38] "Scorechain." [Online]. Available: https://www.scorechain.com

[39] "Official E-wallet Addresses for Donating Crypto to Ukraine." [Online]. Available: https://standwithukraine.com.ua/donation/crypto

[40] United States District Court for the District of Columbia, "Report on the investigation into russian interference in the 2016 presidential election," 7 2018.

[41] N. Barnett, "The Other Bitcoin Boom: Crypto Mining in Russia's Shadow Territories — Royal United Services Institute," The Royal United Services Institute (RUSI), 2024. [Online]. Available: https://www.rusi.org/explore-our-research/publications/commentary/other-bitcoin-boom-crypto-mining-russias-shadow-territories

[42] T. Rid, "All Signs Point to Russia Being Behind the DNC Hack," VICE, 2016. [Online]. Available: https://www.vice.com/en/article/all-signs-point-to-russia-being-behind-the-dnc-hack/

[43] S. Thielman, "DNC email leak: Russian hackers Cozy Bear and Fancy Bear behind breach," The Guardian, 2016. [Online]. Available: https://www.theguardian.com/technology/2016/jul/26/dnc-email-leak-russian-hack-guccifer-2

[44] HYAS, "Solarwinds compromise: Insights into the attacker domain infrastructure," 12 2020. [Online]. Available: https://web.archive.org/web/20201218160801/https://hyas.com/blog/solarwinds-compromise-insights-into-the-attacker-domain-infrastructure

[45] UK National Cyber Security Centre, "UK and US call out Russia for SolarWinds compromise," 2021. [Online]. Available: https://www.ncsc.gov.uk/news/uk-and-us-call-out-russia-for-solarwinds-compromise

[46] Australian Signals Directorate, "Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure," 9 2024. [Online]. Available: https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/russian-military-cyber-actors-target-us-and-global-critical-infrastructure

[47] K. Oosthoek, J. Cable, and G. Smaragdakis, "A Tale of Two Markets: Investigating the Ransomware Payments Economy," *Communications of the ACM*, vol. 66, pp. 74–83, 7 2023. [Online]. Available: https://dl.acm.org/doi/10.1145/3582489

[48] B. Haslhofer, R. Stütz, M. Romiti, and R. King, "Graphsense: A general-purpose cryptoasset analytics platform," *Arxiv pre-print*, 2021. [Online]. Available: https://arxiv.org/abs/2102.13613