# Beating the Blockchain

## Mapping Out Decentralized Namecoin and Emercoin Infrastructure

By Kevin Perlow

## Background

The Namecoin and Emercoin blockchains are designed to provide users with takedown-resistant domain names by distributing and decentralizing DNS records across a large number of devices while incorporating technology that provides historical data integrity. These blockchains support non-ICANN Top-Level Domains (TLDs) (.bit, .coin, .bazar, .lib, and .emc) that users can communicate to via alternate DNS resolution endpoints such as OpenNIC servers.

This BlackHat 2018 whitepaper details techniques designed to:

- Proactively identify malicious domains registered using these blockchains
- Map out additional infrastructure associated with known or suspected malicious domains

## Key Findings

The generation of materials for this whitepaper resulted in the discovery of additional infrastructure related to previously reported malware families, including Dimnie, Neutrino, Smoke Loader, and Necurs. Domains and IP addresses associated with selected activity clusters are available in the appendix.

The most notable findings generated from this research pertain to the "RTM" banking malware first publicly disclosed in ESET's "Read The Manual" report. This malware is designed to target and steal information from users of remote banking and accounting software.[1] Findings associated with this malware include:

1) Strong evidence that the threat actor has continued its operations since ESET publicly disclosed this malware in 2017. As of this writing, this included activity detected on 24 July 2018 targeting a financial officer for an administrative district in a federal subject of Russia as well as email accounts from two Russian energy suppliers and one Russian energy transporter.

2) Evidence that the threat actor responsible for this activity has updated its malware since its disclosure, adding additional applications to the tool's target list.

This paper's primary purpose is to explain and demonstrate the mapping of decentralized infrastructure; in parallel, it will also detail several aspects of the RTM malware given its relevance to this task and its use in narrowly scoped attacks. Readers are encouraged to visit ESET's public report for a more comprehensive overview of RTM's functionality and history.

## Technical Information

Decentralized Systems

Decentralized DNS typically refers to a system in which DNS records are stored across a large distribution of computers, preventing changes to these records from taking place if these changes aren't collectively agreed upon. By pairing this concept with blockchain technology to provide historical data integrity, decentralized DNS operates as a takedown-resistant system for hosting records at a low cost. In recent years, various threat actors have abused this concept by configuring their malware to communicate with these decentralized domain names as well as by registering decentralized domain names that resolve to illegal "carding shops." This type of activity generally resides on two blockchains:

1) **Namecoin**- Namecoin was **r**eleased on 18 April, 2018, allowing users to store DNS records across a decentralized blockchain. The blockchain was created in response to a bounty thread on the Bitcointalk.org forum. [2] Namecoin supports **.bit TLDs** and is built on top of Bitcoin technology.[3]

2) **Emercoin**- Like Namecoin, Emercoin is a digital currency that supports a decentralized DNS for the **.emc, .lib, .coin, and .bazar** zones.[4] Emercoin launched in 2013 and implemented its DNS in 2014.[5]

Each of these blockchains' functions is built upon more traditional cryptocurrency technology and each blockchain supports traditional cryptocurrency operations. As a result, concepts such as an "address" (a hashed and encoded public key for conducting transactions) and a wallet (a representation of a collection of addresses owned by a single entity) [6] [7] apply to these blockchains and can be used to track and correlate transactions.[8]

Most importantly, **querying a domain registered on the Namecoin or Emercoin systems requires a DNS server specifically configured to read and resolve data hosted on these blockchains**. The most common observed method for doing this is to query an OpenNIC DNS server, as the OpenNIC project supports these TLDs.[9] However, other custom nameservers are occasionally used.[10]

Transactional Mapping

Mapping transactions on the blockchain requires a basic understanding of three concepts:

1. **Addresses**- Transactions on a blockchain revolve around the concept of *addresses*, public keys that have been hashed and encoded. Each public key is paired with a private key belonging to an individual and these keys ensure that only that individual can conduct transactions (such as currency transactions or domain operations) with the cryptocurrency assigned to them.[11]

2. **Blocks**- The term "blockchain" is derived from the mechanism used to append data to the decentralized database. When enough "new" data is accumulated, it is added to the blockchain in chunks. A hash of the previous chunk is included in the new dataset, permanently linking these together.[12]

3. **Change**- A transaction on the blockchain requires that the *entire* amount of the output of a previous transaction be spent when it is used as an input for a new transaction. The amount leftover from a transaction is either sent to a new address (under most software configurations) or sent back to the original address.[13]

Transactions are broken down into "inputs" (the sender) and "outputs" (the receiving addresses). Because Namecoin domain operations require that the user pay a fixed fee, differentiating between the "change" address and the "user" address in the outputs of such a transaction is simplified.

The Namecoin blockchain supports three main types of operations: new domain creation, a domain's first update, and a regular domain update. The following diagram illustrates how an analyst can use the concepts of addresses and change to track a user as they create and update domains on the blockchain:

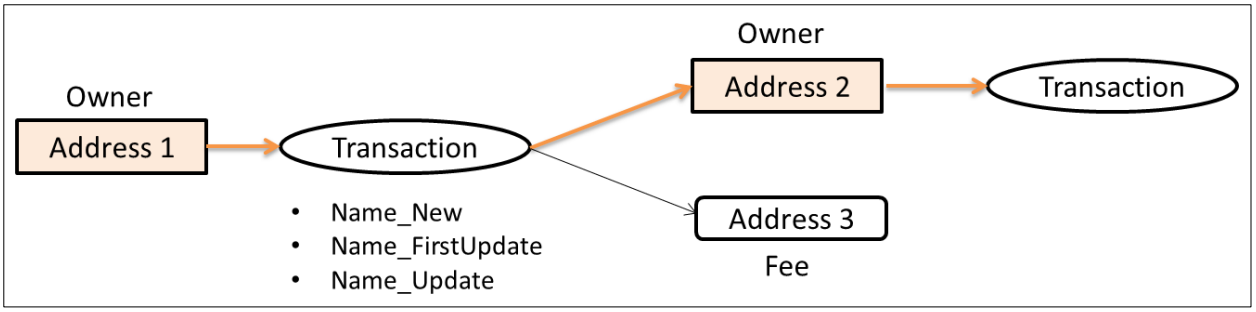



**Figure 1: A series of Namecoin transactions**

In this example, Address 1 is used to conduct an operation (such as creating a new domain). The owner pays a fee, with the leftover amount moving to Address 2, a newly created address assigned to the same individual. This individual may then use Address 2 to conduct another Namecoin operation or to conduct a financial transaction.

Figure 2 demonstrates the application of this analytical method using data taken directly from the Namecoin blockchain. In this example, a threat actor uses a Namecoin transaction to generate a domain later used as a Shifu banking trojan C2 (s3lavaukraine[.]bit, as reported by Palo Alto networks).[14] This figure depicts several items that must be considered in parallel:

- The "input" address of this transaction was previously an "output" address of an operation that updated the IP address for a domain named "healthshop[.]bit."

- The "output" of this slavaukraine transaction is an address that is used to register an additional domain, "klyatiemoskali[.]bit," which is also reported by Palo Alto networks as a Shifu banking trojan C2.

- The Namecoin blockchain serves as a permanent record for all historical IP addresses assigned to these domains and can be used to demonstrate infrastructure overlaps.

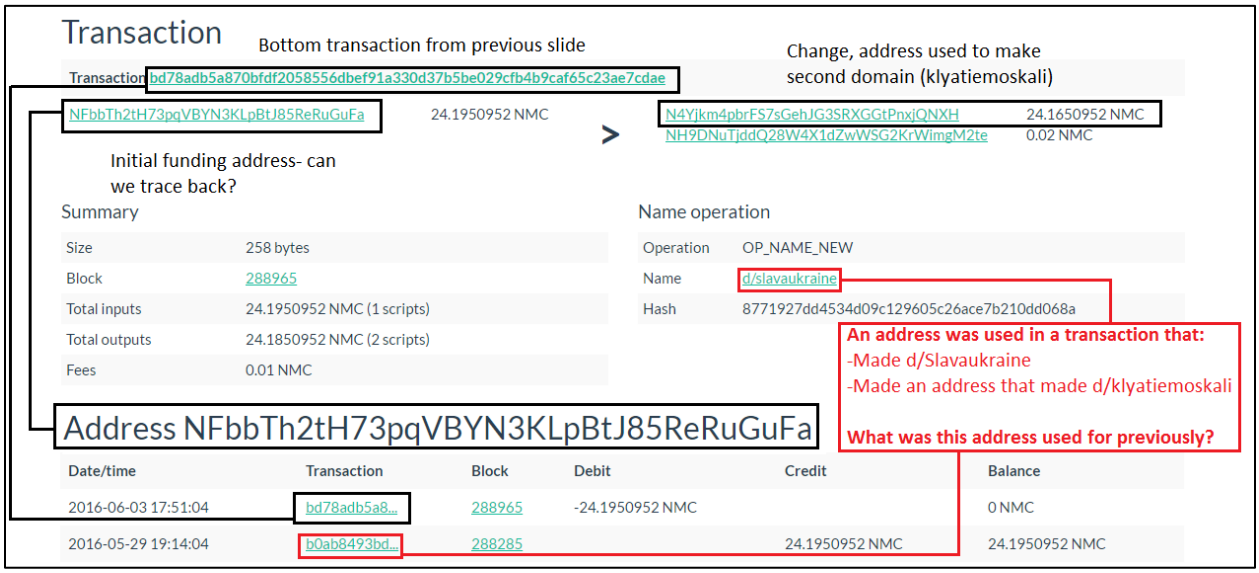



**Figure 2: Examination of a Namecoin transaction used to create a Shifu banking trojan C2**

A side-by-side comparison of two of these domains significantly strengthens the assessment that they belong to the same threat actor, as the domains were often assigned the same IPs on the same dates or resolved to the same IPs within the same timeframe.

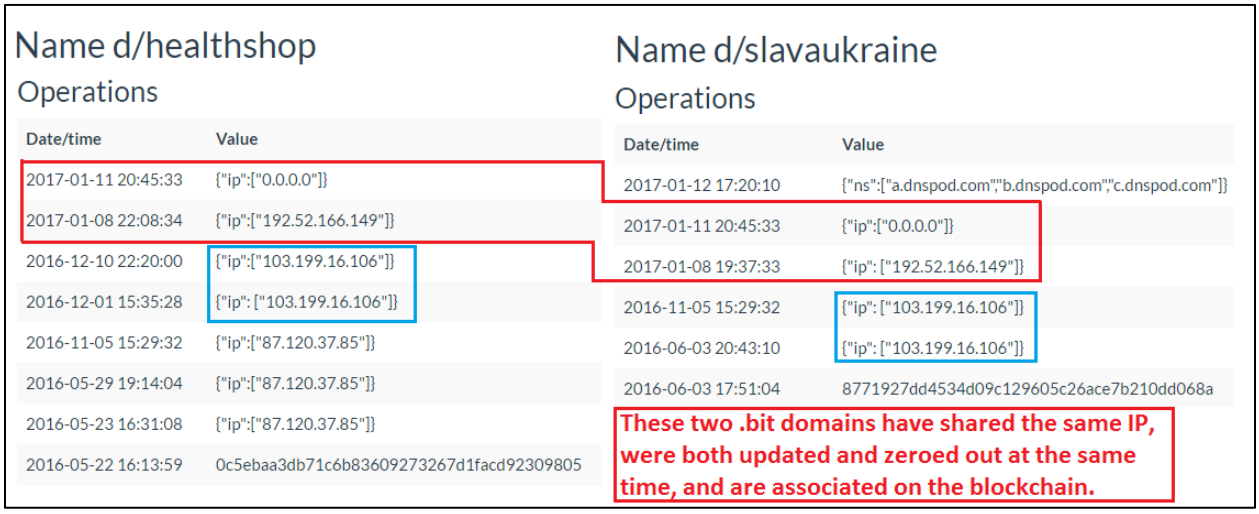



**Figure 3: Side-by-side comparison of healthshop[.]bit and slavaukraine[.]bit**

This technique can be scripted, allowing analysts to scale these data collection and comparison steps. In doing so, over a dozen domains related to this threat can be identified. A full list of these domains is available in the appendix.

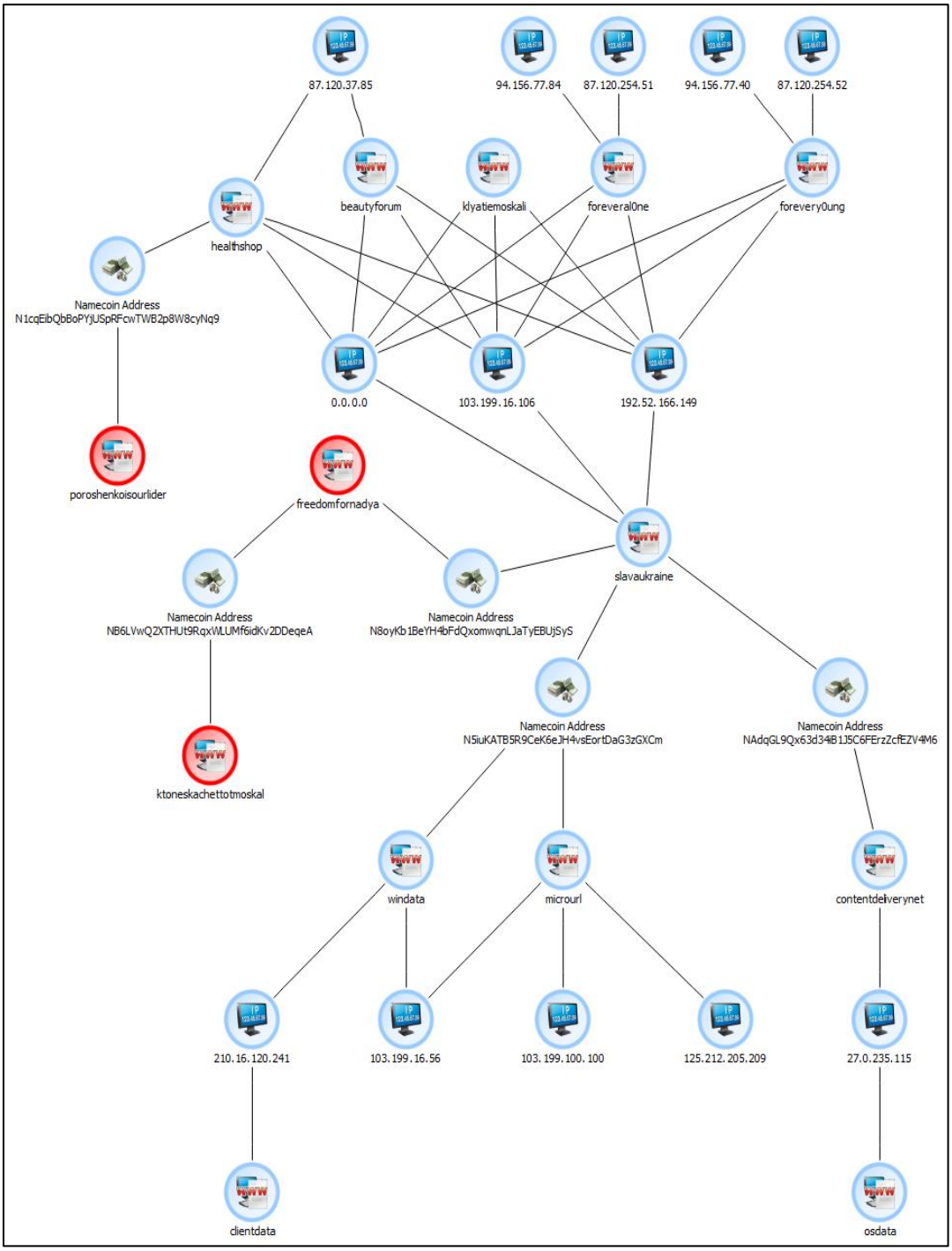



**Figure 4: Infrastructure associated with Shifu banking trojan actors**

Indexing and Pivoting

The above approach serves as a high-confidence mechanism for mapping out infrastructure given the cryptographic relationships necessary to conduct activity on a blockchain; however, this method is cumbersome and requires preexisting knowledge of at least one malicious or suspicious domain.

By **indexing blockchain data using a tool such as Splunk** and combining analytics specific to blockchain technology with traditional pivoting methodologies, an analyst can *proactively* identify malicious domains and leverage Splunk's subsearching features to quickly pivot out to find additional infrastructure. This research primarily uses the following four analytics:

1) Domains with a large number of different historical IP address resolutions.
2) Domains that have operations recorded on a large number of blocks.
3) Domains assigned an unusual or uncommon nameserver.
4) Domains that were created, updated, or modified on the same or nearby block as another malicious domain.

Several of these are derived from a basic principle: it would be atypical for a legitimate user of this technology to be making frequent changes to the IP address resolution for his or her domain, as that would imply a regular changing of infrastructure and would necessitate conducting additional transactions on the blockchain. Put more simply: this would likely be an inconvenience.

Figure 5 highlights several malicious domains that emerge from a Splunk query that uses this metric (there are many valid inputs for such a query, including filtering for unique IPs and filtering out non-IP address entries). This query identified a number of suspicious domains as well as several domains that can quickly be verified as malicious and categorized via OSINT research:

- makron[.]bit (Smoke Loader)[15] [16]
- makronwin[.]bit (Smoke Loader) [17] [18]
- quitsmokings[.]bit (shares infrastructure with Smoke Loader)[19]
- sectools[.]bit (Dimnie) [20] [21]
- vpnvirt[.]bit

A list of infrastructure identified through the pivoting techniques described in this whitepaper is available in the appendix.

| | |
|---|---|
| megashara | 36 |
| bay | 23 |
| makron | 22 |
| bitcoincommodities | 21 |
| makronwin | 20 |
| zexernet | 20 |
| zmanhoodmana | 20 |
| bitshara | 19 |
| satoshidice | 19 |
| generationp | 18 |
| pationare | 18 |
| bitnotes | 17 |
| couchsurfing | 17 |
| levashov | 17 |
| porshegate | 17 |
| quitsmokings | 17 |
| univ | 17 |
| vinik | 17 |
| kuxkux | 15 |
| sectools | 15 |
| weihnachten | 15 |
| bitte-ein | 14 |
| black-market | 14 |
| choosenone | 14 |
| derevo | 14 |
| myblackass | 14 |
| vpnvirt | 14 |
| deltazero | 13 |

**Figure 5: Initial query to identify suspicious domains**

At the time of this research and writing, vpnvirt[.]bit was uncategorized in open source, appearing only in automated sandbox reports as a DNS request. In these sandboxed runs of its parent malware, vpnvirt[.]bit is requested alongside vpnrooter[.]bit, indicating a relationship.[22] Querying for these two domains in the Splunk database presents the user with the IP addresses historically assigned to these domains. These include shared infrastructure and blocks (Figure 6, red) and similar infrastructure (blue).

| block | Domain | DataInput |
|---|---|---|
| 359024 | volstat | 83.243.41.162 |
| 360003 | volstat | 91.191.184.159 |
| 361797 | volstat | 91.191.184.33 |
| 292242 | vpnrooter | 08e1a96c11f141533f9763d32 |
| 292258 | vpnrooter | 185.61.149.70 |
| 298988 | vpnrooter | 185.128.42.237 |
| 299344 | vpnrooter | 91.215.153.31 |
| 306131 | vpnrooter | 213.252.247.94 |
| 309176 | vpnrooter | 185.25.51.25 |
| 317342 | vpnrooter | 213.252.246.115 |
| 323629 | vpnrooter | 185.25.51.221 |
| 344943 | vpnrooter | 185.203.118.168 |
| 346361 | vpnrooter | 173.242.124.228 |
| 350536 | vpnrooter | 103.208.86.122 |
| 353970 | vpnrooter | 185.99.132.51 |
| 354759 | vpnrooter | 169.239.129.25 |
| 292242 | vpnvirt | cdd48b680f6bde040d98bae2 |
| 292254 | vpnvirt | 185.61.149.70 |
| 298988 | vpnvirt | 185.128.42.237 |
| 299344 | vpnvirt | 91.215.153.31 |
| 306131 | vpnvirt | 213.252.247.94 |
| 309186 | vpnvirt | 185.25.51.25 |
| 317342 | vpnvirt | 213.252.246.115 |
| 323637 | vpnvirt | 185.25.51.221 |
| 344943 | vpnvirt | 185.2.82.209 |
| 350536 | vpnvirt | 103.208.86.254 |
| 353970 | vpnvirt | 169.239.129.25 |
| 354759 | vpnvirt | 185.99.132.10 |
| 356512 | vpnvirt | 169.239.129.100 |

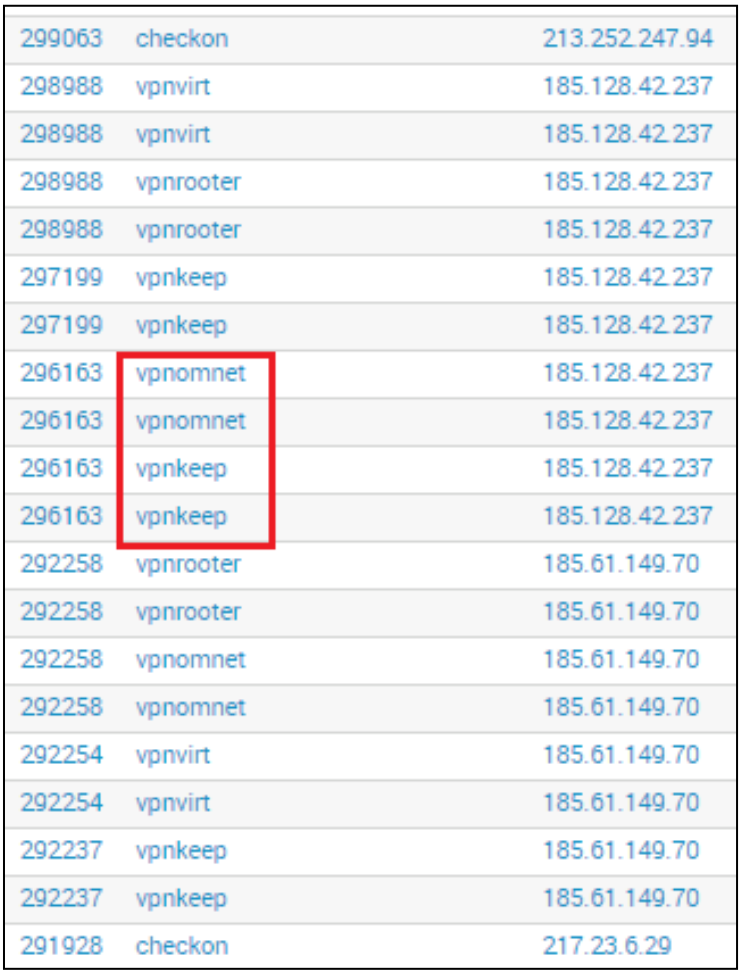
**Figure 6: Pivoting to identify IP addresses for vpnvirt[.]bit and vpnrooter[.]bit**

From this pivot, the following three IPs appear in an open source report titled “Read the Manual” from ESET researchers:[23]

- 185.61.149.70
- 185.128.42.237
- 91.215.153.31

These IP addresses are listed as C2 infrastructure for a malware family referred to as “RTM” (named after a decrypted string found in the malware). This malware is notable for being distributed in narrowly scoped attacks, and is designed to identify and steal information from remote banking and account management software.

As an additional pivoting step, we can strengthen the possibility that the vpnvirt[.]bit and vpnrooter[.]bit domains are associated with this malware by re-inputting (either as a separate query or through a subsearch) the IP addresses historically assigned to these domains. The result of this query will then expand the list of infrastructure to all domains associated with these IP addresses (Figure 7).



| | | |
|---|---|---|
| 299063 | checkon | 213.252.247.94 |
| 298988 | vpnvirt | 185.128.42.237 |
| 298988 | vpnvirt | 185.128.42.237 |
| 298988 | vpnrooter | 185.128.42.237 |
| 298988 | vpnrooter | 185.128.42.237 |
| 297199 | vpnkeep | 185.128.42.237 |
| 297199 | vpnkeep | 185.128.42.237 |
| 296163 | vpnomnet | 185.128.42.237 |
| 296163 | vpnomnet | 185.128.42.237 |
| 296163 | vpnkeep | 185.128.42.237 |
| 296163 | vpnkeep | 185.128.42.237 |
| 292258 | vpnrooter | 185.61.149.70 |
| 292258 | vpnrooter | 185.61.149.70 |
| 292258 | vpnomnet | 185.61.149.70 |
| 292258 | vpnomnet | 185.61.149.70 |
| 292254 | vpnvirt | 185.61.149.70 |
| 292254 | vpnvirt | 185.61.149.70 |
| 292237 | vpnkeep | 185.61.149.70 |
| 292237 | vpnkeep | 185.61.149.70 |
| 291928 | checkon | 217.23.6.29 |

**Figure 7: Additional pivoting**

Two newly identified domains, **vpnomnet[.]bit and vpnkeep[.]bit**, are directly referenced in ESET’s report. In addition, changes to these domains are made in close temporal proximity with the vpnvirt and vpnrooter domains. As a result, analysts can assess with high confidence **that these two domains are related to this threat actor’s activity.**

As an additional step, analysts can reverse engineer the malware communicating with newly discovered domains in order to validate that the same malware family is being used. ESET's "Read the Manual" report highlights several specific technical characteristics for the RTM malware, including:

- A specific export (DllGetClassObject) called to run the malware
- Unique decrypted strings, including "RTM_Module" for which the malware is named
- Unique decrypted configuration fields such as "cc.url.1," "botnet-prefix," and "scan-files"
- A routine that checks window class and title names and compares them to a hardcoded list to identify remote banking and account management software. The malware sets a marker if such software is found.

Figure 8 depicts the decrypted strings identified in memory during manual debugging of the malware. These strings match those described in ESET's report, including the malware's configuration fields.

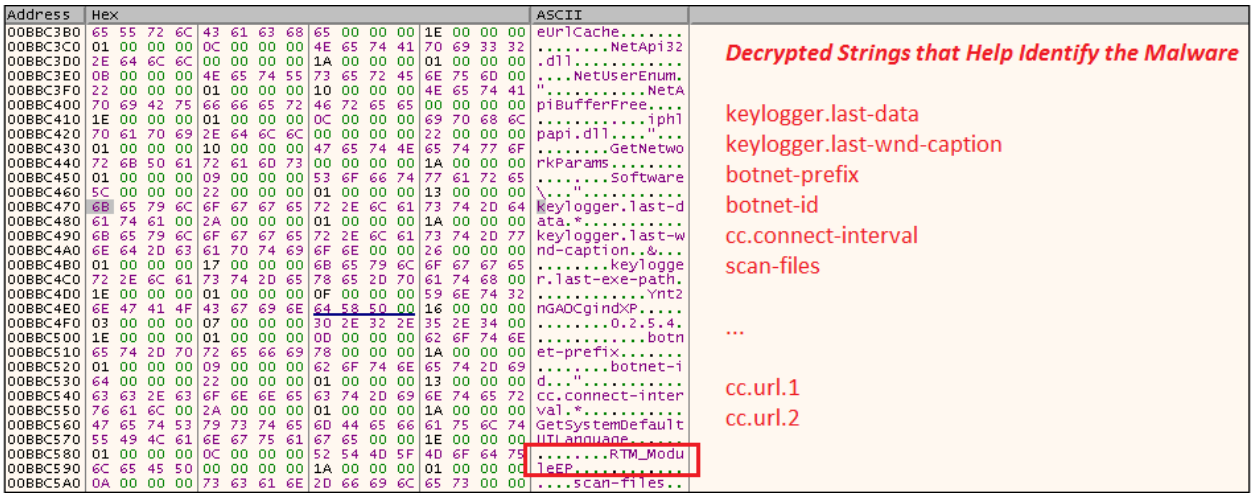



**Figure 8: Decrypted RTM strings**

Figure 9 provides functional validation. In the top code block, the malware attempts to determine whether or not the string "E-Plat" appears in the current window title. E-Plat refers to account and salary management software owned by B&N Bank (БИНБАНК), an Eastern European financial institution.[24] If this software is found, the malware sets a marker for MDM bank (acquired by B&N in 2015/2016 and still referenced in some E-Plat documentation[25]). If not, it jumps to the next check.

This check also aligns with ESET's high-level description of the malware's functionality, providing final validation that the malware identified through this infrastructure pivoting is indeed attributable to the same threat actor group and activities. Notably, ESET's report does not mention the "E-Plat" software as being among the targeted platforms, suggesting that the threat actors may have updated their malware to target new software.

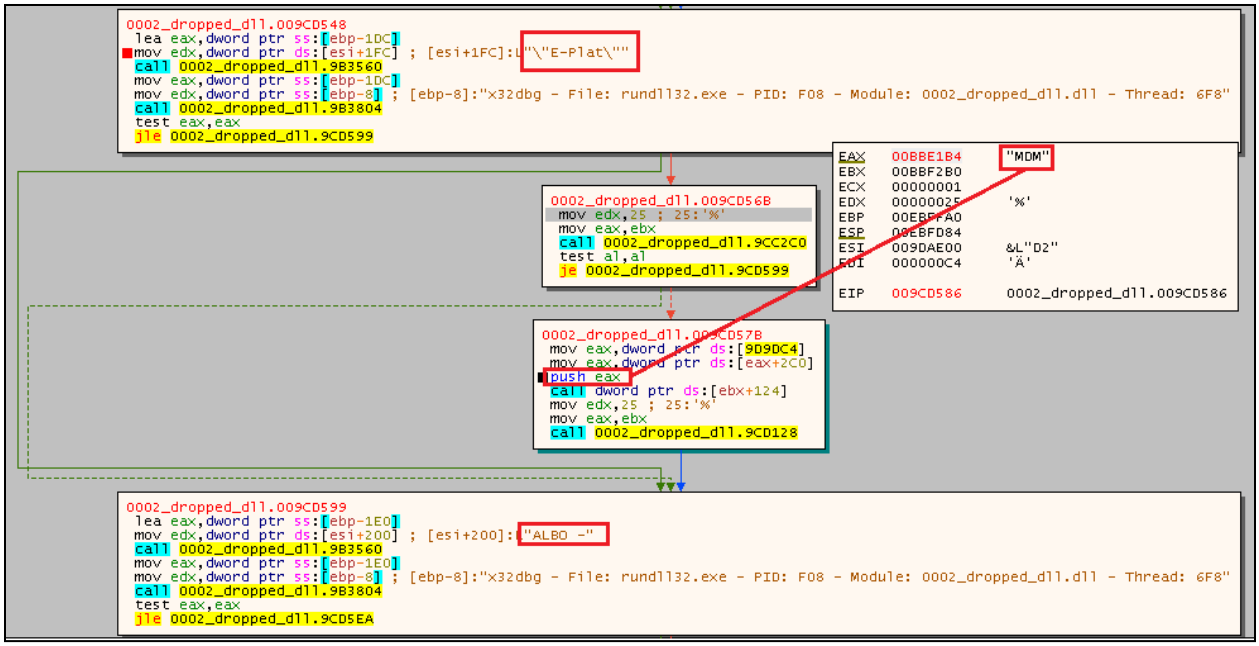



**Figure 9: Software check performed by RTM malware (note that a jump to the "successful" check was forced to generate the condition needed to place the "MDM" marker in the EAX register).**

During reverse engineering, one additional notable characteristic was identified. While the malware will make DNS requests using OpenNIC servers, it will also make a direct GET request to a domain's page on Namecha[.]in, a public Namecoin blockchain database. The malware will pull down the most recent IP address for the domain and use this in place of DNS resolution should traditional mechanisms be unavailable.

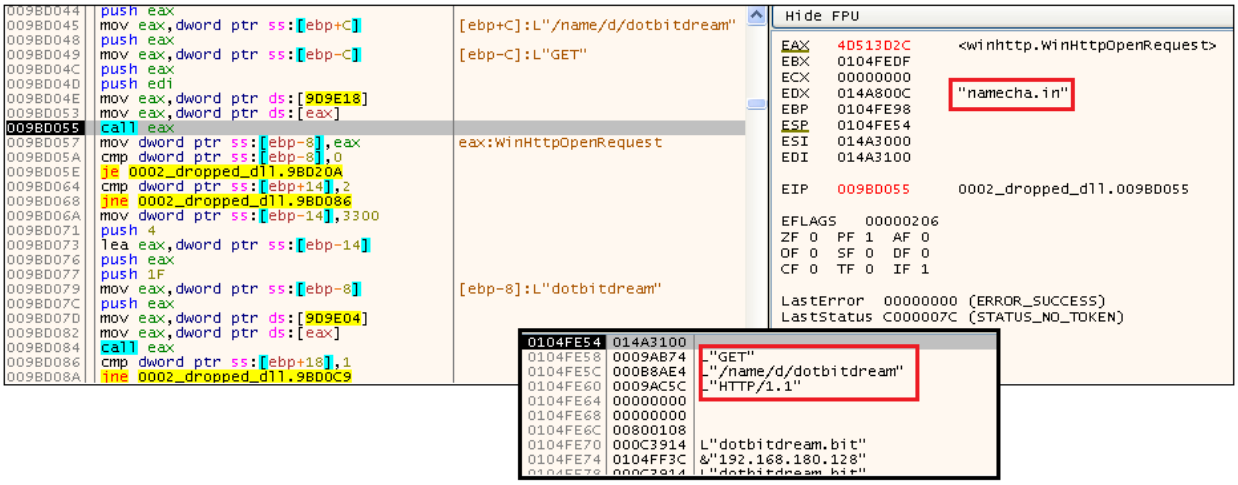



**Figure 10: GET request to Namecha[.]in to resolve the IP for an RTM C2**

*Emercoin*

These pivoting techniques are also applicable to the Emercoin blockchain. For example, pivoting using Jstash[.]bazar (a well-known domain for the Jokerstash carding website) leads to several related domains and IP addresses:

- 185.61.137.166
- 185.61.137.177
- 185.62.190.164
- 190.115.27.130
- cvv[.]bazar
- cvv2[.]bazar
- dumps[.]bazar
- j-stash[.]bazar
- joker-stash[.]bazar
- jokerstash[.]bazar
- stash[.]bazar
- track2[.]bazar

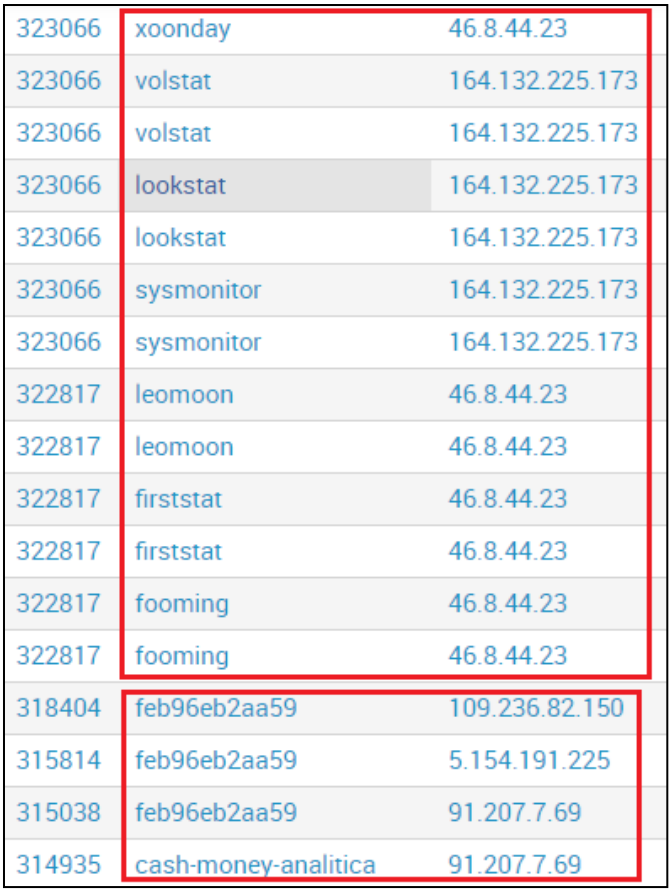
Similarly, the Neutrino C2 "brownsloboz"[26] appears on both blockchains with multiple registered TLDs. By using the IP addresses from one blockchain, an analyst can pivot *across* indexed blockchains through a Splunk subsearch, revealing the following infrastructure:

- 46.183.218.42
- 185.234.216.58
- brownsloboz[.]bit
- weare[.]bit
- porfavor[.]bit
- brownsloboz[.]bazar
- brownsloboz[.]lib
- brownsloboz[.]emc

Analytical Limitations

*Expired Infrastructure*

Whereas the transactional analysis method provides reactive but cryptographically-backed results leading to high-confidence infrastructure relationships, the infrastructure mapping methodology provides faster results and easier pivoting; however, it has analytical limitations. As an example, mapping out infrastructure related to cash-money-analitica[.]bit, an additional ESET-identified RTM C2, leads to several additional domains:

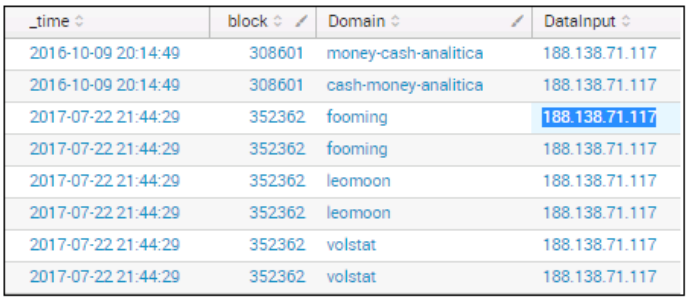


| | | |
|---|---|---|
| 323066 | xoonday | 46.8.44.23 |
| 323066 | volstat | 164.132.225.173 |
| 323066 | volstat | 164.132.225.173 |
| 323066 | lookstat | 164.132.225.173 |
| 323066 | lookstat | 164.132.225.173 |
| 323066 | sysmonitor | 164.132.225.173 |
| 323066 | sysmonitor | 164.132.225.173 |
| 322817 | leomoon | 46.8.44.23 |
| 322817 | leomoon | 46.8.44.23 |
| 322817 | firststat | 46.8.44.23 |
| 322817 | firststat | 46.8.44.23 |
| 322817 | fooming | 46.8.44.23 |
| 322817 | fooming | 46.8.44.23 |
| 318404 | feb96eb2aa59 | 109.236.82.150 |
| 315814 | feb96eb2aa59 | 5.154.191.225 |
| 315038 | feb96eb2aa59 | 91.207.7.69 |
| 314935 | cash-money-analitica | 91.207.7.69 |

**Figure 11: Domains identified by pivoting using cash-money-analitica[.]bit**

One of these domains, feb96eb2aa59[.]bit, is cited by ESET researchers as an RTM C2. However, further analysis (using a Splunk "values" statistical transformation) indicates that the other domains only have a single IP address overlap with these RTM C2s, along with a one-year gap between when each cluster was assigned this IP address (Figure 9).

| | | |
|---|---|---|
| 185.151.245.34 | fooming<br>xoonday | |
| 185.169.229.42 | cash-money-analitica<br>money-cash-analitica | |
| 185.212.128.146 | leomoon | |
| 185.43.223.28 | leomoon | |
| 188.116.40.44 | firststat<br>leomoon<br>testikname<br>volstat | |
| 188.138.71.117 | cash-money-analitica<br>fooming<br>leomoon<br>money-cash-analitica<br>volstat | 308601<br>352362 |
| 193.242.211.137 | fooming<br>leomoon<br>lookstat<br>xoonday | |



| _time | block | Domain | DataInput |
|---|---|---|---|
| 2016-10-09 20:14:49 | 308601 | money-cash-analitica | 188.138.71.117 |
| 2016-10-09 20:14:49 | 308601 | cash-money-analitica | 188.138.71.117 |
| 2017-07-22 21:44:29 | 352362 | fooming | 188.138.71.117 |
| 2017-07-22 21:44:29 | 352362 | fooming | 188.138.71.117 |
| 2017-07-22 21:44:29 | 352362 | leomoon | 188.138.71.117 |
| 2017-07-22 21:44:29 | 352362 | leomoon | 188.138.71.117 |
| 2017-07-22 21:44:29 | 352362 | volstat | 188.138.71.117 |
| 2017-07-22 21:44:29 | 352362 | volstat | 188.138.71.117 |

**Figure 9: Additional analysis on cash-money-analitica[.]bit infrastructure relationships**

OSINT reporting from FireEye researchers associates domains in this additional cluster (such as xoonday[.]bit and volstat[.]bit) with a malware family tracked as CHESSYLITE.[27] Reverse engineering and analysis of a malware sample communicating with these domains[28] indicates that it contains a SOCKS5 module common to several other malware families and that the malware will eventually attempt brute force logins to several APIs using a hardcoded dictionary of stolen credentials.

Given the limited direct and temporal overlaps with the known RTM C2s and this clear difference in functionality, it is likely that these domains are unrelated to the RTM malware or threat actors. Most importantly, this example demonstrates that each additional "layer" of pivoting lowers the confidence level of infrastructure relationships in the absence of additional corroborating data and analysis.

*Nameserver Delegation*

In some cases, threat actors add an NS record in lieu of an IP address when configuring their infrastructure. For example, the Gandcrab C2 "nomoreransom[.]bit"[29] is assigned "dns1[.]soprodns[.]ru" and "dns2[.]soprodns[.]ru" without an IP address. This prevents an analyst from easily identifying and blocking an IP address associated with this malware. Possible solutions to this obstacle include:

- A daily script that performs an DNS query to these name servers to identify and index these IPs
- Parsing PCAP data from blogs that regularly track these threats, such as Malware-Traffic-Analysis[30]

In addition, the use of more unique nameservers can itself expose additional infrastructure. The following domains use a "soprodns" nameserver:

- esetnod32[.]bit
- nomoreransom[.]bit
- emsisoft[.]bit
- gandcrab[.]bit
- bleepingcomputer[.]bit
- kimchenin[.]bit
- spinner[.]bit
- xylibox[.]bit
- sophos[.]bit
- mitnicksecurity[.]bit
- cryptoinsane[.]bit
- securityweekly[.]bit
- darkreading[.]bit

Several of these are widely reported Gandcrab ransomware C2s; of the others, several are also named after security companies, researchers, or publications, suggesting that they may also be related.

**Conclusions**

In recent years, several malware families have adopted decentralized infrastructure to create takedown-resistant domains. This paper has highlighted how analysts can use several characteristics of blockchain technology to map out and identify suspicious or malicious domains and nameservers. These include using the cryptographic nature of blockchain transactions to create high-confidence relationships as well as leveraging pivoting techniques against an indexed dataset. In addition to these more CTI-oriented techniques, analysts can also monitor for DNS queries to non-standard nameservers, including OpenNIC IP addresses, as a potential indicator of anomalous activity.

## Appendix: Selected Clusters

Note: These lists *do not* include the time ranges for when this infrastructure was active. Researchers are encouraged to visit Namecha[.]in to query domains for this information.

**Dimnie**[31] [32] [33]

- avtotransltd[.]bit
- bitmakler[.]bit
- coinsolutions[.]bit
- cryptobase[.]bit
- generationp[.]bit
- gosmos[.]bit
- investorshub[.]bit
- newmotors[.]bit
- oneindexers[.]bit
- oxfordcontractors[.]bit
- porshegate[.]bit
- sonygame[.]bit
- worldmed[.]bit
- 103.208.86.10
- 103.208.86.172
- 103.208.86.205
- 103.208.86.219
- 103.208.86.224
- 103.208.86.3
- 103.208.86.57
- 103.208.86.65
- 104.193.8.12
- 107.181.187.39
- 109.201.142.101
- 109.201.148.85
- 162.213.26.82
- 185.147.34.78
- 185.25.51.177
- 185.61.149.159
- 185.82.217.156
- 185.82.218.111
- 185.82.219.105
- 185.99.132.11
- 185.99.132.110
- 185.99.132.45
- 192.99.81.69
- 195.123.214.74
- 195.123.216.23
- 195.123.217.227
- 195.123.218.177
- 195.123.224.193
- 195.123.224.83
- 195.123.224.87
- 195.123.225.28
- 195.123.233.138
- 195.123.233.150
- 195.123.233.162
- 195.123.233.173
- 195.123.233.180
- 195.123.233.229
- 195.123.233.243
- 199.115.228.44
- 199.168.139.214
- 5.34.183.254
- 86.106.131.71
- 87.120.37.42
- 87.121.52.185
- 92.87.236.203

**Shifu**

- microurl[.]bit
- beautyforum[.]bit
- healthshop[.]bit
- windata[.]bit
- foreveral0ne[.]bit
- forevery0ung[.]bit
- klyatiemoskali[.]bit
- slavaukraine[.]bit
- contentdeliverynet[.]bit
- osdata[.]bit
- clientdata[.]bit
- 125.212.205[.]209
- 103.199.16.56
- 87.120.37.85
- 87.120.254.51
- 87.120.254.52
- 103.199.16.106
- 94.156.77.40
- 94.156.77.84
- 210.16.120.241
- 103.199.100.100
- 27.0.235.115
- 192.52.166.149

**RTM**

*Mail-RU Cluster (associated with **active** RTM domains at the time of this publication)*

- 149.202.30.7
- 185.82.219.79
- 195.123.217.232
- 195.123.217.242
- 195.123.225.58
- 5.149.255.199
- 5.149.255.217
- 54.38.49.245
- mail-ru-stat[.]bit
- mail-ru-stat-cdn[.]bit
- mail-ru-stat-counter[.]bit
- mail-ru-stat-counter-cdn[.]bit

*fde05d0573da Cluster*

- 109.248.32.149
- 109.248.32.152
- 138.201.104.161
- 154.70.153.125
- 158.255.208.197
- 158.255.6.150
- 178.208.91.222
- 185.117.88.123
- 185.117.89.112
- 185.141.25.167
- 185.82.201.45
- 212.48.90.155
- 213.184.127.137
- 5.149.248.164
- 5.154.190.153
- 5.154.190.167
- 5.154.190.168
- 5.154.190.189
- 5.154.191.154
- 5.154.191.174
- 5.154.191.244
- 5.154.191.246
- 50.7.115.64
- 81.19.82.8
- 85.25.41.84
- 86.110.117.5
- 86.110.117.6
- 95.183.52.182
- b9d0f3a3[.]bit
- d47ea26b7faa[.]bit
- dotbitdream[.]bit
- f06f77c950a9cf20c[.]bit
- fde05d0573da[.]bit
- hfh4795hdsk[.]bit
- ltst0105xht0[.]bit
- onewayticket[.]bit

*VPN Cluster*

- 103.208.86.122
- 103.208.86.158
- 103.208.86.254
- 142.0.33.15
- 169.239.129.100
- 169.239.129.25
- 173.242.124.228
- 185.128.42.237
- 185.2.82.209
- 185.203.118.168
- 185.25.51.221
- 185.25.51.25
- 185.61.149.70
- 185.99.132.10
- 185.99.132.51
- 199.180.119.19
- 199.180.119.20
- 213.252.246.115
- 213.252.247.94
- 217.23.6.29
- 91.215.153.31
- applerok[.]bit
- bigleon[.]bit
- checkon[.]bit
- djslon[.]bit
- vpnkeep[.]bit
- vpnomnet[.]bit
- vpnrooter[.]bit
- vpnvirt[.]bit

*Analitica Cluster*

- 131.72.138.169
- 185.141.27.249
- 185.169.229.42
- 188.138.71.117
- 200.74.240.134
- 200.74.240.80
- 37.1.206.78
- 5.154.191.57
- 91.207.7.69
- 93.170.168.218
- 93.190.139.66
- cash-money-analitica[.]bit
- money-cash-analitica[.]bit

[1] https://www.welivesecurity.com/wp-content/uploads/2017/02/Read-The-Manual.pdf
[2] https://bitcointalk.org/index.php?topic=6017
[3] https://bit.namecoin.org/
[4] https://peername.com/emercoin/
[5] https://emercoin.com/en/road-map
[6] https://blockgeeks.com/guides/blockchain-address-101/
[7] https://bitcoin.stackexchange.com/questions/13059/whats-the-difference-between-a-wallet-and-an-address
[8] https://www.sans.org/summit-archives/file/summit-archive-1498165491.pdf
[9] https://www.opennic.org/
[10] https://researchcenter.paloaltonetworks.com/2017/01/unit42-2016-updates-shifu-banking-trojan/
[11] https://blockgeeks.com/guides/blockchain-address-101/
[12] https://blockgeeks.com/guides/what-is-hashing/
[13] https://en.bitcoin.it/wiki/Change
[14] https://researchcenter.paloaltonetworks.com/2017/01/unit42-2016-updates-shifu-banking-trojan/
[15] https://cloudblogs.microsoft.com/microsoftsecure/2018/04/04/hunting-down-dofoil-with-windows-defender-atp/
[16] https://www.hybrid-analysis.com/sample/b75ee6221a09097bde66e5668f6a74c7a968d247b084a339d2a5a2921f41c702?environmentId=100
[17] https://cloudblogs.microsoft.com/microsoftsecure/2018/04/04/hunting-down-dofoil-with-windows-defender-atp/
[18] https://www.hybrid-analysis.com/sample/b75ee6221a09097bde66e5668f6a74c7a968d247b084a339d2a5a2921f41c702?environmentId=100
[19] https://www.malware-traffic-analysis.net/2017/11/02/index.html
[20] https://researchcenter.paloaltonetworks.com/2017/03/unit42-dimnie-hiding-plain-sight/
[21] https://www.hybrid-analysis.com/sample/a8ba70be73578d901c5e2427fd2f63e06801dcba8726a82f1875d84ba147aaa3/58a56f1faac2edca060d6cde
[22] https://www.reverse.it/sample/cfa9e166e70ca46abd21bd7a30e5569bed7e0b22107d6f2a3bbff097b3891e06?environmentId=100
[23] https://www.welivesecurity.com/wp-content/uploads/2017/02/Read-The-Manual.pdf
[24] https://www.binbank.ru/corporate-clients/dbo/eplat/
[25] https://eng.binbank.ru/news/binbank-news/44812/
[26] https://www.fireeye.com/blog/threat-research/2018/04/cryptocurrencies-cyber-crime-blockchain-infrastructure-use.html
[27] https://www.fireeye.com/blog/threat-research/2018/04/cryptocurrencies-cyber-crime-blockchain-infrastructure-use.html
[28] https://www.hybrid-analysis.com/sample/68c746df7df35b3379a4d679fc210abdb2032b3c076ec51a463abe1e0e18345f?environmentId=100
[29] https://www.symantec.com/security-center/writeup/2018-013106-5656-99
[30] https://www.malware-traffic-analysis.net/2018/01/29/index.html
[31] https://researchcenter.paloaltonetworks.com/2017/03/unit42-dimnie-hiding-plain-sight/
[32] https://habr.com/company/bizone/blog/351122/
[33] https://securelist.ru/trojan-dimnie-and-ransomware-purga/90272/