



# RTM: SINK-HOLING THE BOTNET

# WHO WE ARE



**Semyon Rogachev**  
Malware analyst

- 4+ years in malware analysis and incident response
- Strong skills in reverse engineering
- Author and co-author of Group-IB ransomware reports



**Rustam Mirkasymov**  
Threat Intelligence analyst

- 8 years in cyber threat research and threat intelligence
- Strong skills in reverse engineering, knowledge in exploit development and understanding software vulnerabilities mechanisms
- Author / co-author of numerous APT threat reports (including Lazarus, Silence, Cobalt, Moneytaker, RedCurl.)

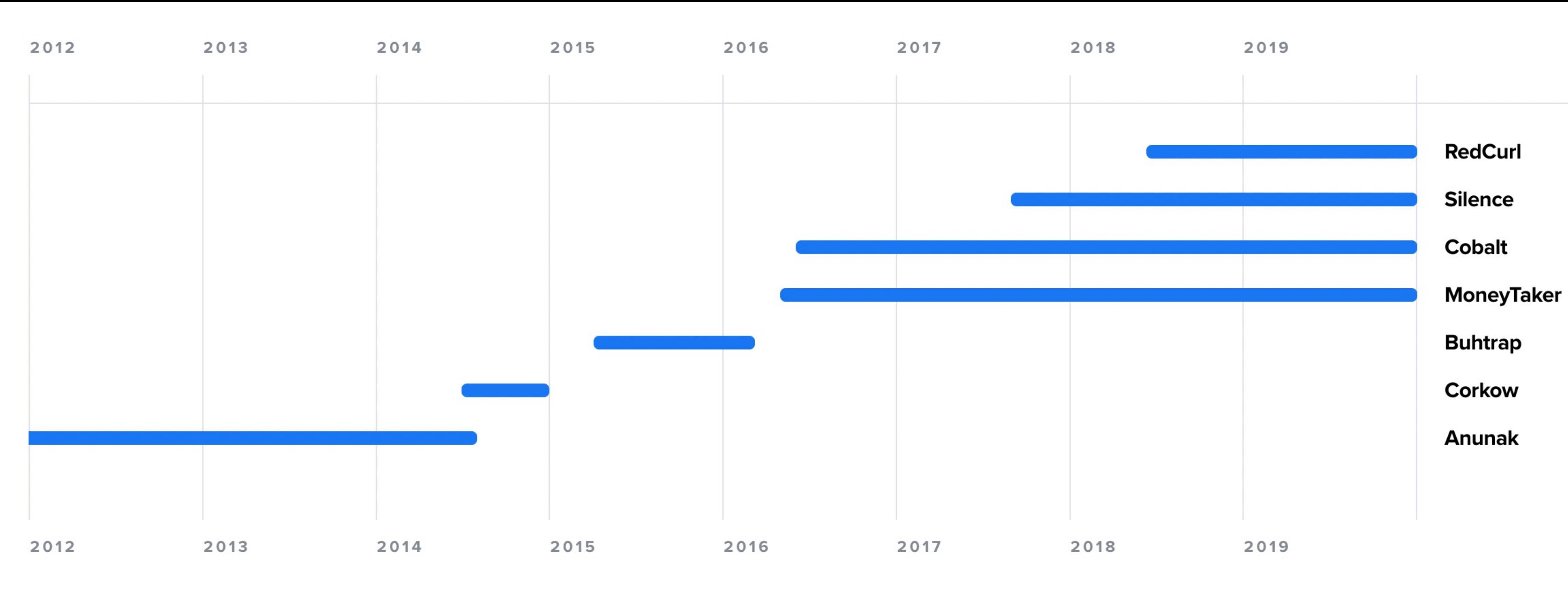


Twitter: @Ta1ien

# GROUPS EVOLUTION

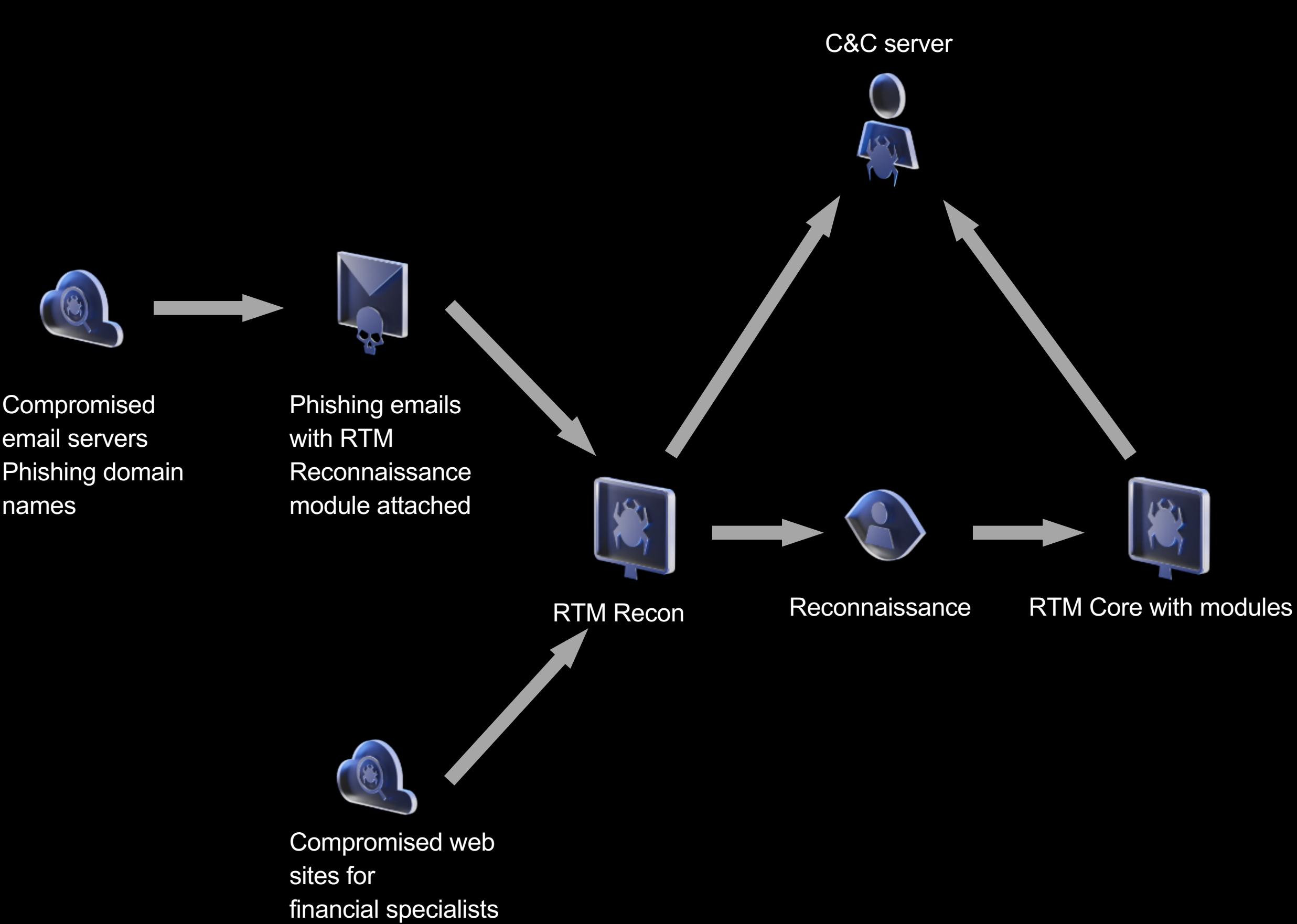


Most of banking hacking groups in 2008-2017 were Russian speaking.





# RTM ATTACK OVERVIEW



## FIRST STAGE – RECONNAISSANCE MODULE

Phishing emails contain a reconnaissance module, which checks if any indicators of financial activity is presented on the infected host.

## SECOND STAGE – RTM CORE

If indicators of the financial activity were found, RTM core module is downloaded from the C2 server. In other case some common malware, like Pony Stealer is downloaded.

## THIRD STAGE – RTM MODULES

RTM Core collects additional information about the infected host, downloads and executes modules, which are used for the network reconnaissance, lateral movement and money stealing.

# FIRST STAGE - RECONNAISSANCE



RTM Reconnaissance module checks browser history to find traces of the following remote banking services:



## SBERBANK

sbi.sberbank  
online.sberbank  
bps-sber



## VTB

bco.vtb24.ru  
dbo.vtb  
bco.vtv.24



## ALFABANK

link.alfabank  
click.alfabank  
ibank.alfa-bank.by



## RAIFFEISEN

elba.raiffeisen  
elbrus.Raiffeisen



## BLOCKCHAIN.INFO

blockchain.info



## WESTERNUNION

wupos.westernunion

# FIRST STAGE - RECONNAISSANCE



RTM Reconnaissance module checks file system to find the traces of the following financial software:



1C

1cv7.exe  
1cv7l.exe  
1cv8.exe



SBERBANK

wclnt.exe



FTC GPK CRYPTOPROVIDER

\_ftcgpk.exe



WEBMONEY

webmoney.exe



CRYPTO WALLETS

wallet.dat  
wallet.dll



QIWI

qiwickashier.exe

# SECOND STAGE – CORE MODULE



After reconnaissance module acquired and run RTM Core, it is capable of execution of the following commands:

Command	Description	Command	Description
del-module	Uninstalls module	hosts-clear	Removes all records from the hosts file
find-files	Scans filesystem for the specified file	cfg-set-*	Commands to manipulate RTM settings
download	Uploads a specified file to the C&C	screenshot	Creates a screenshot every 5 seconds
unload	Closes main window of the RTM	dns	Gets/sets DNS servers via the WMI
uninstall	Stops all activities and removes itself	auto-elevate	UAC bypass
uninstall-lock	Erases MBR, removes itself	reload	Restarts the RTM
shutdown	Shutdowns infected host	cc	Sets new C&C address
reboot	Reboots infected host	get-cc	Sends the list of the C&C addresses
hosts-add	Adds records to the hosts file	botnet-id	Sets new bot ID

# SECOND STAGE – CORE MODULE



After reconnaissance module acquired and run RTM Core, it is capable of execution of the following commands:

Command	Description
prefix	Sets new bot prefix
connect-interval	Sets pause between C&C communications
dbo-scan	Scan for using banking services
kill-process	Terminates specified process
video-process	Starts a video recording thread
video-stop	Stops a video recording thread
msg	Shows a message box



# THIRD STAGE – RTM MODULES



At the third stage additional modules are used. During the tracking of the RTM group, the following modules were detected:

Module name	Module name	Module name
1c_2_kl	chrome_hst	persist
445scan	lpewnd	pony
alfa_scan	domain	proc_lock
anti_mse	ffa	rdp
arp_scan	flash_grab	lpe_evtvwr
bdata	lock_ie	mimi
bss_hide	inj_phone	prc_list
chrome_pw	mitm	stealer

# TYPICAL ATTACK SCHEMES



The screenshot shows a window titled "Платежное поручение (исходящее): Оплата поставщику. Новый \*". The main area contains fields for "Вид операции" (Payment to supplier), "Номер" (Number) set to "27.08.2016 0:00:00", "Оплачено" (Paid) set to "27.08.2016 0:00:00", "Учитывать КПН" (Include KPN), "Вид учета НУ" (Type of accounting NU), "Организация" (Organization) set to "ТОО \"Радуга\"", "Банковский счет" (Bank account) set to "Основной счет", "Счет учета (БУ)" (Accounting account (BU)) set to "1030", "Получатель" (Recipient) set to "ТОО \"Строитель\"", "Счет получателя" (Recipient account) set to "KZ896201369250KZ21489 в АО \"Банк \"Астаны\"", and "Сумма" (Amount) set to "100 000,00" KZT. Below this is a table with columns: N, Договор (Contract), Документ расчетов (Document of calculation), Сумма платежа (Amount of payment), Курс взаиморасчетов (Exchange rate), Сумма взаиморасчетов (Amount of mutual calculation), % НДС (VAT %), Сумма НДС (VAT amount), and Статья Д (Article D). A row is selected with the text "Без договора" (Without contract) and "Договор №1 от 06.01.2016 г." (Contract No. 1 dated 06.01.2016). At the bottom, there are buttons for "Заполнить >>" (Fill in) and "Комментарий:" (Comment:).

## RDP OR TEAMVIEWER

The most frequently seen attack scheme nowadays. Modified version of the TeamViewer is uploaded to the infected host, which allows to transfer money directly, for example, via the browser.

## 1C\_2\_KL MODULE

Used to be frequently used method, but almost gone right now. Modifies the 1C banking software process to modify the 1c\_2\_kl.txt file, which stores the payment data.

## RANSOMWARE

Following the modern trends, RTM is capable of deploying a ransomware. During our monitoring of the RTM activity, at least 4 different were deployed on the compromised machines.

# C&C ADDRESS COMPUTATION



LiveJournal «f72bba81c921.livejournal.com»

[<botnet-id>]<encrypted C&C address>[/<botnet-id>]

The screenshot shows a LiveJournal blog entry titled "f72bba81c921". The entry has a timestamp of "November 4th, 2015, 10:32 pm" and contains several lines of text, each enclosed in brackets. The first line starts with "1" followed by a long string of characters. Subsequent lines are also enclosed in brackets and appear to be parts of the same message or command.

```
[40]1141dde22c5eed944fe46db3c65a272e8e9d843f2f05c51be4ae392003bd4293dd64825a4ba8effb18a288fb4134c3d6437dd527c32551f25ede[40]
[41]804414096c952cb7ed94ab09cb18df7e5f24ce4c61c42c19db11942df38ee8621d844b8b2ae109a7dfa7a606701e54f90d6fef7ba57e270691fd[41]
[30]2328531022a1e8889981282eb32b887ac9d4918b9aa808dee7c47df03cac64019210f272f38224efd505cb1b9e10428392638faf6d28bfc18a2bbfc3f8c1381c872a60cd30e2937bd0c6302abd59ea3270db9c4c3fe6[30]
[31]9134895538b460bcba66a97a07359319c942419d59c2b3986caea06090a08494174a8c73db7e547beb3e71909ed73187c6eb29669d42b9f4edfb2cd524b266d7d7a3e572c0f6f2f4e284ce7263ee93aca28d6b05e0ed[31]
[1]9efc08e5bd3e58df11b6dc74a50218d0374494c32b15445093d11c82e1960f12ae6846219aaf3af0da0dd8b6b5a6df37748c47b9c268a01d[1]
```

<http://f72bba81c921.livejournal.com/data/rss>

## LIVEJOURNAL

First tracked versions of the RTM used LIVEJOURNAL blogs to store the C&C addresses.

## .BIT DOMAINS

Newer versions of the RTM .bit domains as addresses of the C&C servers. .bit domain IP addresses are stored using the Namecoin technology.

## BITCOIN WALLET

The newest versions of the RTM compute C&C server address using the transactions data of the exact Bitcoin wallet.

# BITCOIN BASED ALGORITHM



**RECON:** 1BkeGqpo8M5KNVYXW3obmQt1R58zXAqLBQ

**CORE:** 1CeLgFDu917tgtunhJZ6BA2YdR559Boy9Y



## BLOCKCYpher API

Blockcypher API is leveraged to obtain an information about the transactions of the exact wallet.

## C&C ADDRESS IN TRANSACTION VALUE

After obtaining of the transaction information, RTM extracts the value of the last 2 transactions and interprets it as an IP address octets.

## NO ADDITIONAL TRANSACTIONS DATA CHECK

RTM hasn't been checking which wallet the currency was received from, which made it possible to sinkhole the botnet.

# BITCOIN BASED ALGORITHM



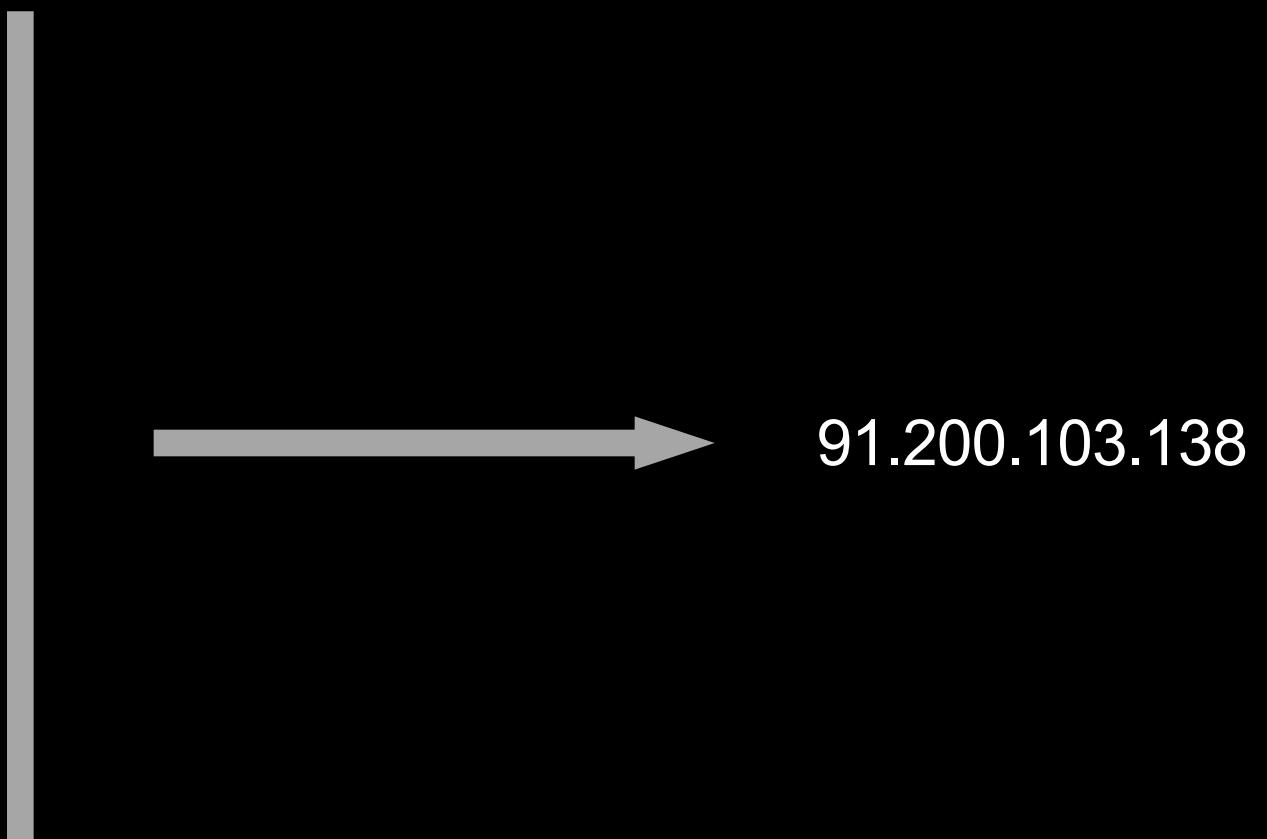
Examples for better understanding

53

```
tx_hash      "6bbfa5406e741cee44ac2c0b1ecfcf1f3f5bb1ed3ed3678a8a05df8532399820"  
block_height 606417  
tx_input_n   -1  
tx_output_n  0  
value        35431 → 0x8A67 → 103.138  
ref_balance  86722  
spent        true  
spent_by     "ad881d022f54180c08ae19078398d65cad38af8078ab6d7bd8c415a6d0ffa929"  
confirmations 126514  
confirmed    "2019-12-03T07:30:57Z"  
double_spend false
```

54

```
tx_hash      "d27ae2c99e96aa9883f156a2af536ab3f1a69f0821cf8525d5f20fcb389cd861"  
block_height 606415  
tx_input_n   -1  
tx_output_n  0  
value        51291 → 0xC85B → 91.200  
ref_balance  51291  
spent        true  
spent_by     "ad881d022f54180c08ae19078398d65cad38af8078ab6d7bd8c415a6d0ffa929"  
confirmations 126516  
confirmed    "2019-12-03T07:15:26Z"  
double_spend false
```



# BITCOIN BASED ALGORITHM



Examples for better understanding: 5<sup>th</sup> December

Fee	0.00002373 BTC (10.500 sat/B - 2.625 sat/WU - 226 bytes)	+0.00035431 BTC
Hash	8ced96b2dc00df9504830303bdd030e8497c97ffc661a7f90fa245b53819570b <a href="#">1DmgXb4oESRsvz641nozM9tR76M1qrBffL</a>	2019-12-05 15:29
	0.00413675 BTC	0.00035431 BTC 0.00375871 BTC
	1CeLgFDu917tgtunhJZ6BA2YdR559Boy9Y <a href="#">1GnimRmFztsJKqeQW8PXCUfzA2ZoaGXq9v</a>	
Fee	0.00003300 BTC (14.602 sat/B - 3.650 sat/WU - 226 bytes)	+0.00051291 BTC
Hash	464a01786f783c8aa9f5f360ee377f3f2f5dfef2261b86cb2c4ac2fe63c0b59 <a href="#">1MPJYJa1knZwVTnmurUnyWZkR7viPNbKjE</a>	2019-12-05 15:27
	0.00468266 BTC	0.00051291 BTC 0.00413675 BTC
	1CeLgFDu917tgtunhJZ6BA2YdR559Boy9Y <a href="#">1DmgXb4oESRsvz641nozM9tR76M1qrBffL</a>	

91.200.103.138

# TRACKING C&CS



```
14
15     BLOCKCHAIN_INFO_URL = "https://api.blockcypher.com/v1/btc/main/addrs/"
16
17
18 ► def blockchain_info_request(blockchain_addr): ...
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37 ► def get_incoming_transactions_list(transactions_json): ...
38
39
40
41
42
43
44
45 ► def get_transactions_till_specific(transactions_list, specific_tx_hash): ...
46
47
48
49
50
51
52
53
54 ► def parse_transactions_json_file(jsonfilename): ...
55
56
57
58
59
60 def get_ips_from_bchain(blockchain_addr):
61     return parse_incoming_trans_json_data(blockchain_info_request(blockchain_addr))
62
63
64 ▼ def parse_incoming_trans_json_data(json_data):
65     incoming_transactions = get_incoming_transactions_list(json.loads(json_data))
66     ips = []
67     IP_octet_count = 0
68     IP_octet_3 = 0
69     IP_octet_4 = 0
70     IP_octet_1 = 0
71     IP_octet_2 = 0
72     i = 1
73 ▼ for tx_idx, trans in enumerate(incoming_transactions):
74     tr_val = trans["value"]
75
76     tr_confirm_time_str = trans["confirmed"]
77     tr_confirm_time = datetime.datetime.strptime(tr_confirm_time_str, '%Y-%m-%dT%H:%M:%SZ')
78     odd_octet = tr_val & 0xff
79     even_octet = (tr_val >> 8) & 0xff
80     ip_half = str(odd_octet) + "." + str(even_octet)
81     # print(str(i) + "\t" + str(hex(tr_val)) + "\t" + ip_half + "\t" + str(tr_confirm_time) + "\t" + trans["tx_hash"])
82     i += 1
83 ▼ if IP_octet_count == 0:
84     IP_octet_3 = tr_val & 0xff
85     IP_octet_4 = (tr_val >> 8) & 0xff
86     IP_octet_count = 2
87     continue
88 ▼ if IP_octet_count == 2:
89     IP_octet_1 = tr_val & 0xff
90     IP_octet_2 = (tr_val >> 8) & 0xff
91     IP_octet_count = 0
92     #print("RTM IP address:\t" + str(IP_octet_1) + "." + str(IP_octet_2) + "." + str(
93     #    IP_octet_3) + "." + str(IP_octet_4) + "\t" + tr_confirm_time_str)
94     ips.append("{}.{1}.{2}.{3}".format(IP_octet_1,IP_octet_2,IP_octet_3,IP_octet_4),tr_confirm_time))
95
return ips
```

The screenshot shows two JSON responses side-by-side. The top response is for 'https://[REDACTED]/rtm/recon/2019-01-01' and the bottom one is for 'https://[REDACTED]/rtm/main/2019-01-01'. Both responses are in JSON format and list IP addresses and their confirmation times.

Index	Time	IP Address
0	2021-01-13	134.209.103.151
1	2021-01-12	206.189.15.193
2	2020-12-23	128.199.183.224
3	2020-12-21	45.61.136.191
4	2020-12-17	165.22.211.203
5	2020-12-17	45.61.136.241
6	2020-12-15	68.183.217.37
7	2020-12-14	157.245.98.183
8	2020-12-11	174.138.44.141
9	2020-12-08	174.138.2.254
10	2020-12-04	45.61.139.98
11	2020-12-03	157.245.142.162
0	2021-01-13	206.166.251.179
1	2021-01-13	91.200.102.113
2	2021-01-12	45.61.136.214
3	2021-01-12	91.200.102.113
4	2020-12-23	45.61.139.20
5	2020-12-23	91.200.102.113
6	2020-12-21	167.172.151.128
7	2020-12-21	91.200.102.113
8	2020-12-17	45.61.136.241
9	2020-12-17	91.200.102.113
10	2020-12-17	45.61.45.61
11	2020-12-17	91.200.45.61

# C&C IS JUST A PROXY

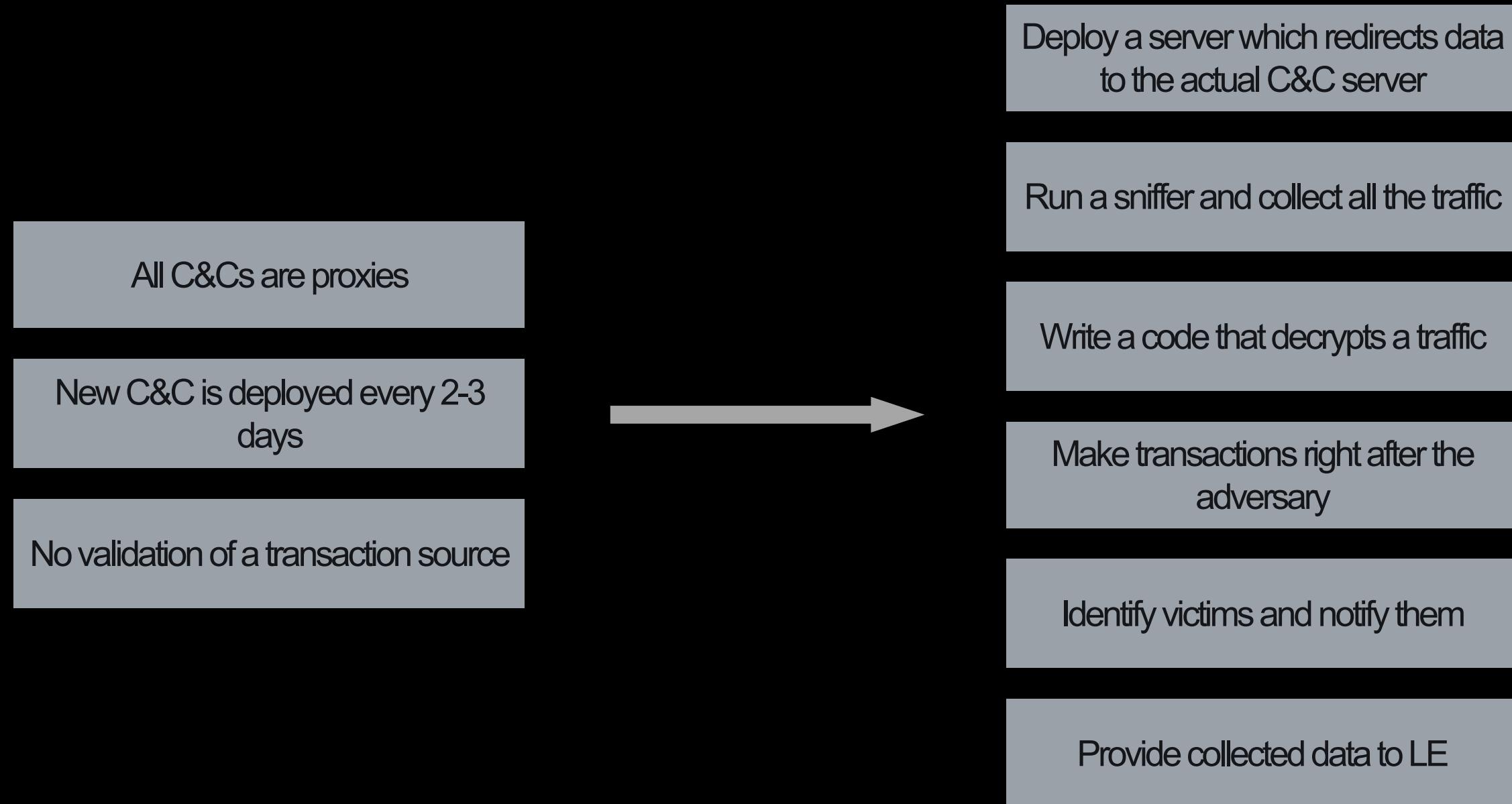


```
access_log /dev/null;
error_log /dev/null;

server {
    listen      *:80;
bought
    location /index.php {
        proxy_set_header Accept-Encoding "";
        #proxy_set_header Host $http_host;
        #proxy_http_version 1.1;
        proxy_buffering off;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For $remote_addr;
        proxy_connect_timeout   600;
        proxy_send_timeout     600;
        proxy_read_timeout     600;
        send_timeout           600;
        proxy_pass http://91.200.103.39/index.php;
    }
    location / { return 404; }
}

#####
#####
```

# SINK-HOLING



# TESTING ATTEMPT



Address	1CeLgFDu917tgtunhJZ6BA2YdR559Boy9Y	
Format	<b>BASE58 (P2PKH)</b>	
Transactions	229	
Total Received	0.08036732 BTC	
Total Sent	0.07801948 BTC	
Final Balance	0.00234784 BTC	

Address	bc1q0nw2g0dgm6shk0xazmaq2tzmwke7ypsz4upzps	
Format	<b>BECH32 (P2WPKH)</b>	
Transactions	6	
Total Received	0.00100106 BTC	
Total Sent	0.00100106 BTC	
Final Balance	0.00000000 BTC	

Transaction should be > 0.00000540

5.2.67.50

Higher fee, faster the confirmation

0x205 -> 0.00000517 < 0.00000540

# DAY X



Hash	69b56b392b69cd9d702456d9306f0af0d5...	2019-12-10 14:15	
	36zoteAyuPk6MSQTtG... 0.00485289 BTC	→	3EHXUWvfXwkc7uA7x... 0.00448062 BTC 1CeLgFDu917tgtunhJZ... 0.00035431 BTC
Fee	0.00001796 BTC (7.213 sat/B - 2.685 sat/WU - 249 bytes)		+0.00035431 BTC 1 confirmation
Hash	b4fa746b85f406c42fb8c0ac256d00766...	2019-12-10 14:20	
	1Bor6v8F3poVEjFsbx3S... 0.00787504 BTC	→	1CeLgFDu917tgtunhJZ6... 0.00013617 BTC 18oktk8rzng3iVFoUhV7... 0.00769864 BTC
Fee	0.00004023 BTC (17.801 sat/B - 4.450 sat/WU - 226 bytes)		+0.00013617 BTC 1 confirmation
Hash	6ed3a947f6652a76820800812834b212c49...	2019-12-10 14:07	
	3ETLaS3ZzSfBEEaoBW... 0.00538376 BTC	→	1CeLgFDu917tgtunhJZ6... 0.00051291 BTC 36zoteAyuPk6MSQTtG... 0.00485289 BTC
Fee	0.00001796 BTC (7.213 sat/B - 2.685 sat/WU - 249 bytes)		+0.00051291 BTC 2 confirmations

ad881d022f54180c08ae19078398d65cad3...	2019-12-10 14:57
1CeLgFDu917tgtunhJZ... 0.00042429 BTC	→
1CeLgFDu917tgtunhJZ6... 0.00051291 BTC	
1CeLgFDu917tgtunhJZ... 0.00035431 BTC	
1CeLgFDu917tgtunhJZ... 0.00023643 BTC	
1CeLgFDu917tgtunhJZ... 0.00018048 BTC	
1CeLgFDu917tgtunhJZ... 0.00035431 BTC	
1CeLgFDu917tgtunhJZ6... 0.00051291 BTC	
1CeLgFDu917tgtunhJZ... 0.00031063 BTC	
1CeLgFDu917tgtunhJZ... 0.00023643 BTC	
1CeLgFDu917tgtunhJZ... 0.00052872 BTC	
0.00064009 BTC (17.875 sat/B - 4.469 sat/WU - 3581 bytes)	-0.00888320 BTC
	Not confirmed

- We transferred money with the minimal fee.
- Every transaction should be confirmed by some amount of other members of the blockchain. Otherwise it will be unconfirmed and can not be observed.
- Our transfers came to the wallet in wrong sequence

# OVERALL STATISTIC



5 LE of different countries were involved	5368 Communicating hosts	3762 Compromised machines identified
5 Years the botnet was alive	6 Different languages were installed on bots	2 Years took to collect enough evidences and make arrests







To fight effectively against  
cybercrime LE agencies  
should collaborate