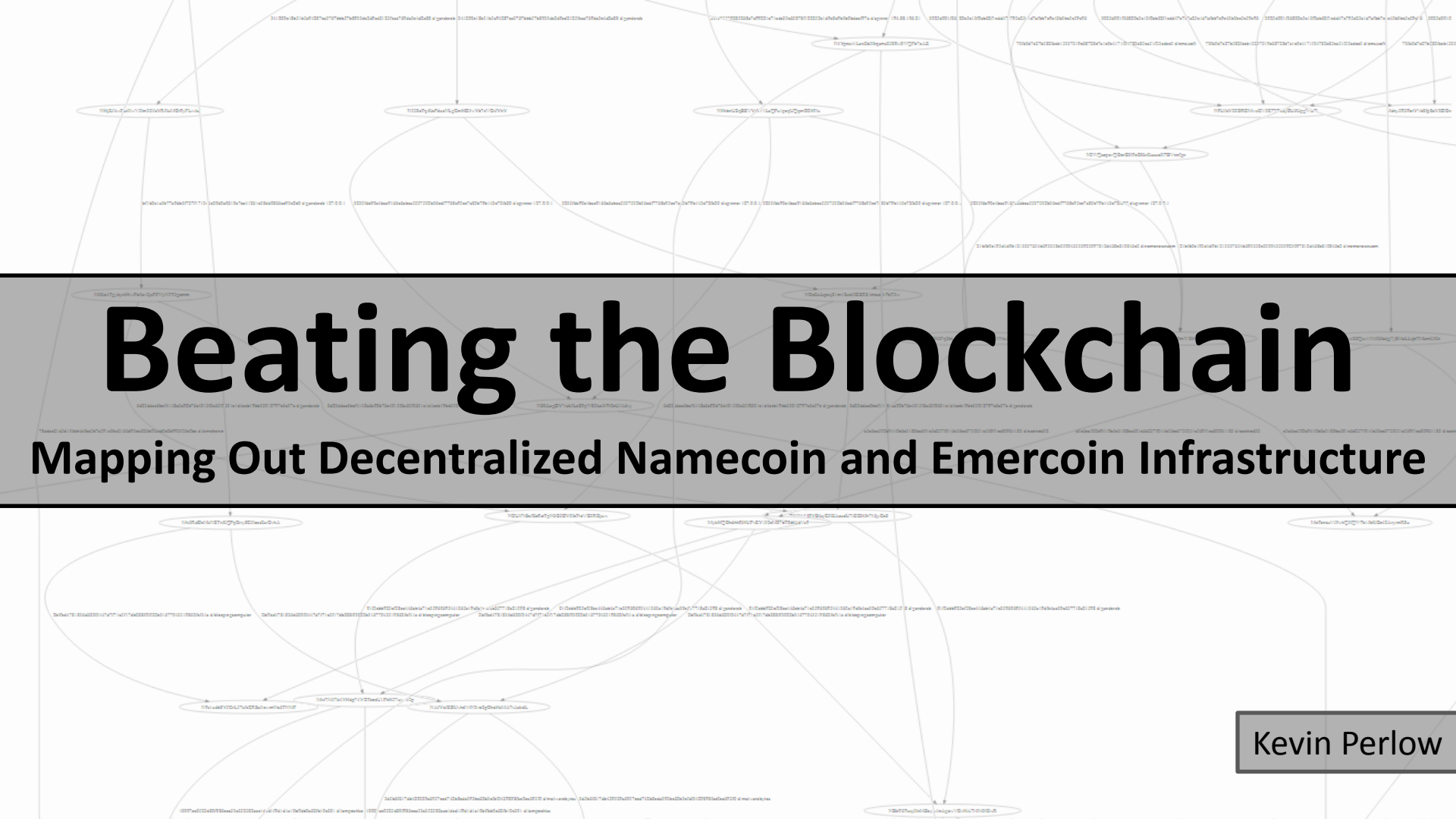

black hat®
USA 2018
AUGUST 4-9, 2018
MANDALAY BAY / LAS VEGAS
#BHUSA / @BLACK HAT EVENTS



Beating the Blockchain

Mapping Out Decentralized Namecoin and Emercoin Infrastructure

Kevin Perlow

About Me

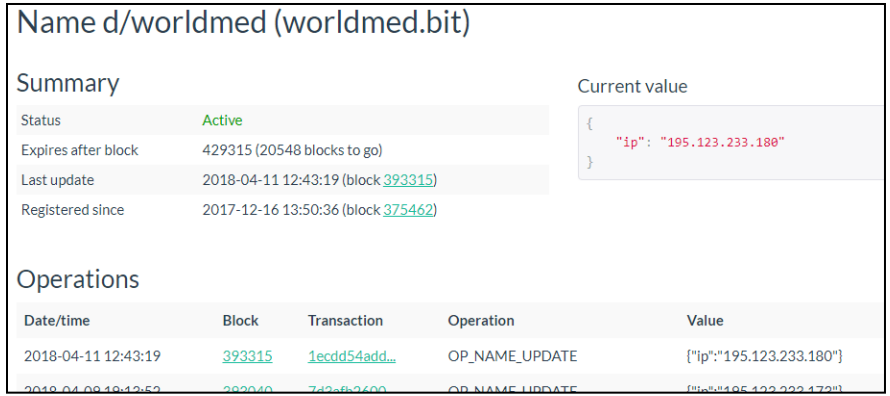
- Reverse Engineering, Threat Intelligence
- Spoke at SANS DFIR in 2016 and 2017
  - https://www.youtube.com/watch?v=DdkLY99HgAA (Yara/VT)
  - https://www.youtube.com/watch?v=1iwsouV8ouQ (Bitcoin Transactions)
- If you're from the future and just need the IOCs:
  - *https://github.com/kevinperlow/BlackHat2018_Blockchain*

Objectives and Goals

- Understand “Decentralized” Infrastructure
  - Namecoin (and Emercoin) Blockchains
  - Transactions, Blocks, TTPs
- Track “Decentralized” Domains
  - Scripting
  - Splunk

Decentralized Domain Name Systems

- Namecoin/Emercoin each sit on a “blockchain”
  - Distributed database
  - Each block holds hash of previous block
  - DNS Query via OpenNIC (typically)



Name d/worldmed (worldmed.bit)

Summary

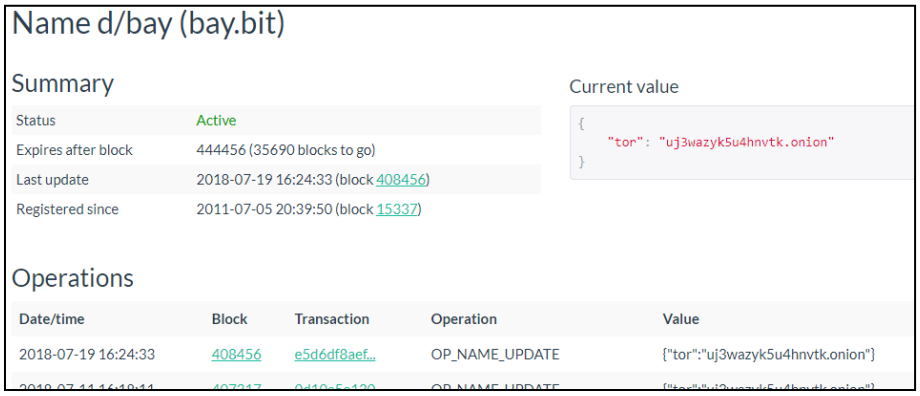
Status	Active
Expires after block	429315 (20548 blocks to go)
Last update	2018-04-11 12:43:19 (block 393315)
Registered since	2017-12-16 13:50:36 (block 375462)

Current value

```
{
    "ip": "195.123.233.180"
}
```

Operations

Date/time	Block	Transaction	Operation	Value
2018-04-11 12:43:19	393315	1ecdd54add...	OP_NAME_UPDATE	{"ip":"195.123.233.180"}



Name d/bay (bay.bit)

Summary

Status	Active
Expires after block	444456 (35690 blocks to go)
Last update	2018-07-19 16:24:33 (block 408456)
Registered since	2011-07-05 20:39:50 (block 15337)

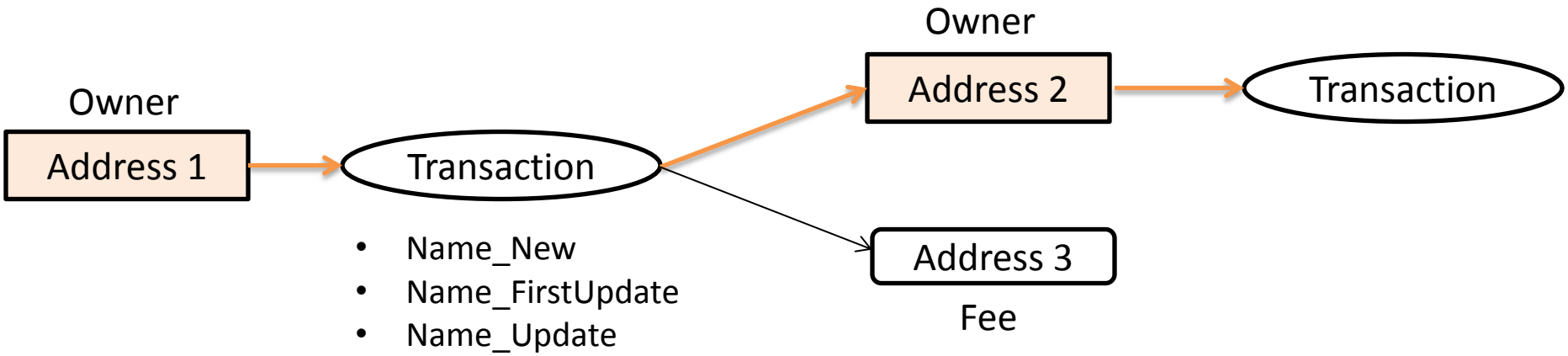
Current value

```
{
    "tor": "uj3wazyk5u4hnvtk.onion"
}
```

Operations

Date/time	Block	Transaction	Operation	Value
2018-07-19 16:24:33	408456	e5d6df8aef...	OP_NAME_UPDATE	{"tor":"uj3wazyk5u4hnvtk.onion"}

Transactions



- You can also use Namecoins as a normal cryptocurrency
- Domain names and IP addresses significantly reduce anonymity

Example (Slavaukraine)

Name d/slavaukraine (slavaukraine.bit)

Status	Active
Expires after block	358723 (15159 blocks to go)
Last update	2017-01-12 17:20:10 (block 322723)
Registered since	2016-06-03 20:43:10 (block 288981)

Operations

Date/time	Block	Transaction	Operation	Value
2017-01-12 17:20:10	322723	159c179a81...	OP_NAME_UPDATE	{"ns":["a.dnspod.com","b.dnspod.com","c.dnspod.com"]}
2017-01-11 20:45:33	322585	cc07584366...	OP_NAME_UPDATE	{"ip":["0.0.0.0"]}
2017-01-08 19:37:33	322040	925d5a6d6a...	OP_NAME_UPDATE	{"ip": ["192.52.166.149"]}
2016-11-05 15:29:32	312309	e3848b6d92...	OP_NAME_UPDATE	{"ip": ["103.199.16.106"]}
2016-06-03 20:43:10	288981	5c9adc978a...	OP_NAME_FIRSTUPDATE	{"ip": ["103.199.16.106"]}
2016-06-03 17:51:04	288965	bd78adb5a8...	OP_NAME_NEW	8771927dd4534d09c129605c26ace7b210dd068a

http://researchcenter.paloaltonetworks.com/2017/01/unit42-2016-updates-shifu-banking-trojan/

Slavaukraine Transaction

Transaction

Bottom transaction from previous slide

Change, address used to make second domain (klyatiemoskali)

Transaction bd78adb5a870bfdf2058556dbef91a330d37b5be029cfb4b9caf65c23ae7cdae

NFbbTh2tH73pqVBYN3KLpBtJ85ReRuGuFa	24.1950952 NMC	>	N4Yjkm4pbrFS7sGehJG3SRXGGtPnxjQNXH 24.1650952 NMC NH9DNuTjddQ28W4X1dZwWSG2KrWimgM2te 0.02 NMC

Initial funding address- can we trace back?

Summary

Size	258 bytes
Block	288965
Total inputs	24.1950952 NMC (1 scripts)
Total outputs	24.1850952 NMC (2 scripts)
Fees	0.01 NMC

Name operation

Operation	OP_NAME_NEW
Name	d/slavaukraine
Hash	8771927dd4534d09c129605c26ace7b210dd068a

An address was used in a transaction that:
-Made d/Slavaukraine
-Made an address that made d/klyatiemoskali

What was this address used for previously?

Address NFbbTh2tH73pqVBYN3KLpBtJ85ReRuGuFa

Date/time	Transaction	Block	Debit	Credit	Balance
2016-06-03 17:51:04	bd78adb5a8...	288965	-24.1950952 NMC		0 NMC
2016-05-29 19:14:04	b0ab8493bd...	288285		24.1950952 NMC	24.1950952 NMC

Comparing Infrastructure

Name d/healthshop

Operations

Date/time	Value
2017-01-11 20:45:33	{"ip":["0.0.0.0"]}
2017-01-08 22:08:34	{"ip":["192.52.166.149"]}
2016-12-10 22:20:00	{"ip":["103.199.16.106"]}
2016-12-01 15:35:28	{"ip": ["103.199.16.106"]}
2016-11-05 15:29:32	{"ip":["87.120.37.85"]}
2016-05-29 19:14:04	{"ip":["87.120.37.85"]}
2016-05-23 16:31:08	{"ip":["87.120.37.85"]}
2016-05-22 16:13:59	0c5ebaa3db71c6b83609273267d1facd92309805

Name d/slavaukraine

Operations

Date/time	Value
2017-01-12 17:20:10	{"ns":["a.dnspod.com","b.dnspod.com","c.dnspod.com"]}
2017-01-11 20:45:33	{"ip":["0.0.0.0"]}
2017-01-08 19:37:33	{"ip": ["192.52.166.149"]}
2016-11-05 15:29:32	{"ip": ["103.199.16.106"]}
2016-06-03 20:43:10	{"ip": ["103.199.16.106"]}
2016-06-03 17:51:04	8771927dd4534d09c129605c26ace7b210dd068a

These two .bit domains have shared the same IP, were both updated and zeroed out at the same time, and are associated on the blockchain.

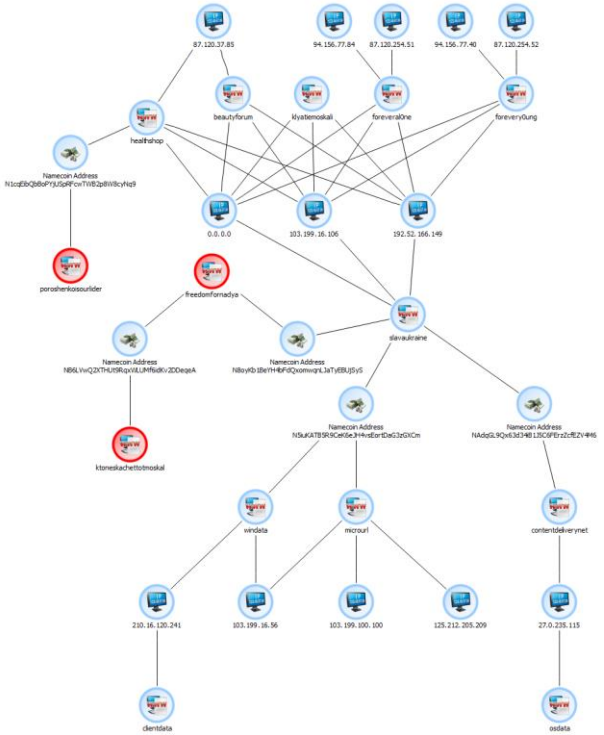
13	d/beautyforum	103.199.16.106
14	d/foreveral0ne	103.199.16.106
15	d/foreveral0ne	103.199.16.106
16	d/forevery0ung	103.199.16.106
17	d/forevery0ung	103.199.16.106
18	d/healthshop	103.199.16.106
19	d/healthshop	103.199.16.106
20	d/klyatiemoskali	103.199.16.106
21	d/klyatiemoskali	103.199.16.106
22	d/slavaukraine	103.199.16.106
23	d/slavaukraine	103.199.16.106
24	d/microurl	103.199.16.56
25	d/microurl	103.199.16.56
26	d/windata	103.199.16.56
27	d/windata	103.199.16.56
28	d/microurl	125.212.205.209
29	d/microurl	127.0.0.1
30	d/microurl	127.0.0.1
31	d/microurl	127.0.0.1
32	d/microurl	127.0.0.1
33	d/windata	127.0.0.1
34	d/windata	127.0.0.1
35	d/windata	127.0.0.1
36	d/windata	127.0.0.1
37	d/clusterdata	127.0.1.1
38	d/clusterdata	127.0.1.1
39	d/beautyforum	192.52.166.149
40	d/foreveral0ne	192.52.166.149
41	d/forevery0ung	192.52.166.149

We can now show that different domains on 103.199.16.106 are related to domains on 192.52.166.149, even if they only used one of the two IPs

Similar IP Space

1	d/microurl	3/29/2016
2	d/microurl	3/29/2016
3	d/microurl	3/29/2016
4	d/microurl	5/20/2016
5	d/healthshop	5/22/2016
6	d/beautyforum	5/22/2016
7	d/healthshop	5/23/2016
8	d/healthshop	5/23/2016
9	d/beautyforum	5/23/2016
10	d/beautyforum	5/23/2016
11	d/windata	5/23/2016
12	d/windata	5/23/2016
13	d/windata	5/23/2016
14	d/foreveral0ne	5/28/2016
15	d/forevery0ung	5/28/2016
16	d/healthshop	5/29/2016
17	d/foreveral0ne	5/29/2016
18	d/foreveral0ne	5/29/2016
19	d/forevery0ung	5/29/2016
20	d/forevery0ung	5/29/2016
21	d/slavaukraine	6/3/2016
22	d/slavaukraine	6/3/2016
23	d/slavaukraine	6/3/2016
24	d/klyatiemoskali	6/3/2016
25	d/klyatiemoskali	6/3/2016
26	d/klyatiemoskali	6/3/2016
27	d/foreveral0ne	6/4/2016
28	d/forevery0ung	6/4/2016
29	d/microurl	10/17/2016

Mapping Relationships



Identified Domains:

- d/slavaukraine
- d/healthshop
- d/klyatiemoskali
- d/contentdeliverynet
- d/foreveral0ne
- d/clientdata
- d/forevery0ung
- d/beautyforum
- d/freedomfornadya
- d/microurl
- d/windata
- d/osdata
- d/ktoneskachettotmoskal
- d/clusterdata

Using Splunk

(or any other indexing/searching mechanism…)

Fields

- Block #
- Time
- Hash
- Operation Type

- Domain
- Data
- IP vs Non-IP
- Blockchain

```
"402989","2018-06-1410:22:00","11ba45ad268074151177a816f779e823b9860557e8e0aa71e927f2b66f2983e5","OP_NAME_FIRSTUPDATE","zadedov","51.15.77.58","iptype","namecc
"402989","2018-06-1410:22:00","11ba45ad268074151177a816f779e823b9860557e8e0aa71e927f2b66f2983e5","OP_NAME_FIRSTUPDATE","zadedov","51.15.77.58","iptype","namecc
"402986","2018-06-1409:51:37","3b67cc4460a730e3143664eac3f5d48596cea806468e2751809598b407373724","OP_NAME_UPDATE","connectionfailed","47.88.222.146","iptype","
"402986","2018-06-1409:51:37","3b67cc4460a730e3143664eac3f5d48596cea806468e2751809598b407373724","OP_NAME_UPDATE","connectionfailed","47.88.222.146","iptype","
"402975","2018-06-1408:20:34","4c06a3646d18f0c0bf9371dc304a2a86ce9646fcb7441518e253f8c83542fd59","OP_NAME_NEW","zadedov","7cad10bc855ae625f0bfe6edffd8993f2051b
"402972","2018-06-1407:48:51","0f8840d3e1901ab4394f872b0c85b2f4a96957dee8df150b3135ebe35bc46bd1","OP_NAME_FIRSTUPDATE","hali","{&#34;name&#34;:&#34;Aphrotronic
"402972","2018-06-1407:48:51","28511c43d52d3c1e97da403e4eb2cb007c485c077aa5a99c28d91f694e3e2627","OP_NAME_FIRSTUPDATE","melodie","{&#34;name&#34;:&#34;Aphrotrc
"402967","2018-06-1407:35:47","d0cc1acb6d73e99acd8c6eac0c3469ade12cba49b9a3c07a5ad1a17ac6bc1d40","OP_NAME_NEW","0847976357357","f4240a18cc8cad7cb8e038e0ab7eec7
"402967","2018-06-1407:35:47","46cf95aaa0fe77f4c50e9af3a0b138e1ca9c76f0c906b5e18ab307deded346bb","OP_NAME_UPDATE","898878768567567653322","193.169.252.65","ipt
"402967","2018-06-1407:35:47","46cf95aaa0fe77f4c50e9af3a0b138e1ca9c76f0c906b5e18ab307deded346bb","OP_NAME_UPDATE","898878768567567653322","193.169.252.65","ipt
"402967","2018-06-1407:35:47","3b7cd0d7df40d15c00933095efd3b327284b8fe98571b2501725abd58f8276e1","OP_NAME_UPDATE","9387723658221","193.169.252.65","iptype","na
"402967","2018-06-1407:35:47","3b7cd0d7df40d15c00933095efd3b327284b8fe98571b2501725abd58f8276e1","OP_NAME_UPDATE","9387723658221","193.169.252.65","iptype","na
"402959","2018-06-1406:02:14","5064fbb2c711698c8e04861947bae51ba66712e47b800939f90e4f5d34526e3c","OP_NAME_NEW","melodie","ad783a4023a0b9e89e0fbd94c9cfb5a670f01
```

Analytics and Pivoting

- Domains With Many IPs
- Close “Block Proximity”
- High “Block Count”
- Odd/Rare Nameserver Delegation

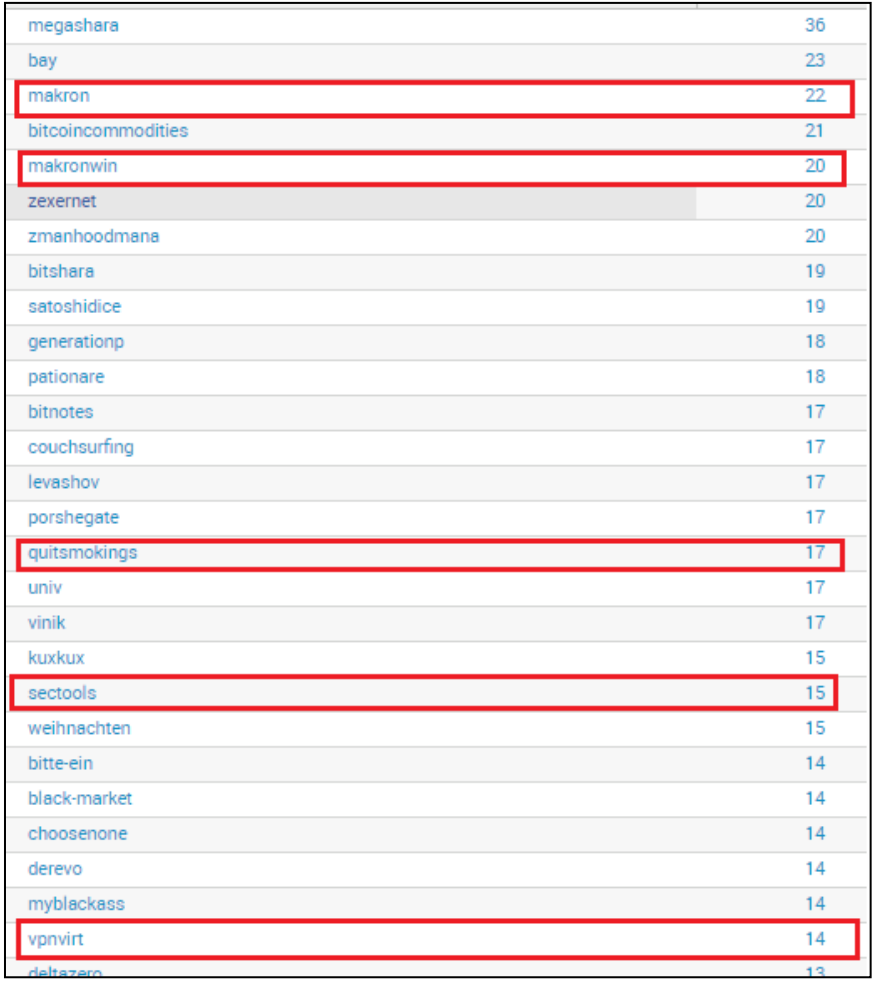
****Key Technique: Splunk Subsearch*

Red Boxes

- Smoke Loader
  - d/Makron (22)
  - d/Makronwin (20)
  - d/quitsmokings (17)

- Dimnie:
  - d/sectools (15)

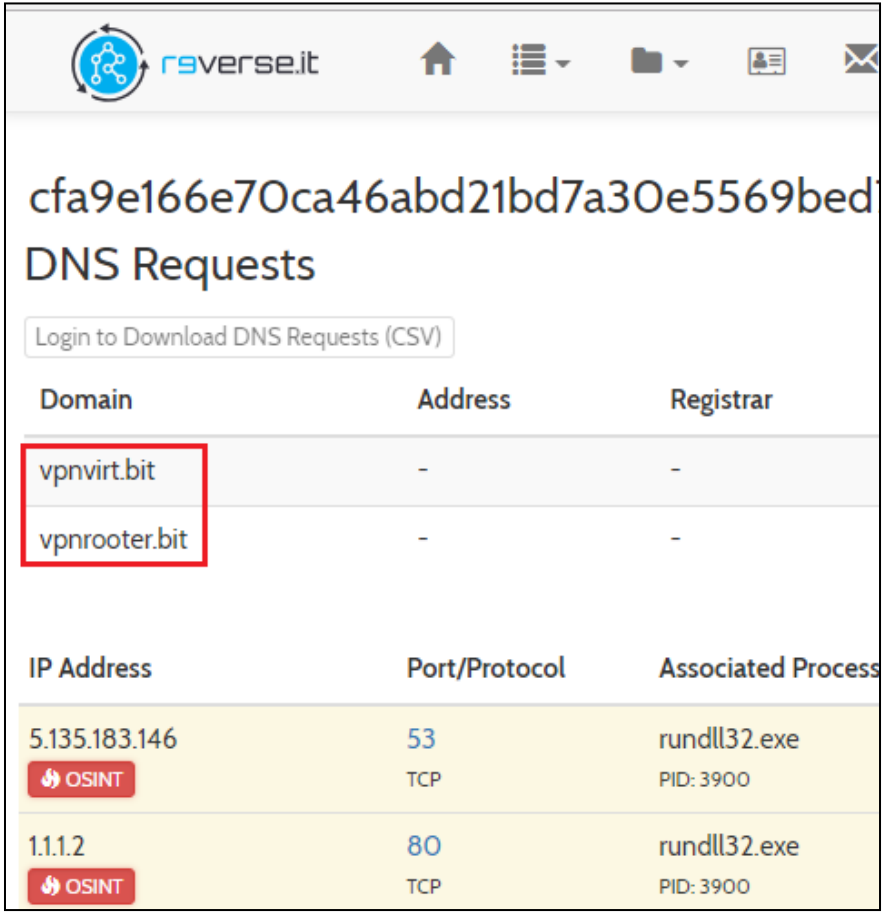
- ?????
  - d/vpnvirt (15)



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

Identified a malware sample communicating with this domain *as well as* a similarly named domain…

Now what?



Shared Blocks

- 292242
- 298988
- 299344
- 306131
- 317342

Shared IPs

- 185.61.149.70
- 185.128.42.237
- 91.215.153.31
- 213.252.247.94
- 185.25.51.25
- 213.252.246.115
- 185.25.51.221

"Close" IPs

- 103.208.86.*
- 185.99.132.*
- 169.239.129.*

Do we know anything about these IPs?

block	Domain	DataInput
359024	volstat	83.243.41.162
360003	volstat	91.191.184.159
361797	volstat	91.191.184.33
292242	vpnrooter	08e1a96c11f141533f9763d3
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	103.208.86.22
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

Next Steps

- IPs Appear in ESET's "Read The Manual" Report
  - 185.61.149.70
  - 185.128.42.237
  - 91.215.153.31

We will take a brief look at the malware shortly; in the meantime, can we "fill in the blanks" on domain relationships?

```
index=*  [search index=*  [search index=* (103.208.86.122 OR 103.208.86.158 OR
103.208.86.254 OR 169.239.129.100 OR 169.239.129.25 OR 173.242.124.228 OR 185.128.42.237
OR 185.2.82.209 OR 185.203.118.168 OR 185.25.51.221 OR 185.25.51.25 OR 185.61.149.70 OR
185.99.132.10 OR 185.99.132.51 OR 213.252.246.115 OR 213.252.247.94 OR 91.215.153.31) |
table Domain |  dedup Domain] type=iptype | table DataInput| regex DataInput!="^0\." | regex
DataInput!="^10\." |regex DataInput!="^192\.168\." | regex DataInput!="^127\." | regex
DataInput!="^1\." ] type=iptype|  table block Domain DataInput
```

- Blue- Domains mapped to the IPs we discovered
- Red- IPs for each of those domains
- Green- Domains for each of those IPs

Relationships

- d/vpnomnet and d/vpnkeep
  - Share IPs with each other
  - Share block updates with each other
  - Share IPs with d/vpnrooter and d/vpnvirt
  - Updated in “close block proximity”

More Importantly

- d/vpnomnet and d/vpnkeep
  - Are listed in ESET’s “Read the Manual” IOC table

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

Examining the Malware

Why do we care?

1. Disclosed in 2017, reported to be narrowly scoped
2. Used same blockchain infrastructure through 2018
3. Targets accounting and remote banking software
4. ***Activity is still happening***
   - Late July: Sent to head of finance for government organization in a Russian administrative district as part of a larger campaign as well as three companies associated with energy supply and transfer.

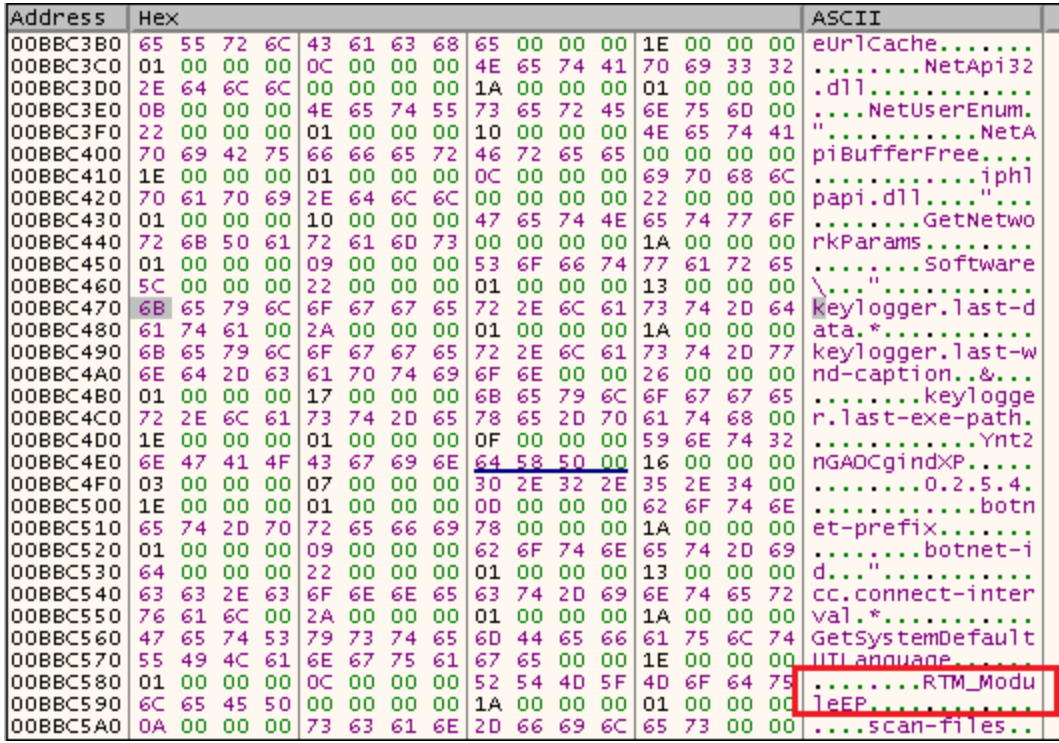
Examining the Malware

How do we know we are looking at the same malware?

Key Facts from ESET Report:

- Targets specific list of accounting software, bank URLs
- Specific DLL Export
- Unique strings, configuration data
  - Botnet-prefix, cc.url.1, dbo-detector-off…
- Functionality
  - Window titles, class names

Decrypted Strings



Address	Hex	ASCII
00BBC3B0	65 55 72 6C 43 61 63 68 65 00 00 00 1E 00 00 00	eUrlCache.......
00BBC3C0	01 00 00 00 0C 00 00 00 4E 65 74 41 70 69 33 32	........NetApi32
00BBC3D0	2E 64 6C 6C 00 00 00 00 1A 00 00 00 01 00 00 00	.dll............
00BBC3E0	0B 00 00 00 4E 65 74 55 73 65 72 45 6E 75 6D 00	....NetUserEnum.
00BBC3F0	22 00 00 00 01 00 00 00 10 00 00 00 4E 65 74 41	"...........NetA
00BBC400	70 69 42 75 66 66 65 72 46 72 65 65 00 00 00 00	piBufferFree....
00BBC410	1E 00 00 00 01 00 00 00 0C 00 00 00 69 70 68 6C	............iphl
00BBC420	70 61 70 69 2E 64 6C 6C 00 00 00 00 22 00 00 00	papi.dll...."....
00BBC430	01 00 00 00 10 00 00 00 47 65 74 4E 65 74 77 6F	........GetNetwo
00BBC440	72 6B 50 61 72 61 6D 73 00 00 00 00 1A 00 00 00	rkParams........
00BBC450	01 00 00 00 09 00 00 00 53 6F 66 74 77 61 72 65	........Software
00BBC460	5C 00 00 00 22 00 00 00 01 00 00 00 13 00 00 00	\..."...........
00BBC470	6B 65 79 6C 6F 67 67 65 72 2E 6C 61 73 74 2D 64	keylogger.last-d
00BBC480	61 74 61 00 2A 00 00 00 01 00 00 00 1A 00 00 00	ata.*...........
00BBC490	6B 65 79 6C 6F 67 67 65 72 2E 6C 61 73 74 2D 77	keylogger.last-w
00BBC4A0	6E 64 2D 63 61 70 74 69 6F 6E 00 00 26 00 00 00	nd-caption..&...
00BBC4B0	01 00 00 00 17 00 00 00 6B 65 79 6C 6F 67 67 65	........keylogge
00BBC4C0	72 2E 6C 61 73 74 2D 65 78 65 2D 70 61 74 68 00	r.last-exe-path.
00BBC4D0	1E 00 00 00 01 00 00 00 0F 00 00 00 59 6E 74 32	............Ynt2
00BBC4E0	6E 47 41 4F 43 67 69 6E 64 58 50 00 16 00 00 00	nGAOCgindXP.....
00BBC4F0	03 00 00 00 07 00 00 00 30 2E 32 2E 35 2E 34 00	........0.2.5.4.
00BBC500	1E 00 00 00 01 00 00 00 0D 00 00 00 62 6F 74 6E	............botn
00BBC510	65 74 2D 70 72 65 66 69 78 00 00 00 1A 00 00 00	et-prefix.......
00BBC520	01 00 00 00 09 00 00 00 62 6F 74 6E 65 74 2D 69	........botnet-i
00BBC530	64 00 00 00 22 00 00 00 01 00 00 00 13 00 00 00	d..."...........
00BBC540	63 63 2E 63 6F 6E 6E 65 63 74 2D 69 6E 74 65 72	cc.connect-inter
00BBC550	76 61 6C 00 2A 00 00 00 01 00 00 00 1A 00 00 00	val.*...........
00BBC560	47 65 74 53 79 73 74 65 6D 44 65 66 61 75 6C 74	GetSystemDefault
00BBC570	55 49 4C 61 6E 67 75 61 67 65 00 00 1E 00 00 00	UILanguage......
00BBC580	01 00 00 00 0C 00 00 00 52 54 4D 5F 4D 6F 64 75	........RTM_Modu
00BBC590	6C 65 45 50 00 00 00 00 1A 00 00 00 01 00 00 00	leEP............
00BBC5A0	0A 00 00 00 73 63 61 6E 2D 66 69 6C 65 73 00 00	....scan-files..

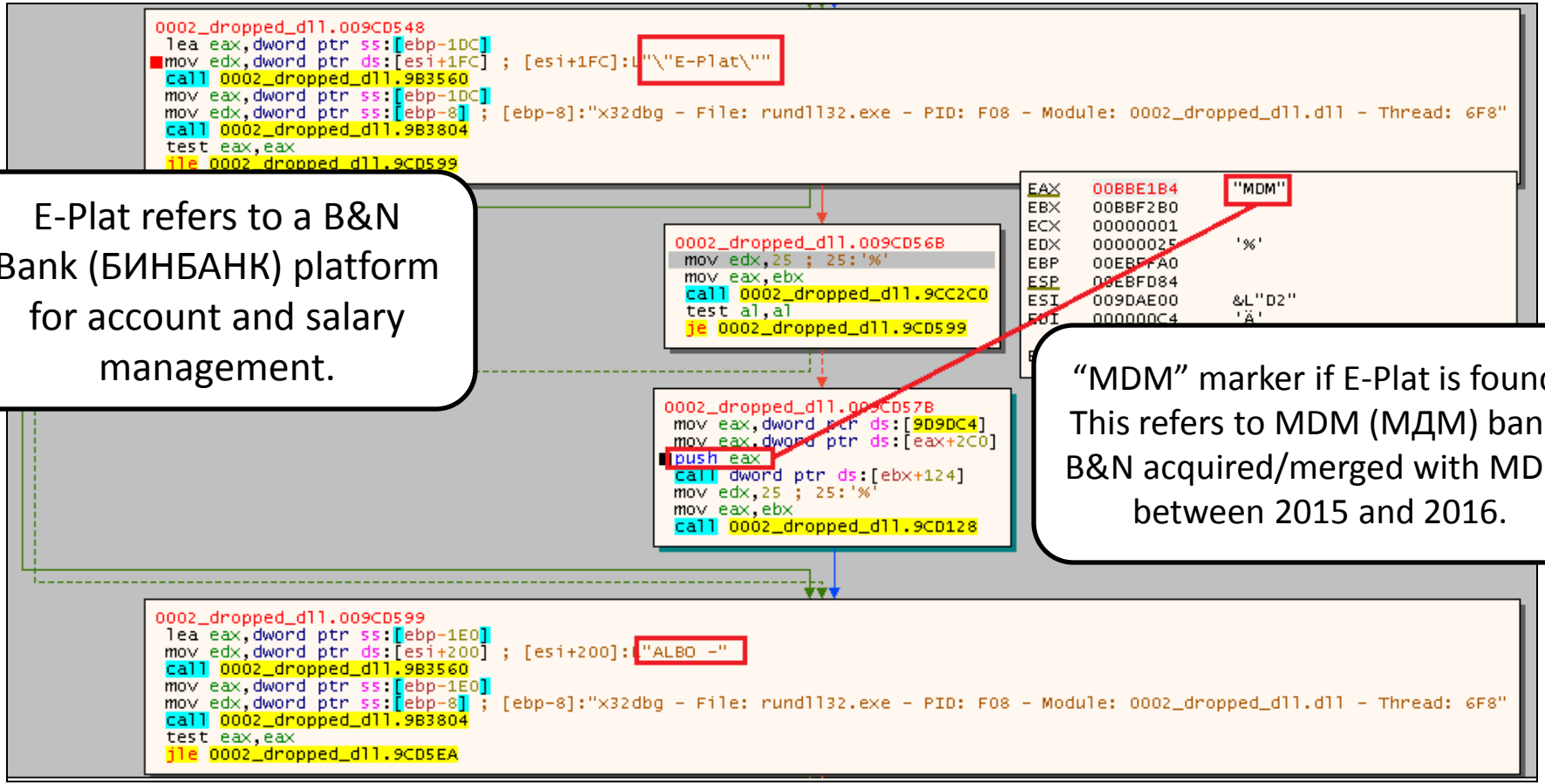
Decrypted Strings that Help Identify the Malware

keylogger.last-data
keylogger.last-wnd-caption
botnet-prefix
botnet-id
cc.connect-interval
scan-files

...

cc.url.1
cc.url.2

Window/Class Check



E-Plat refers to a B&N Bank (БИНБАНК) platform for account and salary management.

"MDM" marker if E-Plat is found. This refers to MDM (МДМ) bank. B&N acquired/merged with MDM between 2015 and 2016.

DNS Requests- Method 1

Sends a DNS request for the .bit domain to a hardcoded OpenNIC server. Pretty standard.

DNS Requests- Method 2

```
009BD044  push eax
009BD045  mov eax,dword ptr ss:[ebp+C]      [ebp+C]:L"/name/d/dotbitdream"
009BD048  push eax
009BD049  mov eax,dword ptr ss:[ebp-C]      [ebp-C]:L"GET"
009BD04C  push eax
009BD04D  push edi
009BD04E  mov eax,dword ptr ds:[9D9E18]
009BD053  mov eax,dword ptr ds:[eax]
009BD055  call eax
009BD057  mov dword ptr ss:[ebp-8],eax      eax:WinHttpOpenRequest
009BD05A  cmp dword ptr ss:[ebp-8],0
009BD05E  je 0002_dropped_dll.9BD20A
009BD064  cmp dword ptr ss:[ebp+14],2
009BD068  jne 0002_dropped_dll.9BD086
009BD06A  mov dword ptr ss:[ebp-14],3300
009BD071  push 4
009BD073  lea eax,dword ptr ss:[ebp-14]
009BD076  push eax
009BD077  push 1F
009BD079  mov eax,dword ptr ss:[ebp-8]      [ebp-8]:L"dotbitdream"
009BD07C  push eax
009BD07D  mov eax,dword ptr ds:[9D9E04]
009BD082  mov eax,dword ptr ds:[eax]
009BD084  call eax
009BD086
009BD08A
```

```
Hide FPU

EAX   4D513D2C   <winhttp.WinHttpOpenRequest>
EBX   0104FEDF
ECX   00000000
EDX   014A800C   "namecha.in"
EBP   0104FE98
ESP   0104FE54
ESI   014A3000
EDI   014A3100

EIP   009BD055   0002_dropped_dll.009BD055

EFLAGS   00000206
ZF 0  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError  00000000 (ERROR_SUCCESS)
LastStatus C000007C (STATUS_NO_TOKEN)
```

```
0104FE54  014A3100
0104FE58  0009AB74  L"GET"
0104FE5C  000B8AE4  L"/name/d/dotbitdream"
0104FE60  0009AC5C  L"HTTP/1.1"
0104FE64  00000000
0104FE68  00000000
0104FE6C  00800108
0104FE70  000C3914  L"dotbitdream.bit"
0104FE74  0104FF3C  &"192.168.180.128"
0104FE78  000C3914  L"dotbitdream.bit"
```

The brute force approach…

Expanding the List of IOCs

We have *four* domains now:

1. What are the IPs for the additional domains?
2. What new domains share those IPs
3. What are the IPs for *those* domains?
4. Keep repeating process.

Alternatively:

1. We can do this using other known domains from the ESET report.

We will take the alternate route to demonstrate identifying false positive connections.

Expanding the List of IOCs (Query)

```
index=*  [search index=* type=iptype  [search index=*  [search index=* cash-money-analitica
type=iptype|  table DataInput | regex DataInput!="^0\." | regex DataInput!="^10\." |regex
DataInput!="^192\.168\." | regex DataInput!="^127\." | regex DataInput!="^1\."] |  table  Domain ] | regex
DataInput!="^0\." |  regex DataInput!="^10\." |regex DataInput!="^192\.168\." | regex DataInput!="^127\." |
regex DataInput!="^1\."| table DataInput ] | regex DataInput!="^10\." |regex DataInput!="^192\.168\." | regex
DataInput!="^127\." | regex DataInput!="^1\."|  table block Domain DataInput
```

- Blue: IPs of Base Domain(s)
- Red: Domains for those IPs
- Green: IPs for the red domains
- Black: Domains for the Green IPs

- xoonday, volstat, lookstat, sysmonitor, leomoon, firststat, fooming
- feb96eb2aa59 (previously disclosed domain) connected
- Are these really connected?

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

Splunk Transforms

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

- Only one IP overlap between ESET RTM domains and the newly identified domains
- Newly identified domains created nearly a year later

Strengthening Assessment

Reverse Engineering

- Map out infrastructure
- Compare samples using unreported domains

Xoonday subset:

- "CHESSYLITE" from FireEye article
- Shares code with SOCKS5 module in Trickbot, socks5systemz, SmokeLoader (huge rabbit hole)
- Will brute force/connect to various APIs (Twitter, Uber, Amazon)
- "*heyfg645fdhwi*" – RC4 key from "BackDoor.TeamViewer.49" report

Xoonday References

- http://www.vkremez.com/2017/11/lets-learn-trickbot-socks5-backconnect.html
- https://www.hybrid-analysis.com/sample/68c746df7df35b3379a4d679fc210abdb2032b3c076ec51a463abe1e0e18345f?environmentId=100
- https://www.reverse.it/sample/eecfb451b2cf0f4043c8d27be443f69164eae22e05eed098d7bc1f7c90c692c9?environmentId=100
- https://www.fireeye.com/blog/threat-research/2018/04/cryptocurrencies-cyber-crime-blockchain-infrastructure-use.html
- https://vms.drweb.com/virus/?i=8161714&lng=en

Emercoin

Emercoin Blockchain

- Similar concept
- Supports .emc, .coin, .lib, .bazar
- Significantly less active
- Not that exciting

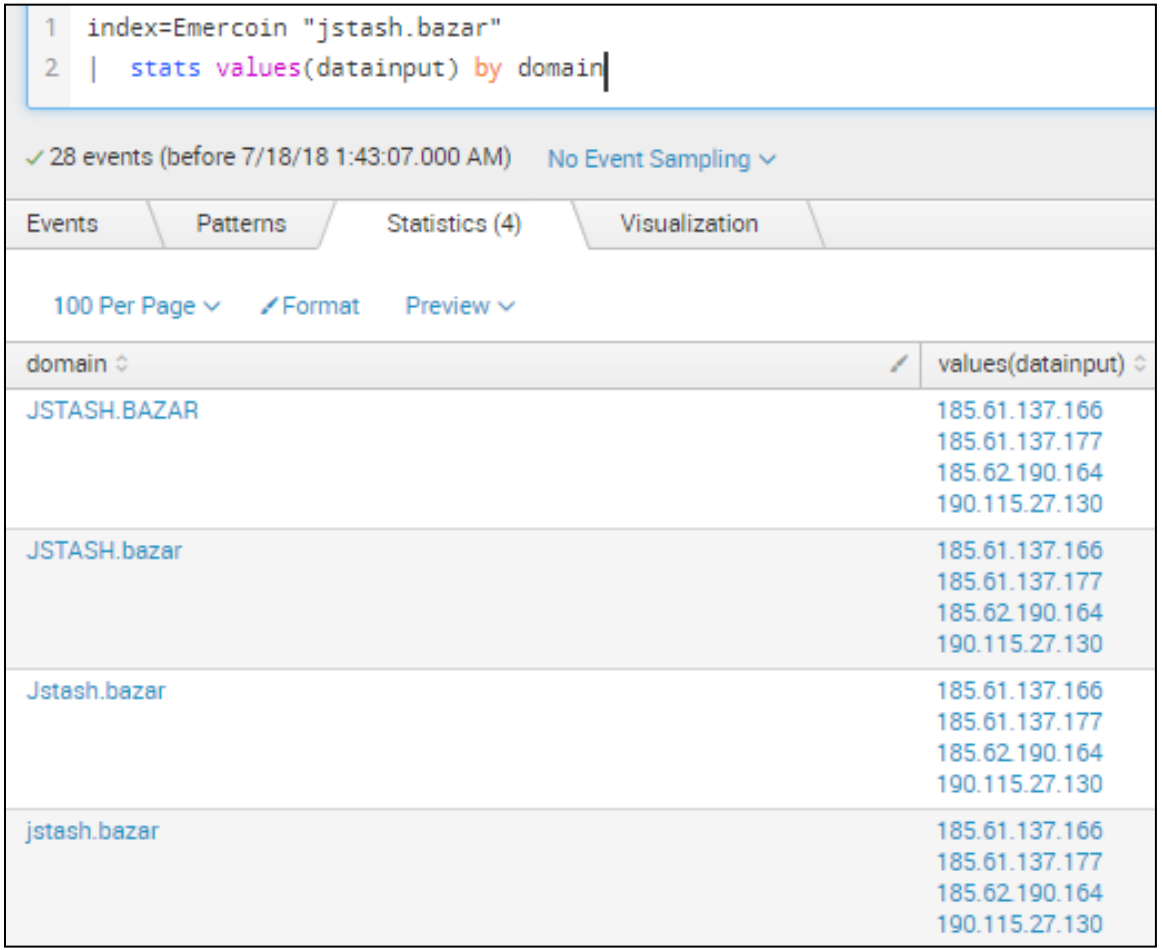
- **Most well-known domain: Jstash[.]bazar

Jstash[.]bazar

- 185.61.137.166
- 185.61.137.177
- 185.62.190.164
- 190.115.27.130

Pivoting

- cvv[.]bazar
- cvv2[.]bazar
- dumps[.]bazar
- j-stash[.]bazar
- joker-stash[.]bazar
- jokerstash[.]bazar
- stash[.]bazar
- track2[.]bazar



Odd Nameservers, Other Tidbits

- crdpro[.]emc, ns1.dnscontrolfff[.]to

- nomoreransom[.]coin, ns1.sinkhole.it
  - Gandcrab C2 (nomoreransom[.]bit is also Gandcrab infrastructure)
  - PCAP data: dns1[.]soprodns[.]ru
    - You can pivot off of this nameserver on both blockchains
  - Failed attempt to sinkhole?

Source: https://isc.sans.edu/forums/diary/GandCrab+Ransomware+Now+Coming+From+Malspam/23321/

- Brownsloboz - .bit, .emc, .bazar, .lib
  - You can actually pivot ***across*** both blockchains to find data here.

Nameserver Delegation

- Gandcrab, Shifu, etc.

- Record looks something like:
  - {"ns":["dns1.soprodns[.]ru","dns2.soprodns[.]ru"]}
  - {"ns":["a.dnspod.com", "b.dnspod.com", "c.dnspod.com"]}

- Simple solution: Map out infrastructure, script a twice-daily nslookup

Concluding Thoughts

You now know how to:

1. Identify potentially malicious decentralized domains.
2. Use two different methods to map out infrastructure on decentralized blockchains.
3. Search for IOCs *across* two blockchains.

You've also learned:

1. About a group using malware that targets accounting and banking software users.
2. That this group is continuing to do this nearly a year after public disclosure.

IOCs from some of the clusters I've mapped out (including RTM) will be available in the white paper and on my Github page (https://github.com/kevinperlow/BlackHat2018_Blockchain)