

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

Ksenia 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

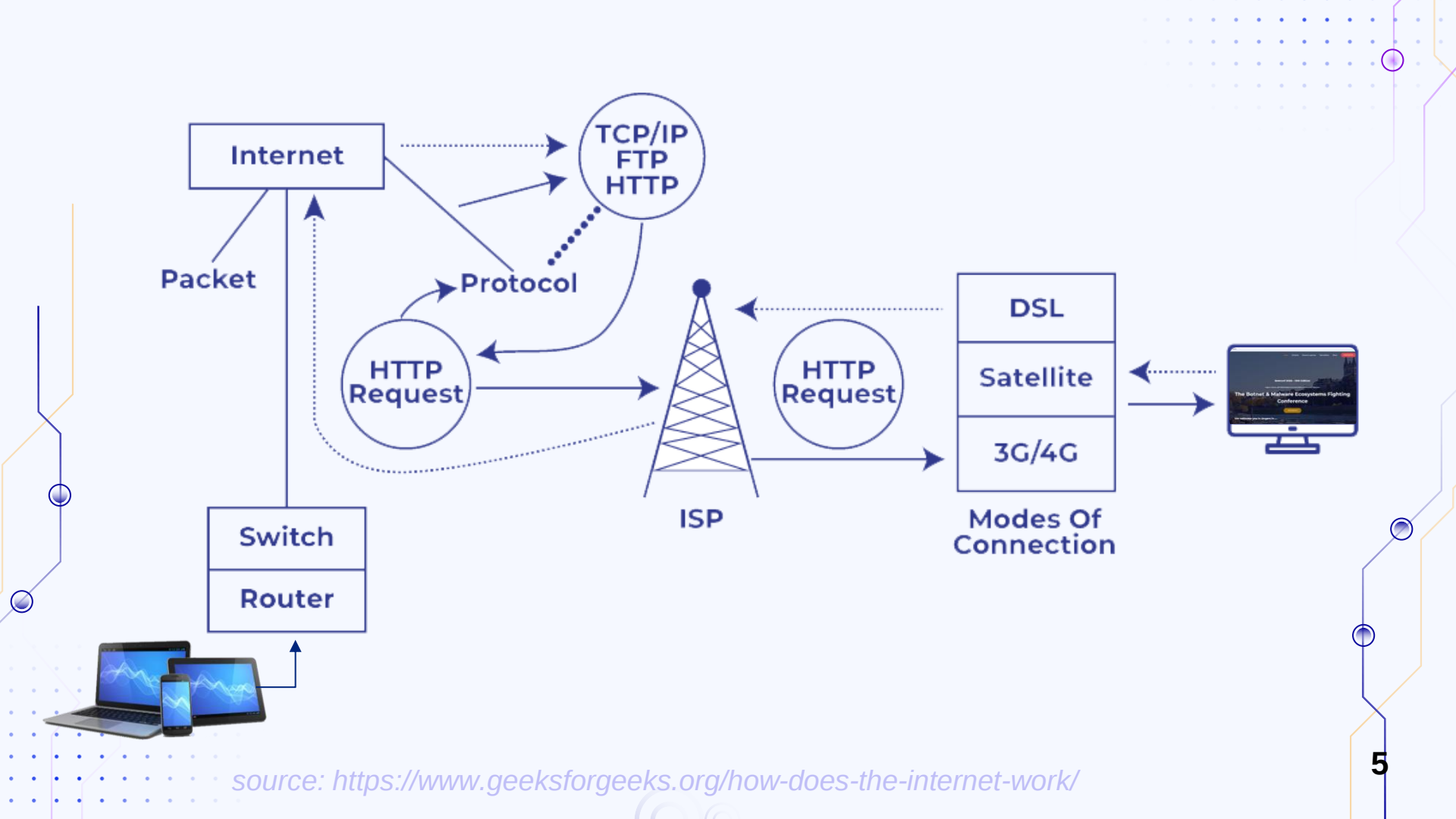
Obfuscation techniques
for C2 communication



01

Introduction to network analytics





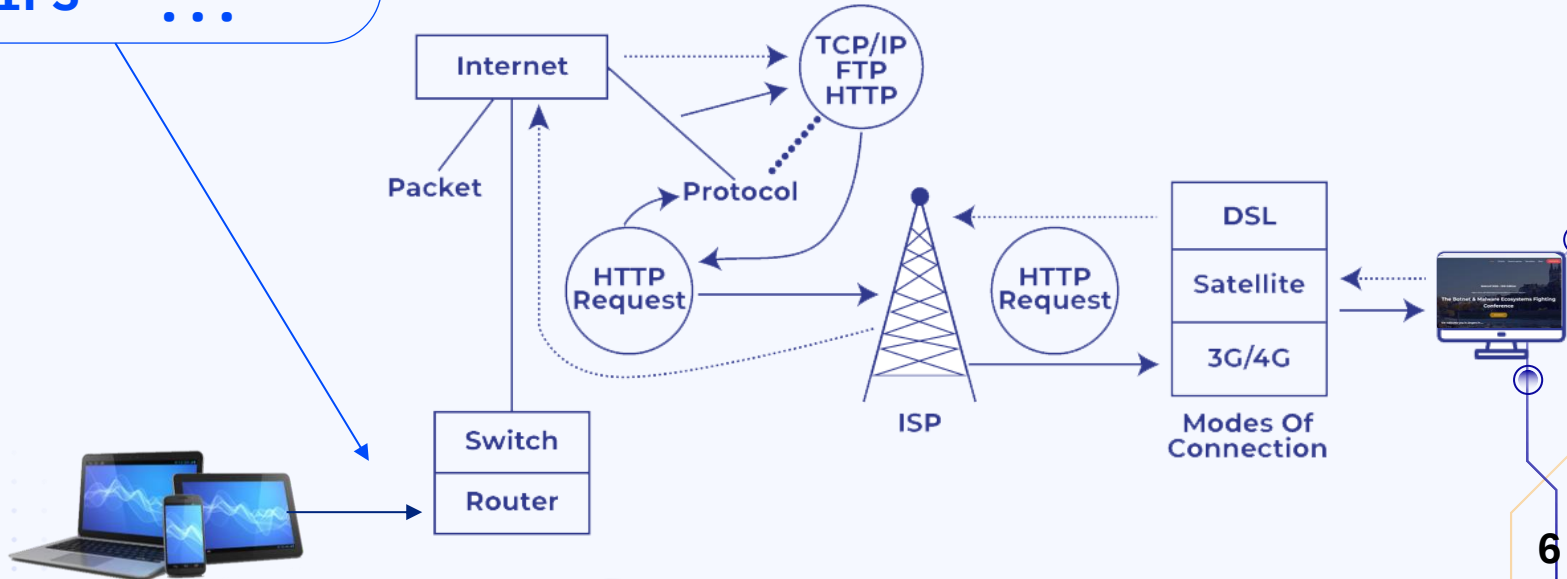
source: <https://www.geeksforgeeks.org/how-does-the-internet-work/>

network security solutions

Firewall **NGFW**
DLP **NTA**
Host-based **NDR**
IDS/IPS **...**

monitoring, analysis, detection

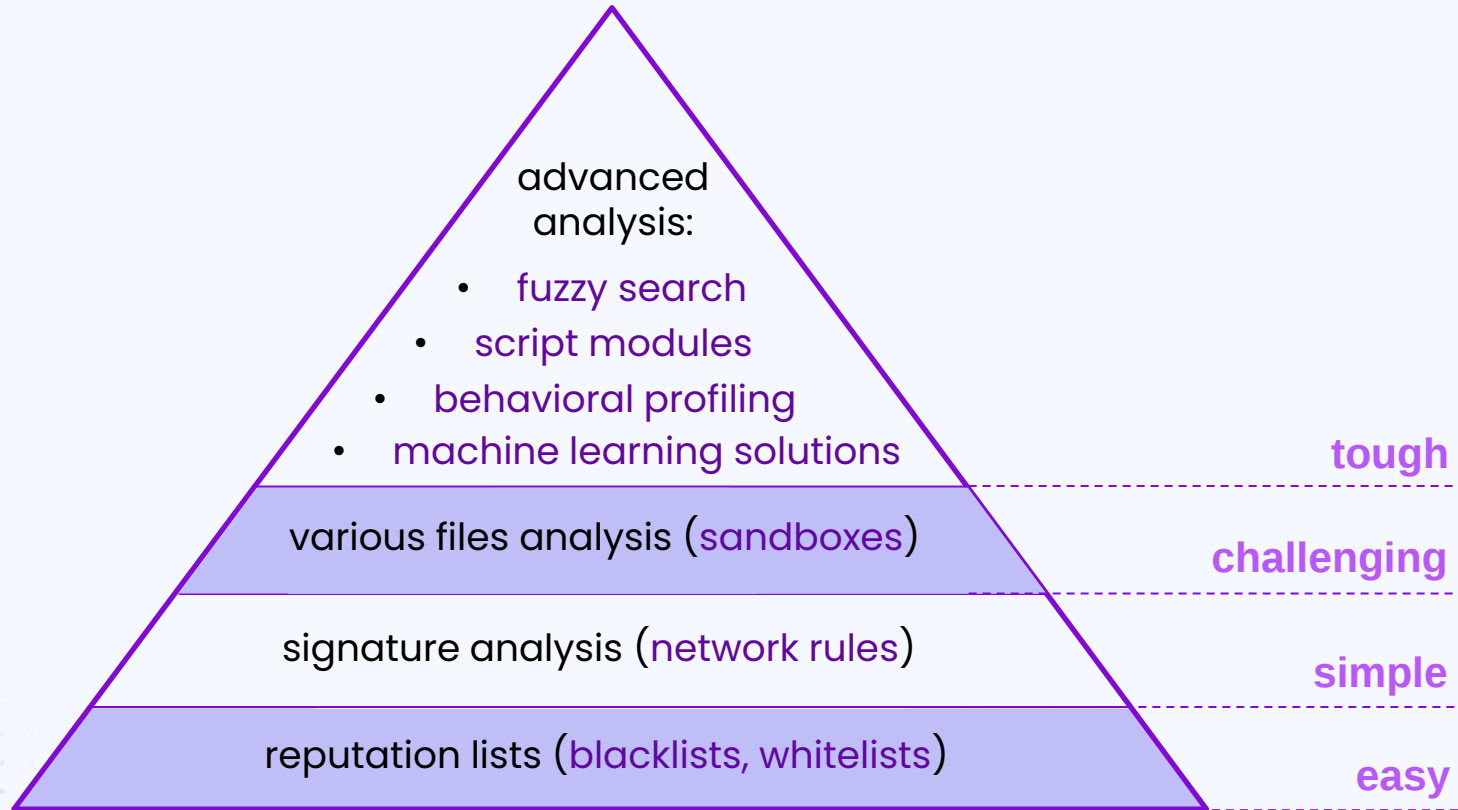
network analysts



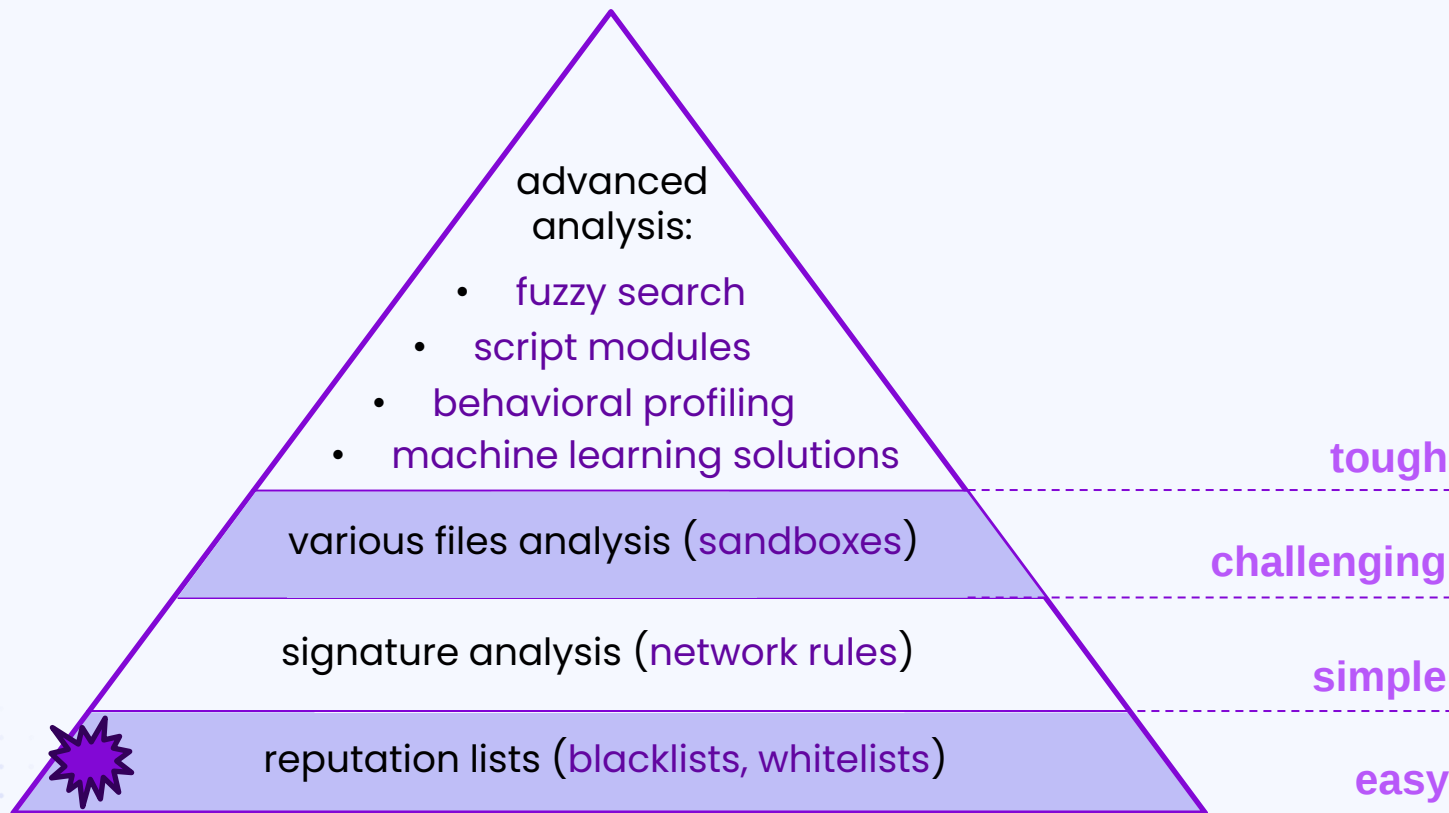
02

Methods for analyzing and detecting suspicious & dangerous activity

Pyramid of ~~pain~~ network traffic analysis technologies



Pyramid of ~~pain~~ network traffic analysis technologies



Reputation lists

URLhaus
from ABUSE²⁴ | SPAMHAUS

[Browse](#) [Hunting Alerts](#) [Access Data](#)

Dateadded (UTC)	Malware URL	Status	Tags
2025-04-19 16:30:23	http://112.248.113.157:36813/i	Online	32-bit elf mips Mozilla
2025-04-19 16:27:10	http://120.61.10.91:54522/i	Online	32-bit elf mips Mozilla
2025-04-19 16:22:12	http://42.231.168.91:34429/bin.sh	Online	32-bit arm elf mirai
2025-04-19 16:21:05	http://219.155.231.114:33687/bin.sh	Online	32-bit elf mips Mozilla

THREAT fox
from ABUSE²⁴ | SPAMHAUS

[Browse IOCs](#) [Share IOCs](#) [IOC Requests](#)

Date (UTC)	IOC	Malware	Tags
2025-04-19 16:13:05	217.114.43.122:4000	Unknown malware	AS199785 censys CHSN-AS EvilGinx
2025-04-19 16:10:05	54.219.14.165:2628	NetSupportManager RAT	AMAZON-02 AS165
2025-04-19 16:05:06	171.227.30.106:6000	Venom RAT	AS7552 c2 censys
2025-04-19 16:03:05	185.177.239.155:443	Havoc	AS215826 c2 censys
2025-04-19 16:01:05	192.153.57.203:8080	Quasar RAT	AS399629 BLNWX
2025-04-19 16:00:07	77.110.106.151:80	Hook	AEZA-AS AS210644
2025-04-19 16:01	auth.echelonai.world	Hook	AS13335 c2 censys
2025-04-19 16:00	128.90.106.203:8808	AsyncRAT	AS40861 asynccrat
2025-04-19 16:00	89.40.31.130:1010	AsyncRAT	AS215117 asynccrat

PhishTank
Out of the Net, into the Tank.

[Home](#) [Add a Phish](#) [Verify a Phish](#) [Phish Search](#) [Stats](#) [FAQ](#) [Developers](#) [Mailin Lists](#) [My Account](#)

Join the fight against phishing

Submit suspected phishing. Track the status of your submissions. Verify other users' submissions. Develop software with our free API.

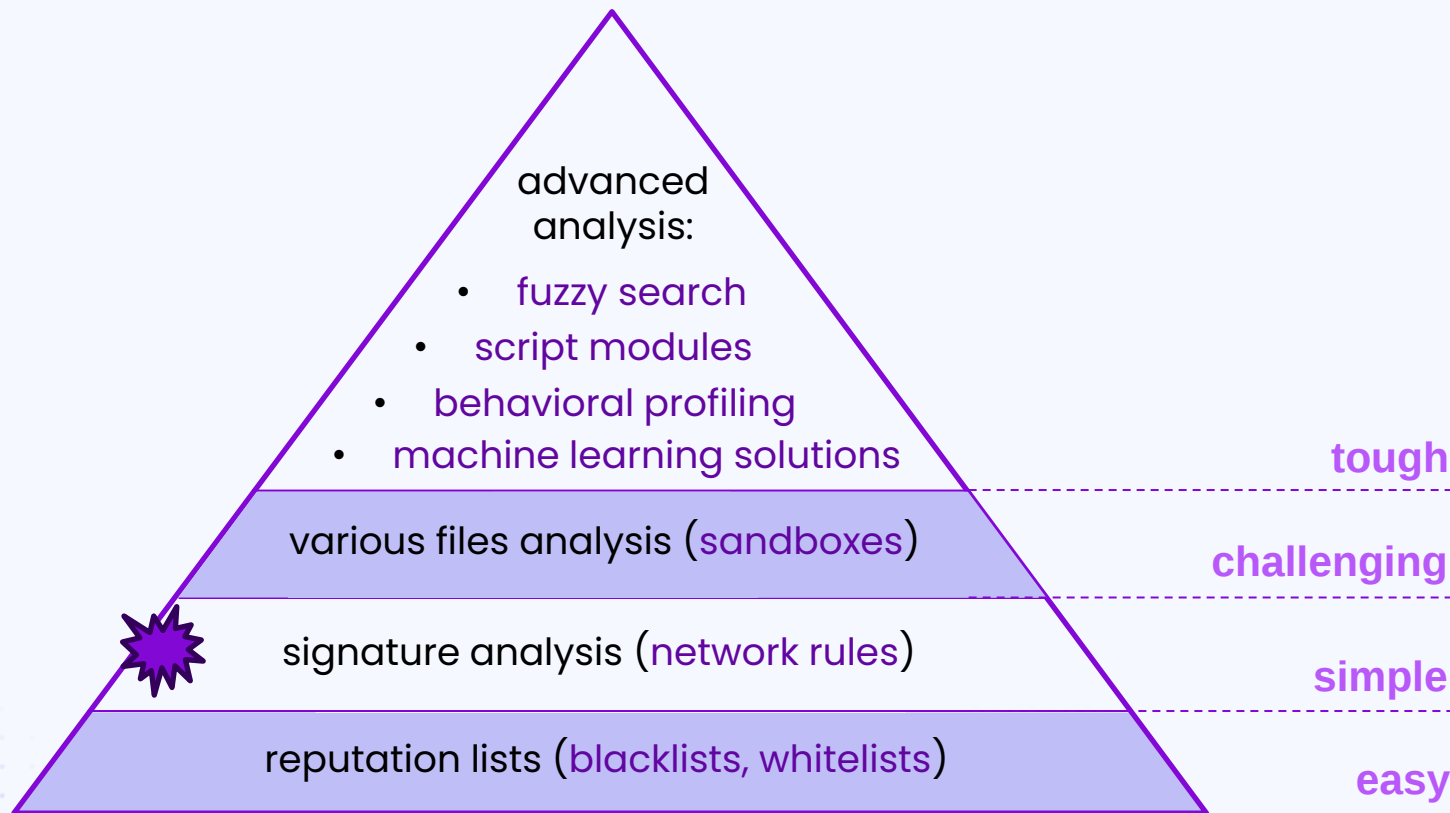
Found a phishing site? Get started now — see if it's in the Tank:
 [Is it a phish?](#)

Recent Submissions

You can help! Sign in or register (free fast!) to verify these suspected phishing.

ID	URL	Submitted by
5067667	https://securedatacfuonline.de	aberratio
5067663	https://stefefinancial.com	aberratio
5067662	https://trackingsavings.com	aberratio
5067661	https://relaycoinlauncher.com	fatid0101
5067659	https://reutoken.ru/	tuandhuong
5067658	https://robobank.com	aberratio
5067657	https://waxonsavingsbank.com	aberratio
5067656	https://iconconcordadmin.auth-cormbase-trust.com	tuandhuong
5067655	https://iconconcordadmin.auth-cormbase-trust.com	tuandhuong
5067652	https://api.auth-cormbase-trust.com	tuandhuong
5067650	https://web-itawiconconcordadmin.auth-cormbase-trust.com	Shindufish
5067647	https://alegropokainie.pl-oferta006947.icu/?id=B...	Amazonsoph

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>

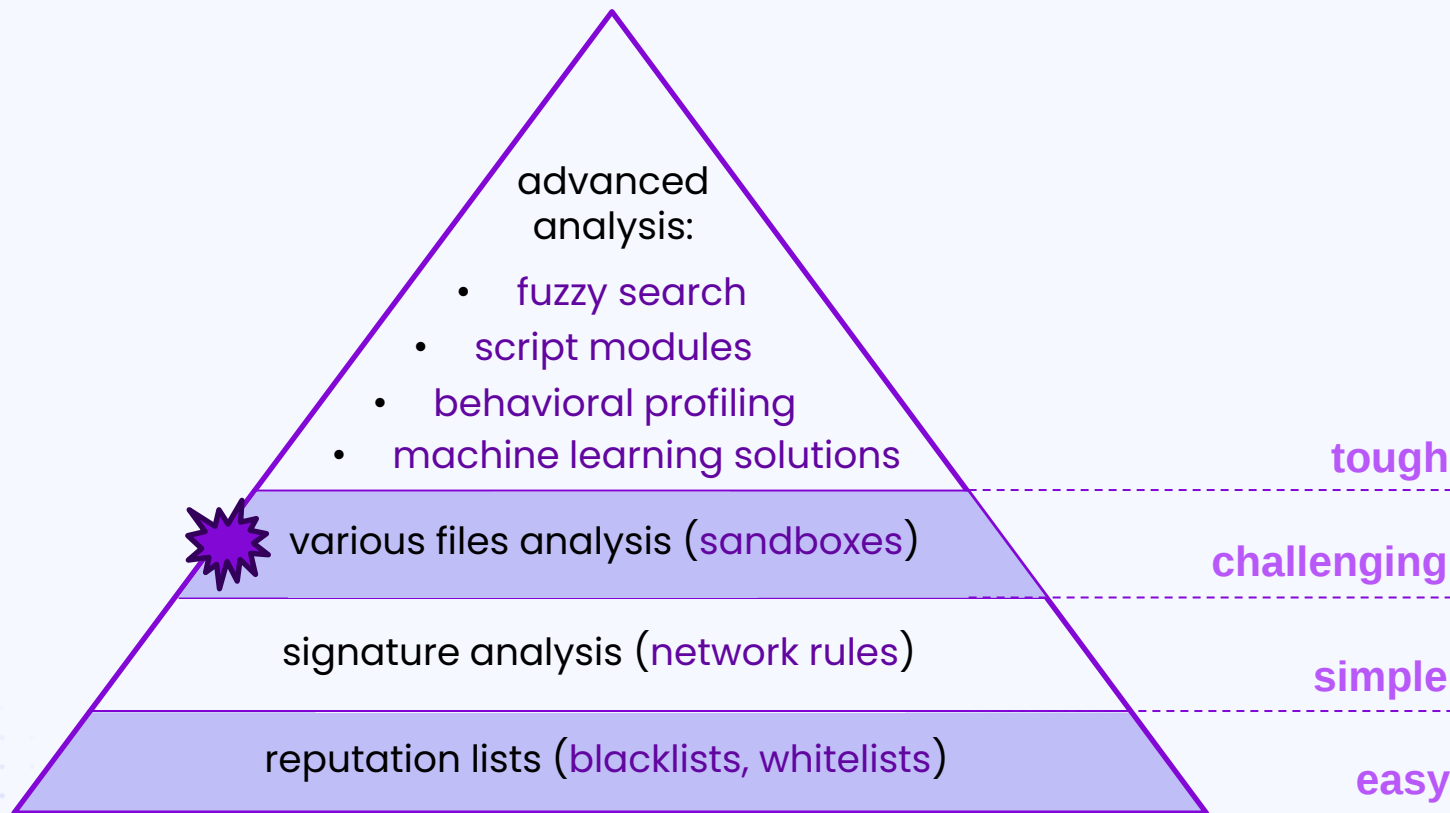
- Emerging Threats Open Ruleset [Proofpoint] ~ 42k rules
[https://rules.emergingthreats.net/open/suricata-%\(_version_\)s/emerging.rules.tar.gz](https://rules.emergingthreats.net/open/suricata-%(_version_)s/emerging.rules.tar.gz)
- PAW Patrues is a collection of rules for IDPS/NSM Suricata engine [pawpatrules]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

updated
regularly

Open-Source rulesets

source: [https://rules.emergingthreats.net/open/suricata-\\$version/emerging.rules.tar.gz](https://rules.emergingthreats.net/open/suricata-$version/emerging.rules.tar.gz)

Pyramid of ~~pain~~ network traffic analysis technologies

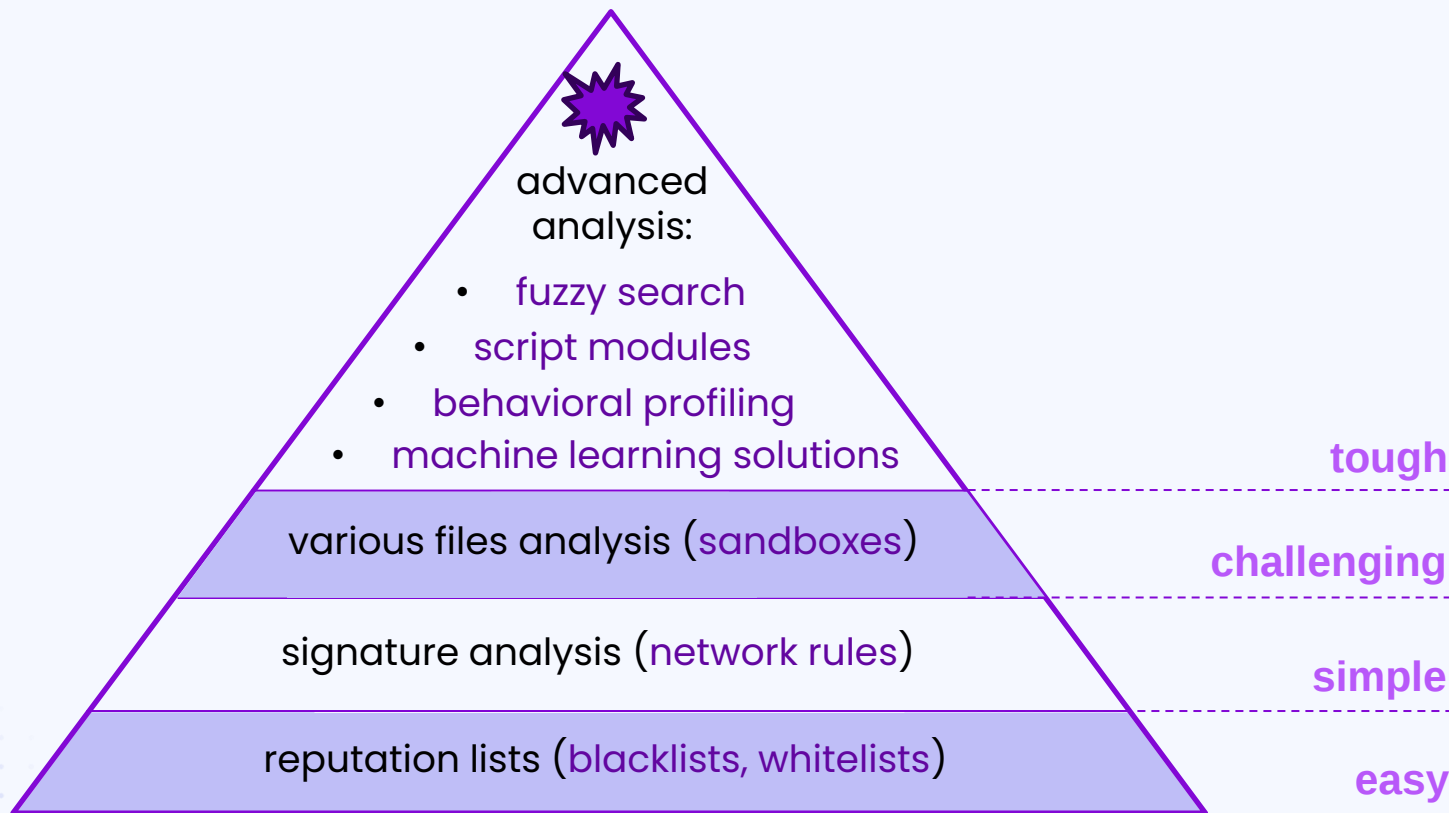


The screenshot displays the 'Linux Analysis Report' interface. At the top, there's a header with the title 'Linux Analysis Report' and a sub-header 'na.eif'. Below this is a navigation bar with icons for 'FAG', 'Analysis', and 'Report'. The main content area is divided into four panels:

- General Information:** A table with fields like Sample name (na.eif), Analysis ID (1982320), MD5, SHA1, SHA256, Tags (Linux/Android), and Info (Logos for Linux, Android, and others).
- Detection:** A vertical stack of colored boxes indicating detection levels: MALICIOUS (red), SUSPICIOUS (orange), CLEAN (green), UNKNOWN (grey), and Promoted (red).
- Signatures:** A list of detection signatures with descriptions, such as 'Indicates a heuristic detection for subdomain sample', 'Indicates subdomain for dropped file', 'Indicates sample detected through community (Yara rule)', 'Web/Ar (Domain detection for subdomain file)', 'Yara detected Foundation', 'Checks files in suspicious directories', 'Executes the "undetect" command for reading DIB IOC set', 'Points for open address', 'Sample contains shell', 'Sample is packed with UPX', and 'Contains hidden files and/or directories'.
- Classification:** A circular diagram with various icons representing different categories or components.

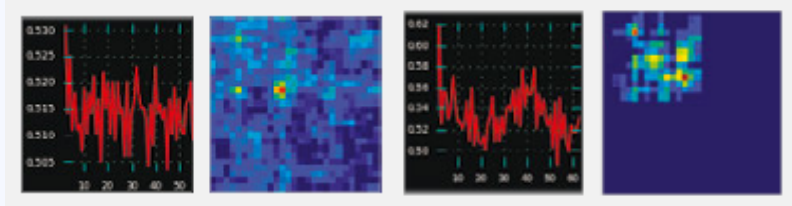
aring

Pyramid of ~~pain~~ network traffic analysis technologies



Advanced analysis

- fuzzy search



- ML solutions



- behavioral profiling



- script modules

```
46 -- Caches the absolute path of a file.
47 local function cache_file_path(file_name)
48     local project_title = sys.get_config_string("project.title")
49     local system_info = sys.get_sys_info()
50     if system_info.system_name == "Linux" then
51         -- Linux uses the $XDG_CONFIG_HOME environment variable as the file path prefix.
52         -- If this variable is not set, then we default to the conventional ~/.config/ prefix.
53         local xdg_config_home = os.getenv("XDG_CONFIG_HOME")
54         if xdg_config_home then
55             file_paths[file_name] = string.format("%s/%s/%s", xdg_config_home, project_title, file_name)
56         else
57             file_paths[file_name] = sys.get_save_file("config/" .. project_title, file_name)
58         end
59     else
60         file_paths[file_name] = sys.get_save_file(project_title, file_name)
61     end
62 end
63
64 -- Checks if a file has the ".json" extension.
65 local function is_json_file(file_name)
66     return string.sub(file_paths[file_name], -5) == ".json"
67 end
68
69 -- Saves data that was written to a file.
70 local function save(file_name, data)
71     -- If this is a JSON file, then save it using Lua's 'io' API.
72     if is_json_file(file_name) then
```

Not only!





03

Obfuscation techniques for C2 communication

Mimicry of legitimate communications

Backdoor TONESHELL

The image shows a Wireshark packet capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. The packet list pane shows several packets, with packet 184 selected. The packet details pane shows the structure of packet 184, which is a TCP RST packet. The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
143	15.351965	192.168.100.1...	103.91.64.250	TCP	66	53894 → 443 [SYN]
144	15.361073	103.91.64.250	192.168.100.197	TCP	66	443 → 53894 [SYN]
145	15.361217	192.168.100.1...	103.91.64.250	TCP	54	53894 → 443 [ACK]
146	15.362144	192.168.100.1...	103.91.64.250	TLSv1.2	114	Application Data
147	15.376573	103.91.64.250	192.168.100.197	TCP	54	443 → 53894 [ACK]
183	24.093126	103.91.64.250	192.168.100.197	TLSv1.2	184	Application Data
184	24.093809	192.168.100.1...	103.91.64.250	TCP	54	53894 → 443 [RST]

Frame 146: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
Ethernet II, Src: 18:f7:78:6f:96:ee (18:f7:78:6f:96:ee), Dst: R
Internet Protocol Version 4, Src: 192.168.100.197, Dst: 103.91.
Transmission Control Protocol, Src Port: 53894, Dst Port: 443,
Transport Layer Security
 TLSv1.2 Record Layer: Application Data Protocol: Hypertext T
 Content Type: Application Data (23)
 Version: TLS 1.2 (0x0303)
 Length: 55
 Encrypted Application Data: 430829767f94c5e27be0210e37ec3
 [Application Data Protocol: Hypertext Transfer Protocol]

```
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 1c 73 cd 0d 12 a8 24 69 1e 5e b3 e4 76 42 89 24 .s....$i ^...vB.$  
00000040 b3 d6 27 73 84 5f d7 c6 a4 fe 40 f7 09 1d 38 56 ..'s... _@...8V  
00000050 5f 0c d9 60 b4 ec d7 ce 75 cd 10 d2 99 13 65 9d ...'.... u.....e.  
00000060 1c 1e c9 24 af 2a 97 24 ae 73 29 63 52 9d a6 3a ...$.*.$ .s)cR...  
00000070 28 54 1b 50 c1 30 ce a8 ab db cf de a1 75 cf ad (T.P.0... ..u..  
00000080 ff 37 .7
```

```
00000000 17 03 03 00 2f 00 00 00 00 00 00 00 00 00 00 00 ....//... ..  
00000010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00000020 00 00 00 00 00 d5 cd 4d 31 23 22 02 55 53 45 52 .....M 1#" .USER  
00000030 2d 50 43 00 -PC.
```

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 f5 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 d6 f9 84 32 b5 84 c0 a6 3e b3 6a 5a 78 bc 10 b0 f4 f5 55 ec a3 00 b5 ..$i .^..vB.$  
00000040 5a 78 bc 10 b0 f4 f5 55 ec a3 00 b5 5a 78 bc 10 b0 f4 f5 55 ec a3 00 b5 s._... ..@...8V  
00000050 5a 78 bc 10 b0 f4 f5 55 ec a3 00 b5 5a 78 bc 10 b0 f4 f5 55 ec a3 00 b5 .... u.....e.  
00000060 5a 78 bc 10 b0 f4 f5 55 ec a3 00 b5 5a 78 bc 10 b0 f4 f5 55 ec a3 00 b5 $.*.$ .s)cR...:  
00000070 5a 78 bc 10 b0 f4 f5 55 ec a3 00 b5 5a 78 bc 10 b0 f4 f5 55 ec a3 00 b5 p.0.. .....u..
```

From Hex

Delimiter
Auto

XOR

Key
430829767f94c5e27be0: HEX

Scheme
Standard ☐ Null preserving

Output

•ñ•DÊDLEENQDESKTOP-JGLJLDNUL

Detection

Mimicry of legitimate communications

- network rules (for specific malware families)

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;)
```

Backdoor TONESHELL

- 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:

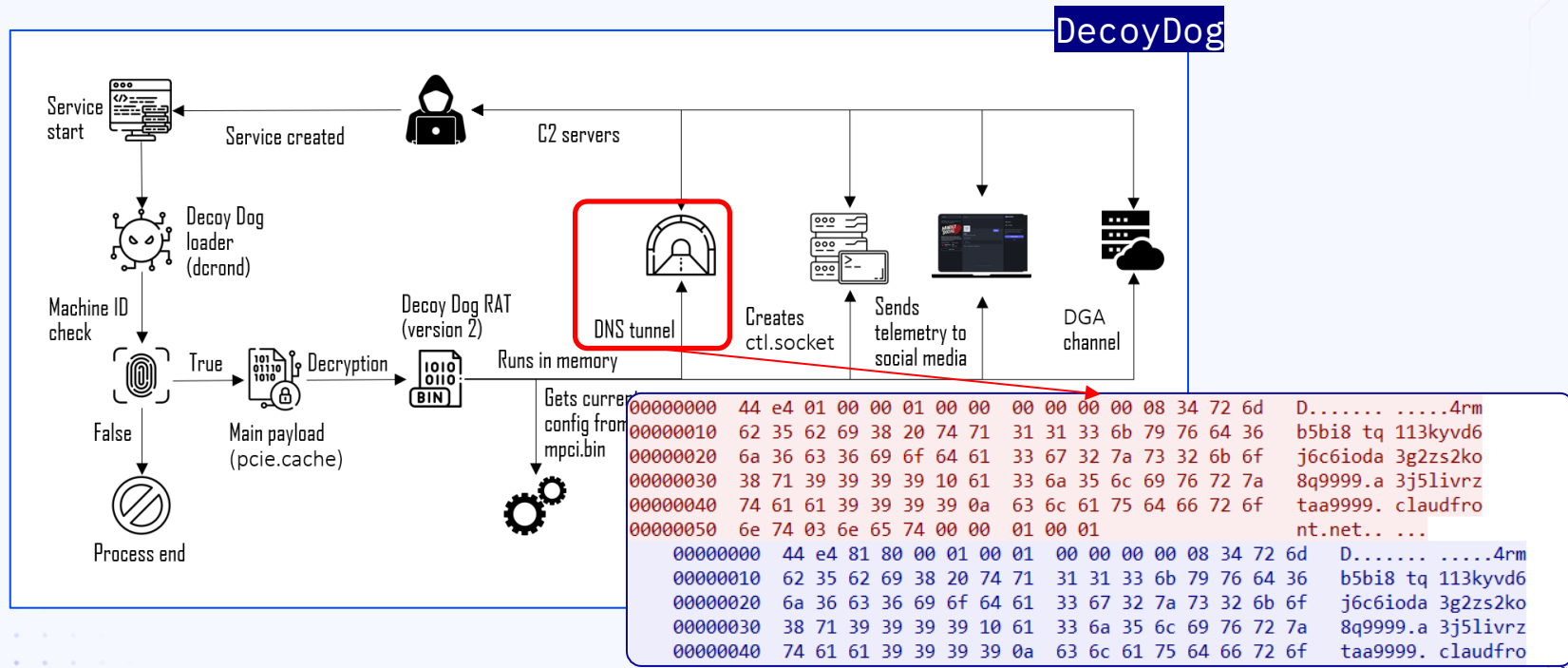
```
cdn.90baf13f03000000040003000000.160303009d0100009903036713bfbela8dea1ce0
b97a5196762fe327f8da77.0a06e9aff09fff3a4f07cc1400002ac02cc02bc030c02f009f00
9ec024c023.c028c027c00ac009c014c013009d009c003d003c00.ns1.brownsr.com
```

Protocol	Length	Info
DNS	110	Standard query 0xe5ac A cdn.0000000001000000010000000000.ns1.brownsr.com
DNS	110	Standard query 0xb78d A cdn.0000000002000000010000000000.ns1.brownsr.com
DNS	110	Standard query 0xdc5e A cdn.0000000003000000010000000000.ns1.brownsr.com
DNS	110	Standard query 0x0600 A cdn.000000000a000000010000000000.ns1.brownsr.com
DNS	110	Standard query 0x4746 A cdn.000000000b000000010000000000.ns1.brownsr.com
DNS	110	Standard query 0x0f5b A cdn.000000000c000000010000000000.ns1.brownsr.com
DNS	110	Standard query 0x09ee A cdn.0000000001300000010000000000.ns1.brownsr.com
DNS	110	Standard query 0x49ed A cdn.0000000001400000010000000000.ns1.brownsr.com
DNS	110	Standard query 0x438b A cdn.0000000001500000010000000000.ns1.brownsr.com
DNS	110	Standard query 0x454a A cdn.0000000001c00000010000000000.ns1.brownsr.com
DNS	110	Standard query 0xab88 A cdn.0000000001d00000010000000000.ns1.brownsr.com
DNS	110	Standard query 0x7871 A cdn.0000000001e00000010000000000.ns1.brownsr.com
DNS	110	Standard query 0x4e4d A cdn.0000000002500000010000000000.ns1.brownsr.com
DNS	110	Standard query 0xc956 A cdn.0000000002600000010000000000.ns1.brownsr.com

0000	52 54 00 36 3e ff 52 54 00 fb 2a cb 08 00 45 00	RT<6>RT ..*...E-
0010	00 60 82 6b 00 00 80 11 cd 66 c0 a8 64 3b 2d 3d	..k....-f..d;=
0020	98 9a e3 55 00 35 00 4c 88 36 e5 ac 01 00 00 01	...U-5-L -6-.....
0030	00 00 00 00 00 00 03 63 64 6e 1c 30 30 30 30 30	c dn-00000
0040	30 30 30 30 31 30 30 30 30 30 30 30 31 30 30 30	00001000 00001000
0050	30 30 30 30 30 30 03 6e 73 31 09 62 72 6f 77	00000000 ns1.brow
0060	6e 73 77 65 72 03 63 6f 6d 00 00 01 00 01	nsr-c0 m-....

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)

TCP Connect Scan

A service / TCP socket is listening on the host to complete the TCP three way handshake.

```

sequenceDiagram
    participant S as Scanner
    participant K as kernel tcp/ip stack
    participant G as GTPDOOR
    S->>K: SYN
    K->>S: SYN ACK
    S->>K: ACK
    K->>S: ACK RST
    S->>G: "GTPDOOR alive"
  
```

ACK Scan

No service / TCP socket required on dest port. Firewall not stateful (does not drop ACK)

```

sequenceDiagram
    participant S as Scanner
    participant K as kernel tcp/ip stack
    participant G as GTPDOOR
    S->>K: ACK
    K->>S: ACK RST
    S->>G: "GTPDOOR alive"
  
```



24

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)	0000	08 00 00 00 00 00 02 00 01 04 06 08 00 27 2c	',
> Linux cooked capture v2	0010	b0 e3 00 00 45 00 00 42 30 05 40 00 40 11 e9 4e	E-B 0-@-N
> Internet Protocol Version 4, Src: 192.168.80.1, Dst: 192.168.80.5	0020	c0 a8 50 01 c0 a8 50 05 89 b3 08 4b 00 2e 21 97	..P..P...K..!
> User Datagram Protocol, Src Port: 35251, Dst Port: 2123	0030	00 01 a2 a1 a4 a3 00 00 a5 a6 a7 a8 a9 01 02 03	C&*&C) &
> GPRS Tunneling Protocol Prime	0040	04 72 1f 18 08 05 0e 00 43 26 2a 26 43 29 20 26	..r.....B1*'+
> Flags: 0x00	0050	42 31 2a 27 40 2b	
> 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			
> Unknown extension header			
> [Expert Info (Warning/Protocol): Unknown extension header]			
> [Unknown extension header]			
> [Severity level: Warning]			
> [Group: Protocol]			
> [Response In: 5]			

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**

.gif

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



image/jpeg

JFIF

```
2d...<BASE64_START>?VvqQAAMAAAEAAAAA/  
8AAlGAAAAAIAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAGAAAAA4fug4AtAnINibgBTM  
0hVhpgYBwcm9ncmFtIGlnbmh5dCBlZSBydW4gaW4gR9ETIG1vZGluDQ0KJAAAAAAAAABQQAATAEDAF/  
66mCAAAAAAAAAAAIAIALATAADGYAAAGAAAAAAAAA/  
1YYAAAgAAAAAAAAAAEAfgAAAAAGABAAAAAAAAAAAAAGAAAAAAAAAACgAAAAgAAAAAAAAAHYUUAABAAABAA  
AAAEAAAEAAAAAAAAABAAAAAAAAAAAAALBWGABLAAAAAGAYAAAEAAAAAAAAAAAAAAAAAAAAAAIAYAAwAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAIAAACAAAAAA  
AAACCAAAEEAAAAAAAAAAAAAAAC50ZHx0AAAAABDCYAAEAAGAA08EAAIAAAAAAAAAAAAAAAAAAAAAAGauncNvY
```

27

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 70 a0 c1 f9 62 2a f3 1e ec b1 6a b7 0a fb 25 3a ....b*...i...%:
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 ce 1f 90 93 73 f2 cf 8a b6 37 0a 5a 08 3e a2 }.....: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."...T...
00000080 2e eb 3b f8 f3 b1 b6 7a fd 71 bf f1 bf 45 6a a8 .;...z...q...Ej.
00000090 39 c5 a3 40 d8 41 d1 96 5c c8 e8 72 69 1c .;...@...i...r...
000000a0 73 d8 2e 82 3e 23 9d 3f 1b 51 e3 98 92 75 .s...>#...P.Q...u
000000b0 39 c5 a3 40 d8 41 d1 96 5c c8 e8 72 69 1c .s...>#...P.Q...u
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 c4 d4 2c 6e 3f 8b f7 4a a9 fc ...8.L...n6...J.
000000e0 27 2a 7b 37 1b 25 eb 1e c2 de dc 49 f5 f3 c6 *[7...l...<.
000000f0 82 74 55 4f a8 49 df 03 c4 00 22 ff ff 92 19 9d .tUO.I...""
00000100 c1 c7 a3 66 ec 22 fd ac c6 1e a0 12 91 2d 9a 61 ...f...f...a
00000110 3a 6c 90 00 41..
00000000 31 36 00 18 d1 39 09 98 69 a4 20 00 3b 23 f1 f6 16.h.9.. i...;#..
00000010 7e de d9 ~..
000000114 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 ....&...&...Y?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...l.bl.e.#
00000023 d5 1e 0f ...
00000137 31 36 00 ea 53 e4 97 1f 22 54 49 ba 0a 70 84 c3 16...S... "Tl..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...l.bl.e.#
00000036 d5 1e 0f ...
0000016D 31 36 00 c0 03 13 bd 9a 4c 3c 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...l.bl.e.#
0000005C d5 1e 0f ...
000001A3 31 36 00 b9 76 63 fe 0b 93 cf 8b 6f 71 f2 f2 6f 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 03 19 81 99 15 1b 08 66 8e a8 a7 ...>#... ..f...
000001D6 a5 6b 9c .k.
```

```
00000000 32 34 35 00 6c 6c 59 32 36 32 53 55 43 5a 34 55 245.11Y2 62SUCZ4U
00000010 4a 4a 62 00 70 66 4d 7a 63 32 4e 4a 6c 4e 4e 55 JJbmfPfz c2ND1FNU
00000020 45 3d 59 32 36 32 53 55 43 5a 34 55 4a 4a 44 45 E=y262SU CZ4UJ3DE
00000030 53 4b 54 4f 50 2d 52 51 38 31 38 34 59 32 36 32 SKTOP-RQ R18fY262
00000040 55 55 43 5a 34 55 4a 4a 61 6c 66 6f 6e 73 59 32 SUCZ4UJJ aIfonsY2
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 CZ4UJ3J
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 3d 53 55 43 5a 34 55 4a 2SUCZ4UJ J
00000100 31 30 37 00 69 6e 66 59 32 36 32 53 55 43 5a 34 107.infY 262SUCZ4
00000110 55 4a 4a 62 6f 6e 4e 43 6a 51 31 4c 6a 67 7a 4c JJJbm0Nc jQ1LjgzL
00000120 6a 49 77 4e 79 34 78 4e 7a 6f 32 4e 54 49 79 4a jIwly4XN zo2NTTyD
00000130 51 70 42 63 48 42 45 59 58 52 68 44 51 70 75 64 QpBcHBEY XRhDQpud
00000140 47 39 7a 61 33 4a 75 62 43 35 6c 65 47 55 4e 43 G9za3JyA C51eGUnc
00000150 6c 52 79 64 57 55 4e 43 6c 52 79 64 57 55 4e 43 1RyduMUNC 1RyduMUNC
00000160 52 79 64 57 55 4e 43 6b 5a 68 62 48 4e 6c 1RyduMUNC kzhHn1
00000170 33 39 00 61 63 74 59 32 36 32 53 55 43 5a 34 55 39.actY2 62SUCZ4U
00000180 4a 4a 55 48 4a 76 5a 33 4a 68 62 53 42 4e 59 57 JJUH3vZ3 JhbSBNIW
00000190 58 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 JJUH3vZ3 JhbSBNIW
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 JJUH3vZ3 JhbSBNIW
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
```

njRAT

Custom encryption, compression and encoding

```
00000000 60 02 00 00 60 02 00 00 31 00 32 00 33 00 34 00 ..... 1.2.3.4.
00000001 35 00 36 00 00 00 00 0f 00 00 78 9c ed 57 3d 6b 5.6..... .x..M=k
00000002 db 50 14 3d 90 a9 da b3 6b ac 87 2d b6 e2 a8 b2 .P..... k..S.....
00000003 0a 81 26 2d a5 90 86 84 0d 38 a5 1a 5a 92 ed .&..... .8.....Z..
00000004 62 37 ae 12 f2 45 09 5d 0a 81 0e a5 4a d6 4e f9 b7....E.] .....C.N.
00000005 1f 99 33 a5 63 b6 1a 4a d7 0e 59 3b b8 e7 5e 59 ..3.c..J ..Yj...^Y
00000006 49 68 02 a9 5d 04 c5 e8 3c de d3 d3 91 04 be 74 Ih... ..C..
00000007 de bd f7 8d a1 84 22 26 59 5a b8 c7 6b 5a 77 50 .....& YZ..kRwP
00000008 81 01 f3 86 94 63 b4 70 7e 78 9d 5b c6 16 da 88 .....c.p ..x...
00000009 f1 1a 6f 99 6d f9 d7 0d fc 7a f7 6d df 45 35 4d .....o.....z.m.E.M
0000000a bc a1 4e 26 b0 81 0e 75 62 b2 6e 53 33 25 aa c6 ..N8.... b..nS3%..
0000000b 5e a5 a4 f9 7f 40 3a a2 74 8c 83 e0 09 e7 b9 89 V....@:.. t.....
0000000c 10 2d ce 71 9e 6b 10 b3 6e 62 89 d7 75 d4 58 0f ..q.k... nb..u.X.
0000000d 60 12 d6 c4 5d cc 29 eb 23 c0 b6 7e d1 42 81 2b ..j... .. ..-..B..
0000000e e4 c0 69 0c 3e e6 d6 ce 09 96 cb f5 b6 50 ad ac ..i..>.. .P..
0000000f ba df 7f 69 b2 3e 83 32 7b 7a 8c 57 2c f7 f6 ce ..i..>2 {z..M.
00000100 0f 4d 4c b3 fd 94 31 f0 61 79 ed 85 7b f1 f6 d5 ML...1. ay...{...
00000101 37 2f ef 72 0c 83 15 aa c0 a7 16 02 96 31 4b 13 7..r... ..1K.
00000102 ab 5c cf 07 ba aa 31 b9 0e 1a dc 13 35 aa c1 24 ..\...1. ....5..
00000103 1b 28 23 ba 89 f9 37 66 23 f9 2b 45 3e 79 3a 70 .(#...7f #..+>:p
00000104 bf 89 d2 ea da 47 5b e3 90 51 d8 64 a4 ed 1c a3 ....G[[ ..Q.d...
00000105 8d b3 2f 47 1f b3 ee c3 a2 32 2d 4a 95 49 88 cd ..G/G...2-..1...
00000106 c8 aa 0f 2b b3 b6 53 7c fd ba 70 90 58 cc ab f3 ....+... ..p.X..
00000107 11 cb 2f 7e 4a 4a 97 8c c3 b2 4c ad 29 d6 d2 58 ..-/..J... ..L...).X
00000108 3c de ff fb 2f 04 6b cb b3 b5 56 62 64 54 19 72 <.../k...VbdTr
00000109 4e 3b 6c a3 3c e4 2c c5 b6 b4 d5 fb 02 f3 4e e6 N;l.<... ..N.
0000010a c6 7b 3d 1c 24 7a 17 ed 26 fc fb 29 da 23 9f .(=.$0Z... ..).#
0000010b 5e 28 a6 2d aa f1 8d ef 78 be f0 07 ff b3 cf 5b ^(-..... }.....[
0000010c fd 36 ee d4 d3 de ba e1 90 c3 cc 31 a2 e8 86 13 ..6..... ..].....>
0000010d 99 ab e2 11 d5 5d a7 3e 9b f4 a6 0d 8d ac 9e 91 ..P..... ..M.7]P.
0000010e 69 aa 3f 15 cf 9b f8 e2 4d 8d be 0a 37 7c 3f 1b i.P..... ..U.....h
0000010f b9 bb 8d 55 d9 d9 9d f0 f5 b3 cb bd ca 88 68 d1 ..U..... ..l.c.....
00000200 83 c7 bd ed e1 21 63 ba 14 fa d5 05 ee a5 e7 1a ..g.s... ..F.B..1..
00000201 bb 8a 67 96 73 8f a3 b5 a2 46 b3 62 13 8c 6c a7 ..#...^... ..i..*..
00000202 29 23 cc d3 5e 7b fd 13 4a c0 d8 69 9b 2a f1 ..w.E3m... ..E.....
00000203 98 77 99 a5 33 6d da f2 7f f5 45 d3 b4 df 15 aa ..g.M... ..#.....
00000204 c4 67 12 4d da 8c cc 23 e5 22 b2 11 19 87 a5 ad ..9.39]..... ..o.o
00000205 e7 e7 80 39 4a 33 39 7d 84 ac db 8c c2 6f c7 6f .....
00000206 da b2 a6 be .....
00000000 1f 00 00 00 1f 00 00 00 31 00 32 00 33 00 34 00 ..... 1.2.3.4.
00000001 35 00 36 00 00 00 01 00 00 78 9c 63 00 00 5.6..... .x.c...
00000002 01 00 01 .....
00000203 01 00 00 32 01 00 00 31 00 32 00 33 00 34 00 2...2... 1.2.3.4.
00000204 35 00 36 00 00 32 75 00 78 9c ed d1 4d 4a 5.6...2u... ..x..Mj
00000205 c3 40 14 00 e0 87 4b c1 3b 78 01 5d e8 d2 33 08 .@...K... ..x...j..
00000206 62 97 22 52 5a a9 62 6a 4a 13 cf fb cf 45 8c 82 f7 b"RZ.bj ..J...E...
00000207 f2 22 be 24 fe 24 52 91 82 b8 cf be 21 93 cc bc ..$.&R... ..l...
00000208 99 c9 9b 9d 28 00 65 04 23 7a 7c 7c 7c 4d 8d .....
00000209 e3 7c df e3 .....
00000000 1f 00 00 00 1f 00 00 00 31 00 32 00 33 00 34 00 ..... 1.2.3.4.
00000001 35 00 36 00 00 00 01 00 00 78 9c 63 00 00 5.6..... .x.c...
00000002 01 00 01 .....
00000203 01 00 00 32 01 00 00 31 00 32 00 33 00 34 00 2...2... 1.2.3.4.
00000204 35 00 36 00 00 32 75 00 78 9c ed d1 4d 4a 5.6...2u... ..x..Mj
00000205 c3 40 14 00 e0 87 4b c1 3b 78 01 5d e8 d2 33 08 .@...K... ..x...j..
00000206 62 97 22 52 5a a9 62 6a 4a 13 cf fb cf 45 8c 82 f7 b"RZ.bj ..J...E...
00000207 f2 22 be 24 fe 24 52 91 82 b8 cf be 21 93 cc bc ..$.&R... ..l...
00000208 99 c9 9b 9d 28 00 65 04 23 7a 7c 7c 7c 4d 8d .....
00000209 e3 7c df e3 .....
00000000 1f 00 00 00 1f 00 00 00 31 00 32 00 33 00 34 00 ..... 1.2.3.4.
00000001 35 00 36 00 00 00 01 00 00 78 9c 63 00 00 5.6..... .x.c...
00000002 01 00 01 .....
00000203 01 00 00 32 01 00 00 31 00 32 00 33 00 34 00 2...2... 1.2.3.4.
00000204 35 00 36 00 00 32 75 00 78 9c ed d1 4d 4a 5.6...2u... ..x..Mj
00000205 c3 40 14 00 e0 87 4b c1 3b 78 01 5d e8 d2 33 08 .@...K... ..x...j..
00000206 62 97 22 52 5a a9 62 6a 4a 13 cf fb cf 45 8c 82 f7 b"RZ.bj ..J...E...
00000207 f2 22 be 24 fe 24 52 91 82 b8 cf be 21 93 cc bc ..$.&R... ..l...
00000208 99 c9 9b 9d 28 00 65 04 23 7a 7c 7c 7c 4d 8d .....
00000209 e3 7c df e3 .....
00000000 1f 00 00 00 1f 00 00 00 31 00 32 00 33 00 34 00 ..... 1.2.3.4.
00000001 35 00 36 00 00 00 01 00 00 78 9c 63 00 00 5.6..... .x.c...
00000002 01 00 01 .....
00000203 01 00 00 32 01 00 00 31 00 32 00 33 00 34 00 2...2... 1.2.3.4.
00000204 35 00 36 00 00 32 75 00 78 9c ed d1 4d 4a 5.6...2u... ..x..Mj
00000205 c3 40 14 00 e0 87 4b c1 3b 78 01 5d e8 d2 33 08 .@...K... ..x...j..
00000206 62 97 22 52 5a a9 62 6a 4a 13 cf fb cf 45 8c 82 f7 b"RZ.bj ..J...E...
00000207 f2 22 be 24 fe 24 52 91 82 b8 cf be 21 93 cc bc ..$.&R... ..l...
00000208 99 c9 9b 9d 28 00 65 04 23 7a 7c 7c 7c 4d 8d .....
00000209 e3 7c df e3 .....
00000000 1f 00 00 00 1f 00 00 00 31 00 32 00 33 00 34 00 ..... 1.2.3.4.
00000001 35 00 36 00 00 00 01 00 00 78 9c 63 00 00 5.6..... .x.c...
00000002 01 00 01 .....
00000203 01 00 00 32 01 00 00 31 00 32 00 33 00 34 00 2...2... 1.2.3.4.
00000204 35 00 36 00 00 32 75 00 78 9c ed d1 4d 4a 5.6...2u... ..x..Mj
00000205 c3 40 14 00 e0 87 4b c1 3b 78 01 5d e8 d2 33 08 .@...K... ..x...j..
00000206 62 97 22 52 5a a9 62 6a 4a 13 cf fb cf 45 8c 82 f7 b"RZ.bj ..J...E...
00000207 f2 22 be 24 fe 24 52 91 82 b8 cf be 21 93 cc bc ..$.&R... ..l...
00000208 99 c9 9b 9d 28 00 65 04 23 7a 7c 7c 7c 4d 8d .....
00000209 e3 7c df e3 .....
00000000 1f 00 00 00 1f 00 00 00 31 00 32 00 33 00 34 00 ..... 1.2.3.4.
00000001 35 00 36 00 00 00 01 00 00 78 9c 63 00 00 5.6..... .x.c...
00000002 01 00 01 .....
00000203 01 00 00 32 01 00 00 31 00 32 00 33 00 34 00 2...2... 1.2.3.4.
00000204 35 00 36 00 00 32 75 00 78 9c ed d1 4d 4a 5.6...2u... ..x..Mj
00000205 c3 40 14 00 e0 87 4b c1 3b 78 01 5d e8 d2 33 08 .@...K... ..x...j..
00000206 62 97 22 52 5a a9 62 6a 4a 13 cf fb cf 45 8c 82 f7 b"RZ.bj ..J...E...
00000207 f2 22 be 24 fe 24 52 91 82 b8 cf be 21 93 cc bc ..$.&R... ..l...
00000208 99 c9 9b 9d 28 00 65 04 23 7a 7c 7c 7c 4d 8d .....
00000209 e3 7c df e3 .....
00000000 1f 00 00 00 1f 00 00 00 31 00 32 00 33 00 34 00 ..... 1.2.3.4.
00000001 35 00 36 00 00 00 01 00 00 78 9c 63 00 00 5.6..... .x.c...
00000002 01 00 01 .....
00000203 01 00 00 32 01 00 00 31 00 32 00 33 00 34 00 2...2... 1.2.3.4.
00000204 35 00 36 00 00 32 75 00 78 9c ed d1 4d 4a 5.6...2u... ..x..Mj
00000205 c3 40 14 00 e0 87 4b c1 3b 78 01 5d e8 d2 33 08 .@...K... ..x...j..
00000206 62 97 22 52 5a a9 62 6a 4a 13 cf fb cf 45 8c 82 f7 b"RZ.bj ..J...E...
00000207 f2 22 be 24 fe 24 52 91 82 b8 cf be 21 93 cc bc ..$.&R... ..l...
00000208 99 c9 9b 9d 28 00 65 04 23 7a 7c 7c 7c 4d 8d .....
00000209 e3 7c df e3 .....
00000000 1f 00 00 00 1f 00 00 00 31 00 32 00 33 00 34 00 ..... 1.2.3.4.
00000001 35 00 36 00 00 00 01 00 00 78 9c 63 00 00 5.6..... .x.c...
00000002 01 00 01 .....
00000203 01 00 00 32 01 00 00 31 00 32 00 33 00 34 00 2...2... 1.2.3.4.
00000204 35 00 36 00 00 32 75 00 78 9c ed d1 4d 4a 5.6...2u... ..x..Mj
00000205 c3 40 14 00 e0 87 4b c1 3b 78 01 5d e8 d2 33 08 .@...K... ..x...j..
00000206 62 97 22 52 5a a9 62 6a 4a 13 cf fb cf 45 8c 82 f7 b"RZ.bj ..J...E...
00000207 f2 22 be 24 fe 24 52 91 82 b8 cf be 21 93 cc bc ..$.&R... ..l...
00000208 99 c9 9b 9d 28 00 65 04 23 7a 7c 7c 7c 4d 8d .....
00000209 e3 7c df e3 .....
00000000 1f 00 00 00 1f 00 00 00 31 00 32 00 33 00 34 00 ..... 1.2.3.4.
00000001 35 00 36 00 00 00 01 00 00 78 9c 63 00 00 5.6..... .x.c...
00000002 01 00 01 .....
00000203 01 00 00 32 01 00 00 31 00 32 00 33 00 34 00 2...2... 1.2.3.4.
00000204 35 00 36 00 00 32 75 00 78 9c ed d1 4d 4a 5.6...2u... ..x..Mj
00000205 c3 40 14 00 e0 87 4b c1 3b 78 01 5d e8 d2 33 08 .@...K... ..x...j..
00000206 62 97 22 52 5a a9 62 6a 4a 13 cf fb cf 45 8c 82 f7 b"RZ.bj ..J...E...
00000207 f2 22 be 24 fe 24 52 91 82 b8 cf be 21 93 cc bc ..$.&R... ..l...
00000208 99 c9 9b 9d 28 00 65 04 23 7a 7c 7c 7c 4d 8d .....
00000209 e3 7c df e3 .....
00000000 1f 00 00 00 1f 00 00 00 31 00 32 00 33 00 34 00 ..... 1.2.3.4.
00000001 35 00 36 00 00 00 01 00 00 78 9c 63 00 00 5.6..... .x.c...
00000002 01 00 01 .....
00000203 01 00 00 32 01 00 00 31 00 32 00 33 00 34 00 2...2... 1.2.3.4.
00000204 35 00 36 00 00 32 75 00 78 9c ed d1 4d 4a 5.6...2u... ..x..Mj
00000205 c3 40 14 00 e0 87 4b c1 3b 78 01 5d e8 d2 33 08 .@...K... ..x...j..
00000206 62 97 22 52 5a a9 62 6a 4a 13 cf fb cf 45 8c 82 f7 b"RZ.bj ..J...E...
00000207 f2 22 be 24 fe 24 52 91 82 b8 cf be 21 93 cc bc ..$.&R... ..l...
00000208 99 c9 9b 9d 28 00 65 04 23 7a 7c 7c 7c 4d 8d .....
00000209 e3 7c df e3 .....
00000000 1f 00 00 00 1f 00 00 00 31 00 32 00 33 00 34 00 ..... 1.2.3.4.
00000001 35 00 36 00 00 00 01 00 00 78 9c 63 00 00 5.6..... .x.c...
00000002 01 00 01 .....
00000203 01 00 00 32 01 00 00 31 00 32 00 33 00 34 00 2...2... 1.2.3.4.
00000204 35 00 36 00 00 32 75 00 78 9c ed d1 4d 4a 5.6...2u... ..x..Mj
00000205 c3 40 14 00 e0 87 4b c1 3b 78 01 5d e8 d2 33 08 .@...K... ..x...j..
00000206 62 97 22 52 5a a9 62 6a 4a 13 cf fb cf 45 8c 82 f7 b"RZ.bj ..J...E...
00000207 f2 22 be 24 fe 24 52 91 82 b8 cf be 21 93 cc bc ..$.&R... ..l...
00000208 99 c9 9b 9d 28 00 65 04 23 7a 7c 7c 7c 4d 8d .....
00000209 e3 7c df e3 .....
00000000 1f 00 00 00 1f 00 00 00 31 00 32 00 33 00 34 00 ..... 1.2.3.4.
00000001 35 00 36 00 00 00 01 00 00 78 9c 63 00 00 5.6..... .x.c...
00000002 01 00 01 .....
00000203 01 00 00 32 01 00 00 31 00 32 00 33 00 34 00 2...2... 1.2.3.4.
00000204 35 00 36 00 00 32 75 00 78 9c ed d1 4d 4a 5.6...2u... ..x..Mj
00000205 c3 40 14 00 e0 87 4b c1 3b 78 01 5d e8 d2 33 08 .@...K... ..x...j..
00000206 62 97 22 52 5a a9 62 6a 4a 13 cf fb cf 45 8c 82 f7 b"RZ.bj ..J...E...
00000207 f2 22 be 24 fe 24 52 91 82 b8 cf be 21 93 cc bc ..$.&R... ..l...
00000208 99 c9 9b 9d 28 00 65 04 23 7a 7c 7c 7c 4d 8d .....
00000209 e3 7c df e3 .....
00000000 1f 00 00 00 1f 00 00 00 31 00 32 00 33 00 34 00 ..... 1.2.3.4.
00000001 35 00 36 00 00 00 01 00 00 78 9c 63 00 00 5.6..... .x.c...
00000002 01 00 01 .....
00000203 01 00 00 32 01 00 00 31 00 32 00 33 00 34 00 2...2... 1.2.3.4.
00000204 35 00 36 00 00 32 75 00 78 9c ed d1 4d 4a 5.6...2u... ..x..Mj
00000205 c3 40 14 00 e0 87 4b c1 3b 78 01 5d e8 d2 33 08 .@...K... ..x...j..
00000206 62 97 22 52 5a a9 62 6a 4a 13 cf fb cf 45 8c 82 f7 b"RZ.bj ..J...E...
00000207 f2 22 be 24 fe 24 52 91 82 b8 cf be 21 93 cc bc ..$.&R... ..l...
00000208 99 c9 9b 9d 28 00 65 04 23 7a 7c 7c 7c 4d 8d .....
00000209 e3 7c df e3 .....
00000000 1f 00 00 00 1f 00 00 00 31 00 32 00 33 00 34 00 ..... 1.2.3.4.
00000001 35 00 36 00 00 00 01 00 00 78 9c 63 00 00 5.6..... .x.c...
00000002 01 00 01 .....
00000203 01 00 00 32 01 00 00 31 00 32 00 33 00 34 00 2...2... 1.2.3.4.
00000204 35 00 36 00 00 32 75 00 78 9c ed d1 4d 4a 5.6...2u... ..x..Mj
00000205 c3 40 14 00 e0 87 4b c1 3b 78 01 5d e8 d2 33 08 .@...K... ..x...j..
00000206 62 97 22 52 5a a9 62 6a 4a 13 cf fb cf 45 8c 82 f7 b"RZ.bj ..J...E...
00000207 f2 22 be 24 fe 24 52 91 82 b8 cf be 21 93 cc bc ..$.&R... ..l...
00000208 99 c9 9b 9d 28 00 65 04 23 7a 7c 7c 7c 4d 8d .....
00000209 e3 7c df e3 .....
00000000 1f 00 00 00 1f 00 00 00 31 00 32 00 33 00 34 00 ..... 1.2.3.4.
00000001 35 00 36 00 00 00 01 00 00 78 9c 63 00 00 5.6..... .x.c...
00000002 01 00 01 .....
00000203 01 00 00 32 01 00 00 31 00 32 00 33 00 34 00 2...2... 1.2.3.4.
00000204 35 00 36 00 00 32 75 00 78 9c ed d1 4d 4a 5.6...2u... ..x..Mj
00000205 c3 40 14 00 e0 87 4b c1 3b 78 01 5d e8 d2 33 08 .@...K... ..x...j..
00000206 62 97 22 52 5a a9 62 6a 4a 13 cf fb cf 45 8c 82 f7 b"RZ.bj ..J...E...
00000207 f2 22 be 24 fe 24 52 91 82 b8 cf be 21 93 cc bc ..$.&R... ..l...
00000208 99 c9 9b 9d 28 00 65 04 23 7a 7c 7c 7c 4d 8d .....
00000209 e3 7c df e3 .....
00000000 1f 00 00 00 1f 00 00 00 31 00 32 00 33 00 34 00 ..... 1.2.3.4.
00000001 35 00 36 00 00 00 01 00 00 78 9c 63 00 00 5.6..... .x.c...
00000002 01 00 01 .....
00000203 01 00 00 32 01 00 00 31 00 32 00 33 00 34 00 2...2... 1.2.3.4.
00000204 35 00 36 00 00 32 75 00 78 9c ed d1 4d 4a 5.6...2u... ..x..Mj
00000205 c3 40 14 00 e0 87 4b c1 3b 78 01 5d e8 d2 33 08 .@...K... ..x...j..
00000206 62 97 22 52 5a a9 62 6a 4a 13 cf fb cf 45 8c 82 f7 b"RZ.bj ..J...E...
00000207 f2 22 be 24 fe 24 52 91 82 b8 cf be 21 93 cc bc ..$.&R... ..l...
00000208 99 c9 9b 9d 28 00 65 04 23 7a 7c 7c 7c 4d 8d .....
00000209 e3 7c df e3 .....
00000000 1f 00 00 00 1f 00 00 00 31 00 32 00 33 00 34 00 ..... 1.2.3.4.
00000001 35 00 36 00 00 00 01 00 00 78 9c 63 00 00 5.6..... .x.c...
00000002 01 00 01 .....
00000203 01 00 00 32 01 00 00 31 00 32 00 33 00 34 00 2...2... 1.2.3.4.
00000204 35 00 36 00 00 32 75 00 78 9c ed d1 4d 4a 5.6...2u... ..x..Mj
00000205 c3 40 14 00 e0 87 4b c1 3b 78 01 5d e8 d2 33 08 .@...K... ..x...j..
00000206 62 97 22 52 5a a9 62 6a 4a 13 cf fb cf 45 8c 82 f7 b"RZ.bj ..J...E...
00000207 f2 22 be 24 fe 24 52 91 82 b8 cf be 21 93 cc bc ..$.&R... ..l...
00000208 99 c9 9b 9d 28 00 65 04 23 7a 7c 7c 7c 4d 8d .....
00000209 e3 7c df e3 .....
00000000 1f 00 00 00 1f 00 00 00 31 00 32 00 33 00 34 00 ..... 1.2.3.4.
00000001 35 00 36 00 00 00 01 00 00 78 9c 63 00 00 5.6..... .x.c...
00000002 01 00 01 .....
00000203 01 00 00 32 01 00 00 31 00 32 00 33 00 34 00 2...2... 1.2.3.4.
00000204 35 00 36 00 00 32 75 00 78 9c ed d1 4d 4a 5.6...2u... ..x..Mj
00000205 c3 40 14 00 e0 87 4b c1 3b 78 01 5d e8 d2 33 08 .@...K... ..x...j..
00000206 62 97 22 52 5a a9 62 6a 4a 13 cf fb cf 45 8c 82 f7 b"RZ.bj ..J...E...
00000207 f2 22 be 24 fe 24 52 91 82 b8 cf be 21 93 cc bc ..$.&R... ..l...
00000208 99 c9 9b 9d 28 00 65 04 23 7a 7c 7c 7c 4d 8d .....
00000209 e3 7c df e3 .....
00000000 1f 00 00 00 1f 00 00 00 31 00 32 00 33 00 34 00 ..... 1.2.3.4.
00000001 35 00 36 00 00 00 01 00 00 78 9c 63 00 00 5.6..... .x.c...
00000002 01 00 01 .....
00000203 01 00 00 32 01 00 00 31 00 32 00 33 00 34 00 2...2... 1.2.3.4.
00000204 35 00 36 00 00 32 75 00 78 9c ed d1 4d 4a 5.6...2u... ..x..Mj
00000205 c3 40 14 00 e0 87 4b c1 3b 78 01 5d e8 d2 33 08 .@...K... ..x...j..
00000206 62 97 22 52 5a a9 62 6a 4a 13 cf fb cf 45 8c 82 f7 b"RZ.bj ..J...E...
00000207 f2 22 be 24 fe 24 52 91 82 b8 cf be 21 93 cc bc ..$.&R... ..l...
00000208 99 c9 9b 9d 28 00 65 04 23 7a 7c 7c 7c 4d 8d .....
00000209 e3 7c df e3 .....
00000000 1f 00 00 00 1f 00 00 00 31 00 32 00 33 00 34 00 ..... 1.2.3.4.
00000001 35 00 36 00 00 00 01 00 00 78 9c 63 00 00 5.6..... .x.c...
00000002 01 00 01 .....
00000203 01 00 00 32 01 00 
```

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

The image displays two screenshots from the Wireshark network protocol analyzer, illustrating the frequency of malicious packets sent by a botnet.

Left Screenshot: HTTP Stream Details

The top pane shows the details of an HTTP GET request:

```
GET /bins/OERSmf8D7NSRv6iuXfcFwgFvenk4sTTqK8 HTTP/1.1
Host: conn.masjesu.zip
User-Agent: Wget/1.21.2
Accept: */*
Accept-Encoding: identity
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.22.1
Date: Fri, 14 Feb 2025 22:28:48 GMT
Content-Type: application/octet-stream
Content-Length: 120808
Connection: keep-alive
Last-Modified: Fri, 14 Feb 2025 22:00:02 GMT
ETag: "67afbce2-1d7e8"
X-Cache-Status: HIT
Accept-Ranges: bytes
```

The bottom pane shows the raw data of the stream, which is a large block of binary data (hex dump).

Right Screenshot: TCP Stream Details

The top pane shows the details of a TCP stream:

```
1. [1;95mDevice Connected: 192.168.100.188 | Port: 22 | Arch: x86_64.[0m
! BOTKILL
.ep
```

The bottom pane shows the raw data of the stream, which is a large block of binary data (hex dump).

Stream Statistics

Both screenshots include a 'Stream' tab at the bottom right, which displays the total number of streams for the selected conversation:

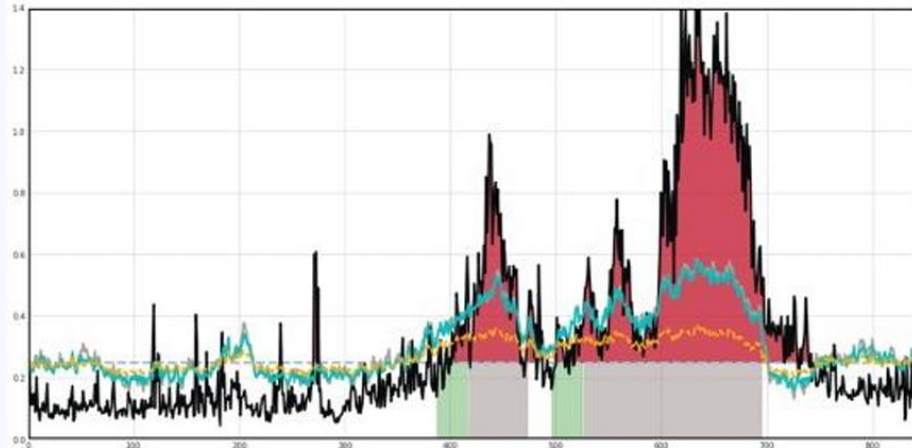
- Left Screenshot: 704 total streams.
- Right Screenshot: 8,368 total streams.

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**



```
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: "1745329633.7278938-23664-4057797581"
Cf-Cache-Status: DYNAMIC
CF-RAY: 934ee603ea79be6f-LHR
alt-svc: h3="443"; ma=86400
```

```
NZ.....@.....!..L.!This program cannot  
$.....RGO...&!...&!.&!.^...&!.DS...&!.M...&!.DS%...&!.DS"...&!.DS"...&!.S...&!.&.....&!  
.S#...&!.Rich.&!.PE d.....g.....P.....  
.....X X...d p.....rdata PE F..  
x.....text.....  
@....pdata.....@ @.rsrc p.....@ @.reloc.....  
ff.....H;  
u.H...f.....u.H.....H.....t9.....t(t.....t  
H.....(.....0.....H.....(.I.....H.....( M.....H.....( H.....\$.H...t$.H...|$ AVH.  
u.....D$@@...=.5.....5.....t0.....! H.....H..  
(u)...].).....t H.....H..  
\5.....@2.....@.....u?.....H.....H..8 t$.H.....t.L.....I.....H..  
&.....A.....u/. ....3.H.....\$0H...t$.8H...|$.HH...A^.....H.....\$.WH...0@.....5/.  
3.H.....\$0H...0...../. ...[.....\$.....4.....u7...o.....  
.....%.....4.....3.....@.....%.....q.....G.....H.....H.....X L...@..  
u.9.....3.....B.....wEH.....H.....u  
D$.0.....D$.0.....L.....I.....D$.0.....L.....  
D$.0.....D$.0.....u6.....u2L...3.I.....H.....H.....H.....t.L...3.I.....  
D$.0.....t)H.....H.....u.....X.....\$0...L.....I.....Y.....D$.0...3..  
H.....\$.H...t$.WH...I.....H.....H.....H.....\$.0H...t$.8H.....@..  
V.....H.....H.....[H.%t H.....L$.H...8.....H.....H.....)H..  
H.....H...D$.8H...H...D$.8H...H.....H.....v H.....H.....D$.0H.....  
H.....L.....Hk.....H.....  
H.....L.....Hk.....H.....  
H.....L.....H.....
```

4d	5a	c2	90	20	00	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	6f	...L..!	IT 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	8d	0a	n	in	DOS
0d	0a	24	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 \$%...&!
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	a2	..&!	..!	&...&!
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\$..
68	16	26	21	c3	a3	20	20	20	20	20	20	20	20	20	20	h.&!	..!	...R!
20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	50			
20	20	64	e2	80	a0	06	20	12	a5	c3	bb	67	20	20	20	d....	g	
20	20	20	20	20	20	c3	b0	20	24	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	10	20	20	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...	

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

VPN (in HTTP)

```
POST / HTTP/1.1
Host: 154.17.253.252:80
Content-Length: 1655
Content-Type: applicati
Cookie: N=es/+G10E0UZSw
kpyWxVjVYL7mBIKcWf9s8Kd
Accept-Encoding: gzip
```

```

[...T.dK.u...|'^.g5.s.R0.....p.DcEw5.v...+.f.....;s.6+~.....8....Q...f.{...j.6]....8L..0Aru.c.Y.E.....V..Yth..G...7.AA&.[...t.)...4....F..a...<].....L
.d.....@*....L.....fx.....F|..A.ew.m..snF.VC.X...R.&2..s.A..o.n..=ZxEY.d..F.jtuCM..H.P...19.A..m+.B.....X.u..7.d.....
.f.wq...}.....Y...}.....K6..Z$.#...nD~\..L...B.....X...H..6..X...Q...t...<k...5..N.....g6.U&...Q...z..Z.G...hh{y...l...*.B.....H...
.iv.....~<.G...~.....<.N.C..dlw.p...l2[f.H.j"...pW~.=.x.u.tnc.F.M.....+.....]lzo{...w...@.....n.^H...I..l...^z...T.l+...
jK\.....\..a.^r1DX...k-Y...0F%.../_iD...233.5.43699600...10...2.18.19.163...HTTP2...HEADERS[]: GET /512/3252/3252741.png
.....>...234.5.470222000...2...10.127.0.54...TCP...443 + 36648 [ACK] Seq=2766 Ack=598 Win=64768 Len=0 TSval=3764134770 TSecr=416473881
f.A?CR...u...l...235.5.470386000...2...10.127.0.54...TCP...443 + 36648 [ACK] Seq=2766 Ack=690 Win=64768 Len=0 TSval=3764134770 TSecr=416473881

```

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

Ksenia Naumova (@naumovax)