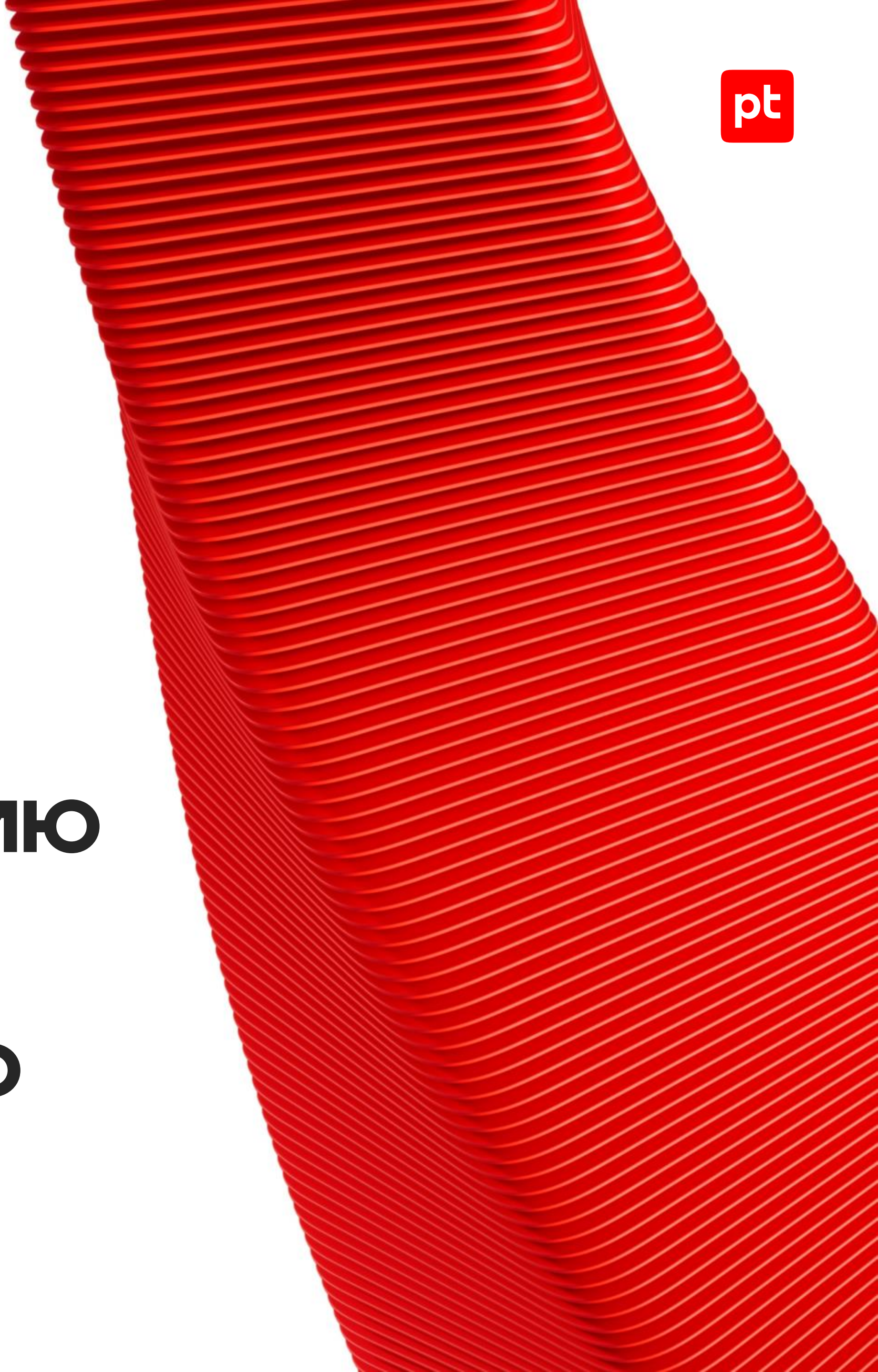
Ксения Наумова

Специалист отдела обнаружения вредоносного ПО
экспертного центра безопасности Positive Technologies

Современные подходы злоумышленников к сокрытию сетевого взаимодействия вредоносного программного обеспечения



Обо мне

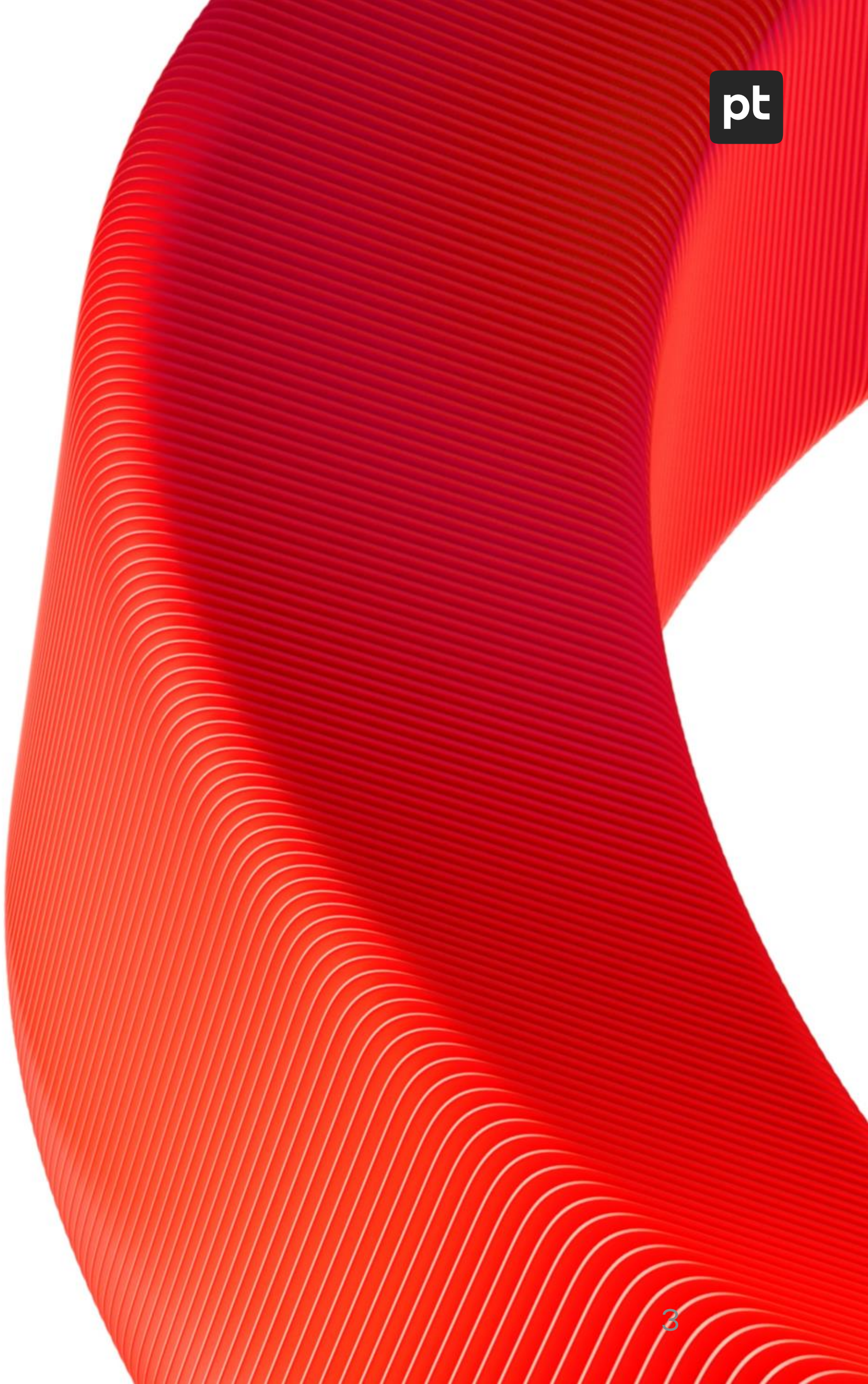
- более 4-х лет работаю в сетевой аналитике вредоносного ПО (Лаборатория Касперского, Positive Technologies)
- закончила бакалавриат по информационной безопасности в МЭИ и заканчиваю магистратуру в МИФИ
- периодически занимаюсь преподавательской деятельностью, в том числе на студенческих программах в Сириусе и в вузах
- активно участвую в жизни ИБ-сообщества – в российских и международных конференциях, в организации соревнований по практической ИБ (CTF)
- веду блог по сетевой аналитике ВПО в твиттере

О чем доклад

Большинство вредоносного ПО использует взаимодействие по сети: для скачивания вредоносных файлов, взаимодействия с управляющим сервером. Для сокрытия трафика хакеры используют различные **методы шифрования и обфускации** — это нужно для того, чтобы специалистам ИБ, изучающим сетевые пакеты, было **сложнее определить вредоносность**.
Сегодня на докладе мы рассмотрим:

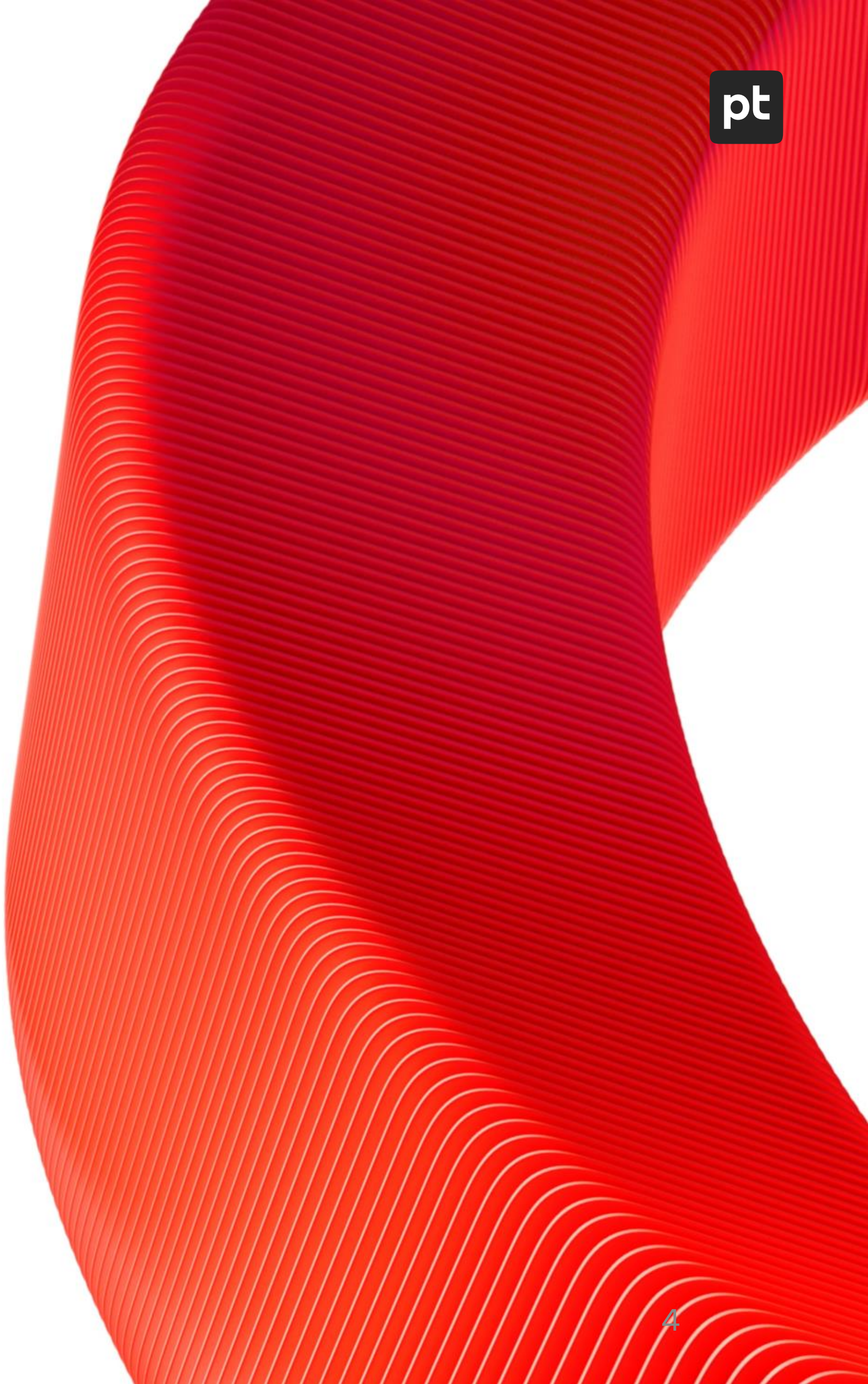
Современные подходы злоумышленников к сокрытию ВПО в сети

Актуальные способы его исследования, детектирования и дальнейшего обнаружения



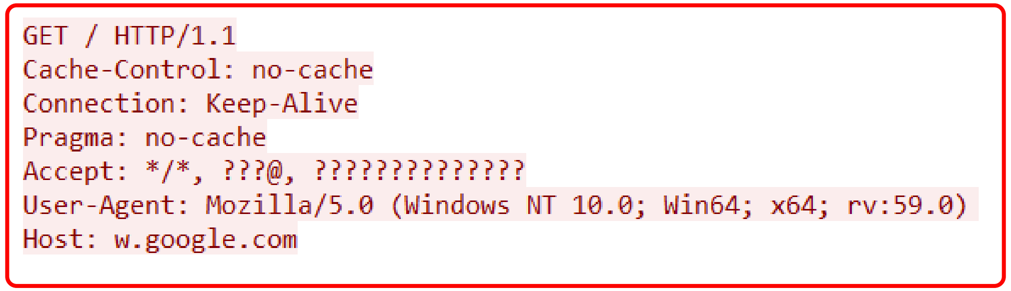
О чем доклад

- Сжатие: zlib, gzip
- Шифрование: AES, RC4
- Мимикрия под TLS
- DNS туннелирование
- Сдвиги и XOR-ы
- Base64, netbios, hex



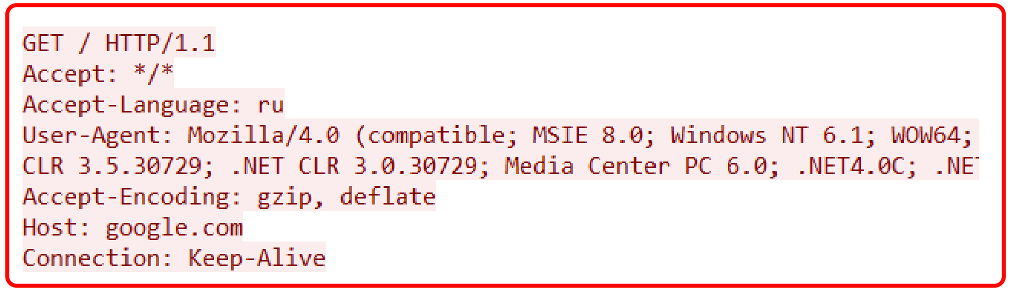
Какой из запросов к google поддельный?

1



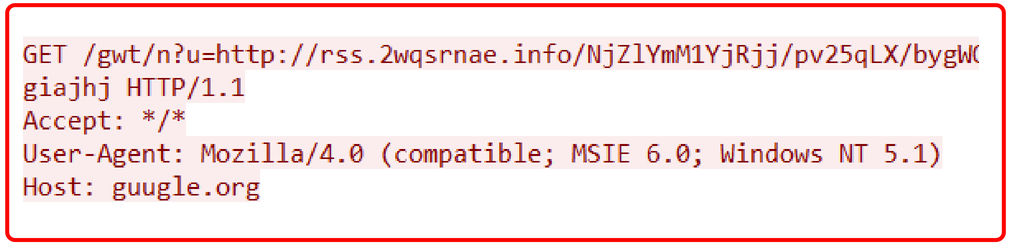
```
GET / HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Accept: */*, ???@, ??????????????
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0)
Host: w.google.com
```

2



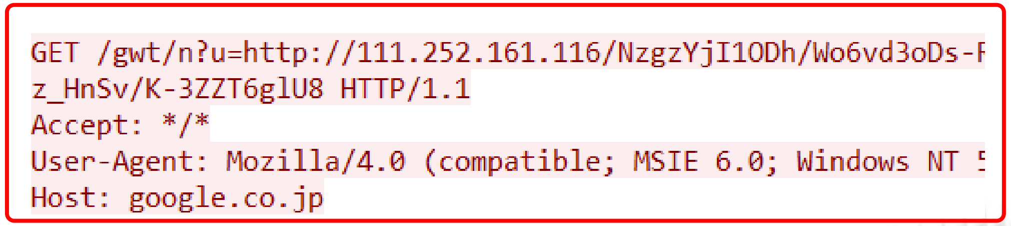
```
GET / HTTP/1.1
Accept: */*
Accept-Language: ru
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64;
CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NE
Accept-Encoding: gzip, deflate
Host: google.com
Connection: Keep-Alive
```

3



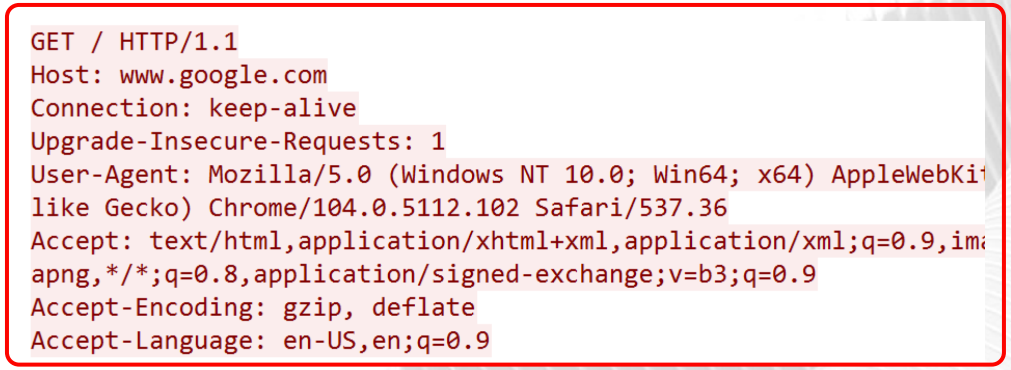
```
GET /gwt/n?u=http://rss.2wqsrnae.info/NjZlYmM1YjRjj/pv25qLX/bygW
giajhj HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: guugle.org
```

4



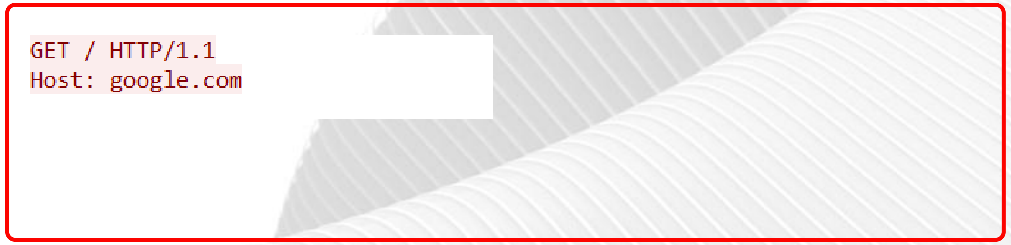
```
GET /gwt/n?u=http://111.252.161.116/NzgzYjI1ODh/Wo6vd3oDs-
z_HnSv/K-3ZZT6glU8 HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT
Host: google.co.jp
```

5



```
GET / HTTP/1.1
Host: www.google.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKi
like Gecko) Chrome/104.0.5112.102 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,im
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

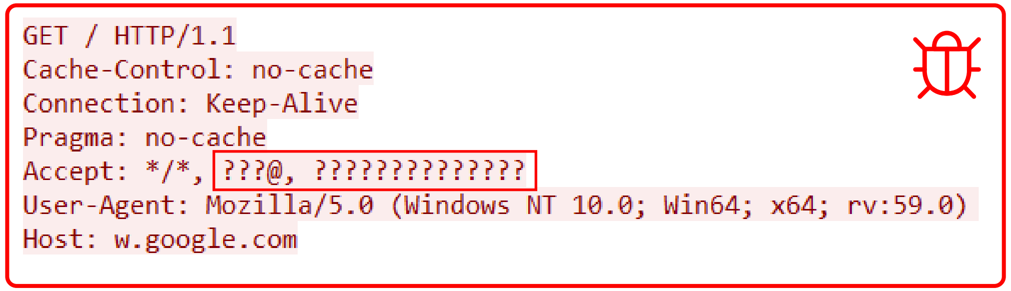
6



```
GET / HTTP/1.1
Host: google.com
```

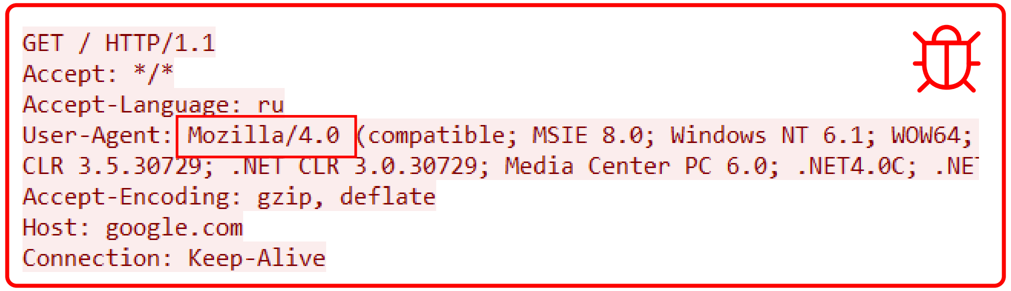
Какой из запросов к google поддельный?

1



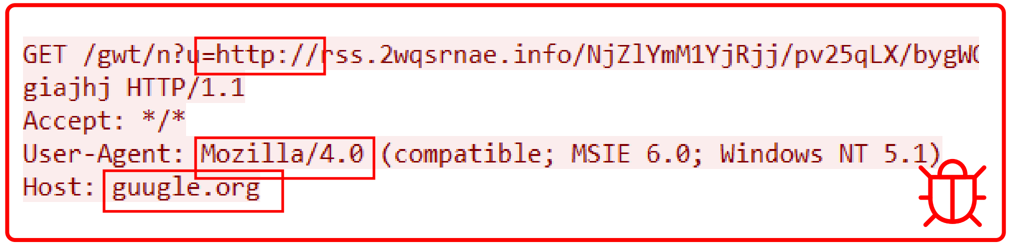
```
GET / HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Accept: */*, ???@, ??????????????
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0)
Host: w.google.com
```

2



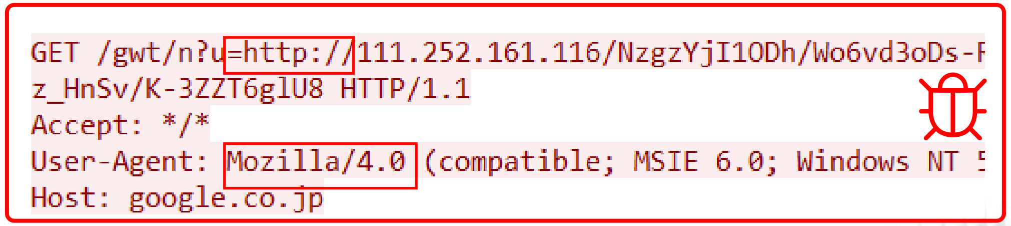
```
GET / HTTP/1.1
Accept: */*
Accept-Language: ru
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64;
CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NE
Accept-Encoding: gzip, deflate
Host: google.com
Connection: Keep-Alive
```

3



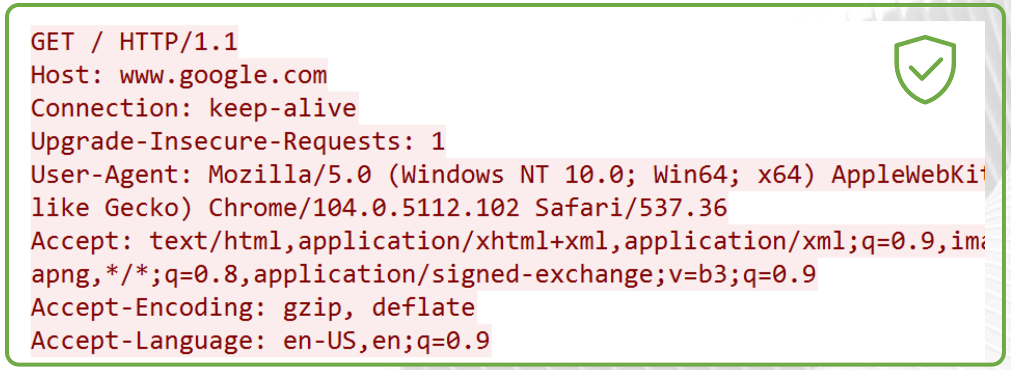
```
GET /gwt/n?u=http://rss.2wqsrnae.info/NjZlYmM1YjRjj/pv25qLX/bygW
giajhj HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: guugle.org
```

4



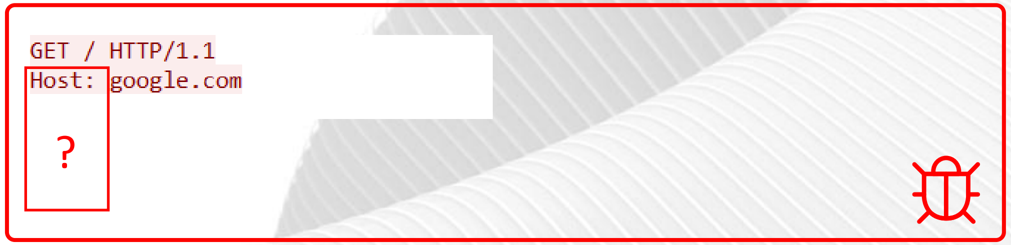
```
GET /gwt/n?u=http://111.252.161.116/NzgzYjI1ODh/Wo6vd3oDs-F
z_HnSv/K-3ZZT6glU8 HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5
Host: google.co.jp
```

5



```
GET / HTTP/1.1
Host: www.google.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit
like Gecko) Chrome/104.0.5112.102 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,ima
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

6



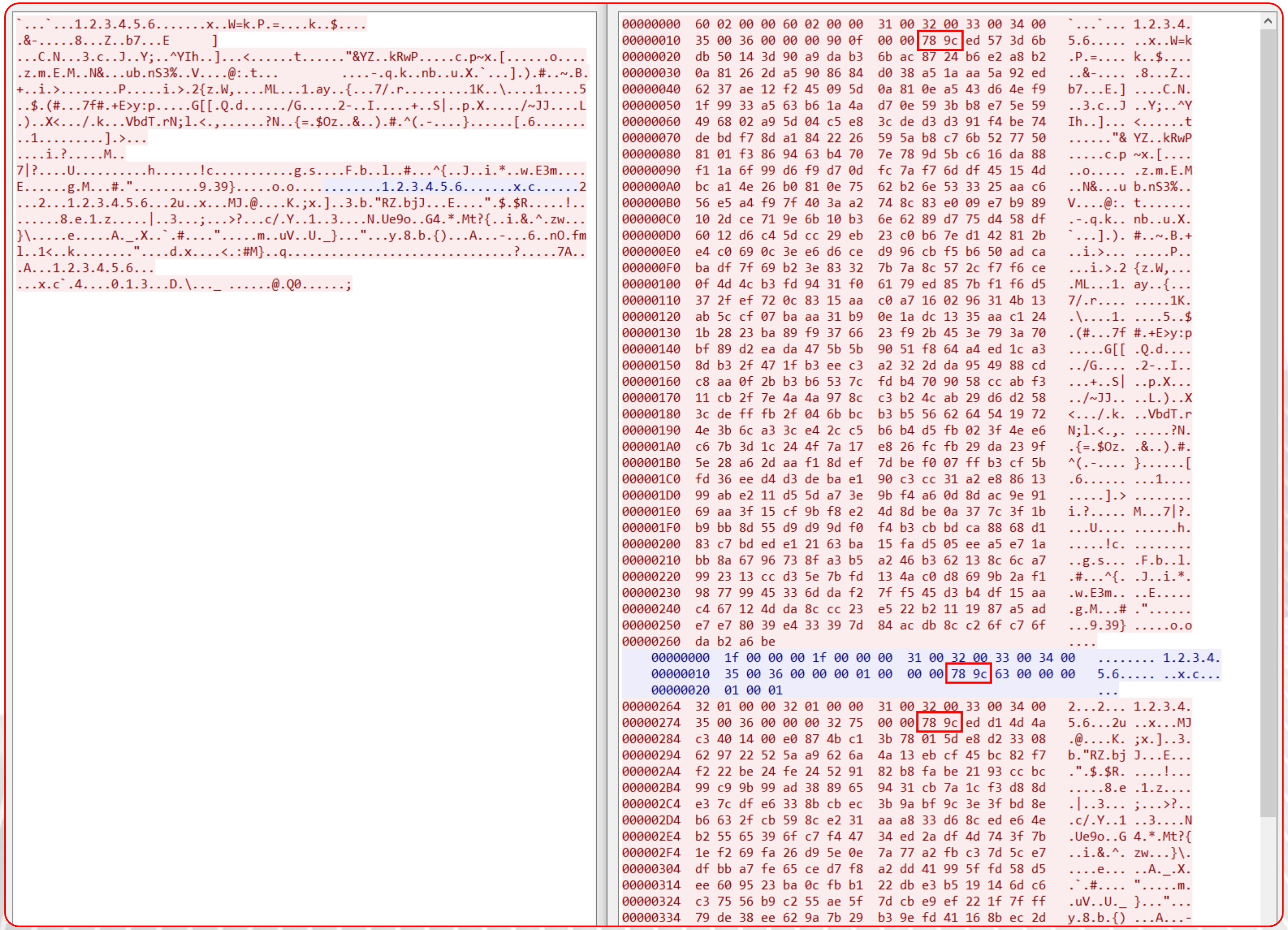
```
GET / HTTP/1.1
Host: google.com

?
```

01

Современные подходы злоумышленников к сокрытию сетевого взаимодействия вредоносного программного обеспечения

Сжатие: zlib, gzip

Gh0st RAT

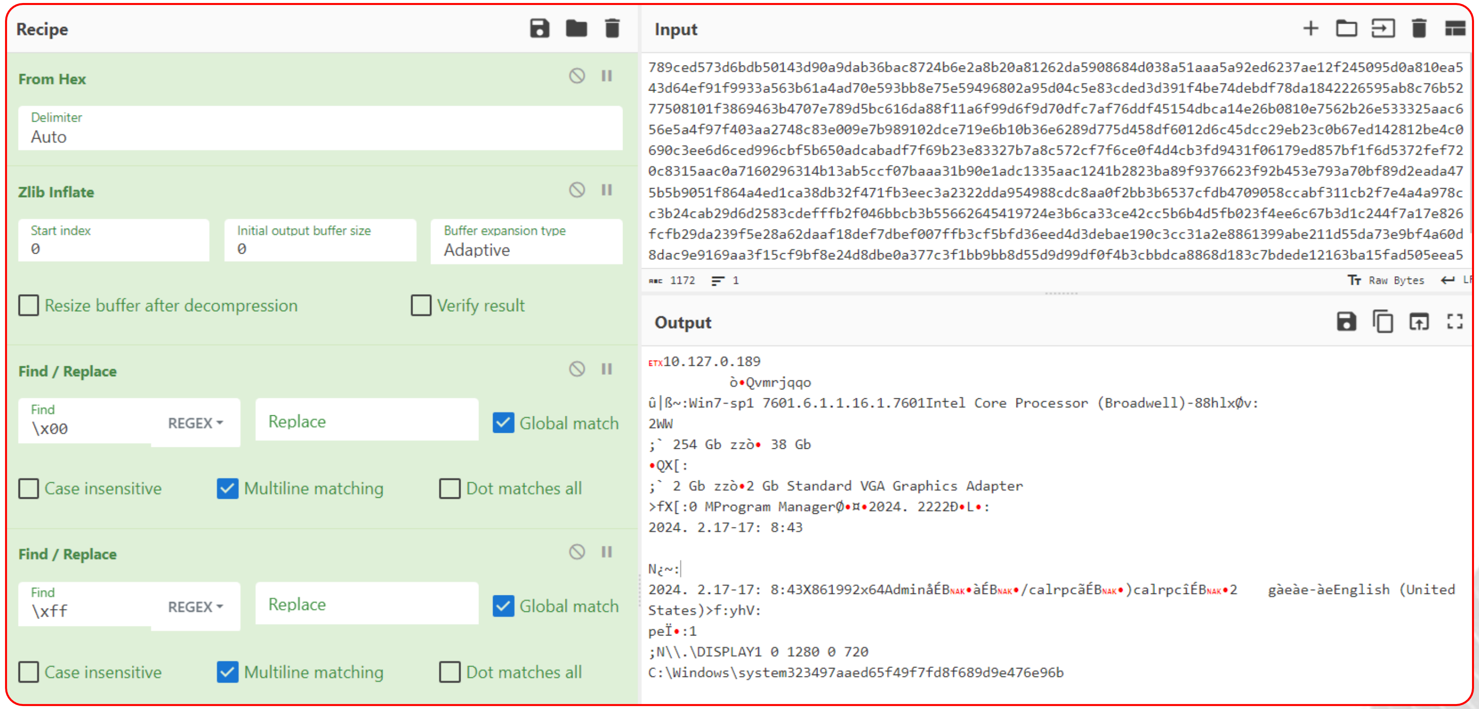


```
`...`...1.2.3.4.5.6.......x..W=k.P.=....k..$....
.&-.....8...Z..b7...E      ]
...C.N...3.c..J..Y;..^YIh..]...<......t......"&YZ..kRwP.....c.p~x.[......o....
.z.m.E.M..N&...ub.nS3%..V....@:.t...          ....-.q.k..nb..u.X.`...].).#..~.B.
+..i.>........P.....i.>.2{z.W,....ML...1.ay..{...7/.r.........1K..\....1.....5
..$.(#...7f#.+E>y:p.....G[[.Q.d....../G.....2-..I.....+..S|..p.X...../~JJ....L
.)..X<.../.k...VbdT.rN;l.<.,......?N..{=.$Oz..&..).#.^(.-....}......[.6.......
..1.........].>...
....i.?.....M..
7|?....U..........h......!c...........g.s....F.b..l..#...^{..J..i.*..w.E3m....
E......g.M...#.".........9.39}.....o.o...........1.2.3.4.5.6.......x.c.......2
...2...1.2.3.4.5.6...2u..x...MJ.@....K.;x.]..3.b."RZ.bjJ...E....".$.$R.....!..
......8.e.1.z.....|..3...;...>?...c/.Y..1..3....N.Ue9o..G4.*.Mt?{..i.&.^.zw...
}\.....e.....A._.X..`.#...."....m..uV..U._}..."...y.8.b.{)...A...-...6..n0.fm
l..1<..k........"....d.x....<.:#M}..q...............................?.....7A..
.A...1.2.3.4.5.6...
...x.c`.4....0.1.3...D.\..._ ......@.Q0......;
```

```
00000000  60 02 00 00 60 02 00 00  31 00 32 00 33 00 34 00   `...`... 1.2.3.4.
00000010  35 00 36 00 00 00 90 0f  00 00 78 9c ed 57 3d 6b   5.6..... ..x..W=k
00000020  db 50 14 3d 90 a9 da b3  6b ac 87 24 b6 e2 a8 b2   .P.=.... k..$....
00000030  0a 81 26 2d a5 90 86 84  d0 38 a5 1a aa 5a 92 ed   ..&-.... .8...Z..
00000040  62 37 ae 12 f2 45 09 5d  0a 81 0e a5 43 d6 4e f9   b7...E.] ....C.N.
00000050  1f 99 33 a5 63 b6 1a 4a  d7 0e 59 3b b8 e7 5e 59   ..3.c..J ..Y;..^Y
00000060  49 68 02 a9 5d 04 c5 e8  3c de d3 d3 91 f4 be 74   Ih..]... <......t
00000070  de bd f7 8d a1 84 22 26  59 5a b8 c7 6b 52 77 50   ......"& YZ..kRwP
00000080  81 01 f3 86 94 63 b4 70  7e 78 9d 5b c6 16 da 88   .....c.p ~x.[....
00000090  f1 1a 6f 99 d6 f9 d7 0d  fc 7a f7 6d df 45 15 4d   ..o..... .z.m.E.M
000000A0  bc a1 4e 26 b0 81 0e 75  62 b2 6e 53 33 25 aa c6   ..N&...u b.nS3%..
000000B0  56 e5 a4 f9 7f 40 3a a2  74 8c 83 e0 09 e7 b9 89   V....@:. t.......
000000C0  10 2d ce 71 9e 6b 10 b3  6e 62 89 d7 75 d4 58 df   .-.q.k.. nb..u.X.
000000D0  60 12 d6 c4 5d cc 29 eb  23 c0 b6 7e d1 42 81 2b   `...].). #..~.B.+
000000E0  e4 c0 69 0c 3e e6 d6 ce  d9 96 cb f5 b6 50 ad ca   ..i.>... .....P..
000000F0  ba df 7f 69 b2 3e 83 32  7b 7a 8c 57 2c f7 f6 ce   ...i.>.2 {z.W,...
00000100  0f 4d 4c b3 fd 94 31 f0  61 79 ed 85 7b f1 f6 d5   .ML...1. ay..{...
00000110  37 2f ef 72 0c 83 15 aa  c0 a7 16 02 96 31 4b 13   7/.r.... .....1K.
00000120  ab 5c cf 07 ba aa 31 b9  0e 1a dc 13 35 aa c1 24   .\....1. ....5..$
00000130  1b 28 23 ba 89 f9 37 66  23 f9 2b 45 3e 79 3a 70   .(#...7f #.+E>y:p
00000140  bf 89 d2 ea da 47 5b 5b  90 51 f8 64 a4 ed 1c a3   .....G[[ .Q.d....
00000150  8d b3 2f 47 1f b3 ee c3  a2 32 2d da 95 49 88 cd   ../G.... .2-..I..
00000160  c8 aa 0f 2b b3 b6 53 7c  fd b4 70 90 58 cc ab f3   ...+..S| ..p.X...
00000170  11 cb 2f 7e 4a 4a 97 8c  c3 b2 4c ab 29 d6 d2 58   ../~JJ.. ..L.)..X
00000180  3c de ff fb 2f 04 6b bc  b3 b5 56 62 64 54 19 72   <.../.k. ..VbdT.r
00000190  4e 3b 6c a3 3c e4 2c c5  b6 b4 d5 fb 02 3f 4e e6   N;l.<.,. .....?N.
000001A0  c6 7b 3d 1c 24 4f 7a 17  e8 26 fc fb 29 da 23 9f   .{=.$Oz. .&..).#.
000001B0  5e 28 a6 2d aa f1 8d ef  7d be f0 07 ff b3 cf 5b   ^(.-.... }......[
000001C0  fd 36 ee d4 d3 de ba e1  90 c3 cc 31 a2 e8 86 13   .6...... ...1....
000001D0  99 ab e2 11 d5 5d a7 3e  9b f4 a6 0d 8d ac 9e 91   .....].> ........
000001E0  69 aa 3f 15 cf 9b f8 e2  4d 8d be 0a 37 7c 3f 1b   i.?..... M...7|?.
000001F0  b9 bb 8d 55 d9 d9 9d f0  f4 b3 cb bd ca 88 68 d1   ...U.... ......h.
00000200  83 c7 bd ed e1 21 63 ba  15 fa d5 05 ee a5 e7 1a   .....!c. ........
00000210  bb 8a 67 96 73 8f a3 b5  a2 46 b3 62 13 8c 6c a7   ..g.s... .F.b..l.
00000220  99 23 13 cc d3 5e 7b fd  13 4a c0 d8 69 9b 2a f1   .#...^{. .J..i.*.
00000230  98 77 99 45 33 6d da f2  7f f5 45 d3 b4 df 15 aa   .w.E3m.. ..E.....
00000240  c4 67 12 4d da 8c cc 23  e5 22 b2 11 19 87 a5 ad   .g.M...# .".....
00000250  e7 e7 80 39 e4 33 39 7d  84 ac db 8c c2 6f c7 6f   ...9.39} .....o.o
00000260  da b2 a6 be                                        ....
    00000000  1f 00 00 00 1f 00 00 00  31 00 32 00 33 00 34 00   ........ 1.2.3.4.
    00000010  35 00 36 00 00 00 01 00  00 00 78 9c 63 00 00 00   5.6..... ..x.c...
    00000020  01 00 01                                           ...
00000264  32 01 00 00 32 01 00 00  31 00 32 00 33 00 34 00   2...2... 1.2.3.4.
00000274  35 00 36 00 00 00 32 75  00 00 78 9c ed d1 4d 4a   5.6...2u ..x...MJ
00000284  c3 40 14 00 e0 87 4b c1  3b 78 01 5d e8 d2 33 08   .@....K. ;x.]..3.
00000294  62 97 22 52 5a a9 62 6a  4a 13 eb cf 45 bc 82 f7   b."RZ.bj J...E...
000002A4  f2 22 be 24 fe 24 52 91  82 b8 fa be 21 93 cc bc   .".$.$R. ....!...
000002B4  99 c9 9b 99 ad 38 89 65  94 31 cb 7a 1c f3 d8 8d   .....8.e .1.z....
000002C4  e3 7c df e6 33 8b cb ec  3b 9a bf 9c 3e 3f bd 8e   .|..3... ;...>?..
000002D4  b6 63 2f cb 59 8c e2 31  aa a8 33 d6 8c ed e6 4e   .c/.Y..1 ..3....N
000002E4  b2 55 65 39 6f c7 f4 47  34 ed 2a df 4d 74 3f 7b   .Ue9o..G 4.*.Mt?{
000002F4  1e f2 69 fa 26 d9 5e 0e  7a 77 a2 fb c3 7d 5c e7   ..i.&.^. zw...}\.
00000304  df bb a7 fe 65 ce d7 f8  a2 dd 41 99 5f fd 58 d5   ....e... ..A._.X.
00000314  ee 60 95 23 ba 0c fb b1  22 db e3 b5 19 14 6d c6   .`.#.... ".....m.
00000324  c3 75 56 b9 c2 55 ae 5f  7d cb e9 ef 22 1f 7f ff   .uV..U._ }..."...
00000334  79 de 38 ee 62 9a 7b 29  b3 9e fd 41 16 8b ec 2d   y.8.b.{) ...A...-
```

Gh0st RAT & PCRAT

декодирование, детектирование, обнаружение



From Hex
Delimiter: Auto

Zlib Inflate
Start index: 0
Initial output buffer size: 0
Buffer expansion type: Adaptive
☐ Resize buffer after decompression ☐ Verify result

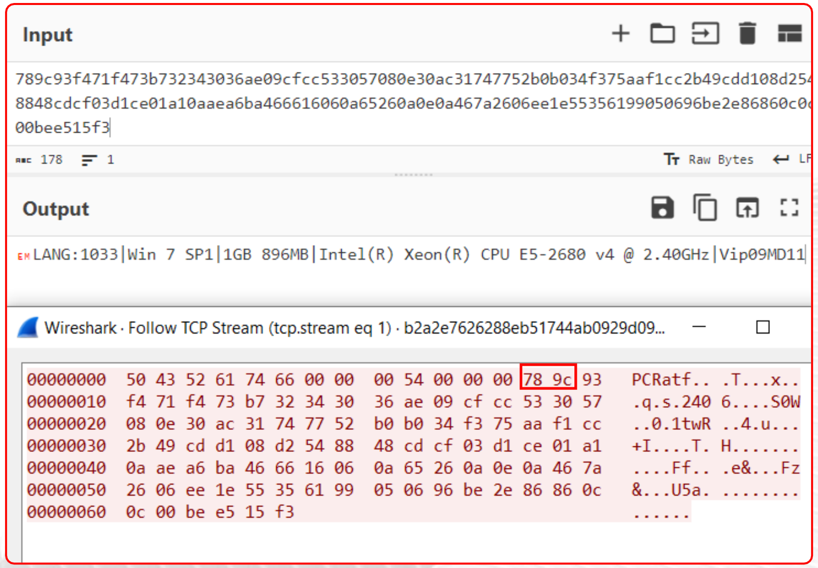
Find / Replace
Find: \x00 REGEX
Replace
☑ Global match
☐ Case insensitive ☑ Multiline matching ☐ Dot matches all

Find / Replace
Find: \xff REGEX
Replace
☑ Global match
☐ Case insensitive ☑ Multiline matching ☐ Dot matches all

```
789ced573d6bdb50143d90a9dab36bac8724b6e2a8b20a81262da5908684d038a51aaa5a92ed6237ae12f245095d0a810ea5
43d64ef91f9933a563b61a4ad70e593bb8e75e59496802a95d04c5e83cded3d391f4be74debdf78da1842226595ab8c76b52
77508101f3869463b4707e789d5bc616da88f11a6f99d6f9d70dfc7af76ddf45154dbca14e26b0810e7562b26e533325aac6
56e5a4f97f403aa2748c83e009e7b989102dce719e6b10b36e6289d775d458df6012d6c45dcc29eb23c0b67ed142812be4c0
690c3ee6d6ced996cbf5b650adcabadf7f69b23e83327b7a8c572cf7f6ce0f4d4cb3fd9431f06179ed857bf1f6d5372fef72
0c8315aac0a7160296314b13ab5ccf07baaa31b90e1adc1335aac1241b2823ba89f9376623f92b453e793a70bf89d2eada47
5b5b9051f864a4ed1ca38db32f471fb3eec3a2322dda954988cdc8aa0f2bb3b6537cfdb4709058ccabf311cb2f7e4a4a978c
c3b24cab29d6d2583cdefffb2f046bbcb3b55662645419724e3b6ca33ce42cc5b6b4d5fb023f4ee6c67b3d1c244f7a17e826
fcfb29da239f5e28a62daaf18def7dbef007ffb3cf5bfd36eed4d3debae190c3cc31a2e8861399abe211d55da73e9bf4a60d
8dac9e9169aa3f15cf9bf8e24d8dbe0a377c3f1bb9bb8d55d9d99df0f4b3cbbdca8868d183c7bdede12163ba15fad505eea5
```

1172 1 Raw Bytes LF

```
␃10.127.0.189
          ò•Qvmrjqqo
û|ß~:Win7-sp1 7601.6.1.1.16.1.7601Intel Core Processor (Broadwell)-88hlxØv:
2WW
;` 254 Gb zzò• 38 Gb
•QX[:
;` 2 Gb zzò•2 Gb Standard VGA Graphics Adapter
>fX[:0 MProgram ManagerØ•¤•2024. 2222Ð•L•:
2024. 2.17-17: 8:43

N¿~:
2024. 2.17-17: 8:43X861992x64AdminåÉB␕•àÉB␕•/calrpcãÉB␕•)calrpcîÉB␕•2    gàeàe-àeEnglish (United
States)>f:yhV:
peÏ•:1
;N\\.\DISPLAY1 0 1280 0 720
C:\Windows\system323497aaed65f49f7fd8f689d9e476e96b
```



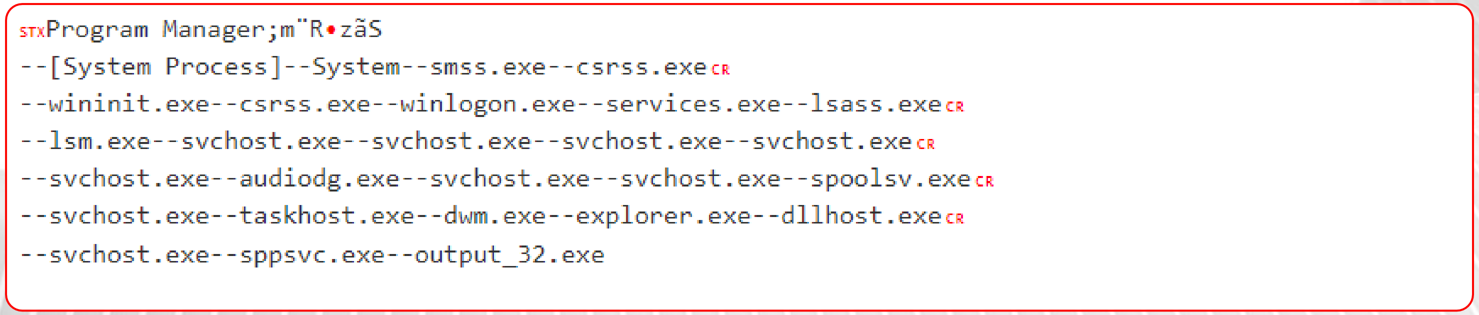
```
789c93f471f473b732343036ae09cfcc533057080e30ac31747752b0b034f375aaf1cc2b49cdd108d254
8848cdcf03d1ce01a10aaea6ba466616060a65260a0e0a467a2606ee1e55356199050696be2e86860c0
00bee515f3
```

178 1 Raw Bytes LF

```
␙LANG:1033|Win 7 SP1|1GB 896MB|Intel(R) Xeon(R) CPU E5-2680 v4 @ 2.40GHz|Vip09MD11
```

Wireshark · Follow TCP Stream (tcp.stream eq 1) · b2a2e7626288eb51744ab0929d09...

```
00000000  50 43 52 61 74 66 00 00  00 54 00 00 00 78 9c 93   PCRatf.. .T...x..
00000010  f4 71 f4 73 b7 32 34 30  36 ae 09 cf cc 53 30 57   .q.s.240 6....S0W
00000020  08 0e 30 ac 31 74 77 52  b0 b0 34 f3 75 aa f1 cc   ..0.1twR ..4.u...
00000030  2b 49 cd d1 08 d2 54 88  48 cd cf 03 d1 ce 01 a1   +I....T. H.......
00000040  0a ae a6 ba 46 66 16 06  0a 65 26 0a 0e 0a 46 7a   ....Ff.. .e&...Fz
00000050  26 06 ee 1e 55 35 61 99  05 06 96 be 2e 86 86 0c   &...U5a. ........
00000060  0c 00 be e5 15 f3                                  ......
```



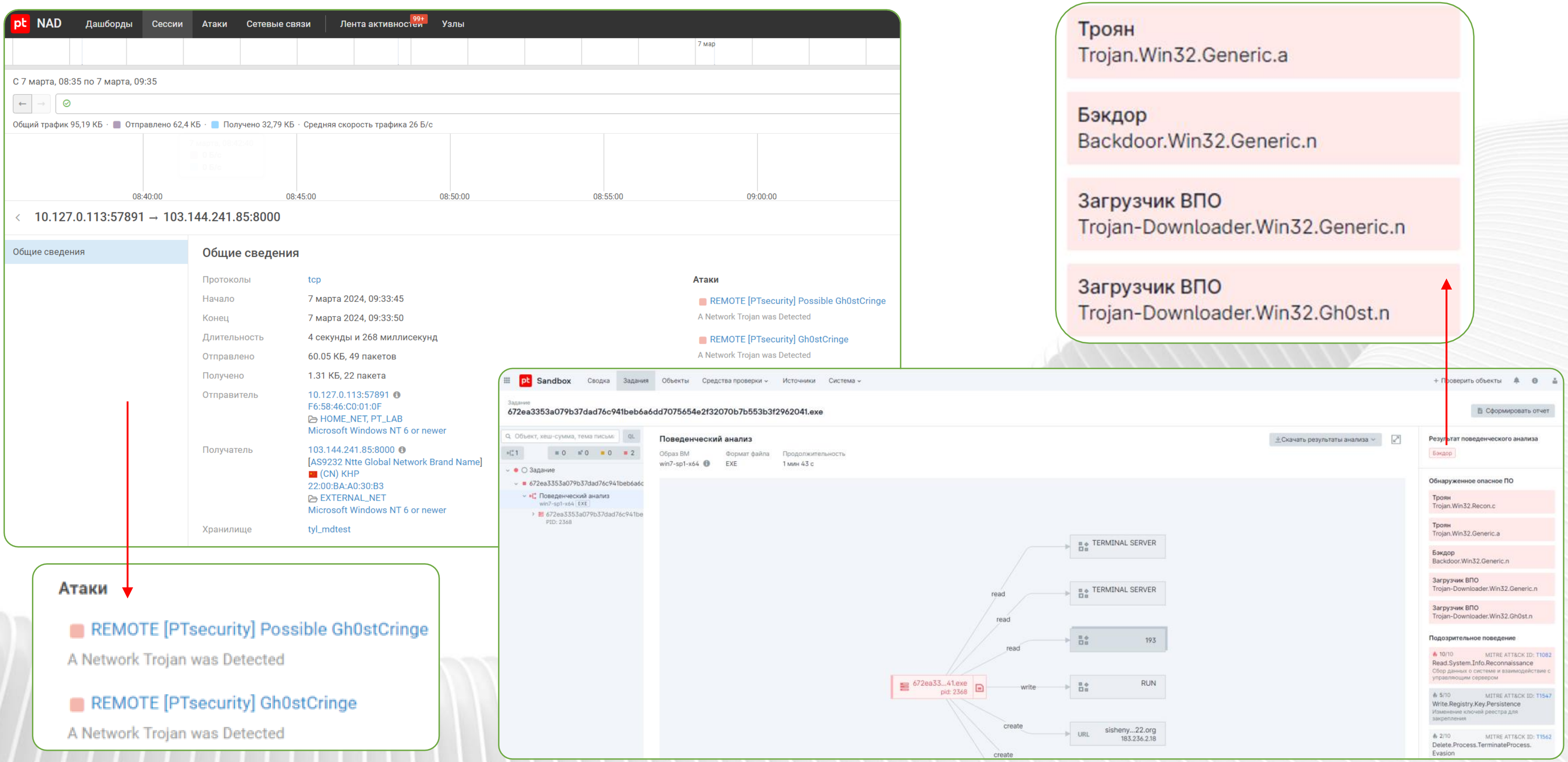
```
␂Program Manager;m¨R•zãS
--[System Process]--System--smss.exe--csrss.exe␍
--wininit.exe--csrss.exe--winlogon.exe--services.exe--lsass.exe␍
--lsm.exe--svchost.exe--svchost.exe--svchost.exe--svchost.exe␍
--svchost.exe--audiodg.exe--svchost.exe--svchost.exe--spoolsv.exe␍
--svchost.exe--taskhost.exe--dwm.exe--explorer.exe--dllhost.exe␍
--svchost.exe--sppsvc.exe--output_32.exe
```

```
Правило 1.
msg: "REMOTE [PTsecurity] Possible Gh0st";
content: "|00|"; offset: 3; depth: 1;
content: "|00|"; distance: 3; within: 1;
content: "|00 00|"; distance: 0;
pcre: "/^([0-9a-f]\x00){4,32}\x00\x00/R";
content: "|78 9c|"; distance: 4; within: 2;
```

```
content: "|00 00 78 9c|";
```

Gh0st RAT & PCRAT

декодирование, детектирование, обнаружение



С 7 марта, 08:35 по 7 марта, 09:35

Общий трафик 95,19 КБ · Отправлено 62,4 КБ · Получено 32,79 КБ · Средняя скорость трафика 26 Б/с

10.127.0.113:57891 → 103.144.241.85:8000

Общие сведения

Общие сведения

Протоколы	tcp
Начало	7 марта 2024, 09:33:45
Конец	7 марта 2024, 09:33:50
Длительность	4 секунды и 268 миллисекунд
Отправлено	60.05 КБ, 49 пакетов
Получено	1.31 КБ, 22 пакета
Отправитель	10.127.0.113:57891 F6:58:46:C0:01:0F HOME_NET, PT_LAB Microsoft Windows NT 6 or newer
Получатель	103.144.241.85:8000 [AS9232 Ntte Global Network Brand Name] (CN) КНР 22:00:BA:A0:30:B3 EXTERNAL_NET Microsoft Windows NT 6 or newer
Хранилище	tyl_mdtest

Атаки

REMOTE [PTsecurity] Possible Gh0stCringe
A Network Trojan was Detected

REMOTE [PTsecurity] Gh0stCringe
A Network Trojan was Detected

Атаки

REMOTE [PTsecurity] Possible Gh0stCringe
A Network Trojan was Detected

REMOTE [PTsecurity] Gh0stCringe
A Network Trojan was Detected

Задание
672ea3353a079b37dad76c941beb6a6dd7075654e2f32070b7b553b3f2962041.exe

- Задание
  - 672ea3353a079b37dad76c941beb6a6c
    - Поведенческий анализ win7-sp1-x64 EXE
      - 672ea3353a079b37dad76c941be PID: 2368

Поведенческий анализ

Образ ВМ	Формат файла	Продолжительность
win7-sp1-x64	EXE	1 мин 43 с

Результат поведенческого анализа
Бэкдор

Обнаруженное опасное ПО

Троян
Trojan.Win32.Recon.c

Троян
Trojan.Win32.Generic.a

Бэкдор
Backdoor.Win32.Generic.n

Загрузчик ВПО
Trojan-Downloader.Win32.Generic.n

Загрузчик ВПО
Trojan-Downloader.Win32.Gh0st.n

Подозрительное поведение

10/10 MITRE ATT&CK ID: T1082
Read.System.Info.Reconnaissance
Сбор данных о системе и взаимодействие с управляющим сервером

5/10 MITRE ATT&CK ID: T1547
Write.Registry.Key.Persistence
Изменение ключей реестра для закрепления

2/10 MITRE ATT&CK ID: T1562
Delete.Process.TerminateProcess.Evasion

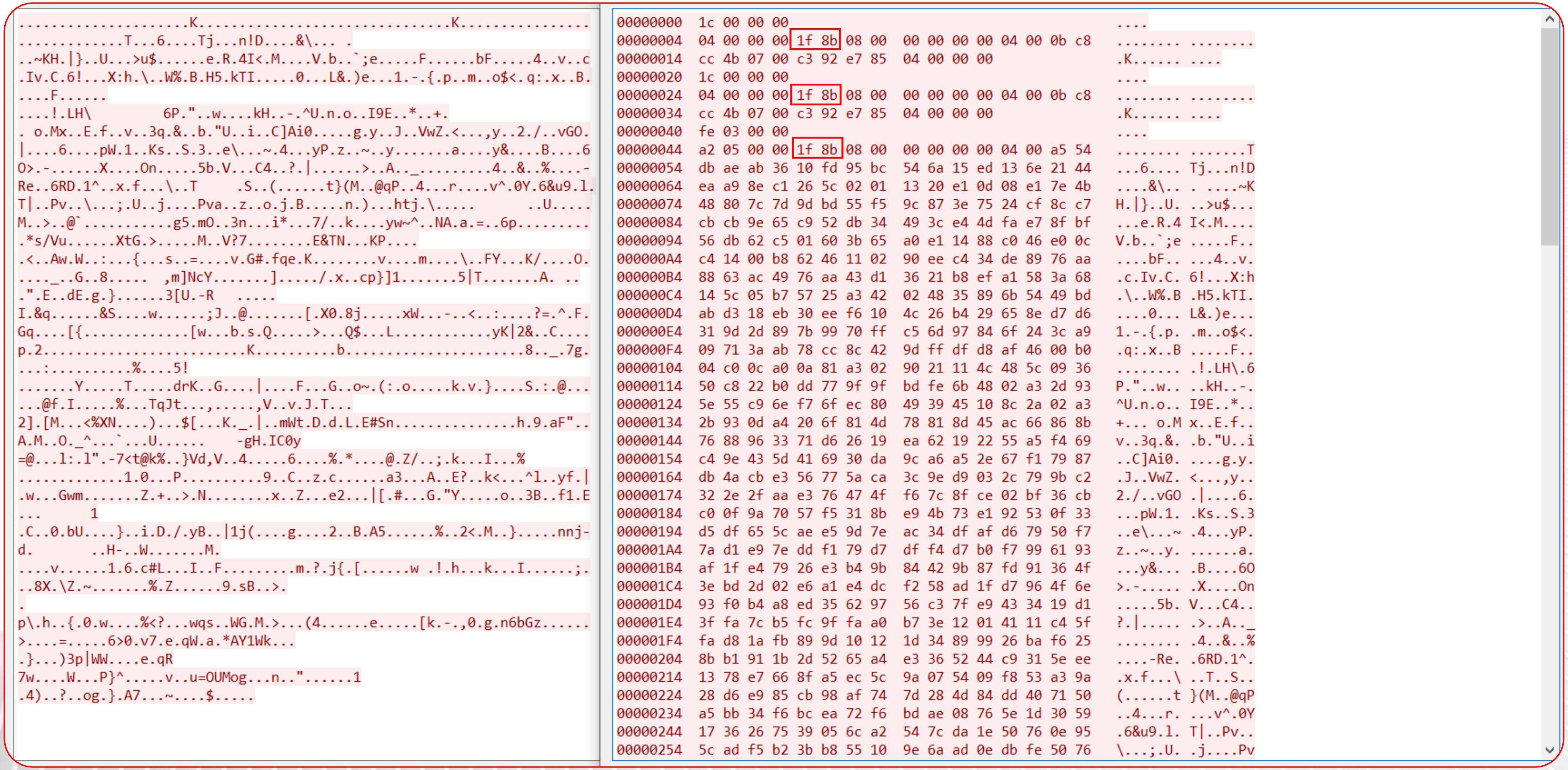
Троян
Trojan.Win32.Generic.a

Бэкдор
Backdoor.Win32.Generic.n

Загрузчик ВПО
Trojan-Downloader.Win32.Generic.n

Загрузчик ВПО
Trojan-Downloader.Win32.Gh0st.n

ZgRAT

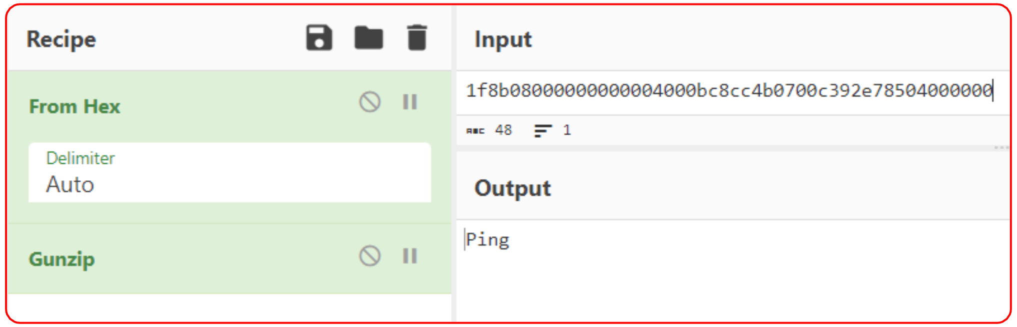


```
.....................K................................K...............
...............T...6....Tj...n!D....&\... .
..~KH.|}..U...>u$......e.R.4I<.M....V.b..`;e.....F......bF.....4..v..c
.Iv.C.6!...X:h.\..W%.B.H5.kTI.....0...L&.)e...1.-.{.p..m..o$<.q:.x..B.
....F......
....!.LH\          6P."..w....kH..-.^U.n.o..I9E..*..+.
. o.Mx..E.f..v..3q.&..b."U..i..C]Ai0.....g.y..J..VwZ.<...,y..2./..vGO.
|....6....pW.1..Ks..S.3..e\...~.4...yP.z..~..y.......a....y&....B....6
O>.-......X....On.....5b.V...C4..?.|......>..A.._.........4..&..%....-
Re..6RD.1^..x.f...\..T      .S..(......t}(M..@qP..4...r....v^.0Y.6&u9.l.
T|..Pv..\...;.U..j....Pva..z..o.j.B.....n.)...htj.\.....      ..U.....
M..>..@`...........g5.mO..3n...i*...7/..k....yw~^..NA.a.=..6p.........
.*s/Vu......XtG.>.....M..V?7.........E&TN...KP....
.<..Aw.W..:...{...s..=....v.G#.fqe.K.........v....m....\..FY...K/....O.
...._..G..8.....  ,m]NcY.......].../.x..cp}]1.......5|T.......A. ..
.".E..dE.g.}......3[U.-R   .....
I.&q......&S....w......;J..@.......[.X0.8j.....xW...-..<..:....?=.^.F.
Gq....[{.............[w...b.s.Q.....>...Q$...L............yK|2&..C....
p.2.......................K.........b.......................8.._.7g.
...:.........%....5!
.......Y.....T.....drK..G....|....F...G..o~.(:.o.....k.v.}....S.:.@...
...@f.I.....%...TqJt...,.....,V..v.J.T...
2].[M...<%XN....)...$[...K._.|..mWt.D.d.L.E#Sn...............h.9.aF"..
A.M..O._^...`...U......     -gH.IC0y
=@...1:.l".-7<t@k%..}Vd,V..4.....6....%.*....@.Z/..;.k...I...%
...............1.0...P..........9..C..z.c......a3...A..E?..k<...^l..yf.|
.w...Gwm.......Z.+..>.N.........x..Z...e2...|[.#...G."Y.....o..3B..f1.E
...       1
.C..0.bU....}..i.D./.yB..|1j(....g....2..B.A5......%..2<.M..}.....nnj-
d.         ..H-..W.......M.
....v......1.6.c#L...I..F.........m.?.j{.[......w .!.h...k...I......;.
..8X.\Z.~.......%.Z......9.sB..>.
.
p\.h..{.0.w....%<?...wqs..WG.M.>...(4......e.....[k.-.,0.g.n6bGz......
>....=.....6>0.v7.e.qW.a.*AY1Wk...
.}...)3p|WW....e.qR
7w....W...P}^.....v..u=OUMog...n..".....1
.4)..?..og.}.A7...~....$.....
```

```
00000000  1c 00 00 00                                       ....
00000004  04 00 00 00 1f 8b 08 00  00 00 00 00 04 00 0b c8  ........ ........
00000014  cc 4b 07 00 c3 92 e7 85  04 00 00 00              .K...... ....
00000020  1c 00 00 00                                       ....
00000024  04 00 00 00 1f 8b 08 00  00 00 00 00 04 00 0b c8  ........ ........
00000034  cc 4b 07 00 c3 92 e7 85  04 00 00 00              .K...... ....
00000040  fe 03 00 00                                       ....
00000044  a2 05 00 00 1f 8b 08 00  00 00 00 00 04 00 a5 54  ........ .......T
00000054  db ae ab 36 10 fd 95 bc  54 6a 15 ed 13 6e 21 44  ...6.... Tj...n!D
00000064  ea a9 8e c1 26 5c 02 01  13 20 e1 0d 08 e1 7e 4b  ....&\.. . ....~K
00000074  48 80 7c 7d 9d bd 55 f5  9c 87 3e 75 24 cf 8c c7  H.|}..U. ..>u$...
00000084  cb cb 9e 65 c9 52 db 34  49 3c e4 4d fa e7 8f bf  ...e.R.4 I<.M....
00000094  56 db 62 c5 01 60 3b 65  a0 e1 14 88 c0 46 e0 0c  V.b..`;e .....F..
000000A4  c4 14 00 b8 62 46 11 02  90 ee c4 34 de 89 76 aa  ....bF.. ...4..v.
000000B4  88 63 ac 49 76 aa 43 d1  36 21 b8 ef a1 58 3a 68  .c.Iv.C. 6!...X:h
000000C4  14 5c 05 b7 57 25 a3 42  02 48 35 89 6b 54 49 bd  .\..W%.B .H5.kTI.
000000D4  ab d3 18 eb 30 ee f6 10  4c 26 b4 29 65 8e d7 d6  ....0... L&.)e...
000000E4  31 9d 2d 89 7b 99 70 ff  c5 6d 97 84 6f 24 3c a9  1.-.{.p. .m..o$<.
000000F4  09 71 3a ab 78 cc 8c 42  9d ff df d8 af 46 00 b0  .q:.x..B .....F..
00000104  04 c0 0c a0 0a 81 a3 02  90 21 11 4c 48 5c 09 36  ........ .!.LH\.6
00000114  50 c8 22 b0 dd 77 9f 9f  bd fe 6b 48 02 a3 2d 93  P."..w.. ..kH..-.
00000124  5e 55 c9 6e f7 6f ec 80  49 39 45 10 8c 2a 02 a3  ^U.n.o.. I9E..*..
00000134  2b 93 0d a4 20 6f 81 4d  78 81 8d 45 ac 66 86 8b  +... o.M x..E.f..
00000144  76 88 96 33 71 d6 26 19  ea 62 19 22 55 a5 f4 69  v..3q.&. .b."U..i
00000154  c4 9e 43 5d 41 69 30 da  9c a6 a5 2e 67 f1 79 87  ..C]Ai0. ....g.y.
00000164  db 4a cb e3 56 77 5a ca  3c 9e d9 03 2c 79 9b c2  .J..VwZ. <...,y..
00000174  32 2e 2f aa e3 76 47 4f  f6 7c 8f ce 02 bf 36 cb  2./..vGO .|....6.
00000184  c0 0f 9a 70 57 f5 31 8b  e9 4b 73 e1 92 53 0f 33  ...pW.1. .Ks..S.3
00000194  d5 df 65 5c ae e5 9d 7e  ac 34 df af d6 79 50 f7  ..e\...~ .4...yP.
000001A4  7a d1 e9 7e dd f1 79 d7  df f4 d7 b0 f7 99 61 93  z..~..y. ......a.
000001B4  af 1f e4 79 26 e3 b4 9b  84 42 9b 87 fd 91 36 4f  ...y&... .B....6O
000001C4  3e bd 2d 02 e6 a1 e4 dc  f2 58 ad 1f d7 96 4f 6e  >.-..... .X....On
000001D4  93 f0 b4 a8 ed 35 62 97  56 c3 7f e9 43 34 19 d1  .....5b. V...C4..
000001E4  3f fa 7c b5 fc 9f fa a0  b7 3e 12 01 41 11 c4 5f  ?.|..... .>..A.._
000001F4  fa d8 1a fb 89 9d 10 12  1d 34 89 99 26 ba f6 25  ........ .4..&..%
00000204  8b b1 91 1b 2d 52 65 a4  e3 36 52 44 c9 31 5e ee  ....-Re. .6RD.1^.
00000214  13 78 e7 66 8f a5 ec 5c  9a 07 54 09 f8 53 a3 9a  .x.f...\ ..T..S..
00000224  28 d6 e9 85 cb 98 af 74  7d 28 4d 84 dd 40 71 50  (......t }(M..@qP
00000234  a5 bb 34 f6 bc ea 72 f6  bd ae 08 76 5e 1d 30 59  ..4...r. ...v^.0Y
00000244  17 36 26 75 39 05 6c a2  54 7c da 1e 50 76 0e 95  .6&u9.l. T|..Pv..
00000254  5c ad f5 b2 3b b8 55 10  9e 6a ad 0e db fe 50 76  \...;.U. .j....Pv
```

ZgRAT

декодирование, детектирование, обнаружение



From Hex

Delimiter
Auto

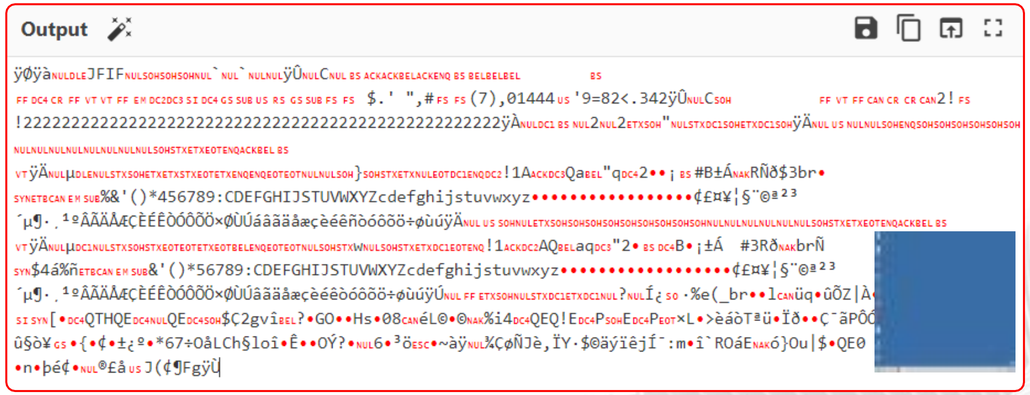
Gunzip

Input

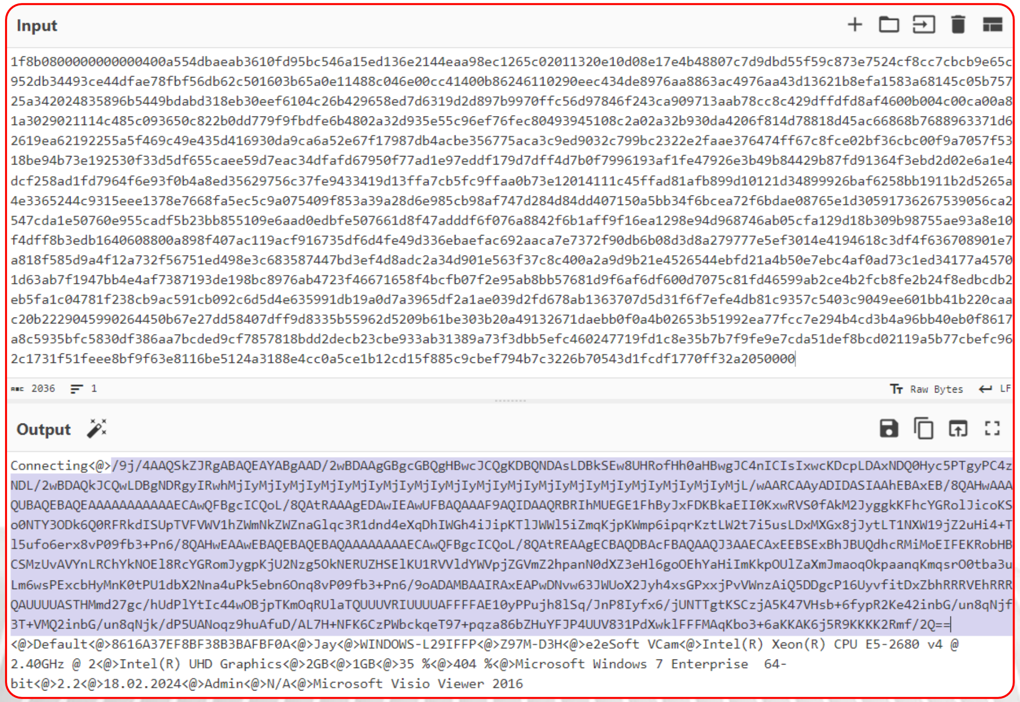
```
1f8b08000000000000004000bc8cc4b0700c392e78504000000
```

Output

```
Ping
```


Output

```
ÿØÿàNULDLEJFIFNULSOHSOHSOHNUL`NUL`NULNULÿÛNULCNULBSACKACKBELACKENQBSBELBELBEL     BS
FFDC4CRFFVTVTFFEMDC2DC3SIDC4GSSUBUSRSGSSUBFSFS $.' ",#FSFS(7),01444US'9=82<.342ÿÛNULCSOH      FFVTFFCANCRCRCAN2!FS
!22222222222222222222222222222222222222222222222222ÿÀNULDC1BSNUL2NUL2ETXSOH"NULSTXDC1SOHETXDC1SOHÿÄNULUSNULNULSOHENQSOHSOHSOHSOHSOHSOH
NULNULNULNULNULNULNULNULSOHSTXETXEOTENQACKBELBS
VTÿÄNULµDLENULSTXSOHETXETXSTXEOTETXENQENQEOTEOTNULNULSOH}SOHSTXETXNULEOTDC1ENQDC2!1AACKDC3QaBEL"qDC42••¡BS#B±ÁNAKRÑð$3br•
SYNETBCANEMSUB%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz•••••••••••••••••¢£¤¥¦§¨©ª²³
´µ¶·¸¹ºÂÃÄÅÆÇÈÉÊÒÓÔÕÖ×ØÙÚâãäåæçèéêñòóôõö÷øùúÿÄNULUSSOHNULETXSOHSOHSOHSOHSOHSOHSOHSOHSOHNULNULNULNULNULNULSOHSTXETXEOTENQACKBELBS
VTÿÄNULµDC1NULSTXSOHSTXEOTEOTETXEOTBELENQEOTEOTNULSOHSTXWNULSOHSTXETXDC1EOTENQ!1ACKDC2AQBELaqDC3"2•BSDC4B•¡±Á #3RðNAKbrÑ
SYN$4á%ñETBCANEMSUB&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz••••••••••••••••••¢£¤¥¦§¨©ª²³
´µ¶·¸¹ºÂÃÄÅÆÇÈÉÊÒÓÔÕÖ×ØÙÚâãäåæçèéêòóôõö÷øùúÿÚNULFFETXSOHNULSTXDC1ETXDC1NUL?NULÍ¿SO·%e(_br••1CANüq•ûÕZ|À
SISYN[•DC4QTHQEDC4NULQEDC4SOH$Ç2gvîBEL?•GO••Hs•08CANéL©•©NAK%i4DC4QEQ!EDC4PSOHEDC4PEOT×L•>èáòTªü•Ïð••Ç¯ãPÔ
û§ò¥GS•{•¢•±¿º•*67÷OåLCh§loî•Ê••OÝ?•NUL6•³öESC•~àÿNUL%ÇøÑJè,ÏY·$©äýïêjÍ¯:m•î`ROáENAKó}Ou|$•QEØ
•n•þé¢•NUL®£åUSJ(¢¶FgÿÙ
```


Input

```
1f8b0800000000000400a554dbaeab3610fd95bc546a15ed136e2144eaa98ec1265c02011320e10d08e17e4b48807c7d9dbd55f59c873e7524cf8cc7cbcb9e65c
952db34493ce44dfae78fbf56db62c501603b65a0e11488c046e00cc41400b86246110290eec434de8976aa8863ac4976aa43d13621b8efa1583a68145c05b757
25a342024835896b5449bdabd318eb30eef6104c26b429658ed7d6319d2d897b9970ffc56d97846f243ca909713aab78cc8c429dffdfd8af4600b004c00ca00a8
1a3029021114c485c093650c822b0dd779f9fbdfe6b4802a32d935e55c96ef76fec80493945108c2a02a32b930da4206f814d78818d45ac66868b768963371d6
2619ea62192255a5f469c49e435d416930da9ca6a52e67f17987db4acbe356775aca3c9ed9032c799bc2322e2faae376474ff67c8fce02bf36cbc00f9a7057f53
18be94b73e192530f33d5df655caee59d7eac34dfafd67950f77ad1e97eddf179d7dff4d7b0f7996193af1fe47926e3b49b84429b87fd91364f3ebd2d02e6a1e4
dcf258ad1fd7964f6e93f0b4a8ed35629756c37fe9433419d13ffa7cb5fc9ffaa0b73e12014111c45ffad81afb899d10121d34899926baf6258bb1911b2d5265a
4e3365244c9315eee1378e7668fa5ec5c9a075409f853a39a28d6e985cb98af747d284d84dd407150a5bb34f6bcea72f6bdae08765e1d30591736267539056ca2
547cda1e50760e955cadf5b23bb855109e6aad0edbfe507661d8f47adddf6f076a8842f6b1aff9f16ea1298e94d968746ab05cfa129d18b309b98755ae93a8e10
f4dff8b3edb1640608800a898f407ac119acf916735df6d4fe49d336ebaefac692aaca7e7372f90db6b08d3d8a279777e5ef3014e4194618c3df4f636708901e7
a818f585d9a4f12a732f56751ed498e3c683587447bd3ef4d8adc2a34d901e563f37c8c400a2a9d9b21e4526544ebfd21a4b50e7ebc4af0ad73c1ed34177a4570
1d63ab7f1947bb4e4af7387193de198bc8976ab4723f46671658f4bcfb07f2e95ab8bb57681d9f6af6df600d7075c81fd46599ab2ce4b2fcb8fe2b24f8edbcdb2
eb5fa1c04781f238cb9ac591cb092c6d5d4e635991db19a0d7a3965df2a1ae039d2fd678ab1363707d5d31f6f7efe4db81c9357c5403c9049ee601bb41b220caa
c20b2229045990264450b67e27dd58407dff9d8335b55962d5209b61be303b20a49132671daebb0f0a4b02653b51992ea77fcc7e294b4cd3b4a96bb40eb0f8617
a8c5935bfc5830df386aa7bcded9cf7857818bdd2decb23cbe933ab31389a73f3dbb5efc460247719fd1c8e35b7b7f9fe9e7cda51def8bcd02119a5b77cbefc96
2c1731f51feee8bf9f63e8116be5124a3188e4cc0a5ce1b12cd15f885c9cbef794b7c3226b70543d1fcdf1770ff32a2050000
```

Output

```
Connecting<@>/9j/4AAQSkZJRgABAQEAYABgAAD/2wBDAAgGBgcGBQgHBwcJCQgKDBQNDAsLDBkSEw8UHRofHh0aHBwgJC4nICIsIxwcKDcpLDAxNDQ0Hyc5PTgyPC4z
NDL/2wBDAQkJCQwLDBgNDRgyIRwhMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjIyMjL/wAARCAAyADIDASIAAhEBAxEB/8QAHwAAA
QUBAQEBAQEAAAAAAAAAAAECAwQFBgcICQoL/8QAtRAAAgEDAwIEAwUFBAQAAAF9AQIDAAQRBRIhMUEGE1FhByJxFDKBkaEII0KxwRVS0fAkM2JyggkKFhcYGRolJicoKS
o0NTY3ODk6Q0RFRkdISUpTVFVWV1hZWmNkZWZnaGlqc3R1dnd4eXqDhIWGh4iJipKTlJWWl5iZmqKjpKWmp6ipqrKztLW2t7i5usLDxMXGx8jJytLT1NXW19jZ2uHi4+T
l5ufo6erx8vP09fb3+Pn6/8QAHwEAAwEBAQEBAQEBAQAAAAAAAAECAwQFBgcICQoL/8QAtREAAgECBAQDBAcFBAQAAQJ3AAECAxEEBSExBhJBUQdhcRMiMoEIFEKRobHB
CSMzUvAVYnLRChYkNOEl8RcYGRomJygpKjU2Nzg5OkNERUZHSElKU1RVVldYWVpjZGVmZ2hpanN0dXZ3eHl6goOEhYaHiImKkpOUlZaXmJmaoqOkpaanqKmqsrO0tba3u
Lm6wsPExcbHyMnK0tPU1dbX2Nna4uPk5ebn6Onq8vP09fb3+Pn6/9oADAMBAAIRAxEAPwDNvw63JWUoX2Jyh4xsGPxxjPvVWnzAiQ5DDgcP16UyvfitDxZbhRRRVEhRRR
QAUUUUASTHMmd27gc/hUdPlYtIc44wOBjpTKmOqRUlaTQUUUVRIUUUUAFFFFAE10yPPujh8lSq/JnP8Iyfx6/jUNTTgtKSCzjA5K47VHsb+6fypR2Ke42inbG/un8qNjf
3T+VMQ2inbG/un8qNjk/dP5UANoqz9huAfuD/AL7H+NFK6CzPWbckqeT97+pqza86bZHuYFJP4UUV831PdXkwlFFFMAqKbo3+6aKKo2Rmf/2Q==
<@>Default<@>8616A37EF8BF38B3BAFBF0A<@>Jay<@>WINDOWS-L29IFFP<@>Z97M-D3H<@>e2eSoft VCam<@>Intel(R) Xeon(R) CPU E5-2680 v4 @
2.40GHz @ 2<@>Intel(R) UHD Graphics<@>2GB<@>1GB<@>35 %<@>404 %<@>Microsoft Windows 7 Enterprise  64-
bit<@>2.2<@>18.02.2024<@>Admin<@>N/A<@>Microsoft Visio Viewer 2016
```

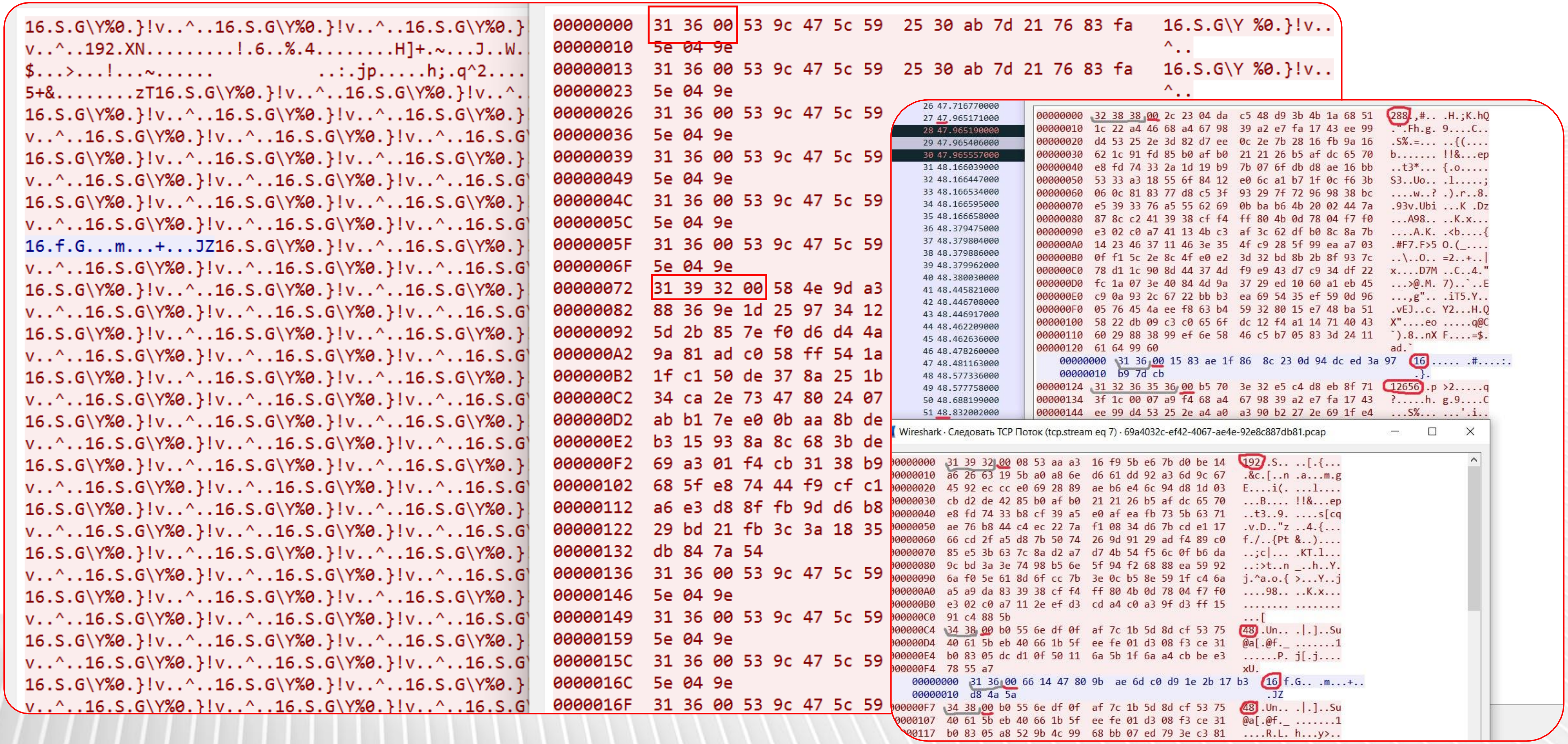
```
Правило 1.
msg: "REMOTE [PTsecurity] zgRAT first packet";
dsize: 4;
stream_size: client, =, 5;
stream_size: server, =, 1;
content: "|00 00|"; offset: 2; depth: 2;
byte_test: 1,<=,0x04,1;
flowbits: set, zgrat_fist_pkt;
flowbits: noalert;

Правило 2.
msg: "REMOTE [PTsecurity] zgRAT second packet";
stream_size: client, >, 19;
stream_size: server, >=, 1;
content: "|00 00 1f 8b 08 00 00 00 00 00 04 00|"; offset: 2; depth: 12;
flowbits: isset, zgrat_fist_pkt;
```

02

Современные подходы злоумышленников к сокрытию сетевого взаимодействия вредоносного программного обеспечения

Шифрование: AES, RC4

Xworm RAT



```
16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..16.S.G\Y%0.}
v..^..192.XN.........!.6..%.4........H]+.~...J..W.
$...>...!...~......              ..:.jp.....h;.q^2....
5+&........zT16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..
16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..16.S.G\Y%0.}
v..^..16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..16.S.G
16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..16.S.G\Y%0.}
v..^..16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..16.S.G
16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..16.S.G\Y%0.}
v..^..16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..16.S.G
16.f.G...m...+...JZ16.S.G\Y%0.}!v..^..16.S.G\Y%0.}
v..^..16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..16.S.G
16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..16.S.G\Y%0.}
v..^..16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..16.S.G
16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..16.S.G\Y%0.}
v..^..16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..16.S.G
16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..16.S.G\Y%0.}
v..^..16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..16.S.G
16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..16.S.G\Y%0.}
v..^..16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..16.S.G
16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..16.S.G\Y%0.}
v..^..16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..16.S.G
16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..16.S.G\Y%0.}
v..^..16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..16.S.G
16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..16.S.G\Y%0.}
v..^..16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..16.S.G
16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..16.S.G\Y%0.}
v..^..16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..16.S.G
16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..16.S.G\Y%0.}
v..^..16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..16.S.G
16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..16.S.G\Y%0.}
v..^..16.S.G\Y%0.}!v..^..16.S.G\Y%0.}!v..^..16.S.G
```

```
00000000  31 36 00 53 9c 47 5c 59  25 30 ab 7d 21 76 83 fa   16.S.G\Y %0.}!v..
00000010  5e 04 9e                                           ^..
00000013  31 36 00 53 9c 47 5c 59  25 30 ab 7d 21 76 83 fa   16.S.G\Y %0.}!v..
00000023  5e 04 9e                                           ^..
00000026  31 36 00 53 9c 47 5c 59
00000036  5e 04 9e
00000039  31 36 00 53 9c 47 5c 59
00000049  5e 04 9e
0000004C  31 36 00 53 9c 47 5c 59
0000005C  5e 04 9e
0000005F  31 36 00 53 9c 47 5c 59
0000006F  5e 04 9e
00000072  31 39 32 00 58 4e 9d a3
00000082  88 36 9e 1d 25 97 34 12
00000092  5d 2b 85 7e f0 d6 d4 4a
000000A2  9a 81 ad c0 58 ff 54 1a
000000B2  1f c1 50 de 37 8a 25 1b
000000C2  34 ca 2e 73 47 80 24 07
000000D2  ab b1 7e e0 0b aa 8b de
000000E2  b3 15 93 8a 8c 68 3b de
000000F2  69 a3 01 f4 cb 31 38 b9
00000102  68 5f e8 74 44 f9 cf c1
00000112  a6 e3 d8 8f fb 9d d6 b8
00000122  29 bd 21 fb 3c 3a 18 35
00000132  db 84 7a 54
00000136  31 36 00 53 9c 47 5c 59
00000146  5e 04 9e
00000149  31 36 00 53 9c 47 5c 59
00000159  5e 04 9e
0000015C  31 36 00 53 9c 47 5c 59
0000016C  5e 04 9e
0000016F  31 36 00 53 9c 47 5c 59
```

```
26 47.716770000
27 47.965171000
28 47.965190000
29 47.965406000
30 47.965557000
31 48.166039000
32 48.166447000
33 48.166534000
34 48.166595000
35 48.166658000
36 48.379475000
37 48.379804000
38 48.379886000
39 48.379962000
40 48.380030000
41 48.445821000
42 48.446708000
43 48.446917000
44 48.462209000
45 48.462636000
46 48.478260000
47 48.481163000
48 48.577336000
49 48.577758000
50 48.688199000
51 48.832002000
```

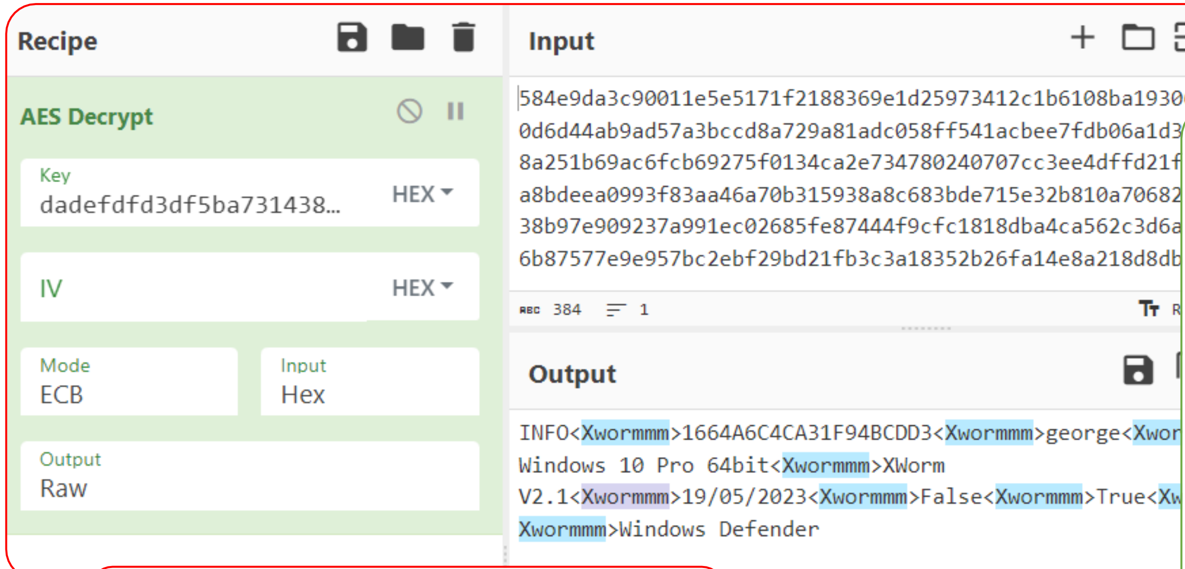
```
00000000  32 38 38 00 2c 23 04 da  c5 48 d9 3b 4b 1a 68 51   288.,#.. .H.;K.hQ
00000010  1c 22 a4 46 68 a4 67 98  39 a2 e7 fa 17 43 ee 99   .".Fh.g. 9....C..
00000020  d4 53 25 2e 3d 82 d7 ee  0c 2e 7b 28 16 fb 9a 16   .S%.=... ..{(....
00000030  62 1c 91 fd 85 b0 af b0  21 21 26 b5 af dc 65 70   b....... !!&...ep
00000040  e8 fd 74 33 2a 1d 19 b9  7b 07 6f db d8 ae 16 bb   ..t3*... {.o.....
00000050  53 33 a3 18 55 6f 84 12  e0 6c a1 b7 1f 0c f6 3b   S3..Uo.. .l.....;
00000060  06 0c 81 83 77 d8 c5 3f  93 29 7f 72 96 98 38 bc   ....w..? .).r..8.
00000070  e5 39 33 76 a5 55 62 69  0b ba b6 4b 20 02 44 7a   .93v.Ubi ...K .Dz
00000080  87 8c c2 41 39 38 cf f4  ff 80 4b 0d 78 04 f7 f0   ...A98.. ..K.x...
00000090  e3 02 c0 a7 41 13 4b c3  af 3c 62 df b0 8c 8a 7b   ....A.K. .<b....{
000000A0  14 23 46 37 11 46 3e 35  4f c9 28 5f 99 ea a7 03   .#F7.F>5 O.(_....
000000B0  0f f1 5c 2e 8c 4f e0 e2  3d 32 bd 8b 2b 8f 93 7c   ..\..O.. =2..+..|
000000C0  78 d1 1c 90 8d 44 37 4d  f9 e9 43 d7 c9 34 df 22   x....D7M ..C..4."
000000D0  fc 1a 07 3e 40 84 4d 9a  37 29 ed 10 60 a1 eb 45   ...>@.M. 7)..`..E
000000E0  c9 0a 93 2c 67 22 bb b3  ea 69 54 35 ef 59 0d 96   ...,g".. .iT5.Y..
000000F0  05 76 45 4a ee f8 63 b4  59 32 80 15 e7 48 ba 51   .vEJ..c. Y2...H.Q
00000100  58 22 db 09 c3 c0 65 6f  dc 12 f4 a1 14 71 40 43   X"....eo .....q@C
00000110  60 29 88 38 99 ef 6e 58  46 c5 b7 05 83 3d 24 11   `).8..nX F....=$.
00000120  61 64 99 60                                        ad.`
    00000000  31 36 00 15 83 ae 1f 86  8c 23 0d 94 dc ed 3a 97   16..... .#....:.
    00000010  b9 7d cb                                           .}.
00000124  31 32 36 35 36 00 b5 70  3e 32 e5 c4 d8 eb 8f 71   12656.p >2.....q
00000134  3f 1c 00 07 a9 f4 68 a4  67 98 39 a2 e7 fa 17 43   ?.....h. g.9....C
00000144  ee 99 d4 53 25 2e a4 a0  a3 90 b2 27 2e 69 1f e4   ...S%... ...'.i..
```

Wireshark · Следовать TCP Поток (tcp.stream eq 7) · 69a4032c-ef42-4067-ae4e-92e8c887db81.pcap

```
00000000  31 39 32 00 08 53 aa a3  16 f9 5b e6 7b d0 be 14   192.S.. ..[.{...
00000010  a6 26 63 19 5b a0 a8 6e  d6 61 dd 92 a3 6d 9c 67   .&c.[..n .a...m.g
00000020  45 92 ec cc e0 69 28 89  ae b6 e4 6c 94 d8 1d 03   E....i(. ...l....
00000030  cb d2 de 42 85 b0 af b0  21 21 26 b5 af dc 65 70   ...B.... !!&...ep
00000040  e8 fd 74 33 b8 cf 39 a5  e0 af ea fb 73 5b 63 71   ..t3..9. ....s[cq
00000050  ae 76 b8 44 c4 ec 22 7a  f1 08 34 d6 7b cd e1 17   .v.D.."z ..4.{...
00000060  66 cd 2f a5 d8 7b 50 74  26 9d 91 29 ad f4 89 c0   f./..{Pt &..)....
00000070  85 e5 3b 63 7c 8a d2 a7  d7 4b 54 f5 6c 0f b6 da   ..;c|... .KT.l...
00000080  9c bd 3a 3e 74 98 b5 6e  5f 94 f2 68 88 ea 59 92   ..:>t..n _..h..Y.
00000090  6a f0 5e 61 8d 6f cc 7b  3e 0c b5 8e 59 1f c4 6a   j.^a.o.{ >...Y..j
000000A0  a5 a9 da 83 39 38 cf f4  ff 80 4b 0d 78 04 f7 f0   ....98.. ..K.x...
000000B0  e3 02 c0 a7 11 2e ef d3  cd a4 c0 a3 9f d3 ff 15   ........ ........
000000C0  91 c4 88 5b                                        ...[
000000C4  34 38 00 b0 55 6e df 0f  af 7c 1b 5d 8d cf 53 75   48.Un.. .|.]..Su
000000D4  40 61 5b eb 40 66 1b 5f  ee fe 01 d3 08 f3 ce 31   @a[.@f._ .......1
000000E4  b0 83 05 dc d1 0f 50 11  6a 5b 1f 6a a4 cb be e3   ......P. j[.j....
000000F4  78 55 a7                                           xU.
    00000000  31 36 00 66 14 47 80 9b  ae 6d c0 d9 1e 2b 17 b3   16 f.G.. .m...+..
    00000010  d8 4a 5a                                           .JZ
000000F7  34 38 00 b0 55 6e df 0f  af 7c 1b 5d 8d cf 53 75   48.Un.. .|.]..Su
00000107  40 61 5b eb 40 66 1b 5f  ee fe 01 d3 08 f3 ce 31   @a[.@f._ .......1
00000117  b0 83 05 a8 52 9b 4c 99  68 bb 07 ed 79 3e c3 81   ....R.L. h...y>..
```

Xworm RAT

декодирование, детектирование, обнаружение



AES Decrypt

Key: dadefdfd3df5ba731438... HEX

IV: HEX

Mode: ECB

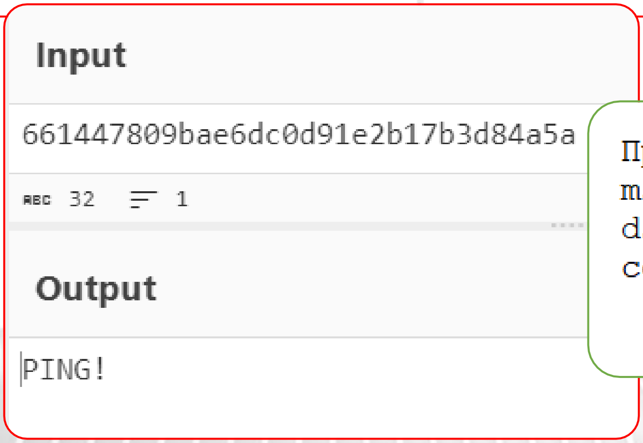
Input: Hex

Output: Raw

```
584e9da3c90011e5e5171f2188369e1d25973412c1b6108ba19306485d2b857ef
0d6d44ab9ad57a3bccd8a729a81adc058ff541acbee7fdb06a1d3
8a251b69ac6fcb69275f0134ca2e734780240707cc3ee4dffd21f
a8bdeea0993f83aa46a70b315938a8c683bde715e32b810a70682
38b97e909237a991ec02685fe87444f9cfc1818dba4ca562c3d6a
6b87577e9e957bc2ebf29bd21fb3c3a18352b26fa14e8a218d8db
```

ABC 384 ☰ 1

```
INFO<Xwormmm>1664A6C4CA31F94BCDD3<Xwormmm>george<Xwor
Windows 10 Pro 64bit<Xwormmm>XWorm
V2.1<Xwormmm>19/05/2023<Xwormmm>False<Xwormmm>True<Xw
Xwormmm>Windows Defender
```



```
661447809bae6dc0d91e2b17b3d84a5a
```

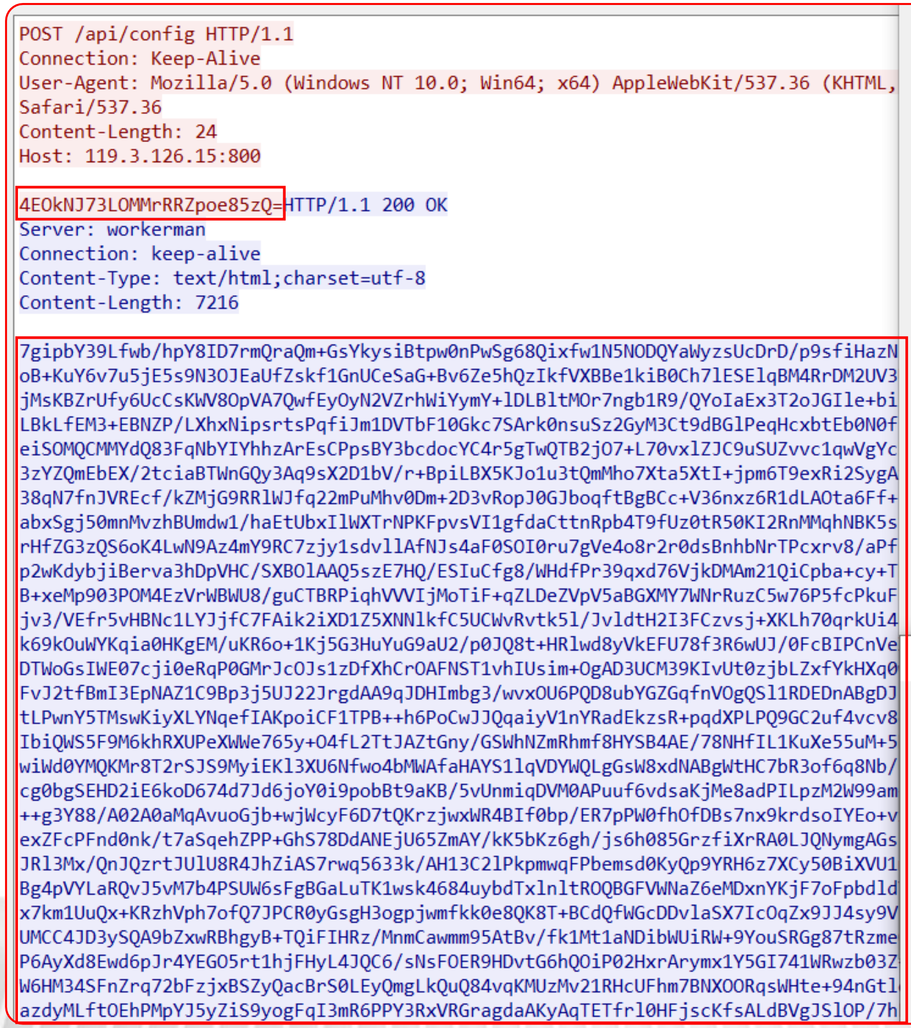
ABC 32 ☰ 1

```
PING!
```

```
Правило 1.
msg: "REMOTE [PTsecurity] Possible XWorm";
content: "|00|"; depth: 8;
pcre: "/^[0-9]{1,6}[0,2,4,6,8]\x00/";
flowbits: set, xworm_pkt;
threshold: type limit, track by_src, seconds 10, count 5;

Правило 2.
msg: "REMOTE [PTsecurity] XWorm";
flow: established, to_client;
content: "|00|"; depth: 8;
pcre: "/^[0-9]{1,6}[0,2,4,6,8]\x00/";
flowbits: isset, xworm_pkt;
flowbits: unset, xworm_pkt;
```

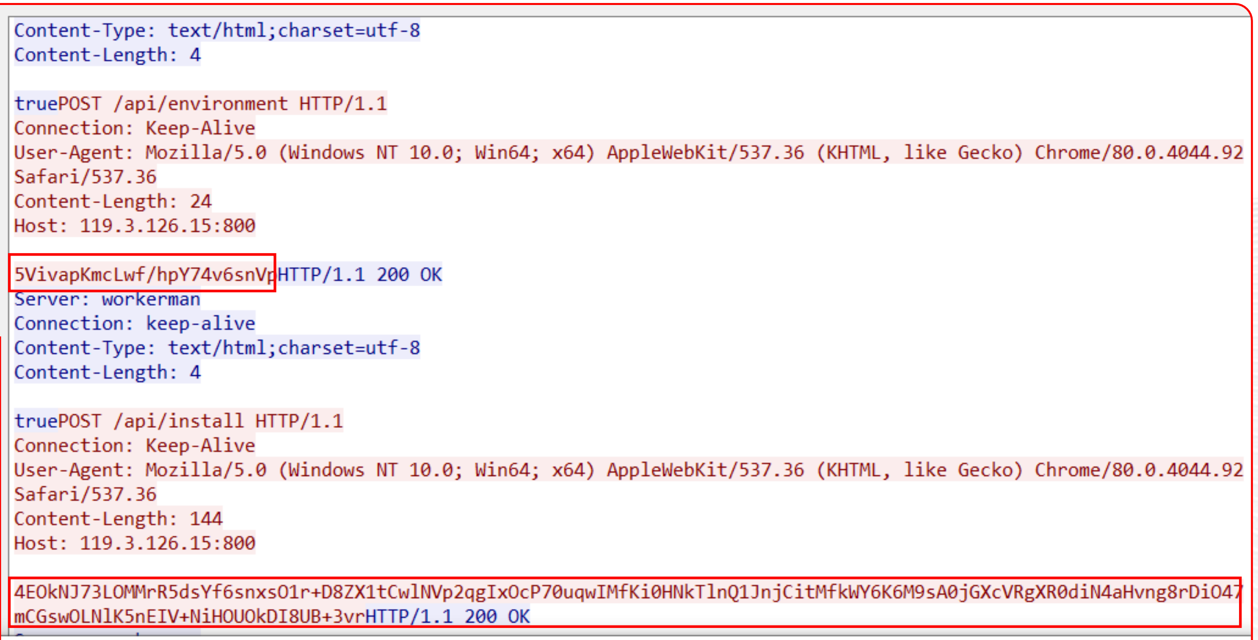
```
Правило 3.
msg: "REMOTE [PTsecurity] Xworm Ping";
dsize: 19;
content: "16|00 53 9c 47 5c 59 25 30 ab 7d 21 76 83 fa 5e 04 9e|"; depth: 19;
```

PlugX backdoor

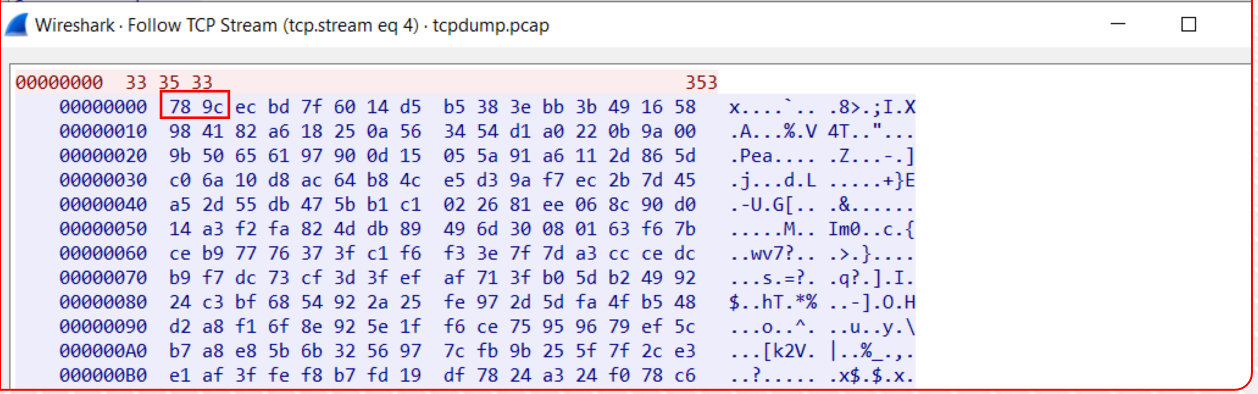


```
POST /api/config HTTP/1.1
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
Safari/537.36
Content-Length: 24
Host: 119.3.126.15:800

4EOkNJ73LOMMrRRZpoe85zQ=HTTP/1.1 200 OK
Server: workerman
Connection: keep-alive
Content-Type: text/html;charset=utf-8
Content-Length: 7216
```

```
7gipbY39Lfwb/hpY8ID7rmQraQm+GsYkysiBtpw0nPwSg68Qixfw1N5NODQYaWyzsUcDrD/p9sfiHazN
oB+KuY6v7u5jE5s9N3OJEaUfZskf1GnUCeSaG+Bv6Ze5hQzIkfVXBBe1kiB0Ch7lESElqBM4RrDM2UV3
jMsKBZrUfy6UcCsKWV8OpVA7QwfEyOyN2VZrhWiYymY+lDLBltMOr7ngb1R9/QYoIaEx3T2oJGIle+bi
LBkLfEM3+EBNZP/LXhxNipsrtsPqfiJm1DVTbF10Gkc7SArk0nsuSz2GyM3Ct9dBGlPeqHcxbtEb0N0f
eiSOMQCMMYdQ83FqNbYIYhhzArEsCPpsBY3bcdocYC4r5gTwQTB2jO7+L70vxlZJC9uSUZvvc1qwVgYc
3zYZQmEbEX/2tciaBTWnGQy3Aq9sX2D1bV/r+BpiLBX5KJo1u3tQmMho7Xta5XtI+jpm6T9exRi2SygA
38qN7fnJVREcf/kZMjG9RRlWJfq22mPuMhv0Dm+2D3vRopJ0GJboqftBgBCc+V36nxz6R1dLAOta6Ff+
abxSgj50mnMvzhBUmdw1/haEtUbxIlWXTrNPKFpvsVI1gfdaCttnRpb4T9fUz0tR50KI2RnMMqhNBK5s
rHfZG3zQS6oK4LwN9Az4mY9RC7zjy1sdvllAfNJs4aF0SOI0ru7gVe4o8r2r0dsBnhbNrTPcxrv8/aPf
p2wKdybjiBerva3hDpVHC/SXBOlAAQ5szE7HQ/ESIuCfg8/WHdfPr39qxd76VjkDMAm21QiCpba+cy+T
B+xeMp903POM4EzVrWBWU8/guCTBRPiqhVVIjMoTiF+qZLDeZVpV5aBGXMY7WNrRuzC5w76P5fcPkuF
jv3/VEfr5vHBNc1LYJjfC7FAik2iXD1Z5XNNlkfC5UCWvRvtk5l/JvldtH2I3FCzvsj+XKLh70qrkUi4
k69kOuWYKqia0HKgEM/uKR6o+1Kj5G3HuYuG9aU2/p0JQ8t+HRlwd8yVkEFU78f3R6wUJ/0FcBIPCnVe
DTWoGsIWE07cji0eRqP0GMrJcOJs1zDfXhCrOAFNST1vhIUsim+OgAD3UCM39KIvUt0zjbLZxfYkHXq0
FvJ2tfBmI3EpNAZ1C9Bp3j5UJ22JrgdAA9qJDHImbg3/wvxOU6PQD8ubYGZGqfnVOgQSl1RDEDnABgDJ
tLPwnY5TMswKiyXLYNqefIAKpoiCF1TPB++h6PoCwJJQqaiyV1nYRadEkzsR+pqdXPLPQ9GC2uf4vcv8
IbiQWS5F9M6khRXUPeXWWe765y+O4fL2TtJAZtGny/GSWhNZmRhmf8HYSB4AE/78NHfIL1KuXe55uM+5
wiWd0YMQKMr8T2rSJS9MyiEKl3XU6Nfwo4bMWAfaHAYS1lqVDYWQLgGsW8xdNABgWtHC7bR3of6q8Nb/
cg0bgSEHD2iE6koD674d7Jd6joY0i9pobBt9aKB/5vUnmiqDVM0APuuf6vdsaKjMe8adPILpzM2W99am
++g3Y88/A02A0aMqAvuoGjb+wjWcyF6D7tQKrzjwxWR4BIf0bp/ER7pPW0fhOfDBs7nx9krdsoIYEo+v
exZFcPFnd0nk/t7aSqehZPP+GhS78DdANEjU65ZmAY/kK5bKz6gh/js6h085GrzfiXrRA0LJQNymgAGs
JRl3Mx/QnJQzrtJUlU8R4JhZiAS7rwq5633k/AH13C2lPkpmwqFPbemsd0KyQp9YRH6z7XCy50BiXVU1
Bg4pVYLaRQvJ5vM7b4PSUW6sFgBGaLuTK1wsk4684uybdTxlnltROQBGFVWNaZ6eMDxnYKjF7oFpbdld
x7km1UuQx+KRzhVph7ofQ7JPCR0yGsgH3ogpjwmfkk0e8QK8T+BCdQfWGcDDvlaSX7IcOqZx9JJ4sy9V
UMCC4JD3ySQA9bZxwRBhgyB+TQiFIHRz/MnmCawmm95AtBv/fk1Mt1aNDibWUiRW+9YouSRGg87tRzme
P6AyXd8Ewd6pJr4YEGO5rt1hjFHyL4JQC6/sNsFOER9HDvtG6hQOiP02HxrArymx1Y5GI741WRwzb03Z
W6HM34SFnZrq72bFzjxBSZyQacBrS0LEyQmgLkQuQ84vqKMUzMv21RHcUFhm7BNXOORqsWHte+94nGtl
azdyMLftOEhPMpYJ5yZiS9yogFqI3mR6PPY3RxVRGragdaAKyAqTETfrl0HFjscKfsALdBVgJSlOP/7h
```



```
Content-Type: text/html;charset=utf-8
Content-Length: 4

truePOST /api/environment HTTP/1.1
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.4044.92
Safari/537.36
Content-Length: 24
Host: 119.3.126.15:800

5VivapKmcLwf/hpY74v6snVpHTTP/1.1 200 OK
Server: workerman
Connection: keep-alive
Content-Type: text/html;charset=utf-8
Content-Length: 4

truePOST /api/install HTTP/1.1
Connection: Keep-Alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.4044.92
Safari/537.36
Content-Length: 144
Host: 119.3.126.15:800

4EOkNJ73LOMMrR5dsYf6snxsO1r+D8ZX1tCwlNVp2qgIxOcP70uqwIMfKi0HNkTlnQ1JnjCitMfkWY6K6M9sA0jGXcVRgXR0diN4aHvng8rDiO47
mCGswOLNlK5nEIV+NiHOUOkDI8UB+3vrHTTP/1.1 200 OK
```

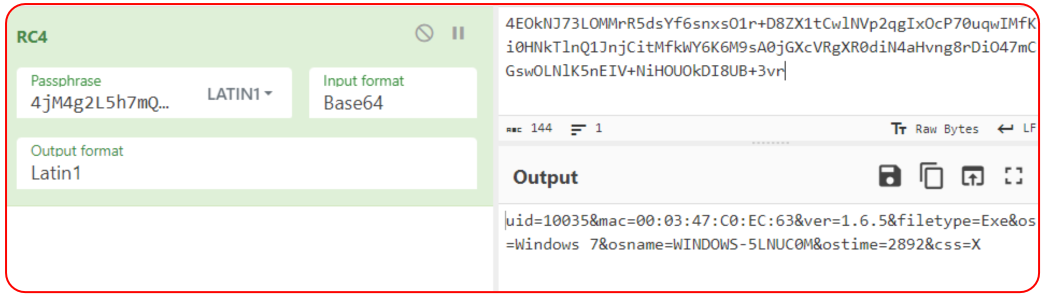


Wireshark · Follow TCP Stream (tcp.stream eq 4) · tcpdump.pcap

```
00000000  33 35 33                                           353
    00000000  78 9c ec bd 7f 60 14 d5  b5 38 3e bb 3b 49 16 58   x....`.. .8>.;I.X
    00000010  98 41 82 a6 18 25 0a 56  34 54 d1 a0 22 0b 9a 00   .A...%.V 4T.."...
    00000020  9b 50 65 61 97 90 0d 15  05 5a 91 a6 11 2d 86 5d   .Pea.... .Z...-.]
    00000030  c0 6a 10 d8 ac 64 b8 4c  e5 d3 9a f7 ec 2b 7d 45   .j...d.L .....+}E
    00000040  a5 2d 55 db 47 5b b1 c1  02 26 81 ee 06 8c 90 d0   .-U.G[.. .&......
    00000050  14 a3 f2 fa 82 4d db 89  49 6d 30 08 01 63 f6 7b   .....M.. Im0..c.{
    00000060  ce b9 77 76 37 3f c1 f6  f3 3e 7f 7d a3 cc ce dc   ..wv7?.. .>.}....
    00000070  b9 f7 dc 73 cf 3d 3f ef  af 71 3f b0 5d b2 49 92   ...s.=?. .q?.].I.
    00000080  24 c3 bf 68 54 92 2a 25  fe 97 2d 5d fa 4f b5 48   $..hT.*% ..-].O.H
    00000090  d2 a8 f1 6f 8e 92 5e 1f  f6 ce 75 95 96 79 ef 5c   ...o..^. ..u..y.\
    000000A0  b7 a8 e8 5b 6b 32 56 97  7c fb 9b 25 5f 7f 2c e3   ...[k2V. |..%_.,.
    000000B0  e1 af 3f fe f8 b7 fd 19  df 78 24 a3 24 f0 78 c6   ..?..... .x$.$.x.
```

PlugX backdoor

декодирование, детектирование, обнаружение

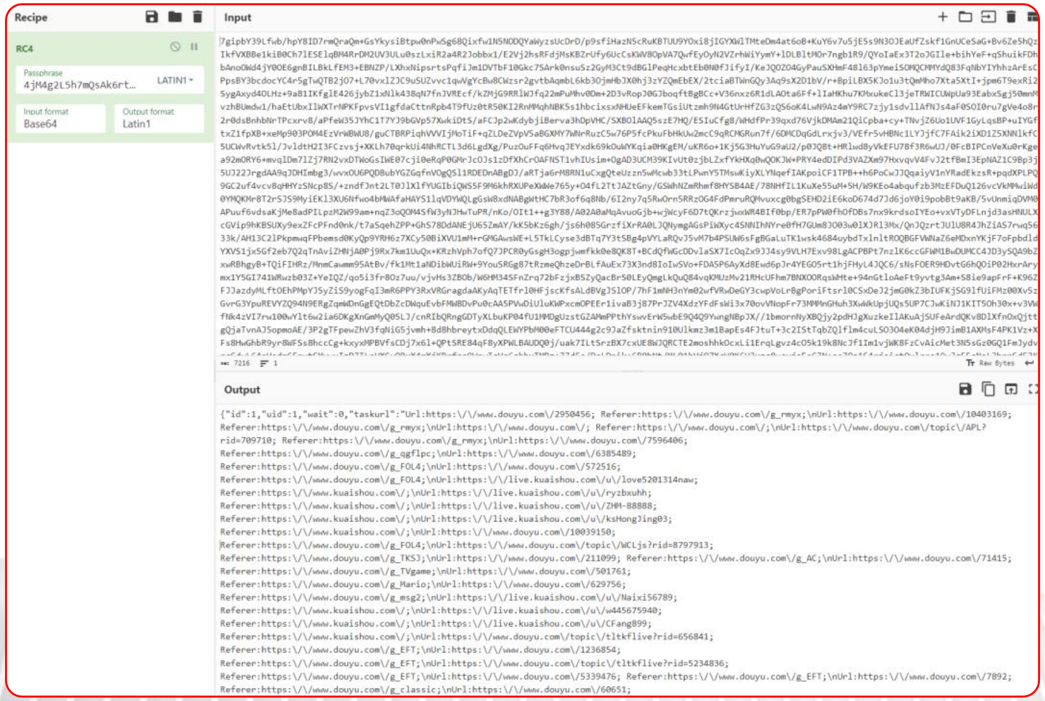


Passphrase: 4jM4g2L5h7mQ… LATIN1
Input format: Base64
Output format: Latin1

```
4EOkNJ73LOMMrR5dsYf6snxsO1r+D8ZX1tCwlNVp2qgIxOcP70uqwIMfK
i0HNkTlnQ1JnjCitMfkWY6K6M9sA0jGXcVRgXR0diN4aHvng8rDiO47mC
GswOLNlK5nEIV+NiHOUOkDI8UB+3vr
```

144 1

```
uid=10035&mac=00:03:47:C0:EC:63&ver=1.6.5&filetype=Exe&os
=Windows 7&osname=WINDOWS-5LNUC0M&ostime=2892&css=X
```



Passphrase: 4jM4g2L5h7mQsAk6rt… LATIN1
Input format: Base64
Output format: Latin1

```
7gipbY39Lfwb/hpY8ID7rmQraQm+GsYkysiBtpw0nPwSg68Qixfw1N5NODQYaWyzsUcDrD/p9sfiHazN5cRuKBTUU9YOxi8jIGYXWlTMteDm4at6oB+KuY6v7u5jE5s9N3OJEaUfZskf1GnUCeSaG+Bv6Ze5hQz
IkfVXBBe1kiB0Ch7lESElqBM4RrDM2UV3ULu0szLxiR2a4R2Jobbx1/E2Vj2hsRFdjMsKBZrUfy6UcCsKWV8OpVA7QwfEyOyN2VZrhWiYymY+lDLBltMOr7ngb1R9/QYoIaEx3T2oJGIle+bihYeF+qShuikFDh
bAnoOWd4jY0OE6gnBILBkLfEM3+EBNZP/LXhxNipsrtsPqfiJm1DVTbF10Gkc7SArk0nsuSz2GyM3Ct9dBGlPeqHcxbtEb0N0fJifyI/KeJQOZO4GyPauSXHmF48l63pYmeiSOMQCMMYdQ83FqNbYIYhhzArEsC
PpsBY3bcdocYC4r5gTwQTB2jO7+L70vxlZJC9uSUZvvc1qwVgYcBw8CWzsr2gvtbAqmbL6kb3OjmHbJX0hj3zYZQmEbEX/2tciaBTWnGQy3Aq9sX2D1bV/r+BpiLBX5KJo1u3tQmMho7Xta5XtI+jpm6T9exRi2
SygAxyd4OLHz+9a81IKfglE426jybZ1xNlk438qN7fnJVREcf/kZMjG9RRlWJfq22mPuMhv0Dm+2D3vRopJ0GJboqftBgBCc+V36nxz6R1dLAOta6Ff+lIaHKhu7KMxukeCl3jeTRWICUWpUa93EabxSgj50mnM
vzhBUmdw1/haEtUbxIlWXTrNPKFpvsVI1gfdaCttnRpb4T9fUz0tR50KI2RnMMqhNBK5s1hbcixsxNHUeEFkemTGsiUtzmh9N4GtUrHfZG3zQS6oK4LwN9Az4mY9RC7zjy1sdvllAfNJs4aF0SOI0ru7gVe4o8r
2r0dsBnhbNrTPcxrv8/aPfeW35JYhC1T7YJ9bGVp57XwkiDtS/aFCJp2wKdybjiBerva3hDpVHC/SXBOlAAQ5szE7HQ/ESIuCfg8/WHdfPr39qxd76VjkDMAm21QiCpba+cy+TNvjZ6Uo1UVF1GyLqsBP+uIYGf
txZ1fpXB+xeMp903POM4EzVrWBWU8/guCTBRPiqhVVVIjMoTiF+qZLDeZVpV5aBGXMY7WNrRuzC5w76P5fcPkuFbHkUw2mcC9qRCMGRun7f/6DMCDqGdLrxjv3/VEfr5vHBNc1LYJjfC7FAik2iXD1Z5XNNlkfC
5UCWvRvtk5l/JvldtH2I3FCzvsj+XKLh70qrkUi4NhRCTL3d6LgdXg/PuzOuFFq6HvqJEYxdk69kOuWYKqia0HKgEM/uKR6o+1Kj5G3HuYuG9aU2/p0JQ8t+HRlwd8yVkEFU78f3R6wUJ/0FcBIPCnVeXu0rKge
a92mORY6+mvqlDm7lZj7RN2vxDTWoGsIWE07cji0eRqP0GMrJcOJs1zDfXhCrOAFNST1vhIUsim+OgAD3UCM39KIvUt0zjbLZxfYkHXq0wQOKJW+PRY4edDIPd3VAZXm97HxvqvV4FvJ2tfBmI3EpNAZ1C9Bp3j
5UJ22JrgdAA9qJDHImbg3/wvxOU6PQD8ubYGZGqfnVOgQSl1RDEDnABgDJ/aRTja6rM8RN1uCxgQteUzzn5wMcwb33tLPwnY5TMswKiyXLYNqefIAKpoiCF1TPB++h6PoCwJJQqaiyV1nYRadEkzsR+pqdXPLPQ
9GC2uf4vcv8qHHYzSNcp8S/+zndfJnt2LT0JlXlfYUGIbiQWS5F9M6khRXUPeXWWe765y+O4fL2TtJAZtGny/GSWhNZmRhmf8HYSB4AE/78NHfIL1KuXe55uM+5H/W9KEo4abqufzb3MzEFDuQ126vcVkMMwiWd
0YMQKMr8T2rSJS9MyiEKl3XU6Nfwo4bMWAfaHAYS1lqVDYWQLgGsW8xdNABgWtHC7bR3of6q8Nb/6I2ny7q5RwOrn5RRzOG4FdPmruRQMvuxcg0bgSEHD2iE6koD674d7Jd6joY0i9pobBt9aKB/5vUnmiqDVM0
APuuf6vdsaKjMe8adPILpzM2W99am+nqZ3oQOM4SfW3yNJHwTuPR/nKo/OIt1++g3Y88/A02A0aMqAvuoGjb+wjWcyF6D7tQKrzjwxWR4BIf0bp/ER7pPW0fhOfDBs7nx9krdsoIYEo+vxVTyDFLnjd3asHNULX
cGVip9hKBSUXy9exZFcPFnd0nk/t7aSqehZPP+GhS78DdANEjU65ZmAY/kK5bKz6gh/js6h08SGrzfiXrRA0LJQNymgAGsPiWXyc4SNNIhNYre0fH7GUm8JO03w0lXJRl3Mx/QnJQzrtJUlU8R4JhZiAS7rwq56
33k/AH13C2lPkpmwqFPbemsd0KyQp9YRH6z7XCy50BiXVU1mM+rGMGAwsWE+L5TkLCyse3dBTq7Y3tSBg4pVYLaRQvJ5vM7b4PSUW6sFgBGaLuTK1wsk4684uybdTxlnltROQBGFVWNaZ6eMDxnYKjF7oFpbdld
YXVS1jx5Gf2eb7Q2qTnAviZHNjA0Pj9Rx7km1UuQx+KRzhVph7ofQ7JPCR0yGsgH3ogpjwmfkk0e8QK8T+BCdQfWGcDDvlaSX7IcOqZx9JJ4sy9VLH7Exv98LgACPBPt7nzlK6ccGFWM1BwDUMCC4JD3ySQA9bZ
xwRBhgyB+TQiFIHRz/MnmCawmm95AtBv/fk1Mt1aNDibWUiRW+9YouSRGg87tRzmeQhzeDrBLfAuEx73X3nd8IoIwSVo+FDA5P6AyXd8Ewd6pJr4YEGO5rt1hjFHyL4JQC6/sNsFOER9HDvtG6hQOiP02HxrAry
mx1Y5GI741WRwzb03Z+YeIQZ/qo5i3fr8Oz7uu/vjvHs3ZBOb/W6HM34SFnZrq72bFzjxBSZyQacBr50LEyQmgLkQuQ84vqKMUzMv21RHcUFhm7BNXOORqsWHte+94nGtloAeFt9yvtg3Am+S8ie9apFrF+K96Z
FJJazdyMLftOEhPMpYJ5yZiS9yogFqI3mR6PPY3RxVRGragdaAKyAqTETfrl0HFjscKfsALdBVgJSlOP/7hF1mNH3nYm02wfVRwDeGY3cwpVoLrBgPoriFtsrl0CSxDeJ2jmG0kZ3bIUFKjSG9lfUiFMz00XvSz
GvrG3YpuREVYZQ94N9ERgZqmWDnGgEQtDbZcDWquEvbFMW8DvPu0cAA5PVwDiUluKWPxcmOPEEr1ivaB3j87PrJZV4XdzYFdFsWi3x70ovVNopFr73MMMnGHuh3XwWkUpjUQs5UP7CJwKiNJ1KIT5Oh30x+v3VW
fNk4zVI7rw100wYlt6w2ia6DKgXnGmMyQ05LJ/cnRIbQRngGDTyXLbuKP04fU1MMDgUzstGZAMmPPthYswvErW5wbE9Q4Q9YwngNBpJX//1bmornNyXBQjy2pdHJgXuzkeIlAKuAjSUFeArdQKv8DlXfnOxQjtt
gQjaTvnAJ5opmoAE/3P2gTFpewZhV3fqNiG5jvmh+8d8hbreytxDdqQLEWYPbM00eFTCU444g2c9JaZfsktnin910Ulkmz3m1BapEs4FJtuT+3c2IStTqbZQlflm4cuLSO3O4eK04djH9JimB1AXMsF4PK1Vz+X
Fs8HwGhbR9yr8WFSs8hccCg+kxyxMPBVfsCDj7x6l+QPtSRE84qF8yXPWLBAUDQ0j/uak7ILtSrzBX7cxUE8WJQRCTE2moshhkOcxLi1ErqLgvz4cO5k19k8NcJf1Im1vjWK8FzCvAicMet3N5sGz0GQ1FmJydv
```

7216 1

```
{"id":1,"uid":1,"wait":0,"taskurl":"Url:https:\/\/www.douyu.com\/2950456; Referer:https:\/\/www.douyu.com\/g_rmyx;\nUrl:https:\/\/www.douyu.com\/10403169;
Referer:https:\/\/www.douyu.com\/g_rmyx;\nUrl:https:\/\/www.douyu.com\/; Referer:https:\/\/www.douyu.com\/;\nUrl:https:\/\/www.douyu.com\/topic\/APL?
rid=709710; Referer:https:\/\/www.douyu.com\/g_rmyx;\nUrl:https:\/\/www.douyu.com\/7596406;
Referer:https:\/\/www.douyu.com\/g_qgflpc;\nUrl:https:\/\/www.douyu.com\/6385489;
Referer:https:\/\/www.douyu.com\/g_FOL4;\nUrl:https:\/\/www.douyu.com\/572516;
Referer:https:\/\/www.douyu.com\/g_FOL4;\nUrl:https:\/\/live.kuaishou.com\/u\/love5201314naw;
Referer:https:\/\/www.kuaishou.com\/;\nUrl:https:\/\/live.kuaishou.com\/u\/ryzbxuhh;
Referer:https:\/\/www.kuaishou.com\/;\nUrl:https:\/\/live.kuaishou.com\/u\/ZHM-88888;
Referer:https:\/\/www.kuaishou.com\/;\nUrl:https:\/\/live.kuaishou.com\/u\/ksHongJing03;
Referer:https:\/\/www.kuaishou.com\/;\nUrl:https:\/\/www.douyu.com\/10039150;
Referer:https:\/\/www.douyu.com\/g_FOL4;\nUrl:https:\/\/www.douyu.com\/topic\/WCLjs?rid=8797913;
Referer:https:\/\/www.douyu.com\/g_TKSJ;\nUrl:https:\/\/www.douyu.com\/211099; Referer:https:\/\/www.douyu.com\/g_AC;\nUrl:https:\/\/www.douyu.com\/71415;
Referer:https:\/\/www.douyu.com\/g_TVgame;\nUrl:https:\/\/www.douyu.com\/501761;
Referer:https:\/\/www.douyu.com\/g_Mario;\nUrl:https:\/\/www.douyu.com\/629756;
Referer:https:\/\/www.douyu.com\/g_msg2;\nUrl:https:\/\/live.kuaishou.com\/u\/Naixi56789;
Referer:https:\/\/www.kuaishou.com\/;\nUrl:https:\/\/live.kuaishou.com\/u\/w445675940;
Referer:https:\/\/www.kuaishou.com\/;\nUrl:https:\/\/live.kuaishou.com\/u\/CFang899;
Referer:https:\/\/www.kuaishou.com\/;\nUrl:https:\/\/www.douyu.com\/topic\/tltkflive?rid=656841;
Referer:https:\/\/www.douyu.com\/g_EFT;\nUrl:https:\/\/www.douyu.com\/1236854;
Referer:https:\/\/www.douyu.com\/g_EFT;\nUrl:https:\/\/www.douyu.com\/topic\/tltkflive?rid=5234836;
Referer:https:\/\/www.douyu.com\/g_EFT;\nUrl:https:\/\/www.douyu.com\/5339476; Referer:https:\/\/www.douyu.com\/g_EFT;\nUrl:https:\/\/www.douyu.com\/7892;
Referer:https:\/\/www.douyu.com\/g_classic;\nUrl:https:\/\/www.douyu.com\/60651;
```

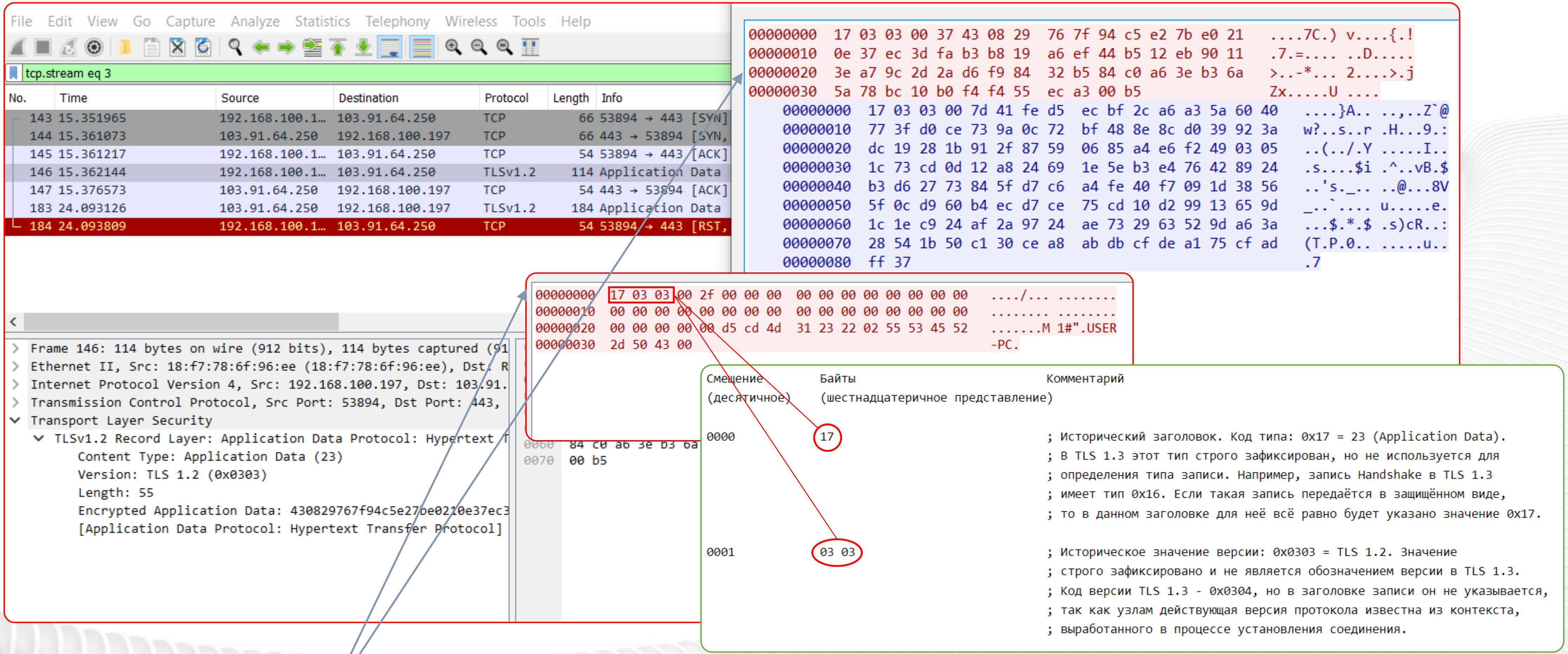
```
Правило 1.
msg: "BACKDOOR [PTsecurity] PlugX";
content: "POST"; http_method;
content: "/api/"; http_uri; depth: 5;
content: "User-Agent: Mozilla/5.0"; http_header;
content: "4EOkNJ73LO"; http_client_body; depth: 10;


Правило 2.
msg: "SUSPICIOUS [PTsecurity] Base64 data in Request";
content: "POST"; http_method;
pcre: "/^.{0,15}([A-Za-z]{4,15}=|)(?:[A-Za-z\d+\/]{4})*
       (?:[A-Za-z\d+\/]{3}=|[A-Za-z\d+\/]{2}==)?$/P";
pcre: "/([a-z][\d]|[A-Z][\d])/P";
pcre: "/([\d][a-z]|[\d][A-Z]|[A-Z]+|[a-z]+|[\d]+|[A-Z]\/|[a-z]\/|[\d]\/)/P";


Правило 3.
msg: "SUSPICIOUS [PTsecurity] Base64 data in Response";
content: "200"; http_stat_code;
pcre: "/^(?:[A-Za-z\d+\/]{4})*(?:[A-Za-z\d+\/]{3}=|[A-Za-z\d+\/]{2}==)?$/Q";
pcre: "/([a-z][\d]|[A-Z][\d])/Q";
pcre: "/([\d][a-z]|[\d][A-Z]|[A-Z]+|[a-z]+|[\d]+|[A-Z]\/|[a-z]\/|[\d]\/)/Q";
pcre: "/([a-z][A-Z][a-z]|[A-Z][a-z][A-Z])/Q";
```

03

Современные подходы злоумышленников к сокрытию сетевого взаимодействия вредоносного программного обеспечения

Мимикрия под TLS

Toneshell Backdoor



```
tcp.stream eq 3
```

```
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 (91
> 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,
v Transport Layer Security
  v 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]
```

```
0060  84 c0 a6 3e b3 6a
0070  00 b5
```

```
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.
```

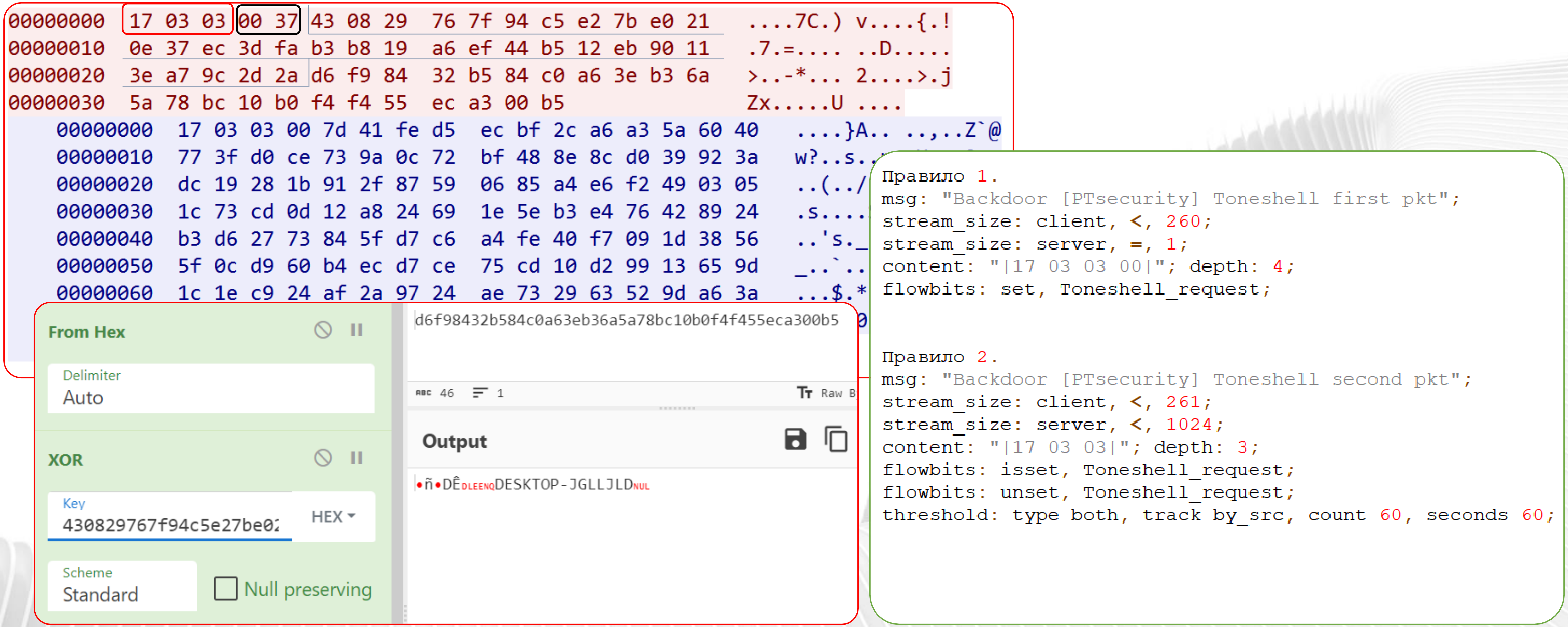
```
Смещение       Байты                              Комментарий
(десятичное)   (шестнадцатеричное представление)

0000           17                                 ; Исторический заголовок. Код типа: 0x17 = 23 (Application Data).
                                                  ; В TLS 1.3 этот тип строго зафиксирован, но не используется для
                                                  ; определения типа записи. Например, запись Handshake в TLS 1.3
                                                  ; имеет тип 0x16. Если такая запись передаётся в защищённом виде,
                                                  ; то в данном заголовке для неё всё равно будет указано значение 0x17.

0001           03 03                              ; Историческое значение версии: 0x0303 = TLS 1.2. Значение
                                                  ; строго зафиксировано и не является обозначением версии в TLS 1.3.
                                                  ; Код версии TLS 1.3 - 0x0304, но в заголовке записи он не указывается,
                                                  ; так как узлам действующая версия протокола известна из контекста,
                                                  ; выработанного в процессе установления соединения.
```

у клиентских пакетов TLS служебная часть больше, так как клиент инициирует подключение и сообщает дополнительные данные

Toneshell Backdoor

декодирование, детектирование, обнаружение

magic bytes   size   xor key 32 bytes



```
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..
    00000020  dc 19 28 1b 91 2f 87 59  06 85 a4 e6 f2 49 03 05   ..(../
    00000030  1c 73 cd 0d 12 a8 24 69  1e 5e b3 e4 76 42 89 24   .s....
    00000040  b3 d6 27 73 84 5f d7 c6  a4 fe 40 f7 09 1d 38 56   ..'s._
    00000050  5f 0c d9 60 b4 ec d7 ce  75 cd 10 d2 99 13 65 9d   _..`..
    00000060  1c 1e c9 24 af 2a 97 24  ae 73 29 63 52 9d a6 3a   ...$.*
```

From Hex

Delimiter: Auto

XOR

Key: 430829767f94c5e27be0: HEX

Scheme: Standard

□ Null preserving

```
d6f98432b584c0a63eb36a5a78bc10b0f4f455eca300b5
```

```
•ñ•DÊDLEENQDESKTOP-JGLLJLDNUL
```

```
Правило 1.
msg: "Backdoor [PTsecurity] Toneshell first pkt";
stream_size: client, <, 260;
stream_size: server, =, 1;
content: "|17 03 03 00|"; depth: 4;
flowbits: set, Toneshell_request;


Правило 2.
msg: "Backdoor [PTsecurity] Toneshell second pkt";
stream_size: client, <, 261;
stream_size: server, <, 1024;
content: "|17 03 03|"; depth: 3;
flowbits: isset, Toneshell_request;
flowbits: unset, Toneshell_request;
threshold: type both, track by_src, count 60, seconds 60;
```

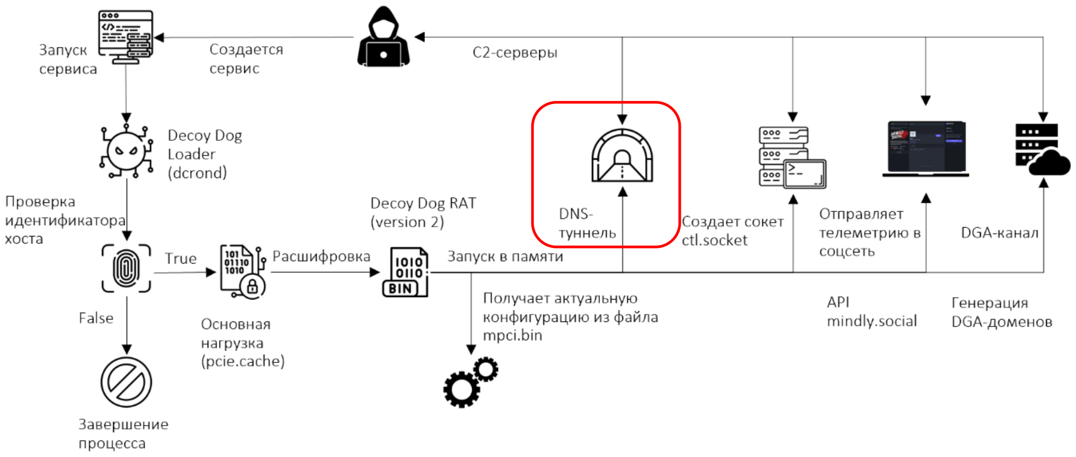
04

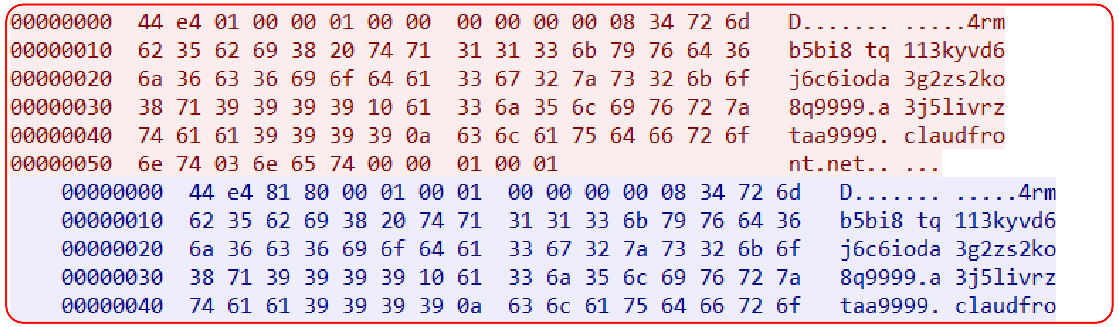
Современные подходы злоумышленников к сокрытию сетевого взаимодействия вредоносного программного обеспечения

DNS туннелирование

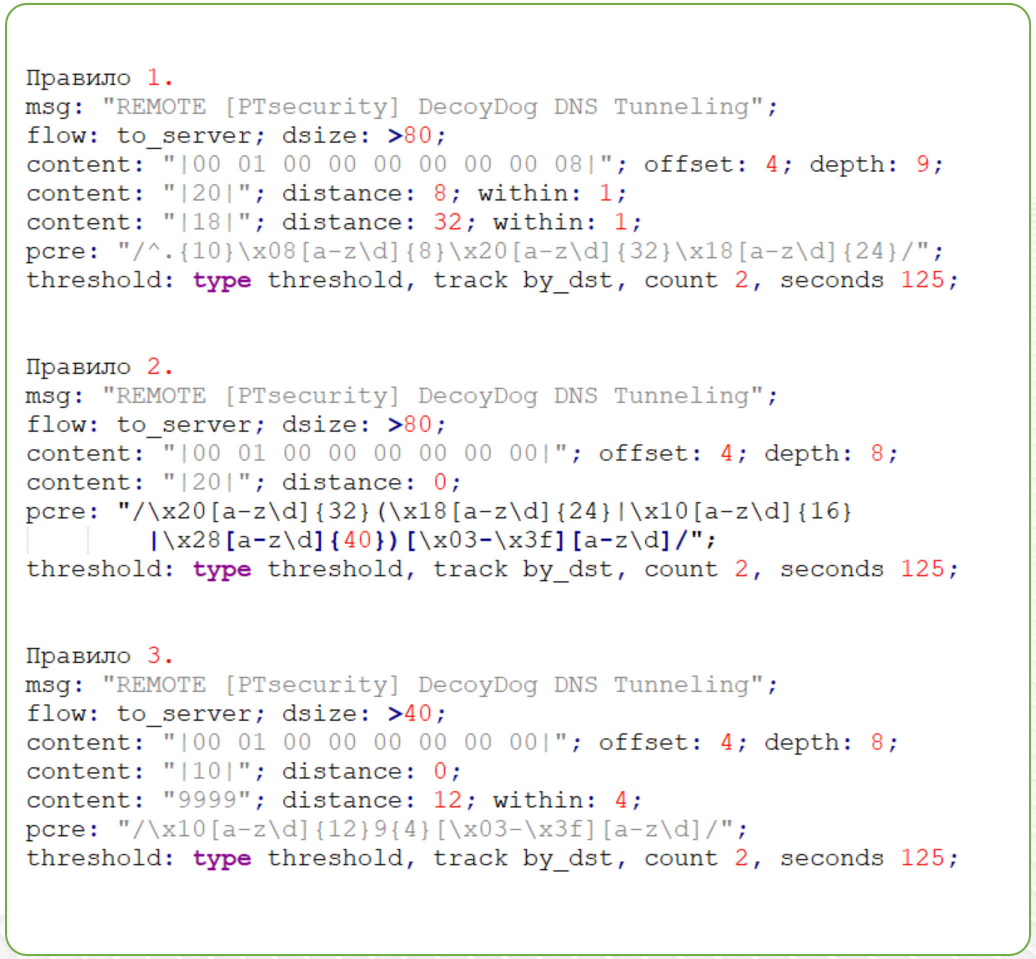
DecoyDog

декодирование, детектирование, обнаружение


Запуск сервиса
Создается сервис
C2-серверы
Decoy Dog Loader (dcrond)
Проверка идентификатора хоста
True
False
Завершение процесса
Основная нагрузка (pcie.cache)
Расшифровка
Decoy Dog RAT (version 2)
Запуск в памяти
DNS-туннель
Создает сокет ctl.socket
Отправляет телеметрию в соцсеть
DGA-канал
Получает актуальную конфигурацию из файла mpci.bin
API mindly.social
Генерация DGA-доменов



```
00000000  44 e4 01 00 00 01 00 00  00 00 00 00 08 34 72 6d   D....... .....4rm
00000010  62 35 62 69 38 20 74 71  31 31 33 6b 79 76 64 36   b5bi8 tq 113kyvd6
00000020  6a 36 63 36 69 6f 64 61  33 67 32 7a 73 32 6b 6f   j6c6ioda 3g2zs2ko
00000030  38 71 39 39 39 39 10 61  33 6a 35 6c 69 76 72 7a   8q9999.a 3j5livrz
00000040  74 61 61 39 39 39 39 0a  63 6c 61 75 64 66 72 6f   taa9999. claudfro
00000050  6e 74 03 6e 65 74 00 00  01 00 01                  nt.net.. ...
    00000000  44 e4 81 80 00 01 00 01  00 00 00 00 08 34 72 6d   D....... .....4rm
    00000010  62 35 62 69 38 20 74 71  31 31 33 6b 79 76 64 36   b5bi8 tq 113kyvd6
    00000020  6a 36 63 36 69 6f 64 61  33 67 32 7a 73 32 6b 6f   j6c6ioda 3g2zs2ko
    00000030  38 71 39 39 39 39 10 61  33 6a 35 6c 69 76 72 7a   8q9999.a 3j5livrz
    00000040  74 61 61 39 39 39 39 0a  63 6c 61 75 64 66 72 6f   taa9999. claudfro
```



```
Правило 1.
msg: "REMOTE [PTsecurity] DecoyDog DNS Tunneling";
flow: to_server; dsize: >80;
content: "|00 01 00 00 00 00 00 00 08|"; offset: 4; depth: 9;
content: "|20|"; distance: 8; within: 1;
content: "|18|"; distance: 32; within: 1;
pcre: "/^.{10}\x08[a-z\d]{8}\x20[a-z\d]{32}\x18[a-z\d]{24}/";
threshold: type threshold, track by_dst, count 2, seconds 125;


Правило 2.
msg: "REMOTE [PTsecurity] DecoyDog DNS Tunneling";
flow: to_server; dsize: >80;
content: "|00 01 00 00 00 00 00 00|"; offset: 4; depth: 8;
content: "|20|"; distance: 0;
pcre: "/\x20[a-z\d]{32}(\x18[a-z\d]{24}|\x10[a-z\d]{16}
        |\x28[a-z\d]{40})[\x03-\x3f][a-z\d]/";
threshold: type threshold, track by_dst, count 2, seconds 125;


Правило 3.
msg: "REMOTE [PTsecurity] DecoyDog DNS Tunneling";
flow: to_server; dsize: >40;
content: "|00 01 00 00 00 00 00 00|"; offset: 4; depth: 8;
content: "|10|"; distance: 0;
content: "9999"; distance: 12; within: 4;
pcre: "/\x10[a-z\d]{12}9{4}[\x03-\x3f][a-z\d]/";
threshold: type threshold, track by_dst, count 2, seconds 125;
```

Примеры C2:

- f4dl3fi9.kwxmohluim2l6axd2iacxlhashdq9999.mjgddgzaoknq9999.claudfront.net
- pre113z6q2ys4isevbarowj6anea9999.yyeefmc5ma999999.beacon.net.eu.org
- 11aje6eo5xaq9999.claudfront.net

https://www.ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/hellhounds-operaciya-lahat/

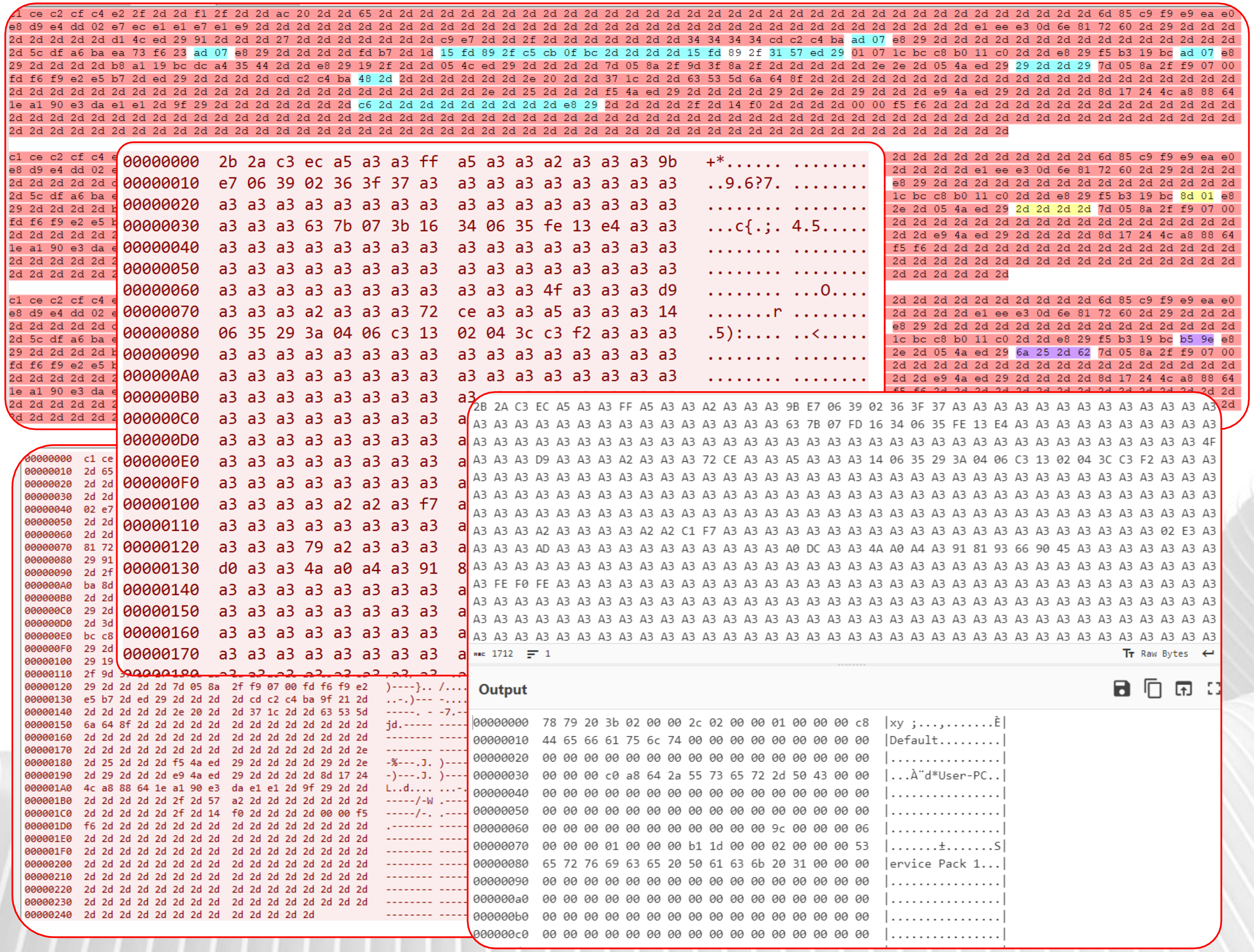
05

Современные подходы злоумышленников к сокрытию сетевого взаимодействия вредоносного программного обеспечения

Сдвиги и XOR-ы

YoungLotus RAT

декодирование, детектирование, обнаружение



```
c1 ce c2 cf c4 e2 2f 2d 2d f1 2f 2d 2d ac 20 2d 2d 65 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 6d 85 c9 f9 e9 ea e0
e8 d9 e4 dd 02 e7 ec e1 e1 e7 e1 e9 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d e1 ee e3 0d 6e 81 72 60 2d 29 2d 2d 2d
2d 2d 2d 2d 2d d1 4c ed 29 91 2d 2d 2d 27 2d 2d 2d 2d 2d 2d 2d c9 e7 2d 2d 2f 2d 2d 2d 2d 2d 2d 2d 34 34 34 34 cd c2 c4 ba ad 07 e8 29 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d
2d 5c df a6 ba ea 73 f6 23 ad 07 e8 29 2d 2d 2d 2d fd b7 2d 1d 15 fd 89 2f c5 cb 0f bc 2d 2d 2d 2d 15 fd 89 2f 31 57 ed 29 01 07 1c bc c8 b0 11 c0 2d 2d e8 29 f5 b3 19 bc ad 07 e8
29 2d 2d 2d 2d b8 a1 19 bc dc a4 35 44 2d 2d e8 29 19 2f 2d 2d 05 4c ed 29 2d 2d 2d 2d 7d 05 8a 2f 9d 3f 8a 2f 2d 2d 2d 2d 2d 2e 2e 2d 05 4a ed 29 29 2d 2d 29 7d 05 8a 2f f9 07 00
fd f6 f9 e2 e5 b7 2d ed 29 2d 2d 2d 2d cd c2 c4 ba 48 2d 2d 2d 2d 2d 2d 2d 2e 20 2d 2d 37 1c 2d 2d 63 53 5d 6a 64 8f 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d
2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2e 2d 25 2d 2d 2d f5 4a ed 29 2d 2d 2d 2d 29 2d 2e 2d 29 2d 2d 2d e9 4a ed 29 2d 2d 2d 2d 8d 17 24 4c a8 88 64
1e a1 90 e3 da e1 e1 2d 9f 29 2d 2d 2d 2d 2d 2d 2d c6 2d 2d 2d 2d 2d 2d 2d 2d 2d e8 29 2d 2d 2d 2d 2f 2d 14 f0 2d 2d 2d 2d 00 00 f5 f6 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d
2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d
2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d
```

```
00000000  2b 2a c3 ec a5 a3 a3 ff  a5 a3 a3 a2 a3 a3 a3 9b   +*...... ........
00000010  e7 06 39 02 36 3f 37 a3  a3 a3 a3 a3 a3 a3 a3 a3   ..9.6?7. ........
00000020  a3 a3 a3 a3 a3 a3 a3 a3  a3 a3 a3 a3 a3 a3 a3 a3   ........ ........
00000030  a3 a3 a3 63 7b 07 3b 16  34 06 35 fe 13 e4 a3 a3   ...c{.;. 4.5.....
00000040  a3 a3 a3 a3 a3 a3 a3 a3  a3 a3 a3 a3 a3 a3 a3 a3   ........ ........
00000050  a3 a3 a3 a3 a3 a3 a3 a3  a3 a3 a3 a3 a3 a3 a3 a3   ........ ........
00000060  a3 a3 a3 a3 a3 a3 a3 a3  a3 a3 a3 4f a3 a3 a3 d9   ........ ...O....
00000070  a3 a3 a3 a2 a3 a3 a3 72  ce a3 a3 a5 a3 a3 a3 14   .......r ........
00000080  06 35 29 3a 04 06 c3 13  02 04 3c c3 f2 a3 a3 a3   .5):.... ..<.....
00000090  a3 a3 a3 a3 a3 a3 a3 a3  a3 a3 a3 a3 a3 a3 a3 a3   ........ ........
000000A0  a3 a3 a3 a3 a3 a3 a3 a3  a3 a3 a3 a3 a3 a3 a3 a3   ........ ........
000000B0  a3 a3 a3 a3 a3 a3 a3 a3  a3
000000C0  a3 a3 a3 a3 a3 a3 a3 a3
000000D0  a3 a3 a3 a3 a3 a3 a3 a3
000000E0  a3 a3 a3 a3 a3 a3 a3 a3
000000F0  a3 a3 a3 a3 a3 a3 a3 a3
00000100  a3 a3 a3 a3 a2 a2 a3 f7
00000110  a3 a3 a3 a3 a3 a3 a3 a3
00000120  a3 a3 a3 79 a2 a3 a3 a3
00000130  d0 a3 a3 4a a0 a4 a3 91  8
00000140  a3 a3 a3 a3 a3 a3 a3 a3
00000150  a3 a3 a3 a3 a3 a3 a3 a3
00000160  a3 a3 a3 a3 a3 a3 a3 a3
00000170  a3 a3 a3 a3 a3 a3 a3 a3
```

```
2B 2A C3 EC A5 A3 A3 FF A5 A3 A3 A2 A3 A3 A3 9B E7 06 39 02 36 3F 37 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3
A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 63 7B 07 FD 16 34 06 35 FE 13 E4 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3
A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 4F
A3 A3 A3 D9 A3 A3 A3 A2 A3 A3 A3 72 CE A3 A3 A5 A3 A3 A3 14 06 35 29 3A 04 06 C3 13 02 04 3C C3 F2 A3 A3 A3
A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3
A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3
A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3
A3 A3 A3 A2 A3 A3 A3 A3 A2 A2 C1 F7 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 02 E3 A3
A3 A3 A3 AD A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A0 DC A3 A3 4A A0 A4 A3 91 81 93 66 90 45 A3 A3 A3 A3 A3 A3 A3
A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3
A3 FE F0 FE A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3
A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3
A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3
A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3 A3
```

Output

```
00000000  78 79 20 3b 02 00 00 2c 02 00 00 01 00 00 00 c8  |xy ;...,.......È|
00000010  44 65 66 61 75 6c 74 00 00 00 00 00 00 00 00 00  |Default.........|
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |................|
00000030  00 00 00 c0 a8 64 2a 55 73 65 72 2d 50 43 00 00  |...À¨d*User-PC..|
00000040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |................|
00000050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |................|
00000060  00 00 00 00 00 00 00 00 00 00 00 9c 00 00 00 06  |................|
00000070  00 00 00 01 00 00 00 b1 1d 00 00 02 00 00 00 53  |.......±.......S|
00000080  65 72 76 69 63 65 20 50 61 63 6b 20 31 00 00 00  |ervice Pack 1...|
00000090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |................|
000000a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |................|
000000b0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |................|
000000c0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  |................|
```

```
Правило 1.
msg: "REMOTE [PTsecurity] YoungLotus first rqs pkt";
flow: established, to_server;
dsize: 482<>487;
stream_size: server, =,1;
stream_size: server, <,2;
stream_size: client, <,488;
byte_extract: 2, 5, byte0;
byte_test: 2, =, byte0, 9;
byte_test: 2, =, byte0, 12;
flowbits: set, YoungLotus_rqs_fstpkt;


Правило 2.
msg: "REMOTE [PTsecurity] YoungLotus first rsp pkt";
flow: established, to_client;
dsize: 16;
stream_size: server, =,17;
stream_size: client, >,0;
stream_size: client, <,488;
byte_extract: 2, 5, byte0;
byte_test: 2, =, byte0, 9;
byte_test: 2, =, byte0, 12;
flowbits: isset, YoungLotus_rqs_fstpkt;
flowbits: unset, YoungLotus_rqs_fstpkt;
flowbits: set, YoungLotus_rsp_fstpkt;


Правило 3.
msg: "REMOTE [PTsecurity] YoungLotus";
flow: established, to_server;
dsize: >1000;
stream_size: server, =,17;
stream_size: client, <,2000;
flowbits: isset, YoungLotus_rsp_fstpkt;
flowbits: unset, YoungLotus_rsp_fstpkt;
```

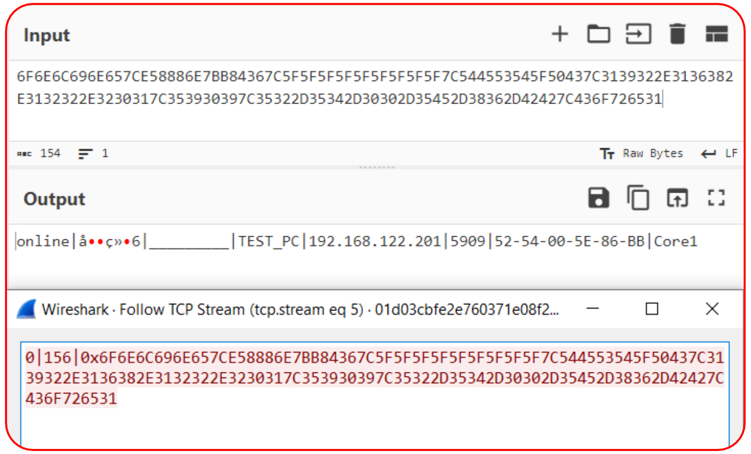
06

Современные подходы злоумышленников к сокрытию сетевого взаимодействия вредоносного программного обеспечения

Base64, netbios, hex…

декодирование, детектирование, обнаружение

Just HEX



Input

```
6F6E6C696E657CE58886E7BB84367C5F5F5F5F5F5F5F5F5F5F7C544553545F50437C3139322E3136382
E3132322E3230317C353930397C35322D35342D30302D35452D38362D42427C436F726531
```

Output

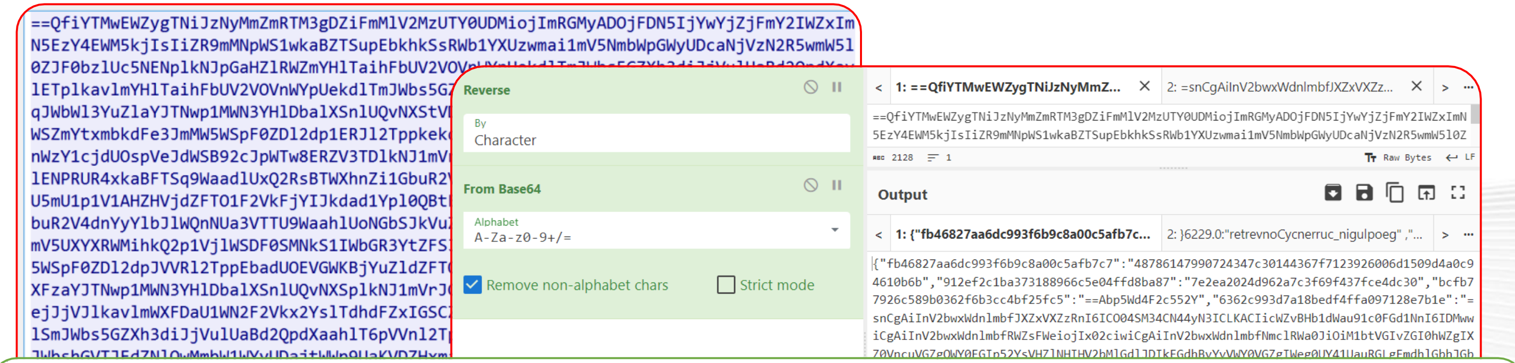
```
online|å••ç»•6|__________|TEST_PC|192.168.122.201|5909|52-54-00-5E-86-BB|Core1
```

Wireshark · Follow TCP Stream (tcp.stream eq 5) · 01d03cbfe2e760371e08f2...

```
0|156|0x6F6E6C696E657CE58886E7BB84367C5F5F5F5F5F5F5F5F5F5F7C544553545F50437C31
39322E3136382E3132322E3230317C353930397C35322D35342D30302D35452D38362D42427C
436F726531
```

```
Правило 1.
msg: "BACKDOOR [PTsecurity] PlugX";
dsize: <256;
stream_size: client, <, 257;
content: "|7c|"; offset: 1; depth: 1;
content: "|7c 30 78|"; distance: 1; within: 10;
fast_pattern;
content: "7c5f5f5f"; within: 50;
content: "7c"; distance: 0; within: 50;
content: "2e"; distance: 0; within: 50;
content: "2e"; distance: 2; within: 8;
content: "2e"; distance: 2; within: 8;
content: "7c"; distance: 2; within: 8;
content: "7c"; distance: 4; within: 12;
content: "2d"; distance: 4; within: 2;
content: "2d"; distance: 4; within: 2;
content: "2d"; distance: 4; within: 2;
content: "2d"; distance: 4; within: 2;
content: "2d"; distance: 4; within: 2;
content: "7c"; distance: 4; within: 2;
```

Just reverse base64



```
==QfiYTMwEWZygTNiJzNyMmZmRTM3gDZiFmMlV2MzUTY0UDMiojImRGMyADOjFDN5IjYwYjZjFmY2IWZxIm
N5EzY4EWM5kjIsIiZR9mMNpWS1wkaBZTSupEbkhkSsRWb1YXUzwmai1mV5NmbWpGWyUDcaNjVzN2R5wmW5l
0ZJF0bzlUc5NENplkNJpGaHZ1RWZmYHlTaihFbUV2VOV
lETplkavlmYHlTaihFbUV2VOVnWYpUekdlTmJWbs5GZ
qJWbWl3YuZlaYJTNwp1MWN3YHlDbalXSnlUQvNXStV
WSZmYtxmbkdFe3JmMW5WSpF0ZDl2dp1ERJl2Tppkek
nWzY1cjdUOspVeJdWSB92cJpWTw8ERZV3TDlkNJ1mV
lENPRUR4xkaBFTSq9WaadlUxQ2RsBTWXhnZi1GbuR2
U5mU1p1V1AHZHVjdZFTO1F2VkFjYIJkdad1Ypl0QBt
buR2V4dnYyYlbJlWQnNUa3VTTU9WaahlUoNGbSJkVu
mV5UXYXRWMihkQ2p1VjlWSDF0SMNkS1IWbGR3YtZFS
5WSpF0ZDl2dpJVVRl2TppEbadUOEVGWKBjYuZldZFT
XFzaYJTNwp1MWN3YHlDbalXSnlUQvNXSplkNJ1mVrJ
ejJjVJlkavlmWXFDaU1WN2F2Vkx2YslTdhdFZxIGSC
lSmJWbs5GZXh3diJjVulUaBd2QpdXaahlT6pVVnl2T
```

Reverse

By
Character

From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars ☐ Strict mode

1: ==QfiYTMwEWZygTNiJzNyMmZ...
2: =snCgAiInV2bwxWdnlmbfJXZxVXZz...
2128
1
Raw Bytes
LF

```
==QfiYTMwEWZygTNiJzNyMmZmRTM3gDZiFmMlV2MzUTY0UDMiojImRGMyADOjFDN5IjYwYjZjFmY2IWZxImN
5EzY4EWM5kjIsIiZR9mMNpWS1wkaBZTSupEbkhkSsRWb1YXUzwmai1mV5NmbWpGWyUDcaNjVzN2R5wmW5l0Z
```

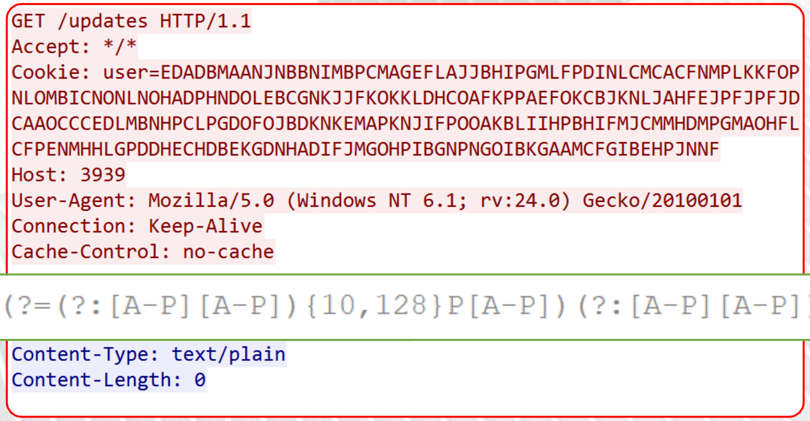
Output

1: {"fb46827aa6dc993f6b9c8a00c5afb7c...
2: }6229.0:"retrevnoCycnerruc_nigulpoeg" ,"...

```
{"fb46827aa6dc993f6b9c8a00c5afb7c7":"48786147990724347c30144367f7123926006d1509d4a0c9
4610b6b","912ef2c1ba373188966c5e04ffd8ba87":"7e2ea2024d962a7c3f69f437fce4dc30","bcfb7
7926c589b0362f6b3cc4bf25fc5":"==Abp5Wd4F2c552Y","6362c993d7a18bedf4ffa097128e7b1e":"=
snCgAiInV2bwxWdnlmbfJXZxVXZzRnI6ICO04SM34CN44yN3ICLKACIicWZvBHb1dWau91c0FGd1NnI6IDMww
iCgAiInV2bwxWdnlmbfRWZsFWeiojIx02ciwiCgAiInV2bwxWdnlmbfNmclRWa0JiOiM1btVGIvZGI0hWZgIX
```

```
Правило 2.
msg: "SUSPICIOUS [PTsecurity] Reverse Base64 data";
flow: established, to_client;
content: "200"; http_stat_code;
pcre: "/^(=[AEIMQUYcgkosw048][A-Za-z\d+\/]{2}|==[AQgw][A-Za-z\d+\/]{1})(?:[A-Za-z\d+\/]{4}){30}/Q";
pcre: "/([\d][a-z]|[\d][A-Z])/QR";
pcre: "/([a-z][A-Z][a-z]|[A-Z][a-z][A-Z])/QR";
```

Just netbios



```
GET /updates HTTP/1.1
Accept: */*
Cookie: user=EDADBMAANJNBBNIMBPCMAGEFLAJJBHIPGMLFPDINLCMCACFNMPLKKFOP
NLOMBICNONLNOHADPHNDOLEBCGNKJJFKOKKLDHCOAFKPPAEFOKCBJKNLJAHFEJPFJPFJD
CAAOCCCEDLMBNHPCLPGDOFOJBDKNKEMAPKNJIFPOOAKBLIIHPBHIFMJCMMHDMPGMAOHFL
CFPENMHHLGPDDHECHDBEKGDNHADIFJMGOHPIBGNPNGOIBKGAAMCFGIBEHPJNNF
Host: 3939
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101
Connection: Keep-Alive
Cache-Control: no-cache
```

```
pcre: "/=(?=(?:[A-P][A-P]){10,128}P[A-P])(?:[A-P][A-P]){128}/CR";
```

```
Content-Type: text/plain
Content-Length: 0
```

Контакты

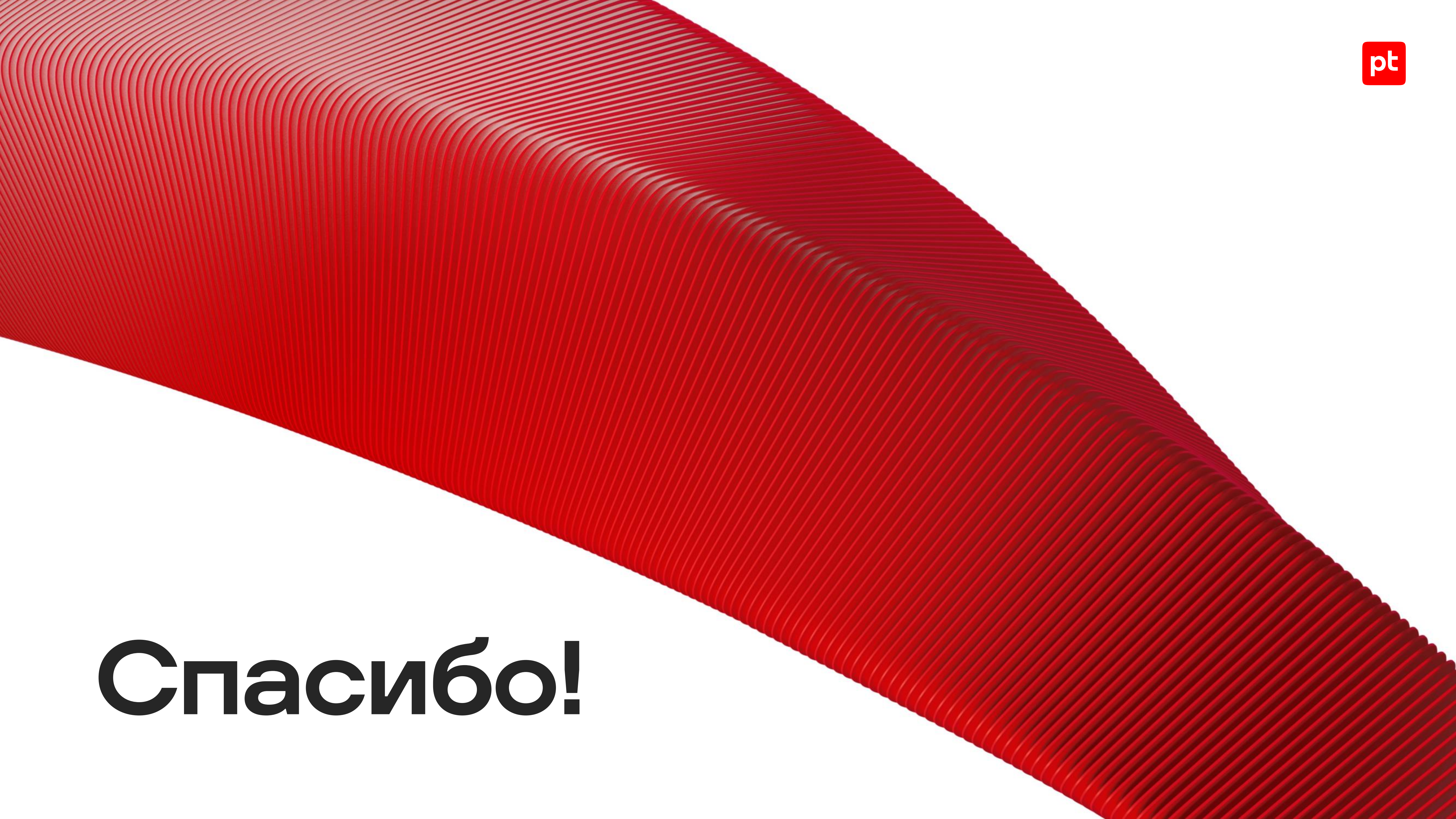
Ксения Наумова

Специалист отдела обнаружения вредоносного ПО
экспертного центра безопасности Positive Technologies

knaumova@ptsecurity.com

@naumovax

habr.com/ru/users/naumovax/publications/articles/



Спасибо!