

SmokeLoader

Historical Changes and Trends

Marcos Alvares
Technical Analysis Cell

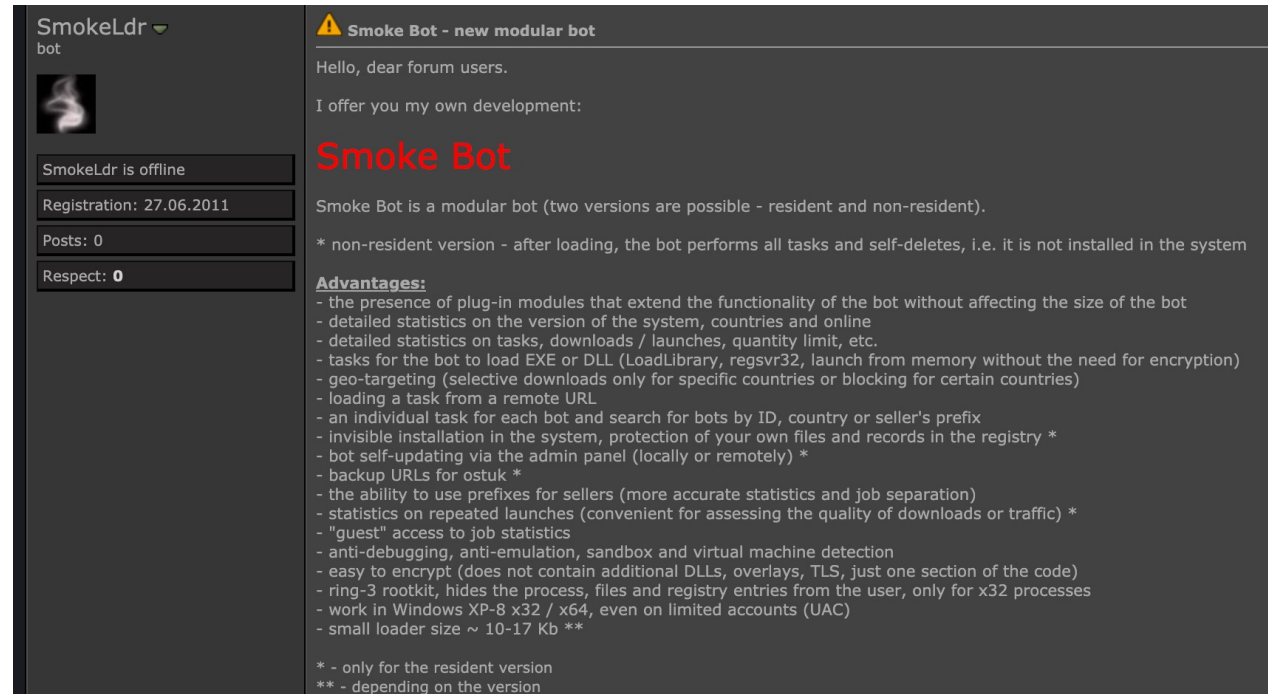


I. Context

Success Factors

Success Factors

■ Business model



The screenshot shows a forum post from a user named 'SmokeLdr' (bot). The user's profile information is visible on the left, including their registration date (27.06.2011) and a 'Respect' score of 0. The main content of the post is a promotional message for 'Smoke Bot', a modular bot. The post includes a warning icon and the title 'Smoke Bot - new modular bot'. The text describes the bot's capabilities and lists several advantages, such as detailed statistics, geo-targeting, and anti-debugging features. The post also includes a list of advantages and a note about the resident version.

SmokeLdr bot

SmokeLdr is offline

Registration: 27.06.2011

Posts: 0

Respect: 0

Smoke Bot - new modular bot

Hello, dear forum users.

I offer you my own development:

Smoke Bot

Smoke Bot is a modular bot (two versions are possible - resident and non-resident).

* non-resident version - after loading, the bot performs all tasks and self-deletes, i.e. it is not installed in the system

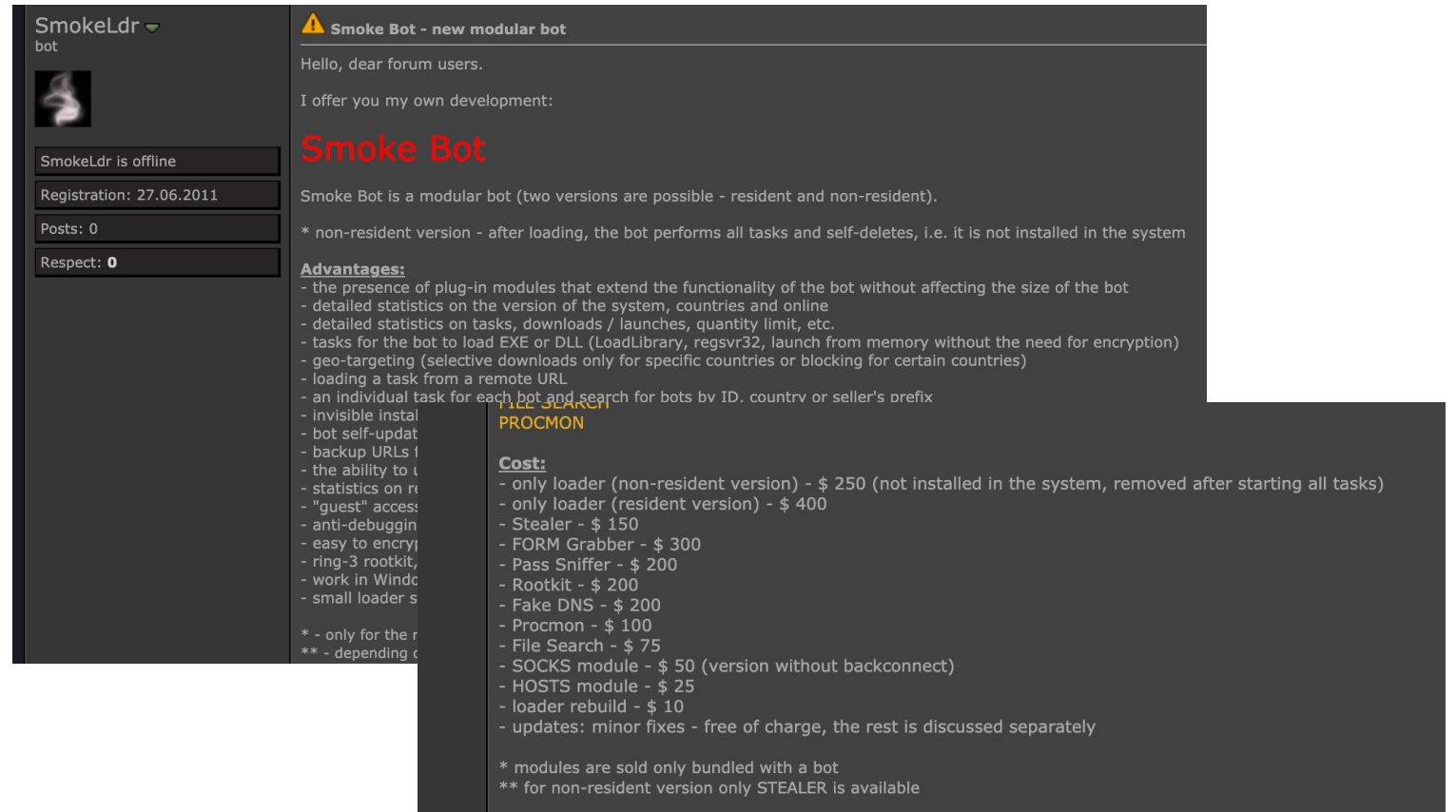
Advantages:

- the presence of plug-in modules that extend the functionality of the bot without affecting the size of the bot
- detailed statistics on the version of the system, countries and online
- detailed statistics on tasks, downloads / launches, quantity limit, etc.
- tasks for the bot to load EXE or DLL (LoadLibrary, regsvr32, launch from memory without the need for encryption)
- geo-targeting (selective downloads only for specific countries or blocking for certain countries)
- loading a task from a remote URL
- an individual task for each bot and search for bots by ID, country or seller's prefix
- invisible installation in the system, protection of your own files and records in the registry *
- bot self-updating via the admin panel (locally or remotely) *
- backup URLs for ostuk *
- the ability to use prefixes for sellers (more accurate statistics and job separation)
- statistics on repeated launches (convenient for assessing the quality of downloads or traffic) *
- "guest" access to job statistics
- anti-debugging, anti-emulation, sandbox and virtual machine detection
- easy to encrypt (does not contain additional DLLs, overlays, TLS, just one section of the code)
- ring-3 rootkit, hides the process, files and registry entries from the user, only for x32 processes
- work in Windows XP-8 x32 / x64, even on limited accounts (UAC)
- small loader size ~ 10-17 Kb **

* - only for the resident version
** - depending on the version

Success Factors

- Business model
- Cost



The screenshot shows a forum post for 'Smoke Bot' by user 'SmokeLdr'. The user's profile on the left indicates they are offline, registered on 27.06.2011, and have 0 posts. The post title is 'Smoke Bot - new modular bot'. The content describes the bot as a modular tool with various tasks and features. It lists several advantages such as plug-in modules, detailed statistics, and geo-targeting. A price list is provided for different modules, including a loader for \$250, a stealer for \$150, and various other tools like FORM Grabber, Pass Sniffer, Rootkit, Fake DNS, Procmon, File Search, SOCKS module, and HOSTS module. The post also mentions that updates are free of charge and that modules are sold bundled with a bot.

SmokeLdr
bot

SmokeLdr is offline

Registration: 27.06.2011

Posts: 0

Respect: 0

Smoke Bot - new modular bot

Hello, dear forum users.

I offer you my own development:

Smoke Bot

Smoke Bot is a modular bot (two versions are possible - resident and non-resident).

* non-resident version - after loading, the bot performs all tasks and self-deletes, i.e. it is not installed in the system

Advantages:

- the presence of plug-in modules that extend the functionality of the bot without affecting the size of the bot
- detailed statistics on the version of the system, countries and online
- detailed statistics on tasks, downloads / launches, quantity limit, etc.
- tasks for the bot to load EXE or DLL (LoadLibrary, regsvr32, launch from memory without the need for encryption)
- geo-targeting (selective downloads only for specific countries or blocking for certain countries)
- loading a task from a remote URL
- an individual task for each bot and search for bots by ID, country or seller's prefix
- Invisible instal
- bot self-updat
- backup URLs f
- the ability to l
- statistics on r
- "guest" acces
- anti-debuggin
- easy to encryp
- ring-3 rootkit,
- work in Windc
- small loader s

* - only for the r
** - depending c

Cost:

- only loader (non-resident version) - \$ 250 (not installed in the system, removed after starting all tasks)
- only loader (resident version) - \$ 400
- Stealer - \$ 150
- FORM Grabber - \$ 300
- Pass Sniffer - \$ 200
- Rootkit - \$ 200
- Fake DNS - \$ 200
- Procmon - \$ 100
- File Search - \$ 75
- SOCKS module - \$ 50 (version without backconnect)
- HOSTS module - \$ 25
- loader rebuild - \$ 10
- updates: minor fixes - free of charge, the rest is discussed separately

* modules are sold only bundled with a bot
** for non-resident version only STEALER is available

Success Factors

- Business model
- Cost
- Complexity

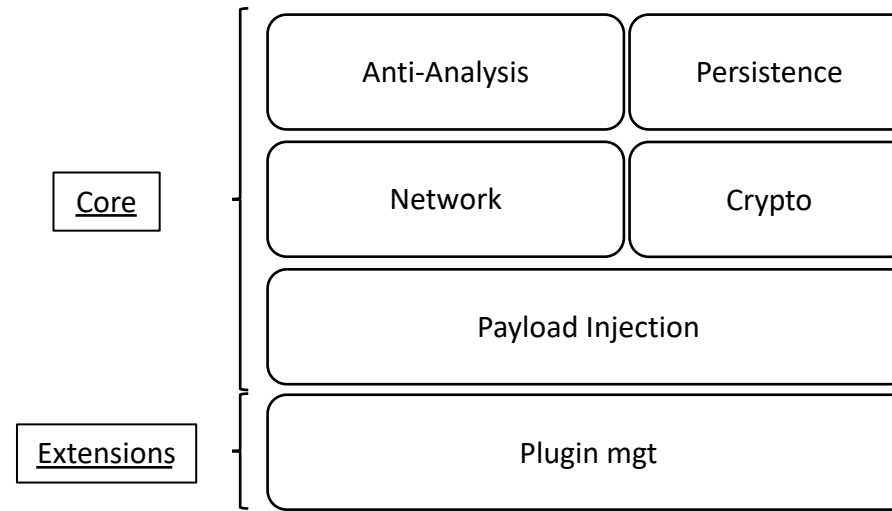
Equipment:

- loader
- builder of prefixes for "sellers"
- admin panel (PHP, MySQL)
- modules (upon purchase)
- parser of STEALER logs with instructions

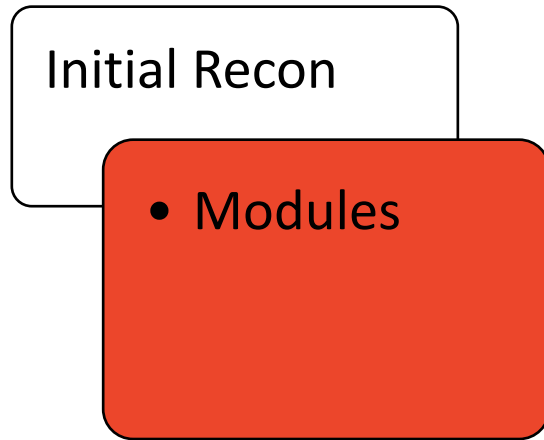
Binary + Panel + Modules

Success Factors

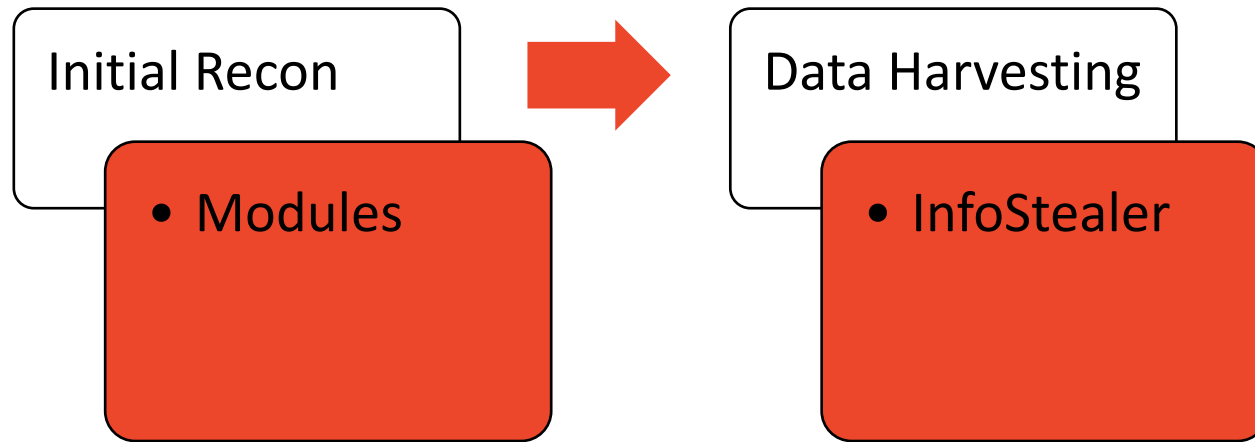
- Business model
- Cost
- Complexity



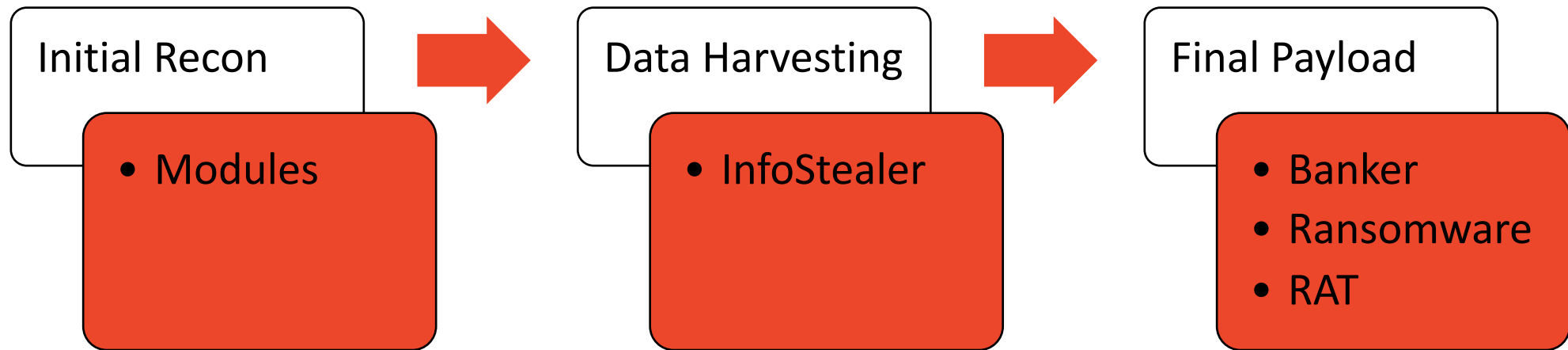
Operational



Operational

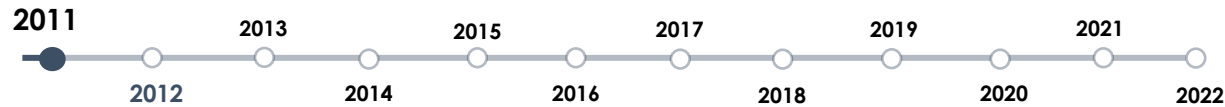


Operational



II. Code & Tactics

Tactics - Starting Point



Smoke Loader, a malware first discovered in 2011, has been used by attackers ever since. Smoke Loader was in steady demand due to its features and detection bypass techniques, which helped di

Smokeloder emerged from the Russian cybercrime underground in 2011. Its developer "SmokeLdr" is known to be customer friendly and they quickly act on customer complaints. Smokeloder is a crime kit that comes with a prebuilt bot, a PHP-based command and control panel, and a user manual. In addition, cybercriminals can purchas

SmokeLoader Analysis

Smokeloder is a downloader/backdoor which has been active since 2011. Over the years it has evolved both its capabilities and the variety of malware it downloads to the infected host. In this post we will have a look at what's changed since the most recent analysis by Checkpoint and present the new features introduced in 2020

Background

Smokeloder is a popular bot and a veteran in its field – being sold on underground cybercriminal markets since 2011, this piece of malware is used mainly for loading other malicious software, usually obtained from a third party. At the same time, it has the capability of loading its own modules, allowing it to conduct a variety of actions without the usage of external

Smokeloder's Hardcoded Domains - Sneaky Third Party Vendor or Cheap Buyer?

Smokeloder is a small modular bot first seen in 2011 [1] mainly used as a dropper for other malware families. Although mainly delivering a second stage stage, Smokeloder implements several malicious capabilities through its modules, such as: keylogging, monitoring, DDOS, DNS redirection and form grabbing. These modules are often used for profiling and accessing infected machi

Smoke Loader first surfaced in June 2011 when it was advertised for sale on grabberz.com¹ and xaker.name² by a user called SmokeLdr.



Smoke Loader

Smoke Loader is a malicious bot application that can be used to load other malware. Smoke Loader has been seen in the wild since at least 2011 and has included a number of different payloads. It is notorious for its use of deception and self-protection. It also comes with several plug-ins. [1] [2]

Tactics - Starting Point

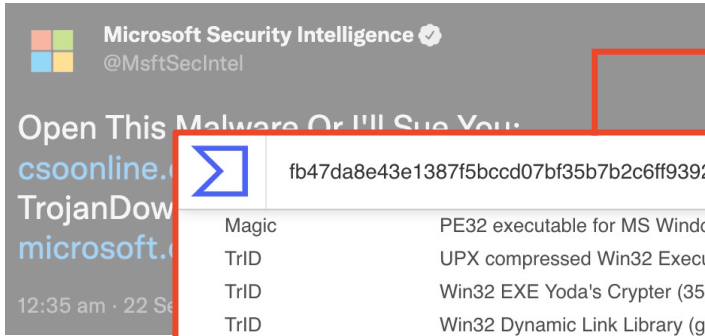
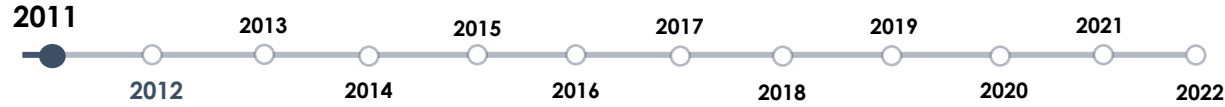


 Microsoft Security Intelligence 
@MsftSecIntel

Open This Malware Or I'll Sue You:
csoonline.com/article/690241..., Detected as
TrojanDownloader:Win32/Dofail.D
microsoft.com/security/porta...

12:35 am · 22 Sep 2011 · Twitter for Websites

Tactics - Starting Point



falcononfly2006[.]ru
falcononfly2007[.]ru

91.229.90[.]139
(UA - 2011)

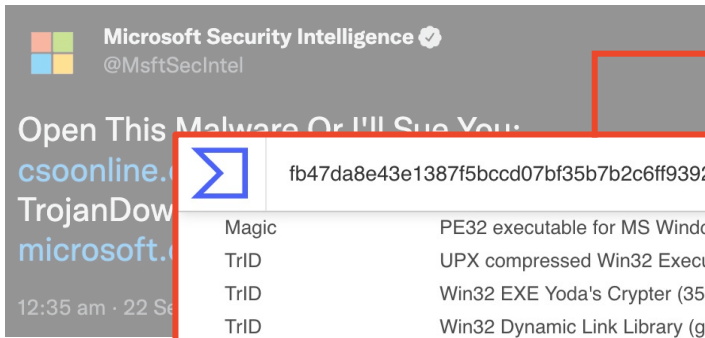
Tactics - Starting Point



falcononfly2006[.]ru
falcononfly2007[.]ru

91.229.90[.]139
(UA - 2011)

livegroup128[.]ru



fb47da8e43e1387f5bccd07bf35b7b2c6ff93920a9ea3cf1817bd2006c4f0b5b

Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	UPX compressed Win32 Executable (35.7%)
TrID	Win32 EXE Yoda's Crypter (35%)
TrID	Win32 Dynamic Link Library (generic) (8.6%)
TrID	Win16 NE executable (generic) (6.6%)
TrID	Win32 Executable (generic) (5.9%)
File size	44.50 KB (45568 bytes)

History

Creation Time	2008-09-16 08:43:02 UTC
First Submission	2011-09-20 06:50:49 UTC
Last Submission	2016-01-25 08:41:57 UTC
Last Analysis	2021-03-21 23:19:12 UTC

Names

2166218

07152b25369fd5c3c664f3e064f0e1d11f3ab8a00accf20680e866748f1c0fbc

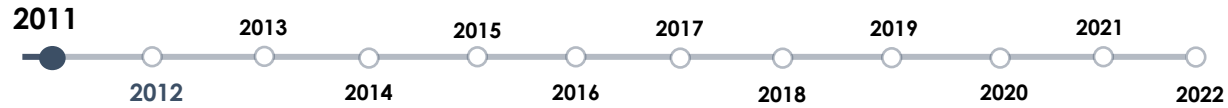
Mutexes Created

- CTF.LBES.MutexDefaultS-1-5-21-1482476501-1645522239-1417001333-500
- CTF.Compart.MutexDefaultS-1-5-21-1482476501-1645522239-1417001333-500
- CTF.Asm.MutexDefaultS-1-5-21-1482476501-1645522239-1417001333-500
- CTF.Layouts.MutexDefaultS-1-5-21-1482476501-1645522239-1417001333-500
- CTF.TMD.MutexDefaultS-1-5-21-1482476501-1645522239-1417001333-500
- CTF.TimListCache.FMPDefaultS-1-5-21-1482476501-1645522239-1417001333-500MUTE
- SHIMLIB_LOG_MUTEX

Mutexes Opened

- SmokeLoader
- ShimCacheMutex

Tactics - Beta



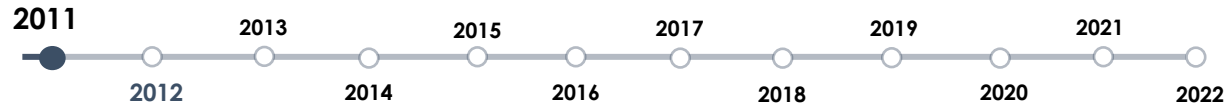
- UPX
- svchost.exe
- Checks connection
- HTTP
- XOR encrypted DLLs

BEACON

```
GET /blog/task.php
```

```
bid=344e17c07cbae8ce&os=6-1-  
7601&uptime=0&rnd=164239896
```


Tactics



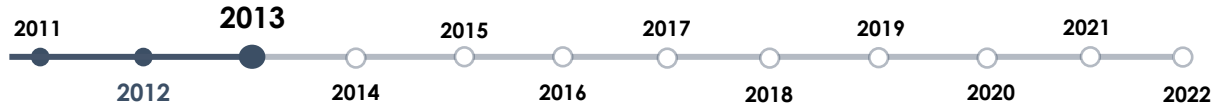
- “getload” command
- “SmokeLoader” mutex
- Commercial version

BEACON

```
GET /m07/index.php
```

```
cmd=getload&login=248B0241860741F51&s  
el=2495&ver=&bits=0
```

Tactics



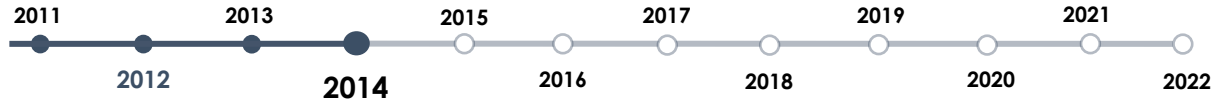
- Replaces SL Mutex
- “s2k13”
- Updates protocol

BEACON

GET /

```
cmd=getload&login=65070D1A4B443C2637F  
ED4E852F9D9F27CBAE8CE&sel=sel2&ver=6.  
1&bits=0&admin=1&hash=
```

Tactics



- explorer.exe
- “s2k14”

BEACON

GET /

```
cmd=getload&login=65070D1A4B443C2637FED4E  
852F9D9F27CBAE8CE&sel=sec6&ver=6.1&bits=0&  
admin=1&hash=
```

Tactics



- Encrypts resources
- HTTP POST
- Placeholders
- RC4

BEACON

POST /

4 Bytes RC4 key

+

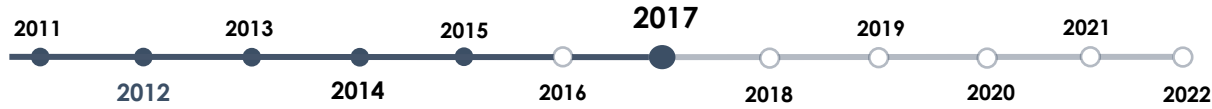
RC4(

2015#DFC547E8B4F619DE561270009ECB1

ACF7CBAE8CE#00015#6.1#0#0#10001#0#

)

Tactics



- Watchdog threads (2)
- New RC4 Crypto scheme
- Removes placeholders
- Namecoins (.bit)
- 63 Bytes checkin

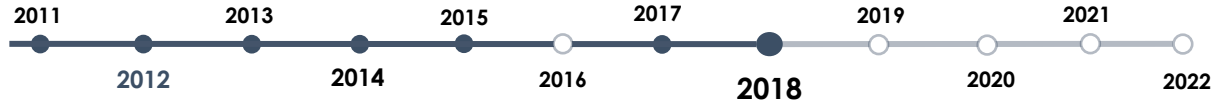
BEACON

POST /

RC4 (

```
E1 07 46 32 38 32 31 38 45 36 46 41 32 45 30 42  á.F28218E6FA2E0B
45 35 39 42 46 42 45 44 44 37 37 36 35 42 35 30  E59BFBEDD7765B50
46 34 37 43 42 41 45 38 43 45 00 73 61 6E 74 00  F47CBAE8CE.sant.
00 61 00 00 11 27 00 00 00 00 00 00 00 00 00 00  .a...'.
)
```

Tactics



- 64 Bits
- PROPagate

BEACON

POST /

RC4(
E2 07 30 31 36 32 33 44 31 43 44 35 44 36 44 37 â.01623D1CD5D6D7
36 33 34 31 34 34 43 32 37 36 38 39 46 32 30 35 634144C27689F205
39 37 37 43 42 41 45 38 43 45 00 00 00 00 00 00 977CBAE8CE.....
00 61 00 00 11 27 00 00 00 00 01 00 00 00 00 .a... '.....
)

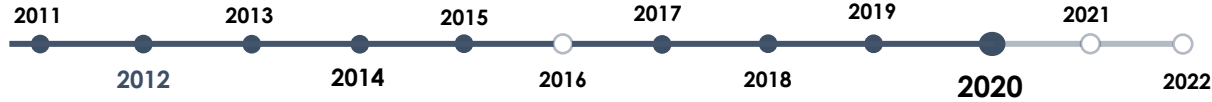
Tactics



- Copy&Load ntdll.dll
- Appends random Bytes
- Cracked version

```
BEACON  
  
POST /  
  
RC4(  
E3 07 32 44 43 43 32 43 35 30 32 46 45 32 45 45  ä.2DCC2C502FE2EE  
45 34 33 34 42 41 38 32 42 37 38 34 43 34 45 36  E434BA82B784C4E6  
39 46 37 43 42 41 45 38 43 45 00 31 31 30 36 00  9F7CBAE8CE.1106.  
00 61 00 00 11 27 00 00 00 00 01 00 00 00 6F 2D  .a...'.o-  
66 6D 24 67 3D 3E 73 5D 6A 71 6B 21 5B 23 77 68  fm$g=>s]jqk![#wh  
71 21 6C 29 24 77 36 60 39 6D 3E 44 3F 68 46 35  q!l)$w6`9m>D?hF5  
3F 68 5A 26 49 3E 49 67 5C 36 65 56 3C 70 52 56  ?hZ&I>Ig\6eV<pRV  
48 3C 3F 68 23 4D 6B 4E 5D 47 5D 77 4E 4F 46 60  H<?h#MkN]G]wNOF`  
2E 59 31 43 40 73 4C 46 69 6F 6A 3F 78 77 6D 61  .Y1C@sLFioj?xwma  
00  
)
```

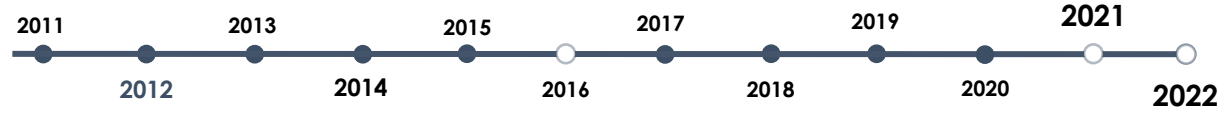
Tactics



- Checks keyboard(UA & RU)
- Checks VM agents
- Stops checking connection
- Removes support to .bit

```
POST /  
  
RC4(  
E4 07 33 44 36 43 34 42 30 42 46 36 45 30 42 38  ä.3D6C4B0BF6E0B8  
31 31 33 39 37 46 34 41 34 30 38 44 33 32 39 37  11397F4A408D3297  
43 36 37 43 42 41 45 38 43 45 00 54 45 53 54 2D  C67CBAE8CE.TEST-  
50 43 00 00 00 00 00 00 00 00 00 00 00 00 00  PC.....  
00 61 00 00 11 27 00 00 00 00 01 00 00 00 60 4C  .a...'.....`L  
21 4F 62 34 60 5F 4C 3A 76 74 25 7A 5E 72 50 2A  !0b4`_L:vt%z^rP*  
46 5D 3F 43 31 3D 6A 26 3E 51 5E 60 5D 50 36 60  F]?C1=j&>Q^`]P6`  
4C 60 52 30 26 64 3E 4D 35 3C 2B 2A 6D 2A 75 41  L`R0&d>M5<+*m*uA  
7A 31 4B 4D 75 76 5A 47 24 63 36 65 64 58 4A 5C  z1KMuvZG$c6edXJ\  
4D 31 2E 54 31 5A 59 5C 64 73 50 46 4B 70 57 4F  M1.T1ZY\dsPFKpW0  
...  
)
```


Tactics



- No major releases

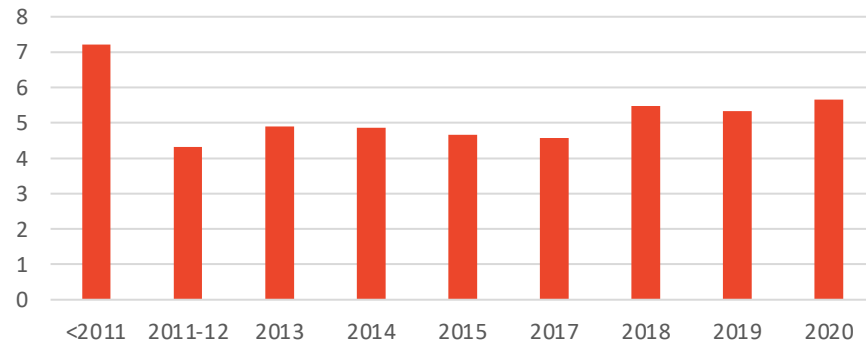
Tactics



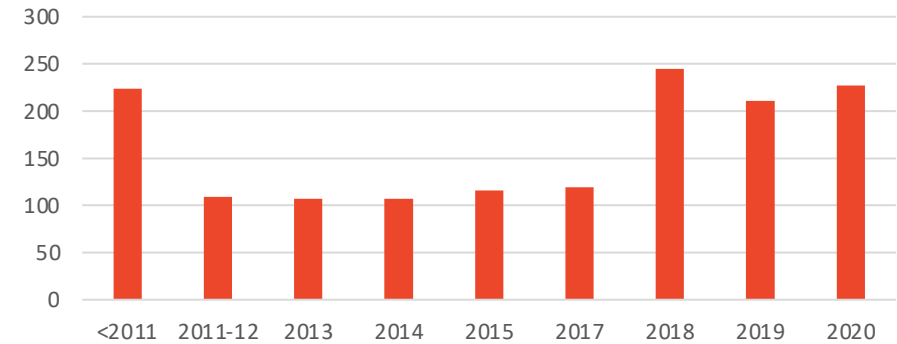
- No major releases

General Code Statistics

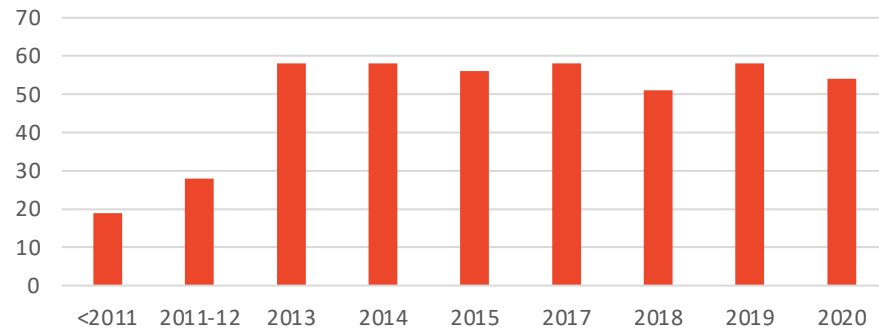
Complexity (AVG)



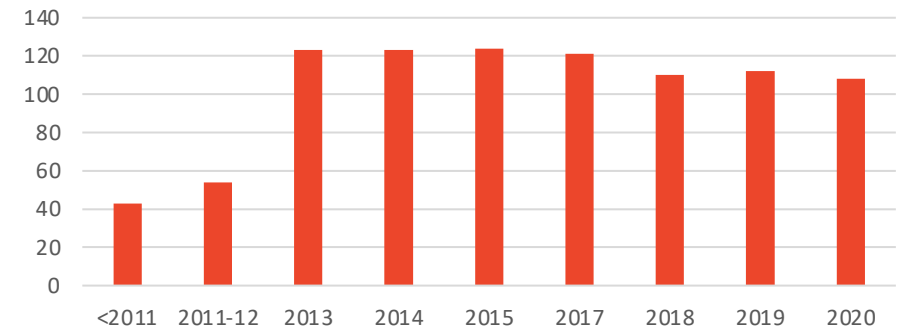
Basic Blocks (#)



Functions (#)

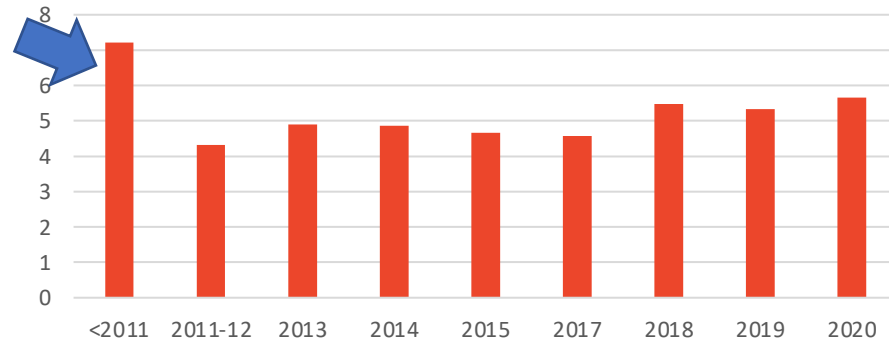


Imports (#)

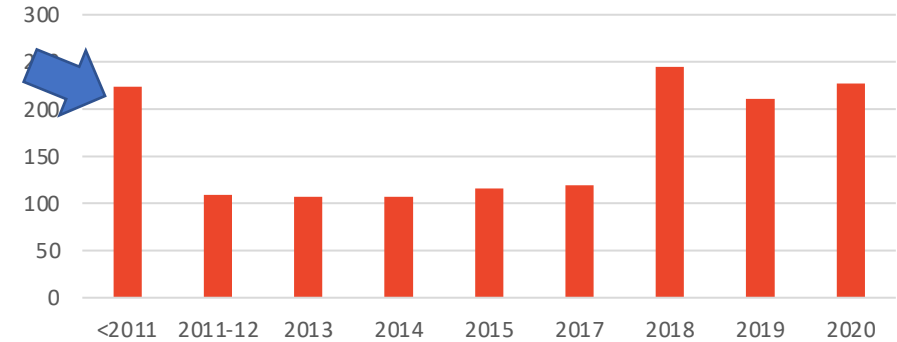


General Code Statistics

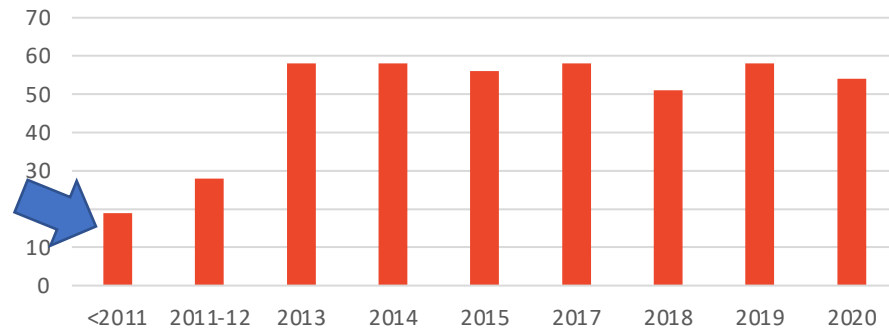
Complexity (AVG)



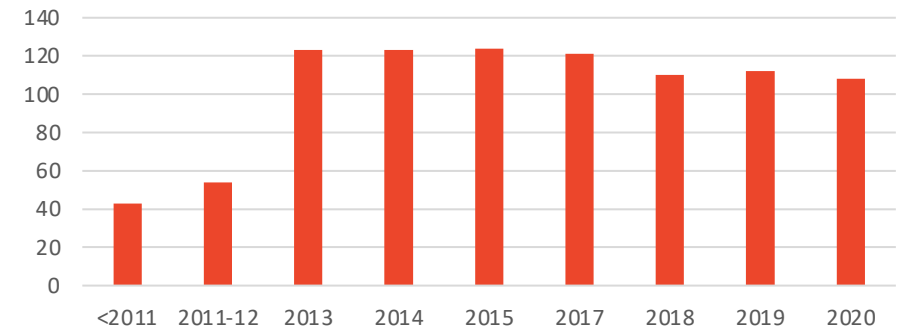
Basic Blocks (#)



Functions (#)

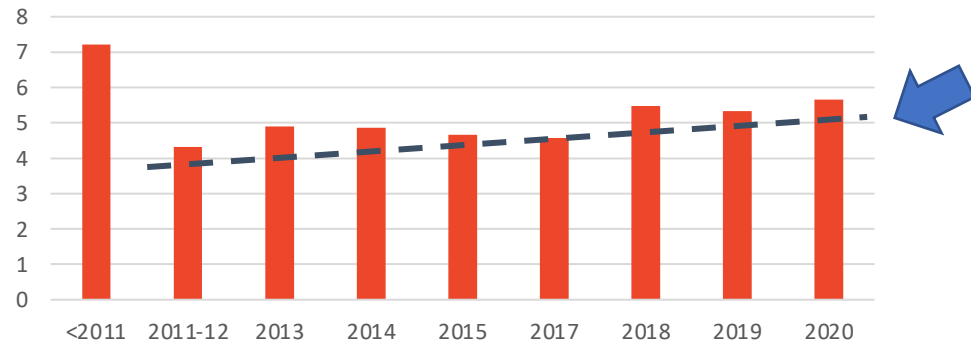


Imports (#)

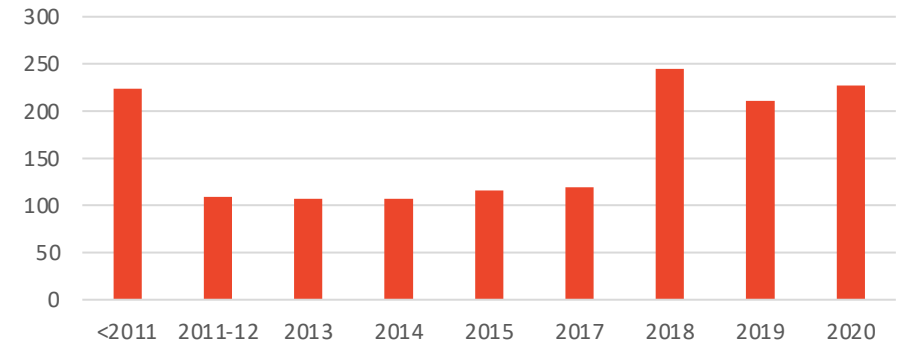


General Code Statistics

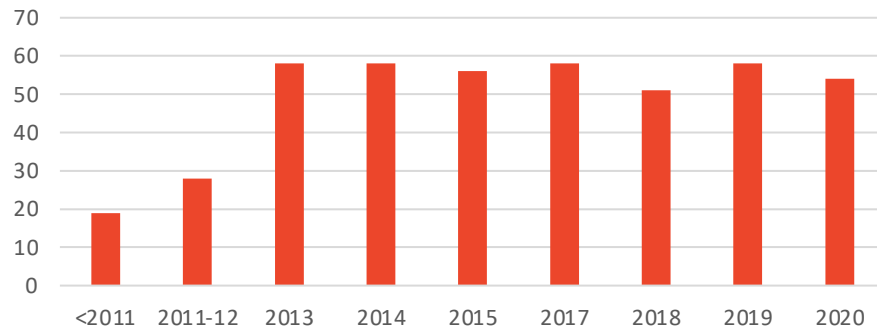
Complexity (AVG)



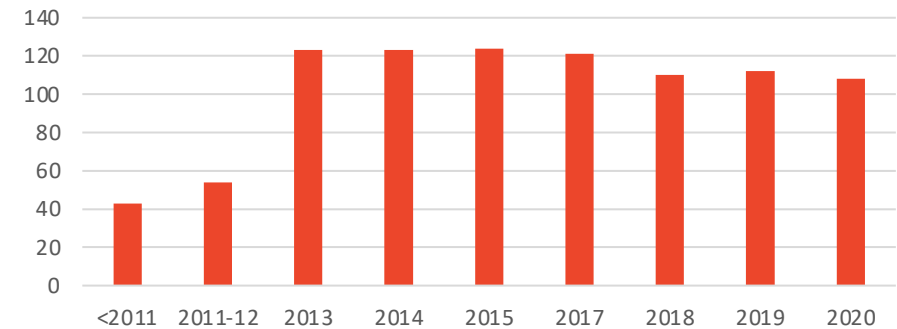
Basic Blocks (#)



Functions (#)

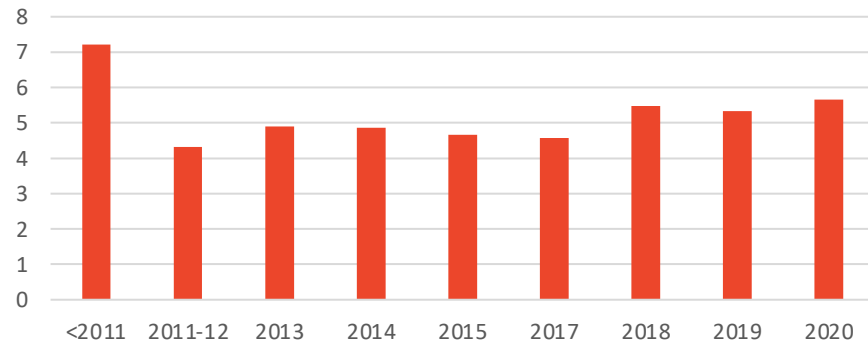


Imports (#)

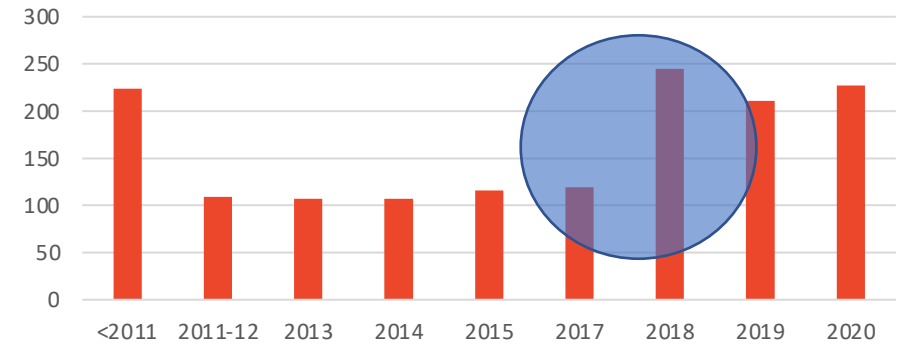


General Code Statistics

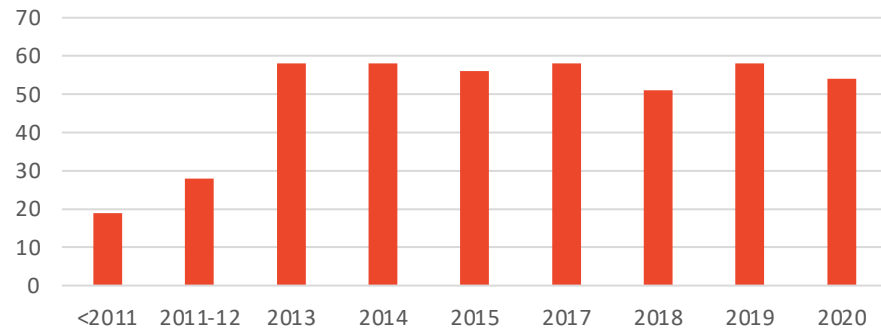
Complexity (AVG)



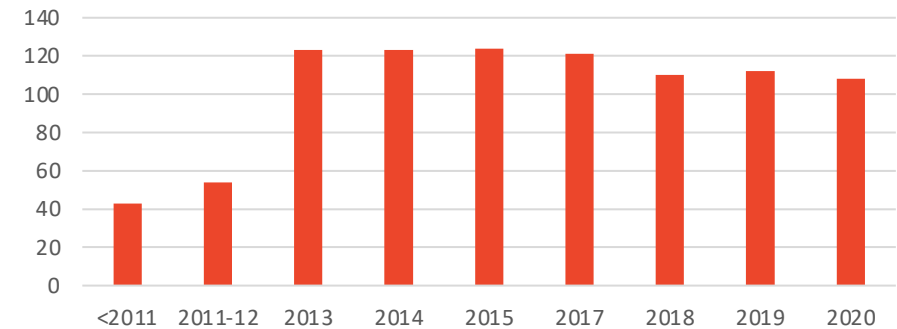
Basic Blocks (#)



Functions (#)



Imports (#)

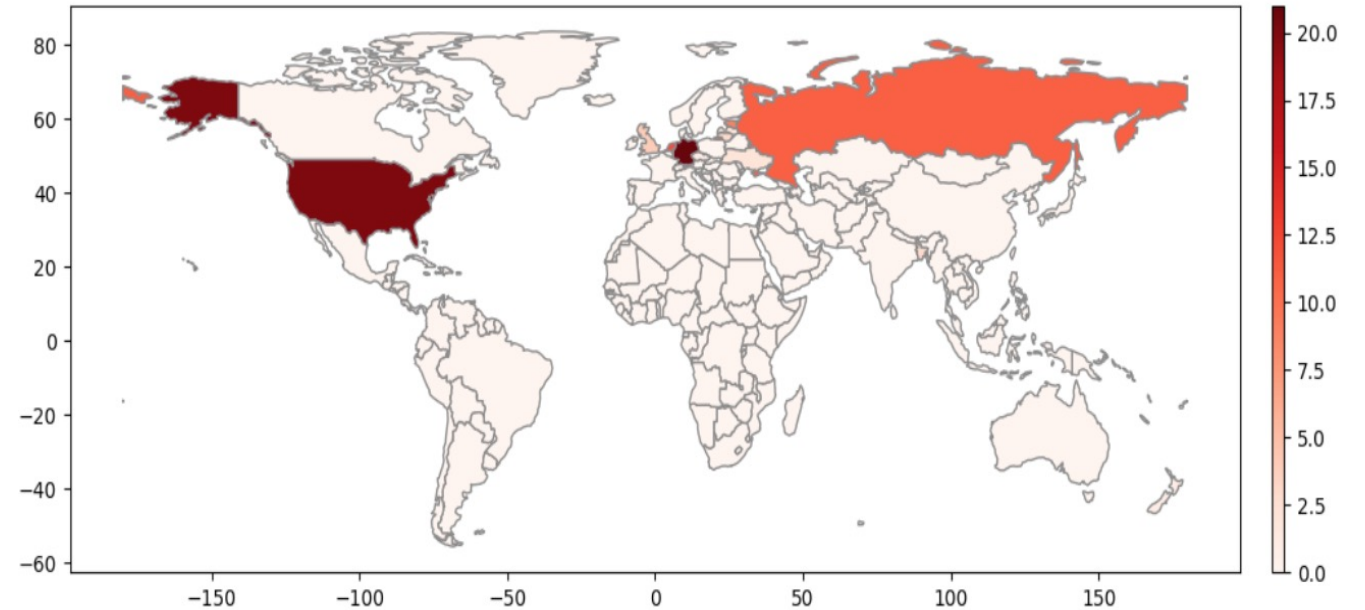


III. Data

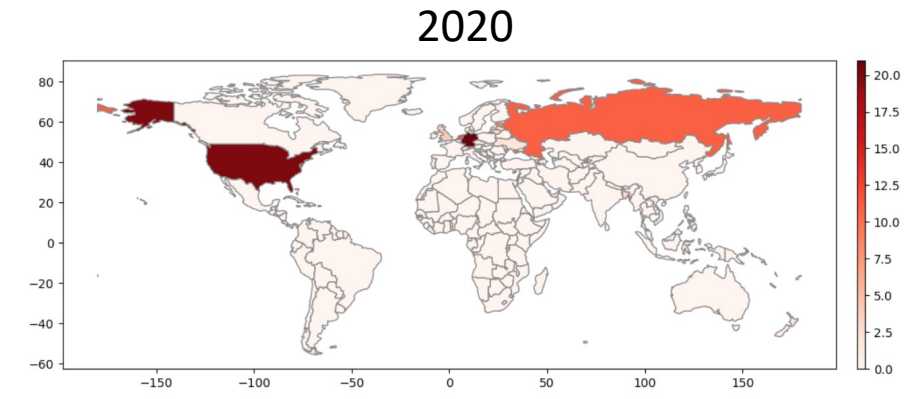
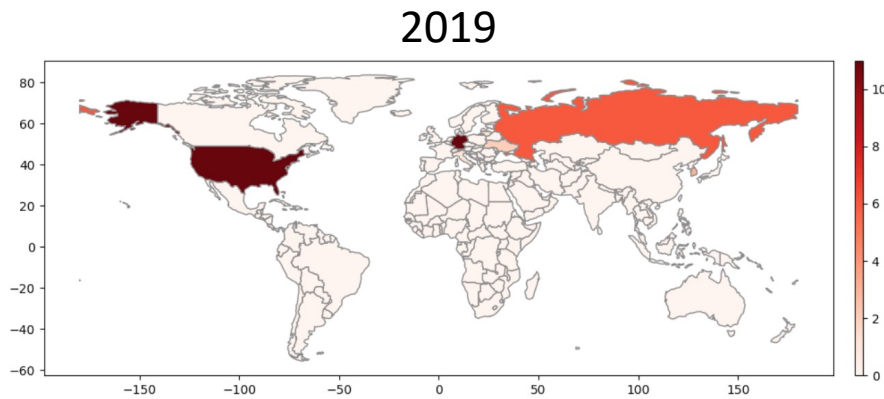
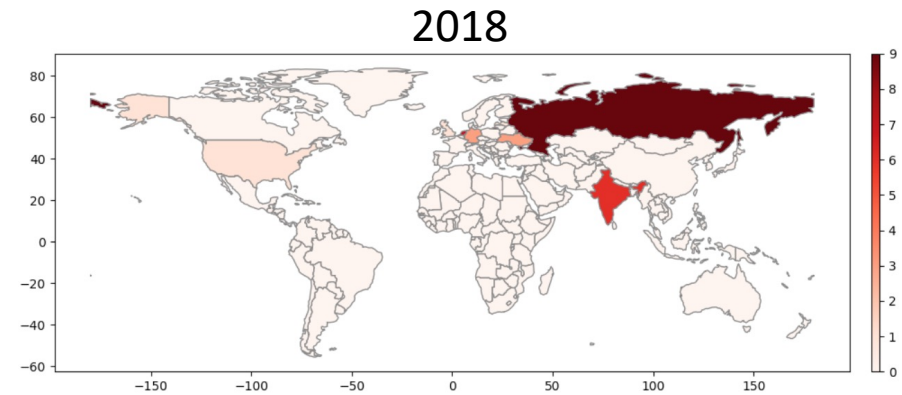
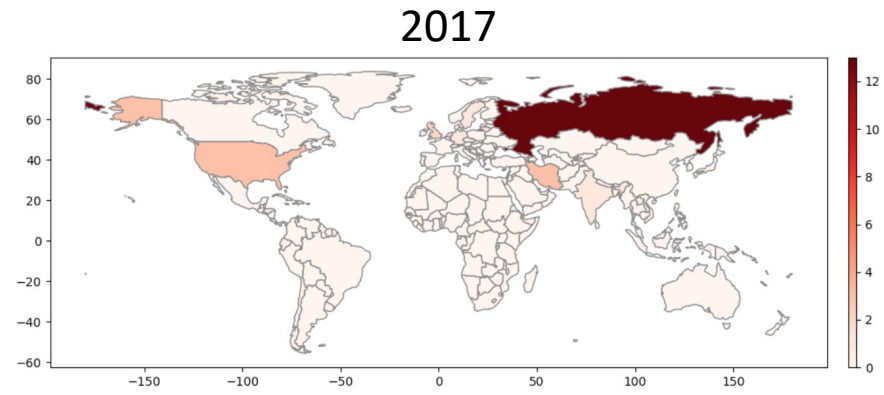
Infra-structure (2020)

- 98 unique domains
- 17 Countries

22	Germany
20	United States
12	Netherlands
11	Russia
8	Estonia
4	United Kingdom
3	Republic of Lithuania
3	France
3	Bulgaria
2	Ukraine
2	Latvia
2	Cyprus
1	United Arab Emirates
1	Singapore
1	New Zealand
1	Hong Kong
1	Czechia



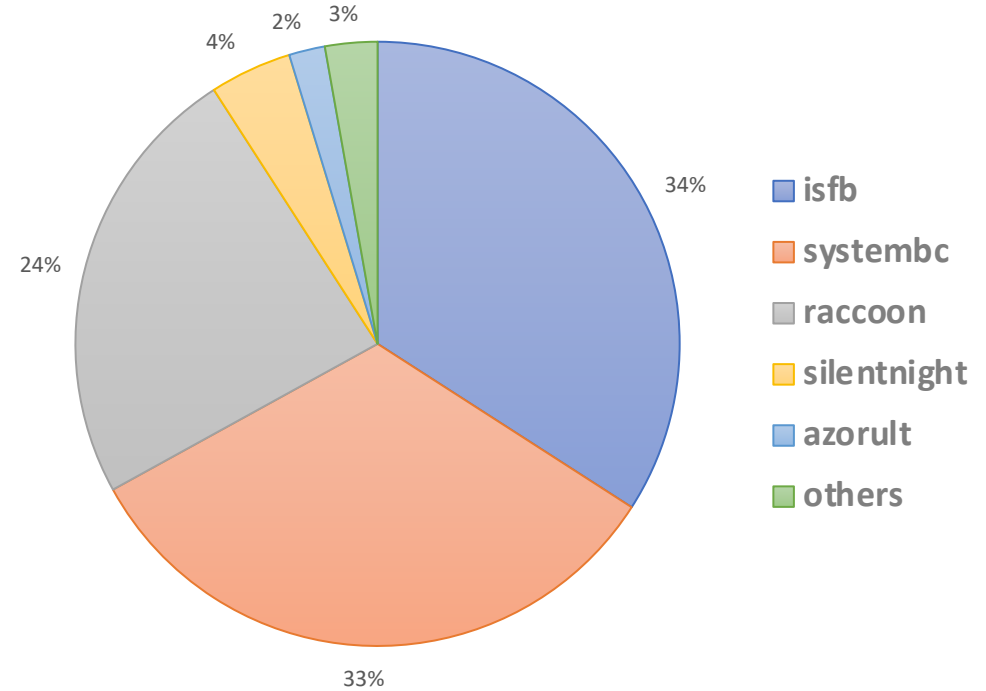
Infra-structure (2017 - 2020)



Payloads (2020)

- 14.113 unique files
- 4.312 configs
- 18 families

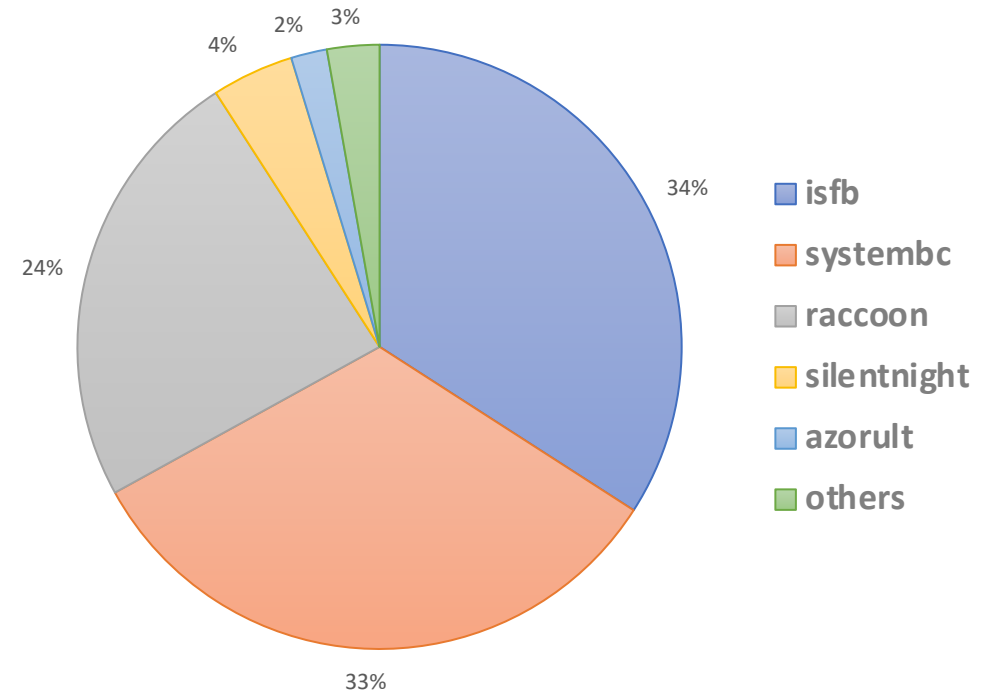
isfb	qakbot
systembc	dridex
raccoon	iceid
vidar	buer
silentnight	trickbot
azorult	danabot
osiris	netwire
photoloader	amadey
nymaim	smokeloader



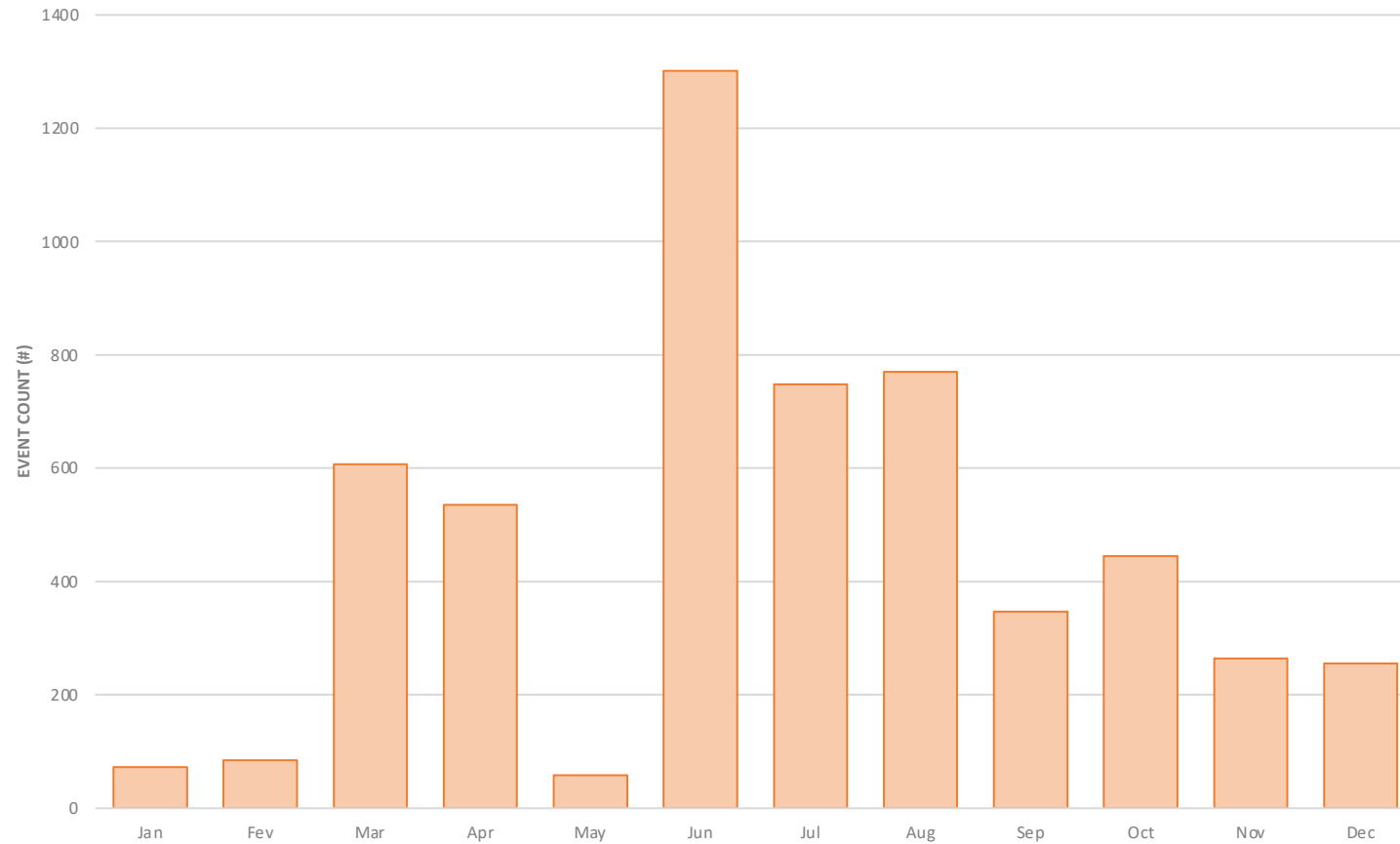
Payloads (2020)

- 14.113 unique files
- 4.312 configs
- 18 families

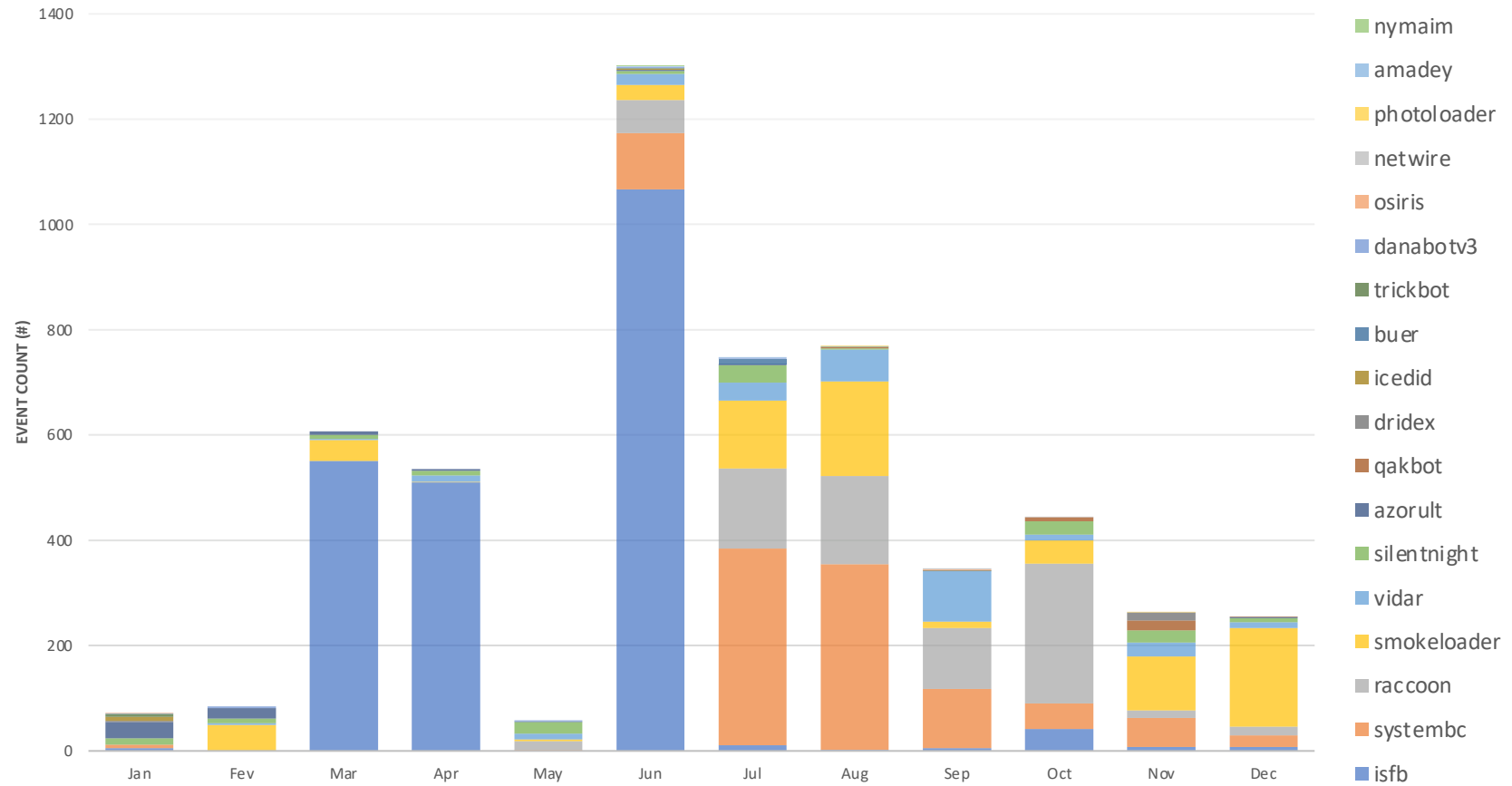
isfb	qakbot
systembc	dridex
raccoon	iceid
vidar	buer
silentnight	trickbot
azorult	danabot
osiris	netwire
photoloader	amadey
nymaim	smokeloader



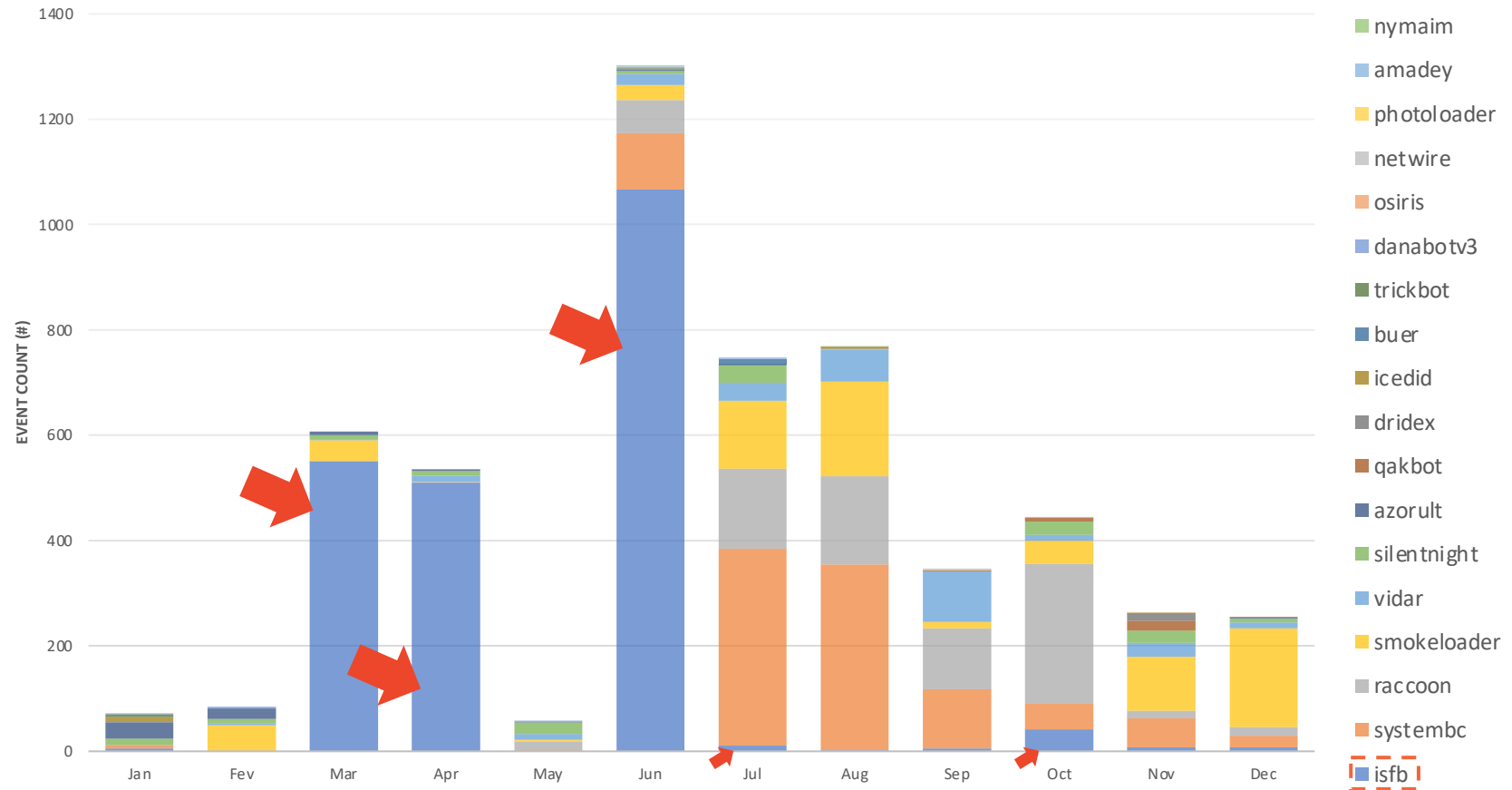
Payloads (2020)



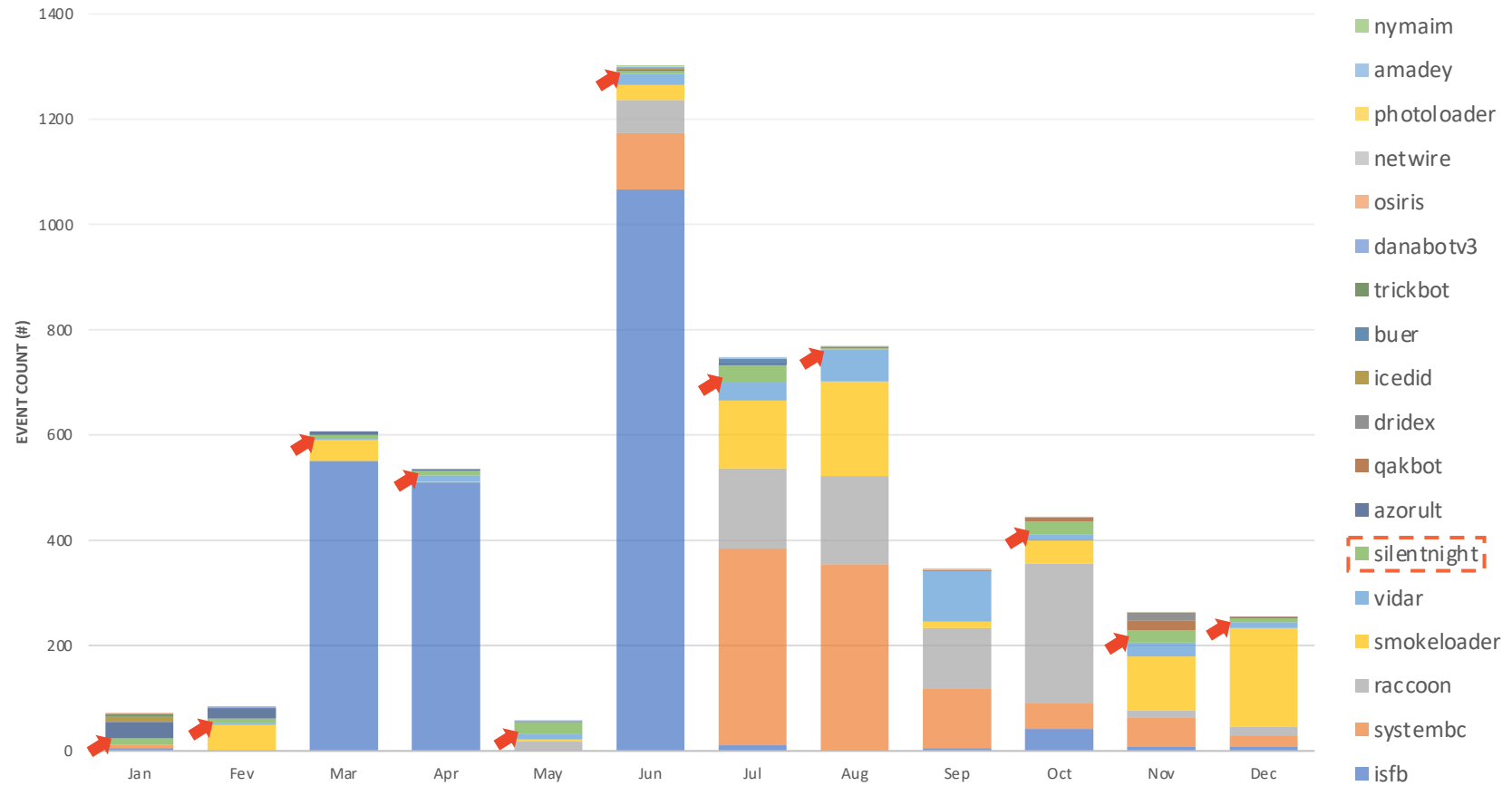
Payloads (2020)



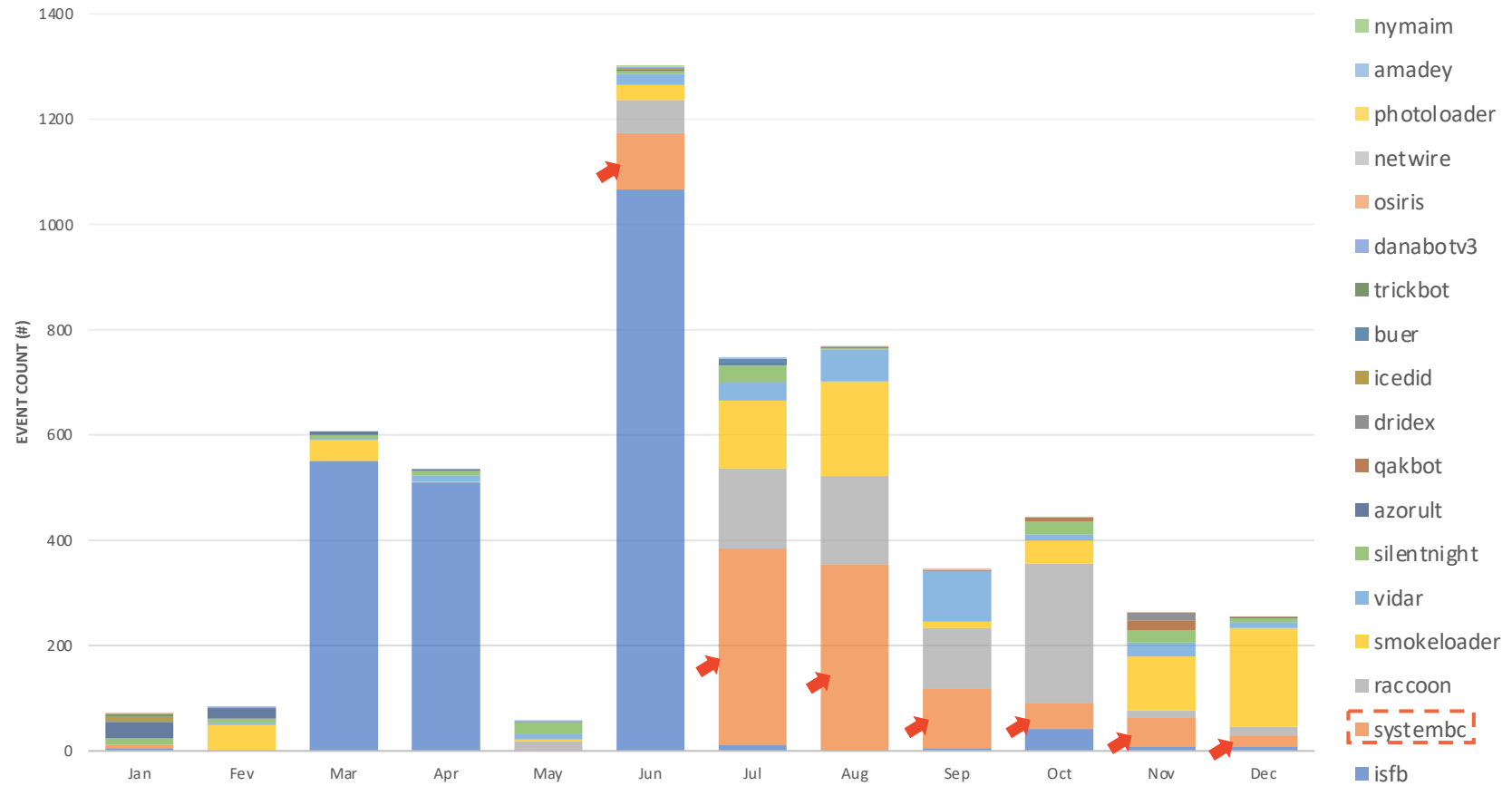
Payloads (2020) - ISFB



Payloads (2020) - Silentnight



Payloads (2020) - SystemBC



Takeaways

- Information about high-profile groups
- Connections among families
- Ransomware families
- International presence

Acknowledgements

- TAC Team
- TCR Team (@mandiant)

Thanks
@marcos_alvares