Different ways to cook a crab…..

Recipes presented by

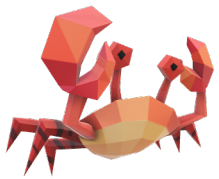
John Fokker McAfee
Alexandre Mundo McAfee

McAfee™
Together is power.

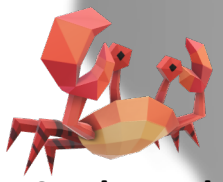
What to expect in our kitchen

- GandCrab Season
- Dissecting the Crab for edible parts and vaccines
- Hunting For Crab
- Finding the right recipe to cook the Crab
- Using the our Recipe for different Ransomware-as-a-Service (RaaS) families

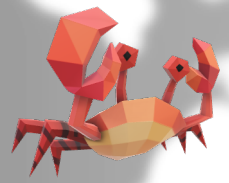
GandCrab Season



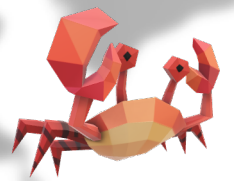
V1 released



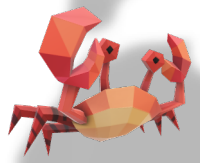
V2 released



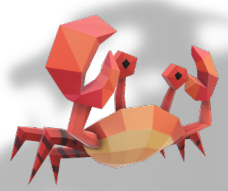
V3 released



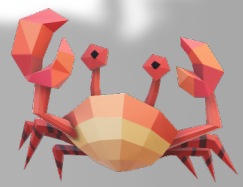
V4 released



V5 released



V5.1 released



V5.2 released

Gandcrab Retired

28 Jan 2018 | March 5 2018 | April 3 2018 | July 2018 | Sept 2018 | Dec 2018 | Feb 2019 | Mar 2019 | Apr 2019 | May 2019 | June 2019

Decryptor V1

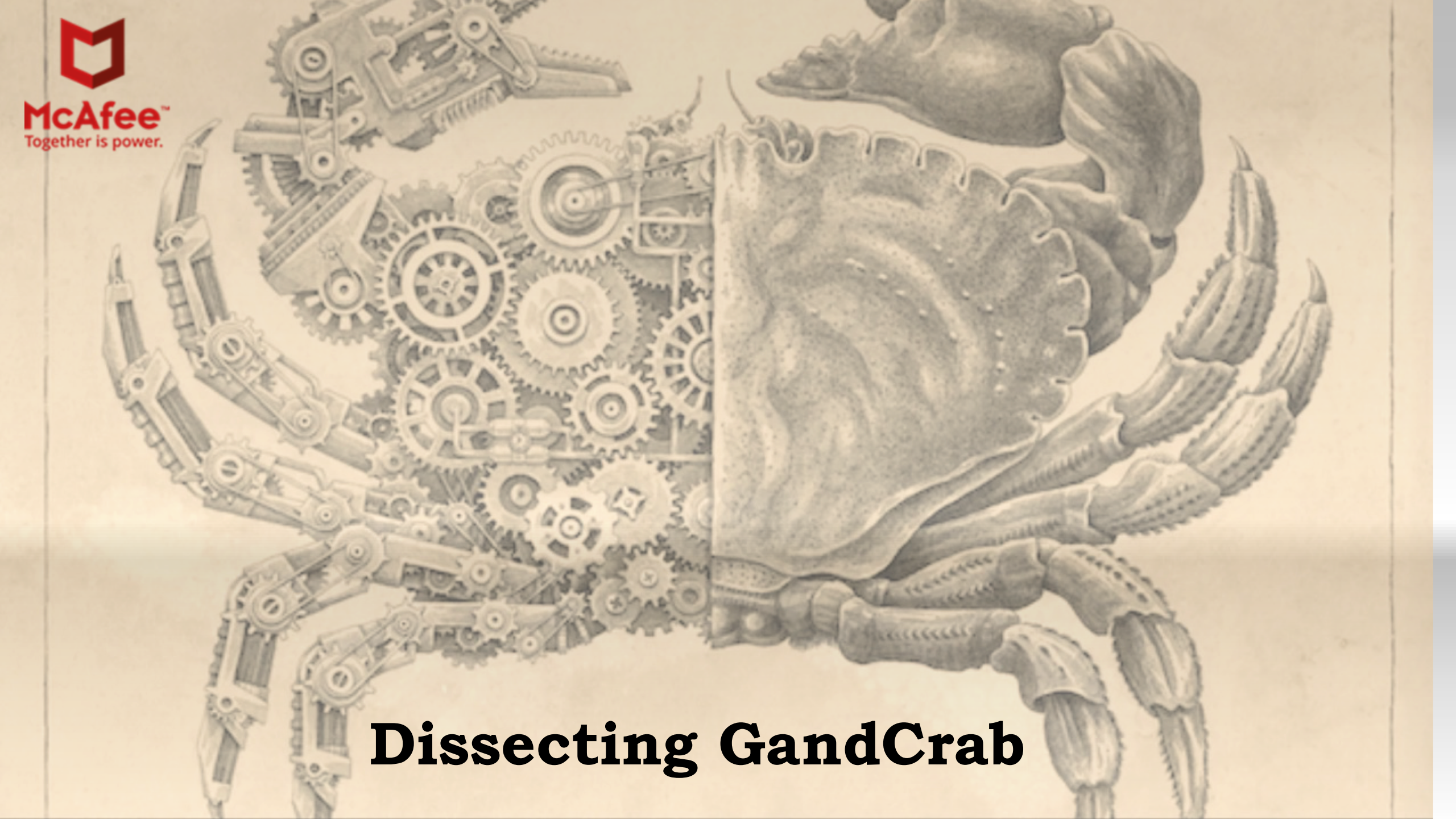
Vaccine 4.x

Vaccine 5.1

Vaccine 5.2

Decryptor V5.03 – v5.1

Decryptor V5.2



Dissecting GandCrab

Checks and Characteristics


```
mov     eax, [ebp+var_1C]
mov     [ebp+var_60], eax
mov     eax, [ebp+var_18]
mov     [ebp+var_44], eax
mov     eax, [ebp+var_14]
push    4                   ; flProtect
mov     [ebp+var_40], eax
mov     eax, [ebp+var_10]
push    3000h               ; flAllocationType
mov     [ebp+var_3C], eax
mov     eax, [ebp-0Ch]
push    114h                ; dwSize
mov     [ebp+var_38], eax
mov     eax, [ebp+var_4]
push    0                   ; lpAddress
mov     dword_417964, offset GandCrabGlobalExpand32ByteKStringForSalsa20 ; "expand 32-byte k\\"
mov     [ebp+var_70], 'apxe'
mov     [ebp+var_5C], '3 dn'
mov     [ebp+var_48], 'yb-2'
mov     [ebp+var_34], 'k et' ; expand 32-byte k
mov     [ebp+var_58], ecx
mov     [ebp+var_54], eax
mov     [ebp+var_50], 0
mov     [ebp+var_4C], 0
call    ds:VirtualAlloc ; reserve memory to keep the RSA1 decrypted blob
push    114h
push    eax
mov     edx, offset GandCrabRSA1KeyCryptedBlob
mov     pbData, eax
lea     ecx, [ebp+var_70]
call    GandCrabManageCryptotRSAXKeyBlob
add     esp, 8
mov     esp, ebp
pop     ebp
retn
```

- Focused on Versions 4 till 5.2
- ты говоришь по русски?
- Salsa 20 vs. AES

Checks and Characteristics

.ani	.msstyles
.cab	.msu
.cpl	.nomedia
.cur	.ocx
.diagcab	.prf
.diagpkg	.rom
.dll	.rtp
.drv	.scr
.lock	.shs
.hlp	.spl
.ldf	.sys
.icl	.theme
.icns	.themepack
.ico	.exe
.ics	.bat
.lnk	.cmd
.key	.gandcrab
.idx	.KRAB
.mod	.CRAB
.mpa	.zerophage_i_li
.msc	ke_your_pictur
.msp	es

- Skipping the following File extensions
- RSA to protect the Salsa20 KEY

Checks and Characteristics

- \ProgramData\
- \IETldCache\
- \Boot\
- \Program Files\
- \Tor Browser\
- \All Users\
- \Local Settings\
- \Windows\

- CSIDL_PROGRAM_FILESX86
- CSIDL_PROGRAM_FILES_COMMON
- CSIDL_WINDOWS
- CSIDL_LOCAL_APPDATA

```
_check_name_of_file_is_forbidden:       ; CODE XREF: GandCrabPrepareNameOfFileWithExtensionKRABAndIfCryptedRenamedWithIt+39
        mov     ecx, edi                ; lpString
        call    GandCrabCheckIfTheNameOfFileIsForbiddenToCrypt
        test    eax, eax
        jnz     short _release_memory_and_exit
        cmp     dword ptr [ebx+20h], 2
        jb      short _release_memory_and_exit
        mov     edx, [ebp+arg_0]
        mov     ecx, edi
        call    GandCrabCryptWithSalsa20TheFileAndSetEndOfFileTheSalsa20KeyAndNonceCryptedAndSizeOfOriginalFile
        test    eax, eax
        jz      short _release_memory_and_exit
        push    esi             ; lpNewFileName
        push    edi             ; lpExistingFileName
        call    ds:MoveFileW
```

- GandCrab doesn´t crypt files in particular folders to avoid destroy the OS or programs in it.
- The malware encrypts files in all folders that its found that are allowed.
- Change the extension of the crypted files with “.KRAB”.
- Delete the Volume Shadow copies.
- Sends information of the victim machine to a list of hardcoded domains.

cmd.exe /c vssadmin delete shadows /all /quiet

\wbem\wmic.exe shadowcopy delete

Building a Vaccine

- Total of 6 Vaccines
- The First most important Vaccine:
  - Registry key alteration
  - Binaries did run but didn't encrypt
  - Only a free GandCrab Wallpaper ;-)
- Public vaccine worked till version 5, <u>almost 6 months!!</u>

Building a Vaccine


```
loc_401070:                             ; CODE XREF: sub_401000+6C↑j
                push    offset szWindow ; lpszWindow
                push    offset szClass  ; "AnaLab_sucks"
                push    0               ; hWndChildAfter
                push    0               ; hWndParent
                call    ds:FindWindowExW
                test    eax, eax
                jz      short loc_401062
                lea     ecx, [ebp+dwProcessId]
                mov     [ebp+dwProcessId], 0
                push    ecx             ; lpdwProcessId
                push    eax             ; hWnd
                call    ds:GetWindowThreadProcessId
                test    eax, eax
                jz      short loc_401062
                push    [ebp+dwProcessId] ; dwProcessId
                push    0               ; bInheritHandle
                push    1FFFFFh         ; dwDesiredAccess
                call    ds:OpenProcess
                test    eax, eax
                jz      short loc_401062
                push    0               ; uExitCode
                push    eax             ; hProcess
                call    ds:TerminateProcess
                jmp     short loc_401062
; ---------------------------------------------------------------------------
```

Version 5 vaccine

- Hidden Window, Persistent Atom to prevent re-encryption
- Mutex name based vaccine
  - Changed several times

Victim Info

- pc_user — Name of the user logged into the machine.
- pc_name — Name of the endpoint infected.
- pc_group — Name of the domain or workgroup of the endpoint.
- AV — Name or names of antivirus products in the endpoint.
- pc_lang — Name of the language or languages of the endpoint.
- pc_keyb — The type of keyboard on the endpoint.
- os_major — The name of the operating system of the endpoint.
- os_bit — The type of CPU of the infected endpoint.
- ransom_id — Unique value for the victim for the ransom note and Onion webpage to pay.
- hdd — Information about the logic units.
- ip — The IP address of the endpoint.

```
---BEGIN PC DATA---
7ftDEgLb/ZS0lcmZbHM61LLJ1QOTD4IKuw6xbpUgQnYNWIoC9J+YYFdxDmCD9MvJNZDUAomVouDKRWHIRHQ
NdA2g0Gq6ADOZFiiPaB4YmV7F5Z/vMAd2+gBv2sJ3GUw17wtxXWKEyuIWo52tHNXKnMJ+BjlCwejeop1qwn
SzGziqAtoTPF/Z3VPDKxsCgRudjoIlpS6naVnumkqGtvabx0rqIyyy9y1Y6lMDmQ7q94Aew4gTmwMkzYb5U
GV+bDWEZysRLSXnNiaPkJ9b5I0tVGYczXSjaI=
---END PC DATA---
```

Hardcoded values as growth indicator

- id The affiliate id number.
- sub_id The sub id of the affiliate id.
- version The internal version number of the malware. In the example below, it is "4.0" but the last version would have shown "5.2".

Crab hunting season is now officially open….

Crab Hunting with yara

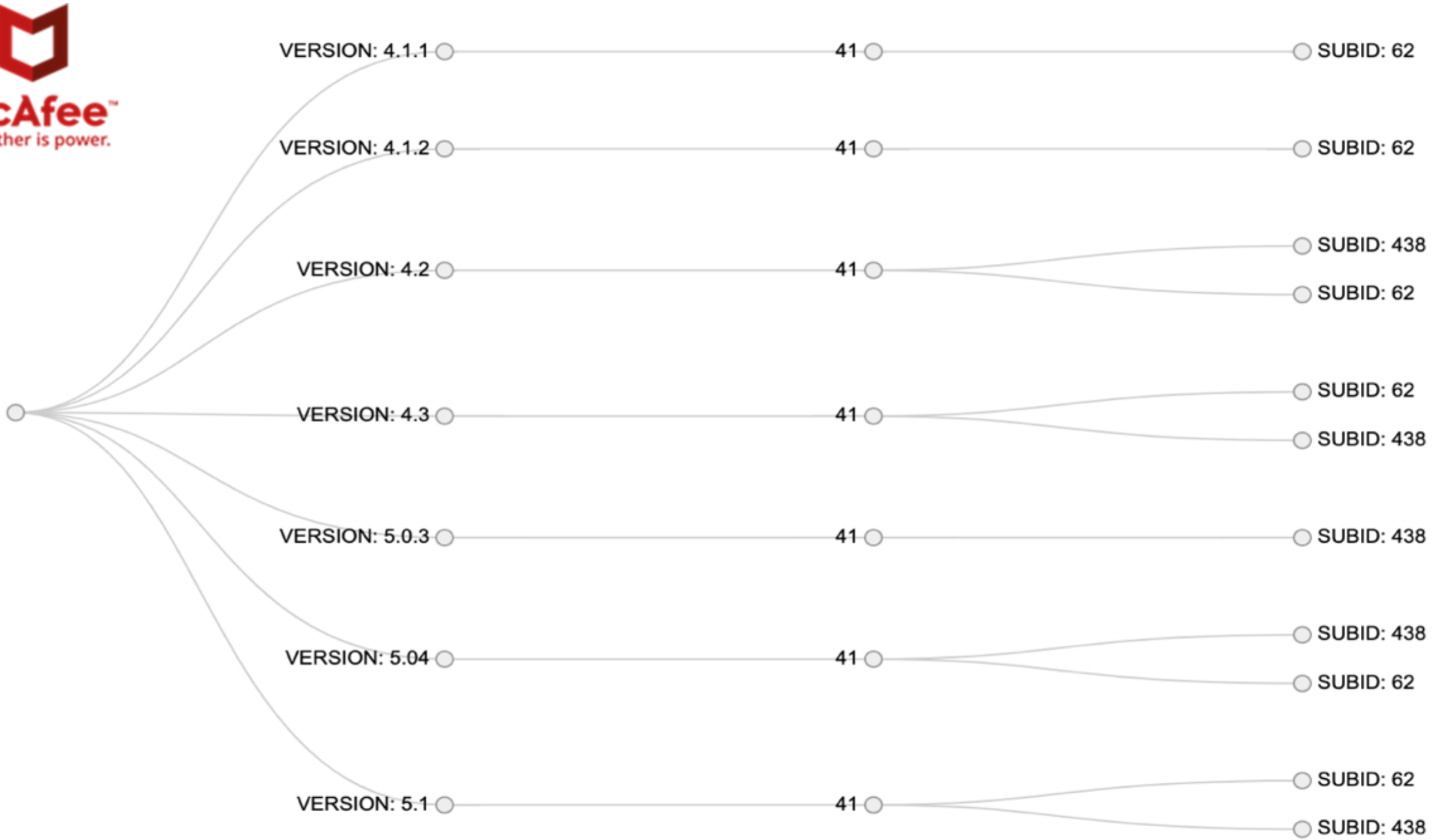
McAfee
Together is power.

yara

Combined with custom tooling turned out to be a perfect net

But how do we cook a good Crab?

2018-06-29	VERSION: 4.0	117	SUBID: 397	8d604e3c567aab3c8cfa2d2c424c09c4	EXE
2018-06-30	VERSION: 4.0	9	SUBID: 9	cbdb4aebbb984096ee54c9eb2b1c128c	EXE
2018-06-30	VERSION: 4.0	15	SUBID: 15	9be5102484d60f074499a8fd4403819c	EXE
2018-06-30	VERSION: 4.0	15	SUBID: 15	77a7573a20dbf141a0ff1e5fade2eae0	EXE
2018-06-30	VERSION: 4.0	41	SUBID: 62	19aa2a0f61f8b928b44de28d16f31174	EXE
2018-07-03	VERSION: 4.1	9	SUBID: 9	946aa4b8273be8d4984e14d6c8c9d3b4	EXE
2018-07-03	VERSION: 4.1	15	SUBID: 15	86613ae664b74c3a464f473408352635	EXE
2018-07-03	VERSION: 4.1	44	SUBID: 83	3eed6f11720e53756db16de1b9a8d561	EXE
2018-07-03	VERSION: 4.1	106	SUBID: 363	b6d06a87b35d15a1b3d9d76aced96f4e	EXE
2018-07-03	VERSION: 4.1	114	SUBID: 383	7fd94b59280d80bcfdd1b3970c4189ed	EXE
2018-07-04	VERSION: 4.1	15	SUBID: 15	fd602a6ae269d8fbc3b2c996678825b7	EXE
2018-07-04	VERSION: 4.1	95	SUBID: 331	2212fac7fcded7f06042d0a0ca67898f	EXE
2018-07-04	VERSION: 4.1	100	SUBID: 411	903f8718a1c3c12042fc44bac6a4c786	EXE
2018-07-04	VERSION: 4.1	106	SUBID: 363	c24b3cf9336e7e994625d223fa7b5f4f	EXE
2018-07-04	VERSION: 4.1	122	SUBID: 403	340117038ae2ef8d07c90c614d652934	EXE
2018-07-05	VERSION: 4.1	110	SUBID: 374	9a680a7ff23746d92f4bb274c50be4a5	DLL
2018-07-05	VERSION: 4.1.1	41	SUBID: 62	24fdd71ded0b9ffecfe3387002f7d361	EXE
2018-07-05	VERSION: 4.1.1	73	SUBID: 414	ef50f5c2d6d8d10d8adc1efb840518d0	EXE
2018-07-05	VERSION: 4.1.1	99	SUBID: 386	cce23a33a5a78b24ef7f5ced7d715d95	EXE
2018-07-05	VERSION: 4.1.1	99	SUBID: 386	f876735f6d4f076dfb148c63c4ba5a3a	EXE
2018-07-05	VERSION: 4.1.1	99	SUBID: 386	9b785e93d9ce42f6213d2c2a1ecc8293	EXE
2018-07-05	VERSION: 4.1.1	99	SUBID: 417	c6b0fbf5190d3850b212c53e6ed56886	EXE
2018-07-05	VERSION: 4.1.1	99	SUBID: 417	9c973702f8b40793c3ab60329dad7263	EXE
2018-07-05	VERSION: 4.1.1	99	SUBID: 417	62fd133df8be543900aabe64b707896b	EXE
2018-07-05	VERSION: 4.1.1	124	SUBID: 413	a74c335c0ee5958929b99cb14726cd9a	EXE
2018-07-05	VERSION: 4.1.1	128	SUBID: 423	e8e19525aa73d1714f15552d166aaa84	EXE
2018-07-06	VERSION: 4.1.1	111	SUBID: 375	6b8872624f0427deaf8df292038e657a	DLL
2018-07-13	VERSION: 4.1.2	41	SUBID: 62	75f215c1f086c47ee45392bd188909d0	EXE
2018-07-13	VERSION: 4.1.2	57	SUBID: 133	0301296543c91492d49847ae636857a4	EXE
2018-07-13	VERSION: 4.1.2	57	SUBID: 133	2aad5ce883a44154e7d7a9d982bb286c	EXE
2018-07-13	VERSION: 4.1.3	57	SUBID: 133	3cef3301e48135dc3159181aa500bfe8	EXE
2018-07-19	VERSION: 4.1.2	15	SUBID: 15	5c3bed3feaea533d2eb537850aa7079c	EXE
2018-07-19	VERSION: 4.1.2	15	SUBID: 15	b8381b2b78d8e4088aca4f3c1535fea2	EXE
2018-07-19	VERSION: 4.1.2	41	SUBID: 62	2d617c60478949d900cf37d3dfaf527a	EXE
2018-07-19	VERSION: 4.1.2	79	SUBID: 250	9ec04ede383aad5a6774696a361d515b	EXE
2018-07-19	VERSION: 4.2	41	SUBID: 438	2f09d9e81aa3c7ff0437625f976510ca	EXE
2018-07-19	VERSION: 4.2	41	SUBID: 62	38a803baf56ec45e8b7db3ce610afac2	EXE
2018-07-19	VERSION: 4.2	79	SUBID: 250	0b216cdb07d901c41514a7baabfbf055	EXE
2018-07-19	VERSION: 4.2	95	SUBID: 332	0d97b152305de1324901dbeebe644506	EXE
2018-07-19	VERSION: 4.2	99	SUBID: 448	2c79b1c6565616109cd38bd13e1b6019	EXE
2018-07-19	VERSION: 4.2	99	SUBID: 448	4893880bce579d21085eacea2f6d2b8e	EXE
2018-07-19	VERSION: 4.2	131	SUBID: 432	9f59740a5d45cf545e2fd591b9ba0428	EXE
2018-07-19	VERSION: 4.2	136	SUBID: 443	3b74163ebab14e3736424a4d83077bf7	EXE
2018-07-31	VERSION: 4.2.1	128	SUBID: 453	451394162783f2662924dbc01c8cc963	EXE


VERSION: 4.1.1
41
SUBID: 62
VERSION: 4.1.2
41
SUBID: 62
VERSION: 4.2
41
SUBID: 438
SUBID: 62
VERSION: 4.3
41
SUBID: 62
SUBID: 438
VERSION: 5.0.3
41
SUBID: 438
VERSION: 5.04
41
SUBID: 438
SUBID: 62
VERSION: 5.1
41
SUBID: 62
SUBID: 438

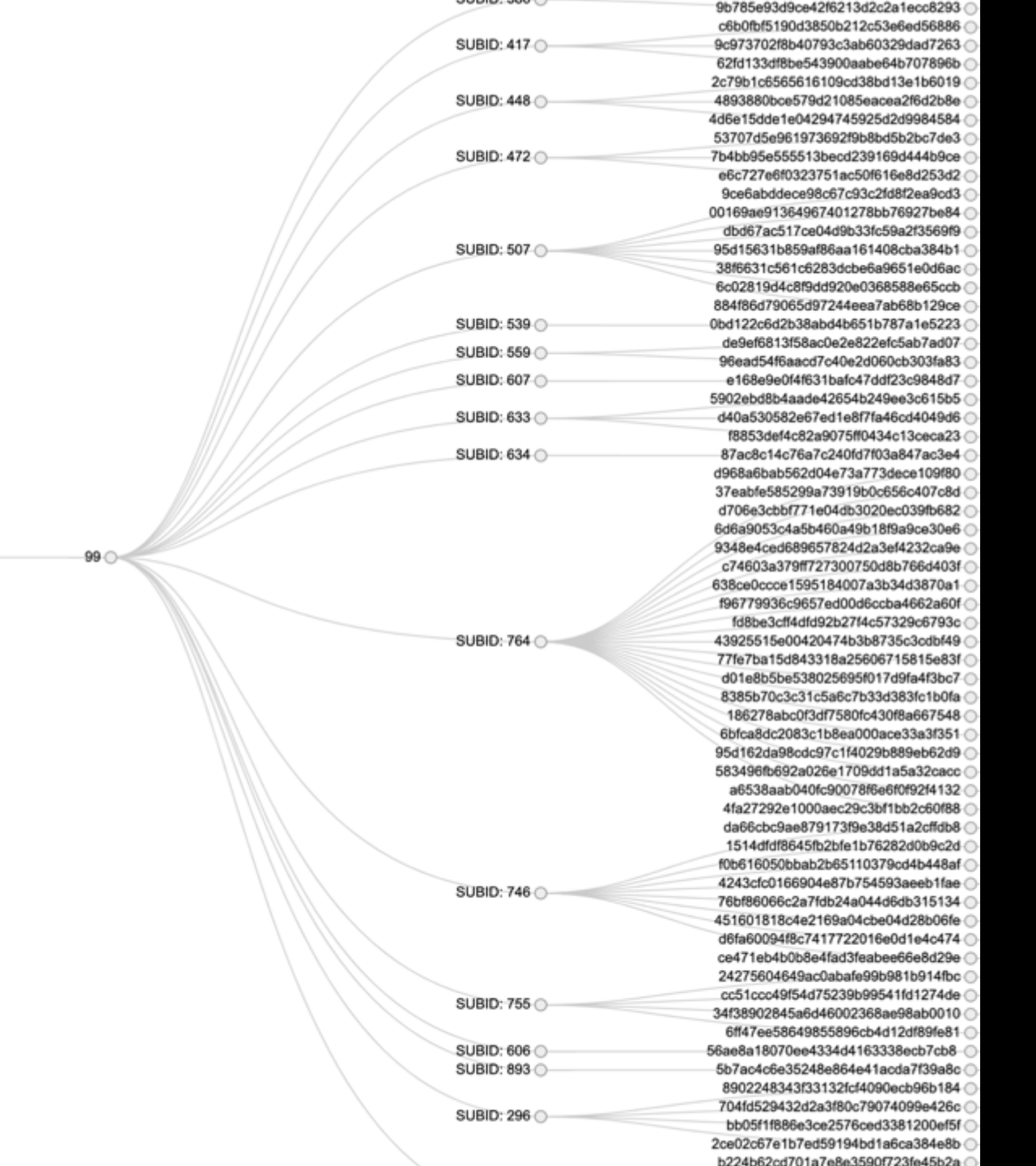
McAfee™
Together is power.

Mixing the ingredients together

McAfee
Together is power.

Meet nr 99
The most active Gandcrab Affiliate

15,41,170 are other top affiliate numbers



GandCrab Version 5.2, Feb 2019;

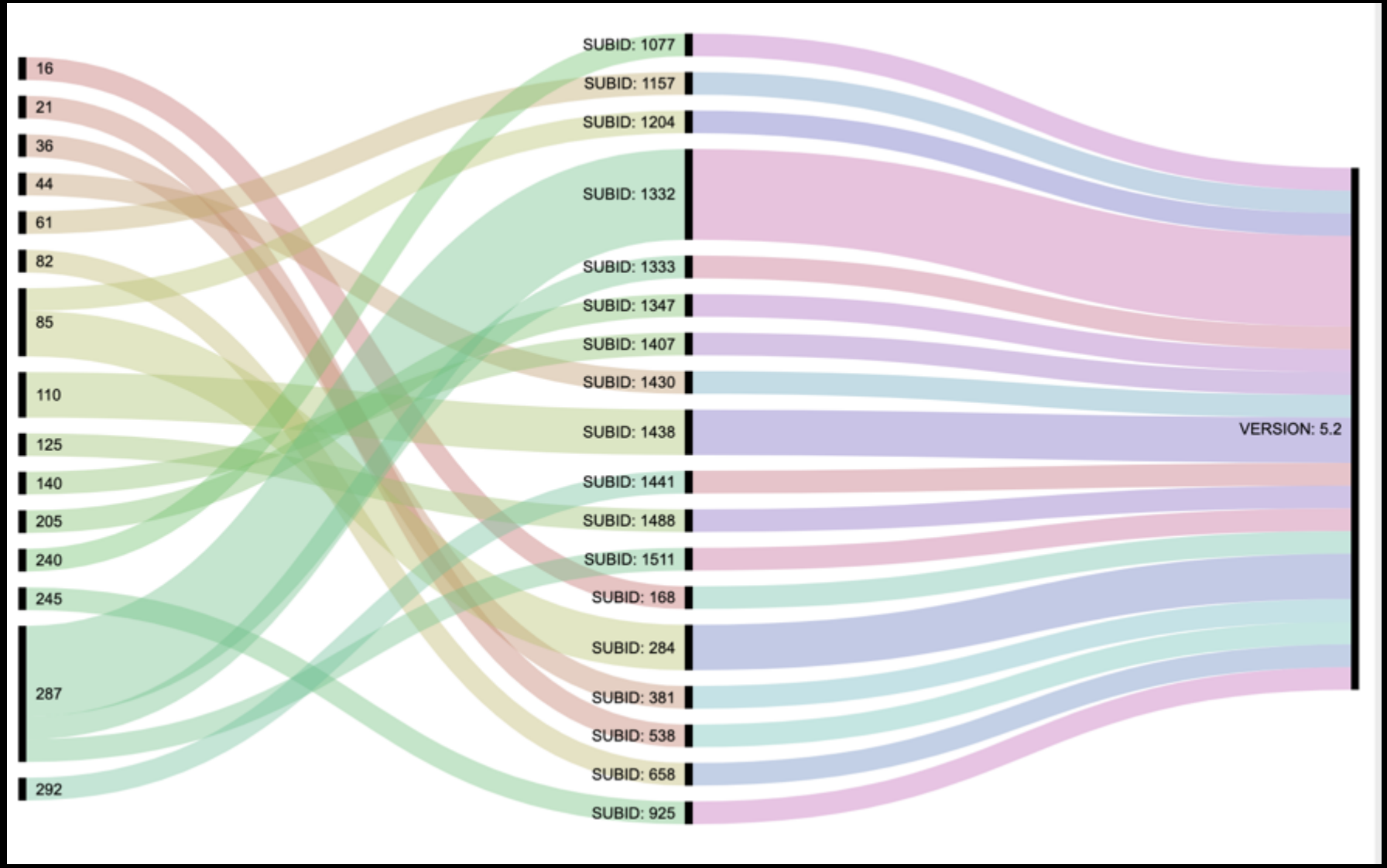
The big Affiliates left the party early.

Was there another party?

Or were numbers

15, 41,99,170

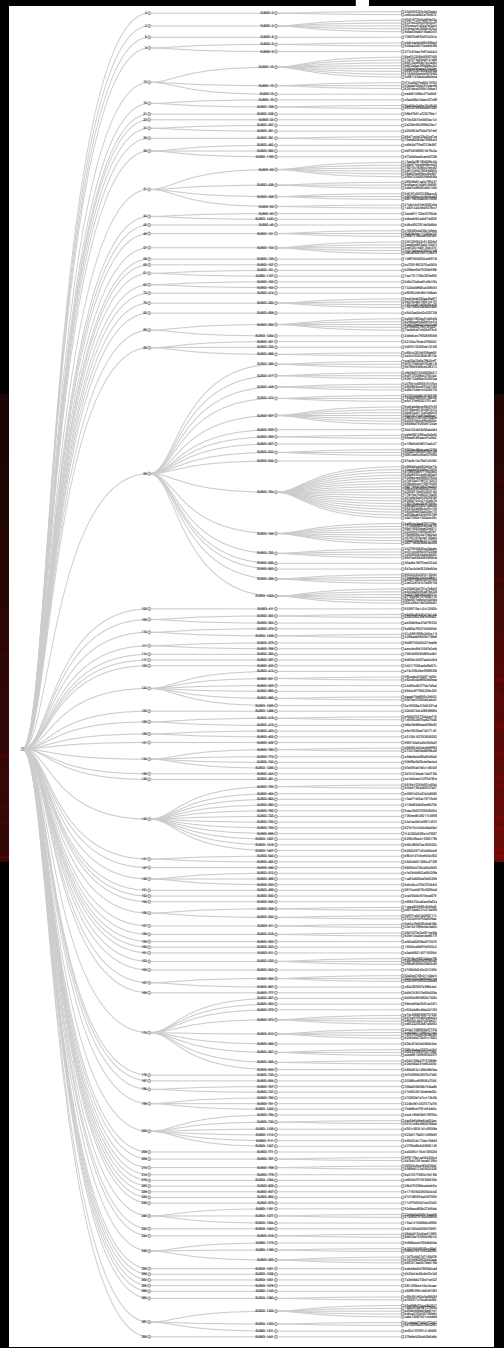
ready for bed?



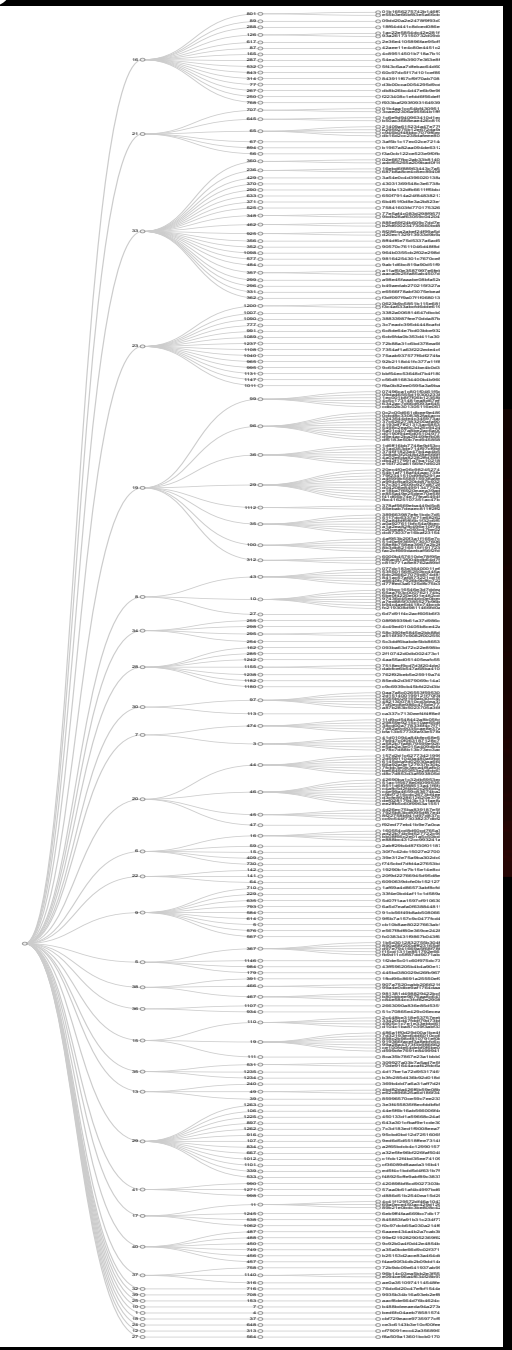
Using our recipe for a different RaaS

McAfee
Together is power.

Gandcrab
Affiliate Structure



REvil
Affiliate structure



Sodinokibi research Blog

Was the similarity a coincidence?

UNKN
byte

Seller
12 posts
Registration
04.07.2019 (ID: 94 090)

Posted: 4th of July

A complaint

Due to the fact that we are expanding activity, we invite adverts by:

- Spam
- Dedikam and networks;
- Doorway traffic and other living things;

We work in a private mode. Limited number of seats.
Get ready for an interview and show your evidence of the quality of the installations. We are not a test site, and the "learners" and "I will try / I will try" there is nothing to do. We have been working for several years, the topic is more than 5 years.
The software is fully operational and ready to go.

Excerpt from the rules:

1. It is forbidden to work in the CIS (including Ukraine);
2. Starting rate from 60% in your direction. After the first 3 payments - 70%.

Short description of the software: **private ransomware written in pure C, using inline-assembler with the possibility of modifying functionality out of the box according to the RaaS business model.**
The software has statistics, a payment page and "trial decoders" on the payment page. No school emails. More information can be obtained during the interview.
The first contact in the PM.

+ Quote

~~Lalartu~~
b376ded0 crc32

~~Deactivated~~
1,281 publications
Registration
12/14/2017 (ID: 84 236)
Activities
other

Posted: 4th of July

I work with these nice young people, very nice, very.

I switched to them after the crab, what I tell you, the crab was worse, then my envelope not only grew, it broke through the ceiling and grows further. And this is thanks to the fact that people are not being recruited here if only they were, builds are cleaner, sometimes they are missed with closed eyes, sweetie.

I welcome you to this forum ❤

+ Quote

Fooling the Crab

Social Engineer a Decryption

Things we learned:

Agile (Malware) coding has a higher chance of exploitable mistakes
Investigate a RaaS as a Business and look for the administration

Hard coded ID number analysis helps find:
- Key Affiliates
- Early insights in RaaS changes
- Potential disruption targets
- Provide distribution insights
- Chain of Custody (Victim-Sample-Affiliate)

It is up to us (SEC industry) to go step further in the analysis, LEA doesn't always have that option but are faced with the same problem….

BON APPÉTIT!

John Fokker @john_fokker
Alexandre Mundo @ValthekOn

McAfee™
Together is power.