



Qbot Code Evolution

Deep Malware Analysis and Intelligence

Who are we?

Carlos Rubio Ricote

Malware reverse engineer

Currently at: Threatray

Formerly: Blueliv, S21sec, Panda Security...

Blog: <http://reversingminds-blog.logdown.com/>



Markel Picado Ortiz (d00rt)

Malware reverse engineer

Currently at: Threatray

Formerly: Sophos, Hatching (tria.ge), Panda Security, S21Sec...

Twitter: @D00RT_RM

Github: <https://github.com/d00rt>

Blog: <https://d00rt.blogspot.com/>

Intro

Index

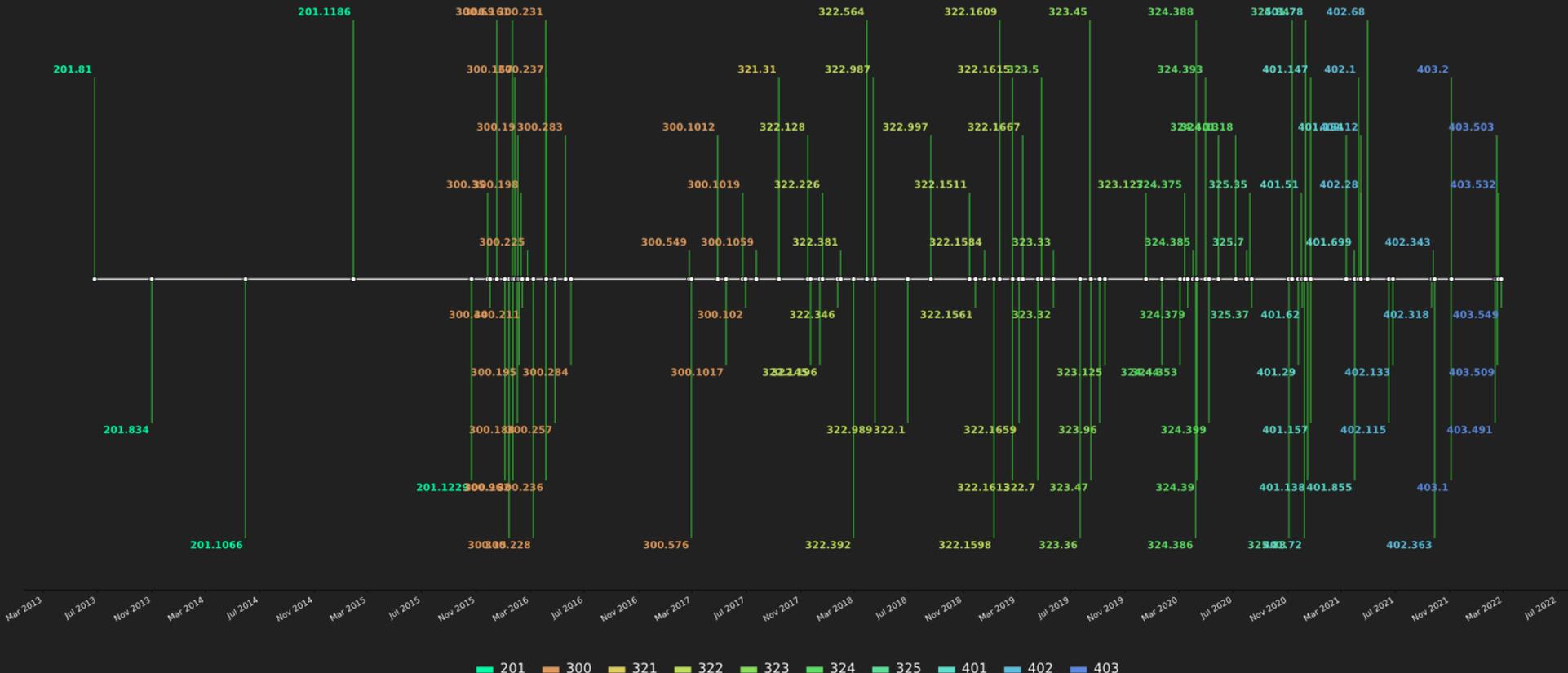
Table of contents

- Brief introduction to Qbot
- Technical summary of Qbot
- Qbot code evolution
- Converting metadata into insights
- Conclusion

What is Qbot?

- Historically known as a banking trojan / credential harvester
- Active since 2007
- Modular framework
- Currently one of the most prevalent malware (Distributed by TA551, TA570, TA571, TA577...)
- Continuous development

Qbot Version Timeline (2013-2022)

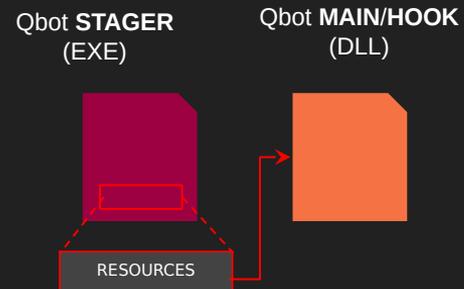


What is Qbot?

(tech view)

- Historically composed by 2 elements
 - **STAGER** (exe)
 - **MAIN DLL** (dll)

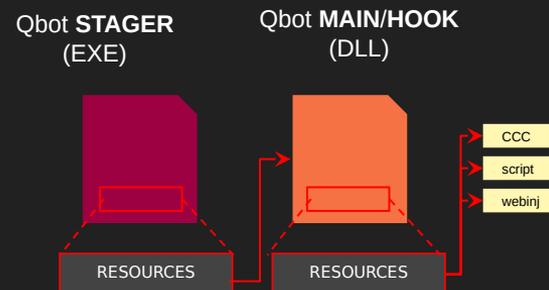
- **MAIN DLL** is embedded into stager's resources



- **STAGER** goals
 - Installation
 - Persistence
 - Main DLL injection

- **MAIN DLL** also has artifacts in its resources
 - CC config
 - Script for malware updates
 - Antisession Webinjects

- **MAIN DLL goals**
 - Network traffic interception
 - Steal credentials
 - Lateral movements
 - Run commands periodically
 - Handle received commands from the CC



Qbot code evolution

2013-2022

Disclaimer

- Based in our telemetry
 - Missing changes
- We are not covering all changes in this talk
 - Time
 - Whitepaper / Blog
 - Transformation to more advanced and modular malware

Qbot **STAGER**
(EXE)



Qbot **MAIN/HOOK**
(DLL)



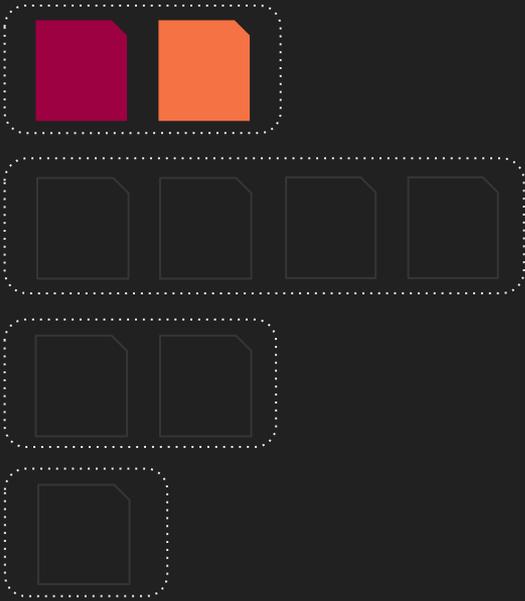
Version: 201.X

~ Jun 2013



~ Release date

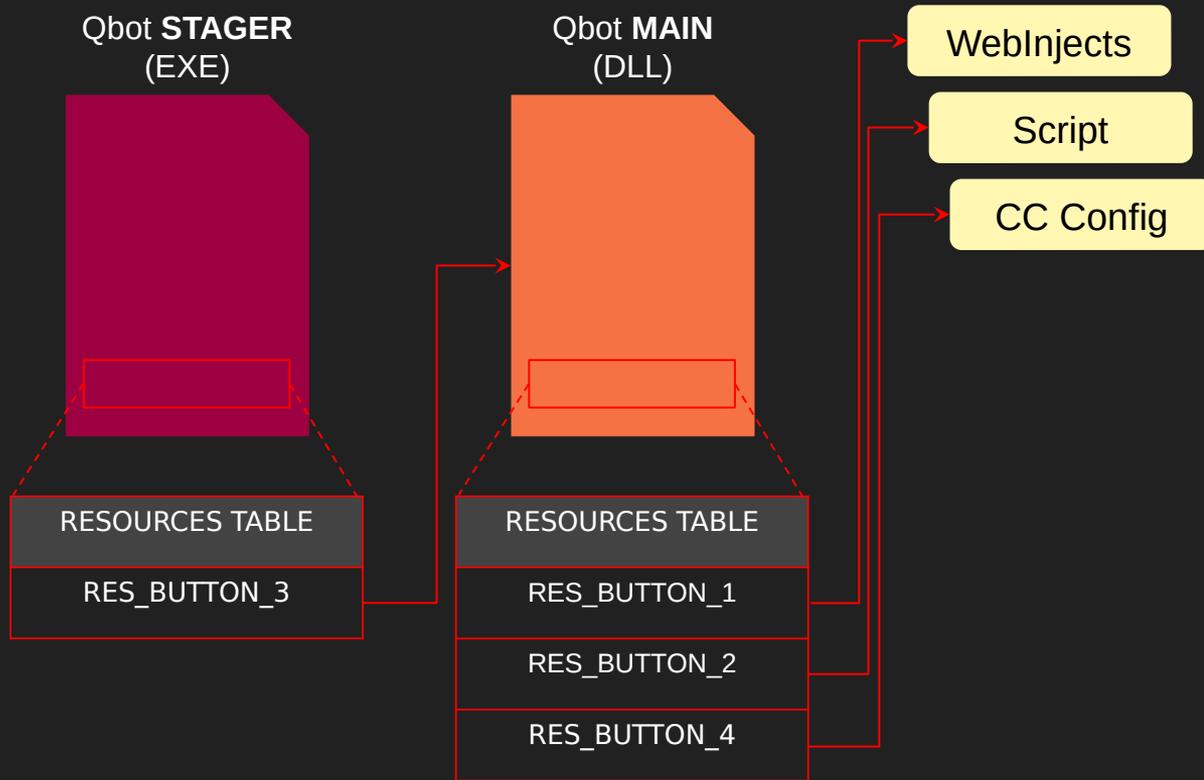


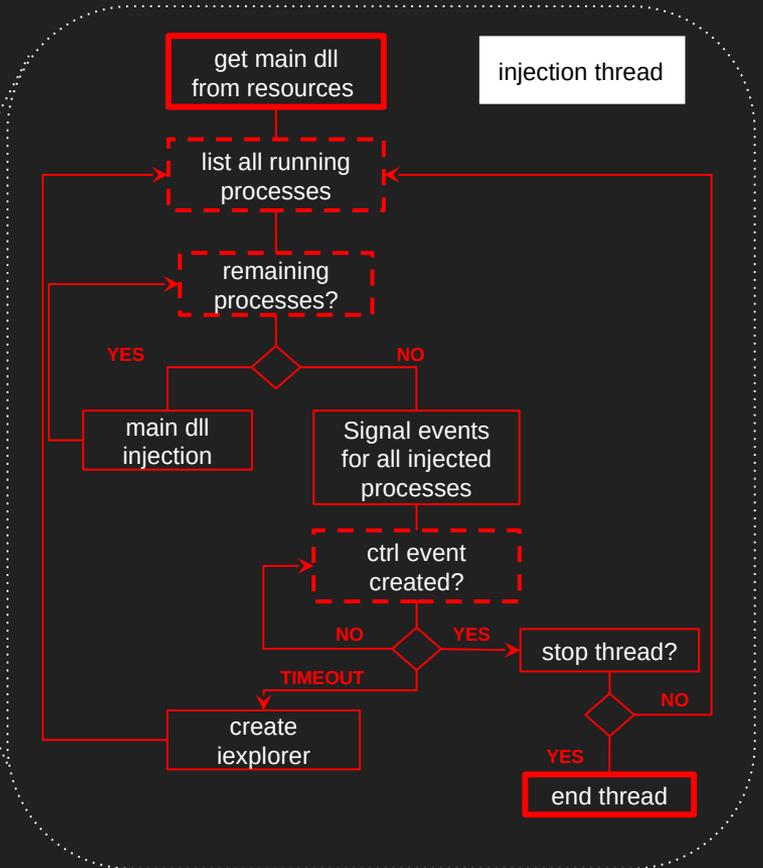
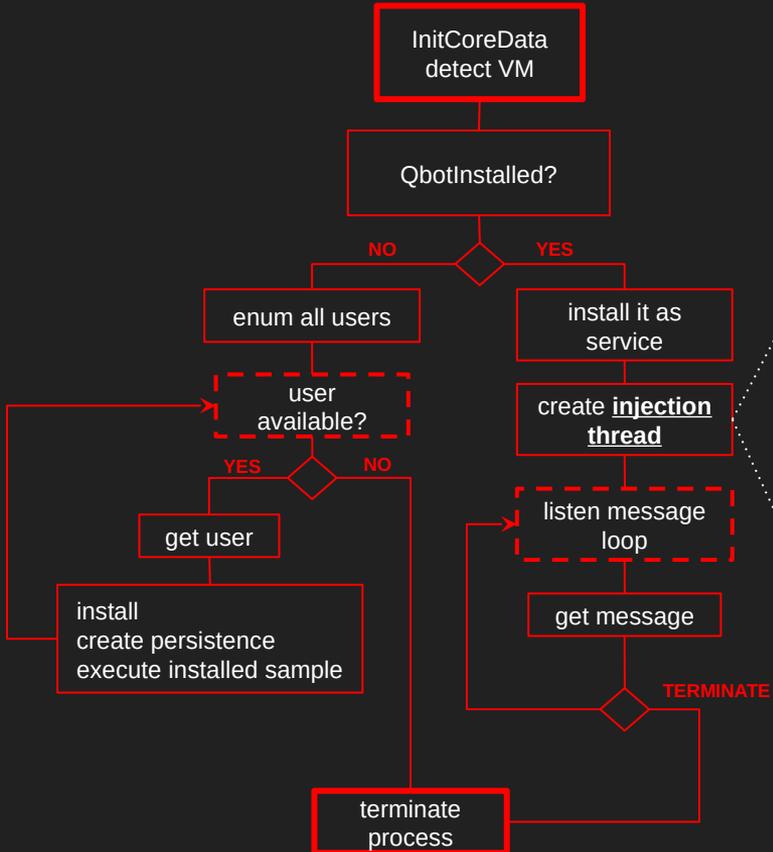


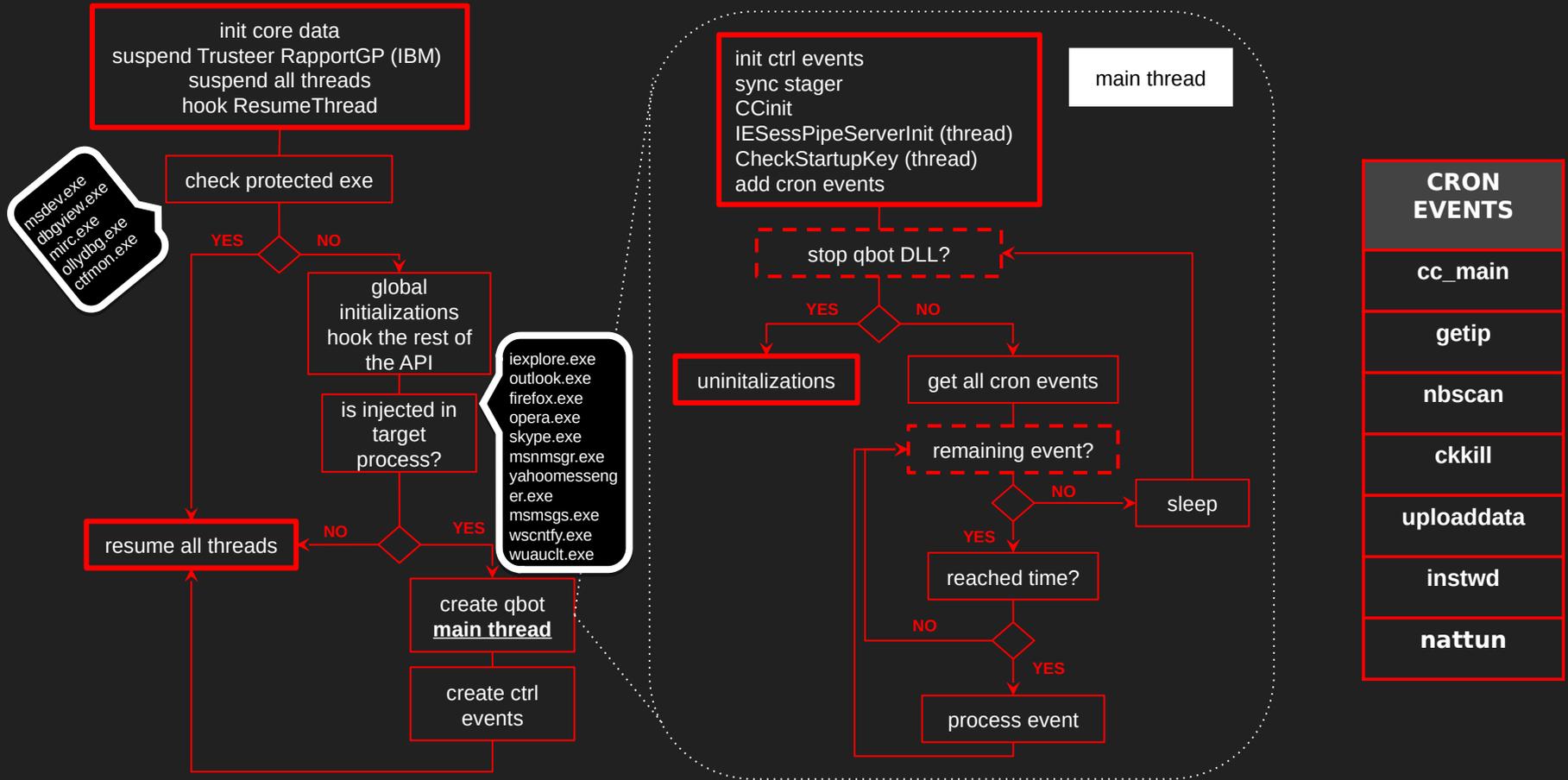
Qbot version:

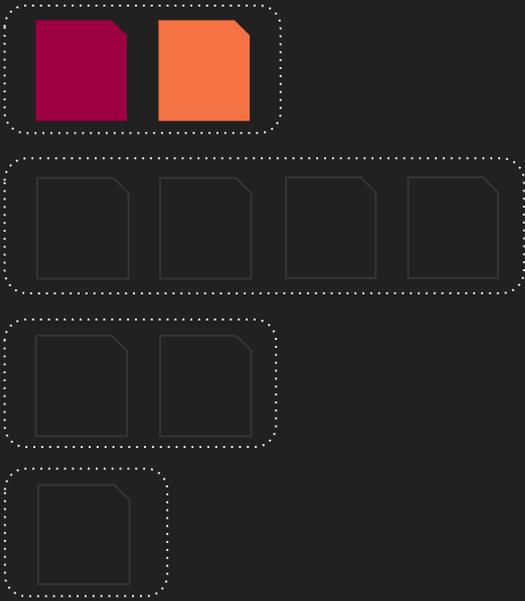
201.X

~Jun 2013







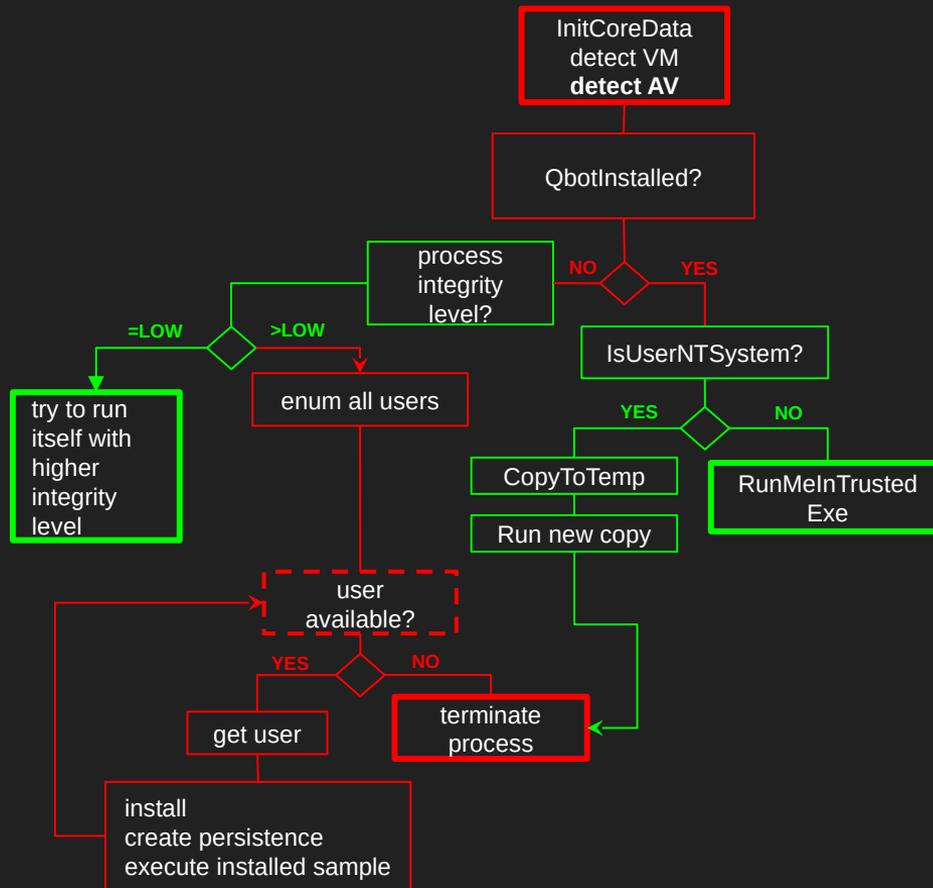


Qbot version:

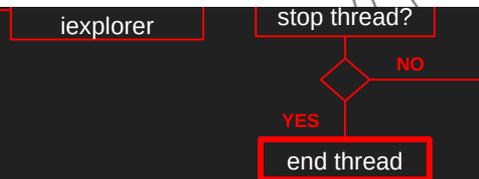
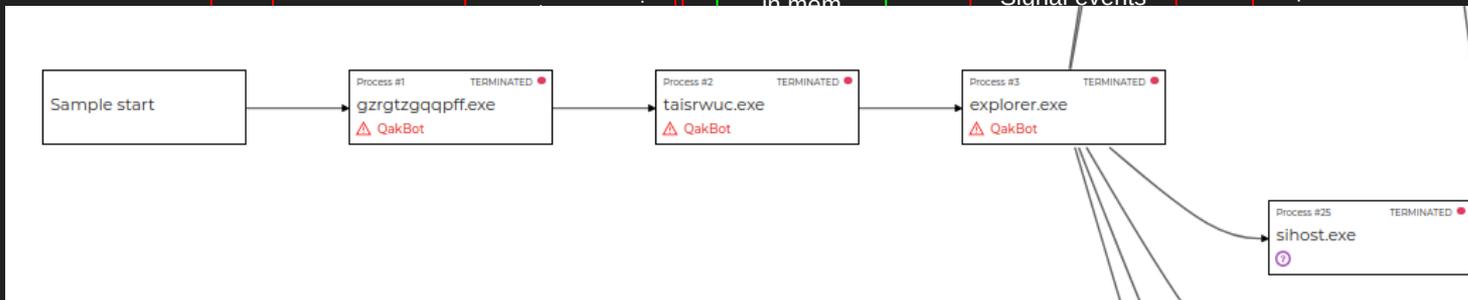
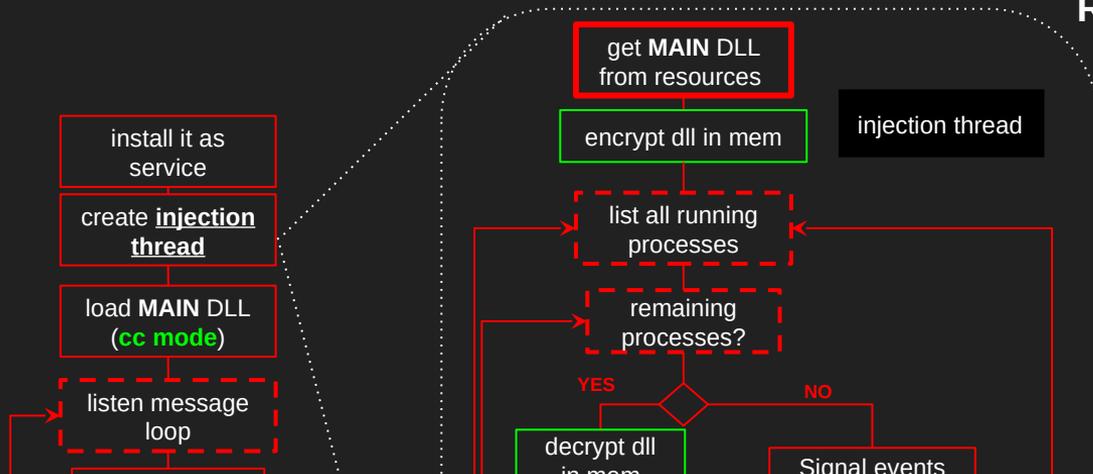
300.X

~Nov 2015

- Main DLL Execution mode



Run explorer.exe
Self injection



MAIN DLL Execution mode

QBOT 200.X

```
INJECTED_IN_TARGET_PROCESS = InjectedInTargetProcess(MODULEBASENAME);
j_ProcessTrusteerThreads();
ResumeSuspendAllThreads(0);
SetResumeThreadHook();
if ( ThreadDesktopRelatedStuff() )
{
    sub_10016AE5();
    SetUpHooks2();
}
else if ( !CheckProtectedExe(MODULEBASENAME) )
{
    sub_10001CAA();
    GenerateConfigFilename();
    sub_100022B2();
    mutex_creation();
    init_glob_vars();
    sub_1000102D();
    init_tcp_sess();
    HttpAuthInit();
    SetUpAllHooks();
    if ( INJECTED_IN_TARGET_PROCESS )
    {
        CreateQbotMainThread(1);
        CreateEventsAndControlThread();
    }
}
ResumeSuspendAllThreads(1);
```

QBOT 300.X

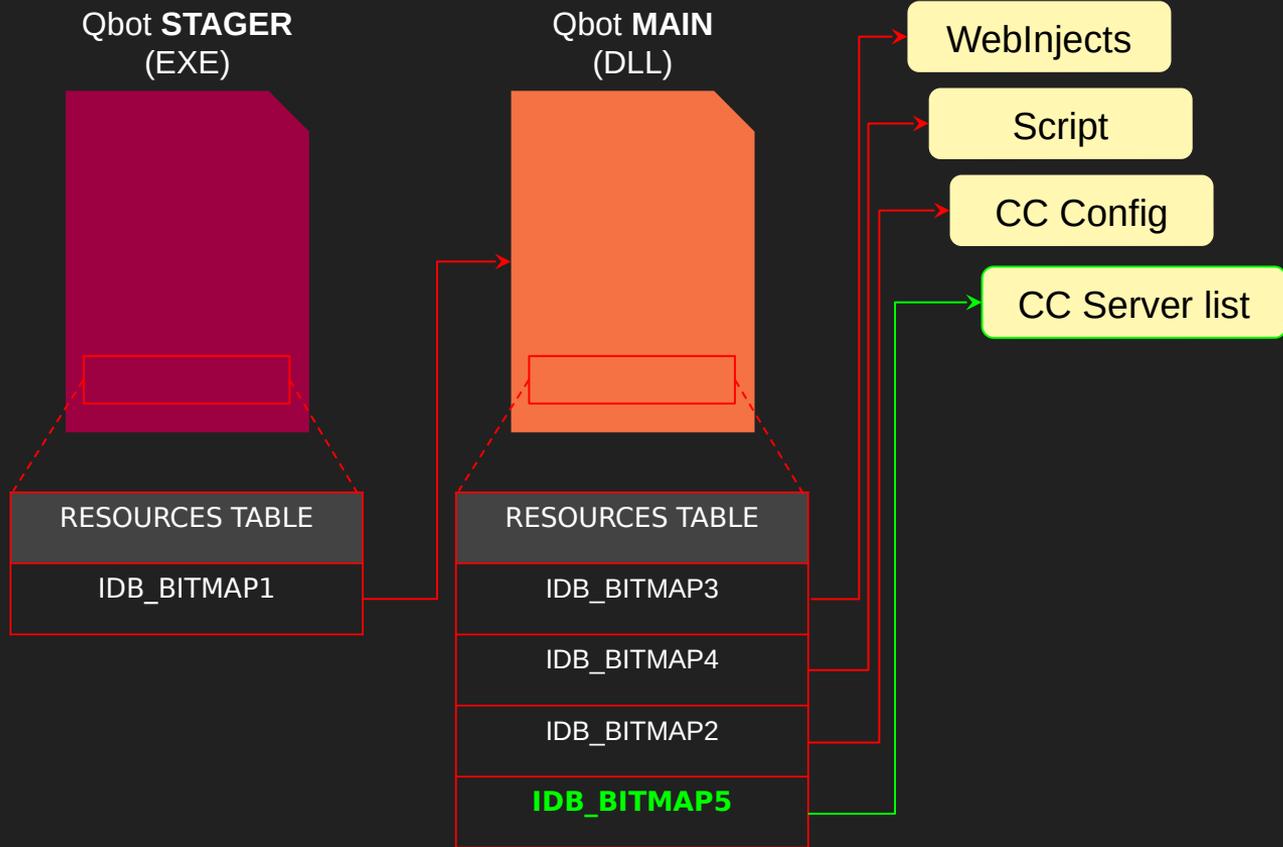
```
PROTECTED_EXE_LIST = ParseStringItems(dword_100396B0, 59, 0, (int)&dword_10023608);
if ( Module && *(DWORD *)&Module->ExecutionMode == 1 )
{
    MAIN_THREAD_HANDLER = (int)CreateThread(0, 0, qbot_main_thread, 0, 0, (LPDWORD)&lpReserved);
}
else
{
    InitHooks();
    if ( CheckProtectedExe(dword_10039608) )
    {
        hinstDLL = (HINSTANCE)SuspendAllThreads(&fdwReason);
        SetResumeThreadHook();
        RunHooks((int)hinstDLL, fdwReason);
        sub_10011280((LPCSTR *)&hinstDLL, 4 * fdwReason);
    }
    else
    {
        init_glob_vars();
        sub_1000175D();
        sub_10007720();
        mutex_creation();
        sub_10005157();
        sub_1000146C();
        init_tcp_sess();
        HttpAuthInit();
        sub_10004CE8();
        j_ProcessTrusteerThreads();
        hinstDLL = (HINSTANCE)SuspendAllThreads(&fdwReason);
        SetResumeThreadHook();
        HookLdrLoadDll();
        sub_10003102();
        sub_1000312F();
        if ( sub_10004F53() )
```

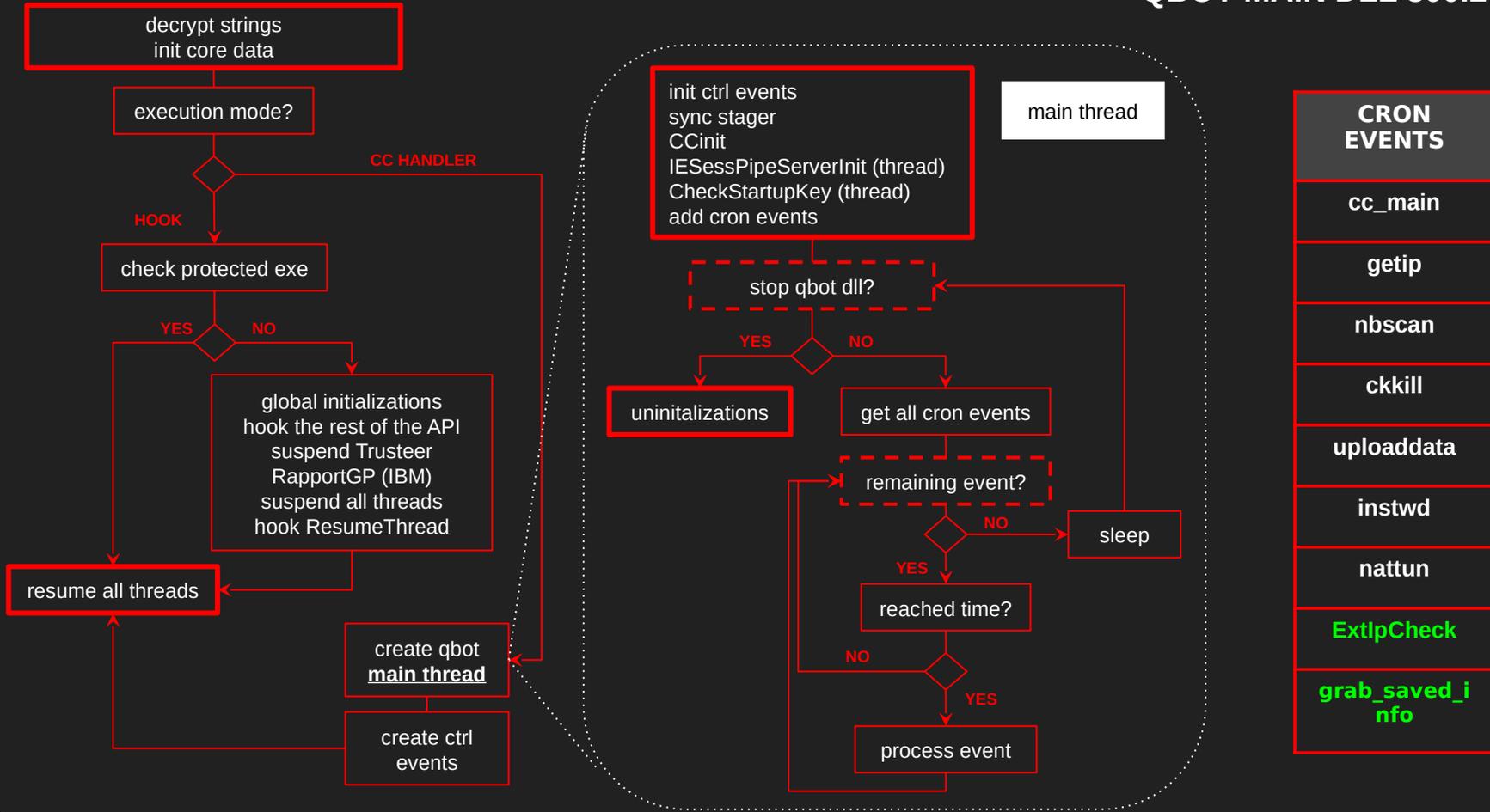


Qbot version:

300.257

~April 2016
- CC List





CRON EVENTS
cc_main
getip
nbscan
ckkill
uploaddata
instwd
nattun
ExtIpCheck
grab_saved_info

STAGER

- run_as_exe_installer modified

QBOT >300.X

```
int __cdecl run_as_exe_installer(int a1)
{
  UINT DriveTypeA; // eax
  CHAR RootPathName[16]; // [esp+4h] [ebp-10h] BYREF

  memset(&unk_7000F740, 0, 20);
  if ( ExistingFileName[1] != 58
      || (strncpy(RootPathName, ExistingFileName, 3),
          DriveTypeA = GetDriveTypeA(RootPathName),
          DRIVETYPE = 4,
          DriveTypeA != 2) )
  {
    DRIVETYPE = 2;
  }
  dword_7000F74C = a1;
  MINOR_VERSION_AUX = MINOR_VERSION;
  qbot_install_main((int)&unk_7000F740);
  return 0;
}
```

QBOT >300.257

```
int __cdecl run_as_exe_installer(int a1, int a2)
{
  UINT DriveTypeA; // eax
  CHAR RootPathName[16]; // [esp+4h] [ebp-10h] BYREF

  memset(&unk_410740, 0, 20);
  if ( ExistingFileName[1] != 58
      || (strncpy(RootPathName, ExistingFileName, 3),
          DriveTypeA = GetDriveTypeA(RootPathName),
          DRIVETYPE = 4,
          DriveTypeA != 2) )
  {
    DRIVETYPE = 2;
  }
  dword_41074C = a1;
  MINOR_VERSION_AUX = MINOR_VERSION;
  if ( a2 )
    qbot_install_main_system(&unk_410740); // <- New function
  else
    qbot_install_main(&unk_410740);
  return 0;
}
```

- **MAIN DLL**

- Added the DGA as secondary option if it can not obtain the CC list from its resources

QBOT >300.X

```
int __cdecl EnumCCServers(int a1, int ( __cdecl *a2)(CHAR *, int *, int), int a3)
{
    // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

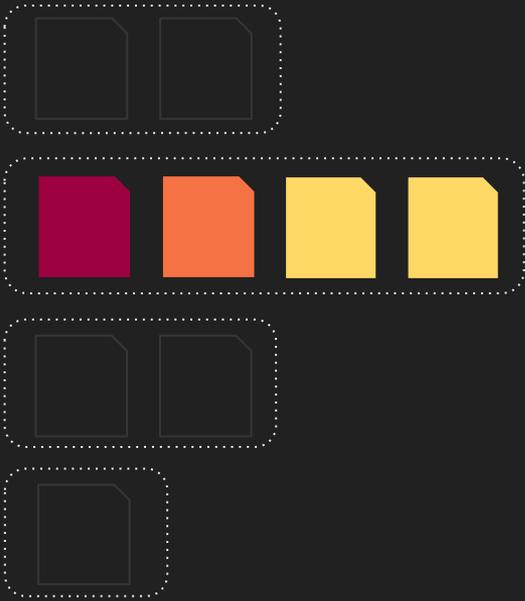
    if ( !String1
        || (LODWORD(v3) = get_system_time(0), v3 >= qword_10026050 + 43200)
        || (my_concat_strings(&byte_1001C2C5, (int)v8, 1024, off_10039810), result =

        // DGA Algorithm
        if ( sub_10016866(String, 100) )
        {
            v5 = sub_100167D3(String);
            if ( sub_10016AF8() > 0 )
                ++v5;
            sub_10013A1F(v5, v7);
            v12 = 0;
            while ( 2 )
            {
                v11 = 5;
                v13 = sub_100169ED(v7, 5, 1);
                if ( v13 )
                {
                    for ( i = 0; i < 0x14; i += 4 )
```

QBOT >300.257

```
1 int __cdecl EnumCCServers(int a1, int ( __cdecl *a2)(LPCSTR, const char *, int, int), int a3)
2 {
3     // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]
4
5     cc_selected = -1;
6     if ( !*lpString1
7         || (LODWORD(v4) = get_system_time(0), v4 >= qword_1002EF60 + 43200)
8         || (result = a2(lpString1, dword_1002EF50, a1, a3), cc_selected = result, result < 0) )
9     {
10        dwBytes = 0;
11        EncCCList = GetResData(HMODULE, RESOURCE_NAME, (int)&dwBytes, 0, 0, 0);
12        if ( EncCCList )
13        {
14            DecCCList = sxor2_open_from_mem(EncCCList, dwBytes, 0, 0);
15            v18 = DecCCList;
16            if ( DecCCList )
```

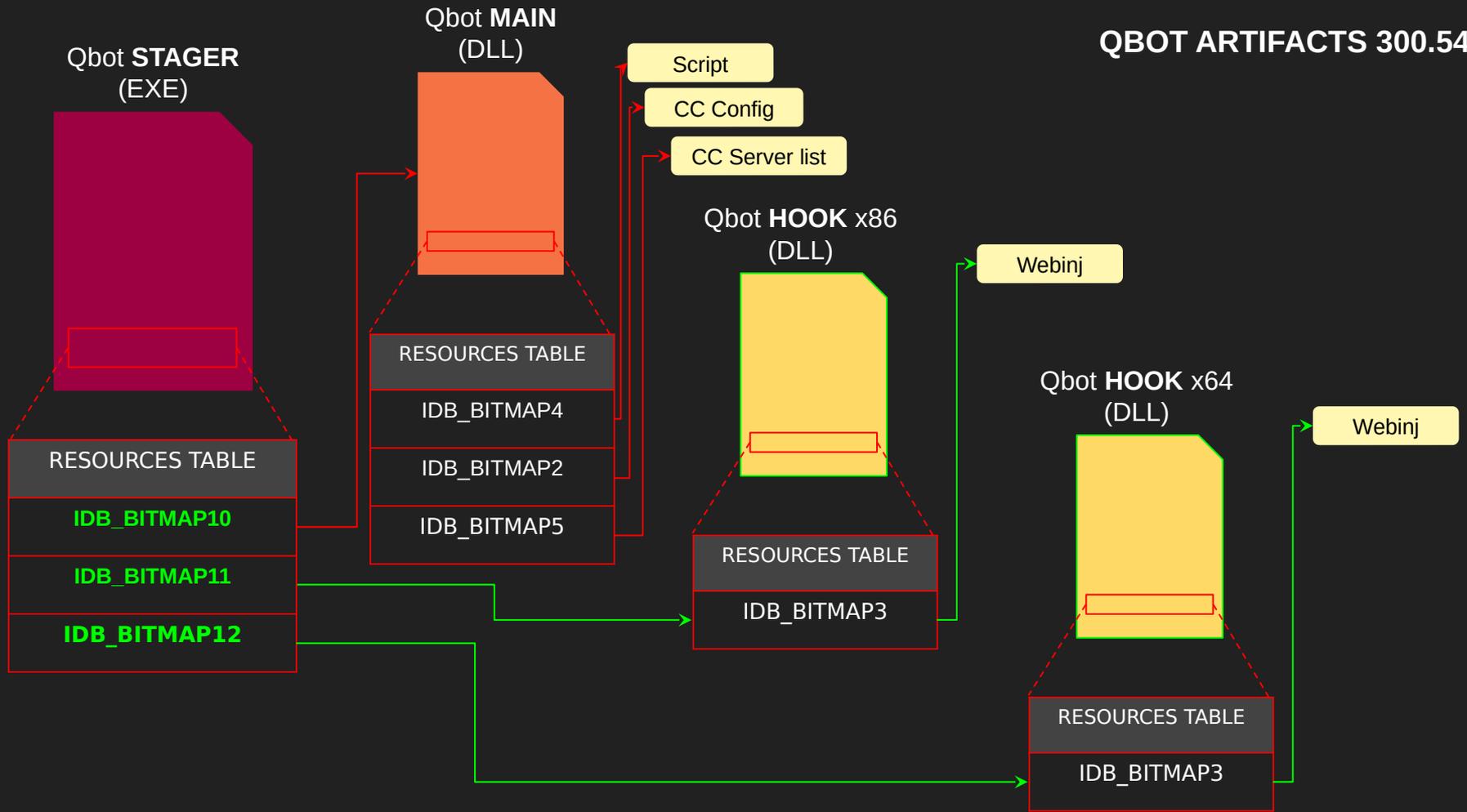
```
44 }
45 if ( cc_selected < 0 )
46 {
47     // DGA Algorithm
48     if ( sub_1001CB50(String, 100) )
49     {
50         v12 = sub_1001CABD(String);
51         if ( sub_1001CDCF() > 0 )
52             ++v12;
53         sub_10019EE2(v12, v14);
54         v20 = 0;
55         while ( 2 )
```

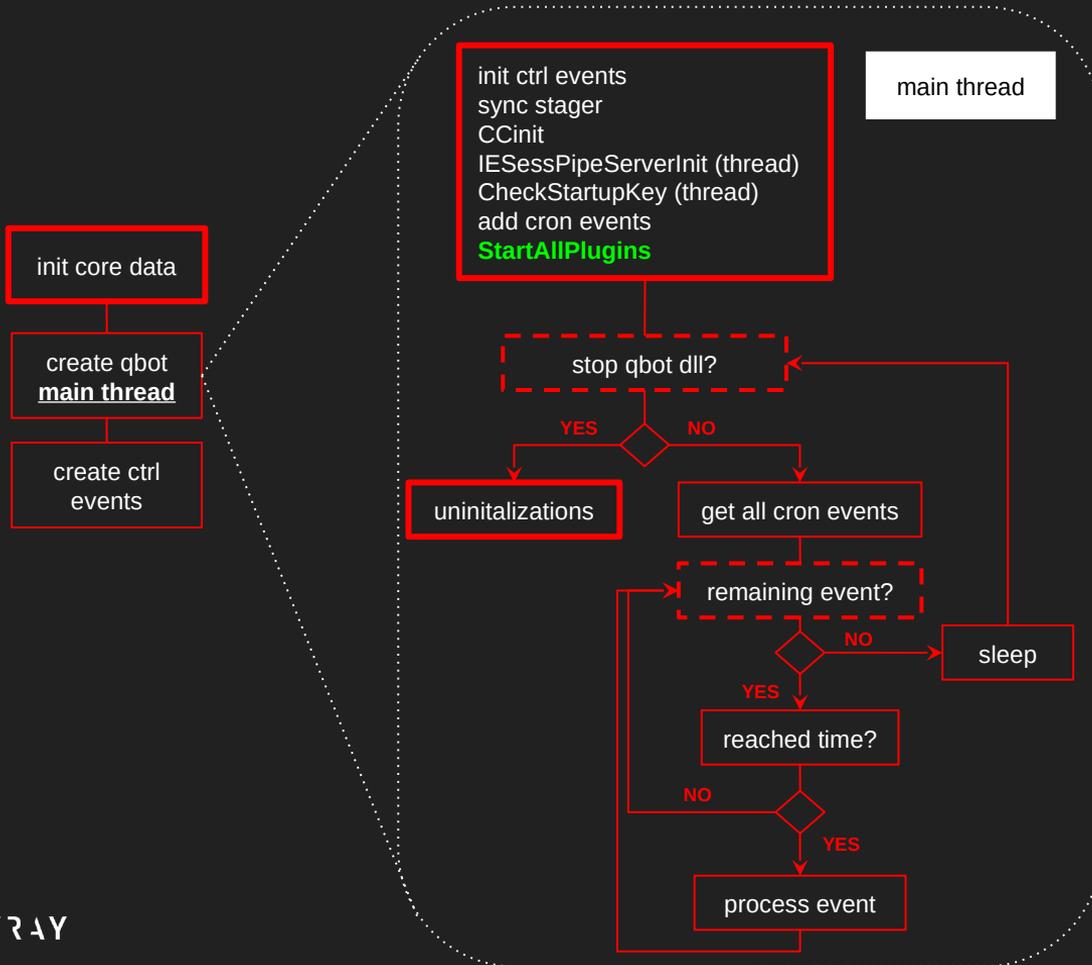


Qbot version:

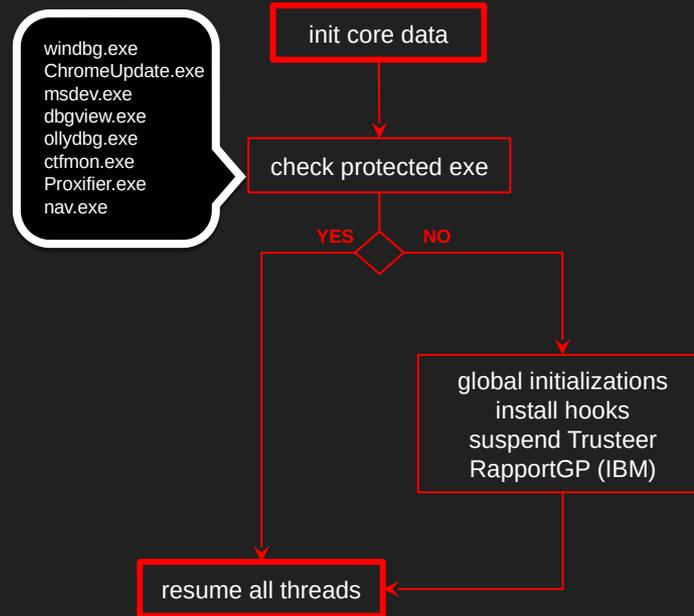
300.549

~Feb 2017
Plugin support





CRON EVENTS
cc_main
getip
nbscan
ckill
uploaddata
instwd
nattun
ExtIpCheck
grab_saved_info



MAIN DLL

- Plugin support

```
dd 19h
dd 1
dd offset cmd_wgetexe_h
dd 1Ah
dd 1
dd offset cmd_plugin_install_h
dd 1Bh
dd 1
dd offset cmd_plugin_on_h
dd 1Ch
dd 1
dd offset cmd_plugin_off_h
dd 1Dh
dd 1
dd offset cmd_plugin_uninstall_h
dd 1Eh
dd 1
dd offset cmd_plugin_reset_h
```

MAIN DLL

- The fields in the config are renamed to numbers to hide their meaning
- This is applied not only to the fields in the hardcoded config but also to any field in the config

QBOT >300.257

```
cc_server_port=16763
cc_server_pass=iJKcdgJ67dcj=██████████
ftphost_1=66.96.133.9:help:eT██████████
ftphost_2=196.12.12.88:log@zica.co.zm:██████████
ftphost_3=91.199.120.147:logs@ixl030cf.ixl.es:██████████
ftphost_4=50.87.114.63:cpanel@itsolution-lb.com:██████████
ldr=0
worm_disabled=1
ctstmp=1469457173
```

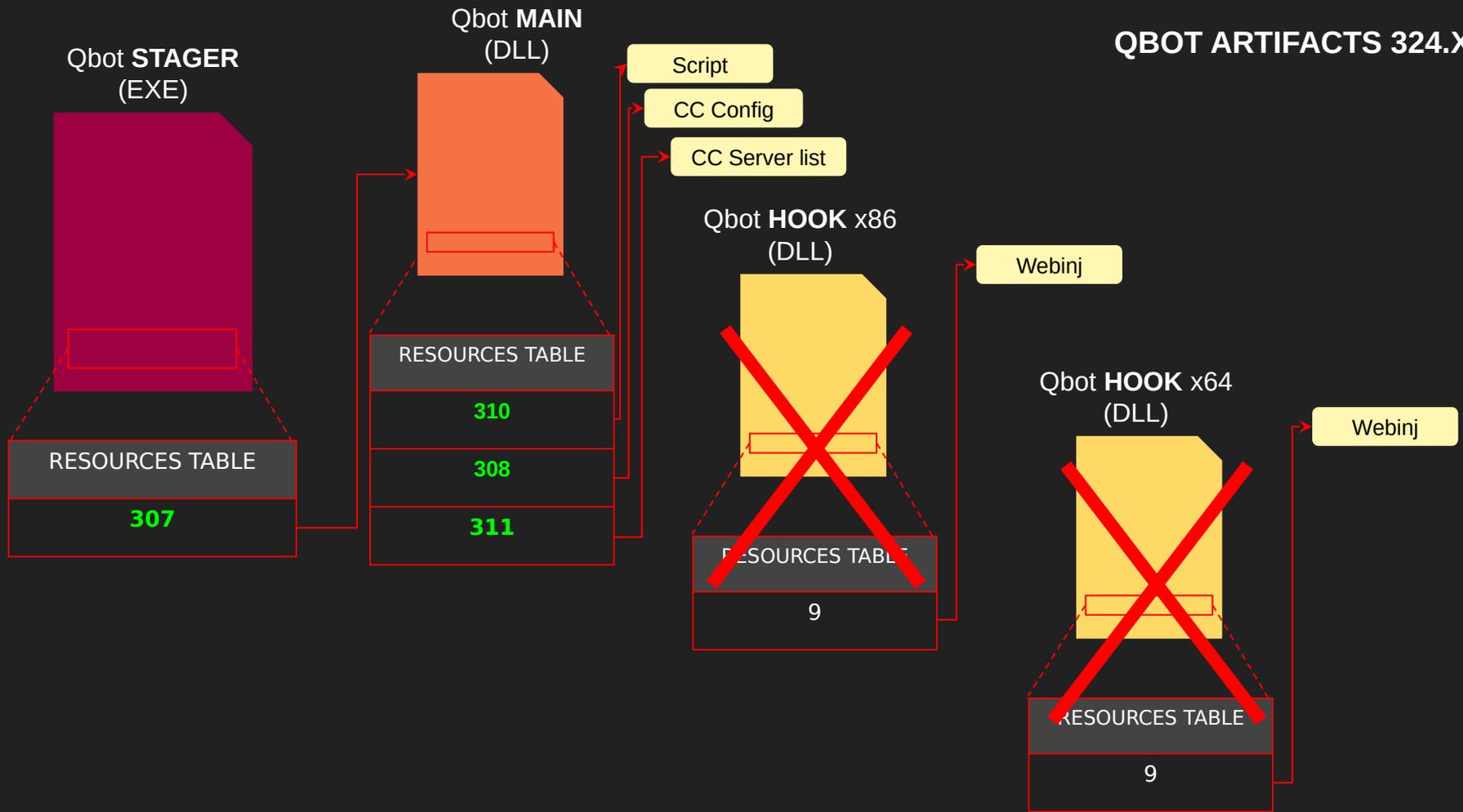
QBOT >300.549

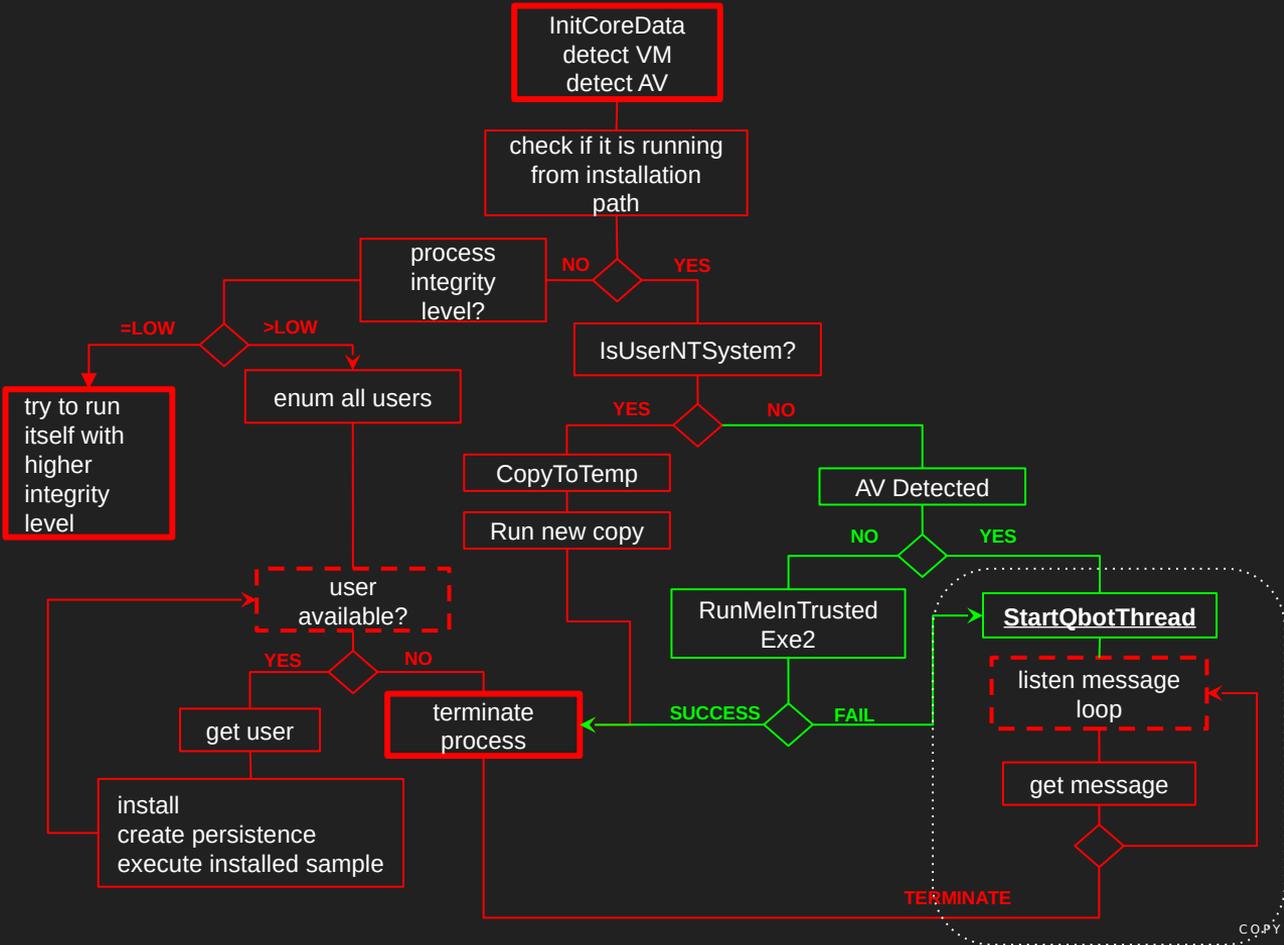
```
22=66.96.133.9:help:eT5TerAcnFe6~:
23=174.123.38.58:log@thebrainregistry.com:4B██████████u:
24=61.221.12.26:logger@ostergift.com:34██████████S:
25=67.222.137.18:logger@grupocrepusculo.net:p4██████████R:
26=107.6.152.61:logger@trussedup.com:R██████████IV:
3=1487787908
```

Qbot version:

324.X

~Jan 2020





MAIN DLL

- Managed the webinjects as Plugin

QBOT >300.257

```
1 int __cdecl update_webfix(int arglist, const CHAR *lpString)
2 {
3     // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXP
4
5     *v17 = 0;
6     v14 = 0;
7     v16 = 0;
8     v13 = 0;
9     v15 = 0;
10    if ( arglist != 1 && arglist != 2 )
11    {
12        log_error(0, "update_webfix(): bad type: %u", arglist);
13        return -1;
14    }
15    log("update_webfix(): started dwType=[%u]", arglist);
16    v4 = strlenA(lpString);
17    v14 = base64_decode(lpString, v4, &v13);
18    if ( !v14 )
19    {
20        log_error(0, "update_webfix(): base64_decode() failed");
21        return -2;
22    }
23    sub_1000A511(arglist);
24    my_concat_strings("\\", PathName, 260, WORKDIRIRECTORY);
25    if ( !CreateDirectoryA(PathName, 0) )
26    {
27        SetLastError = GetLastError();
28        log_error(LastError, "update_webfix(): CreateDirectory('%s'
29    )
30    my_concat_strings("\\", PathName, 260, PathName);
31    v6 = sub_100219E3(v14, v13, &v16);
32    if ( v6 > 0 )
33    {
34        v7 = sxor2_open(PathName, 2, WindowName, 2);
35        v15 = v7;
36        if ( v7 )
37        {
38            if ( sxor2_write(v7, v16, v6) >= 0 )
39            {
40                if ( schedule_reload_1() >= 0 )
41                {
42                    log("update_webfix(): ===>>> update complete");
```

QBOT >324.X

```
1 int __cdecl update_webinj(int a1, LPCSTR lpString)
2 {
3     // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO E
4
5     v16 = 0;
6     v14 = 0;
7     v15 = 0;
8     if ( a1 != 1 && a1 != 2 )
9     return -1;
10    v12 = base64_decode(lpString, &v15);
11    if ( !v12 )
12    return -2;
13    v3 = strlenA(WindowName);
14    v4 = hash_crc32(0, WindowName, v3);
15    sub_10011F82(v7, a1 + v4);
16    *(&v7[623] + sub_10012E39(v8, 10)) = 46;
17    lpPathName = ConcatStringA(word_1002D520);
18    lpString2 = ConcatStringA(lpPathName);
19    CreateDirectoryW(lpPathName, 0);
20    v11 = sub_1001800C(&v14);
21    if ( v11 > 0 )
22    {
23        if ( sxor2_open(lpString2, 2, WindowName, 2) )
24        {
25            if ( sxor2_write(v14, v11) >= 0 )
26            {
27                free_mem();
28                v9 = ConcatStringA(word_1002D520);
29                if ( MyMoveFile(lpString2) < 0 )
30                    v16 = -7;
31                heap_free(-2, &v9);
32                v5 = v16 < 0;
33                if ( !v16 )
34                {
35                    if ( (sub_100054A6(0x2DEB8B96) & 0x80000000) == 0 )
36                        sub_10005877();
37                    EnablePlugin(0x2DEB8B96);
```

crc32("plugin_hook")
==
0x2deb8b96

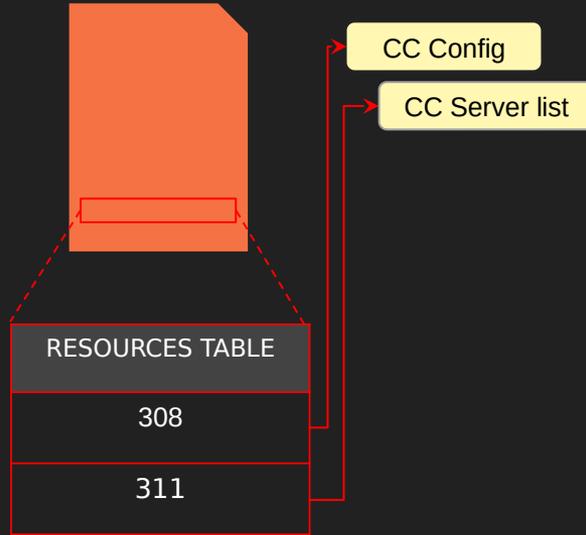
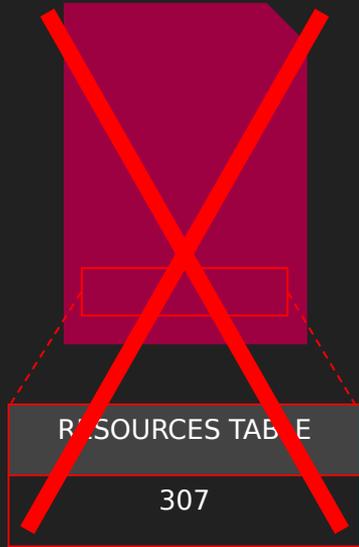
Qbot version:

401.X

~Nov 2020

Qbot MAIN
(DLL)

Qbot STAGER
(EXE)



- Current Major version 403
- From version ≥ 401
 - They have join in same binary the **STAGER** and the **MAIN DLL**
 - This new binary is a DLL which does the persistence and communication with the C2
 - All previous functionalities has been moved to Plugins
 - + Webinjects
 - + Password grabber
 - + Proxy
 - + Hidden VNC
 - + ...

Qbot **STAGER**
(EXE)



Qbot **MAIN/HOOK**
(DLL)



Version: 201.X

~ Jun 2013

~ Release date

Qbot **STAGER**
(EXE)



Qbot **MAIN**
(DLL)



Qbot **HOOK** x86
(DLL)



Qbot **HOOK** x64
(DLL)



Version: >300.549

~ Feb 2017

Qbot **STAGER**
(EXE)



Qbot **MAIN**
(DLL)



Version: >324.X

~ Jan 2020

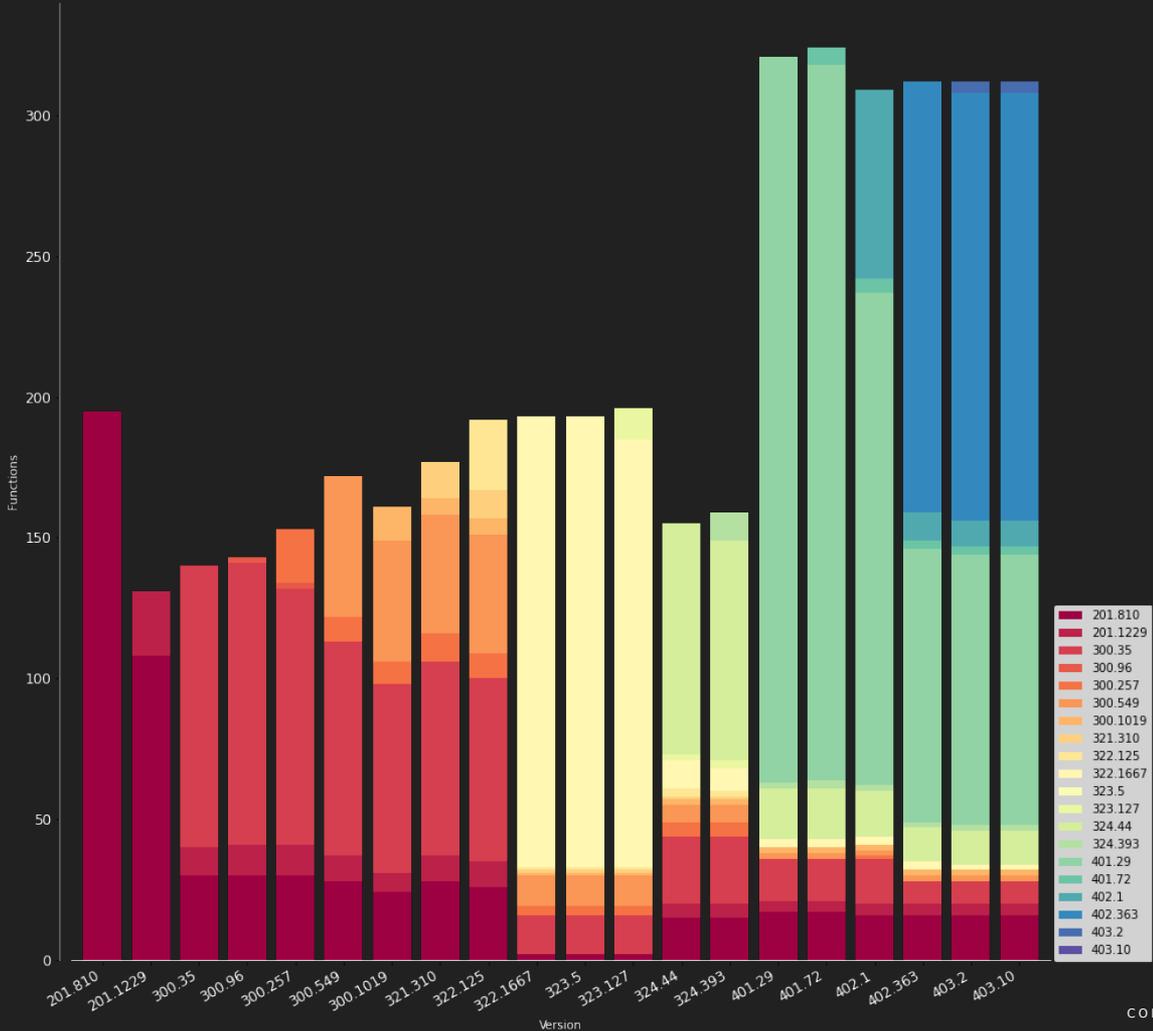
Qbot **STAGER + MAIN**
(DLL)



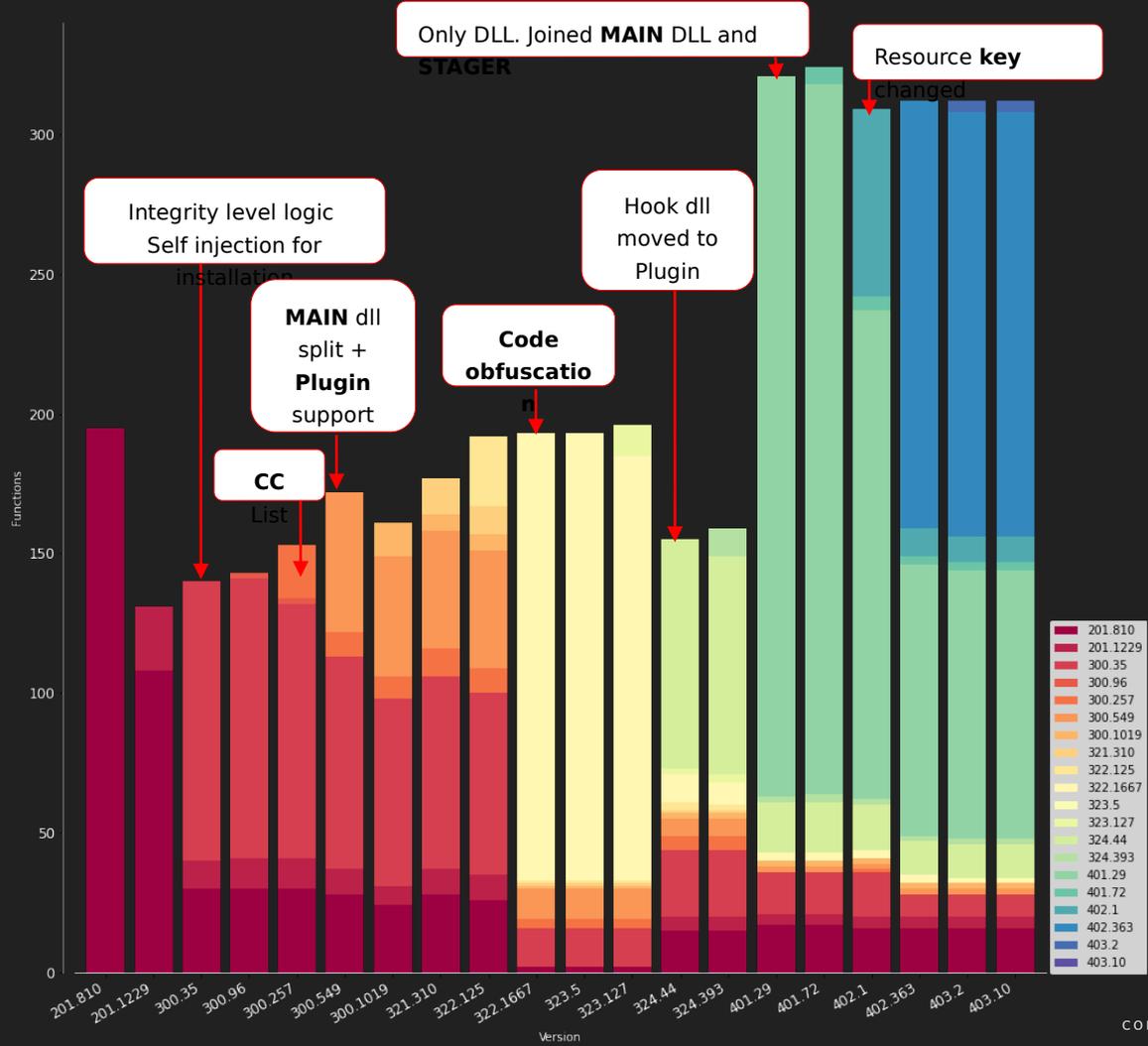
Version: >401.X

~ Nov 2020

Qbot STAGER



Qbot STAGER



Metadata -> Insights

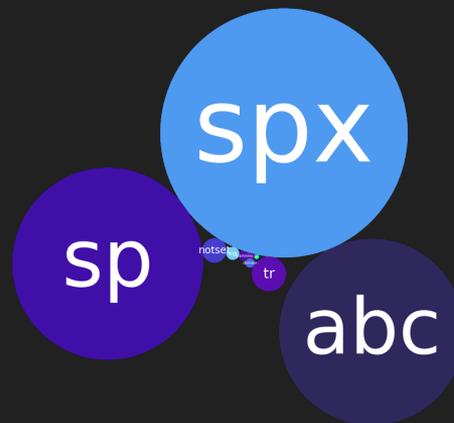
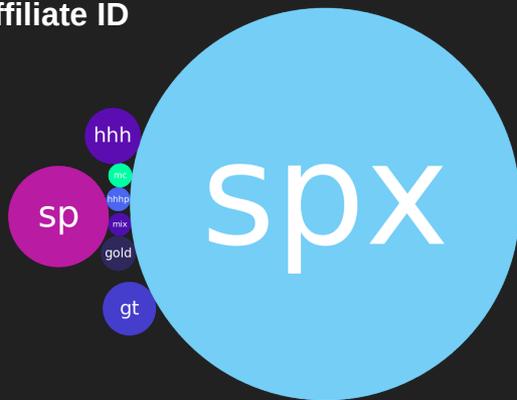
Affiliate ID/ Version / Timestamp

Affiliate ID	Version	Timestamp	
spx112	201.81	22 January 2018 17:23:46	(1516641826)
tr	201.834	30 January 2019 17:43:09	(1548870189)
AA	300.400	17 March 2020 16:17:44	(1584461864)
abc12	321.128	8 February 2021 11:02:19	(1612782139)
abc13	322.1598	18 February 2021 14:02:49	(1613656969)
obama72	323.36	12 December 2021 18:25:30	(1639333530)
obama73	324.386	15 February 2022 11:01:24	(1644922884)
clinton1	401.855	9 March 2022 15:46:32	(1646840792)
clinton10	403.263	4 April 2022 7:42:58	(1649058178)

Before 2020

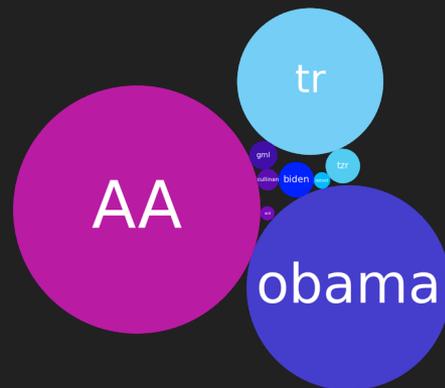
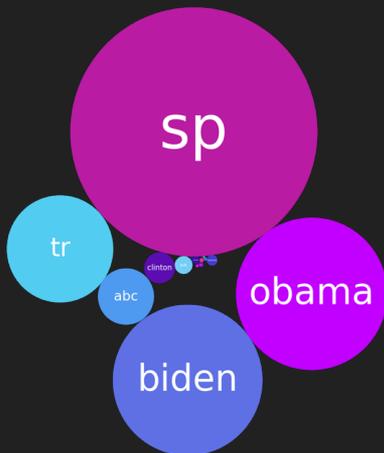
2020-2021

Samples Affiliates ID

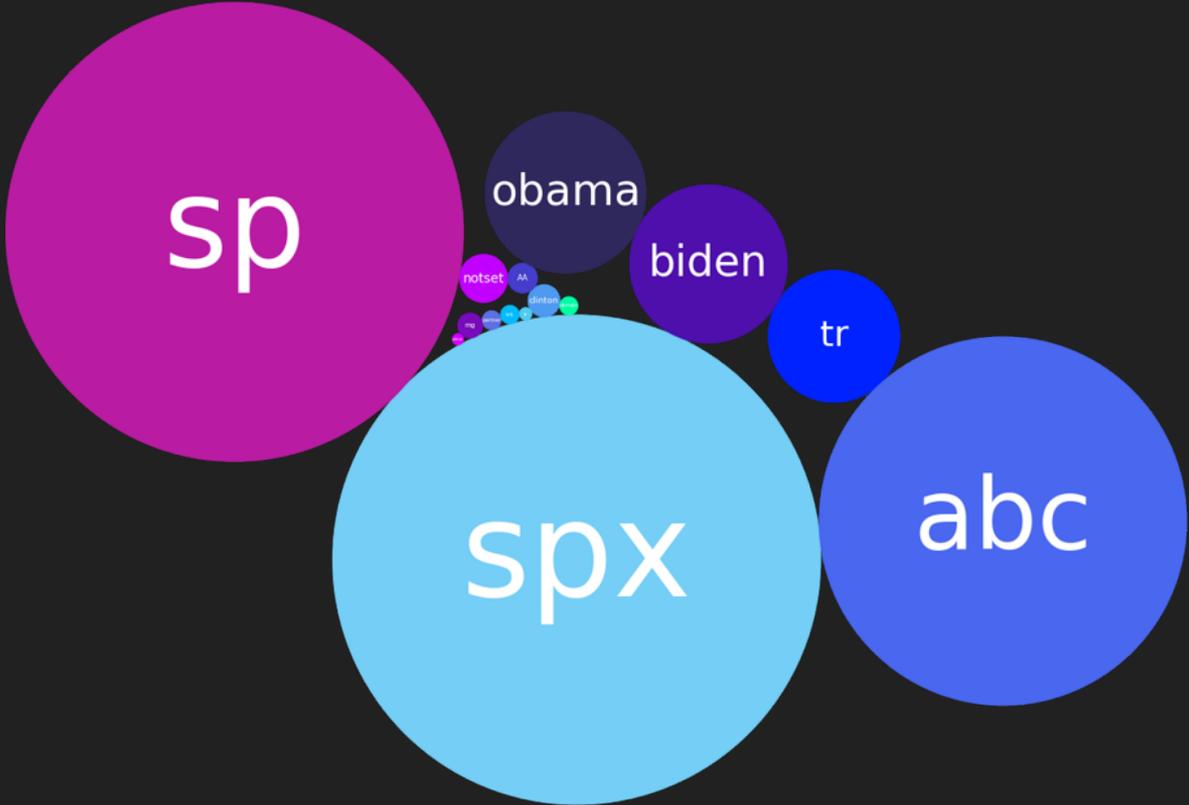


2021-2022

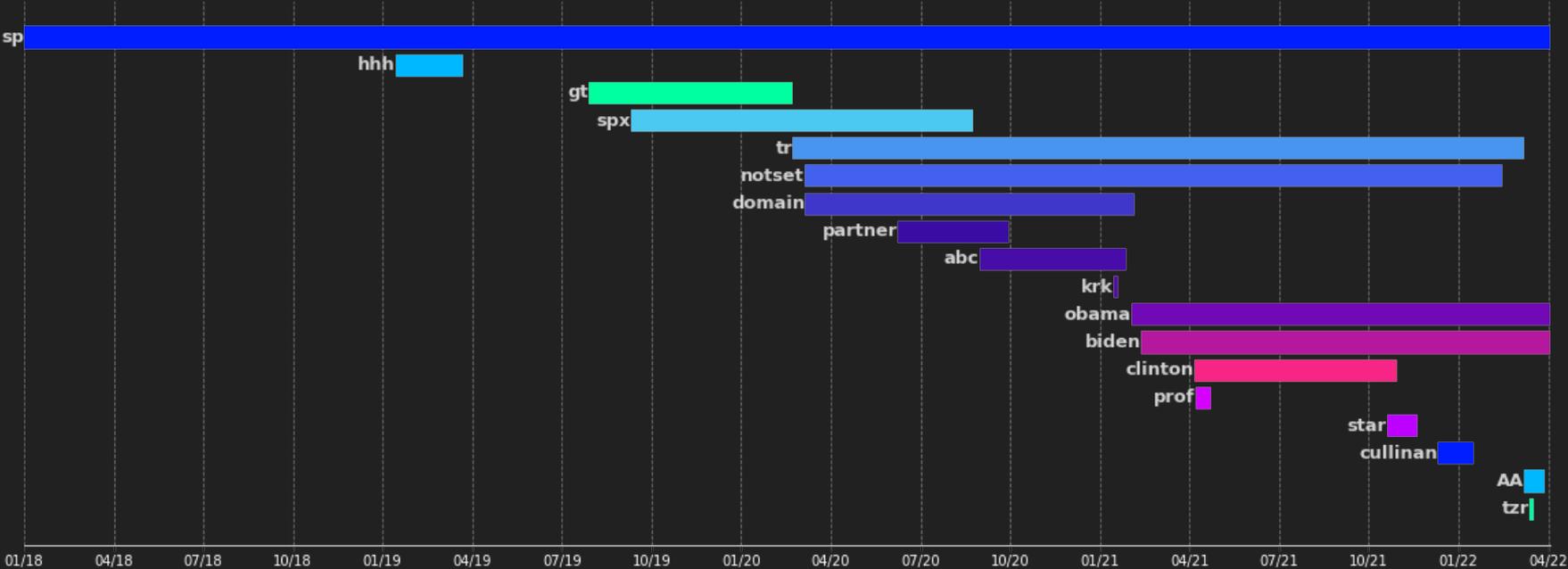
2022



Samples Affiliate ID – All



Relevant Affiliate IDs



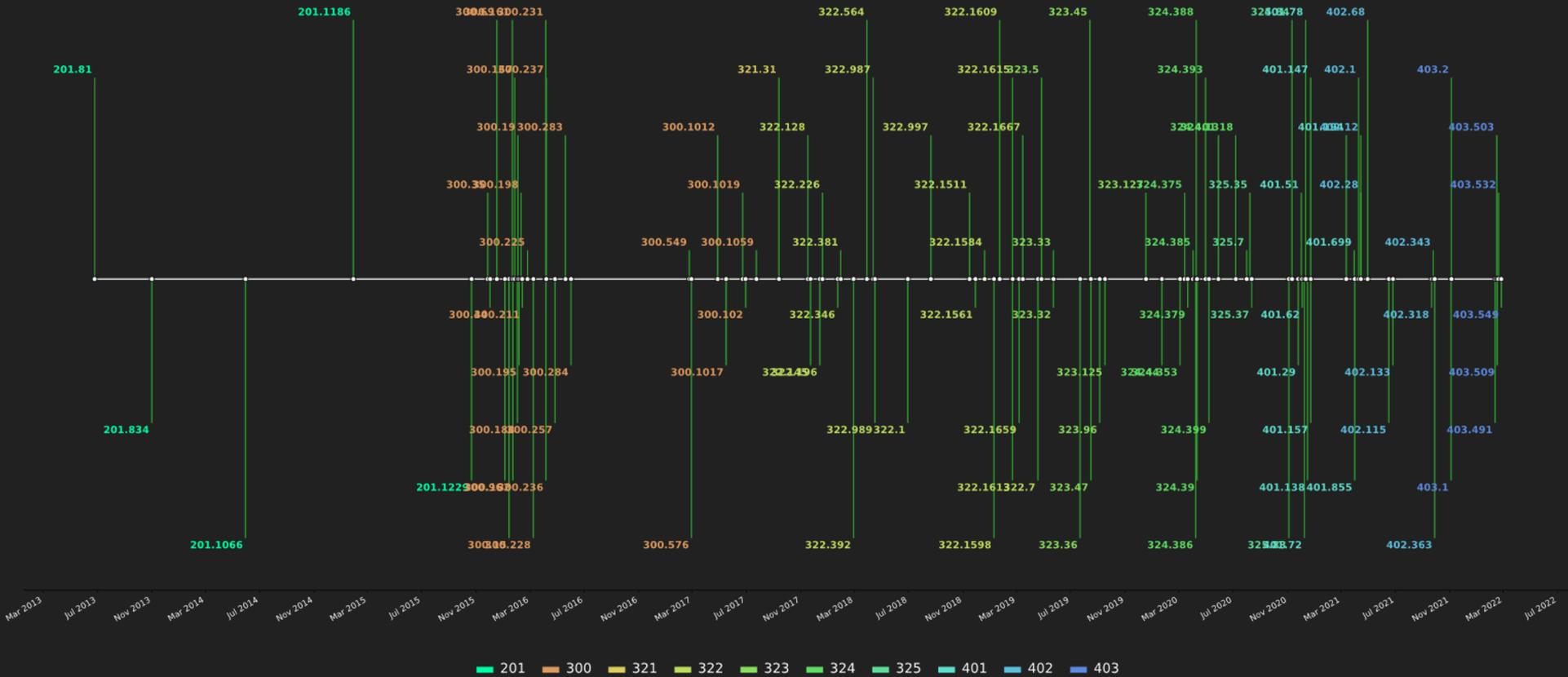
Qbot Affiliate ID / Version / Timestamp



- 325.14
- 325.59
- 401.62
- 401.138
- 402.1
- 402.68
- 402.318
- 402.363
- 403.1
- 403.509
- 325.42
- 401.29
- 401.78
- 401.194
- 402.12
- 402.115
- 402.343
- 403.2
- 403.491
- 403.549
- 325.43

Conclusion

Qbot Version Timeline (2013-2022)





THREATRAY

Ready for the Threatray Advantage?

VISIT [HTTPS://THREATRAY.COM](https://threatray.com) OR CONTACT US AT [INFO@THREATRAY.COM](mailto:info@threatray.com)