Let's Learn: In-Depth Reversing of Qakbot "qbot" Banker Part 1

vkremez.com/2018/07/lets-learn-in-depth-reversing-of-qakbot.html

Goal: Reverse engineer and analyze the Qakbot banker with the focus on its core functionality, new configuration, and decoded template.

> #Emotet and #Qakbot
> Invoice-75301.doc [Old Template]
> 5f894602e88263e34dcdbb2eb2da3078
>
> polysorce,com/newsletter/En_us/Invoice/Invoice-75301
>
> Payload download exe"png" files, signed by thawte, Inc
>
> Use Invoke-DOSfuscation pic.twitter.com/TGkaQzAUBR
> — _(⊙_⊙)_/ (@pollo290987) July 25, 2018

Malware Sources:
Invoice-75301.doc(5f894602e88263e34dcdbb2eb2da3078)
Original Signed Packed Qakbot Banker
(805f48f1295e28cc82c180844e3165d6)

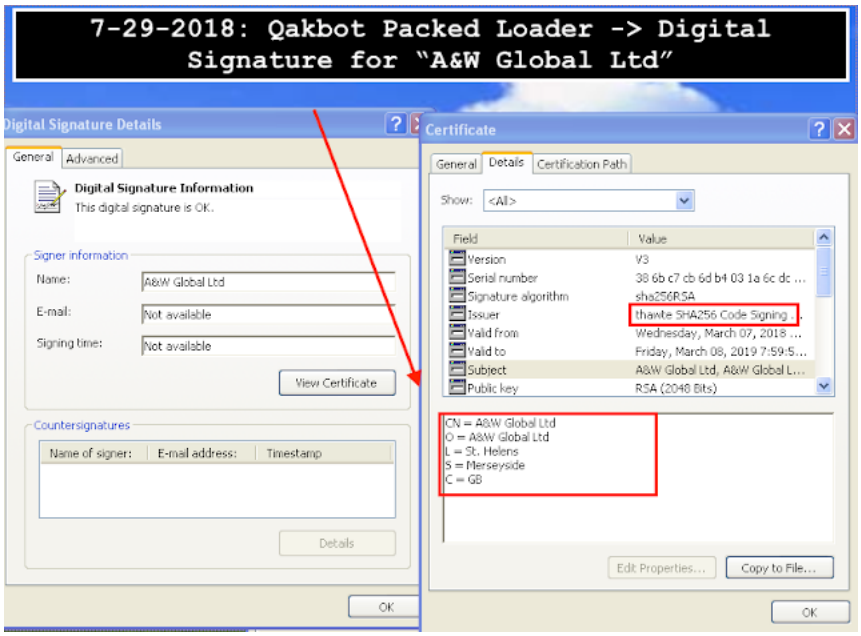
- Unpacked Qakbot Core x86 (95ec8de64002fc5de7c04ceba04702da)
  - Qbot Communicator Dll x86 (7dad18c4d149849c727fe39eee184fe8)
  - Qbot Inject Dll x64 (03e78339b09aa5e9885c24b2e8af84f4)
  - Qbot persistence script (c4eaff27f786204627c5b2b915e9c801)

Background
While investigating one notable infection chain distribution (thanks to @pollo290987), linked to both Emotet Loader and Qakbot Banker, I decided to take a deeper dive into the QakBot binary and its related component with the focus on core functionality. Qakbot is one of the oldest but yet-still-active bankers on the financial malware landscape operating since 2009. Qbot is a credential-stealing financial malware known to target customers of financial institutions for account takeover fraud (ATO). The malware has worm capabilities to self-replicate through shared networks, drives, and removable media, and is notable for active directory bruteforcing as detailed by IBM X-Force.
Outline:
The following functions of interest will be analyzed:

```
I. Packed Digitally Signed Qakbot Loader
II. Unpacked Core qbot
A. Decryption XOR Routine
III. "Explorer" Process Injection
IV. Qakbot Configuration
V. Anti-Analysis
VI. Persistency Mechanism
VII. Yara Signature
A. Qakbot Unpacked Core
B. Qakbot Communicator DLL
C. Qakbot Inject DLL
VIII. Indicators of Compromise
IX. Addendum: Full Decoded First-Layer Template
```

I. Packed Digitally Signed Qakbot Loader
The malware initial packed loader is digitally signed with Thawte in order to bypass possible trust-based detection with the following company "A&W Global Ltd."

```
CN = A&W Global Ltd
O = A&W Global Ltd
L = St. Helens
S = Merseyside
C = GB
```



The initial loader simply self-injects and unpacks the core malware in memory. The module can be retrieved vis scanning mapped memory region and dumping the unmapped executable, which would be the Qakbot core component. One of the notable details behind the banker execution is that the malware overwrites the launched executable with the Calculator utility in %WINDIR%\System32 via the CreateProcessA. More specifically, the qbot uses the calc.exe utility to invoke a ping command that will repeat six times in a loop:

```
|hWnd = NULL
|Operation = NULL
|FileName = "cmd.exe"
|Parameters = " /c ping.exe -n 6 127.0.0.1 &  type "C:\Windows\System32\calc.exe" > "PATH_TO_QBOT"
|DefDir = NULL
\IsShown = 0
```

II.Unpacked Core Qakbot

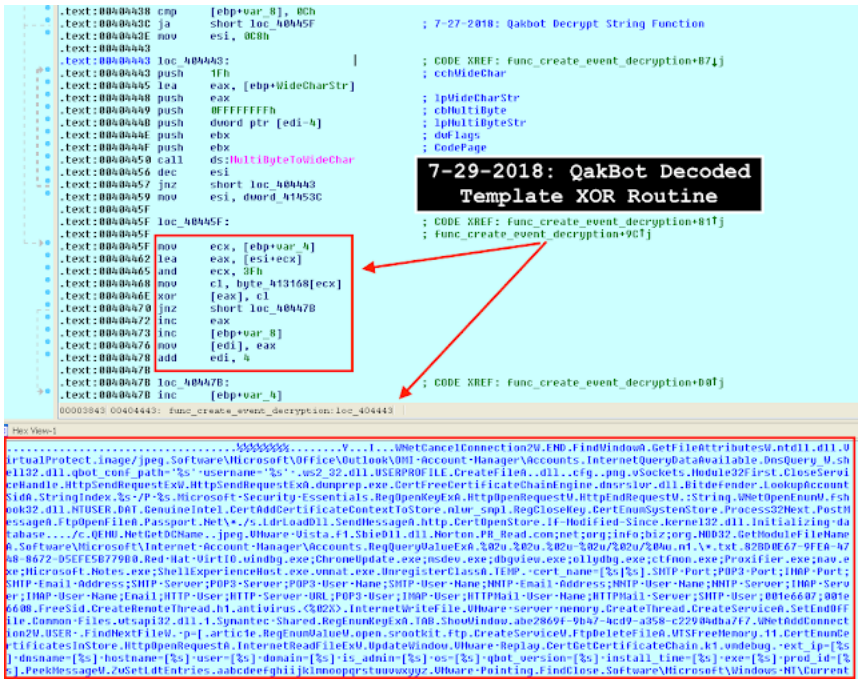
The unpacked core qbot, coded in Microsoft Visual C++, was compiled on January 29, 2018 06:25:49 with 9 imported DLL libraries with the five usual sections (.text -> .rsrc) with no anomalies. The coding style of Qakbot reveals heavy reliance of the developer on Ansi equivalent Microsoft API calls, which likely speaks to the older code base since most of the recent malware relies more on Unicode API equivalents. The bot primarily coordinates injection functions and control via IPC (inter-process communication) with named pipes.

The Qakbot code reveals a lot of functionality including its Domain Generation Algorithm with domain TLD ("com;net;org;info;biz;org"), which version was well-documented by Johannes Bader. The qbot also communicates via FTP with available credentials. The qbot checks the machine speed by downloading a sample via "https://cdn[.]speedof[.]me/sample4096k[.]bin?r=0.%u."

Notably, the malware also "relaxes" Windows Defender and disables in registry via “SubmitSamplesConsent" and alters "SpynetReporting."

A. QakBot Decryption XOR Routine

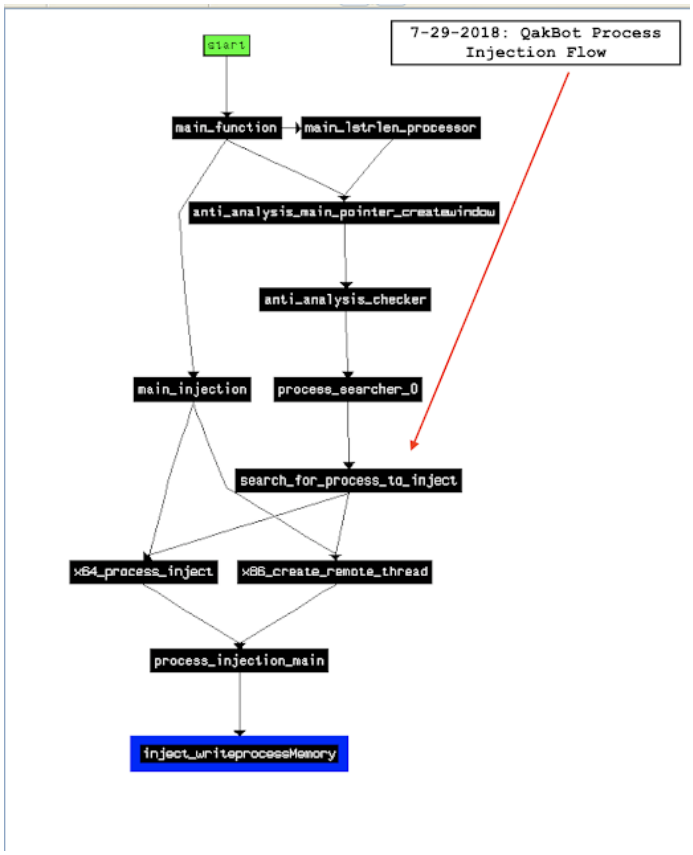
Once executed, however, Qakbot leverages XOR decryption function with & 0x3f coupled with Windows API call MultiByteToWideChar to convert byte to unicode strings while iterating through the encoded blob.



The pseudo-coded C++ template related to the main string deobfuscated is as follows:

```
if ( v14 )
     {
        WideCharStr = 0;
        decrypt_iterate_func(&v13, 0, 62);
        if ( v15 <= 12 )
       {
          v6 = 200;
          do
          {
            MultiByteToWideChar(0, 0, (LPCSTR)*(v5 - 1), -1, &WideCharStr, 31);
            --v6;
          }
          while ( v6 );
          v4 = (const CHAR *)dword_41453C; // location of encoded data
        }
      }
      v7 = &v4[v16];    // v16 = 0x2AA9u
      v8 = byte_413168[v16 & 0x3F];
      v9 = v8 == v4[v16];
      *v7 ^= v8;
      if ( v9 )
      {
        ++v15;
        *v5 = v7 + 1;
        ++v5;
      }
      ++v16;
```

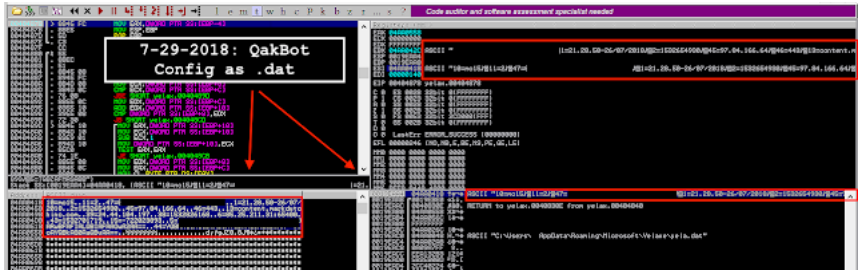
}III. "Explorer" Process Injection



The execution sequence is as follows injecting code into "explorer.exe" in both x86 and x64 variants:
start -> main_function -> main_injection -> x86_create_remote_thread/x64_process_inject -> process_injection_main -> inject_writeprocessMemory

IV. Qakbot Configuration

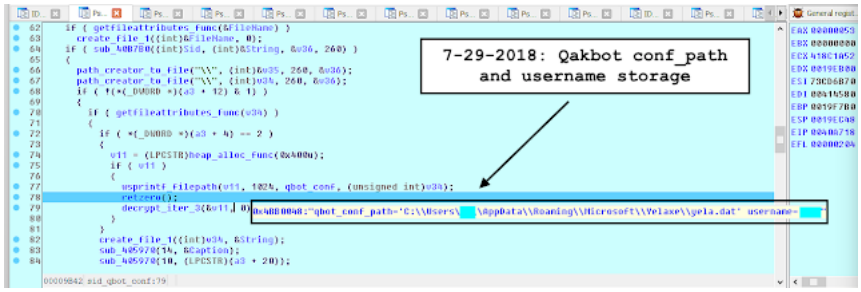
Qakbot configuration stored as .dat in %APPDATA% as numeric field values as follows:



The config is retrieved as follows via the following call chain:
start -> main_function -> GetDrive_type_func -> net_server_lookup_function -> anti-analysis -> trytoget_sid_user_as -> bot_config -> qbot_conf

Some of the notable Qakbot configurations details were noted by BAE Systems in 2016. It appears that the field "10" carries the unique name such as "mc15," which is a possible designation of the qbot botnet.

Qbot Configuration
10=mc15 (possible botnet name)
11=2 (number of hardcoded C2)
47=bot id as uppercase alphanumeric
1=date of qbot install in HH:MM:ss-dd/mm/yyyy
2=victim qbot install
45=C2 IP
46=C2 port
13=C2 domain
39=victim external IP
38=last victim call to C2 (time in Unix)
6=C2 IP:port
43=time of record ((time in Unix)
15=unknown
5=victim network shares
44=victim share credentials



The bot id generation function is as follows leveraging "ProductID" value in Registry, coupled with the output of GetComputerNameA and GetVolumeInformationA as follows:

```
v2 = lpString;
 *(_DWORD *)v14 = 0;
 nSize = 0;
 decrypt_iterate_func(lpString, 0, 256);
 v12 = 256;
 v11 = RegOpenKeyExA(-2147483646, SOFTWARE_path, 0, 131097, &lpString);
 if ( !v11 )
   v11 = RegQueryValueExA(lpString, ProductId, 0, 0, v2, &v12);
 RegCloseKey(lpString);
 if ( v11 )
   *(_WORD *)v2 = 48;
 nSize = 256 - lstrlenA(v2);
 v3 = lstrlenA(v2);
 GetComputerNameA((LPSTR)&v2[v3], &nSize);
 if ( !GetVolumeInformationA(&unk_411C48, &v9, 256, v14, 0, 0, &v10, 256) )
   *(_DWORD *)v14 = 0;
 v4 = v14[0];
 v5 = 256 - lstrlenA(v2);
 v6 = lstrlenA(v2);
 wsprintf_filepath(&v2[v6], v5, (int)"%u", v4);
 lstrcatA((LPSTR)v2, lpString2);
 nSize = lstrlenA(v2);
 CharUpperBuffA((LPSTR)v2, nSize);
```

Notably, the malware does not appear to store in the config file but rather uses the following config fields for FTP communication:

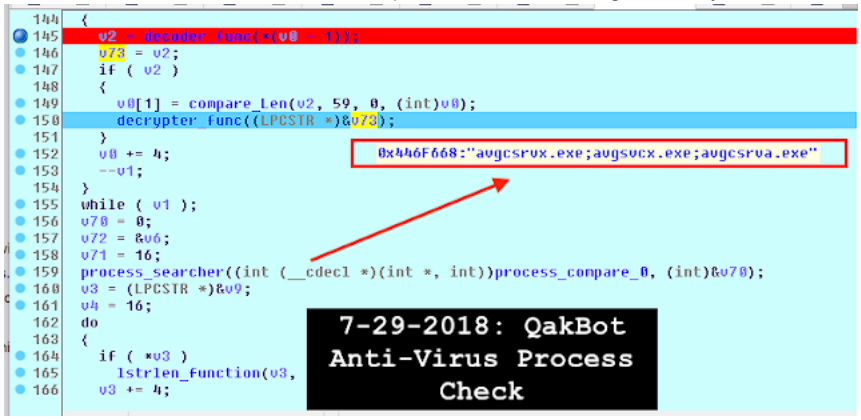
Qbot Additional Config
3=time of config (time in Unix)

22=ftp server1 with credential for C2 communications
23=ftp server2 with credential for C2 communications
24=ftp server3 with credential for C2 communications
25=ftp server4 with credential for C2 communications
26=ftp server5 with credential for C2 communications

The croncache is as follows:
12960;5;1532655973|15;8;1532722066|3;1;1532722258|4294967295;23;1532655912|300;13;1532722066|2736;3;1532701702|5;21;1532722066|

V. Qbot Anti-Analysis

The malware check for various anti-virus processes while running the binary.



- avgcsrvx.exe;avgsvcx.exe;avgcsrva.exe
- ccSvcHst.exe
- MsMpEng.exe
- mcshield.ex
- avp.exe
- egui.exe;ekrn.exe
- bdagent.exe;vsserv.exe;vsservppl.exe
- AvastSvc.exe
- coreServiceShell.exe;PccNTMon.exe;NTRTScan.exe.
- SAVAdminService.exe;SavService.exe
- fhoster32.exe
- WRSA.exe
- vkise.exe;isesrv.exe;cmdagent.exe
- ByteFence.exe
- MBAMService.exe
- fmon.exe

Additionally, the malware checks for a plethora of anti-analysis and anti-virtual machines. One of the techniques is used to compare CPUID. This instruction is executed with EAX=1 as input, the return value describes the processors features. The 31st bit of ECX on a physical machine will be equal to 0. On a guest VM it will equal to 1.

```
anti_VM_cpuid((int)&String1);
  _EAX = 1;
  __asm { cpuid }
  v16 = _ECX;
  return _ECX == 1 && !lstrcmpiA(&String1, GenuineIntel);
}
```

DLL (GetModuleHandleA):

- fshook32.dll (F-Secure)
- SbieDll.dll (Sandboxie)
- aswhookx.dll (Avasr)
- sf2.dll (Avst)
- dbghelp.dll
- avcuf32.dll (BitDefender)

For example,

```
BOOL check_as_dll()
{
  return dword_415934 & 0x82 && (GetModuleHandleA(aswhooka_dll) || GetModuleHandleA(aswhooks_dll));
}
```

Anti-Virus:

- Bitdefender
- Microsoft Security Essentials
- Norton
- NOD32
- Symantec
- mcafee
- kaspersky
- Avast
- Trend Micro

Filename check:

- mlwr_smpl
- antivirus
- srootkit (AVG)
- sample.exe
- sample

Anti-Virtual Machine:

- QEMU
- VMware
- vmdebug
- vmx_svga
- VirtIO
- RedHat
- vmacthlp.exe
- vmtoolsd.exe
- SVGA
- VMaudio
- vmrawdsk
- SCSI
- VBoxGuest
- vm3dmp
- vmxnet

Other:

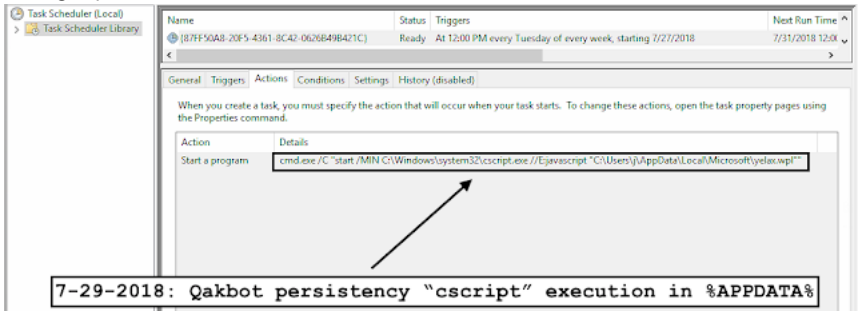
- windump.exe
- artifact.exe

Mutex Check:

_AVIRA_71855

VI. Persistency Mechanism

Qakbot sets run persistence via task scheduler as well as curious JavaScript execution via "cscript.exe //E:javascript" with the qbot loader file ending .wpl



VII. Yara Signatures

```
rule crimeware_win32_qbot_unpacked_core {
 meta:
 description = "Detects unpacked Qakbot core"
  author = "@VK_Intel"
  date = "2018-07-29"
  hash = "95ec8de64002fc5de7c04ceba04702da"
 strings:
  $s0 = "powershell.exe" fullword ascii
  $s1 = "%s\\%d.exe" fullword ascii
  $s2 = "%s\\system32\\" fullword ascii
  $s3 = "000223" fullword ascii
  $s5 = "000001" fullword ascii
  $s6 = "000111" fullword ascii
  $s7 = "000005" fullword ascii
  $s8 = "Akernel32" fullword ascii
  $s9 = "ipconfig netstat" fullword ascii
  $s10 = "Win32_Process" fullword ascii
  $s11 = "NtQuerySystemInformation" fullword ascii
 condition:
  uint16(0) == 0x5a4d and filesize < 500KB and all of them
}

rule crimeware_win32_qbot_communicatorDll {
 meta:
  description = "Detects Qakbot Communicator DLL"
  author = "@VK_Intel"
  date = "2018-07-29"
  hash = "7dad18c4d149849c727fe39eee184fe8"
 strings:
  $s0 = "powershell.exe" fullword ascii
  $s1 = "User-Agent: Microsoft-Windows/%u.%u UPnP/1.0" fullword ascii
  $s2 = "\\\\.\\pipe\\%ssp" fullword ascii
  $s3 = "http://www.ip-adress.com" fullword ascii
  $s4 = "%s\\%s.exe" fullword wide
  $s5 = "POST %s HTTP/%s" fullword ascii
  $s6 = "urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1" fullword ascii
  $s7 = "HOST: %s:1900" fullword ascii
  $s8 = "GetPortMappingNumberOfEntries" fullword ascii
  $s9 = "GetSpecificPortMappingEntry" fullword ascii
  $s10 = "%s\\tmp_%u.exe" fullword ascii
  $s11 = "GetConnectionTypeInfo" fullword ascii
  $s12 = "\\AppData\\LocalLow\\" fullword ascii
  $s13 = "%s\\~%s.tmp" fullword ascii
  $s14 = "%s\\system32\\" fullword ascii
 condition:
  uint16(0) == 0x5a4d and filesize < 200KB and 10 of them
}

rule crimeware_win64_qbot_injectedDll {
 meta:
  description = "Detects Qakbot Inject DLL"
  author = "@VK_Intel"
  date = "2018-07-29"
  hash = "03e78339b09aa5e9885c24b2e8af84f4"
 strings:
  $s0 = "chrome.dll" fullword ascii
  $s1 = "\\\\.\\pipe\\%ssp" fullword ascii
  $s2 = "content-security-policy-report-only" fullword ascii
  $s3 = "\\AppData\\LocalLow\\" fullword ascii
  $s4 = "content-security-policy" fullword ascii
  $s5 = "cookie=[" fullword ascii
  $s6 = "referer=[" fullword ascii
  $s7 = "X-Frame-Options" fullword ascii
  $s8 = "user.js" fullword wide

  $op0 = { e8 99 b0 00 00 44 8b 5d c4 44 01 5b 18 41 80 3e }
  $op1 = { e8 f1 ec ff ff 48 89 84 24 98 }
  $op2 = { 48 8b 53 28 48 8b c8 e8 ca 6a 00 00 eb 03 41 8b }
 condition:
  uint16(0) == 0x5a4d and filesize < 421KB and all of ($s*) and 1 of ($op*)
}
```

VIII. Indicators of Compromise (IOCs)

A. The observed list of C2 servers

66.189.228[.]49;0;995
70.169.12[.]141;0;443
150.200.247[.]87;0;443
71.77.22[.]206;0;443
76.73.202[.]82;0;443
74.88.210[.]56;0;995
97.97.160[.]42;0;443
146.135.9[.]64;0;443
71.190.202[.]120;0;443
47.223.85[.]33;0;443
98.26.2[.]182;0;443
50.111.32[.]211;0;443
68.207.33[.]232;0;2222
68.173.55[.]51;0;443
76.186.82[.]51;0;443
67.197.104[.]90;0;443
73.40.24[.]158;0;443
50.42.189[.]206;0;993
65.116.179[.]83;0;443
50.32.243[.]36;0;443
185.219.83[.]73;0;443
72.133.105[.]155;0;443
216.201.159[.]118;0;443
68.207.43[.]173;0;443
216.218.74[.]196;0;443
96.248.15[.]254;0;995
75.189.235[.]216;0;443
98.103.2[.]226;0;443
24.100.46[.]201;0;2222
24.11.50[.]136;0;443
75.109.193[.]173;0;2087
73.106.122[.]121;0;443
173.160.3[.]209;0;443
70.118.18[.]242;0;443
24.163.66[.]146;0;443
173.248.24[.]230;0;443
68.129.231[.]84;0;443
174.48.72[.]160;0;443
216.93.143[.]182;0;995
184.180.157[.]203;0;2222
68.49.120[.]179;0;443
75.109.193[.]173;0;1194
75.109.193[.]173;0;8443
98.16.70[.]197;0;2222
47.134.236[.]166;0;443
105.227.20[.]203;0;443
97.70.129[.]250;0;443
24.228.185[.]224;0;2222
72.174.25[.]139;0;443
24.209.137[.]134;0;443
98.225.141[.]232;0;443
67.197.97[.]144;0;443
173.81.42[.]136;0;21
24.155.191[.]156;0;995
97.84.210[.]38;0;2222
93.108.180[.]227;0;443
190.185.219[.]110;0;443
63.79.135[.]0;0;443
96.73.55[.]193;0;993
207.178.109[.]161;0;443
99.197.182[.]183;0;443
67.83.122[.]112;0;2222
50.198.141[.]161;0;2078
47.40.29[.]239;0;443
12.2.201[.]35;0;443
76.176.7[.]41;0;443
75.127.141[.]50;0;995
71.210.153[.]133;0;443
189.175.147[.]195;0;443
73.231.147[.]128;0;443
73.130.229[.]200;0;443
67.11.27[.]100;0;443
12.196.116[.]242;0;443
216.21.168[.]27;0;32101
24.6.31[.]163;0;443
216.21.168[.]27;0;995
96.40.85[.]72;0;443
69.129.12[.]186;0;21
71.172.250[.]114;0;443
73.152.213[.]187;0;80
68.226.136[.]96;0;443
71.222.141[.]81;0;61200
76.182.33[.]43;0;2222

```
24.180.160[.]192;0;443
173.160.3[.]209;0;995
97.70.85[.]248;0;443
24.180.246[.]147;0;443
173.70.44[.]171;0;443
216.21.168[.]27;0;50000
24.180.246[.]147;0;443
96.32.171[.]132;0;443
47.48.236[.]98;0;2222
70.182.79[.]66;0;443
173.80.75[.]177;0;443
24.141.179[.]121;0;443
204.85.12[.]25;0;443
24.175.103[.]122;0;995
24.252.80[.]93;0;443
68.206.135[.]146;0;443
184.174.166[.]107;0;443
71.33.192[.]23;0;995
24.190.226[.]234;0;443
71.10.155[.]97;0;443
24.180.246[.]147;0;443
181.93.205[.]181;0;443
207.243.48[.]26;0;443
68.113.142[.]24;0;465
72.193.162[.]108;0;443
68.59.209[.]183;0;995
98.243.166[.]148;0;443
72.179.39[.]89;0;443
67.76.37[.]105;0;443
174.109.117[.]152;0;443
73.52.101[.]153;0;80
70.21.182[.]149;0;2222
24.180.246[.]147;0;443
65.191.74[.]248;0;443
65.40.207[.]151;0;995
73.183.145[.]218;0;2222
209.213.24[.]194;0;443
68.207.33[.]242;0;443
172.87.188[.]2;0;443
65.132.30[.]18;0;443
104.153.240[.]6;0;2222
24.93.104[.]154;0;443
75.106.233[.]194;0;443
65.191.128[.]99;0;443
65.169.66[.]123;0;2222
71.172.250[.]114;0;443
67.55.174[.]194;0;443
107.15.153[.]110;0;8443
205.169.108[.]194;0;443
47.221.46[.]163;0;443
71.48.218[.]91;0;995
73.74.72[.]141;0;443
71.85.72[.]9;0;443
172.164.17[.]102;0;443
173.191.238[.]124;0;995
47.186.93[.]228;0;443
184.191.61[.]13;0;32100
209.180.154[.]97;0;995
68.133.47[.]150;0;443
75.189.239[.]153;0;443
204.85.12[.]26;0;443
76.101.165[.]66;0;443
97.84.166[.]64;0;443
72.133.75[.]134;0;443
68.207.45[.]236;0;443
104.153.240[.]6;0;2222
206.67.215[.]7;0;443
206.67.215[.]7;0;443
```

B. Qbot Configuration

```
10=mc15
11=2
47=REDACTED
1=REDACTED
2=REDACTED
45=97.84.166[.]64
46=443
13=content[.]markdutchinc[.]com
39=REDACTED
38=REDACTED
6=85.25.211[.]31:65400
43=REDACTED
15=-722023893
5=REDACTED
44=REDACTED
3=REDACTED
22=37.60.244[.]211:backup_manager@garciasdrywall[.]com:REDACTED:
23=198.38.77[.]162:backup_manager@worldexpresscargo[.]com:REDACTED:
24=61.221.12[.]26:logger@ostergift[.]com:REDACTED:
25=67.222.137[.]18:logger@grupocrepusculo[.]net:REDACTED:
26=107.6.152[.]61:logger@trussedup[.]com:REDACTED:
```

IX. Appendix: Full Decoded First-Layer Template

```
WNetCancelConnection2W
END
FindWindowA
GetFileAttributesW
ntdll.dll
VirtualProtect
image/jpeg
Software\Microsoft\Office\Outlook\OMI
Account
Manager\Accounts
InternetQueryDataAvailable
DnsQuery_W
shell32.dll
qbot_conf_path='%s'
username='%s'
ws2_32.dll
USERPROFILE
CreateFileA
.dll
.cfg
.png
vSockets
Module32First
CloseServiceHandle
HttpSendRequestExW
HttpSendRequestExA
dumprep.exe
CertFreeCertificateChainEngine
dnsrslvr.dll
Bitdefender
LookupAccountSidA
StringIndex
%s
/P
%s
Microsoft
Security
Essentials
RegOpenKeyExA
HttpOpenRequestW
HttpEndRequestW
:String
WNetOpenEnumW
fshook32.dll
NTUSER.DAT
GenuineIntel
CertAddCertificateContextToStore
mlwr_smpl
RegCloseKey
CertEnumSystemStore
Process32Next
PostMessageA
FtpOpenFileA
Passport.Net\*
/s
LdrLoadDll
SendMessageA
http
CertOpenStore
If-Modified-Since
kernel32.dll
Initializing
database...
/c
QEMU
NetGetDCName
.jpeg
VMware
Vista
f1
SbieDll.dll
Norton
PR_Read
com;net;org;info;biz;org
NOD32
GetModuleFileNameA
Software\Microsoft\Internet
Account
Manager\Accounts
RegQueryValueExA
%02u.%02u.%02u-%02u/%02u/%04u
m1
\*.txt
```

```
82BD0E67-9FEA-4748-8672-D5EFE5B779B0
Red
Hat
VirtIO
windbg.exe;ChromeUpdate.exe;msdev.exe;dbgview.exe;ollydbg.exe;ctfmon.exe;Proxifier.exe;nav.exe;Microsoft.Notes.exe;ShellExperienceHc

vmnat.exe
UnregisterClassA
TEMP
cert_name=[%s|%s]
SMTP
Port;POP3
Port;IMAP
Port;SMTP
Email
Address;SMTP
Server;POP3
Server;POP3
User
Name;SMTP
User
Name;NNTP
Email
Address;NNTP
User
Name;NNTP
Server;IMAP
Server;IMAP
User
Name;Email;HTTP
User;HTTP
Server
URL;POP3
User;IMAP
User;HTTPMail
User
Name;HTTPMail
Server;SMTP
User;001e6607;001e6608
FreeSid
CreateRemoteThread
h1
antivirus
<%02X>
InternetWriteFile
VMware
server
memory
CreateThread
CreateServiceA
SetEndOfFile
Common
Files
wtsapi32.dll
1
Symantec
Shared
RegEnumKeyExA
TAB
ShowWindow
abe2869f-9b47-4cd9-a358-c22904dba7f7
WNetAddConnection2W
USER
FindNextFileW
p=[
artic1e
RegEnumValueW
open
srootkit
ftp
CreateServiceW
FtpDeleteFileA
WTSFreeMemory
11
CertEnumCertificatesInStore
HttpOpenRequestA
InternetReadFileExW
UpdateWindow
VMware
Replay
CertGetCertificateChain
k1
vmdebug
```

```
ext_ip=[%s]
dnsname=[%s]
hostname=[%s]
user=[%s]
domain=[%s]
is_admin=[%s]
os=[%s]
qbot_version=[%s]
install_time=[%s]
exe=[%s]
prod_id=[%s]
PeekMessageW
ZwSetLdtEntries
aabcdeefghiijklmnoopqrstuuvwxyyz
VMware
Pointing
FindClose
Software\Microsoft\Windows
NT\CurrentVersion\Windows
Messaging
Subsystem\Profiles
facebook.com/login.php
vmx_svga
mcafee
DestroyWindow
abc
Microsoft
vmacthlp.exe
GetLastError
ReadProcessMemory
ZwQueryInformationThread
k2
Mozilla/5.0
(Windows
NT
6.1;
rv:54.0)
Gecko/20100101
Firefox/54.0
2
InternetGetLastResponseInfoA
APPDATA
RegEnumValueA
dnsapi.dll
VirtualFreeEx
WindowsLive:name=*
ExpandEnvironmentStringsA
CreateDirectoryA
WTSQueryUserToken
cookie=[%s]
WSAConnect
i1
kb
WTSEnumerateSessionsA
PR_Close
DisplayName
Remote
Procedure
Call
(RPC)
Service
kaspersky
WSASetLastError
sample.exe
vmtoolsd.exe
FindNextFileA
ZwQuerySystemInformation
crypt32.dll
CertAddCRLContextToStore
InternetOpenUrlA
SOFTWARE\Microsoft\Windows
NT\CurrentVersion
HOME
netapi32.dll
CertGetEnhancedKeyUsage
WriteFile
https://cdn.speedof.me/sample4096k.bin?r=0.%u
CredEnumerateW
CreateWindowExA
\Cookies
*.*
advapi32.dll
WaitForSingleObject
```

```
InternetCrackUrlA
%u.%u.%u.%u
000
FindFirstFileA
wpl
url=[%s]
user=[%s]
pass=[%s]
InternetOpenA
POP3
Password;IMAP
Password;NNTP
Password;HTTPMail
Password;SMTP
Password;POP3
Password2;IMAP
Password2;NNTP
Password2;HTTPMail
Password2;SMTP
Password2
.swf
Avast
MiniDumpWriteDump
CertCloseStore
DeleteFileA
\Application
Data\Macromedia\Flash
Player\#SharedObjects
GetExitCodeProcess
RegSetValueExA
cmd.exe
artifact.exe
rsaenh.dll
.css
nspr4.dll
NetShareEnum
RegQueryInfoKeyA
RegCreateKeyExA
sbtisht
PFXExportCertStore
WSAStartup
If-None-Match
VirtualProtectEx
CertSetCertificateContextProperty
WSACleanup
_qbot
]
b=[
220d5cc1
vmscsi
CreateFileW
connect
LOCALAPPDATA
at.exe
%u:%u
"%s"
/I
AllocateAndInitializeSid
url=[%s]
VMware
VMaudio
i2
image/pjpeg
%H.%M.%S-%d/%m/%Y
dwwin.exe
CryptAcquireCertificatePrivateKey
w1
c1
aswhookx.dll
host=[%s:%u]
user=[%s]
pass=[%s]
AVG
siteadvisor.com;avgthreatlabs.com;safeweb.norton.com
very
big
postdata
%u
bytes
CredEnumerateA
HttpQueryInfoW
VMware
SVGA
```

```
1234567890
InternetReadFileExA
InternetConnectA
Software\Microsoft\Internet
Explorer\IntelliForms\Storage2
CertCreateCertificateChainEngine
SetCurrentDirectoryA
TE
Trend
Micro
vmrawdsk
.gif
CredFree
CreateToolhelp32Snapshot
Process32First
explorer.exe
ChromeUpdate.exe
DeleteService
Cookie:
dwErr=%u
szOldRunMutex='%s'
username='%s'
CertGetCRLContextProperty
AdjustTokenPrivileges
aswhooka.dll
GetCurrentProcessId
SetFilePointer
dwErr=%u
qbot_run_mutex='%s'
username='%s'
InternetOpenW
CharToOemBuffA
PR_SetError
9
wininet.dll
security
NetUserEnum
ZwResumeThread
t=%s
time=[%02d:%02d:%02d-%02d/%02d/%d]
HttpAddRequestHeadersA
mpr.dll
StartServiceA
VBoxVideo
runas
uno
InternetQueryOptionA
OpenProcess
Norton
Internet
Security
application/x-shockwave-flash
ProductId
WNetCloseEnum
OpenThread
%%%02X
https://
iphlpapi.dll
aaebcdeeifghiiojklmnooupqrstuuyvwxyyaz
DELETE
]
cookie_data=[
HttpQueryInfoA
data=[%s]
DeleteUrlCacheEntryW
CertGetNameStringW
InterlockedCompareExchange
InternetSetOptionA
e161255a
nss3.dll
windump.exe
Dnscache
CreateProcessW
CryptUnprotectData
GetClipboardData
svchost.exe
WSAGetLastError
OpenSCManagerW
abcdefghijklmnopqrstuvwxyz
Module32Next
.exe
CertFreeCertificateChain
s2
```

```
CryptFindOIDInfo
DeleteServiceW
Virtual
HD
.ani
.ico
ResumeThread
PostQuitMessage
InternetSetStatusCallback
cnn.com;microsoft.com;baidu.com;facebook.com;yahoo.com;wikipedia.org;qq.com;linkedin.com;mail.ru
GetForegroundWindow
220d5cd0
VirtualAllocEx
InternetReadFile
VMware
SCSI
LocalFree
GetCurrentThreadId
Query_Main
url=[%s]
data=[%s]
3
\sf2.dll
GetProcAddress
PASS
GetExitCodeThread
DispatchMessageA
0123456789
CryptEnumOIDInfo
iedw.exe
CertFreeCRLContext
RIGHT
user_pref("network.http.spdy.enabled.http2",
false);
CloseHandle
comet.yahoo.com;.hiro.tv;safebrowsing.google.com;geo.query.yahoo.com;googleusercontent.com;salesforce.com;officeapps.live.com;storag
optimizer.com;.adworldmedia.com;seekmo.com;r777r.info;sipuku.com;eorezo.com;newasp.com.cn;wpzkq.com;radialpoint.com;owlforce.com;.mi
services.com;zynga.com;.5min.com;netflix.com;tubemogul.com;youtube.com;brightcove.com;mochibot.com;fwmrm.net;mendeley.com
PR_OpenTCPSocket
PR_GetNameForIdentity
avcuf32.dll
mutex
_AVIRA_71855
CreateProcessA
referer=[%s]
&dump=
PROGRAMFILES
ReadFile
GetMessageW
dbghelp.dll
h3
InternetGetCookieA
HttpSendRequestA
FtpGetFileA
.jpg
StartServiceW
cert_data=[
%s_%s_%u.zip
SetLastError
.js?
GetCurrentDirectoryA
cookie_name=[
ansfltr
DnsQuery_A
CertFreeCertificateContext
ProfileImagePath
u1
LEFT
NetApiBufferFree
*/*
PeekMessageA
metsvc-server.exe
time=[%d:%d:%d-%d/%d/%d]
ex_code=0x%08x
ex_addr=0x%p
ex_module=[%s]
ex_module_base=0x%p
nick=[%s]
th_args=[%08x]
th_flags=[0x%08x]
qbot_version=[%s]
WriteProcessMemory
CertAddCTLContextToStore
```

```
ProgramFiles(x86)
5e7e8100
sample
Software\Microsoft\Windows\CurrentVersion\Uninstall
InternetGetCookieExA
Software\\Microsoft\\Windows\\CurrentVersion\\Internet
Settings\\Zones\\
%s%s/dupinst.php?n=%s&bg=%s&r=%u
SetEntriesInAclA
ESCAPE
CPExportKey
ShellExecuteA
https
]
t=[
send
FindFirstFileW
TranslateMessage
AVAST
Software
cryptui.dll
MessageBoxA
rsabase.dll
OpenSCManagerA
WSASend
VMware
Accelerated
8
%%%02x
WNetEnumResourceW
PR_Write
GetMessageA
InternetQueryOptionW
Avast
Global
VMAUDIO
ObtainUserAgentString
urlmon.dll
DefWindowProcA
StackWalk64
DnsQueryExW
PStoreCreateInstance
h2
InternetCloseHandle
cmd
/c
ping
-n
10
localhost
&&
rmdir
/S
/Q
"%s"
RegisterClassExA
DnsQueryExA
i3
RegDeleteValueA
PR_GetError
GetUrlCacheEntryInfoA
10
MoveFileA
NetWkstaGetInfo
HttpEndRequestA
crashdata=
ZwReadFile
HttpSendRequestW
CWSandbox
treasurygateway;ecash.arvest.com;.ntrs.com;tdcommercialbanking.com;olb-
ebanking.com;webinfoplus.mandtbank.com;accessmoneymanager.com;commerceconnections.commercebank.com;schwabinstitutional.com;intellix.
access.com;nj00-wcm;commercial.bnc.ca;/clkccm/;paylinks.cunet.org;e-
facts.org;accessonline.abnamro.com;providentnjolb.com;firstmeritib.com;corporatebanking;firstmeritib.com/defaultcorp.aspx;e-
moneyger.com;jsp/mainWeb.jsp;svbconnect.com;premierview.membersunited.org;each.bremer.com;iris.sovereignbank.com;/wires/;paylinks.cu
eb.ibanking-services.com;cashproonline.bankofamerica.com;/cashplus/;ebanking-services.com;/cashman/;web-cashplus.com;treas-
mgt.frostbank.com;business-eb.ibanking-
services.com;treasury.pncbank.com;access.jpmorgan.com;tssportal.jpmorgan.com;ktt.key.com;onlineserv/CM;premierview.membersunited.org
achweb.bankofamerica.com;businessaccess.citibank.citigroup.com;businessonline.huntington.com;/cmserver/;goldleafach.com;iachwellspro

pstorec.dll
VBoxGuest
wpq
ivm-inject.dll
```

```
GetModuleHandleA
BACKSP
url=[%s]
lb=[%s]
data=[%s]
PR_Poll
vm3dmp
vmxnet
norton
GetUrlCacheEntryInfoW
.lnk
user32.dll
.js
LdrGetProcedureAddress
SetNamedSecurityInfoA
GetFileAttributesA
LoadLibraryA
Basic
CertDuplicateCRLContext
Software\Microsoft\Windows
Messaging
Subsystem
image/gif
GetVolumeInformationA
SOFTWARE\Microsoft\Windows
NT\CurrentVersion\ProfileList
b9819c52
```