[QuickNote] Qakbot 5.0 – Decrypt strings and configuration

Published: 2024-04-24 · Archived: 2026-04-05 15:50:14 UTC

In this new sample, threat actor has updated Qakbot's codebase to support 64-bit versions of Windows.

Here is the pseudocode for the string decryption functions in the 64-bit and 32-bit versions:

As the pictures show, the decryption process in the 64-bit version is similar to the previous version. However, the difference is that the `xor_key_blob` in this new version has been encrypted. Therefore, before performing the decryption to the original string, it will call the `qbot_decrypt_xor_key_blob` function (`0x180011504`) which I have circled in red above to decrypt the original `xor_key_blob` .

(1) Calculates the `SHA256` hash for the blob data at addresses `0x180029700 (0x9F bytes)` and `0x180028150 (0x63 bytes)` and uses the calculated hash values as the `AES Key` .

(2) The first `16 bytes` of the `enc_xor_key_blob` at addresses `0x18002AFE0 (0xA0 bytes)` and `0x1800281C0 (0xD0 bytes)` are used as the `AES IV` :

(3) Decrypts the encrypted blob data (*except for the first 16 bytes used as* `AES IV`) using AES in `CBC` mode. The result is the `xor_key_blob` used to decrypt the strings.

With the decrypted `xor_key_blob` above, we can completely write an idapython script to decrypt the strings and add comments related to the decrypted strings to facilitate the analysis of Qakbot code.

Here is my idapython script (*Don't blame my code if you don't want your eyes to bleed* :), *just wanted to share it in case someone need to use it for reference.*)

```
[+] Decrypt all strings with index boundary is 0x1836
index: 0x0, decrypted string: %SystemRoot%\SysWOW64\xwizard.exe
index: 0x22, decrypted string: .dat
index: 0x27, decrypted string: kernelbase.dll
index: 0x36, decrypted string: WBJ_IGNORE
index: 0x41, decrypted string: mpr.dll
index: 0x49, decrypted string: %SystemRoot%\explorer.exe
index: 0x63, decrypted string: %SystemRoot%\System32\CertEnrollCtrl.exe
index: 0x8c, decrypted string: https
index: 0x92, decrypted string: SentinelServiceHost.exe;SentinelStaticEngine.exe;SentinelAgent.exe;Se
index: 0x104, decrypted string: open
index: 0x109, decrypted string: root\SecurityCenter2
index: 0x11e, decrypted string: %SystemRoot%\SysWOW64\SndVol.exe
index: 0x13f, decrypted string: %u.%u.%u.%u.%u.%u.%04x
index: 0x156, decrypted string: 1234567890
index: 0x161, decrypted string: %SystemRoot%\System32\Utilman.exe
index: 0x183, decrypted string: snxhk_border_mywnd
```

```
index: 0x196, decrypted string: %SystemRoot%\SysWOW64\wextract.exe
index: 0x1b9, decrypted string: avgcsrvx.exe;avgsvcx.exe;avgcsrva.exe
index: 0x1df, decrypted string: Win32_PhysicalMemory
index: 0x1f4, decrypted string: Caption
index: 0x1fc, decrypted string: ByteFence.exe
index: 0x20a, decrypted string: aswhooka.dll
index: 0x217, decrypted string: dwengine.exe;dwarkdaemon.exe;dwwatcher.exe
index: 0x242, decrypted string: %SystemRoot%\SysWOW64\grpconv.exe
index: 0x264, decrypted string: VRTUAL;VMware;VMW;Xen
index: 0x27a, decrypted string: SELECT * FROM AntiVirusProduct
index: 0x299, decrypted string: %s\%08X.dll
index: 0x2a5, decrypted string: wininet.dll
index: 0x2b1, decrypted string: avp.exe;kavtray.exe
index: 0x2c5, decrypted string: rundll32.exe
index: 0x2d3, decrypted string: Create
index: 0x2da, decrypted string: WQL
index: 0x2de, decrypted string: %SystemRoot%\System32\sethc.exe
index: 0x2fe, decrypted string: AvastSvc.exe;aswEngSrv.exe;aswToolsSvc.exe;afwServ.exe;aswidsagent.e
index: 0x351, decrypted string: Software\Classes
index: 0x362, decrypted string: vkise.exe;isesrv.exe;cmdagent.exe
index: 0x384, decrypted string: LastBootUpTime
index: 0x393, decrypted string: MS_VM_CERT;VMware;Virtual Machine
index: 0x3b5, decrypted string: Winsta0
index: 0x3bd, decrypted string: .dll
index: 0x3c2, decrypted string: Caption,Description,DeviceID,Manufacturer,Name,PNPDeviceID,Service,S
index: 0x40c, decrypted string: SonicWallClientProtectionService.exe;SWDash.exe
index: 0x43c, decrypted string: t=%s time=[%02d:%02d:%02d-%02d/%02d/%d]
index: 0x464, decrypted string: SystemRoot
index: 0x46f, decrypted string: CommandLine
index: 0x47b, decrypted string: %SystemRoot%\SysWOW64\explorer.exe
index: 0x49e, decrypted string: SOFTWARE\Wow6432Node\Microsoft AntiMalware\SpyNet
index: 0x4d0, decrypted string: %s\system32\
index: 0x4dd, decrypted string: SELECT * FROM Win32_OperatingSystem
index: 0x501, decrypted string: wbj.go
index: 0x508, decrypted string: System32
index: 0x511, decrypted string: CynetEPS.exe;CynetMS.exe;CynetConsole.exe
index: 0x53b, decrypted string: C:\INTERNAL\__empty
index: 0x54f, decrypted string: cmd.exe
index: 0x557, decrypted string: SOFTWARE\Microsoft\Windows\CurrentVersion\Run
index: 0x585, decrypted string: */*
index: 0x589, decrypted string: MsMpEng.exe
index: 0x595, decrypted string: image/pjpeg
index: 0x5a1, decrypted string: {%02X%02X%02X%02X-%02X%02X-%02X%02X-%02X%02X-%02X%02X%02X%02X%02X%02
index: 0x5e8, decrypted string: urlmon.dll
index: 0x5f3, decrypted string: type=0x%04X
index: 0x5ff, decrypted string: TRUE
index: 0x604, decrypted string: Win32_ComputerSystem
```

```
index: 0x619, decrypted string: %SystemRoot%\System32\backgroundTaskHost.exe
index: 0x646, decrypted string: ALLUSERSPROFILE
index: 0x656, decrypted string: .exe
index: 0x65b, decrypted string: \\.\pipe\
index: 0x665, decrypted string: advapi32.dll
index: 0x672, decrypted string: application/x-shockwave-flash
index: 0x690, decrypted string: %ProgramFiles%\Windows Media Player\wmplayer.exe
index: 0x6c1, decrypted string: ntdll.dll
index: 0x6cb, decrypted string: %SystemRoot%\SysWOW64\Utilman.exe
index: 0x6ed, decrypted string: CfGetPlatformInfo
index: 0x6ff, decrypted string: userenv.dll
index: 0x70b, decrypted string: LocalLow
index: 0x714, decrypted string: FALSE
index: 0x71a, decrypted string: coreServiceShell.exe;PccNTMon.exe;NTRTScan.exe
index: 0x749, decrypted string: Sophos UI.exe;SophosUI.exe;SAVAdminService.exe;SavService.exe
index: 0x787, decrypted string: image/jpeg
index: 0x792, decrypted string: image/gif
index: 0x79c, decrypted string: displayName
index: 0x7a8, decrypted string: Name
index: 0x7ad, decrypted string: Win32_PnPEntity
index: 0x7bd, decrypted string: .cfg
index: 0x7c2, decrypted string: APPDATA
index: 0x7ca, decrypted string: winsta0\default
index: 0x7da, decrypted string: %SystemRoot%\SysWOW64\CertEnrollCtrl.exe
index: 0x803, decrypted string: %SystemRoot%\SysWOW64\backgroundTaskHost.exe
index: 0x830, decrypted string: pstorec.dll
index: 0x83c, decrypted string: RepUx.exe
index: 0x846, decrypted string: aaebcdeeifghiiojklmnooupqrstuuyvwxyyaz
index: 0x86d, decrypted string: \sf2.dll
index: 0x876, decrypted string: %SystemRoot%\System32\dxdiag.exe
index: 0x897, decrypted string: CSFalconService.exe;CSFalconContainer.exe
index: 0x8c1, decrypted string: vbs
index: 0x8c5, decrypted string: WRSA.exe
index: 0x8ce, decrypted string: crypt32.dll
index: 0x8da, decrypted string: setupapi.dll
index: 0x8e7, decrypted string: c:\saurufdifsdudqat.sys
index: 0x8ff, decrypted string: %ProgramFiles(x86)%\Windows Media Player\wmplayer.exe
index: 0x935, decrypted string: netapi32.dll
index: 0x942, decrypted string: SOFTWARE\Microsoft\Microsoft Antimalware\Exclusions\Paths
index: 0x97c, decrypted string: VMware;PROD_VIRTUAL_DISK;VIRTUAL-DISK;XENSRC;20202020
index: 0x9b2, decrypted string: %SystemRoot%\System32\grpconv.exe
index: 0x9d4, decrypted string: SpyNetReporting
index: 0x9e4, decrypted string: wtsapi32.dll
index: 0x9f1, decrypted string: wpcap.dll
index: 0x9fb, decrypted string: Packages
index: 0xa04, decrypted string: %SystemRoot%\explorer.exe
index: 0xa1e, decrypted string: regsvr32.exe
```

```
index: 0xa2c, decrypted string: aswhookx.dll
index: 0xa39, decrypted string: Content-Type: application/x-www-form-urlencoded
index: 0xa69, decrypted string: %SystemRoot%\SysWOW64\SearchIndexer.exe
index: 0xa91, decrypted string: %SystemRoot%\SysWOW64\AtBroker.exe
index: 0xab4, decrypted string: %SystemRoot%\System32\WerFault.exe
index: 0xad7, decrypted string: SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths
index: 0xb0c, decrypted string: vmnat.exe
index: 0xb16, decrypted string: SubmitSamplesConsent
index: 0xb2b, decrypted string: SysWOW64
index: 0xb34, decrypted string: shell32.dll
index: 0xb40, decrypted string: wmic process call create 'expand "%S" "%S"'

index: 0xb6d, decrypted string: ROOT\CIMV2
index: 0xb78, decrypted string: Win32_Product
index: 0xb86, decrypted string: LOCALAPPDATA
index: 0xb93, decrypted string: %SystemRoot%\SysWOW64\mobsync.exe
index: 0xbb5, decrypted string: ws2_32.dll
index: 0xbc0, decrypted string: WScript.Sleep %u
Set objWMIService = GetObject("winmgmts:" & "{impersonationLevel=impersonate}!\\.\%coot\cimv2")
Set objProcess = GetObject("winmgmts:root\cimv2:Win32_Process")
errReturn = objProcess.Create("%s", null, nul, nul)
WScript.Sleep 2000
Set fso = CreateObject("Scripting.FileSystemObject")
fso.DeleteFile("%s")
index: 0xd02, decrypted string: bcrypt.dll
index: 0xd0d, decrypted string: SOFTWARE\Wow6432Node\Microsoft\Windows Defender\Spynet
index: 0xd44, decrypted string: abcdefghijklmnopqrstuvwxyz
index: 0xd5f, decrypted string: fshoster32.exe
index: 0xd6e, decrypted string: %SystemRoot%\System32\SearchIndexer.exe
index: 0xd96, decrypted string: reg.exe ADD "HKLM\%s" /f /t %s /v "%s" /d "%s"
index: 0xdc5, decrypted string: Set objWMIService = GetObject("winmgmts:" & "{impersonationLevel=impe
Set objProcess = GetObject("winmgmts:root\cimv2:Win32_Process")
errReturn = objProcess.Create("%s", null, nul, nul)
index: 0xe99, decrypted string: gdi32.dll
index: 0xea3, decrypted string: Set objWMIService = GetObject("winmgmts:" & "{impersonationLevel=impe
Set colFiles = objWMIService.ExecQuery("Select * From CIM_DataFile Where Name = '%s'")
For Each objFile in colFiles
objFile.Copy("%s")
Next
index: 0xf8f, decrypted string: Win32_Process
index: 0xf9d, decrypted string: SELECT * FROM Win32_Processor
index: 0xfbb, decrypted string: user32.dll
index: 0xfc6, decrypted string: Win32_Bios
index: 0xfd1, decrypted string: %SystemRoot%\SysWOW64\explorer.exe
index: 0xff4, decrypted string: MBAMService.exe;mbamgui.exe
index: 0x1010, decrypted string: %SystemRoot%\SysWOW64\mspaint.exe
index: 0x1032, decrypted string: frida-winjector-helper-32.exe;frida-winjector-helper-64.exe;tcpdump
```

```
index: 0x12f8, decrypted string: %SystemRoot%\System32\wextract.exe
index: 0x131b, decrypted string: egui.exe;ekrn.exe
index: 0x132d, decrypted string: select
index: 0x1335, decrypted string: %SystemRoot%\System32\wermgr.exe
index: 0x1356, decrypted string: iphlpapi.dll
index: 0x1363, decrypted string: SOFTWARE\Microsoft\Windows Defender\SpyNet
index: 0x138e, decrypted string: %SystemRoot%\SysWOW64\dxdiag.exe
index: 0x13af, decrypted string: %SystemRoot%\SysWOW64\WerFault.exe
index: 0x13d2, decrypted string: %SystemRoot%\System32\AtBroker.exe
index: 0x13f5, decrypted string: %SystemRoot%\SysWOW64\sethc.exe
index: 0x1415, decrypted string: %S.%06d
index: 0x141d, decrypted string: c:\\
index: 0x1422, decrypted string: S:(ML;;NW;;;LW)
index: 0x1432, decrypted string: fmon.exe
index: 0x143b, decrypted string: %SystemRoot%\System32\xwizard.exe
index: 0x145d, decrypted string: cscript.exe
index: 0x1469, decrypted string: Initializing database...
index: 0x1482, decrypted string: xagtnotif.exe;AppUIMonitor.exe
index: 0x14a1, decrypted string: %ProgramFiles%\Internet Explorer\iexplore.exe
index: 0x14cf, decrypted string: Win32_DiskDrive
index: 0x14df, decrypted string: aabcdeefghiijklmnoopqrstuuvwxyyz
index: 0x1500, decrypted string: %SystemRoot%\System32\mobsync.exe
index: 0x1522, decrypted string: %SystemRoot%\SysWOW64\wermgr.exe
index: 0x1543, decrypted string: kernel32.dll
index: 0x1550, decrypted string: %SystemRoot%\System32\mspaint.exe
index: 0x1572, decrypted string: bdagent.exe;vsserv.exe;vsservppl.exe
index: 0x1597, decrypted string: SOFTWARE\Microsoft\Microsoft AntiMalware\SpyNet
index: 0x15c7, decrypted string: Caption,Description,Vendor,Version,InstallDate,InstallSource,Packag
index: 0x1610, decrypted string: NTUSER.DAT
index: 0x161b, decrypted string: ccSvcHst.exe;NortonSecurity.exe;nsWscSvc.exe
index: 0x1648, decrypted string:  from
index: 0x164f, decrypted string: mcshield.exe
index: 0x165c, decrypted string: %SystemRoot%\System32\SndVol.exe
index: 0x167d, decrypted string: VMware;VMW;QEMU
index: 0x168d, decrypted string: QEMU;VMware Pointing;VMware Accelerated;VMware SCSI;VMware SVGA;VMw
index: 0x179d, decrypted string: shlwapi.dll
index: 0x17a9, decrypted string: csc_ui.exe
index: 0x17b4, decrypted string: CrAmTray.exe
index: 0x17c1, decrypted string: Mozilla/5.0 (Windows NT 6.1; rv:77.0) Gecko/20100101 Firefox/77.0
index: 0x1803, decrypted string: %ProgramFiles(x86)%\Internet Explorer\iexplore.exe

[+] Decrypt all strings with index boundary is 0x5ad
index: 0x0, decrypted string: SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList
index: 0x39, decrypted string: ProgramData
index: 0x45, decrypted string: netstat -nao
index: 0x52, decrypted string: %s "$%s = \"%s\"; & $%s"
index: 0x6b, decrypted string: net localgroup
```

```
index: 0x7a, decrypted string: powershell.exe
index: 0x89, decrypted string: route print
index: 0x95, decrypted string: "%s\system32\schtasks.exe" /Create /ST %02u:%02u /RU "NT AUTHORITY\SY
index: 0x10a, decrypted string: Component_08
index: 0x117, decrypted string: ERROR: GetModuleFileNameW() failed with error: ERROR_INSUFFICIENT_BU
index: 0x160, decrypted string: net view
index: 0x169, decrypted string: ipconfig /all
index: 0x177, decrypted string: Self check
index: 0x182, decrypted string: T2X!wWMVH1UkMHD7SBdbgfgXrNBd(5dmRNbBI9
index: 0x1a9, decrypted string: 4Lm7DW&yMF*ELN4D8oNp0CtKUf*C2LAstORIBV
index: 0x1d0, decrypted string: Start screenshot
index: 0x1e1, decrypted string: %s.%u
index: 0x1e7, decrypted string: adrclient.dll
index: 0x1f5, decrypted string: net share
index: 0x1ff, decrypted string: qwinsta
index: 0x207, decrypted string: \System32\WindowsPowerShell\v1.0\powershell.exe
index: 0x237, decrypted string: at.exe %u:%u "%s" /I
index: 0x24c, decrypted string: Self test FAILED!!!
index: 0x260, decrypted string: Component_07
index: 0x26d, decrypted string: whoami /all
index: 0x279, decrypted string:  /c ping.exe -n 6 127.0.0.1 &  type "%s\System32\calc.exe" > "%s"
index: 0x2bb, decrypted string: error res='%s' err=%d len=%u
index: 0x2d8, decrypted string: nltest /domain_trusts /all_trusts
index: 0x2fa, decrypted string: .lnk
index: 0x2ff, decrypted string: cmd
index: 0x303, decrypted string: schtasks.exe /Create /RU "NT AUTHORITY\SYSTEM" /SC ONSTART /TN %u /T
index: 0x355, decrypted string: %s \"$%s = \\\"%s\\\"; & $%s\"
index: 0x374, decrypted string: ERROR: GetModuleFileNameW() failed with error: %u
index: 0x3a6, decrypted string: schtasks.exe /Delete /F /TN %u
index: 0x3c5, decrypted string: arp -a
index: 0x3cc, decrypted string: Self check ok!
index: 0x3db, decrypted string: cmd.exe /c set
index: 0x3ea, decrypted string: %s %04x.%u %04x.%u res: %s seh_test: %u consts_test: %d vmdetected: 
index: 0x443, decrypted string: Microsoft
index: 0x44d, decrypted string: powershell.exe -encodedCommand %S
index: 0x46f, decrypted string: SELF_TEST_1
index: 0x47b, decrypted string: microsoft.com,google.com,kernel.org,www.wikipedia.org,oracle.com,ver
index: 0x501, decrypted string: c:\ProgramData
index: 0x510, decrypted string: nslookup -querytype=ALL -timeout=12 _ldap._tcp.dc._msdcs.%s
index: 0x54c, decrypted string: %u;%u;%u;
index: 0x556, decrypted string: powershell.exe -encodedCommand
index: 0x576, decrypted string: runas
index: 0x57c, decrypted string: /teorema505
index: 0x588, decrypted string: Self test OK.
index: 0x596, decrypted string: ProfileImagePath
```

```
index: 0x5a7, decrypted string: p%08x
```

Based on the list of decrypted strings above, after analyzing the code and comparing it to the old idb of the 32-bit version, I found a string at offset `0x182` that is used for the decoding process of Campaign and C2 addresses of Qakbot:

The decryption process in this new version has some changes compared to the old version that I described here:

The function `qbot_aes_decrypt_and_check_sha256_wrap` **(0x180015D14)** makes a call to the function `qbot_aes_decrypt_and_check_sha256`.

Based on the pseudocode above, the encrypted data is declared as a struct as follows:

The code in function `qbot_aes_decrypt_and_check_sha256 (0x1800163E8)` reuses the `qbot_decrypt_xor_key_blob function (0x180011504)` that I described above to perform data decryption. Specifically:

The decrypted data includes the first `32 bytes (0x20)` as the *`sha256 checksum`*, which is used to verify the integrity of the decrypted configuration. The entire pseudocode for the function is shown below:

The method of decrypting C2 address list follows the same procedure as described above.

A Python script can be rewritten to automate the entire process of decoding Campaign and C2 addresses. The results obtained are:

```
# QakBot Config
----
   ID : b'tchk08'
   b'40' : b'1'
   Timestamp : 21:22:34 31-01-2024
----
# QakBot C2 address
```
```
31.210.173.10:443
185.156.172.62:443
185.113.8.123:443
```

Source: https://kienmanowar.wordpress.com/2024/04/24/quicknote-qakbot-5-0-decrypt-strings-and-configuration/