Kalle Jalkanen AB8822

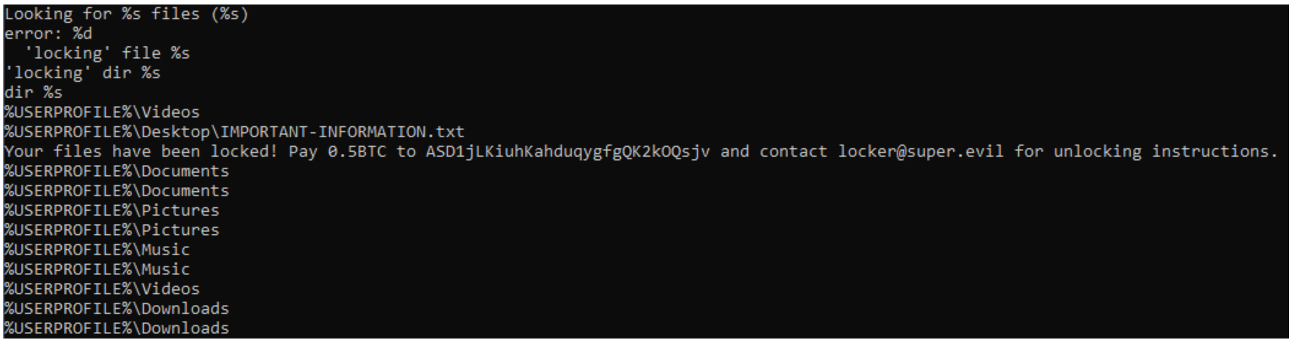
time used: 4,5 hours

Summary

This winlab02 is ransomware. It encrypts user home folder files so they cannot be accessed. Looks like only pdf, xlsx, docx, jpg, png, doc xls and txt files is in its scope. It creates txt file to desktop where it asks 0.5 Bitcoins to get files back. This file also includes attackers email address.

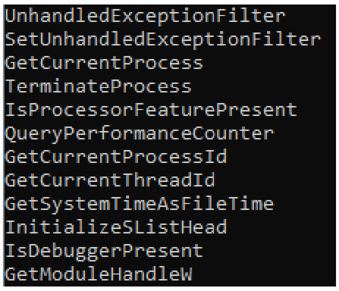
Static analyzing

Looking from strings looks like this is some kind of ransomware. It might block access to user's folders and then ask for ransom in Bitcoins. This ransom text is created to desktop/IMPORTANT-INFORMATION.txt.



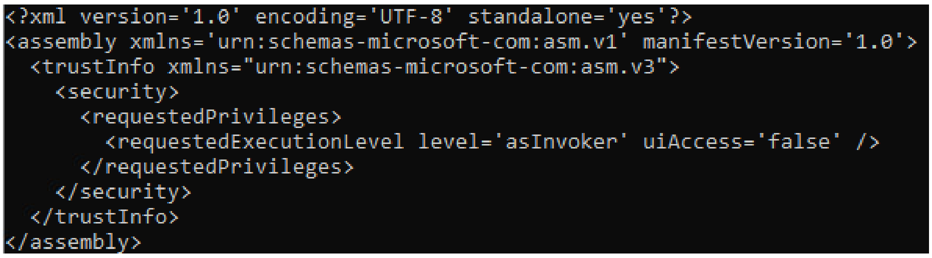
```
Looking for %s files (%s)
error: %d
  'locking' file %s
'locking' dir %s
dir %s
%USERPROFILE%\Videos
%USERPROFILE%\Desktop\IMPORTANT-INFORMATION.txt
Your files have been locked! Pay 0.5BTC to ASD1jLKiuhKahduqygfgQK2kOQsjv and contact locker@super.evil for unlocking instructions.
%USERPROFILE%\Documents
%USERPROFILE%\Documents
%USERPROFILE%\Pictures
%USERPROFILE%\Pictures
%USERPROFILE%\Music
%USERPROFILE%\Music
%USERPROFILE%\Videos
%USERPROFILE%\Downloads
%USERPROFILE%\Downloads
```

This looks like it has some kind of debugger identifier that may cause program to modify its behavior because of 'IsDebuggerPresent' found.



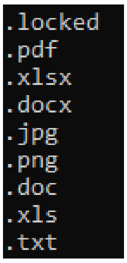
```
UnhandledExceptionFilter
SetUnhandledExceptionFilter
GetCurrentProcess
TerminateProcess
IsProcessorFeaturePresent
QueryPerformanceCounter
GetCurrentProcessId
GetCurrentThreadId
GetSystemTimeAsFileTime
InitializeSListHead
IsDebuggerPresent
GetModuleHandleW
```

This XML requests the application to run with the same privilege level as its parent process.



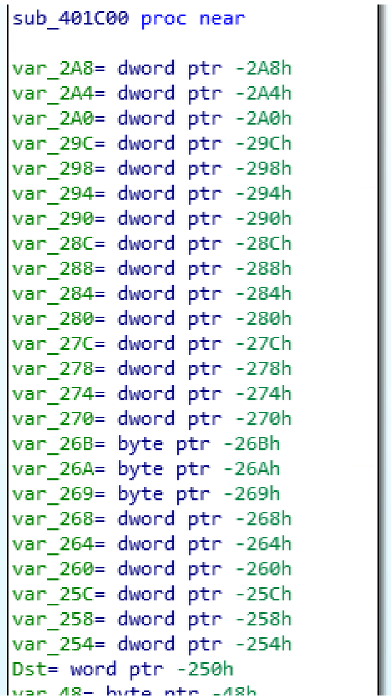
```
<?xml version='1.0' encoding='UTF-8' standalone='yes'?>
<assembly xmlns='urn:schemas-microsoft-com:asm.v1' manifestVersion='1.0'>
  <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
    <security>
      <requestedPrivileges>
        <requestedExecutionLevel level='asInvoker' uiAccess='false' />
      </requestedPrivileges>
    </security>
  </trustInfo>
</assembly>
```

Looks like it affects only these file types that I found from strings.



```
.locked
.pdf
.xlsx
.docx
.jpg
.png
.doc
.xls
.txt
```

From IDA I found sub_401C00 which looks like it might be encryption process, but I did not get how it works.

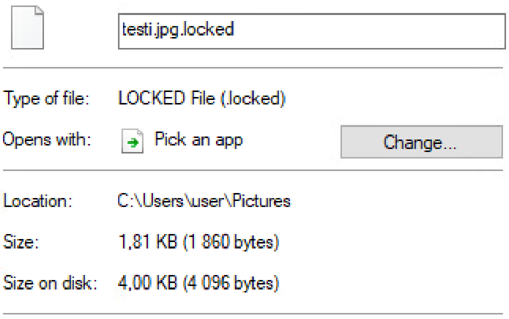


```
sub_401C00 proc near

var_2A8= dword ptr -2A8h
var_2A4= dword ptr -2A4h
var_2A0= dword ptr -2A0h
var_29C= dword ptr -29Ch
var_298= dword ptr -298h
var_294= dword ptr -294h
var_290= dword ptr -290h
var_28C= dword ptr -28Ch
var_288= dword ptr -288h
var_284= dword ptr -284h
var_280= dword ptr -280h
var_27C= dword ptr -27Ch
var_278= dword ptr -278h
var_274= dword ptr -274h
var_270= dword ptr -270h
var_26B= byte ptr -26Bh
var_26A= byte ptr -26Ah
var_269= byte ptr -269h
var_268= dword ptr -268h
var_264= dword ptr -264h
var_260= dword ptr -260h
var_25C= dword ptr -25Ch
var_258= dword ptr -258h
var_254= dword ptr -254h
Dst= word ptr -250h
var_48= byte ptr -48h
```

Dynamic analyzing

Running winlab02.exe adds .locked end to files in users folders. It also reduces file size and removing .locked end does not fix the file. It does not lock zip, exe or msi files so it locks only file types found in static analyzing.



testi.jpg.locked

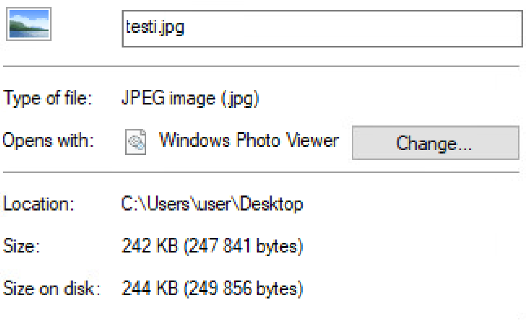
Type of file: LOCKED File (.locked)

Opens with: Pick an app

Location: C:\Users\user\Pictures

Size: 1,81 KB (1 860 bytes)

Size on disk: 4,00 KB (4 096 bytes)



testi.jpg

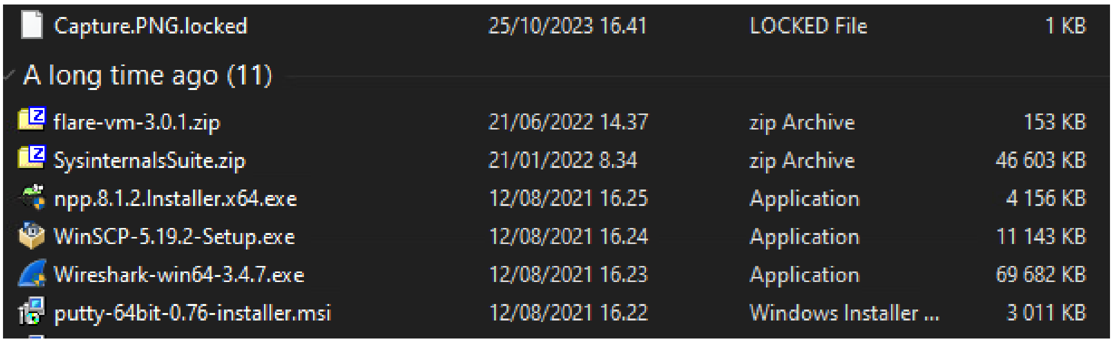
Type of file: JPEG image (.jpg)

Opens with: Windows Photo Viewer

Location: C:\Users\user\Desktop

Size: 242 KB (247 841 bytes)

Size on disk: 244 KB (249 856 bytes)



Capture.PNG.locked	25/10/2023 16.41	LOCKED File	1 KB
A long time ago (11)			
flare-vm-3.0.1.zip	21/06/2022 14.37	zip Archive	153 KB
SysinternalsSuite.zip	21/01/2022 8.34	zip Archive	46 603 KB
npp.8.1.2.Installer.x64.exe	12/08/2021 16.25	Application	4 156 KB
WinSCP-5.19.2-Setup.exe	12/08/2021 16.24	Application	11 143 KB
Wireshark-win64-3.4.7.exe	12/08/2021 16.23	Application	69 682 KB
putty-64bit-0.76-installer.msi	12/08/2021 16.22	Windows Installer ...	3 011 KB

It also creates that txt file mentioned earlier to desktop. I did not find anything else what this winlab02.exe does with dynamic analysis.