blog.cyble.com /2022/02/03/koxic-ransomware-deep-diveanalysis/

Koxic Ransomware Deep-dive Analysis

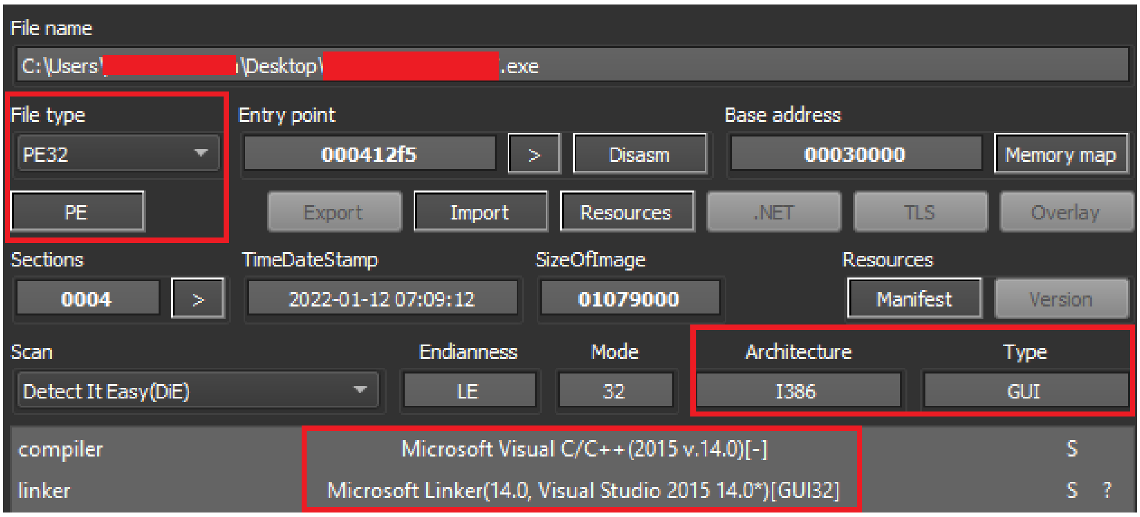
: 2/3/2022

Ransomware groups are posing a more significant and multi-pronged danger to organizations worldwide. The biggest hazard to businesses is losing access to their systems and data. Furthermore, ransomware gangs' potential to expose data if their ransom demands are rejected or reported to law enforcement agencies has become more concerning.

Cyble Research Labs have come through new ransomware known as Koxic. This blog showcases the deep-dive analysis of one of the Koxic ransomware samples to identify their capabilities and the way to secure yourself/your organization from them.

Technical Analysis

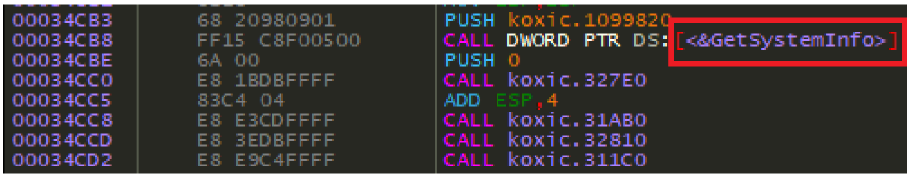
Based on static analysis, we found that the malicious file is a 32-bit Graphical User Interface (GUI) based binary, as shown in Figure 1.



File name: C:\Users\[redacted]\Desktop\[redacted].exe
File type: PE32
Entry point: 000412f5
Base address: 00030000
Sections: 0004
TimeDateStamp: 2022-01-12 07:09:12
SizeOfImage: 01079000
Scan: Detect It Easy(DiE)
Endianness: LE
Mode: 32
Architecture: I386
Type: GUI
compiler: Microsoft Visual C/C++(2015 v.14.0)[-] S
linker: Microsoft Linker(14.0, Visual Studio 2015 14.0*)[GUI32] S ?

Figure 1 Static File Information of Koxic Sample

After execution, Koxic Ransomware tries to get system information using *GetSystemInfo() API,* which extracts the information such as ProcessorType, NumberOfProcessors, etc.



```
00034CB3    68 20980901    PUSH koxic.1099820
00034CB8    FF15 C8F00500  CALL DWORD PTR DS:[<&GetSystemInfo>]
00034CBE    6A 00          PUSH 0
00034CC0    E8 1BDBFFFF    CALL koxic.327E0
00034CC5    83C4 04        ADD ESP,4
00034CC8    E8 E3CDFFFF    CALL koxic.31AB0
00034CCD    E8 3EDBFFFF    CALL koxic.32810
00034CD2    E8 E9C4FFFF    CALL koxic.311C0
```

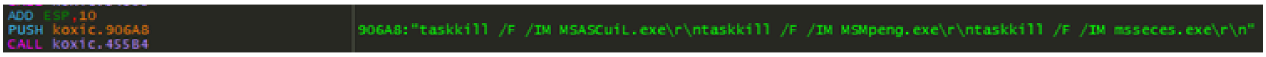
Figure 2 Koxic Ransomware Collect System Info

The following Registry values are added/modified by the ransomware, which helps the attacker set the Remote Desktop services settings, disables windows defender features, removes security and maintenance icons, and disables notifications and action centers.

- SOFTWARE\\Policies\\Microsoft\\Windows NT\\Terminal Services\\MaxDisconnectionTime
- SOFTWARE\\Policies\\Microsoft\\Windows NT\\Terminal Services\\MaxIdleTime
- SOFTWARE\\Policies\\Microsoft\\Windows\\HomeGroup\\DisableHomeGroup

- SOFTWARE\\Policies\\Microsoft\\Windows Defender\\DisableAntiSpyware
- SOFTWARE\\Policies\\Microsoft\\Windows Defender\\AllowFastServiceStartup
- SOFTWARE\\Policies\\Microsoft\\Windows Defender\\ServiceKeepAlive
- SOFTWARE\\Policies\\Microsoft\\Windows Defender\\Real-Time Protection\\DisableRealtimeMonitoring
- SOFTWARE\\Policies\\Microsoft\\Windows Defender\\Real-Time Protection\\DisableBehaviorMonitoring
- SOFTWARE\\Policies\\Microsoft\\Windows Defender\\Real-Time Protection\\DisableScanOnRealtimeEnable
- SOFTWARE\\Policies\\Microsoft\\Windows Defender\\Real-Time Protection\\DisableIOAVProtection
- SOFTWARE\\Policies\\Microsoft\\Windows Defender\\Real-Time Protection\\DisableOnAccessProtection
- SOFTWARE\\Microsoft\\Windows Defender\\Spynet\\DisableBlockAtFirstSeen
- SOFTWARE\\Microsoft\\Windows Defender\\Spynet\\SubmitSamplesConsent
- SOFTWARE\\Microsoft\\Windows Defender\\UX Configuration\\NotificationSuppress
- SOFTWARE\\Microsoft\\Windows Defender\\Features\\TamperProtection
- Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\HideSCAHealth
- Software\\Policies\\Microsoft\\Windows\\Explorer\\DisableNotificationCenter

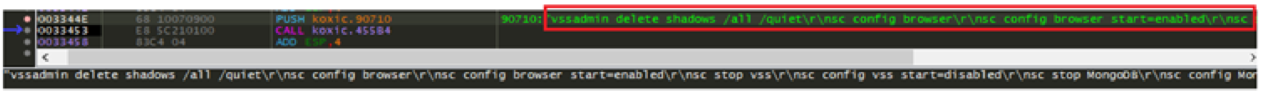
If they are actively running in the system, the ransomware terminates processes such as MSASCuiL.exe, MSMpeng.exe, and msseces.exe.



```
ADD ESP,10
PUSH koxic.906A8          906A8:"taskkill /F /IM MSASCuiL.exe\r\ntaskkill /F /IM MSMpeng.exe\r\ntaskkill /F /IM msseces.exe\r\n"
CALL koxic.455B4
```

Figure 3 Kills Windows Security Apps

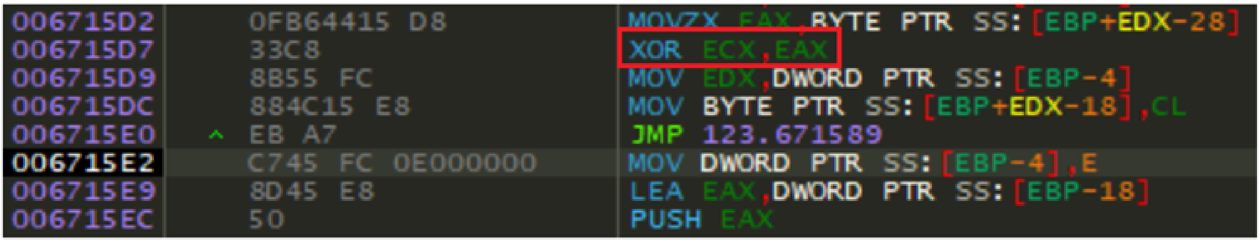
The malware also deletes the shadow copies using vssadmin and disables the database applications such as MongoDB, SQLWrite, and MSSQLServerOLAPService before starting the encryption.



```
003344E   68 10070900   PUSH koxic.90710   90710:"vssadmin delete shadows /all /quiet\r\nsc config browser\r\nsc config browser start=enabled\r\nsc
0033453   E8 5C210100   CALL koxic.455B4
0033458   83C4 04       ADD ESP,4
"vssadmin delete shadows /all /quiet\r\nsc config browser\r\nsc config browser start=enabled\r\nsc stop vss\r\nsc config vss start=disabled\r\nsc stop MongoDB\r\nsc config Mo
```

Figure 4 Deletes Shadow Copies

Then, it executes a custom decryption logic for getting the name of the ransom note, as shown in the below figure.



```
006715D2      0FB64415 D8      MOVZX EAX,BYTE PTR SS:[EBP+EDX-28]
006715D7      33C8             XOR ECX,EAX
006715D9      8B55 FC          MOV EDX,DWORD PTR SS:[EBP-4]
006715DC      884C15 E8        MOV BYTE PTR SS:[EBP+EDX-18],CL
006715E0  ^   EB A7            JMP 123.671589
006715E2      C745 FC 0E000000 MOV DWORD PTR SS:[EBP-4],E
006715E9      8D45 E8          LEA EAX,DWORD PTR SS:[EBP-18]
006715EC      50               PUSH EAX
```

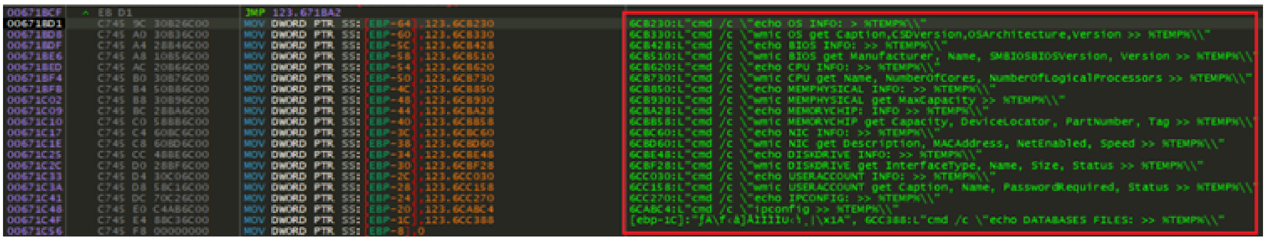
Figure 5 Decryption Loop

After identifying the ransom note name, the ransomware calls the following APIs for getting the system privileges which supports the encryption process.

- SeBackupPriviledge(): This API grants access to the attacker for reading files for their encryption process.
- SeRestorePriviledge(): Grants access to attacker for writing files.

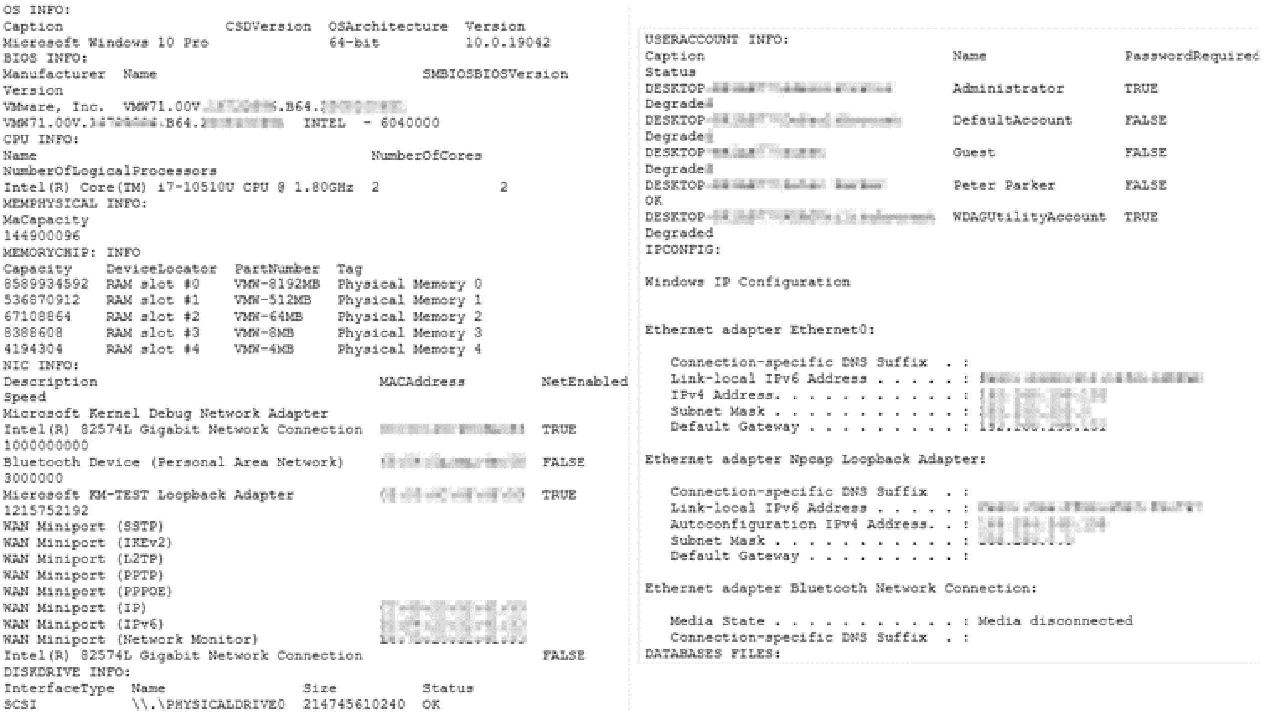
- SeManageVolumePriviledge(): Allows attackers to understand the volume details for their encryption process.
- SeTakeOwnershipPriviledge(): Allows attackers to take ownership of files or other objects.

The ransomware then steals sensitive system information and writes it to a file named “MOJPMLVBJ” in the TEMP folder, as shown in Figures 6 and 7. After the encryption process, the stolen information ends up with the attacker.



```
00671BCF   ^ EB D1            JMP 123.6718A2
00671BD1     C745 9C 30B26C00  MOV DWORD PTR SS:[EBP-64],123.6CB230   6CB230:L"cmd /c \"echo OS INFO: > %TEMP%\\"
00671BD8     C745 A0 30B36C00  MOV DWORD PTR SS:[EBP-60],123.6CB330   6CB330:L"cmd /c \"wmic OS get Caption,CSDVersion,OSArchitecture,Version >> %TEMP%\\"
00671BDF     C745 A4 28B46C00  MOV DWORD PTR SS:[EBP-5C],123.6CB428   6CB428:L"cmd /c \"echo BIOS INFO: >> %TEMP%\\"
00671BE6     C745 A8 10B56C00  MOV DWORD PTR SS:[EBP-58],123.6CB510   6CB510:L"cmd /c \"wmic BIOS get Manufacturer, Name, SMBIOSBIOSVersion, Version >> %TEMP%\\"
00671BED     C745 AC 20B66C00  MOV DWORD PTR SS:[EBP-54],123.6CB620   6CB620:L"cmd /c \"echo CPU INFO: >> %TEMP%\\"
00671BF4     C745 B0 30B76C00  MOV DWORD PTR SS:[EBP-50],123.6CB730   6CB730:L"cmd /c \"wmic CPU get Name, NumberOfCores, NumberOfLogicalProcessors >> %TEMP%\\"
00671BFB     C745 B4 50B86C00  MOV DWORD PTR SS:[EBP-4C],123.6CB850   6CB850:L"cmd /c \"echo MEMPHYSICAL INFO: >> %TEMP%\\"
00671C02     C745 B8 30B96C00  MOV DWORD PTR SS:[EBP-48],123.6CB930   6CB930:L"cmd /c \"wmic MEMPHYSICAL get MaxCapacity >> %TEMP%\\"
00671C09     C745 BC 28BA6C00  MOV DWORD PTR SS:[EBP-44],123.6CBA28   6CBA28:L"cmd /c \"echo MEMORYCHIP: INFO >> %TEMP%\\"
00671C10     C745 C0 58BB6C00  MOV DWORD PTR SS:[EBP-40],123.6CBB58   6CBB58:L"cmd /c \"wmic MEMORYCHIP get Capacity, DeviceLocator, PartNumber, Tag >> %TEMP%\\"
00671C17     C745 C4 60BC6C00  MOV DWORD PTR SS:[EBP-3C],123.6CBC60   6CBC60:L"cmd /c \"echo NIC INFO: >> %TEMP%\\"
00671C1E     C745 C8 60BD6C00  MOV DWORD PTR SS:[EBP-38],123.6CBD60   6CBD60:L"cmd /c \"wmic NIC get Description, MACAddress, NetEnabled, Speed >> %TEMP%\\"
00671C25     C745 CC 48BE6C00  MOV DWORD PTR SS:[EBP-34],123.6CBE48   6CBE48:L"cmd /c \"echo DISKDRIVE INFO: >> %TEMP%\\"
00671C2C     C745 D0 28BF6C00  MOV DWORD PTR SS:[EBP-30],123.6CBF28   6CBF28:L"cmd /c \"wmic DISKDRIVE get InterfaceType, Name, Size, Status >> %TEMP%\\"
00671C33     C745 D4 30C06C00  MOV DWORD PTR SS:[EBP-2C],123.6CC030   6CC030:L"cmd /c \"echo USERACCOUNT INFO: >> %TEMP%\\"
00671C3A     C745 D8 58C16C00  MOV DWORD PTR SS:[EBP-28],123.6CC158   6CC158:L"cmd /c \"wmic USERACCOUNT get Caption, Name, PasswordRequired, Status >> %TEMP%\\"
00671C41     C745 DC 70C26C00  MOV DWORD PTR SS:[EBP-24],123.6CC270   6CC270:L"cmd /c \"echo IPCONFIG: >> %TEMP%\\"
00671C48     C745 E0 C4AB6C00  MOV DWORD PTR SS:[EBP-20],123.6CABC4   6CABC4:L"cmd /c \"ipconfig >> %TEMP%\\"
00671C4F     C745 E4 88C36C00  MOV DWORD PTR SS:[EBP-1C],123.6CC388   [ebp-1C]:"ƒA\f‹â]AIIIIU‹\¸|\x1A", 6CC388:L"cmd /c \"echo DATABASES FILES: >> %TEMP%\\"
00671C56     C745 F8 00000000  MOV DWORD PTR SS:[EBP-8],0
```

Figure 6 Commands to steal system information



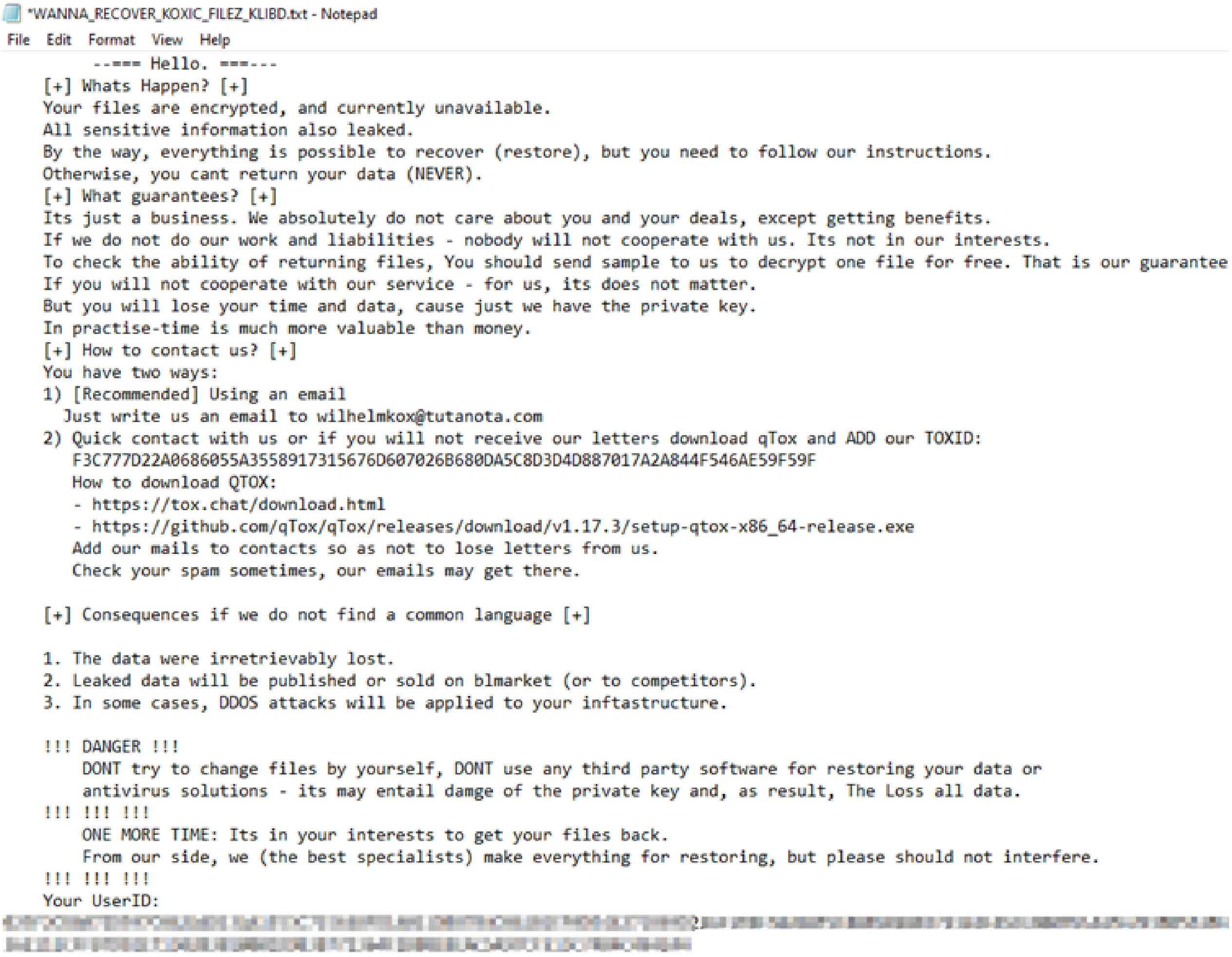
```
OS INFO:
Caption                      CSDVersion  OSArchitecture  Version
Microsoft Windows 10 Pro                 64-bit          10.0.19042
BIOS INFO:
Manufacturer  Name                                      SMBIOSBIOSVersion
Version
VMware, Inc.  VMW71.00V.[redacted].B64.[redacted]
VMW71.00V.[redacted].B64.[redacted]  INTEL  - 6040000
CPU INFO:
Name                                    NumberOfCores
NumberOfLogicalProcessors
Intel(R) Core(TM) i7-10510U CPU @ 1.80GHz  2              2
MEMPHYSICAL INFO:
MaCapacity
144900096
MEMORYCHIP: INFO
Capacity    DeviceLocator  PartNumber  Tag
8589934592  RAM slot #0    VMW-8192MB  Physical Memory 0
536870912   RAM slot #1    VMW-512MB   Physical Memory 1
67108864    RAM slot #2    VMW-64MB    Physical Memory 2
8388608     RAM slot #3    VMW-8MB     Physical Memory 3
4194304     RAM slot #4    VMW-4MB     Physical Memory 4
NIC INFO:
Description                             MACAddress         NetEnabled
Speed
Microsoft Kernel Debug Network Adapter
Intel(R) 82574L Gigabit Network Connection  [redacted]    TRUE
1000000000
Bluetooth Device (Personal Area Network)    [redacted]    FALSE
3000000
Microsoft KM-TEST Loopback Adapter          [redacted]    TRUE
1215752192
WAN Miniport (SSTP)
WAN Miniport (IKEv2)
WAN Miniport (L2TP)
WAN Miniport (PPTP)
WAN Miniport (PPPOE)
WAN Miniport (IP)                           [redacted]
WAN Miniport (IPv6)
WAN Miniport (Network Monitor)
Intel(R) 82574L Gigabit Network Connection                 FALSE
DISKDRIVE INFO:
InterfaceType  Name              Size          Status
SCSI           \\.\PHYSICALDRIVE0  214745610240  OK
```

```
USERACCOUNT INFO:
Caption                        Name                PasswordRequired
Status
DESKTOP[redacted]              Administrator       TRUE
Degraded
DESKTOP[redacted]              DefaultAccount      FALSE
Degraded
DESKTOP[redacted]              Guest               FALSE
Degraded
DESKTOP[redacted]              Peter Parker        FALSE
OK
DESKTOP[redacted]              WDAGUtilityAccount  TRUE
Degraded
IPCONFIG:

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : [redacted]
   IPv4 Address. . . . . . . . . . . : [redacted]
   Subnet Mask . . . . . . . . . . . :
   Default Gateway . . . . . . . . . :

Ethernet adapter Npcap Loopback Adapter:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : [redacted]
   Autoconfiguration IPv4 Address. . : [redacted]
   Subnet Mask . . . . . . . . . . . :
   Default Gateway . . . . . . . . . :

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
DATABASES FILES:
```

Figure 7 Stolen information

The malware calls *GetLogicalDrives()* function to get the details of the drive in the victim's machine for encrypting the files. Next, the malware creates a mutex named "*atus*" to make sure another instance of the same program is not running on the machine. Finally, it drops ransom notes in all the locations.

The below figure demonstrates the ransom note dropped by the malware with the name "*WANNA_RECOVER_KOXIC_FILEZ_KLIBD.txt*" to instruct the victims to pay the ransom money for the decryption keys.



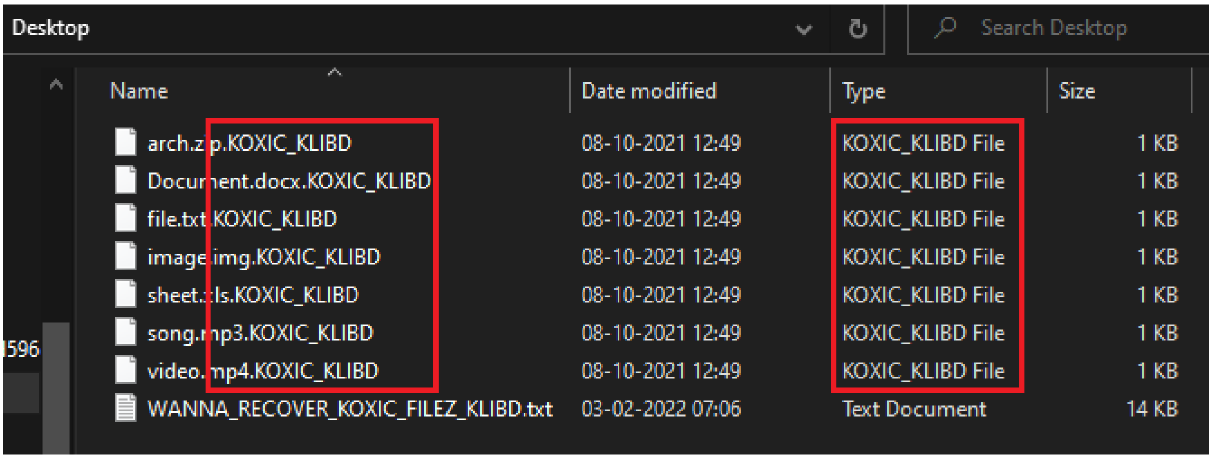
*WANNA_RECOVER_KOXIC_FILEZ_KLIBD.txt - Notepad

```
     --=== Hello. ===---
  [+] Whats Happen? [+]
  Your files are encrypted, and currently unavailable.
  All sensitive information also leaked.
  By the way, everything is possible to recover (restore), but you need to follow our instructions.
  Otherwise, you cant return your data (NEVER).
  [+] What guarantees? [+]
  Its just a business. We absolutely do not care about you and your deals, except getting benefits.
  If we do not do our work and liabilities - nobody will not cooperate with us. Its not in our interests.
  To check the ability of returning files, You should send sample to us to decrypt one file for free. That is our guarantee
  If you will not cooperate with our service - for us, its does not matter.
  But you will lose your time and data, cause just we have the private key.
  In practise-time is much more valuable than money.
  [+] How to contact us? [+]
  You have two ways:
  1) [Recommended] Using an email
     Just write us an email to wilhelmkox@tutanota.com
  2) Quick contact with us or if you will not receive our letters download qTox and ADD our TOXID:
     F3C777D22A0686055A3558917315676D607026B680DA5C8D3D4D887017A2A844F546AE59F59F
     How to download QTOX:
     - https://tox.chat/download.html
     - https://github.com/qTox/qTox/releases/download/v1.17.3/setup-qtox-x86_64-release.exe
     Add our mails to contacts so as not to lose letters from us.
     Check your spam sometimes, our emails may get there.

  [+] Consequences if we do not find a common language [+]

  1. The data were irretrievably lost.
  2. Leaked data will be published or sold on blmarket (or to competitors).
  3. In some cases, DDOS attacks will be applied to your inftastructure.

  !!! DANGER !!!
      DONT try to change files by yourself, DONT use any third party software for restoring your data or
      antivirus solutions - its may entail damge of the private key and, as result, The Loss all data.
  !!! !!! !!!
      ONE MORE TIME: Its in your interests to get your files back.
      From our side, we (the best specialists) make everything for restoring, but please should not interfere.
  !!! !!! !!!
  Your UserID:
[redacted]
```

Figure 8 Ransom note

In their ransom note, the TAs have instructed victims to contact them via qTox on their TOXID: *F3C777D22A0686055A3558917315676D607026B680DA5C8D3D4D887017A2A844F546AE59F59F* and have also given an Email ID: *wilhelmkox@tutanota[.]com.* In case the victim does not pay the ransom, the attackers, through the ransom note, threaten the victims to leak or sell their data to black-market or to competitors, and they also threaten for DDOS attack on the victim's infrastructure.

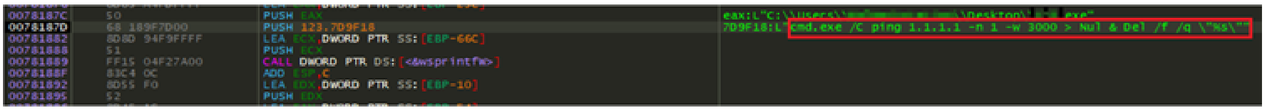
After dropping the ransom notes, the malware encrypts the files on the victim's machine and appends the extension with "*KOXIC_KLIBD*" as shown in the below figure.



Name	Date modified	Type	Size
arch.zip.KOXIC_KLIBD	08-10-2021 12:49	KOXIC_KLIBD File	1 KB
Document.docx.KOXIC_KLIBD	08-10-2021 12:49	KOXIC_KLIBD File	1 KB
file.txt.KOXIC_KLIBD	08-10-2021 12:49	KOXIC_KLIBD File	1 KB
image.img.KOXIC_KLIBD	08-10-2021 12:49	KOXIC_KLIBD File	1 KB
sheet.xls.KOXIC_KLIBD	08-10-2021 12:49	KOXIC_KLIBD File	1 KB
song.mp3.KOXIC_KLIBD	08-10-2021 12:49	KOXIC_KLIBD File	1 KB
video.mp4.KOXIC_KLIBD	08-10-2021 12:49	KOXIC_KLIBD File	1 KB
WANNA_RECOVER_KOXIC_FILEZ_KLIBD.txt	03-02-2022 07:06	Text Document	14 KB

Figure 9 Encrypted Files on the Machine

Finally, the malware deletes itself using *CreateProcess() API*, as shown in Figure 10.



```
0078187C   50             PUSH EAX                          eax:L"C:\\Users\\[redacted]\Desktop\\[redacted].exe"
0078187D   68 189F7D00    PUSH 123.7D9F18                   7D9F18:L"cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q \"%s\""
00781882   8D8D 94F9FFFF  LEA ECX,DWORD PTR SS:[EBP-66C]
00781888   51             PUSH ECX
00781889   FF15 04F27A00  CALL DWORD PTR DS:[<&wsprintfW>]
0078188F   83C4 0C        ADD ESP,C
00781892   8D55 F0        LEA EDX,DWORD PTR SS:[EBP-10]
00781895   52             PUSH EDX
```

Figure 10 Malware Deletes Executable after Execution

Conclusion

To update their Ransomware programs with new Tactics, Techniques, and Procedures (TTPs) to target devices, TAs continually add new functionality to their code. Based on these interpretations, we can reasonably predict that future Koxic versions will include even more improvements.

We continuously monitor Koxic's extortion campaigns and update our readers with the latest information.

Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the best practices given below:

Safety measures needed to prevent ransomware attacks

- Conduct regular backup practices and keep those backups offline or in a separate network.
- Turn on the automatic software update feature on your computer, mobile, and other connected devices wherever possible and pragmatic.
- Use a reputed anti-virus and Internet security software package on your connected devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments without verifying their authenticity.

Users should take the following steps after the ransomware attack

- Detach infected devices on the same network.
- Disconnect external storage devices if connected.
- Inspect system logs for suspicious events.

Impacts and cruciality Of Koxic Ransomware

- Loss of Valuable data.
- Loss of organization's reliability or integrity.
- Loss of organization's businesses information.
- Disruption in organization operation.
- Economic loss.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1078	-Valid Accounts
Execution	T1059	-Command and Scripting Interpreter
Privilege Escalation	T1548	-Abuse Elevation Control Mechanism
Defense Evasion	T1112	-Modify Registry
	T1027	-Obfuscated Files or Information
	T1562.001	-Impair Defenses: Disable or Modify Tools
Discovery	T1082	-System Information Discovery
	T1083	-File and Directory Discovery
Impact	T1490	-Inhibit System Recovery

T1489	-Service Stop
T1486	-Data Encrypted for Impact

Indicators of Compromise (IOCs)

Indicators	Indicator type	Description
699159e695e230a48d94b6103b48940ed596d0b48fb6d936c04d86eed539cecd	SHA256	Koxic Executable
wilhelmkox@tutanota[.]com	Email ID	Email ID mentioned in Koxic Ransom Note