AntiRansomware Tools Thoroughly Tested Part 1

Information Security Inc.

Contents

- What is Ransomware?
- Rise of Ransomware
- Ransomware Testing Environment
- Cybereason RansomFree
- References

What is Ransomware?

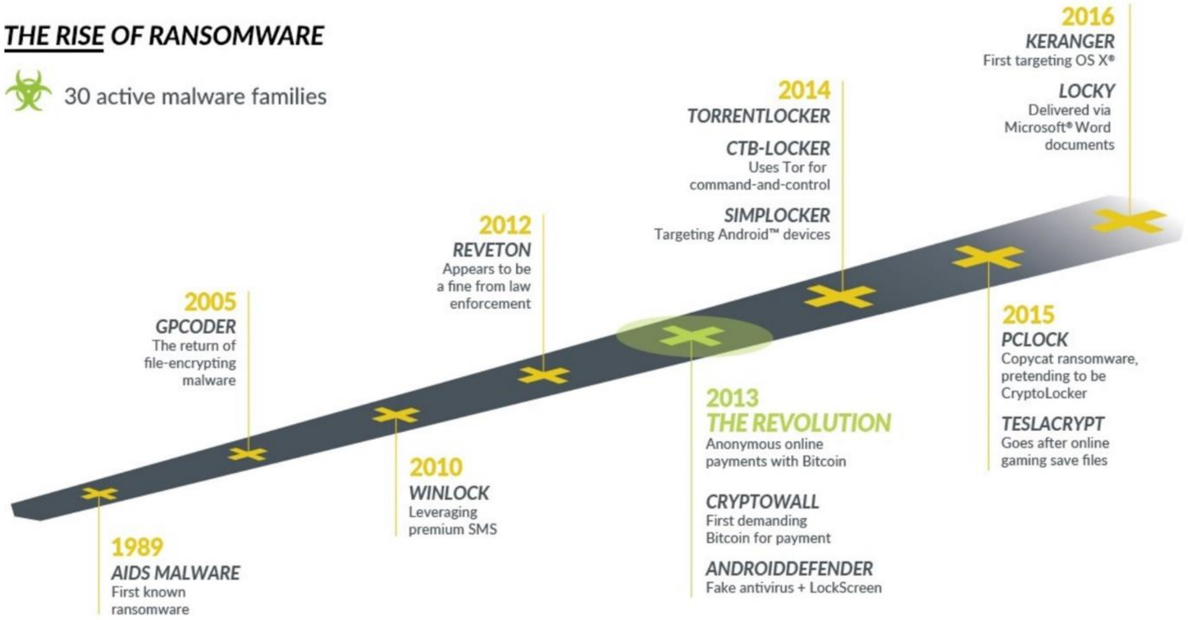
- **Ransomware** is a type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid
- Ransomware is malicious code that is used by cybercriminals to launch data kidnapping and lockscreen attacks
- The motive for ransomware attacks is monetary

What is

RANSOMWARE?

A type of malware that can stop you from using your PC, rename, or encrypt your files so you can't use them. You may be warned that you need to pay money, Bit-Coins, complete surveys, or perform other actions before you can use your PC again.

Rise of Ransomware



THE RISE OF RANSOMWARE

30 active malware families

1989
AIDS MALWARE
First known ransomware

2005
GPCODER
The return of file-encrypting malware

2010
WINLOCK
Leveraging premium SMS

2012
REVETON
Appears to be a fine from law enforcement

2013
THE REVOLUTION
Anonymous online payments with Bitcoin

CRYPTOWALL
First demanding Bitcoin for payment

ANDROIDDEFENDER
Fake antivirus + LockScreen

2014
TORRENTLOCKER

CTB-LOCKER
Uses Tor for command-and-control

SIMPLOCKER
Targeting Android™ devices

2015
PCLOCK
Copycat ransomware, pretending to be CryptoLocker

TESLACRYPT
Goes after online gaming save files

2016
KERANGER
First targeting OS X®

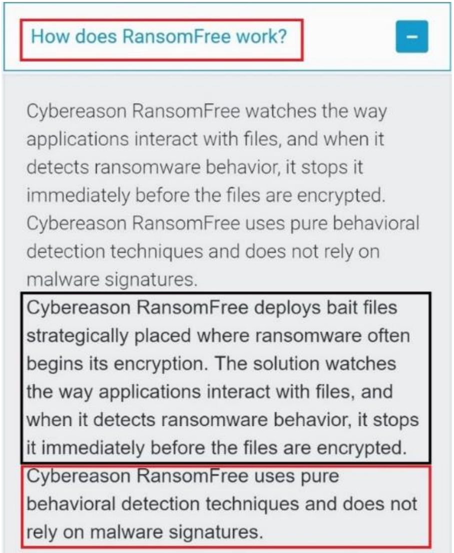
LOCKY
Delivered via Microsoft® Word documents

Ransomware Testing Envinronment

- Victim machine: Windows 7 Ultimate SP1 x64
- Ransomware: Zepto ransomware (https://www.tripwire.com/state-of-security/latest-security-news/the-newest-online-threat-zepto-ransomware/)

Cybereason RansomFree

- Download link: https://ransomfree.cybereason.com/download/
- How does RansomFree work?

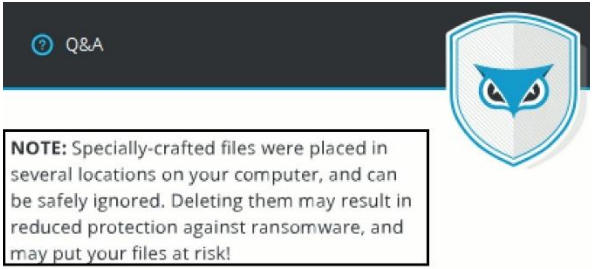


How does RansomFree work?

Cybereason RansomFree watches the way applications interact with files, and when it detects ransomware behavior, it stops it immediately before the files are encrypted. Cybereason RansomFree uses pure behavioral detection techniques and does not rely on malware signatures.

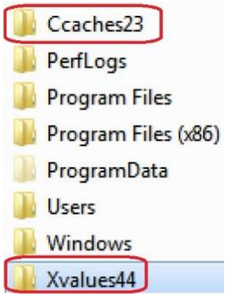
Cybereason RansomFree deploys bait files strategically placed where ransomware often begins its encryption. The solution watches the way applications interact with files, and when it detects ransomware behavior, it stops it immediately before the files are encrypted.

Cybereason RansomFree uses pure behavioral detection techniques and does not rely on malware signatures.



Q&A

NOTE: Specially-crafted files were placed in several locations on your computer, and can be safely ignored. Deleting them may result in reduced protection against ransomware, and may put your files at risk!



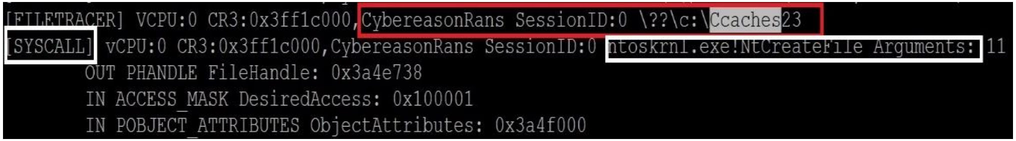
- Ccaches23
- PerfLogs
- Program Files
- Program Files (x86)
- ProgramData
- Users
- Windows
- Xvalues44

Cybereason RansomFree

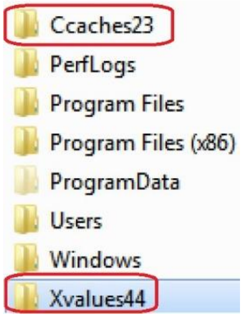
- How does RansomFree work?

◎ CybereasonRans uses !NtCreateFile function (https://goo.gl/dNd3Hx) to create bait folders and files in mutiple locations

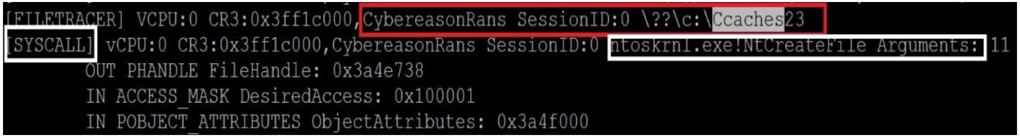
◎ Creating bait folders



```
[FILETRACER] VCPU:0 CR3:0x3ff1c000,CybereasonRans SessionID:0 \??\c:\Ccaches23
[SYSCALL] vCPU:0 CR3:0x3ff1c000,CybereasonRans SessionID:0 ntoskrnl.exe!NtCreateFile Arguments: 11
        OUT PHANDLE FileHandle: 0x3a4e738
        IN ACCESS_MASK DesiredAccess: 0x100001
        IN POBJECT_ATTRIBUTES ObjectAttributes: 0x3a4f000
```



Ccaches23
PerfLogs
Program Files
Program Files (x86)
ProgramData
Users
Windows
Xvalues44



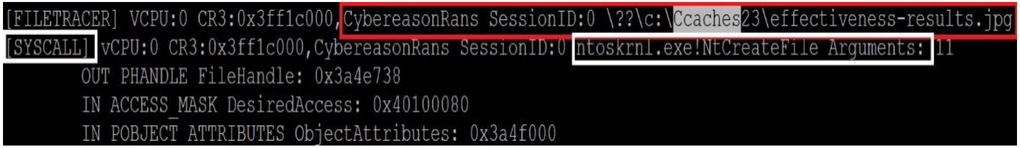
```
[FILETRACER] VCPU:0 CR3:0x3ff1c000,CybereasonRans SessionID:0 \??\c:\Ccaches23
[SYSCALL] vCPU:0 CR3:0x3ff1c000,CybereasonRans SessionID:0 ntoskrnl.exe!NtCreateFile Arguments: 11
        OUT PHANDLE FileHandle: 0x3a4e738
        IN ACCESS_MASK DesiredAccess: 0x100001
        IN POBJECT_ATTRIBUTES ObjectAttributes: 0x3a4f000
```

Cybereason RansomFree

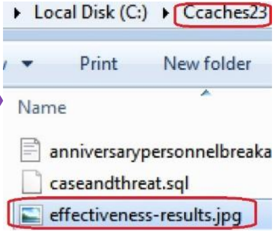
- How does RansomFree work?

◎ CybereasonRans uses !NtCreateFile function (https://goo.gl/dNd3Hx) to create bait folders and files in multiple locations

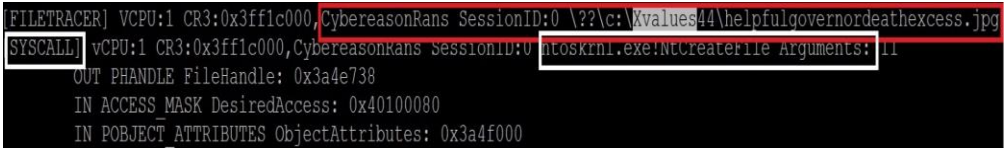
◎ Creating bait files inside the folders



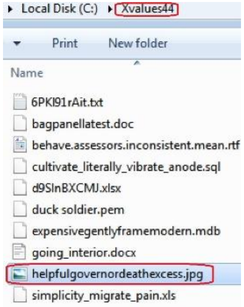
```
[FILETRACER] VCPU:0 CR3:0x3ff1c000,CybereasonRans SessionID:0 \??\c:\Ccaches23\effectiveness-results.jpg
[SYSCALL] vCPU:0 CR3:0x3ff1c000,CybereasonRans SessionID:0 ntoskrnl.exe!NtCreateFile Arguments: 11
        OUT PHANDLE FileHandle: 0x3a4e738
        IN ACCESS_MASK DesiredAccess: 0x40100080
        IN POBJECT_ATTRIBUTES ObjectAttributes: 0x3a4f000
```



anniversarypersonnelbreaka
caseandthreat.sql
effectiveness-results.jpg



```
[FILETRACER] VCPU:1 CR3:0x3ff1c000,CybereasonRans SessionID:0 \??\c:\Xvalues44\helpfulgovernordeathexcess.jpg
[SYSCALL] vCPU:1 CR3:0x3ff1c000,CybereasonRans SessionID:0 ntoskrnl.exe!NtCreateFile Arguments: 11
       OUT PHANDLE FileHandle: 0x3a4e738
       IN ACCESS_MASK DesiredAccess: 0x40100080
       IN POBJECT_ATTRIBUTES ObjectAttributes: 0x3a4f000
```

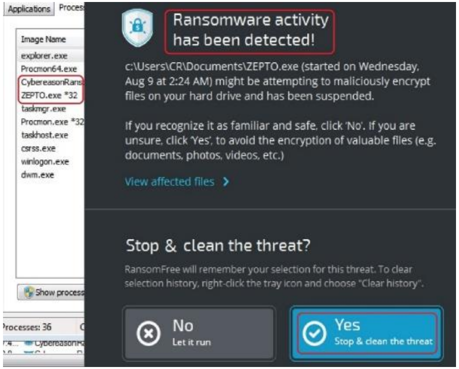


6PKI91rAit.txt
bagpanellatest.doc
behave.assessors.inconsistent.mean.rtf
cultivate_literally_vibrate_anode.sql
d9SlnBXCMJ.xlsx
duck soldier.pem
expensivegentlyframemodern.mdb
going_interior.docx
helpfulgovernordeathexcess.jpg
simplicity_migrate_pain.xls

Cybereason RansomFree

- How does RansomFree work? When detecting suspecting behavior kill the process

Cybereason RansomFree monitors your system for ransomware related behavior, and will alert you immediately of any suspicion, both locally or on a network drive.



Ransomware activity has been detected!

c:\Users\CR\Documents\ZEPTO.exe (started on Wednesday, Aug 9 at 2:24 AM) might be attempting to maliciously encrypt files on your hard drive and has been suspended.

If you recognize it as familiar and safe, click 'No'. If you are unsure, click 'Yes', to avoid the encryption of valuable files (e.g. documents, photos, videos, etc.)

Stop & clean the threat?

RansomFree will remember your selection for this threat. To clear selection history, right-click the tray icon and choose "Clear history".

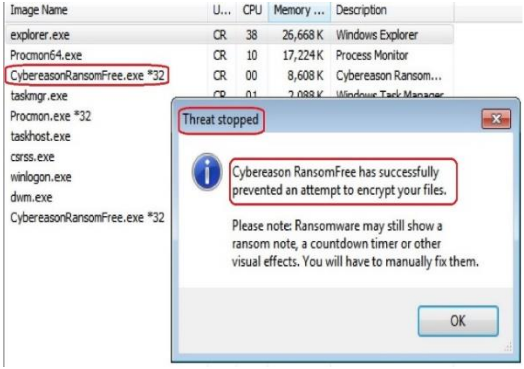


Image Name	U...	CPU	Memory ...	Description
explorer.exe	CR	38	26,668 K	Windows Explorer
Procmon64.exe	CR	10	17,224 K	Process Monitor
CybereasonRansomFree.exe *32	CR	00	8,608 K	Cybereason Ransom...
taskmgr.exe	CR	01	2,088 K	Windows Task Manager
Procmon.exe *32				
taskhost.exe				
csrss.exe				
winlogon.exe				
dwm.exe				
CybereasonRansomFree.exe *32				

Threat stopped

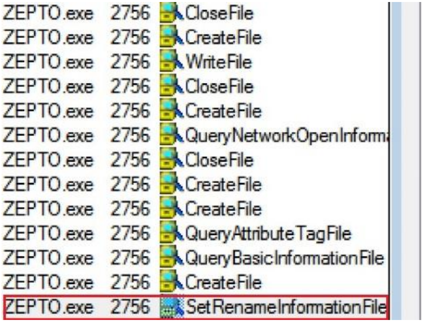
Cybereason RansomFree has successfully prevented an attempt to encrypt your files.

Please note: Ransomware may still show a ransom note, a countdown timer or other visual effects. You will have to manually fix them.

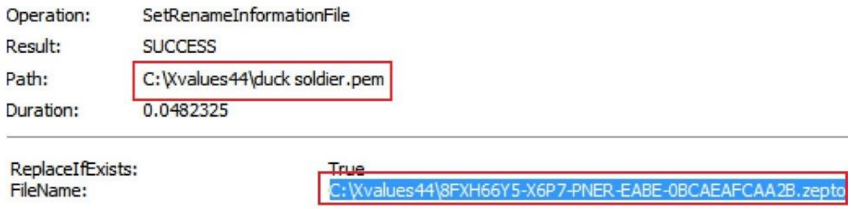
Cybereason RansomFree

- How does RansomFree work?

◎ Ransomware is adding .zepto extension to bait files using NtSetInformationFile function (https://goo.gl/3V1UMv)

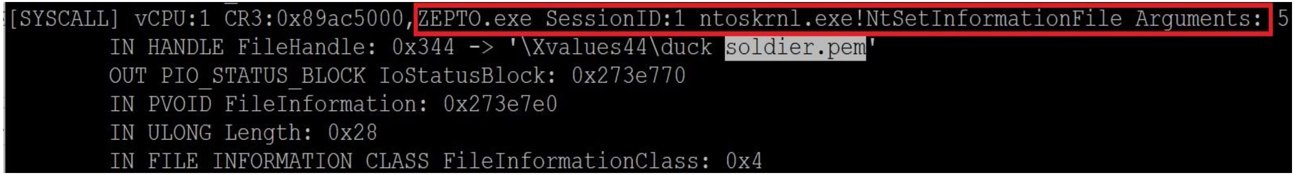


```
ZEPTO.exe  2756  CloseFile
ZEPTO.exe  2756  CreateFile
ZEPTO.exe  2756  WriteFile
ZEPTO.exe  2756  CloseFile
ZEPTO.exe  2756  CreateFile
ZEPTO.exe  2756  QueryNetworkOpenInform
ZEPTO.exe  2756  CloseFile
ZEPTO.exe  2756  CreateFile
ZEPTO.exe  2756  CreateFile
ZEPTO.exe  2756  QueryAttributeTagFile
ZEPTO.exe  2756  QueryBasicInformationFile
ZEPTO.exe  2756  CreateFile
ZEPTO.exe  2756  SetRenameInformationFile
```



```
Operation:    SetRenameInformationFile
Result:       SUCCESS
Path:         C:\Xvalues44\duck soldier.pem
Duration:     0.0482325

ReplaceIfExists:        True
FileName:               C:\Xvalues44\8FXH66Y5-X6P7-PNER-EABE-0BCAEAFCAA2B.zepto
```



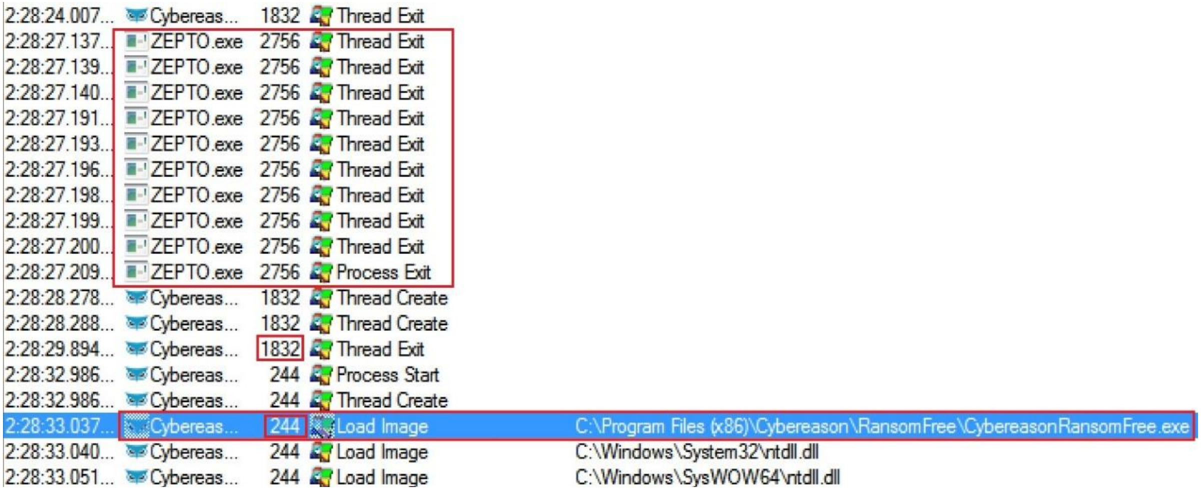
```
[SYSCALL] vCPU:1 CR3:0x89ac5000,ZEPTO.exe SessionID:1 ntoskrnl.exe!NtSetInformationFile Arguments: 5
        IN HANDLE FileHandle: 0x344 -> '\Xvalues44\duck soldier.pem'
        OUT PIO_STATUS_BLOCK IoStatusBlock: 0x273e770
        IN PVOID FileInformation: 0x273e7e0
        IN ULONG Length: 0x28
        IN FILE_INFORMATION_CLASS FileInformationClass: 0x4
```

Cybereason RansomFree

RansomFree cybereason

- How does RansomFree work?

◎ RansomFree kills ransomware’s threads and the parent process and loads a new image of itself starting a new process with ID 244



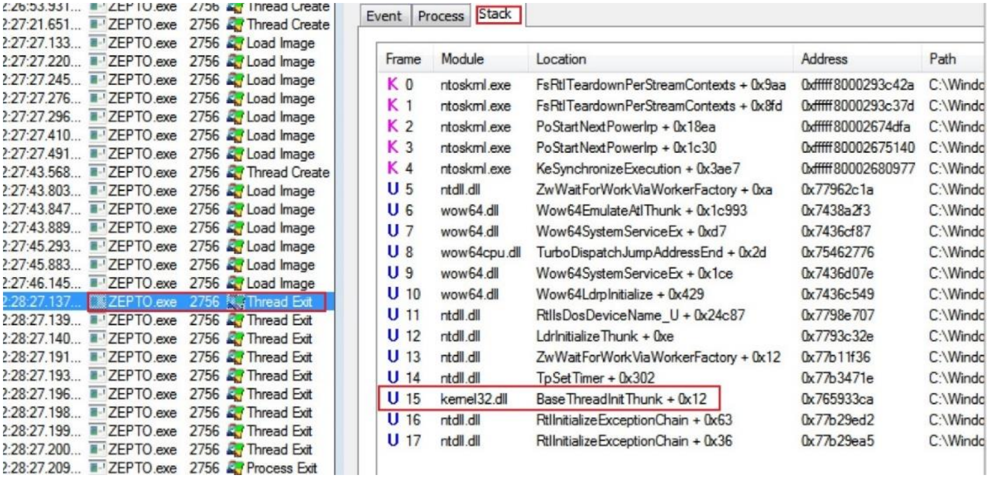
```
2:28:24.007...  Cybereas...   1832  Thread Exit
2:28:27.137...  ZEPTO.exe     2756  Thread Exit
2:28:27.139...  ZEPTO.exe     2756  Thread Exit
2:28:27.140...  ZEPTO.exe     2756  Thread Exit
2:28:27.191...  ZEPTO.exe     2756  Thread Exit
2:28:27.193...  ZEPTO.exe     2756  Thread Exit
2:28:27.196...  ZEPTO.exe     2756  Thread Exit
2:28:27.198...  ZEPTO.exe     2756  Thread Exit
2:28:27.199...  ZEPTO.exe     2756  Thread Exit
2:28:27.200...  ZEPTO.exe     2756  Thread Exit
2:28:27.209...  ZEPTO.exe     2756  Process Exit
2:28:28.278...  Cybereas...   1832  Thread Create
2:28:28.288...  Cybereas...   1832  Thread Create
2:28:29.894...  Cybereas...   1832  Thread Exit
2:28:32.986...  Cybereas...    244  Process Start
2:28:32.986...  Cybereas...    244  Thread Create
2:28:33.037...  Cybereas...    244  Load Image     C:\Program Files (x86)\Cybereason\RansomFree\CybereasonRansomFree.exe
2:28:33.040...  Cybereas...    244  Load Image     C:\Windows\System32\ntdll.dll
2:28:33.051...  Cybereas...    244  Load Image     C:\Windows\SysWOW64\ntdll.dll
```

Cybereason RansomFree

- How does RansomFree work?

◎ Thread stack before exiting

◎ BaseThreadInitThunk function (https://goo.gl/rm79Bd) calls the thread start address. If the thread returns it will terminate the thread and delete it’s stack



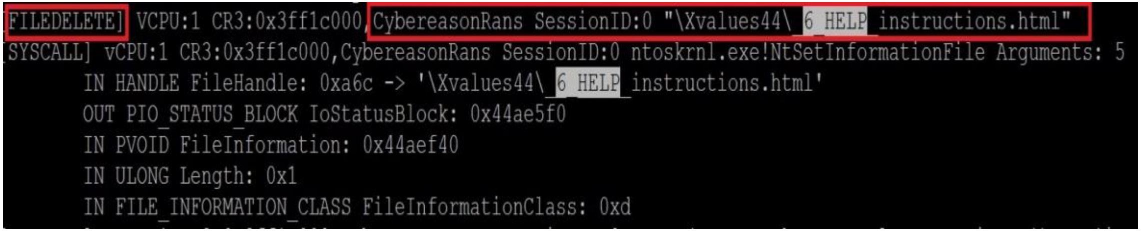
```
2:26:53.931...  ZEPTO.exe  2756  Thread Create
2:27:21.651...  ZEPTO.exe  2756  Thread Create
2:27:27.133...  ZEPTO.exe  2756  Load Image
2:27:27.220...  ZEPTO.exe  2756  Load Image
2:27:27.245...  ZEPTO.exe  2756  Load Image
2:27:27.276...  ZEPTO.exe  2756  Load Image
2:27:27.296...  ZEPTO.exe  2756  Load Image
2:27:27.410...  ZEPTO.exe  2756  Load Image
2:27:27.491...  ZEPTO.exe  2756  Load Image
2:27:43.568...  ZEPTO.exe  2756  Thread Create
2:27:43.803...  ZEPTO.exe  2756  Load Image
2:27:43.847...  ZEPTO.exe  2756  Load Image
2:27:43.889...  ZEPTO.exe  2756  Load Image
2:27:45.293...  ZEPTO.exe  2756  Load Image
2:27:45.883...  ZEPTO.exe  2756  Load Image
2:27:46.145...  ZEPTO.exe  2756  Load Image
2:28:27.137...  ZEPTO.exe  2756  Thread Exit
2:28:27.139...  ZEPTO.exe  2756  Thread Exit
2:28:27.140...  ZEPTO.exe  2756  Thread Exit
2:28:27.191...  ZEPTO.exe  2756  Thread Exit
2:28:27.193...  ZEPTO.exe  2756  Thread Exit
2:28:27.196...  ZEPTO.exe  2756  Thread Exit
2:28:27.198...  ZEPTO.exe  2756  Thread Exit
2:28:27.199...  ZEPTO.exe  2756  Thread Exit
2:28:27.200...  ZEPTO.exe  2756  Thread Exit
2:28:27.209...  ZEPTO.exe  2756  Process Exit
```

Frame	Module	Location	Address	Path
K 0	ntoskrnl.exe	FsRtlTeardownPerStreamContexts + 0x9aa	0xfffff8000293c42a	C:\Windo
K 1	ntoskrnl.exe	FsRtlTeardownPerStreamContexts + 0x8fd	0xfffff8000293c37d	C:\Windo
K 2	ntoskrnl.exe	PoStartNextPowerIrp + 0x18ea	0xfffff80002674dfa	C:\Windo
K 3	ntoskrnl.exe	PoStartNextPowerIrp + 0x1c30	0xfffff80002675140	C:\Windo
K 4	ntoskrnl.exe	KeSynchronizeExecution + 0x3ae7	0xfffff80002680977	C:\Windo
U 5	ntdll.dll	ZwWaitForWorkViaWorkerFactory + 0xa	0x77962c1a	C:\Windo
U 6	wow64.dll	Wow64EmulateAtlThunk + 0x1c993	0x7438a2f3	C:\Windo
U 7	wow64.dll	Wow64SystemServiceEx + 0xd7	0x7436cf87	C:\Windo
U 8	wow64cpu.dll	TurboDispatchJumpAddressEnd + 0x2d	0x75462776	C:\Windo
U 9	wow64.dll	Wow64SystemServiceEx + 0x1ce	0x7436d07e	C:\Windo
U 10	wow64.dll	Wow64LdrpInitialize + 0x429	0x7436c549	C:\Windo
U 11	ntdll.dll	RtlIsDosDeviceName_U + 0x24c87	0x7798e707	C:\Windo
U 12	ntdll.dll	LdrInitializeThunk + 0xe	0x7793c32e	C:\Windo
U 13	ntdll.dll	ZwWaitForWorkViaWorkerFactory + 0x12	0x77b11f36	C:\Windo
U 14	ntdll.dll	TpSetTimer + 0x302	0x77b3471e	C:\Windo
U 15	kernel32.dll	BaseThreadInitThunk + 0x12	0x765933ca	C:\Windo
U 16	ntdll.dll	RtlInitializeExceptionChain + 0x63	0x77b29ed2	C:\Windo
U 17	ntdll.dll	RtlInitializeExceptionChain + 0x36	0x77b29ea5	C:\Windo

Cybereason RansomFree

- How does RansomFree work?

◎ RansomFree deletes files generated by ransomware



```
[FILEDELETE] VCPU:1 CR3:0x3ff1c000,CybereasonRans SessionID:0 "\Xvalues44\_6_HELP_instructions.html"
[SYSCALL] vCPU:1 CR3:0x3ff1c000,CybereasonRans SessionID:0 ntoskrnl.exe!NtSetInformationFile Arguments: 5
        IN HANDLE FileHandle: 0xa6c -> '\Xvalues44\_6_HELP_instructions.html'
        OUT PIO_STATUS_BLOCK IoStatusBlock: 0x44ae5f0
        IN PVOID FileInformation: 0x44aef40
        IN ULONG Length: 0x1
        IN FILE_INFORMATION_CLASS FileInformationClass: 0xd
```

References

- Wikipedia

https://en.wikipedia.org/wiki/Ransomware

- Knowbe

https://www.knowbe4.com/ransomware

- Heimdal security

https://heimdalsecurity.com/blog/what-is-ransomware-protection