



Practical Malware Analysis & Triage

Malware Analysis Report

WannaHusky

Oct 2022 | Vien Amor V | v1.0



Table of Contents

Table of Contents.....	2
Executive Summary.....	3
High-Level Technical Summary	4
Malware Composition.....	6
Basic Static Analysis	8
Basic Dynamic Analysis	10
Advanced Static Analysis.....	12
Advanced Dynamic Analysis	15
Indicators of Compromise	17
Network Indicators	Error! Bookmark not defined.
Host-based Indicators.....	Error! Bookmark not defined.
Rules & Signatures	18
Appendices	Error! Bookmark not defined.
A. Yara Rules.....	Error! Bookmark not defined.
B. Callback URLs	Error! Bookmark not defined.
C. Decompiled Code Snippets	Error! Bookmark not defined.

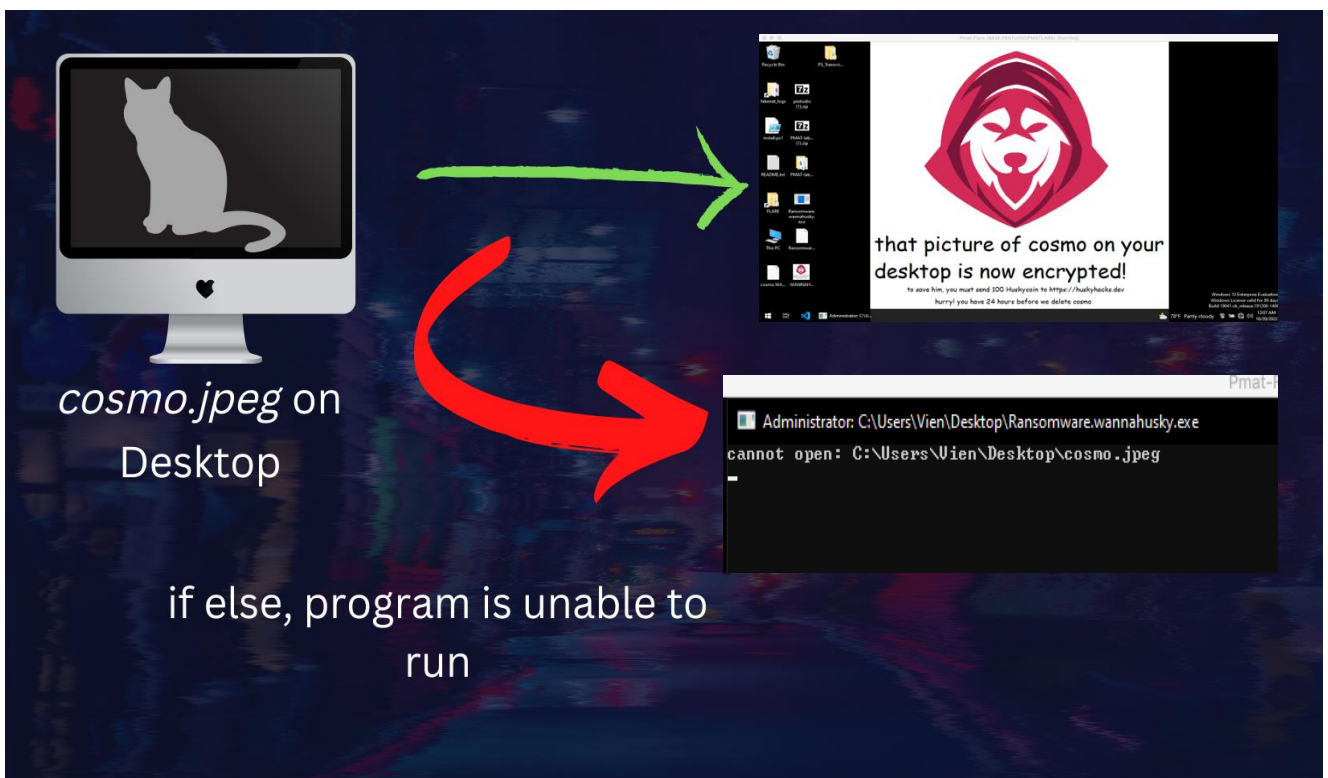
Executive Summary

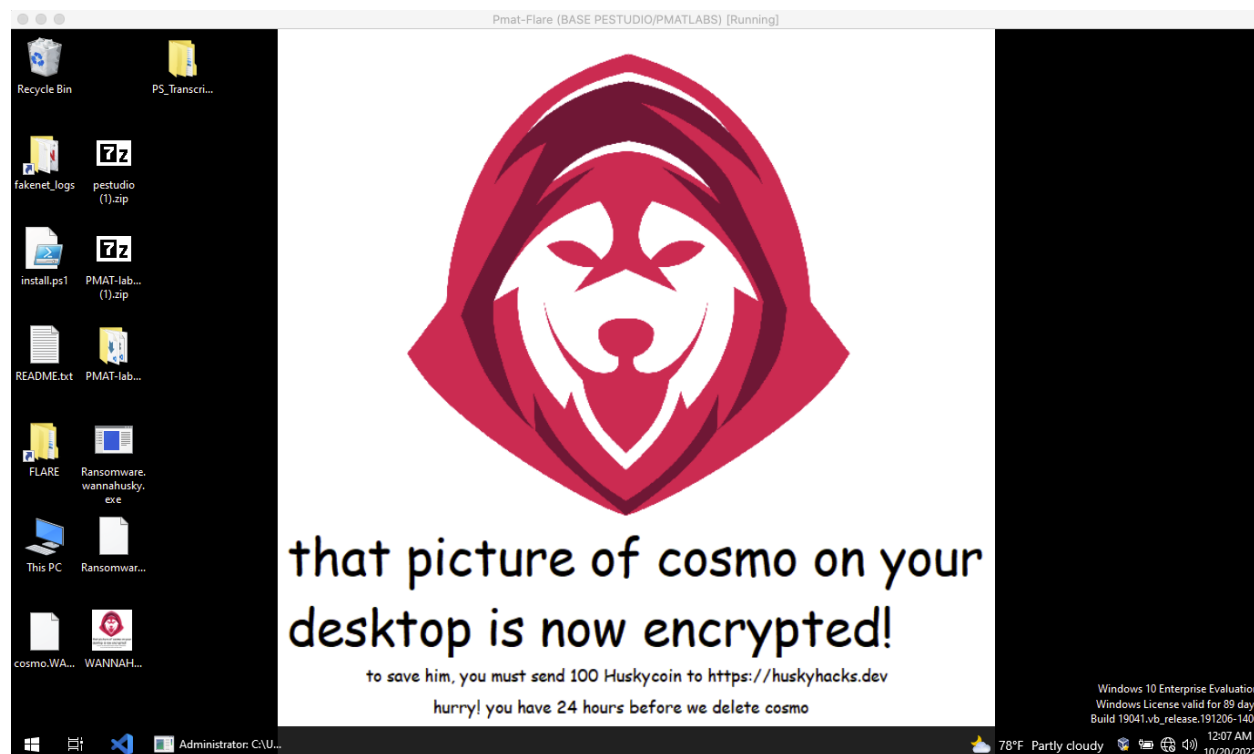
Filename	Ransomware[.]wannahusky[.]exe
SHA256 hash	3d35cebcf40705c23124fdc4656a7f400a316b8e96f1f9e0c187e82a9d17dca3

WannaHusky is a ransomware that requires encrypts files, specifically *cosmo.jpeg*, and demands Huskycoin as payment for files to be decrypted. It is a binary compiled using Nim and defaces the users' desktop. For this program to be executed, *cosmos.jpeg*, must be enabled on the users' desktop; if not, a cmd prompt will execute and program will not run intended. When executed correctly, user experiences a large HuskyHacks Logo in the background under the filename *WANNAHUSKY.png*. File *cosmo.jpeg* now becomes *cosmo.WANNAHUSKY* (encrypted). Finally, executable file *ps1.ps1* is located on the desktop which runs a command prompt executing a process tree.

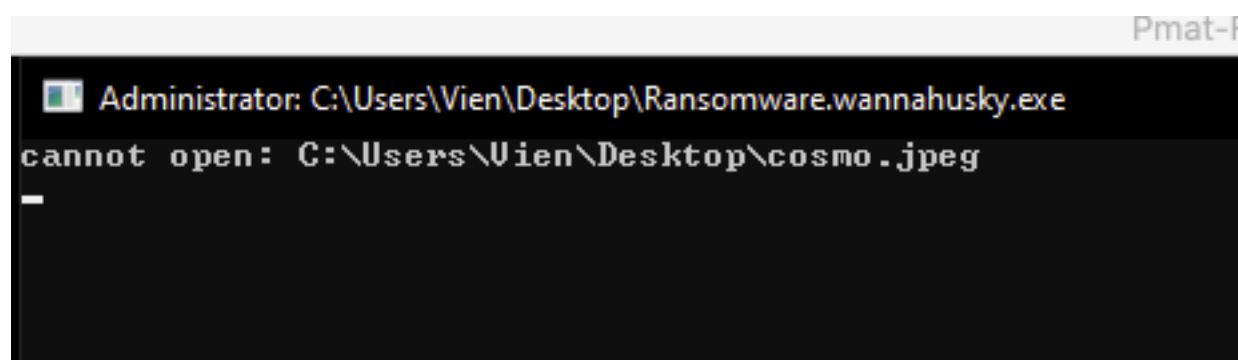
High-Level Technical Summary

For WannaHusky to be executed, a filename *cosmos.jpeg* must be on the user's desktop. If *cosmos* is not located on desktop, we get an error and ransomware does not run as intended.





(Figure 1.1 – Enlarged Successful Ransomware Execution)



(Figure 1.2 – Enlarged Unsuccessful Ransomware Execution)



Malware Composition

WannaHusky consists of the following components:

Hash Values:

File Name	SHA256 Hash
Ransomware[.]Wannahusky[.]exe	3d35cebcf40705c23124fdc4656a7f400a316b8e96f1f9e0c187e82a9d17dca3
Ps1.ps1	D6317374F879CD4E67FBE9DDC0D283926489F4C0D6CF07D912A247E5CFDE99

Additional resources

OSINT Tools	Description
VirusTotal	33 / 71 security vendors and no sandboxes flagged this file as malicious
AlienVault	File Score 2.8 Low Risk

VirusTotal

3d35cebcf40705c23124fdc4656a7f400a316b8e96f1f9e0c187e82a9d17dca3

33 / 71

33 security vendors and no sandboxes flagged this file as malicious

3d35cebcf40705c23124fdc4656a7f400a316b8e96f1f9e0c187e82a9d17dca3

Ransomware.wannahusky.exe.malz

403.23 KB Size

2022-10-20 01:47:30 UTC 8 hours ago

detect-debug-environment direct-cpu-clock-access long-sleeps overlay peexe runtime-modules

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 1

Security Vendors' Analysis

Ad-Aware	Gen:Variant.Jaik.60609	ALYac	Trojan.Ransom.Filecoder
Arcabit	Trojan.Jaik.DECC1	Avast	Win32:Trojan-gen
AVG	Win32:Trojan-gen	BitDefender	Gen:Variant.Jaik.60609
BitDefenderTheta	Gen:NN.ZexaF.34726.z8Z@aaL9d5p	Bkav Pro	W32.AIDetect.malware2
Cylance	Unsafe	Elastic	Malicious (moderate Confidence)
Emsisoft	Gen:Variant.Jaik.60609 (B)	eScan	Gen:Variant.Jaik.60609
ESET-NOD32	A Variant Of Win32/Filecoder.OJX	GData	Gen:Variant.Jaik.60609

(Figure 1.3 – VirusTotal Analysis Report)

Ransomware[.]wannahusky[.]exe
Oct 2022
v1.0



AlienVault

The screenshot shows the AlienVault interface with the following details:

- Navigation Bar:** Includes links for Browse, Scan Endpoints, Create Pulse, Submit Sample, API Integration, Malware Families, and a search bar with the hash 3d35cebcf40705c231. It also has Login and Sign Up buttons.
- File Hash:** 3d35cebcf40705c23124fdc4656a7f400a316b8e96f1f9e0c187e82a9d... with an "Add to Pulse" button.
- Analysis Overview:**
 - Analysis Date:** 10 months ago
 - File Score:** 2.8 (Low Risk)
 - Alerts:** network_icmp, deletes_executed_files, creates_exe, suspicious_process, packer_entropy, console_output
 - Related Pulses:** OTX User-Created Pulses (1)
 - Related Tags:** 13 Related Tags: practical, wannahusky, executive summary, desktop, hash [More](#)
 - File Type:** PE32 executable (console) Intel 80386, for MS Windows
 - Compilation Date:** October 10th, 2021 - 10:08:25 AM
 - Size:** 403 KB (412905 bytes)
 - MD5:** 0287b38f8240a025b30c0a231ea403fc
 - SHA1:** 691ac1b4b7b494f7b56eff0b48ba3e31a14e0d7d
 - SHA256:** 3d35cebcf40705c23124fdc4656a7f400a316b8e96f1f9e0c18
 - IMPHASH:** a97ffe6ec502dacc4c154f9dc2b58725
 - PEHASH:** 2ffaf1dc303f3741e0877cfc7262463763f58931
 - External Resources:** [VirusTotal](#)
 - VirusTotal:** VirusTotal API key required
 - Screenshots:** [Redacted]

(Figure 1.4 – AlienVault Analysis)

The screenshot shows the Alerts section of the AlienVault interface. It includes a table of alerts with the following data:

NAME	DESCRIPTION	SEVERITY	ATT&CK TECHNIQUE	TECHNIQUE ID
network_icmp	Generates some ICMP traffic	High		
deletes_executed_files	Deletes executed files from disk	High	Indicator Removal on Host	T1070
creates_exe	Creates executable files on the filesystem	Medium	Execution through Module Load	T1129
suspicious_process	Creates a suspicious process	Medium		
packer_entropy	The binary likely contains encrypted or compressed data indicative of a packer	Medium	Software Packing	T1045
console_output	Command line console output was observed	Low		

(Figure 1.5 – AlienVault Alert Analysis. Additional indicator that IoC removes itself from host if not executed correctly.)

Ransomware[.]wannahusky[.]exe
Oct 2022
v1.0

Showcasing different methods that is essential when triaging malware

Showcasing different methods that is essential when triaging malware

(Figure 1.6 – Using Floss to initially see the strings of the binary. Here we see few examples showing the ransomware sample being built by the Nim binary.)



```
Cmdr
peekDataImpl
writeDataImpl
flushImpl
@cannot write to stream
@tree C:\
@Desktop\ps1.ps1
@powershell
@Desktop\ps1.ps1
@$code = @'
using System.Runtime.InteropServices;
namespace Win32{
    public class Wallpaper{
        [DllImport("user32.dll", CharSet=CharSet.Auto)]
        static extern int SystemParametersInfo (int uAction , int uParam , string lpvParam , int fuWinIni) ;
        public static void SetWallpaper(string thePath){
            SystemParametersInfo(20,0,thePath,3);
        }
    }
}
add-type $code
$currDir = Get-Location
$wallpaper = ".\WANNAHUSKY.PNG"
$fullpath = Join-Path -path $currDir -ChildPath $wallpaper
[Win32.Wallpaper]::SetWallpaper($fullpath)
@Desktop\WANNAHUSKY.png
~rIDATx^
}1JSpT.:
!p;Y`vN!W
$ _P!OqY
^k@/2%F
^+|B%Y3L
)%h%Meo
```

(Figure 1.7 – Another juicy string found in the CLI. Here we see class `Desktop\WANNAHUSKY.png` source-code being built onto the desktop.)

location	flag (13)	hint (4633)	group (10)	value (11171)
0x0000F9C4	-	-	-	readLineImpl
0x0000F9D1	-	-	-	readDataImpl
0x0000F9DE	-	-	-	peekDataImpl
0x0000F9EB	-	-	-	writeDataImpl
0x0000F9F9	-	-	-	flushImpl
0x0000FA03	-	-	-	data
0x0000FA08	-	-	-	pos
0x0000FA27	-	-	-	@cannot write to stream
0x0000FA47	-	-	-	@tree C:\
0x0000FA58	-	file	-	@Desktop\ps1.ps1
0x0000FA73	-	-	-	@powershell
0x0000FA87	-	file	-	@Desktop\ps1.ps1
0x0000FAA7	-	rtti	-	@\$code = @'
0x0000FAB3	-	-	-	using System.Runtime.InteropServices;
0x0000FADA	-	-	-	namespace Win32{
0x0000FAF0	-	-	-	public class Wallpaper{
0x0000FB0D	-	-	-	[DllImport("user32.dll", CharSet=CharSet.Auto)]
0x0000FB43	-	-	-	static extern int SystemParametersInfo (int uAction , int uParam , string lpvParam , int fuW...
0x0000FB80	-	-	-	public static void SetWallpaper(string thePath){
0x0000FBEB	-	-	-	SystemParametersInfo(20,0,thePath,3);
0x0000FC29	-	-	-	add-type \$code
0x0000FC39	-	-	-	\$currDir = Get-Location
0x0000FC51	-	-	-	\$wallpaper = ".\WANNAHUSKY.PNG"

(Figure 1.8 – Additional confirmation of strings within `ransomware[.]wannahusky[.]exe` using pestudio)

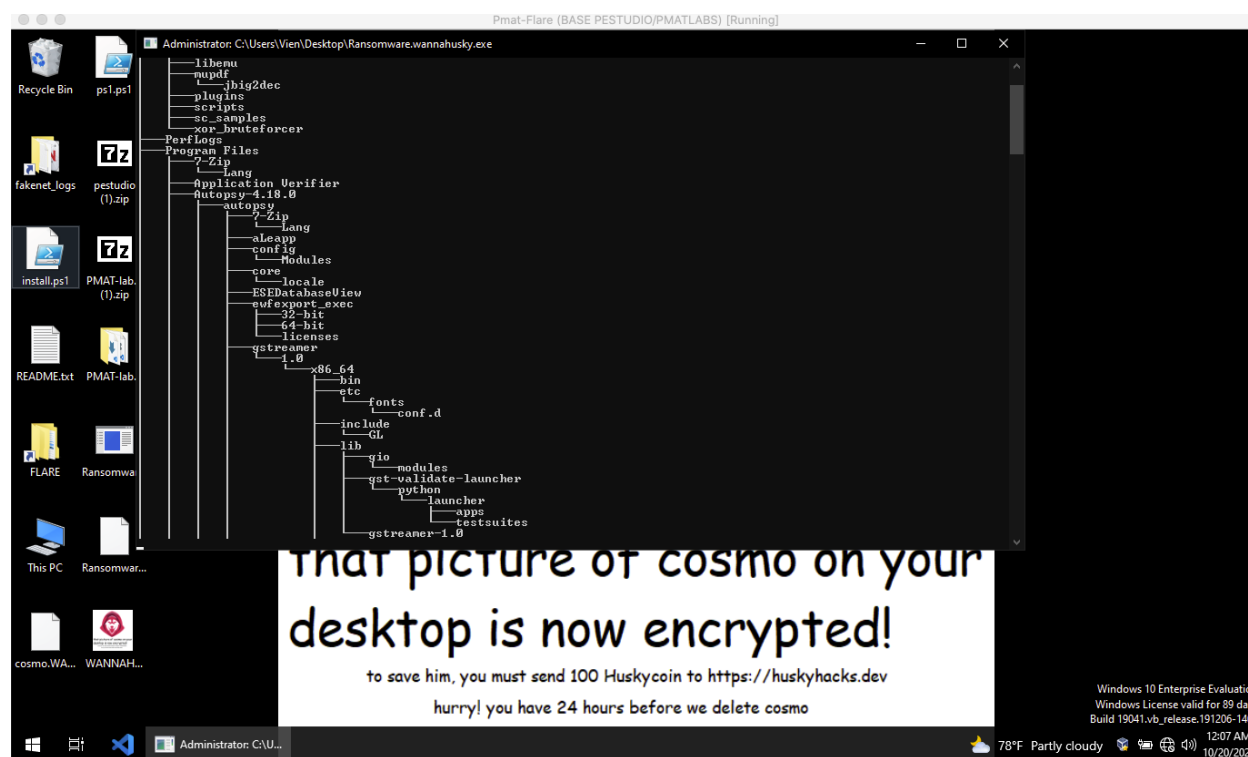


Basic Dynamic Analysis

Initial Detonation

When executable file has been successfully “Run as Administrator”, host computer has now been altered and four new changes has been committed to the users’ desktop. Changes include wallpaper change, encryption of *cosmos.jpeg* -> *cosmos.WANNAHUSKY*, and two new file additions – *WANNAHUSKY.png* and *ps1.ps1* – have been added to the desktop. (See figure 1.1)

Additionally, a command prompt executes onto our computer and we see a stream of processes happening in the command line.



(Figure 1.9 – Commands being executed when binary runs successfully.)

Procmon

Upon detonation we utilize Procmon to see the process of WannaHusky and the Files created within the computer.

Ransomware[.]wannahusky[.]exe
Oct 2022
v1.0



☐ Only show processes still running at end of current trace
☒ Timelines cover displayed events only

Process	Description	Image P...	L	Company	Owner	Command	Start Time
csrss.exe (504)	Client Server Runt...	C:\Wind...		Microsoft Corporat...	NT AUTHORITY\...	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20...	9/25/2022 9:35:2...
winlogon.exe (564)	Windows Logon A...	C:\Wind...		Microsoft Corporat...	NT AUTHORITY\...	winlogon.exe	9/25/2022 9:35:2...
fontdrvhost.exe (700)	Usermode Font Dr...	C:\Wind...		Microsoft Corporat...	Font Driver Host...	"fontdrvhost.exe"	9/25/2022 9:35:2...
dwm.exe (952)	Desktop Window ...	C:\Wind...		Microsoft Corporat...	Window Manager...	"dwm.exe"	9/25/2022 9:35:2...
Explorer.EXE (2660)	Windows Explorer	C:\Wind...		Microsoft Corporat...	C:\Windows\Explorer.EXE		9/25/2022 12:36:...
VBoxTray.exe (3708)	VirtualBox Guest ...	C:\Wind...		Oracle Corporation	DESKTOP-V3RT...	"C:\Windows\System32\VBoxTray.exe"	9/25/2022 12:36:...
msedge.exe (3772)	Microsoft Edge	C:\Progra...		Microsoft Corporat...	DESKTOP-V3RT...	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" -no-startup-window -...	9/25/2022 12:36:...
msedge.exe (3804)	Microsoft Edge	C:\Progra...		Microsoft Corporat...	DESKTOP-V3RT...	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" -type=crashpad-handl...	9/25/2022 12:36:...
msedge.exe (4008)	Microsoft Edge	C:\Progra...		Microsoft Corporat...	DESKTOP-V3RT...	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" -type=utility -utility-su...	9/25/2022 12:36:...
msedge.exe (4016)	Microsoft Edge	C:\Progra...		Microsoft Corporat...	DESKTOP-V3RT...	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" -type=utility -utility-su...	9/25/2022 12:36:...
msedge.exe (4024)	Microsoft Edge	C:\Progra...		Microsoft Corporat...	DESKTOP-V3RT...	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" -type=utility -utility-su...	9/25/2022 12:36:...
Procmon.exe (1528)	Process Monitor	C:\Progra...		Sysinternals - ww...	DESKTOP-V3RT...	"C:\ProgramData\chocolatey\lib\sysinternals\tools\Procmon.exe"	10/20/2022 12:5...
Procmon64.exe (4660)	Process Monitor	C:\Users\...		Sysinternals - ww...	DESKTOP-V3RT...	"C:\Users\Vien\AppData\Local\Temp\Procmon64.exe" /originalpath "C:\ProgramData...	10/20/2022 12:5...
Ransomware.wannahusky.exe (4596)	Ransomware.wannahusky.exe	C:\Users\...			DESKTOP-V3RT...	"C:\Users\Vien\Desktop\Ransomware.wannahusky.exe"	10/20/2022 12:5...
conhost.exe (4624)	Console Window ...	C:\Wind...		Microsoft Corporat...	DESKTOP-V3RT...	"C:\Windows\system32\conhost.exe 0xfffff -ForceV1"	10/20/2022 12:5...
cmd.exe (4560)	Windows Comma...	C:\Wind...		Microsoft Corporat...	DESKTOP-V3RT...	C:\Windows\system32\cmd.exe /c powershell C:\Users\Vien\Desktop\ps1.ps1	10/20/2022 12:5...
powershell.exe (1140)	Windows PowerS...	C:\Wind...		Microsoft Corporat...	DESKTOP-V3RT...	powershell C:\Users\Vien\Desktop\ps1.ps1	10/20/2022 12:5...
GoogleCrashHandler.exe (3608)	Google Crash Han...	C:\Progra...		Google LLC	NT AUTHORITY\...	"C:\Program Files (x86)\Google\Update\1.3.36.152\GoogleCrashHandler.exe"	9/25/2022 12:36:...
GoogleCrashHandler64.exe (3620)	Google Crash Han...	C:\Progra...		Google LLC	NT AUTHORITY\...	"C:\Program Files (x86)\Google\Update\1.3.36.152\GoogleCrashHandler.exe"	9/25/2022 12:36:...

Description:
Company:
Path: C:\Users\Vien\Desktop\Ransomware.wannahusky.exe
Command: "C:\Users\Vien\Desktop\Ransomware.wannahusky.exe"
User: DESKTOP-V3RTA1S\Vien
PID: 4596 Started: 10/20/2022 12:51:41 AM
Exited: 10/20/2022 12:51:46 AM

Go To Event Include Process Include Subtree Close

(Figure 2.0 – Utilizing Procmon to see the parent tree of Ransomware WannaHusky.)

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
11:50:...	Ransomware.w...	2004	Process Start		SUCCESS	Parent PID: 2660, ...
11:50:...	Ransomware.w...	2004	Thread Create		SUCCESS	Thread ID: 3156
11:50:...	Ransomware.w...	2004	Load Image	C:\Users\Vien\Desktop\Ransomware.wannahusky.exe	SUCCESS	Image Base: 0x400...
11:50:...	Ransomware.w...	2004	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7fd...
11:50:...	Ransomware.w...	2004	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x7fd...
11:50:...	Ransomware.w...	2004	CreateFile	C:\Windows\Prefetch\RANSOMWARE.WANNAHUSKY.EXE...	NAME NOT FOUND	Desired Access: G...
11:50:...	Ransomware.w...	2004	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Q...
11:50:...	Ransomware.w...	2004	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Q...
11:50:...	Ransomware.w...	2004	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\...	NAME NOT FOUND	Length: 80
11:50:...	Ransomware.w...	2004	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
11:50:...	Ransomware.w...	2004	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\...	REPARSE	Desired Access: Q...
11:50:...	Ransomware.w...	2004	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\...	NAME NOT FOUND	Desired Access: Q...
11:50:...	Ransomware.w...	2004	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\...	REPARSE	Desired Access: Q...
11:50:...	Ransomware.w...	2004	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
11:50:...	Ransomware.w...	2004	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\...	NAME NOT FOUND	Length: 24
11:50:...	Ransomware.w...	2004	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
11:50:...	Ransomware.w...	2004	CreateFile	C:\Windows	SUCCESS	Desired Access: E...
11:50:...	Ransomware.w...	2004	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x7fd...
11:50:...	Ransomware.w...	2004	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x7fd...
11:50:...	Ransomware.w...	2004	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access: R...
11:50:...	Ransomware.w...	2004	CreateFile	C:\Windows	SUCCESS	Desired Access: R...
11:50:...	Ransomware.w...	2004	QueryNameInfo	C:\Windows	SUCCESS	Name: \Windows
11:50:...	Ransomware.w...	2004	CloseFile	C:\Windows	SUCCESS	
11:50:...	Ransomware.w...	2004	RegOpenKey	HKLM\Software\Microsoft\Wow64\...	SUCCESS	Desired Access: R...
11:50:...	Ransomware.w...	2004	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\...	NAME NOT FOUND	Length: 520
11:50:...	Ransomware.w...	2004	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\...	SUCCESS	Type: REG_SZ, Le...
11:50:...	Ransomware.w...	2004	RegCloseKey	HKLM\SOFTWARE\Microsoft\Wow64\...	SUCCESS	
11:50:...	Ransomware.w...	2004	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x7fd...
11:50:...	Ransomware.w...	2004	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Q...

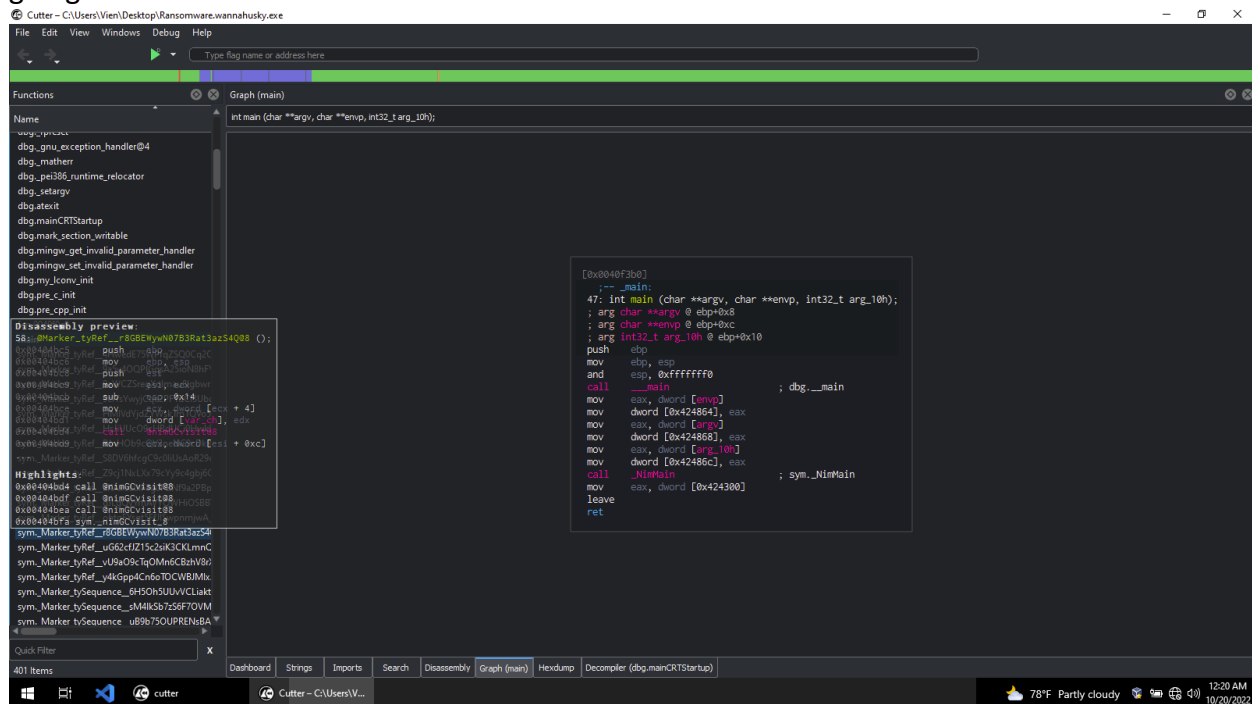
Showing 417 of 405,534 events (0.10%) Backed by virtual memory

(Figure 2.1 – Deeper Procmon Investigation. Here we filter out Parent Name understand the process of how WannaHusky is executed within the hosts' binary.)

Ransomware[.]wannahusky[.]exe
Oct 2022
v1.0

Advanced Static Analysis

We dig deeper utilizing Cutter to understand the innards of this malware to fully grasp what is going on.



(Figure 2.2 – Finding the main call function in the malware sample. Note: “main” is the primary function where the executable file begins its execution.)

There will be three functions/strings that we will be utilizing in within Cutter.

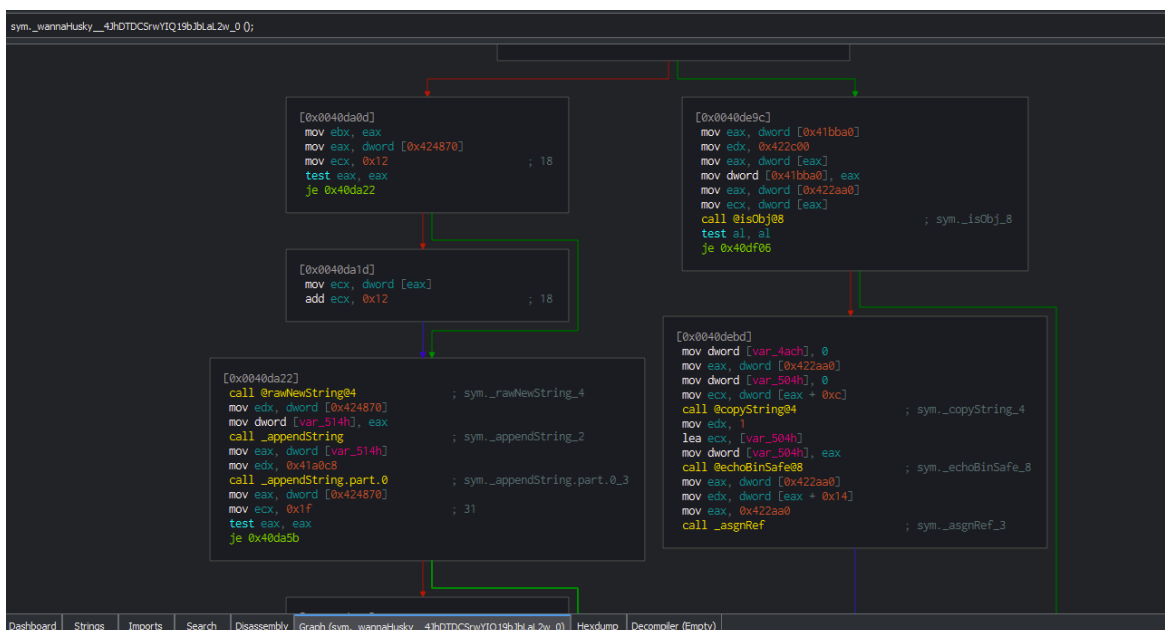
- Sym._wannahusky_4JhTDCSrWYIQ19bJbLaL2w_0
 - Function responsible for encryption and deletion of *cosmos.jpeg* and rewriting it as *cosmo.WANNAHUSKY.png*.
- Sym._changeBackground_4JhDTDCSrrwYIQ19bJbLaL2w_2_0
 - Responsible for changing the Desktop Background.
- Sym._nosexecShellCmd_4
 - Responsible for spawning *ps1.ps1* on the Desktop.



Sym. wannaHusky 4JhTDCSrWYIQ19bJbLaL2w 0

```
[0x0040d9c7]
1365: @wannaHusky__4JhTDCSrWYIQ19bJbLaL2w@0 ();
; var int32_t var_534h @ ebp-0x534
; var int32_t var_530h @ ebp-0x530
; var int32_t var_52ch @ ebp-0x52c
; var int32_t var_528h @ ebp-0x528
; var int32_t var_524h @ ebp-0x524
; var int32_t var_520h @ ebp-0x520
; var uint32_t var_51ch @ ebp-0x51c
; var uint32_t var_518h @ ebp-0x518
; var int32_t var_514h @ ebp-0x514
; var uint32_t var_510h @ ebp-0x510
; var uint32_t var_50ch @ ebp-0x50c
; var int32_t var_504h @ ebp-0x504
; var int32_t var_500h @ ebp-0x500
; var int32_t var_4f0h @ ebp-0x4f0
; var int32_t var_4d0h @ ebp-0x4d0
; var int32_t var_4b0h @ ebp-0x4b0
; var uint32_t var_4ach @ ebp-0x4ac
; var int32_t var_4a8h @ ebp-0x4a8
; var int32_t var_468h @ ebp-0x468
; var int32_t var_240h @ ebp-0x240
; var int32_t var_ch @ ebp-0xc
; var int32_t var_4h_4 @ esp+0x10
; var int32_t var_4h_3 @ esp+0x1c
; var int32_t var_8h @ esp+0x20
; var int32_t var_4h_2 @ esp+0x28
; var int32_t var_4h @ esp+0x2c
; var int32_t var_8h_2 @ esp+0x30
; var int32_t var_sp_ch @ esp+0x34
; var int32_t var_10h @ esp+0x38
; var int32_t var_14h @ esp+0x3c
push ebp
mov ebp, esp
push edi
push esi
push ebx
sub esp, 0x54c
mov eax, dword [0x41bba0]
mov dword [var_4h], 0
mov dword [var_4b0h], eax
```

(Figure 2.3 – Main call for wannaHusky beginning to allocate different strings and functions within Cutter)

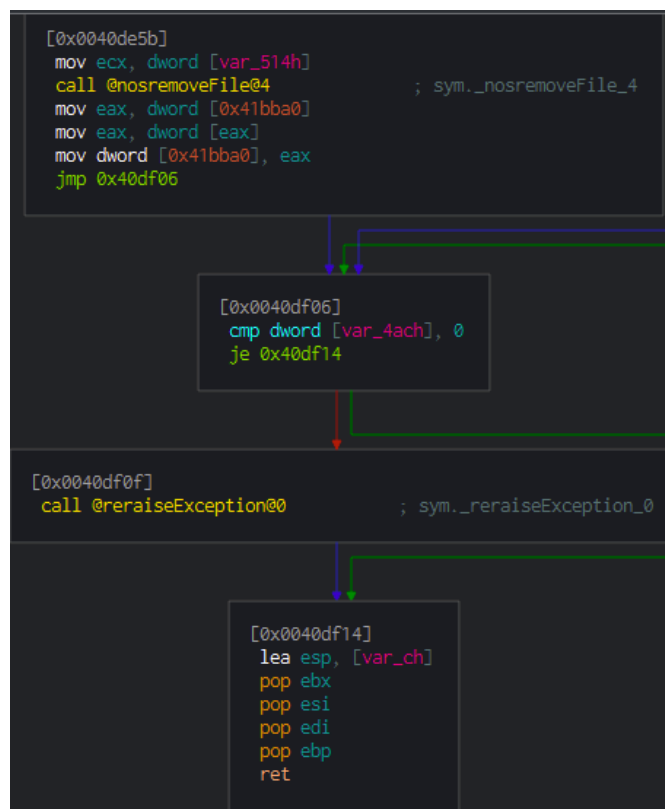




(Figure 2.4 – Main Calls breaking out into different functions)

```
[0x0040dde7]
call @rawNewString@4          ; sym._rawNewString_4
mov  edx, dword [0x424870]
call _appendString           ; sym._appendString_2
mov  edx, 0x41a000
call _appendString.part.0    ; sym._appendString.part.0_3
mov  edx, ebx
mov  ecx, eax
call @writeFile__D6Pj9c29aCLEJP9beOWa08HYA@8 ; sym._writeFile__D6Pj9c29aCLEJP9beOWa08HYA_8
mov  ecx, 0x412100
call @newStringStream__9aLRtgEYeRMrZKrObto0slQ@4 ; sym._newStringStream__9aLRtgEYeRMrZKrObto0slQ_4
mov  eax, dword [0x424870]
mov  ecx, 0x16                ; 22
test eax, eax
je  0x40de27
```

(Figure 2.5 – Function where cosmo.jpeg begins to be rewritten.)



(Figure 2.6 – Final removal of cosmo.jpeg and spawn of encrypted comso.WANNACRY)



Advanced Dynamic Analysis

Further Analysis within Cutter debugging WannaHusky.

Sym. changeBackground_4JhDTDCSrwYIQ19bJbLaL2w_2_0

```
Decompiler (sym._wannaHusky__4JhDTDCSrwYIQ19bJbLaL2w_0)

for (iVar5 = 8; iVar5 != 0; iVar5 = iVar5 + -1) {
    *piVar7 = *piVar4;
    piVar4 = piVar4 + 1;
    piVar7 = piVar7 + 1;
}
@init__QeKCvRTxwnkv4EgDHKgXYA@20(0x20, (int32_t)&var_500h, 0x10);
uVar6 = arg_ch;
if (placeholder_19 != (uint32_t *)0x0) {
    uVar6 = *placeholder_19;
}
_encrypt__dcoBdmUaaCC9cnR23eFSLAbcmode((int32_t)(placeholder_19 + 2), uVar6);
@burnMem__4FZHyZ34TGxTmMy6XY9c0Sg@8();
@init__QeKCvRTxwnkv4EgDHKgXYA@20(0x20, (int32_t)&var_500h, 0x10);
if (placeholder_15 != (uint32_t *)0x0) {
    arg_ch = *placeholder_15;
}
_encrypt__dcoBdmUaaCC9cnR23eFSLAbcmode((int32_t)(placeholder_15 + 2), arg_ch);
@burnMem__4FZHyZ34TGxTmMy6XY9c0Sg@8();
@encode__npLRSgmGJDNX8bfurW5iRw@12(0);
@rawNewString@4(extraout_ECX);
_appendString();
_appendString.part.0();
@writeFile__D6Pj9c29aCLEJP9be0Wa08HYA@8();
@newStringStream__9aLRtgEYeRMrZKr0bto0s1Q@4();
@rawNewString@4();
_appendString();
_appendString.part.0();
iVar5 = @newFileStream__cwYJiP3D7DOTCJxCdBqBZQ@12(-1);
if (iVar5 != 0) {
    uVar2 = @writeLine__2KoDZXJB4LmoH7PHLGmZ9cg@12(1);
    @close__y1KA3B0U09bKtU09am9a9avRYQ_4@4(uVar2);
}
@nosremoveFile@4();
*(int32_t *)0x41bba0 = (int32_t *)0x41bba0;
} else {
    *(int32_t *)0x41bba0 = (int32_t *)0x41bba0;
    cVar1 = @isObj@8();
    if (cVar1 != '\0') {
        var_4ach = 0;
        @copyString@4();
        @echoBinSafe@8();
        _asgnRef();
    }
}
```

(Figure 2.7 – Decompiler of changeBackground___*** showing files being encrypted, encoded, and removed. Note: For this specific language Ghidra language must be enabled.)



Sym. nosexecShellCmd 4

```
Decompiler (sym._wannaHusky_4JhDTDCSrwYIQ19bJbLaL2w_0)

}
@init__QeKCvRTxwnkv4EgDHkgXYA@20(0x20, (int32_t)&var_500h, 0x10);
uVar6 = arg_ch;
if (placeholder_19 != (uint32_t *)0x0) {
    uVar6 = *placeholder_19;
}
_encrypt__dcoBdmUaaCC9cnR23eFSLAbcmode((int32_t)(placeholder_19 + 2), uVar6);
@burnMem__4FZHyZ34TGxTmMy6XY9cOSg@8();
@init__QeKCvRTxwnkv4EgDHkgXYA@20(0x20, (int32_t)&var_500h, 0x10);
if (placeholder_15 != (uint32_t *)0x0) {
    arg_ch = *placeholder_15;
}
_encrypt__dcoBdmUaaCC9cnR23eFSLAbcmode((int32_t)(placeholder_15 + 2), arg_ch);
@burnMem__4FZHyZ34TGxTmMy6XY9cOSg@8();
@encode__npLRSgmGJDNX8bfurW5iRw@12(0);
@rawNewString@4(extraout_ECX);
_appendString();
_appendString.part.0();
@writeFile__D6Pj9c29aCLEJP9beOWa08HYA@8();
@newStringStream__9aLRtgEYeRMrZKrObtoOs1Q@4();
@rawNewString@4();
_appendString();
_appendString.part.0();
iVar5 = @newFileStream__cwYJiP3D7DOTCJxCdBqBZQ@12(-1);
if (iVar5 != 0) {
    uVar2 = @writeLine__2KoDZXJB4LmoH7PHLGmZ9cg@12(1);
    @close__y1KA3B0U09bKtU09am9a9avRYQ_4@4(uVar2);
}
@nosremoveFile@4();
*(int32_t *)0x41bba0 = (int32_t *)*(int32_t *)0x41bba0;
} else {
    *(int32_t *)0x41bba0 = (int32_t *)*(int32_t *)0x41bba0;
    cVar1 = @isObj@8();
    if (cVar1 != '\0') {
        var_4ach = 0;
        @copyString@4();
        @echoBinSafe@8();
        _asgnRef();
    }
}
```

(Figure 2.8 – Decompiler of nosexecShellCmd also displaying encryption, encoding, and writeFiles.)



Indicators of Compromise

Network Indicators

Detonating WannaHusky does not beacon out to any external URL file while having REMNux, inetsim, and wireshark enabled. There has not been any attempt within ransomware[.]wannacry[.]exe to reach out to any other hosts or domain, therefore no network indicators currently.

Host-Based Indicators

- Ransomware note saved on the Desktop both as background and *WANNAHUSKY.png*
- Spawn of ps1.ps1
- *Cmd.exe* window and a Processing tree is being executed



Yara Rules & Signatures

Yara rules based on investigation and triaging. These rules will help mitigate and detect if ransomware[.]wannahusky[.]exe will be executed on the host computer.

```
// V. Yara Rule Writing

rule wannaHusky_yara {

  meta:
    author = "Vien"
    date = "2022-10-20"
    desc = "Creating Yara Rules for WannaHusky Ransomware"
    file = "Ransomware[.]wannahusky[.]exe"
    hash = "3d35cebcf40705c23124fdc4656a7f400a316b8e96f1f9e0c187e82a9d17dca3"

  strings:
    // Generating a set of strings to set the criteria for our rule
    $string1 = "WANNAHUSKY.png" ascii
    $string2 = "./build" ascii
    $string3 = "cosmo.WANNAHUSKY" ascii
    $string4 = "MZ" ascii

  condition:
    // Fill out conditions that must be met to identify binary
    $string4 at 0 and
    ($string2 or $string3 or $string1)
}
```

(Figure 2.9 – Yara rules based on criteria found within the ransomware binary)



```
Cmdr
λ yara32 yara.rule Ransomware.wannahusky.exe -s -w -p 32
wannahusky_yara Ransomware.wannahusky.exe
0xfc0:$string1: WANNAHUSKY.png
0x19486:$string2: ./build
0x20786:$string2: ./build
0x2570c:$string2: ./build
0x2aa6a:$string2: ./build
0x2ab45:$string2: ./build
0x2ad25:$string2: ./build
0x2fdac:$string2: ./build
0x3262b:$string2: ./build
0x32702:$string2: ./build
0x34a23:$string2: ./build
0x34c92:$string2: ./build
0x3502a:$string2: ./build
0x35109:$string2: ./build
0x351ec:$string2: ./build
0x3b2af:$string2: ./build
0x3b5e9:$string2: ./build
0x3b6c3:$string2: ./build
0x40e96:$string2: ./build
0x4356a:$string2: ./build
0x4364b:$string2: ./build
0x43768:$string2: ./build
0x494e3:$string2: ./build
0x495d7:$string2: ./build
0x49878:$string2: ./build
0x17c10:$string3: cosmo.WANNAHUSKY
0x17cb7:$string3: cosmo.WANNAHUSKY
0x0:$string4: MZ
```

(Figure 3.0 – Successful Yara Rule execution against Ransomware[.]wannahusky[.]exe)



Conclusion

WannaHusky[.]exe is a ransomware developed by Threat Actor HuskyHacks, where group demands crypto payment for the decryption of file *cosmos.jpeg*. However, for program to fully run, *cosmos.jpeg* must be located on the Desktop. At the time of writing, there has been no remediation or mitigation techniques to remove ransomware[.]wannahusky[.]exe at this time.