ICELAND.EXE

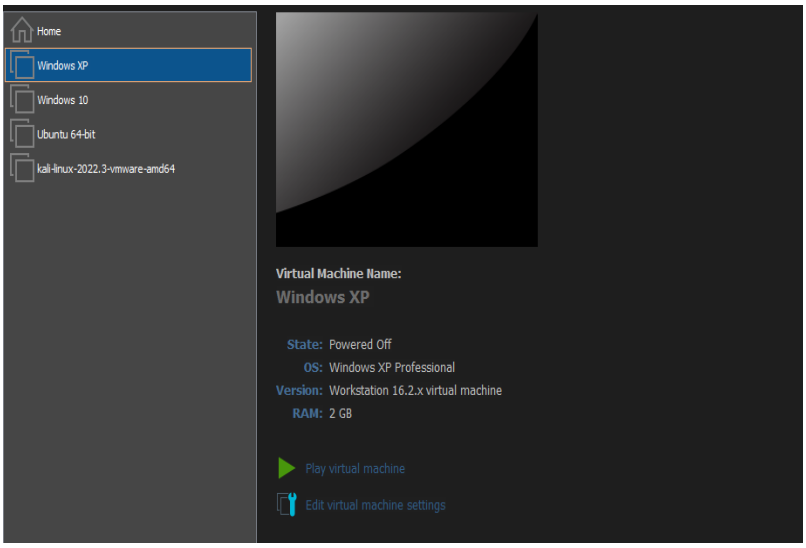
MALWARE ANALYSIS

Presented for :
Qasem Abu Al-Haija

Presented by :
Ahmad Althyab
Ali AlDrabkih

Set up a virtualized environment using VMware Player for Win-XP/Win-10 Oss :

I have two environments to work on:



Windows XP (32-bit):

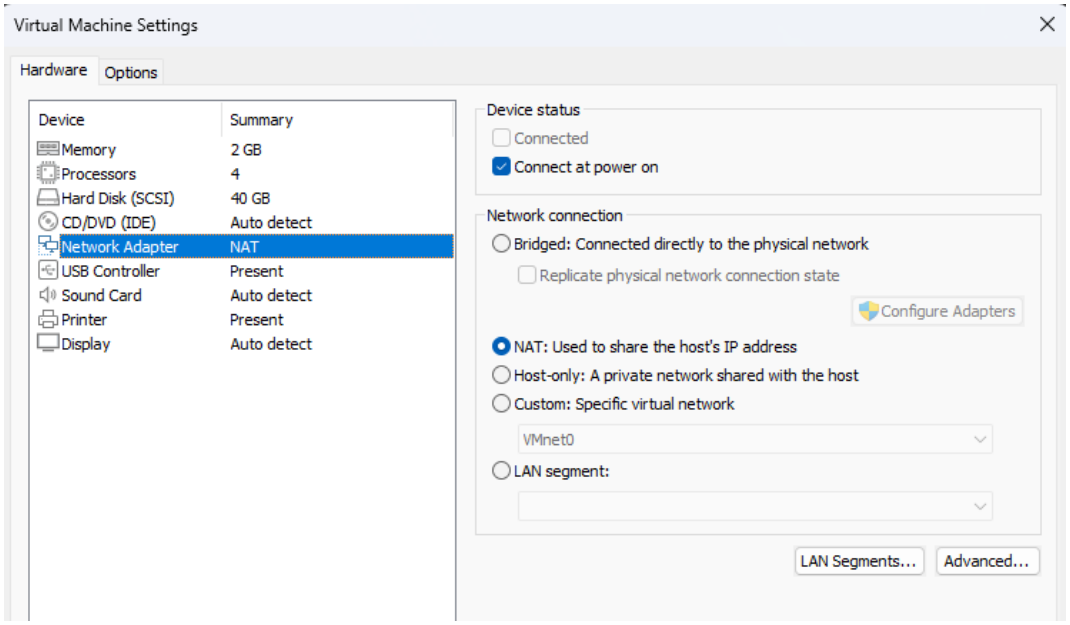
- Legacy environment for studying older malware.
- Vulnerable system due to lack of updates.

Windows 10:

- Modern architecture for analyzing current malware.
- Enhanced security with regular update

Combining both Windows XP and Windows 10 environments provides a comprehensive analysis platform, covering both legacy and contemporary aspects of malware behavior.

Configure your virtual networking using NAT mode.



Using **NAT** in the VM for malware analysis provides a **secure and efficient setup**. It allows the VM to access the internet while safeguarding its internal structure, ensuring anonymity. NAT's mapping of private to public IP addresses enhances security and resource utilization in the analysis environment.

Search the internet for malware (.exe) for Windows XP OS and I found this malware:

Name: Iceland

Type of File: Application (.exe)

Description: Iceland

Location: C:\Documents and Settings\Administrator\Desktop

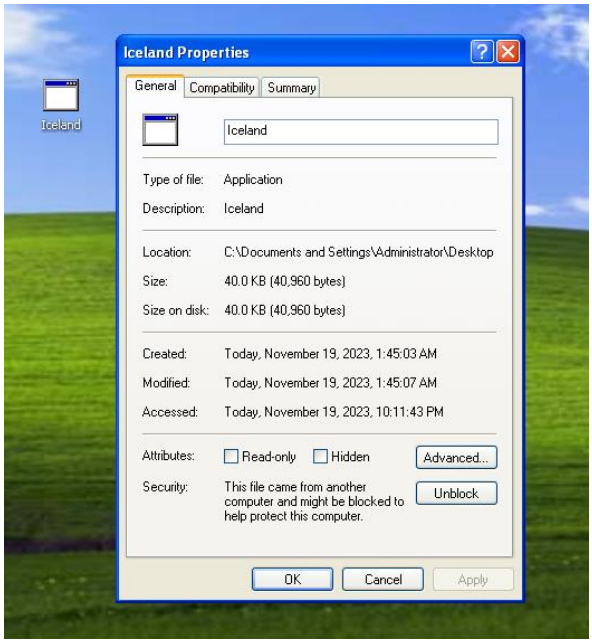
Size: 40.0 KB (40,960 bytes)

Size on Disk: 40.0 KB (40,960 bytes)

Created: November 19, 2023, 1:45:03 AM

Modified: November 19, 2023, 1:45:07 AM

Accessed: November 19, 2023, 10:11:43 PM



This file, named "Iceland," is identified as an application with a size of 40.0 KB. Located on the desktop.

static malware analysis

VirusTotal:

The analysis on **VirusTotal** for **"Iceland.exe"** by **35 security vendors**, including no sandbox detections, reveals the following details:

File Name: Iceland.exe

File Hash (SHA256):
36185cabb5d7838465ab8b507dd1031833147f5aa6a9016a71caf4552244b098

Basic properties

MD5	c997f4dbbd2190dd8ad1713a23867467
SHA-1	d7ef27ac1182336153dcc9c4b645665e31298fdd
SHA-256	36185cabb5d7838465ab8b507dd1031833147f5aa6a9016a71caf4552244b098
Vhash	044056651d15556bzcvz9025z
Authentihash	4a265c67fb0aba9803159334f5973d33689454f40c70137dea0306dd7b2c1a1a
Imphash	9fd725b5ac22007b9a790400d7a16a70
SSDEEP	768:NyzrM0ZGS3fNjReE5XpQHKAGwDFZ7KjdSd:1SPdReElpQCwDFqdG
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable for MS Windows (console) Intel 80386 32-bit
TrID	Win64 Executable (generic) (61.7%) | Win32 Dynamic Link Library (generic) (14.7%) | Win32 Executable (generic) (10%) | OS/2 Executable (generic) (4.5%) | Generic Win/DOS Executable (4.4%)
File size	40.00 KB (40960 bytes)

His target is Machine Intel 386 or later processors and compatible processors.

And it has one relation:

Contacted IP addresses (1)

IP	Detections	Autonomous System	Country
20.189.79.72	0 / 88	8075	HK

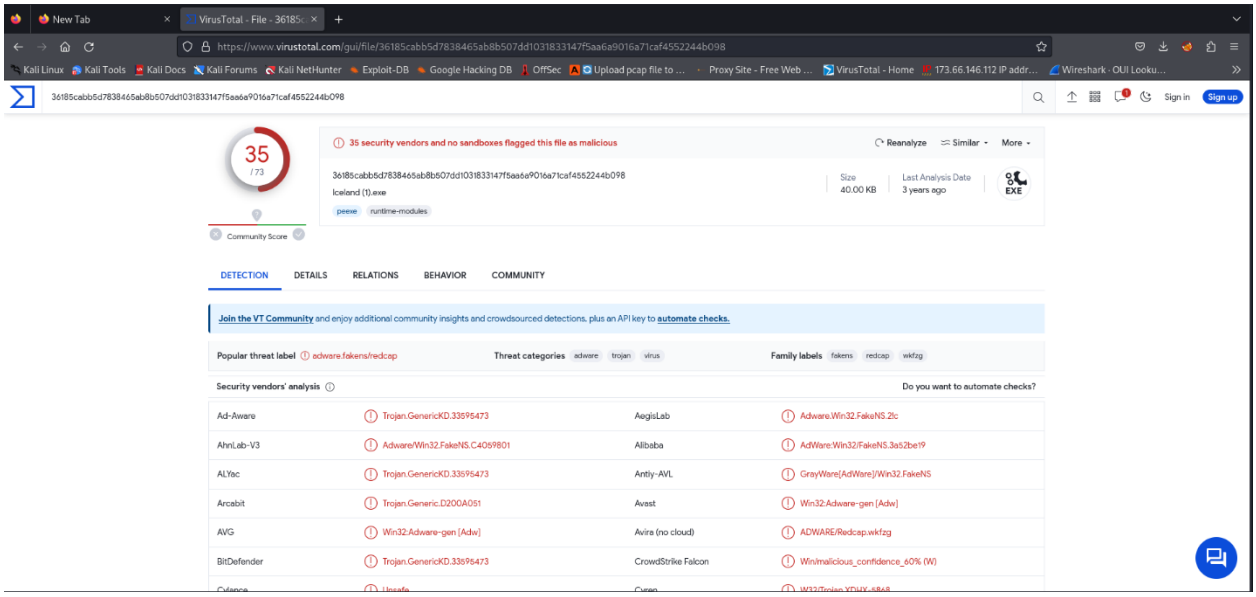
Graph Summary

Detected Threat Categories:

- Adware
- Trojan
- Virus

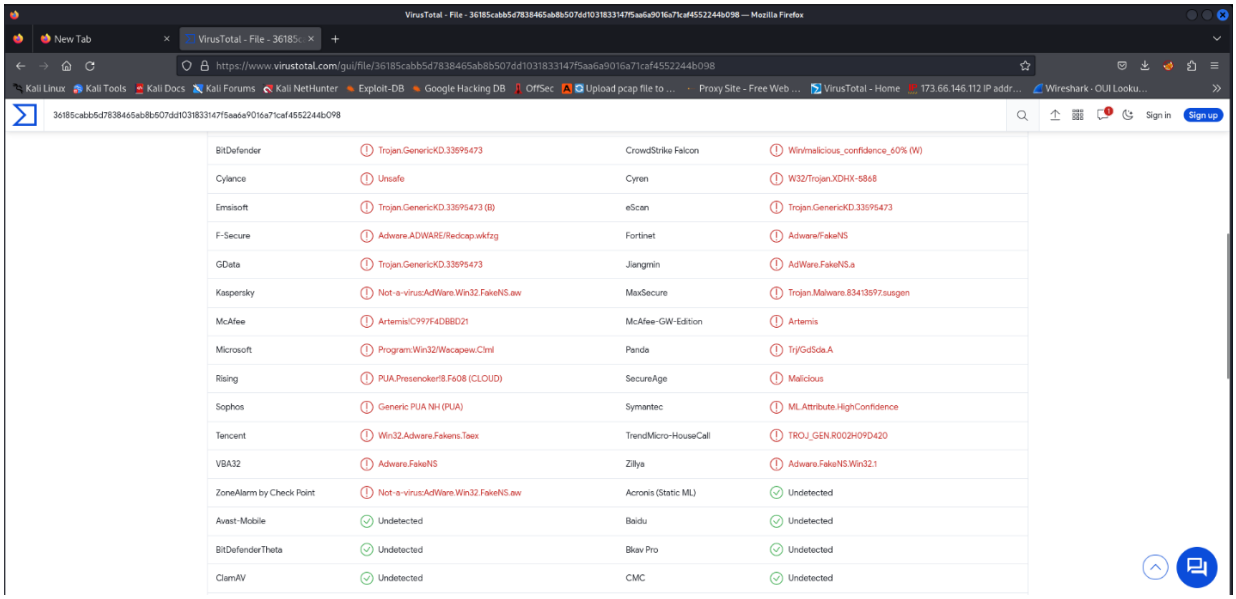
Family Labels:

- Fakens
- Redcap
- Wkfzg



Notable Vendor Detections:

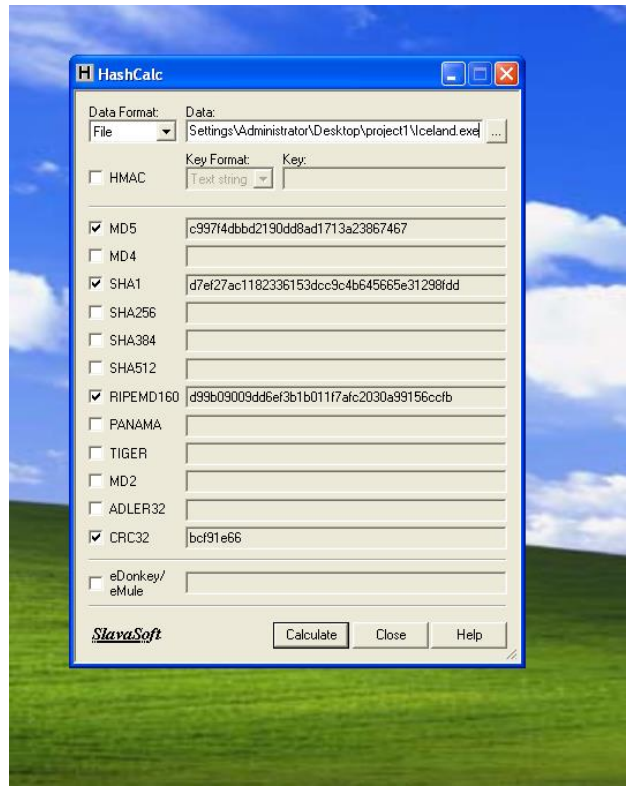
- **Ad-Aware:** Trojan.GenericKD.33595473
- **AhnLab-V3:** Adware/Win32.FakeNS.C4059801
- **Alibaba:** AdWare:Win32/FakeNS.3a52be19
- **Avira:** ADWARE/Redcap.wkfzg
- **BitDefender:** Trojan.GenericKD.33595473
- **CrowdStrike Falcon:** Win/malicious_confidence_60% (W)
- **Kaspersky:** Not-a-virus:AdWare.Win32.FakeNS.aw
- **Microsoft:** Program:Win32/Wacapew.C!ml
- **Sophos:** Generic PUA NH (PUA)
- **Symantec:** ML.Attribute.HighConfidence



BitDefender	Trojan.GenericKD.33595473	CrowdStrike Falcon	Win/malicious_confidence_60% (W)
Cylance	Unsafe	Cyren	W32/Trojan.XDHX-5868
Emsisoft	Trojan.GenericKD.33595473 (B)	eScan	Trojan.GenericKD.33595473
F-Secure	Adware.ADWARE/Redcap.wkfzg	Fortinet	Adware/FakeNS
GData	Trojan.GenericKD.33595473	Jiangmin	AdWare.FakeNS.a
Kaspersky	Not-a-virus:AdWare.Win32.FakeNS.aw	MaxSecure	Trojan.Malware.834135 97.susgen
McAfee	Artemis!C997F4DBBD21	McAfee-GW-Edition	Artemis
Microsoft	Program:Win32/Wacapew.C!ml	Panda	Trj/GdSda.A
Rising	PUA.Presenoker!8.F608 (CLOUD)	SecureAge	Malicious
Sophos	Generic PUA NH (PUA)	Symantec	ML.Attribute.HighConfidence
Tencent	Win32.Adware.Fakens.Tsex	TrendMicro-HouseCall	TROJ_GEN.R002H09D420
VBA32	Adware.FakeNS	Zillya	Adware.FakeNS.Win32.1
ZoneAlarm by Check Point	Not-a-virus:AdWare.Win32.FakeNS.aw	Acronis (Static ML)	Undetected
Avast-Mobile	Undetected	Baidu	Undetected
BitDefenderTheta	Undetected	Bkav Pro	Undetected
ClamAV	Undetected	CMC	Undetected

These results collectively indicate a consensus among security vendors regarding the file's association with adware and Trojan categories, with family labels such as Fakens, Redcap, and Wkfzg.

The hash values obtained using HashCalc for the analyzed file are as follows:



MD5: c997f4dbbd2190dd8ad1713a23867467

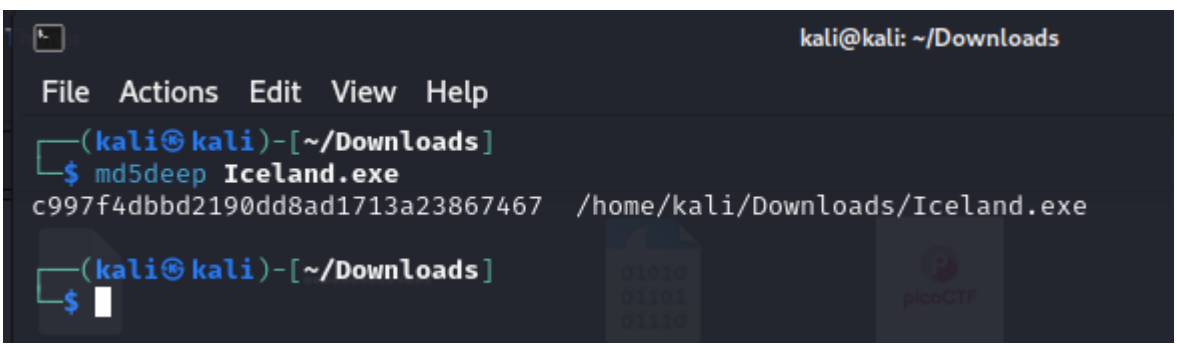
SHA1: d7ef27ac1182336153dcc9c4b645665e31298fdd

These hash values serve as unique fingerprints for the file, aiding in verification and comparison during malware analysis.

MD5Deep :

The MD5 hash value for the file **"Iceland.exe",** obtained using the **md5deep** command, is:

c997f4dbbd2190dd8ad1713a23867467



HashDeep :

Consistent hash values across multiple tools, like HashCalc, md5deep and HashDeep , confirm the file's unchanged content and enhance reliability in malware analysis.

Strings :

The provided strings output indicates a mix of recognizable strings, potential indicators of malicious behavior, and references to system functions and libraries. Here's a summarized overview:

Strings of Interest:

- "This!sN@tThe51ag"
- "thisisnotaproperurltohaaveadnsentrybutletstry.try"
- "Thisismyperfectdomainwhichwillrevealtheflag123456789.flag"

```
This!sN@tThe51ag
thisisnotaproperurltohaaveadnsentrybutletstry.try
Thisismyperfectdomainwhichwillrevealtheflag123456789.flag
```

- "Connection: close"
- "GET / HTTP/1.1"
- "Host: hoba_yalla"

```
Host:
hoba_yalla
```

File Paths and Debug Information:

- "C:\Users\Kamal\Documents\yasuo\Release\yasuo.pdb"
- References to various sections and libraries like "MSVCP140.dll," "WS2_32.dll," and "KERNEL32.dll."

```
RSDS
C:\Users\Kamal\Documents\yasuo\Release\yasuo.pdb
GCTL
```

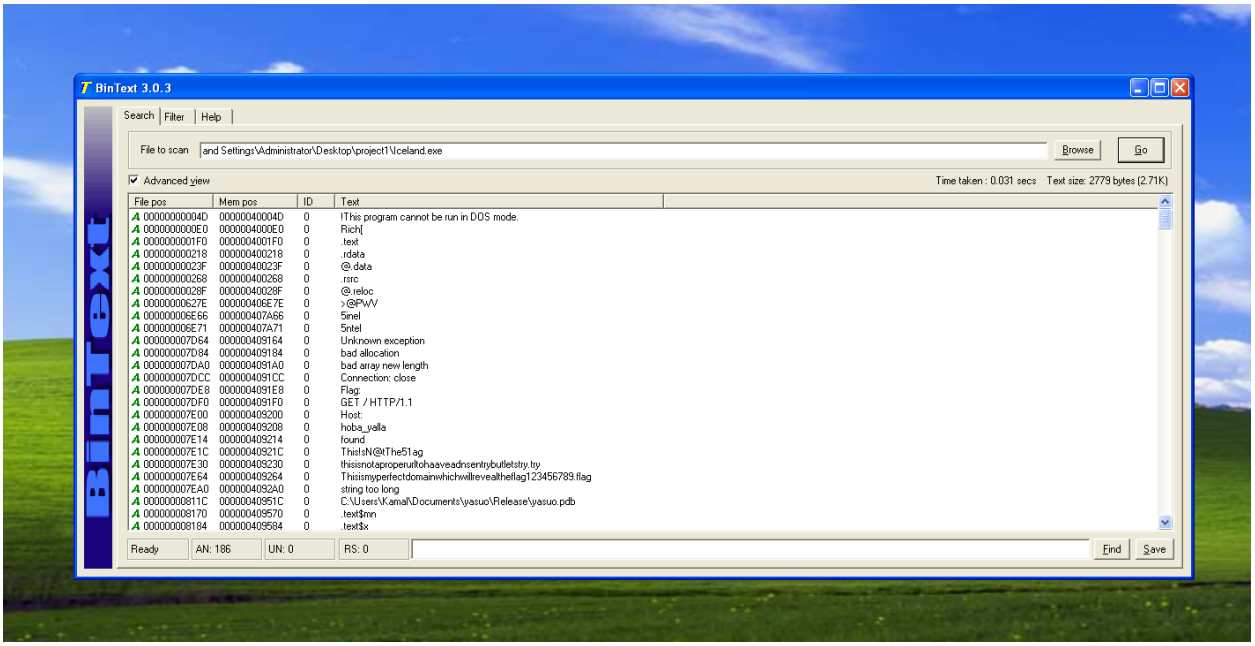
Function References:

- References to functions like **__CxxFrameHandler3**, **__std_terminate, __std_exception_copy**, **__std_exception_destroy**, etc

```
__CxxFrameHandler3
__std_terminate
__std_exception_copy
__std_exception_destroy
_CxxThrowException
```

BinText

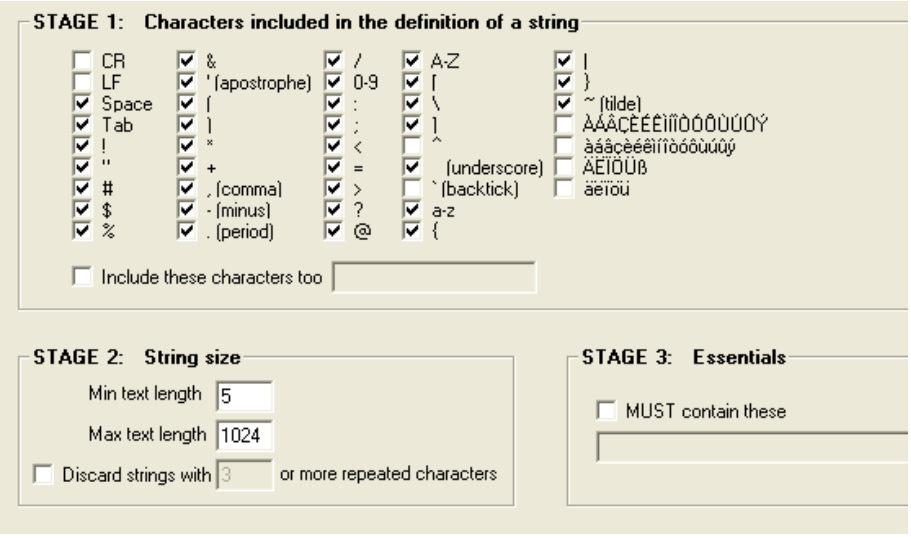
Here Also you can fined all Previous strings in windows :



such as some Strings of Interest and File Paths:

A 000000007C1C	00000040921C	0	This!sN@tThe51ag
A 000000007C30	000000409230	0	thisisnotaproperurltohaaveadnsentrybutletstry.try
A 000000007C64	000000409264	0	Thisismyperfectdomainwhichwillrevealtheflag123456789.flag
A 000000007CA0	0000004092A0	0	string too long
A 000000007F1C	00000040951C	0	C:\Users\Kamal\Documents\yasuo\Release\yasuo.pdb

I can make a filter also :



PEiD:

The PEiD (PE Identifier) analysis for the file "Iceland" using the following information:

File Path: C:\Documents and Settings\Administrator\Desktop\project1\Iceland

Entrypoint Address: 00007179

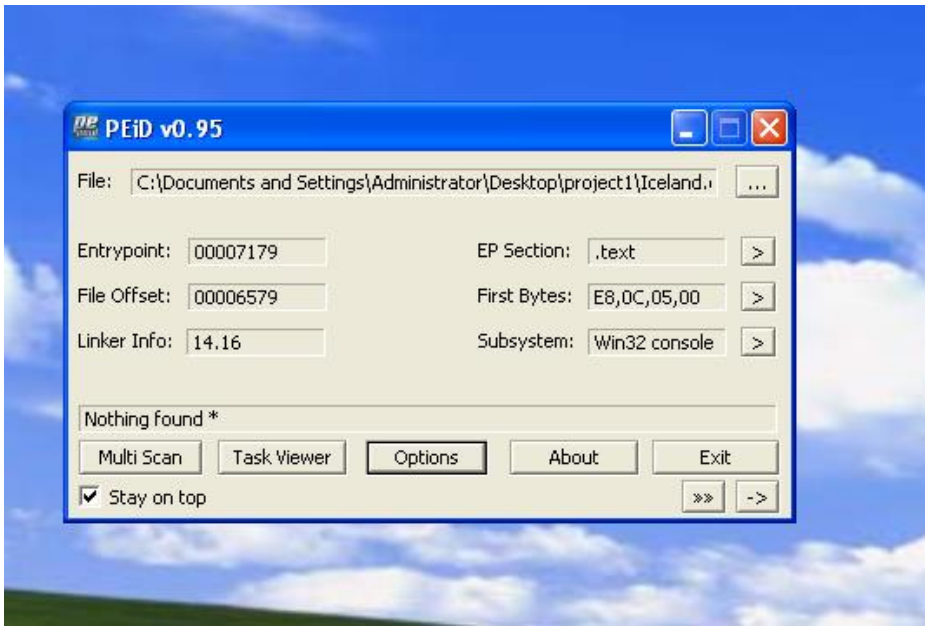
Entrypoint Section: .text

File Offset : 00006579

First Bytes: E8, 0C, 05, 00

Linker Info: 14.16

Subsystem: Win32 console

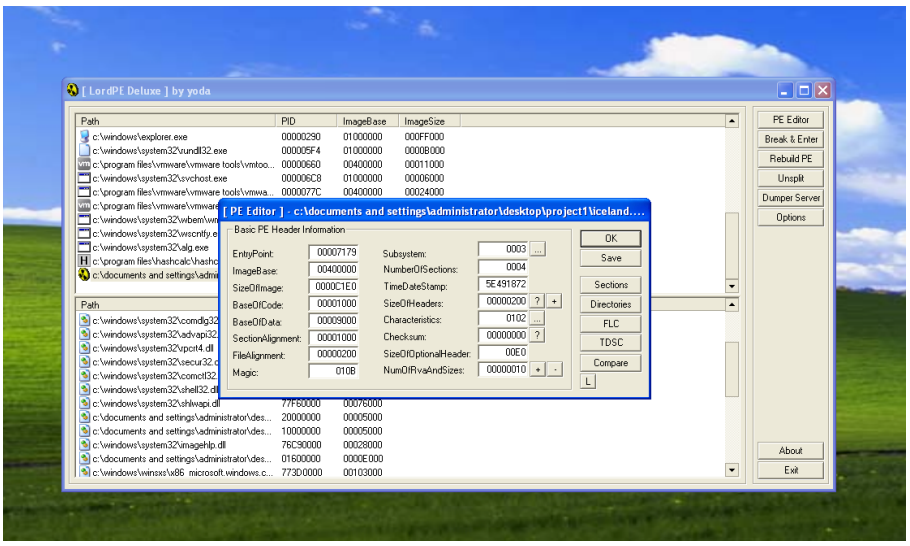


Additionally, the analysis reports **"Nothing found",** suggesting that **PEiD did not identify any specific packer** or compiler signatures in the file.

In summary, the file appears to be a Win32 console executable with an entry point in the "text" section. No specific packer or compiler information was detected by PEiD during the analysis.

LordPE :

here also I checked the PE Editor and I have this information :



EntryPoint Address: 00007179

Subsystem: 0003 (Win32 Console)

Image Base: 00400000

Number of Sections: 0004

Size of Image: 0000C1E0

TimeDateStamp: 5E491872

Base of Code: 00001000

Size of Headers: 0000C1E0

Base of Data: 00009000

Section Alignment: 00001000

Checksum: TDSC

File Alignment: 00000200

Size of Optional Header: 00E0

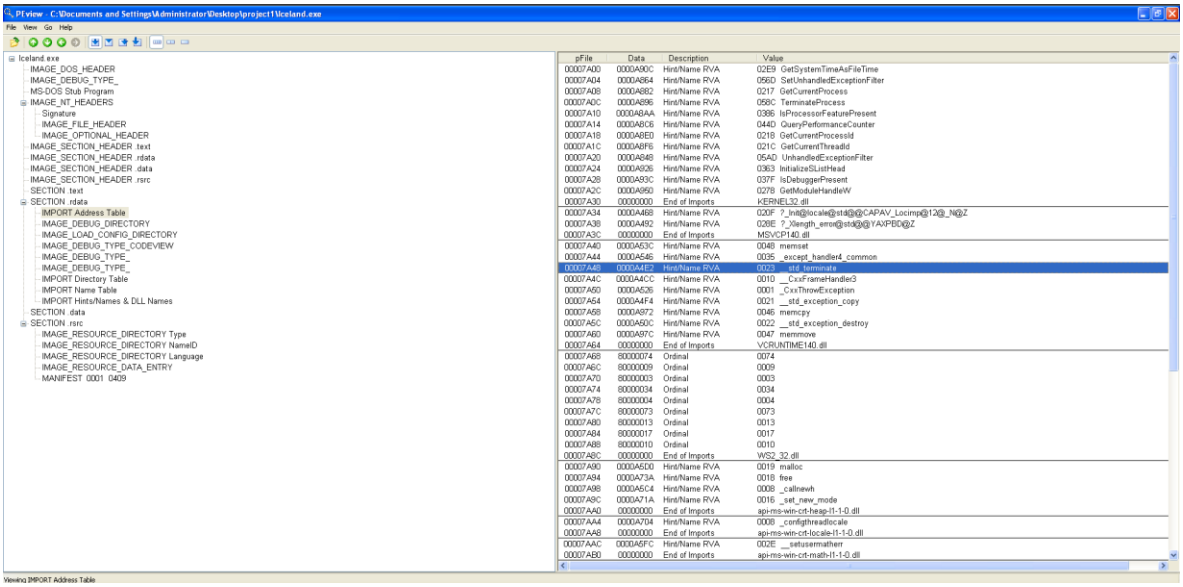
Magic: 0108 (PE32 Executable)

Number of Rva and Sizes: 00000010

The analysis provides essential information about the PE structure, including the entry point, subsystem type (Win32 Console), image base, number of sections, file characteristics, section alignment, and other header details.

PEview :

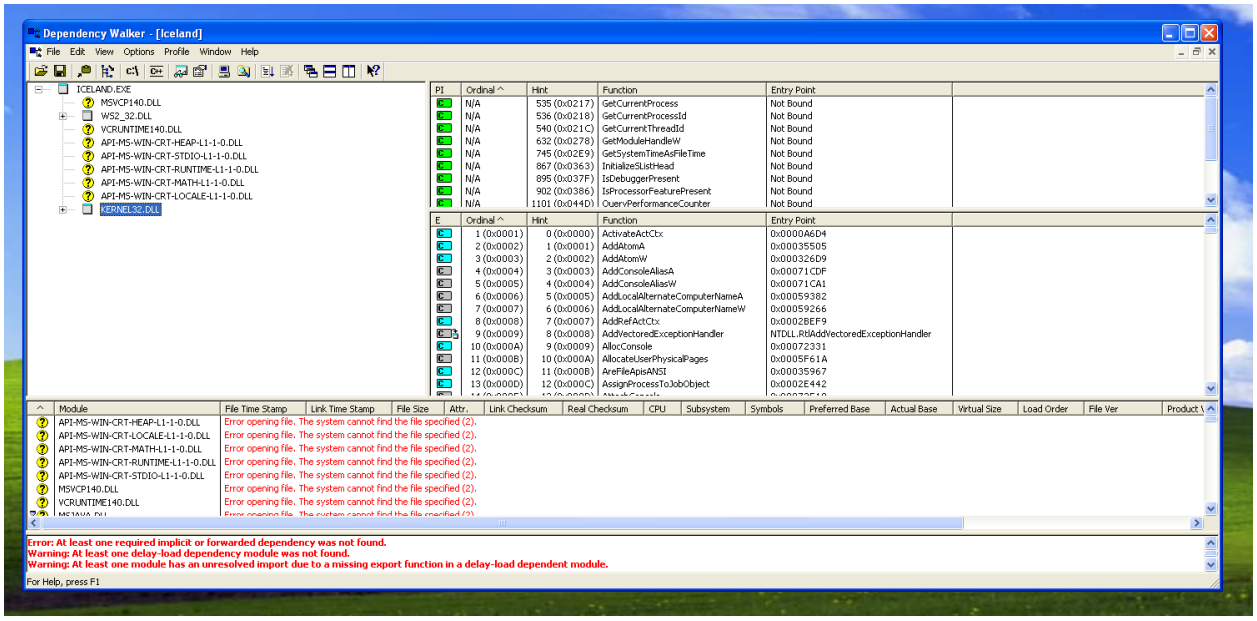
There is a lot import functions ; it’s a .exe file



using a tool like **PEview,** it indicates that the executable relies on various external functions from dynamic-link libraries (DLLs) or other modules to perform specific tasks. Importing functions allow the executable to access functionalities that are not directly present in its code but are provided by external libraries.

Dependency Walker:

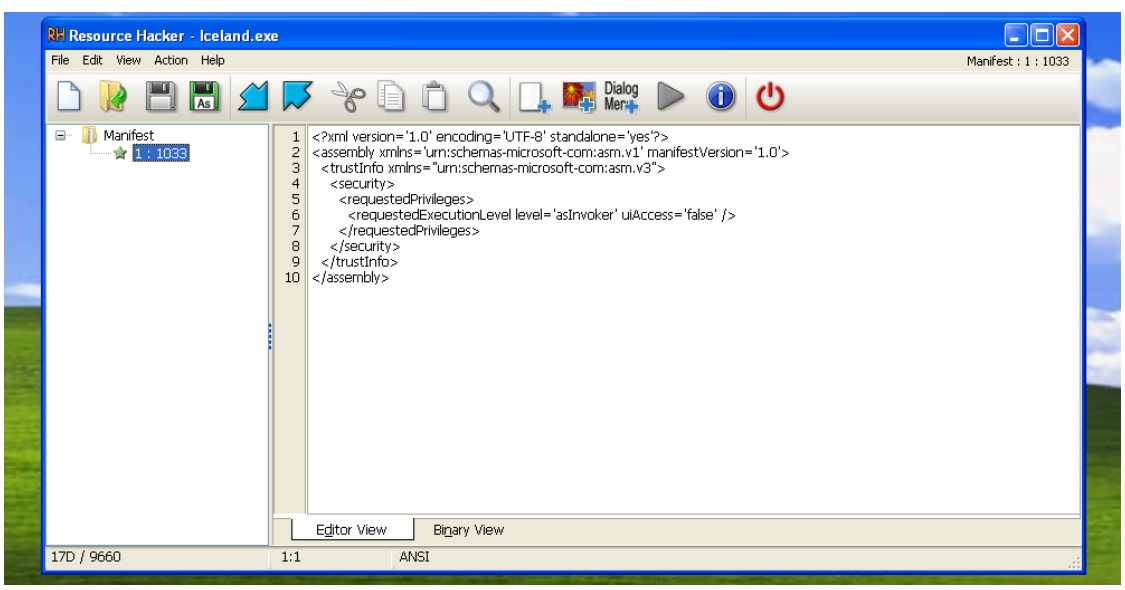
Based on my examination in malware analysis, I anticipate the file to be potentially malicious due to the limited presence of DLL files.



However, it's crucial to conduct further analysis, considering factors such as behavioral patterns, code scrutiny, and the file's origin, to substantiate any suspicions and make a conclusive determination regarding its nature.

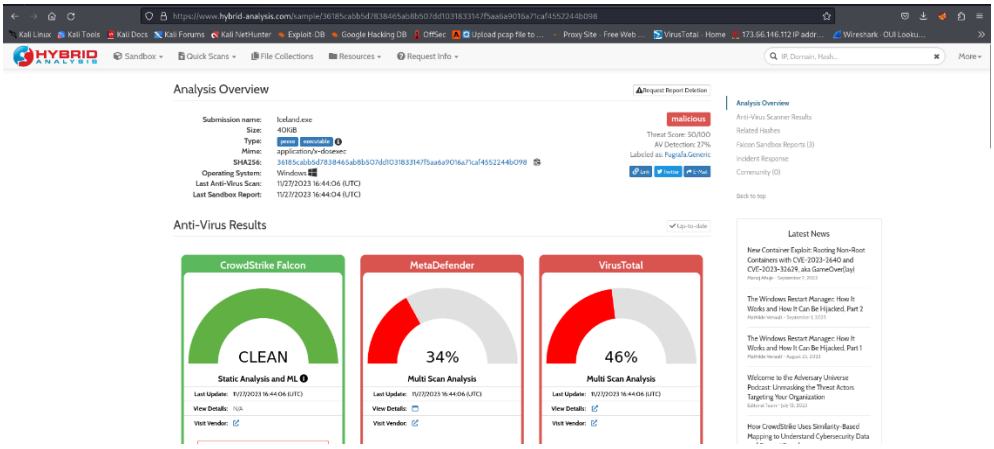
Resource Hacker:

I only found only Manifest



Dynamic analysis

First for Free Sandbox I used hybrid-analysis.com :



The executable file, Iceland.exe (Hash: c997f4dbbd2190dd8ad1713a23867467), has been identified as malicious.

And a related file, Iceland.zip (Hash:34233824813fca9c245f065b47e6952a995ce652c9c02c0c12cc2a4a303cb758), is also confirmed to be malicious. Both files exhibit behavior consistent with harmful activities.

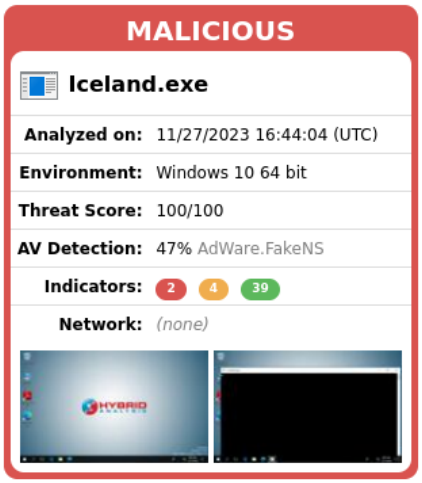
Related Hashes

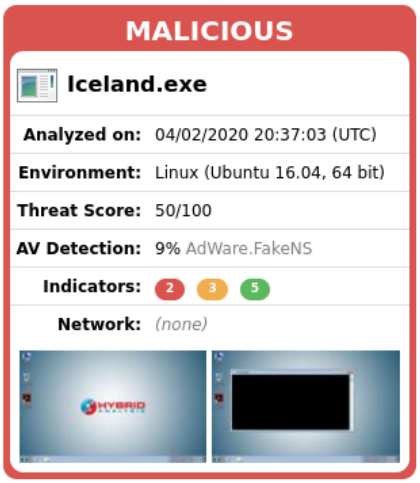
Related files

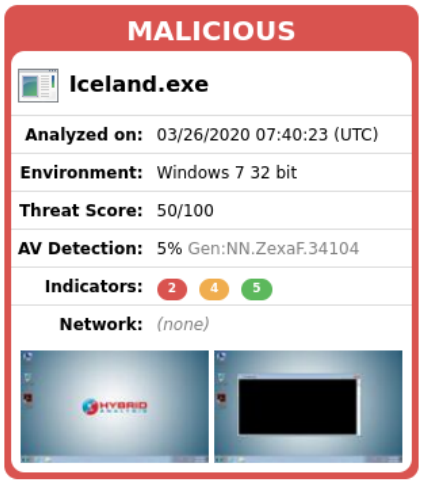
Name	Verdict
Iceland.zip 34233824813fca9c245f065b47e6952a995ce652c9c02c0c12cc2a4a303cb758	malicious

And in this analysis, we explore the threat posed by the executable file *Iceland.exe* across diverse computing environments, including Windows 10, Linux (Ubuntu 16.04), and Windows 7. Examining threat scores, antivirus detections, and indicators provides a comprehensive perspective on the malware's behavior and potential risks .

Falcon Sandbox Reports







Windows 10 (64-bit) Analysis:

The analysis of *Iceland.exe* on Windows 10 (64-bit) conducted on 11/27/2023 revealed an alarming threat score of 100/100, indicating a highly malicious nature. Notably, 47% of antivirus engines flagged the file as "**AdWare.FakeNS**" . While specific indicators were identified, no network activity was reported. This emphasizes the severity of the threat on this platform, warranting immediate attention and response to mitigate potential risks.

Linux (Ubuntu 16.04, 64-bit) Analysis:

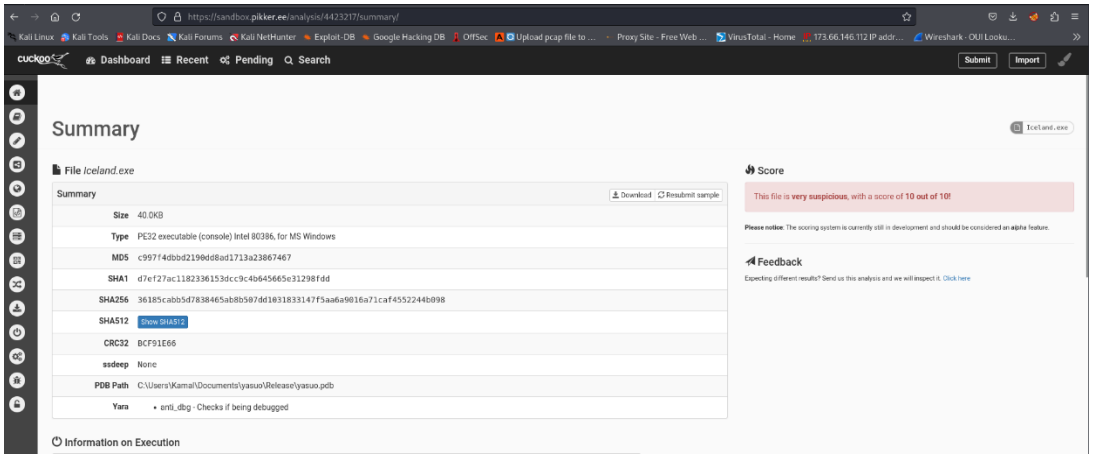
In the Linux environment (Ubuntu 16.04, 64-bit) on 04/02/2020, *Iceland.exe* exhibited a moderate threat level with a score of 50/100. The AV detection rate for "**AdWare.FakeNS"** was 9%, suggesting a potential risk. Similar to the Windows 10 analysis, specific indicators were observed, but no network activity was reported. This underscores the adaptability of the malware across different operating systems and the importance of cross-platform vigilance.

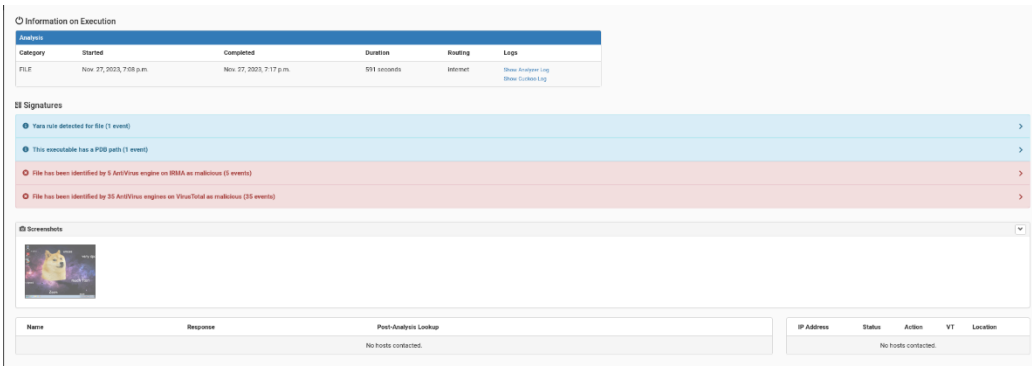
Windows 7 (32-bit) Analysis:

Analyzed on 03/26/2020, the examination of *Iceland.exe* on Windows 7 (32-bit) yielded a threat score of 50/100, signifying a considerable risk. The AV detection rate was 5%, with detection for "**Gen:NN.ZexaF.34104"**. As seen in other analyses, indicators were present without any reported network activity. While the threat level is notable, the lower AV detection rate on this platform emphasizes the dynamic nature of the malware and the necessity for comprehensive security measures across diverse systems.

And when I used sandbox.pikker.ee :

The analysis conducted on sandbox.pikker.ee revealed that **Iceland.exe** has been flagged as "**very suspicious**" with a high score of **10 out of 10.**





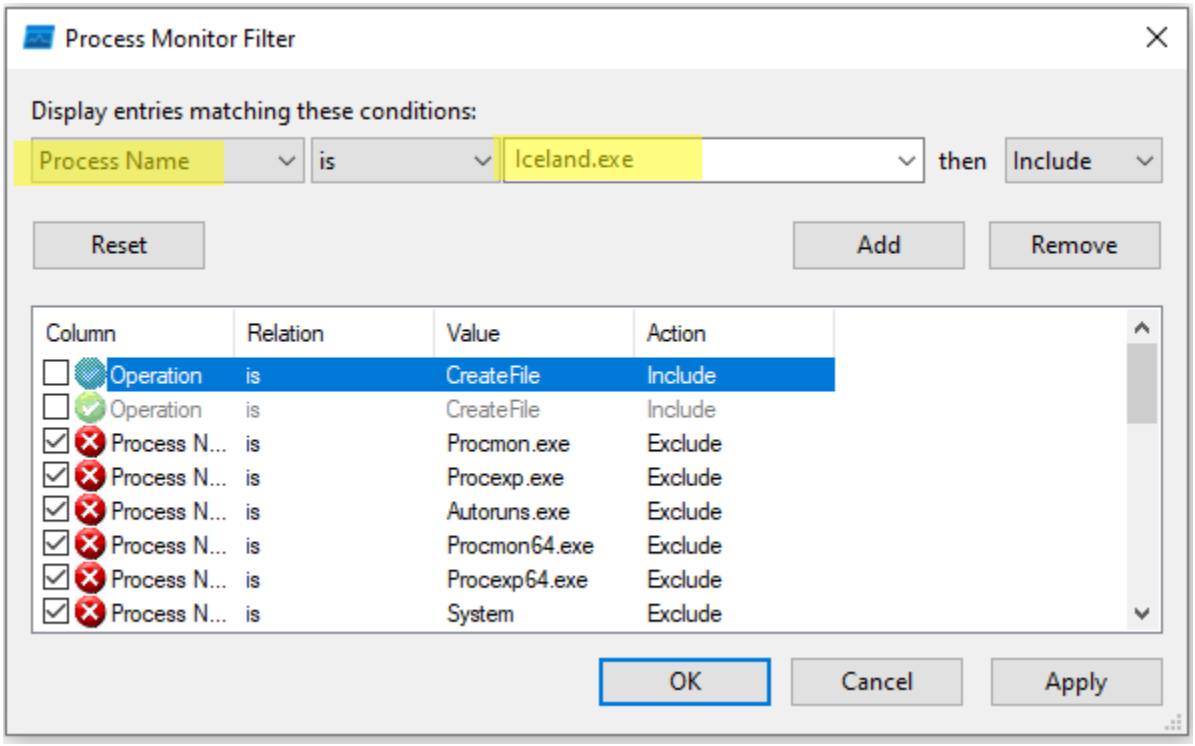
Furthermore, the file has been identified as **malicious** by **five different antivirus engines on IRMA**, with a total of five recorded events. These findings strongly indicate the malicious nature of the executable.

File has been identified by 5 AntiVirus engine on IRMA as malicious (5 events)	
G Data Antivirus (Windows)	Virus: Gen:Variant.Fugrafa.143502 (Engine A)
Avast Core Security (Linux)	FileRepMalware [Adw]
F-Secure Antivirus (Linux)	Adware.ADWARE/Redcap.wkfzg (3, 1, 1) [Aquarius]
eScan Antivirus (Linux)	Gen:Variant.Fugrafa.143502(DB)
Bitdefender Antivirus (Linux)	Gen:Variant.Fugrafa.143502

Additionally, while one screenshot has been obtained during the investigation, its significance in the context of the malware remains uncertain. Further analysis may be required to determine its relevance to the overall threat landscape posed by **Iceland.exe**.

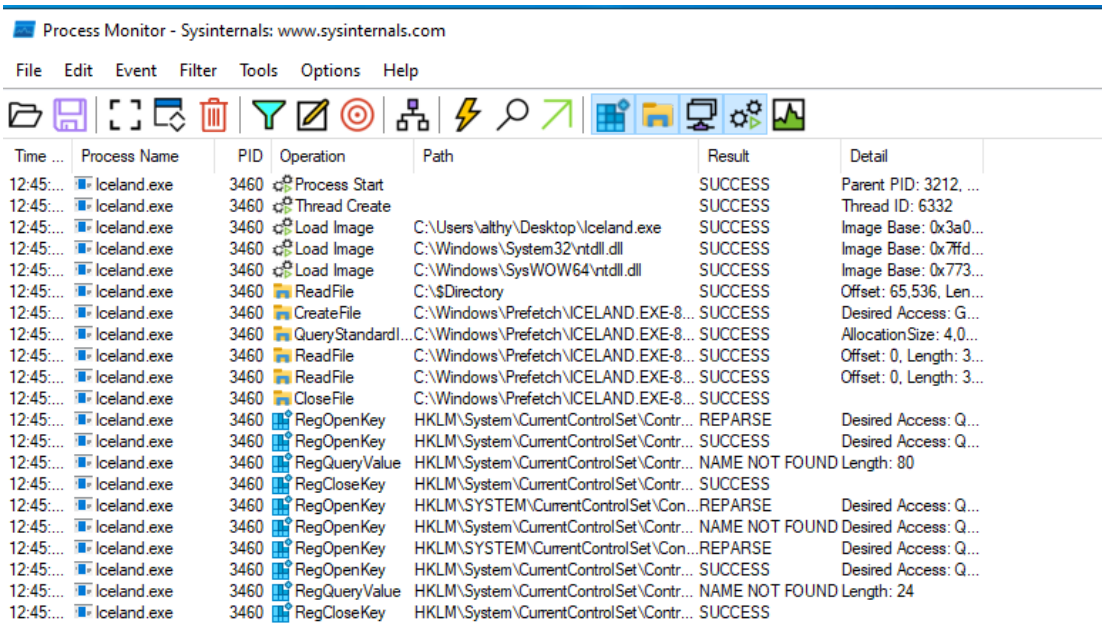
ProcMon tool :

Utilizing **ProcMon**, a tailored filter was implemented to focus on the malware's nomenclature. The malware was then executed to observe and analyze its distinctive activities within the system. This method aims to provide concise insights into the behavioral patterns for an in-depth malware analysis report.



During malware execution, it was determined that the threat utilized two distinct **DLL files**, specifically **`ntdll.dll`**, indicating potential exploitation of low-level system functions.

Noteworthy file creation and reading operations were also observed, highlighting a multifaceted impact on system integrity. These findings contribute to a holistic comprehension of the malware's capabilities and associated risks, forming a foundation for dynamic analysis.



Further exploration revealed that the malware created the threats and processes, followed by exit the thread.

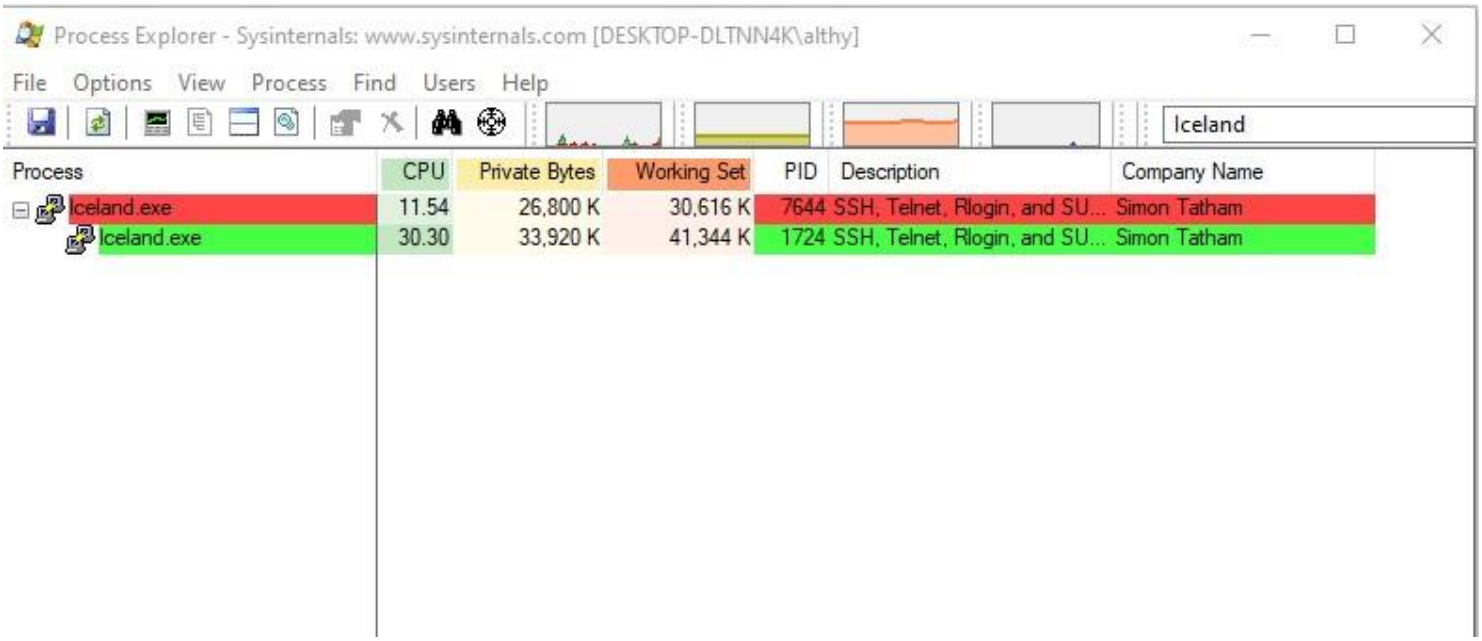
12:45:...	Iceland.exe	3460	Thread Create		SUCCESS	Thread ID: 5516
12:45:...	Iceland.exe	3460	Process Create	C:\Windows\SysWOW64\WerFault.exe	SUCCESS	PID: 7140, Comma...
12:45:...	Iceland.exe	3460	Thread Exit		SUCCESS	Thread ID: 4436, ...
12:45:...	Iceland.exe	3460	Thread Exit		SUCCESS	Thread ID: 5516, ...
12:45:...	Iceland.exe	3460	Thread Exit		SUCCESS	Thread ID: 6332, ...
12:45:...	Iceland.exe	3460	Process Exit		SUCCESS	Exit Status: -10737...
12:45:...	Iceland.exe	3460	RegOpenKey	HKLM\System\CurrentControlSet\Servi...	SUCCESS	Desired Access: All...
12:45:...	Iceland.exe	3460	RegQueryValue	HKLM\System\CurrentControlSet\Servi...	SUCCESS	Type: REG_BINA...
12:45:...	Iceland.exe	3460	RegSetValue	HKLM\System\CurrentControlSet\Servi...	SUCCESS	Type: REG_BINA...
12:45:...	Iceland.exe	3460	RegCloseKey	HKLM\System\CurrentControlSet\Servi...	SUCCESS	

This behavior suggests a deliberate and controlled strategy employed by the malware, likely for evasive measures or to conceal its presence by creating and terminating threats and processes in a sequenced manner. Understanding this pattern is crucial for anticipating the malware's tactics and enhancing countermeasures against its activities.

Process Explorer :

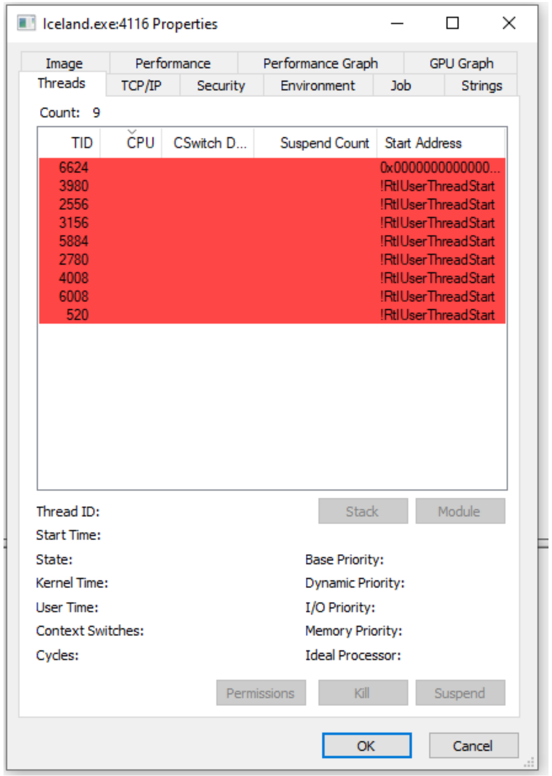
Like the previous program, I created a filter to find the malware and ran the malware to monitor what would happen .

Process Explorer unveiled two processes with PID numbers **7644** and **1724**, denoted in **red** (**Terminated processes**) and **green (New processes)** , displaying CPU usages of **11%** and **30%**, respectively. These processes, Descripe as **SSH, Rlogin, and SU** , exhibited working set sizes of **30,616 K** and **41,344 K**. The **elevated CPU usage** alongside privileged access activities suggests a potential security concern, necessitating further investigation into the nature and legitimacy of these processes.



Examining the malware properties revealed the creation of **9 threats**, as detailed in the accompanying image, suggesting a complex and potentially harmful nature.

Even after a thorough look into the malware, I don't find the strings. This suggests the malware might be using advanced techniques to hide its code and operations, making the analysis more challenging.



Count: 9

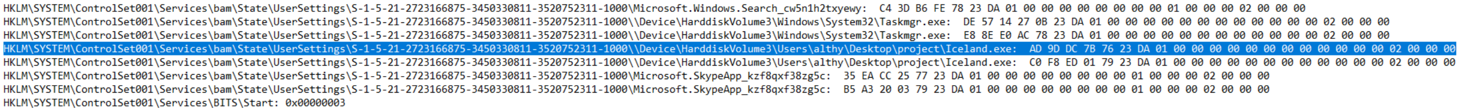
TID	CPU	CSwitch D...	Suspend Count	Start Address
6624				0x0000000000000...
3980				!RtlUserThreadStart
2556				!RtlUserThreadStart
3156				!RtlUserThreadStart
5884				!RtlUserThreadStart
2780				!RtlUserThreadStart
4008				!RtlUserThreadStart
6008				!RtlUserThreadStart
520				!RtlUserThreadStart

Thread ID:
Start Time:
State:
Kernel Time:
User Time:
Context Switches:
Cycles:
Base Priority:
Dynamic Priority:
I/O Priority:
Memory Priority:
Ideal Processor:

RegShot tool :

Upon conducting a comparative analysis using **RegShot** before and after the execution of the malware, notable changes in the Windows Registry were identified.

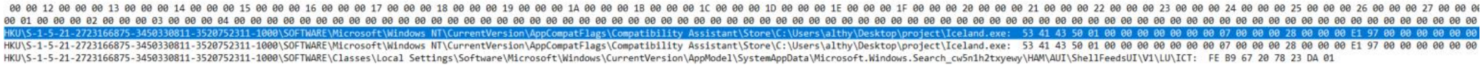
The first detect of malware was in Values modified in this command:



```
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2723166875-3450330811-3520752311-1000\Microsoft.Windows.Search_cw5n1h2txyewy:  C4 3D B6 FE 78 23 DA 01 00 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2723166875-3450330811-3520752311-1000\\Device\HarddiskVolume3\Windows\System32\Taskmgr.exe:  DE 57 14 27 0B 23 DA 01 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2723166875-3450330811-3520752311-1000\\Device\HarddiskVolume3\Windows\System32\Taskmgr.exe:  E8 8E E0 AC 78 23 DA 01 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2723166875-3450330811-3520752311-1000\\Device\HarddiskVolume3\Users\althy\Desktop\project\Iceland.exe:  AD 9D DC 7B 76 23 DA 01 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2723166875-3450330811-3520752311-1000\\Device\HarddiskVolume3\Users\althy\Desktop\project\Iceland.exe:  C0 F8 ED 01 79 23 DA 01 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2723166875-3450330811-3520752311-1000\Microsoft.SkypeApp_kzf8qxf38zg5c:  35 EA CC 25 77 23 DA 01 00 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2723166875-3450330811-3520752311-1000\Microsoft.SkypeApp_kzf8qxf38zg5c:  B5 A3 20 03 79 23 DA 01 00 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00
HKLM\SYSTEM\ControlSet001\Services\BITS\Start: 0x00000003
```

The added hexadecimal values (AD 9D DC 7B 76 23 DA 01 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00) indicate a modification induced by the malware. These changes likely represent alterations to the user settings associated with the **"Iceland.exe"** application for the specified user.

Second detected was in Values modified also in this command:

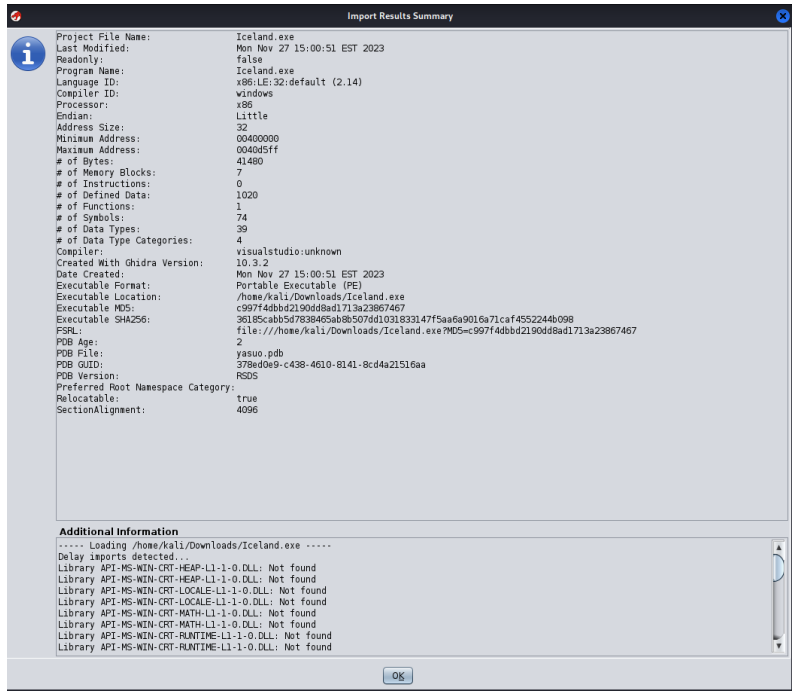


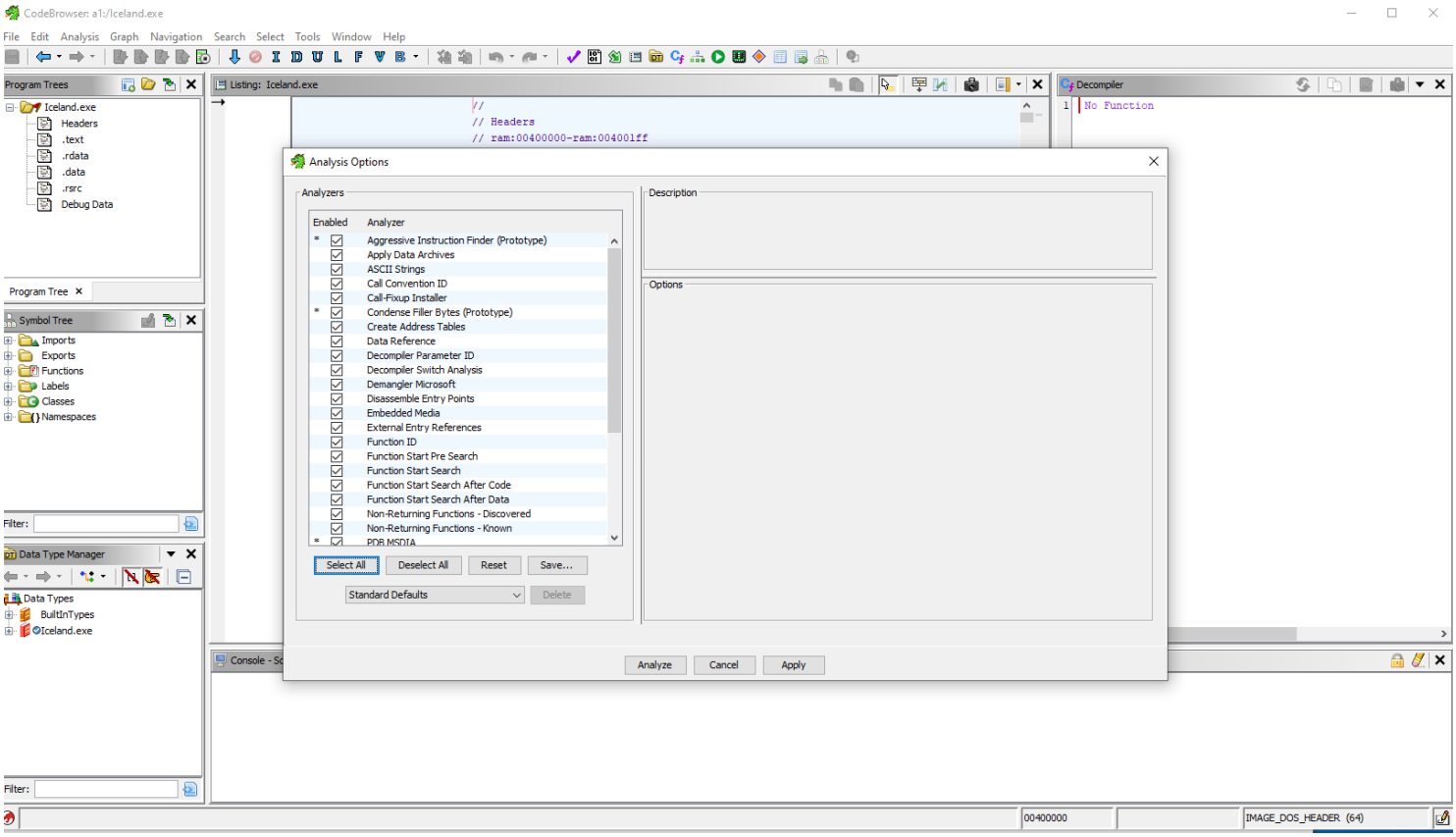
```
 00 00 12 00 00 00 13 00 00 00 14 00 00 00 15 00 00 00 16 00 00 00 17 00 00 00 18 00 00 00 19 00 00 00 1A 00 00 00 1B 00 00 00 1C 00 00 00 1D 00 00 00 1E 00 00 00 1F 00 00 00 20 00 00 00 21 00 00 00 22 00 00 00 23 00 00 00 24 00 00 00 25 00 00 00 26 00 00 00 27 00 00
00 01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-2723166875-3450330811-3520752311-1000\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\C:\Users\althy\Desktop\project\Iceland.exe:  53 41 43 50 01 00 00 00 00 00 00 00 07 00 00 00 28 00 00 00 E1 97 00 00 00 00 00 00
HKU\S-1-5-21-2723166875-3450330811-3520752311-1000\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\C:\Users\althy\Desktop\project\Iceland.exe:  53 41 43 50 01 00 00 00 00 00 00 00 07 00 00 00 28 00 00 00 E1 97 00 00 00 00 00 00
HKU\S-1-5-21-2723166875-3450330811-3520752311-1000\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Search_cw5n1h2txyewy\HAM\AUI\ShellFeedsUI\V1\LU\ICT:  FE B9 67 20 78 23 DA 01
```

The malware, upon analysis, exhibited modifications within the registry key related to compatibility flags for **"Iceland.exe"** .The changes involved additions of hexadecimal values, indicating potential manipulations, while also featuring alterations suggesting data replacement or removal.

Ghidra:

The project file "Iceland.exe" is a 32-bit, little-endian executable created with Visual Studio. It contains 7 memory blocks, 1 function, and 74 symbols. The executable, last modified on Mon Nov 27, 2023, has an MD5 checksum of c997f4dbbd21 and SHA256 of 36185cabb5d7. Debug information includes a PDB file named "yasuo.pdb" with age 2 and GUID 378ed0e9-c438-4610-8141-8cd4a21516aa. The executable is relocatable, has a section alignment of 4096, and was analyzed using Ghidra version 10.3.2.





I've enabled a comprehensive set of analyzers for the project, including Aggressive Instruction Finder, ASCII Strings, Imports, Exports, and more. This thorough selection aims to provide detailed insights into the executable's structure and behavior for effective malware analysis.