Malware Analysis Report

Article · November 2021

1 author:

Anoja Kumudunee
Sri Lanka Institute of Information Technology
4 PUBLICATIONS 1 CITATION
SEE PROFILE

Malware Analysis Report

Analyst:
Name: Somasiri J.P.A.K
Reg No: IT18127492

Submitted to
Sri Lanka Institute of Information Technology

November 2, 2021

DECLERATION

I declare that this is my own work, and this report does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any other university or Institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Registration Number: IT18127492

Name: Somasiri J.P.A.K

ABSTRACT

Cybercrime is becoming more common with each passing day, and criminals are coming up with new ways to destroy their targets through propagating worms and malware. In a fast - changing world technologies and innovations are released on a daily basis; it is possible to attack a system and exploit the system's vulnerabilities. Malware's impact, according to studies, is worsening. Malware is any harmful software that is designed to carry out malicious actions on a computer system. Virus, worms, backdoors, trojans, backdoors and adware are some examples for malwares. There are various kind of malware analysis such as dynamic analysis, static analysis and behavior analysis. There are some drawbacks to static malware analysis. Dynamic malware analysis is the preferred method of malware analysis, and it can be done with a variety of tool and techniques.

Portable Document Format (PDF) files are one of the methods used to distribute malware. Keyloggers are another type of malware that users may encounter.

These malwares get installed in the systems with or without the user concern. They have the ability to steal, damage, corrupt important or the personal data which is owned by the user. Every day, antivirus companies get a thousand pieces of potentially harmful software that might disrupt systems.

Key words: Portable Document Format (PDF), Dynamic malware analysis, malware, cyber crime

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF APPENDICES

LIST OF ABBREVETIONS

Abbreviation	*Description*
PDF	Portable Document Format
PE	Portable Executable
OS	Operating System
HxD	Hex editor

ABOUT COMPANY

Stark Industries can be considered as a well-reputed weapons manufacture in the United State. Stark Industries has received the majority of US military contracts and has also involved in the private military sector. Specifically, with S.H.E.I.L.D., which is a private entity funded by the security council of the world. The entire company is based in Manhattan, New York, and it comprises of the headquarters, manufacturing unit, storage unit, and distribution unit.

As Stark Industries is a world-renowned weapon manufacturer, it rents firearms and imports and exports weaponry for other countries. Stark industries contain a large number of assets such as Experimental Weapons Information System (EWIS), Sales Management System (SMS), Employee Management System (EMS), Workforce Management System (WMS), Importing and Exporting Firearms management System (IEFMS), Document Management System (DMS), Inventory Management System (IMS), Rental Management System (RMS).

APPRAISAL RECEIVERS

Table 1: Appraisal Receivers

Position	Name
Organization Owner	Tony Stark
CEO	Pepper Potts
System Custodian	James Rhodes
Database Administrator	Peter Parker
Security Administrator	Happy Hogan
Network and Computer System Administrator	Nick Fury

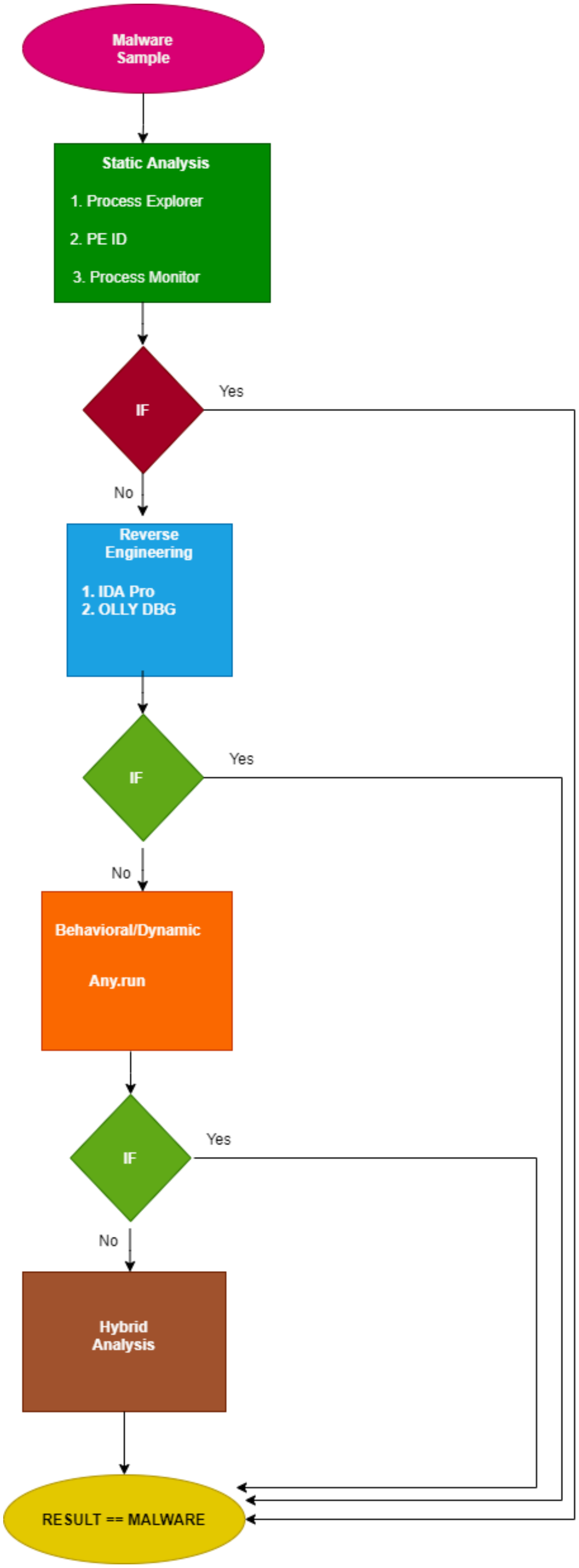
INTRODUCTION

Malware is an abbreviation for malicious software, which is meant to harm a computer without the user's knowledge. There are various kind of malwares such as viruses, trojans, worms, spywares and rootkits. Malware is a key element of several vulnerabilities. Companies struggle to comprehend the malware that they come across. Understanding how to detect malware allows you to take control of the situation. The process of determining the objective and features of a given malware sample, such as a virus, worm, or Trojan horse, is known as malware analysis. The procedure is required in order to build efficient detecting tools for malicious programs. Static analysis tools attempt to analyze a binary without actually running it. After a binary has been executed, live analysis techniques will examine its behavior.

Static analysis refers to the process of evaluating software without running it. There are various kind of static analysis techniques. Additionally, useful information can be retrieved by exploiting the metadata of a specific file format. It includes a number on UNIX, that may indicate the type of the file. A lot of information can be gathered like the compilation time stamp, imports and exports. Mostly malwares are in obfuscated format. It is done by using packers. When the malware is packed it is hard to recover. Major part of static analysis is the disassembly. It is done with tools like IDA Pro, that are able of reversing machine code to assembly language. Because the source code is not executed in static analysis, it is more secure than dynamic analysis.

Dynamic malware analysis is the process of analyzing malware within a controlled environment. It is done in order to analyze the behavior of the malware. This is conducted with the use of a sandbox. And the sandbox is a controlled environment that is used to isolate the process of malware.

The malware analysis report covers the malicious attacks that Stark Industries had to deal with. The figure below illustrates the malware analysis process that was used during the analysis.


Malware Sample
Static Analysis
1. Process Explorer
2. PE ID
3. Process Monitor
IF
Yes
No
Reverse Engineering
1. IDA Pro
2. OLLY DBG
IF
Yes
No
Behavioral/Dynamic
Any.run
IF
Yes
No
Hybrid Analysis
RESULT == MALWARE

BACKGROUND

This malware analysis report was conducted over stark industries, Manhattan, New York City, from October 5th, 2021, to November 5th, 2021. The malware analysis is carried out by identifying significant malwares that have an impact on the company's information assets, as well as potential threats to information security aspects such as the confidentiality, availability and integrity, of the company's entire critical data resources. known malware analysis techniques, tools and technologies. The goal of this malware analysis approach was to identify and assess vulnerabilities and risks associated to Stark Industries' various critical information assets.

In the United States, Stark Industries is a well-known firearm manufacturer. Stark Industries receives the majority of US military contracts, and it has also been involved in private military industries.

Stark Industries own a Documents Management System (DMS) which may keep all the documents. The Documents Management System (DMS) is used to collect, track, monitor, and store all types of documents in order to eliminate paper. Also, this Document Management System (DMS) includes licenses, patents, agreements and also the permits. Every day, the administrators of the Documents Management System received emails, and this malware analysis report is about a Malicious payload PDF file that they received from an unknown sender.

And also, the analysis team could find a keylogger which was installed to track all the passwords, administrator’s internet behaviors, chat messages among the high-level management of the Stark Industries. The keylogger aimed the Experimental Weapons Information System (EWIS) of the company. This EWIS is a $100,000 system that contains all information on weapons in the experimental stage. Designing, developing, modifying, testing, and analyzing are all processes in an experiment.

STARK

FINDINGS 01

025ba9ce4a2118a9ca7b115c8869ff73bc16bad3732ba359cef1e60ad8f961f9

Labels

Phishing

Basic Details

Name: 025ba9ce4a2118a9ca7b115c8869ff73bc16bad3732ba359cef1e60ad8f961f9

File Type: PDF

File Size: 40.96 KB

MD5: 01f03f3cc923583a5157243f2a90879d

SHA-1: 0ccc56a8c890053314ac4d0948a5f1f040624ed5

SHA-256: 025ba9ce4a2118a9ca7b115c8869ff73bc16bad3732ba359cef1e60ad8f961f9

Vhash: 9dcf8653401561d19b368901d71bd53eb

SHA-512:

41698e5ca4579b369372e3e3a7e5e05004e25eb9965e650df30b98ba7ec2182a374c7560c1d5f1e06a9b282aa864153d6c4b1d6ed04300b6a8d359aec4a117df

SSDEEP:

768:6gGzpD9KyYiQy+w13VJsxOG0ZTD+qB5F+x06qH2RnzJttJLf:nGF5PYE+w10rcjF+x060UnttJLf

TrID: Adobe Portable Document Format

Entropy: 7.711

First-Bytes: hex,25 50 44 46 2D 31 2E 34 0A 31 20 30 20 6F 62 6A 0A 3C 3C 0A 2F 54 69 74 6C 65 20 28 FE FF 00 44 00

First-bytes: text, % P D F - 1 . 4 .. 1   0   o b j .. < < .. / T i t l e (.. .. .. D ..

Document creator: LibreOffice

Document producer: LibreOffice

Document title: Death in Tehran Parable

Document subject: Death in tehran parable. From a number of different stories to existentialism/humanism, one story that has always lingered in

Document Pages: 2

Anti-Virus

Antiy-AVL: Trojan/Generic.ASMalwRG.12D

CAT-Quick Heal: PDF.Phishing.39982

DrWeb: PDF.Phisher.197

GData: PDF.Trojan-Stealer.Phishing. E

Ikarus: Trojan.PDF.Phishing

Description

A Spear - phishing Link was discovered in the malicious PDF document. In an attempt to obtain access to the victim's systems, adversaries may send Spear - phishing emails with malicious links. A URL is included in the PDF file. These are the URLs included in the document.

"https://ttraff.me/wix?keyword=death+in+tehran+parable" (Based on: "025ba9ce4a2118a9ca7b115c8869ff73bc16bad3732ba359cef1e60ad8f961f9")

"https://static.usrfiles.com/ugd/5be868_661b97dcf71e4c54800795ecce1d754a.pdf" (Based on: "025ba9ce4a2118a9ca7b115c8869ff73bc16bad3732ba359cef1e60ad8f961f9")

"http://files.all4pawsdogrescue.com.au/uploads/1/3/0/7/130776296/3560341.pdf" (Based on: "025ba9ce4a2118a9ca7b115c8869ff73bc16bad3732ba359cef1e60ad8f961f9")

"http://bujilami.vitalis-foundation.net/uploads/1/3/2/6/132681495/3872217.pdf" (Based on: "025ba9ce4a2118a9ca7b115c8869ff73bc16bad3732ba359cef1e60ad8f961f9")

"https://static.usrfiles.com/ugd/6cf804_8f214cda00aa458092795d69de279b5c.pdf" (Based on: "025ba9ce4a2118a9ca7b115c8869ff73bc16bad3732ba359cef1e60ad8f961f9")

"https://static.usrfiles.com/ugd/e9cba9_d58e05da9d6a4b8699d554058415ce5e.pdf" (Based on: "025ba9ce4a2118a9ca7b115c8869ff73bc16bad3732ba359cef1e60ad8f961f9")

"https://cdn.shopify.com/s/files/1/0428/8148/2919/files/birches_analysis.pdf" (Based on: "025ba9ce4a2118a9ca7b115c8869ff73bc16bad3732ba359cef1e60ad8f961f9")

"https://static.usrfiles.com/ugd/d8966e_d9f7c2b6768e4d719f413432cd8e6e0b.pdf" (Based on: "025ba9ce4a2118a9ca7b115c8869ff73bc16bad3732ba359cef1e60ad8f961f9")

"http://files.midvalleydoulas.net/uploads/1/3/1/4/131406391/lonanis-rulufuwigivur.pdf" (Based on: "025ba9ce4a2118a9ca7b115c8869ff73bc16bad3732ba359cef1e60ad8f961f9")
"https://static.usrfiles.com/ugd/911c12_4e6864392c234d5b99364c831dda6646.pdf" (Based on: "025ba9ce4a2118a9ca7b115c8869ff73bc16bad3732ba359cef1e60ad8f961f9")

Customer Impact

- Change internet explorer settings.

TypeValue: REG_DWORD

Key:

HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\INTERNETEXPLORER\MAIN\FEATURECONTROL\FEATURE_BROWSER_EMULATION

Value: 10001

Name: ACRORD32.EXE

Operation: WRITE

- Start Internet Explorer

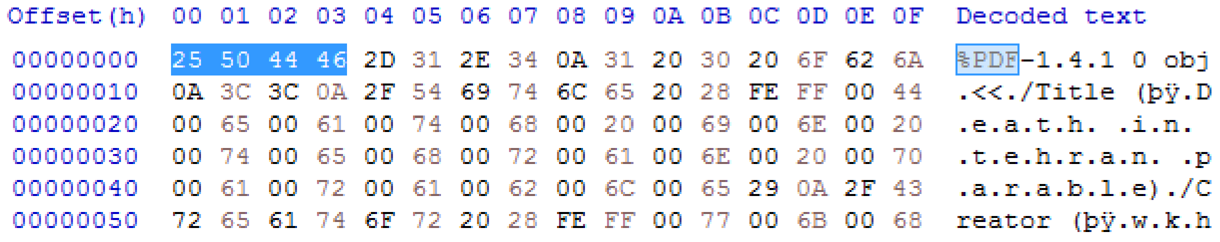
Cmdline:"C:\ProgramFiles\Internet Explorer\iexplore.exe" https://ttraff.me/wix?keyword=death+in+tehran+parable

Analysis Process

A PDF may contain texts, images, and also codes. The flexibility of the PDFs is used by hackers unnecessarily. Hackers may exploit these PDFs. These PDF files may expose important details and also it may open the backdoor for hackers to enter your working environment.

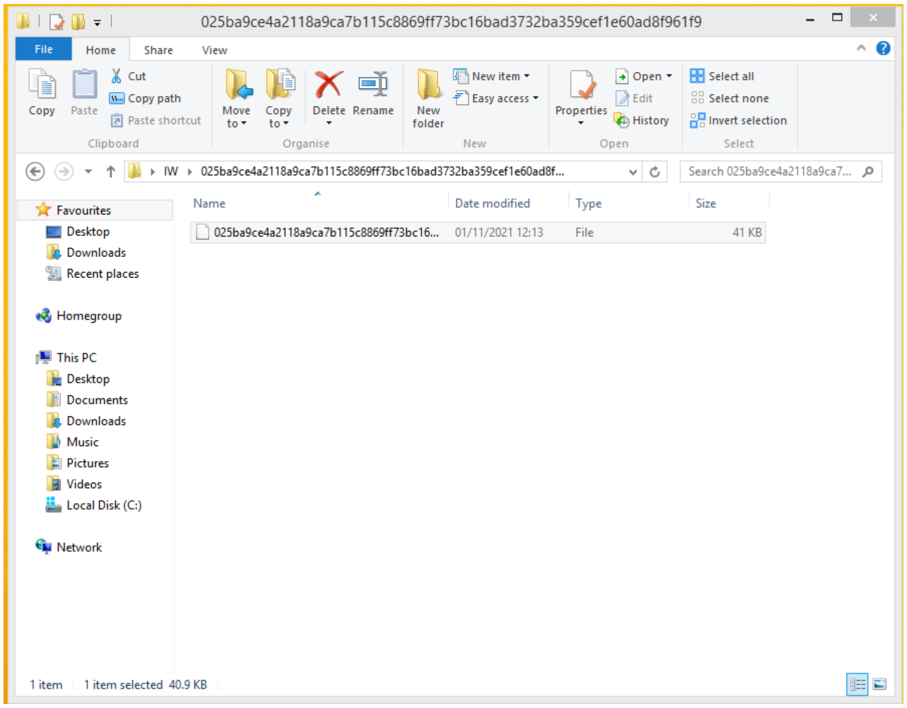
- Hex Editor (HxD)

As shown in the figure 3 first the file type should be identified. File type identification is very useful because if helps to identify the targeted Operating System and the architecture. Here the found malware is in PDF format. If the file type contains %PDF-1.4 or something it gives the file type is PDF and its version is 1.4. Hex editor is used to identify the file type.



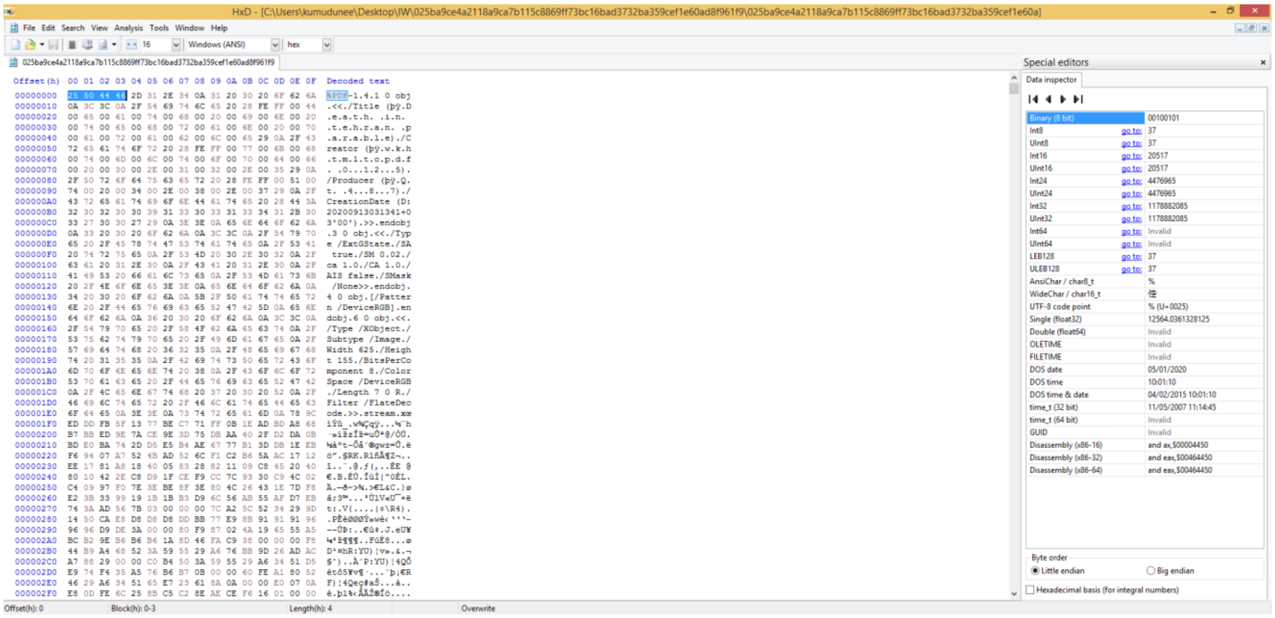
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  25 50 44 46 2D 31 2E 34 0A 31 20 30 20 6F 62 6A  %PDF-1.4.1 0 obj
00000010  0A 3C 3C 0A 2F 54 69 74 6C 65 20 28 FE FF 00 44  .<<./Title (þÿ.D
00000020  00 65 00 61 00 74 00 68 00 20 00 69 00 6E 00 20  .e.a.t.h. .i.n.
00000030  00 74 00 65 00 68 00 72 00 61 00 6E 00 20 00 70  .t.e.h.r.a.n. .p
00000040  00 61 00 72 00 61 00 62 00 6C 00 65 29 0A 2F 43  .a.r.a.b.l.e)./C
00000050  72 65 61 74 6F 72 20 28 FE FF 00 77 00 6B 00 68  reator (þÿ.w.k.h
```

Figure 1: File Type



Name	Date modified	Type	Size
025ba9ce4a2118a9ca7b115c8869ff73bc16...	01/11/2021 12:13	File	41 KB

Figure 2: Malware File


HxD - [C:\Users\kumudunee\Desktop\IW\025ba9ce4a2118a9ca7b115c8869ff73bc16bad3732ba359cef1e60ad8f961f9\025ba9ce4a2118a9ca7b115c8869ff73bc16bad3732ba359cef1e60a]
File
Edit
Search
View
Analysis
Tools
Window
Help
16
Windows (ANSI)
hex
025ba9ce4a2118a9ca7b115c8869ff73bc16bad3732ba359cef1e60ad8f961f9
Special editors
Data inspector
Overwrite

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  25 50 44 46 2D 31 2E 34 0A 31 20 30 20 6F 62 6A  %PDF-1.4.1 0 obj
00000010  0A 3C 3C 0A 2F 54 69 74 6C 65 20 28 FE FF 00 44  .<<./Title (þÿ.D
00000020  00 65 00 61 00 74 00 68 00 20 00 69 00 6E 00 20  .e.a.t.h. .i.n. 
00000030  00 74 00 65 00 68 00 72 00 61 00 6E 00 20 00 70  .t.e.h.r.a.n. .p
00000040  00 61 00 72 00 61 00 62 00 6C 00 65 29 0A 2F 43  .a.r.a.b.l.e)./C
00000050  72 65 61 74 6F 72 20 28 FE FF 00 77 00 6B 00 68  reator (þÿ.w.k.h
00000060  00 74 00 6D 00 6C 00 74 00 6F 00 70 00 64 00 66  .t.m.l.t.o.p.d.f
00000070  00 20 00 30 00 2E 00 31 00 32 00 2E 00 35 29 0A  . .0...1.2...5).
00000080  2F 50 72 6F 64 75 63 65 72 20 28 FE FF 00 51 00  /Producer (þÿ.Q.
00000090  74 00 20 00 34 00 2E 00 38 00 2E 00 37 29 0A 2F  t. .4...8...7)./
000000A0  43 72 65 61 74 69 6F 6E 44 61 74 65 20 28 44 3A  CreationDate (D:
000000B0  32 30 32 30 30 39 31 33 30 33 31 33 34 31 2B 30  20200913031341+0
000000C0  33 27 30 30 27 29 0A 3E 3E 0A 65 6E 64 6F 62 6A  3'00').>>.endobj
000000D0  0A 33 20 30 20 6F 62 6A 0A 3C 3C 0A 2F 54 79 70  .3 0 obj.<<./Typ
000000E0  65 20 2F 45 78 74 47 53 74 61 74 65 0A 2F 53 41  e /ExtGState./SA
000000F0  20 74 72 75 65 0A 2F 53 4D 20 30 2E 30 32 0A 2F   true./SM 0.02./
00000100  63 61 20 31 2E 30 0A 2F 43 41 20 31 2E 30 0A 2F  ca 1.0./CA 1.0./
00000110  41 49 53 20 66 61 6C 73 65 0A 2F 53 4D 61 73 6B  AIS false./SMask
00000120  20 2F 4E 6F 6E 65 3E 3E 0A 65 6E 64 6F 62 6A 0A   /None>>.endobj.
00000130  34 20 30 20 6F 62 6A 0A 5B 2F 50 61 74 74 65 72  4 0 obj.[/Patter
00000140  6E 20 2F 44 65 76 69 63 65 52 47 42 5D 0A 65 6E  n /DeviceRGB].en
00000150  64 6F 62 6A 0A 36 20 30 20 6F 62 6A 0A 3C 3C 0A  dobj.6 0 obj.<<.
00000160  2F 54 79 70 65 20 2F 58 4F 62 6A 65 63 74 0A 2F  /Type /XObject./
00000170  53 75 62 74 79 70 65 20 2F 49 6D 61 67 65 0A 2F  Subtype /Image./
00000180  57 69 64 74 68 20 36 32 35 0A 2F 48 65 69 67 68  Width 625./Heigh
00000190  74 20 31 35 35 0A 2F 42 69 74 73 50 65 72 43 6F  t 155./BitsPerCo
000001A0  6D 70 6F 6E 65 6E 74 20 38 0A 2F 43 6F 6C 6F 72  mponent 8./Color
000001B0  53 70 61 63 65 20 2F 44 65 76 69 63 65 52 47 42  Space /DeviceRGB
000001C0  0A 2F 4C 65 6E 67 74 68 20 37 20 30 20 52 0A 2F  ./Length 7 0 R./
000001D0  46 69 6C 74 65 72 20 2F 46 6C 61 74 65 44 65 63  Filter /FlateDec
000001E0  6F 64 65 0A 3E 3E 0A 73 74 72 65 61 6D 0A 78 9C  ode.>>.stream.xœ
000001F0  ED DD FB 5F 13 77 BE C7 71 FF 0B 1E AD BD A8 68  íÝû_.w¾Çqÿ...½¨h
00000200  B7 BB ED 9E 7A CE 9E 3D 75 DB AA 40 2F D2 DA 0B  ·»ížzÎž=uÛª@/ÒÚ.
00000210  BD E0 BA 74 2D D5 E5 B4 AE 67 77 B1 3D DB 1E EB  ½àºt-Õå´®gw±=Û.ë
00000220  F6 94 07 A7 52 4B AD 52 6C F1 C2 B6 5A AC 17 12  ö".§RK.RlñÂ¶Z¬..
00000230  EE 17 81 A8 18 40 05 83 28 82 11 09 C8 45 20 40  î..¨.@.ƒ(‚..ÈE @
00000240  80 10 42 2E C8 D9 1F CE F9 CC 7C 93 30 C9 4C 02  €.B.ÈÙ.ÎùÌ|"0ÉL.
00000250  C4 09 97 F0 7E 3E BE 8F 3E 80 4C 26 43 1E 7D F8  Ä.—ð~>¾.>€L&C.}ø
00000260  E2 3B 33 99 19 1B 1B B3 D9 6C 56 AB 55 AF D7 EB  â;3™...³ÙlV«U¯×ë
00000270  74 3A AD 56 7B 03 00 00 00 7C A2 5C 52 34 29 9D  t:.V{....|¢\R4).
00000280  14 50 CA E8 D8 D8 D8 DD BB 77 E9 8B 91 91 91 96  .PÊèØØØÝ»wé‹'''–
00000290  96 96 D9 DE 3A 00 00 80 F9 87 02 4A 19 65 55 A5  ––ÙÞ:..€ù‡.J.eU¥
000002A0  BC B2 9E B6 B6 B6 1A 8D 46 FA C9 38 00 00 00 F8  ¼²ž¶¶¶..FúÉ8...ø
000002B0  44 B9 A4 68 52 3A 59 55 29 A6 76 BB 9D 26 AD AC  D¹¤hR:YU)¦v».&.¬
000002C0  A7 88 29 00 00 C0 B4 50 3A 59 55 29 A6 34 51 D5  §ˆ)..À´P:YU)¦4QÕ
000002D0  E9 74 F4 35 A5 76 B6 B7 0B 00 00 60 FE A1 80 52  étô5¥v¶·...`þ¡€R
000002E0  46 29 A6 34 51 65 E7 23 61 8A 0A 00 00 E0 07 0A  F)¦4Qeç#aŠ...à..
000002F0  E8 0D FE 6C 25 8B C5 C2 8E AE CE F6 16 01 00 00  è.þl%‹ÅÂŽ®Îö....
```

Data inspector		
Binary (8 bit)		00100101
Int8	go to:	37
UInt8	go to:	37
Int16	go to:	20517
UInt16	go to:	20517
Int24	go to:	4476965
UInt24	go to:	4476965
Int32	go to:	1178882085
UInt32	go to:	1178882085
Int64	go to:	Invalid
UInt64	go to:	Invalid
LEB128	go to:	37
ULEB128	go to:	37
AnsiChar / char8_t		%
WideChar / char16_t		偅
UTF-8 code point		% (U+0025)
Single (float32)		12564.0361328125
Double (float64)		Invalid
OLETIME		Invalid
FILETIME		Invalid
DOS date		05/01/2020
DOS time		10:01:10
DOS time & date		04/02/2015 10:01:10
time_t (32 bit)		11/05/2007 11:14:45
time_t (64 bit)		Invalid
GUID		Invalid
Disassembly (x86-16)		and ax,$00004450
Disassembly (x86-32)		and eax,$00464450
Disassembly (x86-64)		and eax,$00464450

Byte order
● Little endian ○ Big endian

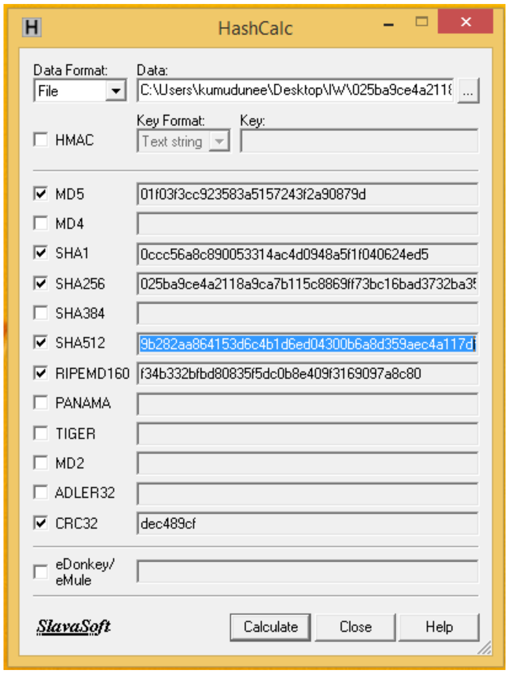
□ Hexadecimal basis (for integral numbers)

Offset(h): 0 Block(h): 0-3 Length(h): 4

Figure 3: File type identification

- HashCalc

Hash calculation is used to generate the cryptographic hashes for the malware file. MD 5, SHA-1, SHA-256, SHA-512 are the hashing algorithms which are using in the malware identification process. This process may give use a unique digest which is called as fingerprint. In order to identify malwares accurately hashes are used, and it make the analysis process easy.



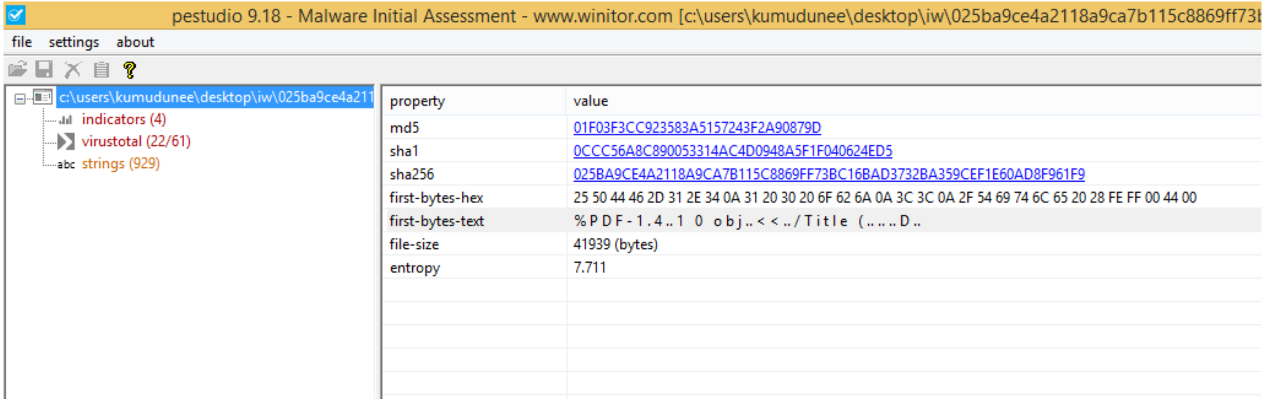
Data Format: File
Data: C:\Users\kumudunee\Desktop\IW\025ba9ce4a211

☐ HMAC Key Format: Text string Key:

☑ MD5	01f03f3cc923583a5157243f2a90879d
☐ MD4	
☑ SHA1	0ccc56a8c890053314ac4d0948a5f1f040624ed5
☑ SHA256	025ba9ce4a2118a9ca7b115c8869ff73bc16bad3732ba3
☐ SHA384	
☑ SHA512	9b282aa864153d6c4b1d6ed04300b6a8d359aec4a117d
☑ RIPEMD160	f34b332bfbd80835f5dc0b8e409f3169097a8c80
☐ PANAMA	
☐ TIGER	
☐ MD2	
☐ ADLER32	
☑ CRC32	dec489cf
☐ eDonkey/ eMule	

Figure 4: Hash Calculation

- PE Studio

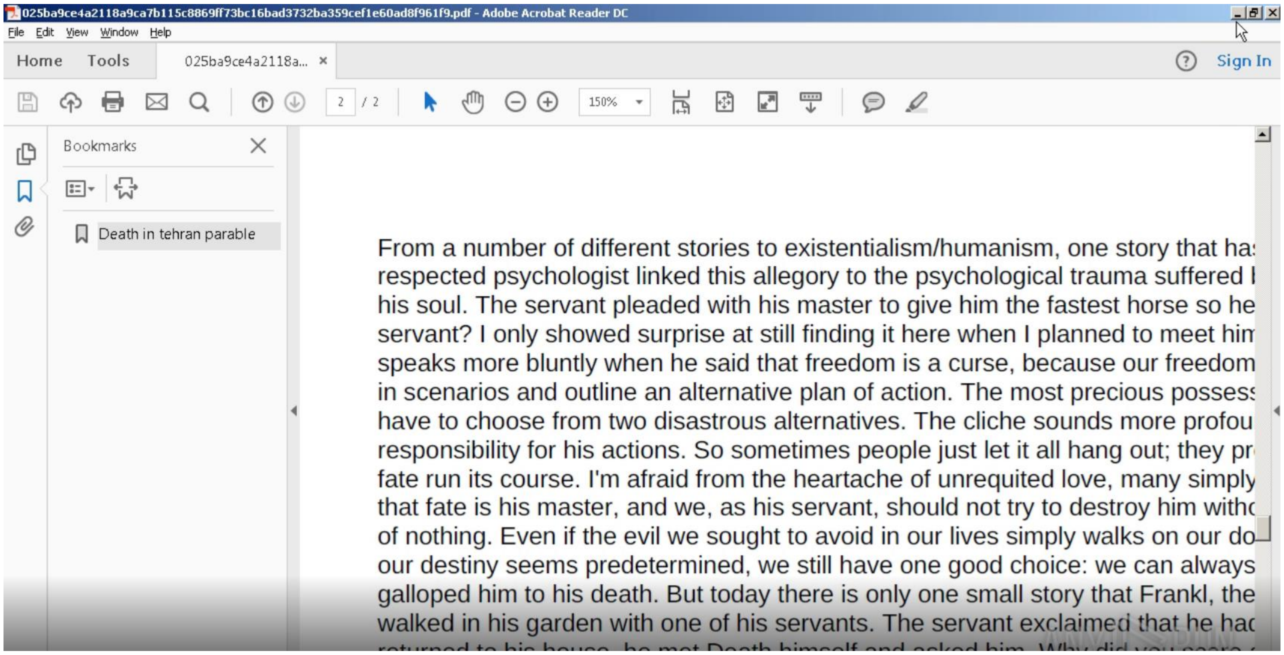


pestudio 9.18 - Malware Initial Assessment - www.winitor.com [c:\users\kumudunee\desktop\iw\025ba9ce4a2118a9ca7b115c8869ff73b

c:\users\kumudunee\desktop\iw\025ba9ce4a211
indicators (4)
virustotal (22/61)
strings (929)

property	value
md5	01F03F3CC923583A5157243F2A90879D
sha1	0CCC56A8C890053314AC4D0948A5F1F040624ED5
sha256	025BA9CE4A2118A9CA7B115C8869FF73BC16BAD3732BA359CEF1E60AD8F961F9
first-bytes-hex	25 50 44 46 2D 31 2E 34 0A 31 20 30 20 6F 62 6A 0A 3C 3C 0A 2F 54 69 74 6C 65 20 28 FE FF 00 44 00
first-bytes-text	% P D F - 1 . 4 .. 1 0 o b j .. < < .. / T i t l e (.. .. .. D ..
file-size	41939 (bytes)
entropy	7.711

Figure 5: PE Studio usage in analysis


025ba9ce4a2118a9ca7b115c8869ff73bc16bad3732ba359cef1e60ad8f961f9.pdf - Adobe Acrobat Reader DC
File Edit View Window Help
Home Tools
025ba9ce4a2118a... ×
Sign In
2 / 2
150%
Bookmarks
Death in tehran parable

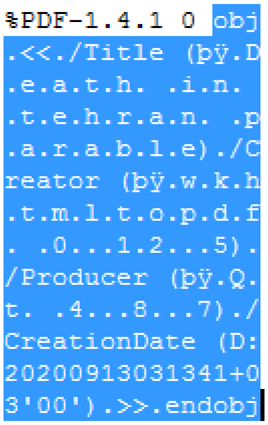
From a number of different stories to existentialism/humanism, one story that ha
respected psychologist linked this allegory to the psychological trauma suffered
his soul. The servant pleaded with his master to give him the fastest horse so he
servant? I only showed surprise at still finding it here when I planned to meet hi
speaks more bluntly when he said that freedom is a curse, because our freedom
in scenarios and outline an alternative plan of action. The most precious posses
have to choose from two disastrous alternatives. The cliche sounds more profou
responsibility for his actions. So sometimes people just let it all hang out; they pr
fate run its course. I'm afraid from the heartache of unrequited love, many simply
that fate is his master, and we, as his servant, should not try to destroy him with
of nothing. Even if the evil we sought to avoid in our lives simply walks on our do
our destiny seems predetermined, we still have one good choice: we can always
galloped him to his death. But today there is only one small story that Frankl, the
walked in his garden with one of his servants. The servant exclaimed that he ha
returned to his house, he met Death himself and asked him, Why did you scare

Figure 6: Executed PDF malware file

- PdfStreamDumper

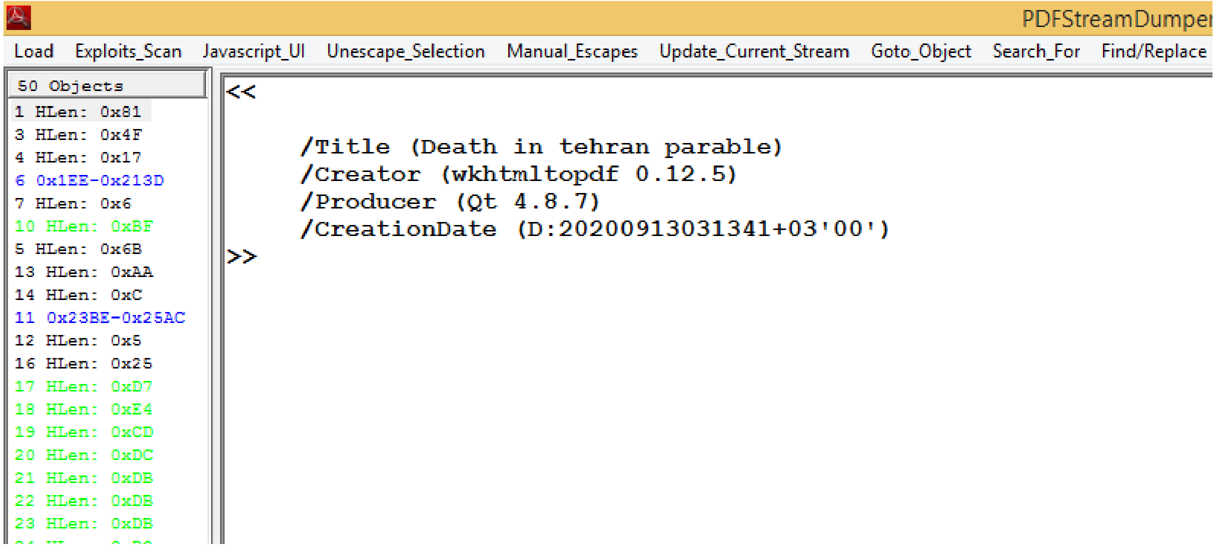
In order to analyze the body of the PDF file PdfStreamDumper is used. A PDF document is a group of objects that each consist of a single self-contained sequence of bytes together with the related structural information. The header includes details about the PDF language's version. A PDF file's header appears at the top of the document. If the file's header is missing, the PDF renderer ignores it.

The body is made up with one or more items. Objects come in a variety of forms, including strings, numbers, dictionaries, bool, and streams. Fonts, pictures, pages, and embedded scripts such as JavaScript and Acrobat forms are all part of an object's information.



```
%PDF-1.4.1 0 obj
.<<./Title (þÿ.D
.e.a.t.h. .i.n.
.t.e.h.r.a.n. .p
.a.r.a.b.l.e)./C
reator (þÿ.w.k.h
.t.m.l.t.o.p.d.f
. .0...1.2...5).
/Producer (þÿ.Q.
t. .4...8...7)./
CreationDate (D:
20200913031341+0
3'00').>>.endobj
```

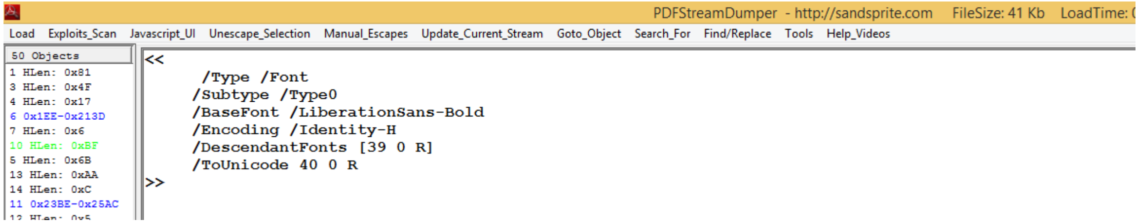
Figure 7: PDF stream object



```
50 Objects
1 HLen: 0x81
3 HLen: 0x4F
4 HLen: 0x17
6 0x1EE-0x213D
7 HLen: 0x6
10 HLen: 0xBF
5 HLen: 0x6B
13 HLen: 0xAA
14 HLen: 0xC
11 0x23BE-0x25AC
12 HLen: 0x5
16 HLen: 0x25
17 HLen: 0xD7
18 HLen: 0xE4
19 HLen: 0xCD
20 HLen: 0xDC
21 HLen: 0xDB
22 HLen: 0xDB
23 HLen: 0xDB
```

```
<<

    /Title (Death in tehran parable)
    /Creator (wkhtmltopdf 0.12.5)
    /Producer (Qt 4.8.7)
    /CreationDate (D:20200913031341+03'00')
>>
```

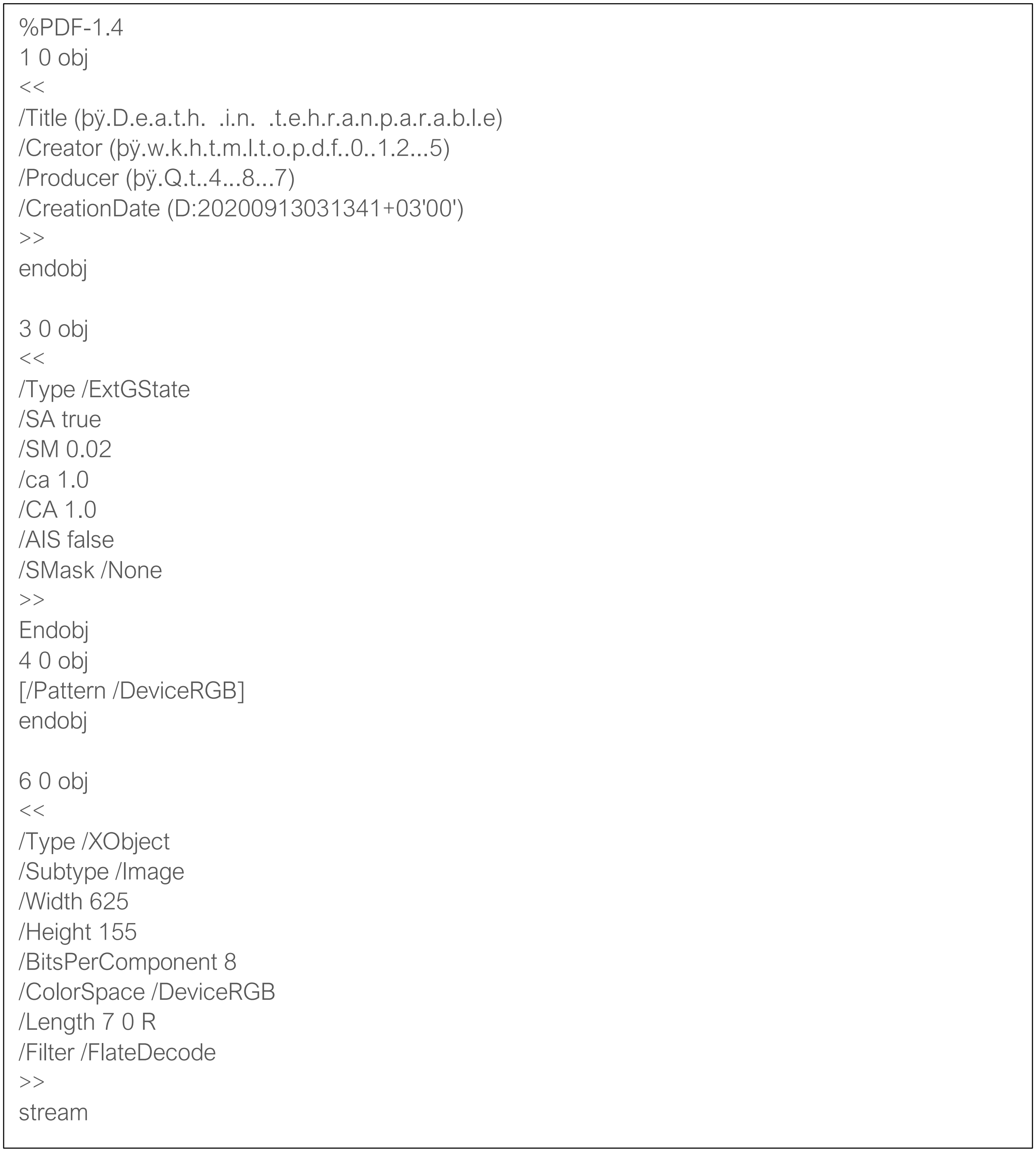
Figure 8: PDF Body



```
50 Objects
1 HLen: 0x81
3 HLen: 0x4F
4 HLen: 0x17
6 0x1EE-0x213D
7 HLen: 0x6
10 HLen: 0xBF
5 HLen: 0x6B
13 HLen: 0xAA
14 HLen: 0xC
11 0x23BE-0x25AC
12 HLen: 0x5
```

```
<<
     /Type /Font
    /Subtype /Type0
    /BaseFont /LiberationSans-Bold
    /Encoding /Identity-H
    /DescendantFonts [39 0 R]
    /ToUnicode 40 0 R
>>
```

Figure 9: PDF Body



```
%PDF-1.4
1 0 obj
<<
/Title (þÿ.D.e.a.t.h.  .i.n.  .t.e.h.r.a.n.p.a.r.a.b.l.e)
/Creator (þÿ.w.k.h.t.m.l.t.o.p.d.f..0..1.2...5)
/Producer (þÿ.Q.t..4...8...7)
/CreationDate (D:20200913031341+03'00')
>>
endobj

3 0 obj
<<
/Type /ExtGState
/SA true
/SM 0.02
/ca 1.0
/CA 1.0
/AIS false
/SMask /None
>>
Endobj
4 0 obj
[/Pattern /DeviceRGB]
endobj

6 0 obj
<<
/Type /XObject
/Subtype /Image
/Width 625
/Height 155
/BitsPerComponent 8
/ColorSpace /DeviceRGB
/Length 7 0 R
/Filter /FlateDecode
>>
stream
```

Here is an example of a PDF document.

Mitigations and Best Practices

- Advanced email security should be implemented.
- JavaScript can be disabled from the PDF reader that you are using
- Don’t permit PDF readers to use external apps to execute non-PDF files.
- Make sure that your PDF readers software and Antivirus software are updated.
- c6f78Should not download or open files which are sent by unknown email senders.
- It is better to educate users
- Keep regular offline backups.

FINDINGS 02

Ardamax Keylogger

Labels

Keylogger

Basic Details

Name: ArdamaxKeylogger

File Type: Win32 EXE

File Size: 783.91 KB

MD5: e33af9e602cbb7ac3634c2608150dd18

SHA-1: 8f6ec9bc137822bc1ddf439c35fedc3b847ce3fe

SHA-256: 8c870eec48bc4ea1aca1f0c63c8a82aaadaf837f197708a7f0321238da8b6b75

SHA-512:

2ae5003e64b525049535ebd5c42a9d1f6d76052cccaa623026758aabe5b1d1b5781ca91c727f3ecb9ac3
0b829b8ce56f11b177f220330c704915b19b37f8f418

Vhash 085046655d151bzf18lz1fz

Authentihash: bd0ef20d5ab6f6ab56355b666d16639d8770b54c003d046799d19491aca168e5

SSDEEP:

12288:0E9uQlDTt8c/wtocu3HhGSrIilDhlPnRq/iI7UOvqF8dtbcZl36VBqWPH:FuqD2cYWzBGZohlE/zUD8/bgl2qW/

TrID: Generic Win/DOS Executable (50%)

TrID: DOS Executable Generic (49.9%)

Entropy: 7.997

Magic: PE32 executable for MS Windows (GUI) Intel 80386 32-bit

PEiD packer: Microsoft Visual C++

Subsystem: GUI

Anti-Virus

Ad-Aware: Dropped: Application.Keylogger. Ardamax.Gen

AhnLab-V3: Trojan/Win32.Ardamax.R1645

Alibaba: TrojanSpy: Win32/Ardamax.582c6805

ALYac: Trojan.Keylogger. ArdamaxKey

Portable Executable Information

Compilation Timestamp: Wed Mar 04 14:29:05 2009

Description

Ardamax Keylogger is a commercialized keylogger that captures every keystroke entered and follows the user's internet behavior. It has the amazing ability to hide itself when functioning. Logs are either emailed to a customizable address or uploaded to a specified FTP server. This should be manually installed.

It has the ability to capture chats. It may allow to record the conversations in google Talk, Skype, yahoo messenger etc. They can stay invisible. It hides from the task manager, start menu and also from the windows start folder. Consumers will be unaware that a key logger is recording every phrase they write in a chat window or password field on their devices. The application records the names and addresses of all websites visited in Internet Explorer, Chrome, Firefox, and Opera, as well as other popular browsers. It will keep tracks of all concealed letters or characters typed passwords and the URLs.

Customer Impact

- Change the system partition.
- Remove data from the device
- For maximum impact, data is encrypted.
- Utilize accessibility features to your advantage
- Lockout the device.
- Carrier billing fraud

Remote service Effects

- Without authorization, track a device remotely.
- Data wiped remotely without any authentication
- Have the ability to obtain cloud backups of the device.

Network Effects

- Swapping sim cards
- Control device communication
- Spy on unencrypted network traffic
- Denial of service or jamming

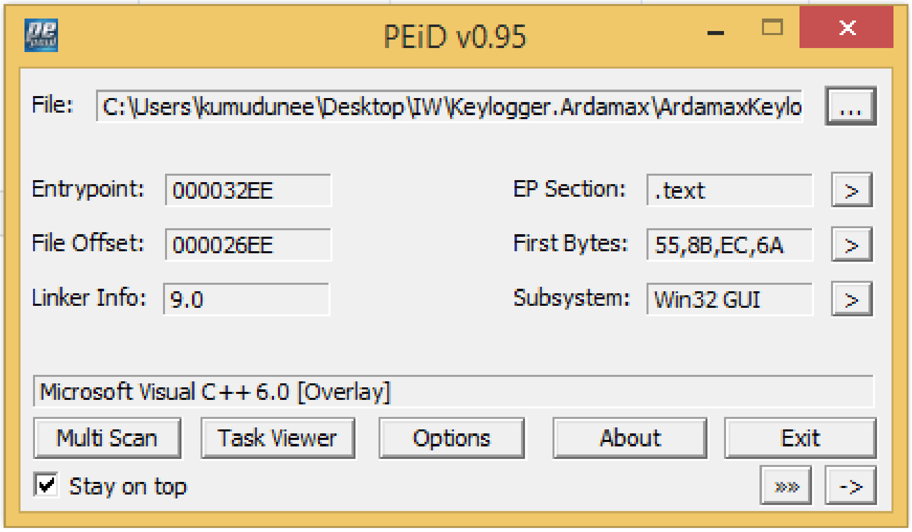
- ➢ Wi-fi access points are rouged.

Mitigating Techniques

- ➢ Train users on possible phishes as well as how to manage them effectively on a regular basis.
- ➢ Keep firmware updates and patches up to date
- ➢ Keep backup data.

Analysis Process

When the malware is uploaded to the virustotal.com platform, we could see the malware has bee identified as a keylogger by so many antivirus programs. So, it is also possible that it's a keylogger (Figure 14). As shown in the Figure 15 file type is identified. Here the file type is MZE. The Exeinfo PE tool is used to check whether the malware is packed or not, as shown in Figure 10.



PEiD v0.95

File: C:\Users\kumudunee\Desktop\IW\Keylogger.Ardamax\ArdamaxKeylo

Entrypoint: 000032EE

EP Section: .text

File Offset: 000026EE

First Bytes: 55,8B,EC,6A

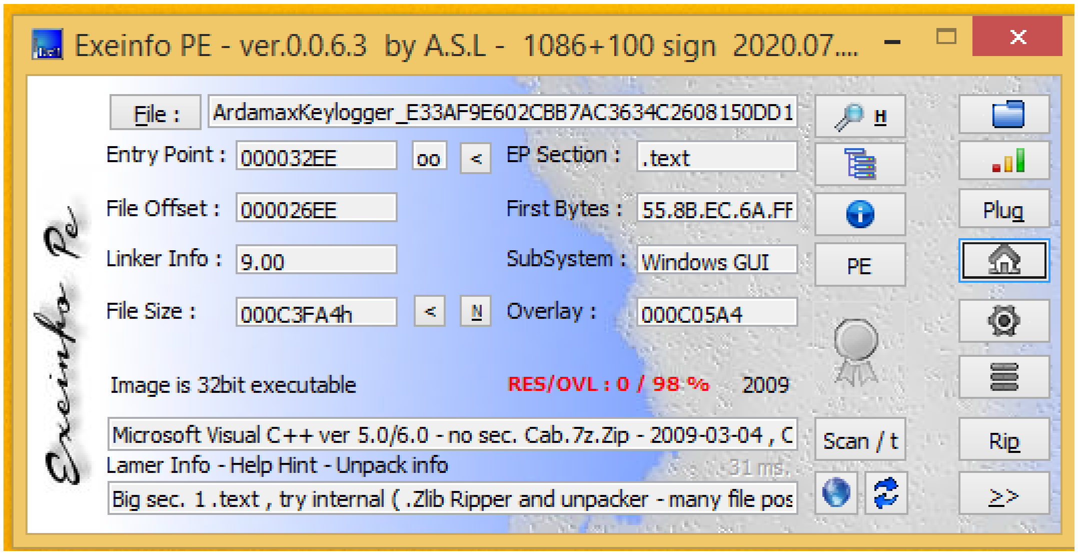
Linker Info: 9.0

Subsystem: Win32 GUI

Microsoft Visual C++ 6.0 [Overlay]

☑ Stay on top

Figure 10: Using PEiD



Exeinfo PE - ver.0.0.6.3 by A.S.L - 1086+100 sign 2020.07....

File : ArdamaxKeylogger_E33AF9E602CBB7AC3634C2608150DD1

Entry Point : 000032EE oo < EP Section : .text

File Offset : 000026EE First Bytes : 55.8B.EC.6A.FF

Linker Info : 9.00 SubSystem : Windows GUI

File Size : 000C3FA4h < N Overlay : 000C05A4

Image is 32bit executable RES/OVL : 0 / 98 % 2009

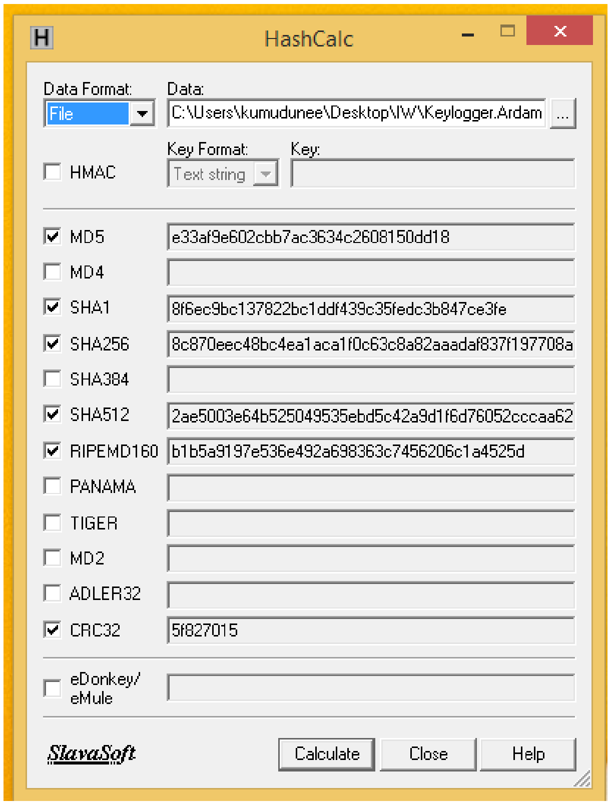
Microsoft Visual C++ ver 5.0/6.0 - no sec. Cab.7z.Zip - 2009-03-04 , C

Lamer Info - Help Hint - Unpack info 31 ms.

Big sec. 1 .text , try internal (.Zlib Ripper and unpacker - many file pos

Figure 11: Using Exeinfo PE

When evaluated with the strings.exe program, there have been no related keylogger functions in this virus. I believe this malware is packaged and so does not display any relevant imports. With the use of ExEinfo PE (Figure 11) and PEiD (Figure 10) tool we could find that the malware contains an overlay. Executing this malware sample has the ability to drop down the directories in C:\%Windir%\System32.



Data Format: File

Data: C:\Users\kumudunee\Desktop\IW\Keylogger.Ardam

□ HMAC

Key Format: Text string

Key:

☑ MD5 e33af9e602cbb7ac3634c2608150dd18

□ MD4

☑ SHA1 8f6ec9bc137822bc1ddf439c35fedc3b847ce3fe

☑ SHA256 8c870eec48bc4ea1aca1f0c63c8a82aaadaf837f197708a

□ SHA384

☑ SHA512 2ae5003e64b525049535ebd5c42a9d1f6d76052cccaa62

☑ RIPEMD160 b1b5a9197e536e492a698363c7456206c1a4525d

□ PANAMA

□ TIGER

□ MD2

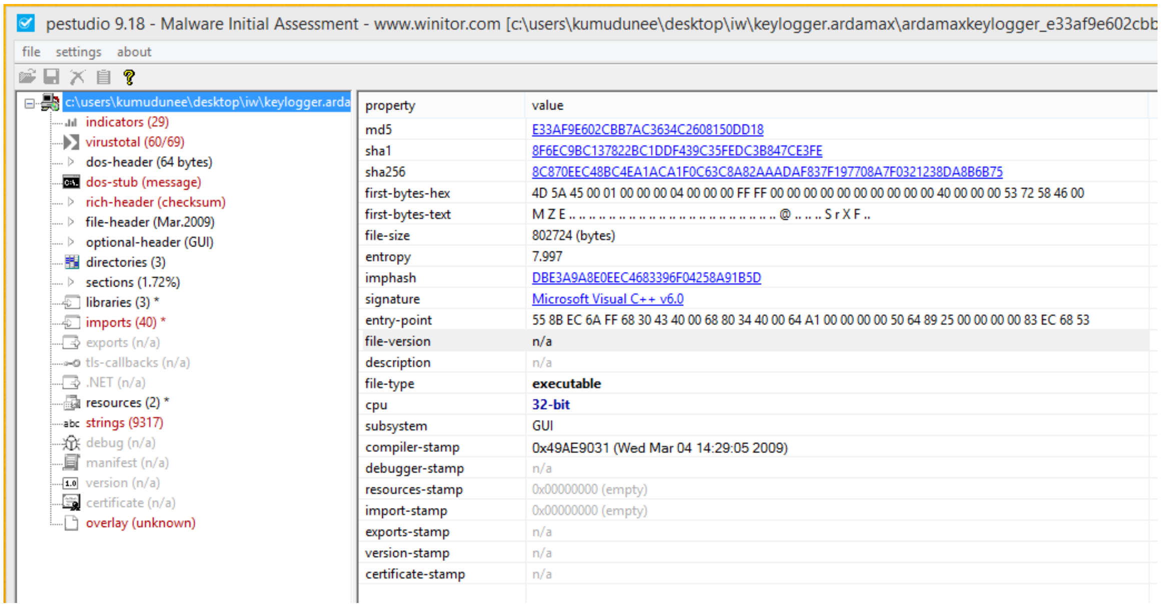
□ ADLER32

☑ CRC32 5f827015

□ eDonkey/ eMule

Figure 12: Using HashCalc

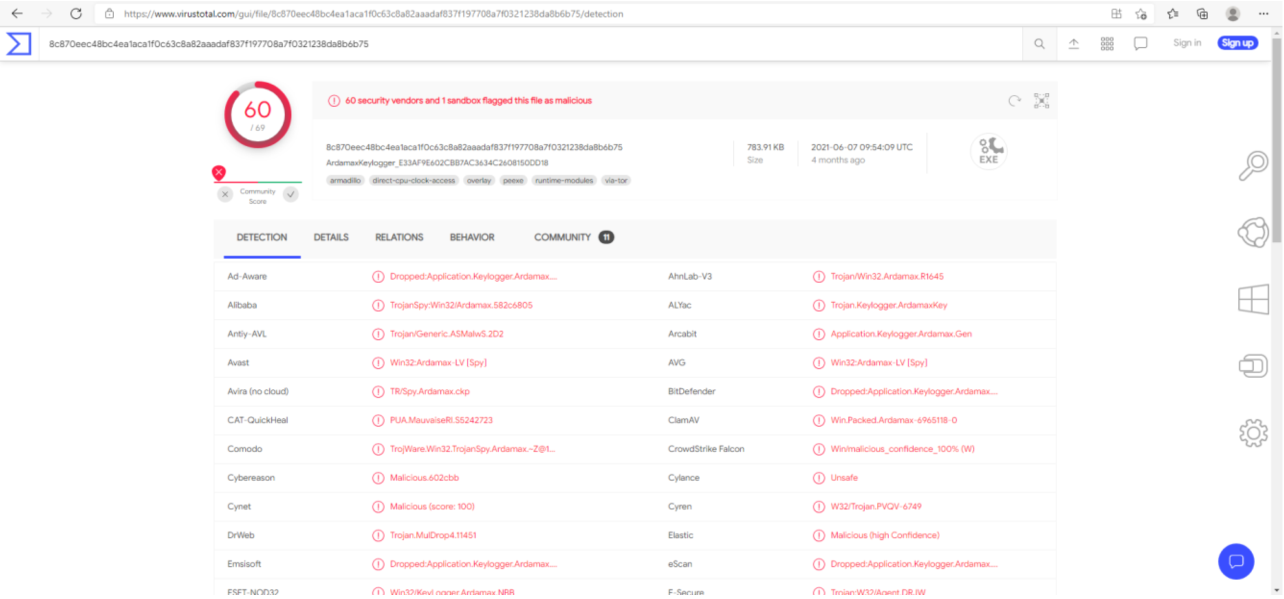
with the use of HashCalc tool hash value is calculated.


pestudio 9.18 - Malware Initial Assessment - www.winitor.com [c:\users\kumudunee\desktop\iw\keylogger.ardamax\ardamaxkeylogger_e33af9e602cbb
file
settings
about

- c:\users\kumudunee\desktop\iw\keylogger.arda
  - indicators (29)
  - virustotal (60/69)
  - dos-header (64 bytes)
  - dos-stub (message)
  - rich-header (checksum)
  - file-header (Mar.2009)
  - optional-header (GUI)
  - directories (3)
  - sections (1.72%)
  - libraries (3) *
  - imports (40) *
  - exports (n/a)
  - tls-callbacks (n/a)
  - .NET (n/a)
  - resources (2) *
  - strings (9317)
  - debug (n/a)
  - manifest (n/a)
  - version (n/a)
  - certificate (n/a)
  - overlay (unknown)

property	value
md5	E33AF9E602CBB7AC3634C2608150DD18
sha1	8F6EC9BC137822BC1DDF439C35FEDC3B847CE3FE
sha256	8C870EEC48BC4EA1ACA1F0C63C8A82AAADAF837F197708A7F0321238DA8B6B75
first-bytes-hex	4D 5A 45 00 01 00 00 00 04 00 00 00 FF FF 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 53 72 58 46 00
first-bytes-text	M Z E .. .. @ .. .. .. S r X F ..
file-size	802724 (bytes)
entropy	7.997
imphash	DBE3A9A8E0EEC4683396F04258A91B5D
signature	Microsoft Visual C++ v6.0
entry-point	55 8B EC 6A FF 68 30 43 40 00 68 80 34 40 00 64 A1 00 00 00 00 50 64 89 25 00 00 00 00 83 EC 68 53
file-version	n/a
description	n/a
file-type	**executable**
cpu	**32-bit**
subsystem	GUI
compiler-stamp	0x49AE9031 (Wed Mar 04 14:29:05 2009)
debugger-stamp	n/a
resources-stamp	0x00000000 (empty)
import-stamp	0x00000000 (empty)
exports-stamp	n/a
version-stamp	n/a
certificate-stamp	n/a

Figure 13: Using pestudio


https://www.virustotal.com/gui/file/8c870eec48bc4ea1aca1f0c63c8a82aaadaf837f197708a7f0321238da8b6b75/detection
8c870eec48bc4ea1aca1f0c63c8a82aaadaf837f197708a7f0321238da8b6b75
Sign in
Sign up
60
/ 69
Community Score
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 11
EXE

60 security vendors and 1 sandbox flagged this file as malicious

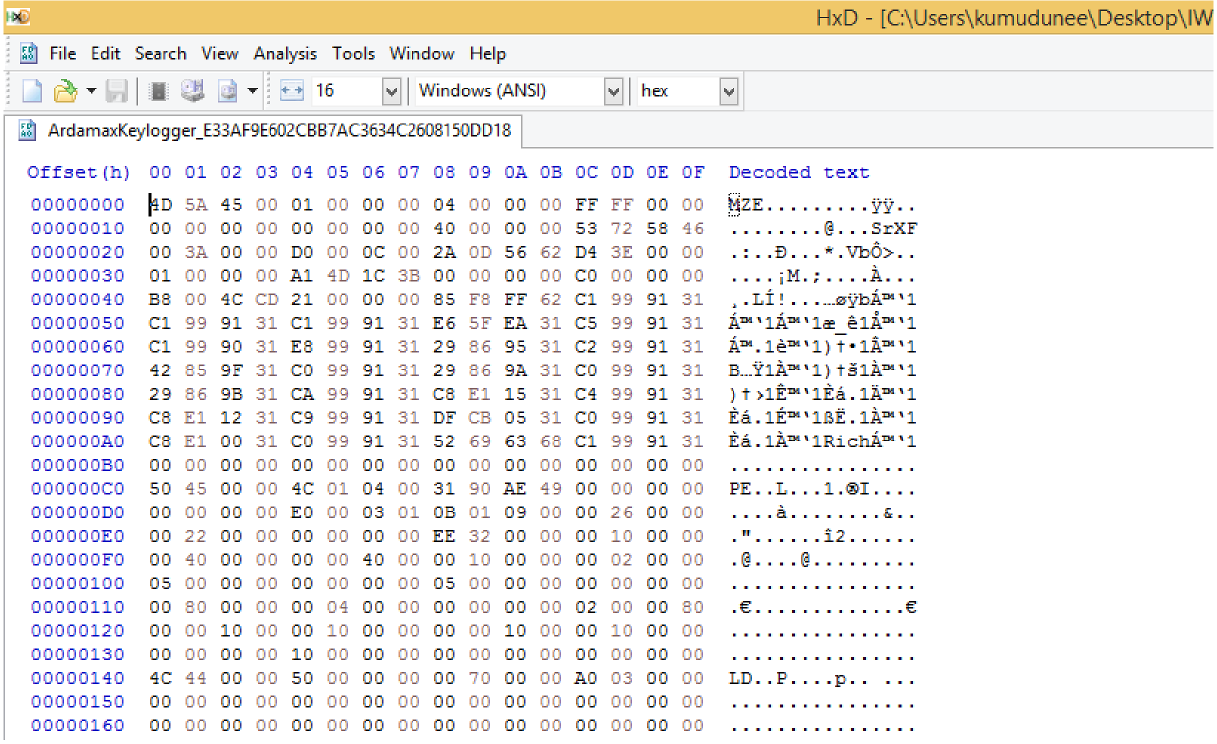
8c870eec48bc4ea1aca1f0c63c8a82aaadaf837f197708a7f0321238da8b6b75
ArdamaxKeylogger_E33AF9E602CBB7AC3634C2608150DD18
armadillo direct-cpu-clock-access overlay peexe runtime-modules via-tor

783.91 KB
Size

2021-06-07 09:54:09 UTC
4 months ago

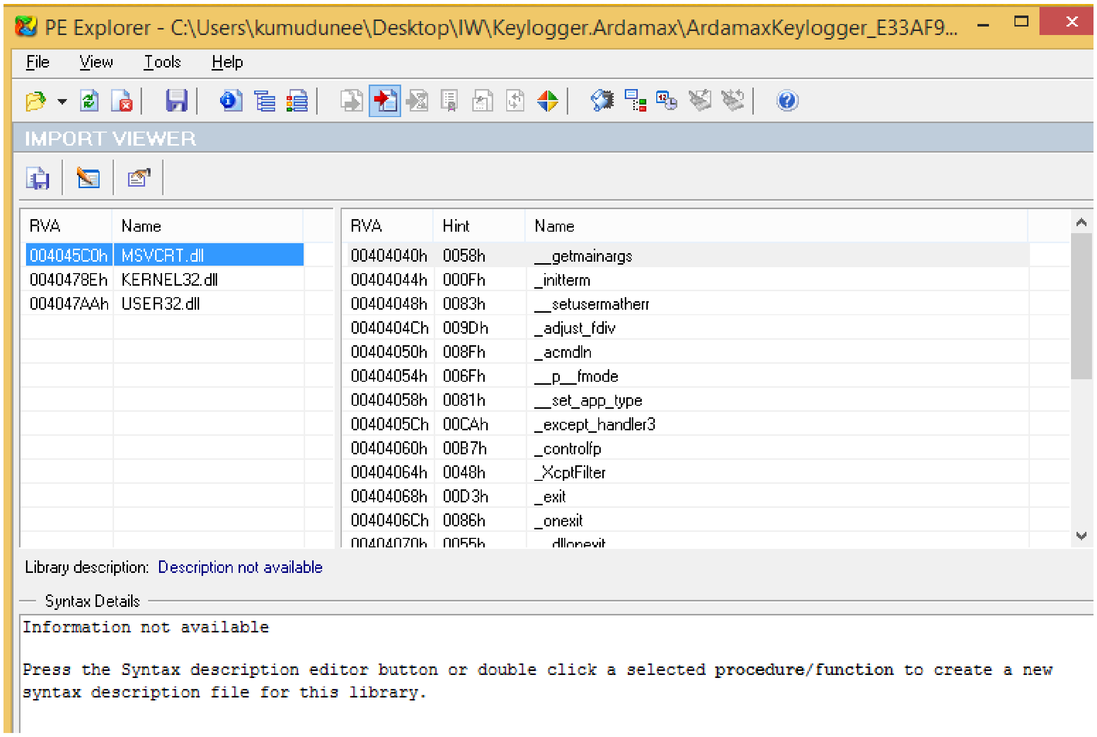
Ad-Aware	Dropped:Application.Keylogger.Ardamax....	AhnLab-V3	Trojan/Win32.Ardamax.R1645
Alibaba	TrojanSpy:Win32/Ardamax.582c6805	ALYac	Trojan.Keylogger.ArdamaxKey
Antiy-AVL	Trojan/Generic.ASMalwS.2D2	Arcabit	Application.Keylogger.Ardamax.Gen
Avast	Win32:Ardamax-LV [Spy]	AVG	Win32:Ardamax-LV [Spy]
Avira (no cloud)	TR/Spy.Ardamax.ckp	BitDefender	Dropped:Application.Keylogger.Ardamax....
CAT-QuickHeal	PUA.MauvaiseRI.S5242723	ClamAV	Win.Packed.Ardamax-6965118-0
Comodo	TrojWare.Win32.TrojanSpy.Ardamax.~Z@1...	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.602cbb	Cylance	Unsafe
Cynet	Malicious (score: 100)	Cyren	W32/Trojan.PVQV-6749
DrWeb	Trojan.MulDrop4.11451	Elastic	Malicious (high Confidence)
Emsisoft	Dropped:Application.Keylogger.Ardamax....	eScan	Dropped:Application.Keylogger.Ardamax....
ESET-NOD32	Win32/KeyLogger.Ardamax.NBB	F-Secure	Trojan:W32/Agent.DRJW

Figure 14: VirusTotal Report


HxD - [C:\Users\kumudunee\Desktop\IW
File
Edit
Search
View
Analysis
Tools
Window
Help
16
Windows (ANSI)
hex
ArdamaxKeylogger_E33AF9E602CBB7AC3634C2608150DD18

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  4D 5A 45 00 01 00 00 00 04 00 00 00 FF FF 00 00  MZE.........ÿÿ..
00000010  00 00 00 00 00 00 00 00 40 00 00 00 53 72 58 46  ........@...SrXF
00000020  00 3A 00 00 D0 00 0C 00 2A 0D 56 62 D4 3E 00 00  .:..Ð...*.VbÔ>..
00000030  01 00 00 00 A1 4D 1C 3B 00 00 00 00 C0 00 00 00  ....¡M.;....À...
00000040  B8 00 4C CD 21 00 00 00 85 F8 FF 62 C1 99 91 31  ¸.LÍ!...…øÿbÁ™‘1
00000050  C1 99 91 31 C1 99 91 31 E6 5F EA 31 C5 99 91 31  Á™‘1Á™‘1æ_ê1Å™‘1
00000060  C1 99 90 31 E8 99 91 31 29 86 95 31 C2 99 91 31  Á™.1è™‘1)†•1Â™‘1
00000070  42 85 9F 31 C0 99 91 31 29 86 9A 31 C0 99 91 31  B…Ÿ1À™‘1)†š1À™‘1
00000080  29 86 9B 31 CA 99 91 31 C8 E1 15 31 C4 99 91 31  )†›1Ê™‘1Èá.1Ä™‘1
00000090  C8 E1 12 31 C9 99 91 31 DF CB 05 31 C0 99 91 31  Èá.1É™‘1ßË.1À™‘1
000000A0  C8 E1 00 31 C0 99 91 31 52 69 63 68 C1 99 91 31  Èá.1À™‘1RichÁ™‘1
000000B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000C0  50 45 00 00 4C 01 04 00 31 90 AE 49 00 00 00 00  PE..L...1.®I....
000000D0  00 00 00 00 E0 00 03 01 0B 01 09 00 00 26 00 00  ....à........&..
000000E0  00 22 00 00 00 00 00 00 EE 32 00 00 00 10 00 00  ."......î2......
000000F0  00 40 00 00 00 00 40 00 00 10 00 00 00 02 00 00  .@....@.........
00000100  05 00 00 00 00 00 00 00 05 00 00 00 00 00 00 00  ................
00000110  00 80 00 00 00 04 00 00 00 00 00 00 02 00 00 80  .€.............€
00000120  00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00  ................
00000130  00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00  ................
00000140  4C 44 00 00 50 00 00 00 00 70 00 00 A0 03 00 00  LD..P....p.. ...
00000150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Figure 15: File type identification



PE Explorer - C:\Users\kumudunee\Desktop\IW\Keylogger.Ardamax\ArdamaxKeylogger_E33AF9...

RVA	Name
004045C0h	MSVCRT.dll
0040478Eh	KERNEL32.dll
004047AAh	USER32.dll

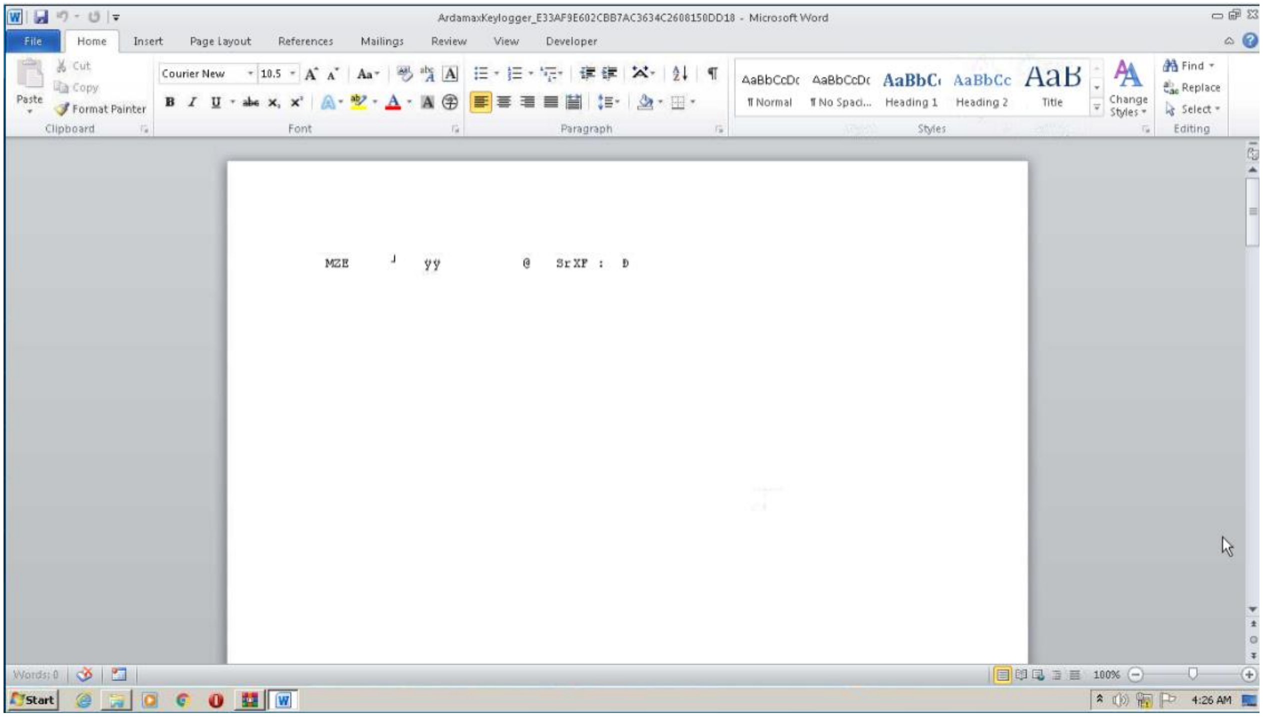
RVA	Hint	Name
00404040h	0058h	__getmainargs
00404044h	000Fh	_initterm
00404048h	0083h	__setusermatherr
0040404Ch	009Dh	_adjust_fdiv
00404050h	008Fh	_acmdln
00404054h	006Fh	__p__fmode
00404058h	0081h	__set_app_type
0040405Ch	00CAh	_except_handler3
00404060h	00B7h	_controlfp
00404064h	0048h	_XcptFilter
00404068h	00D3h	_exit
0040406Ch	0086h	_onexit
00404070h	0055h	__dllonexit

Library description: Description not available

Syntax Details

```
Information not available

Press the Syntax description editor button or double click a selected procedure/function to create a new
syntax description file for this library.
```

Figure 16: Imports



ArdamaxKeylogger_E33AF9E602CBB7AC3634C2608150DD18 - Microsoft Word

```
MZE      ┘  yy         @   SrXF :  Þ
```

Figure 17: Malware File Opened in MS Word

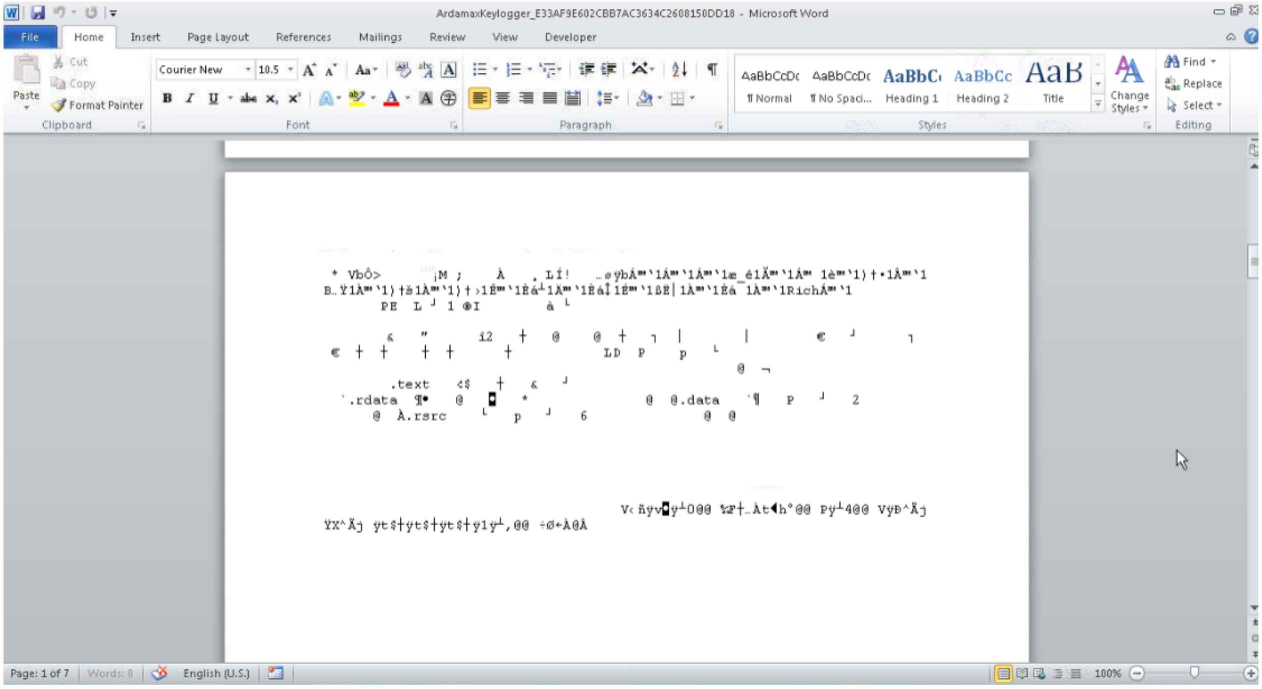
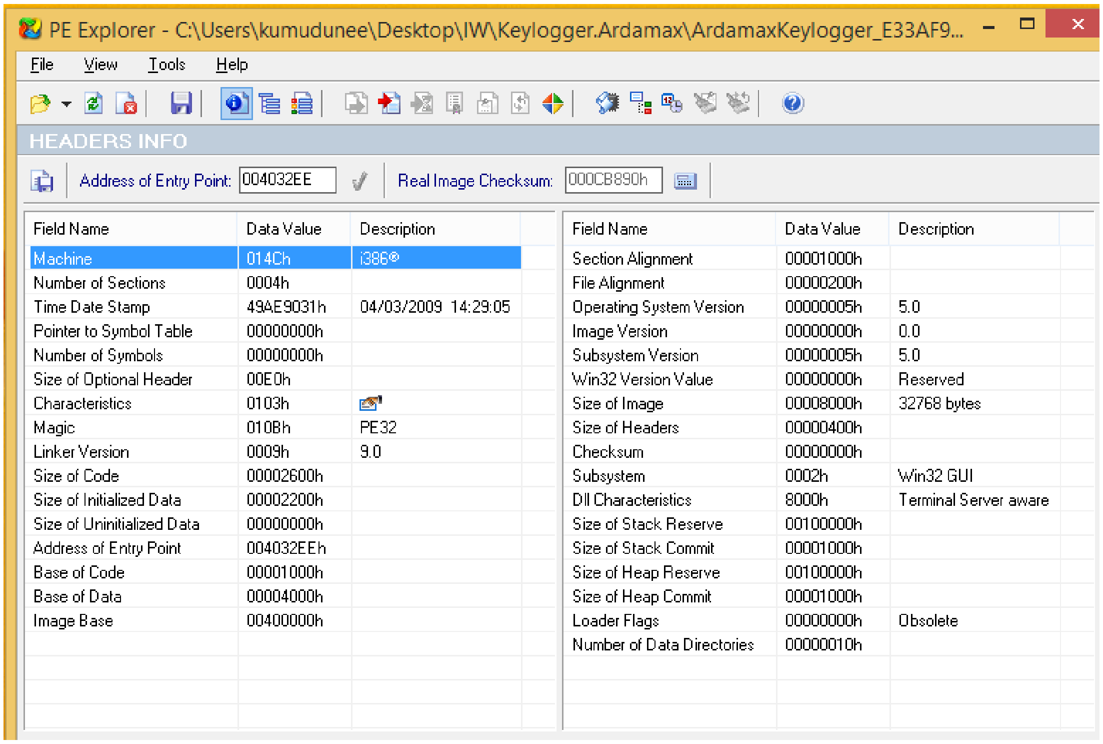


Figure 18: Malware File Opened in MS Word


PE Explorer - C:\Users\kumudunee\Desktop\IW\Keylogger.Ardamax\ArdamaxKeylogger_E33AF9...
File
View
Tools
Help
HEADERS INFO

Address of Entry Point: 004032EE

Real Image Checksum: 000CB890h

Field Name	Data Value	Description
Machine	014Ch	i386®
Number of Sections	0004h	
Time Date Stamp	49AE9031h	04/03/2009 14:29:05
Pointer to Symbol Table	00000000h	
Number of Symbols	00000000h	
Size of Optional Header	00E0h	
Characteristics	0103h	
Magic	010Bh	PE32
Linker Version	0009h	9.0
Size of Code	00002600h	
Size of Initialized Data	00002200h	
Size of Uninitialized Data	00000000h	
Address of Entry Point	004032EEh	
Base of Code	00001000h	
Base of Data	00004000h	
Image Base	00400000h	

Field Name	Data Value	Description
Section Alignment	00001000h	
File Alignment	00000200h	
Operating System Version	00000005h	5.0
Image Version	00000000h	0.0
Subsystem Version	00000005h	5.0
Win32 Version Value	00000000h	Reserved
Size of Image	00008000h	32768 bytes
Size of Headers	00000400h	
Checksum	00000000h	
Subsystem	0002h	Win32 GUI
Dll Characteristics	8000h	Terminal Server aware
Size of Stack Reserve	00100000h	
Size of Stack Commit	00001000h	
Size of Heap Reserve	00100000h	
Size of Heap Commit	00001000h	
Loader Flags	00000000h	Obsolete
Number of Data Directories	00000010h	

Figure 19: Using PE Explorer

The malware's execution cycle has the following steps.

- The keylogger executable file drops a numerous file, including DLL, to the %tmp% folder.
- The harmful method Ardamax.exe executes the dropped DLL, which is used to place the keylogger files in a hidden location in the system folder.
- Lastly, the keylogger DPBJ.exe is run, which logs keystrokes and captured screenshots.

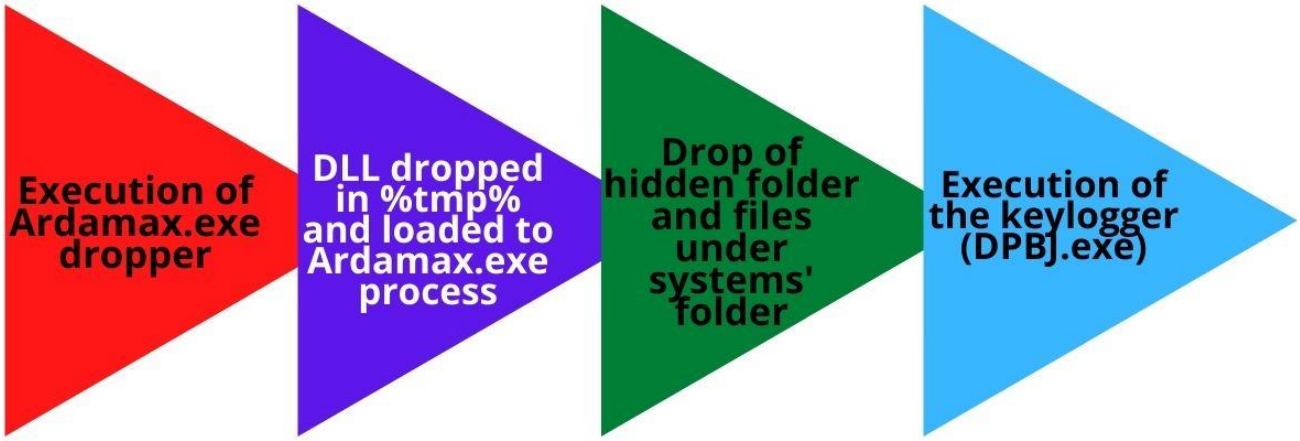
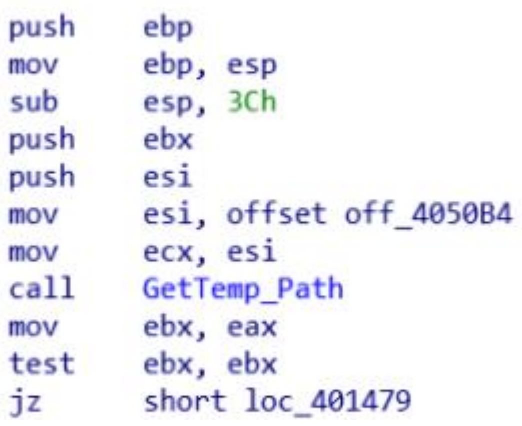

Execution of Ardamax.exe dropper
DLL dropped in %tmp% and loaded to Ardamax.exe process
Drop of hidden folder and files under systems' folder
Execution of the keylogger (DPBJ.exe)

Figure 20: Malware Execution Cycle

Execution of Ardamax Dropper

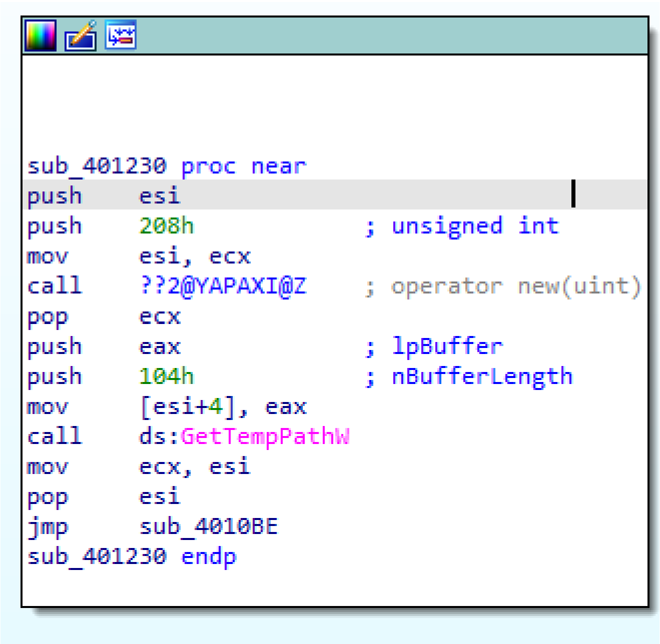
When the victim executes, the keylogger Ardmax.exe runs in the GetTemp path, that may collect the wondows %temp% for subsequent use (Figure 21).



```
push    ebp
mov     ebp, esp
sub     esp, 3Ch
push    ebx
push    esi
mov     esi, offset off_4050B4
mov     ecx, esi
call    GetTemp_Path
mov     ebx, eax
test    ebx, ebx
jz      short loc_401479
```

Figure 21: Get Temp Path

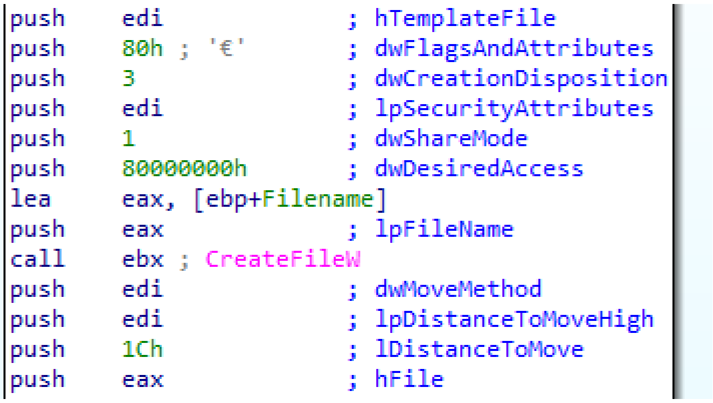
GetTemp Path invokes GetTempPathW to acquire the system's temporary file based on the disassembly output from IDA.



```
sub_401230 proc near
push    esi
push    208h            ; unsigned int
mov     esi, ecx
call    ??2@YAPAXI@Z    ; operator new(uint)
pop     ecx
push    eax             ; lpBuffer
push    104h            ; nBufferLength
mov     [esi+4], eax
call    ds:GetTempPathW
mov     ecx, esi
pop     esi
jmp     sub_4010BE
sub_401230 endp
```

Figure 22: GetTempPathW

The next procedure invokes CreateFileW. Ardamax drops numerous files to the temp folder during this operation, such as the previously indicated randomly named DLL.

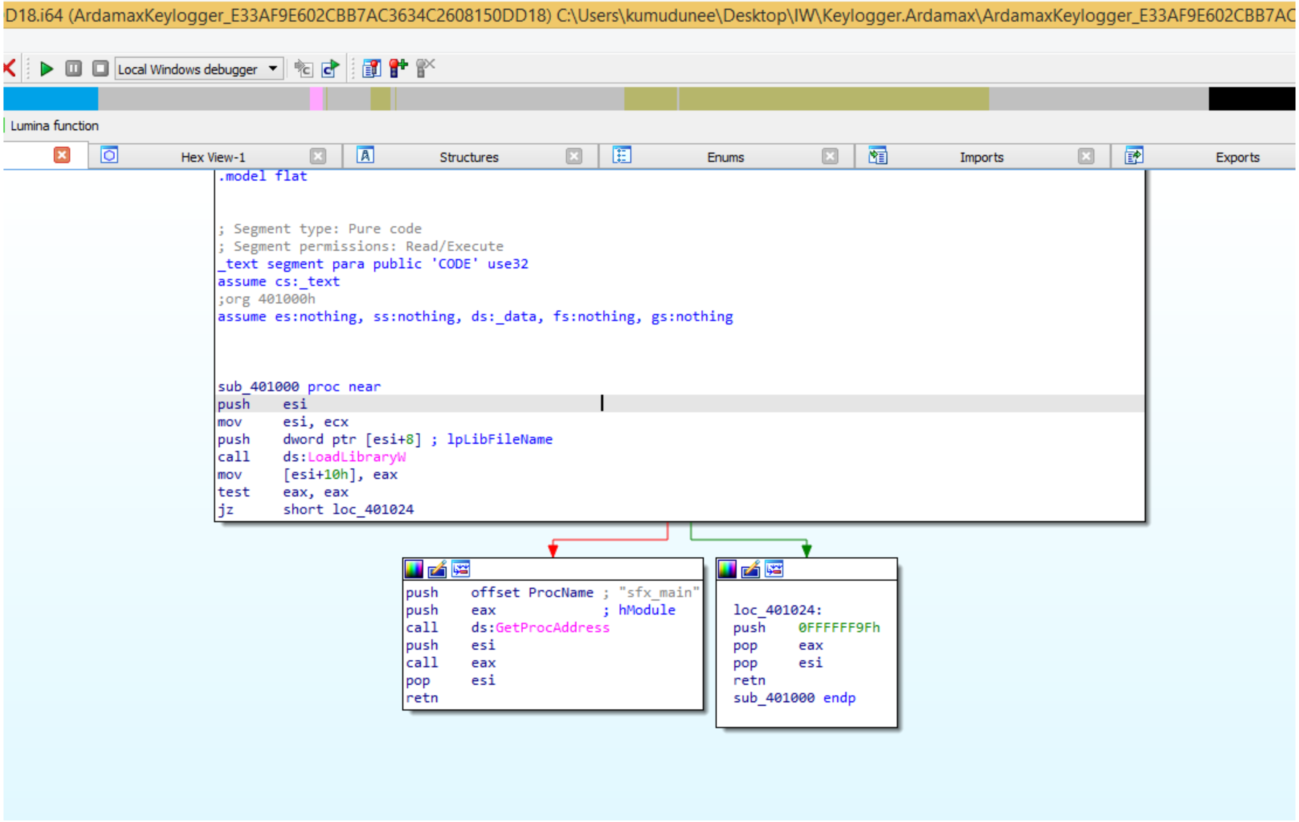


```
push    edi             ; hTemplateFile
push    80h ; '€'       ; dwFlagsAndAttributes
push    3               ; dwCreationDisposition
push    edi             ; lpSecurityAttributes
push    1               ; dwShareMode
push    80000000h       ; dwDesiredAccess
lea     eax, [ebp+Filename]
push    eax             ; lpFileName
call    ebx ; CreateFileW
push    edi             ; dwMoveMethod
push    edi             ; lpDistanceToMoveHigh
push    1Ch             ; lDistanceToMove
push    eax             ; hFile
```

Figure 23: CreateFileW

Execution of Ardamax DLL

When the DLL load is successfully, the dropper would execute GetProcAddress to obtain the sfx_main address of the DLL.



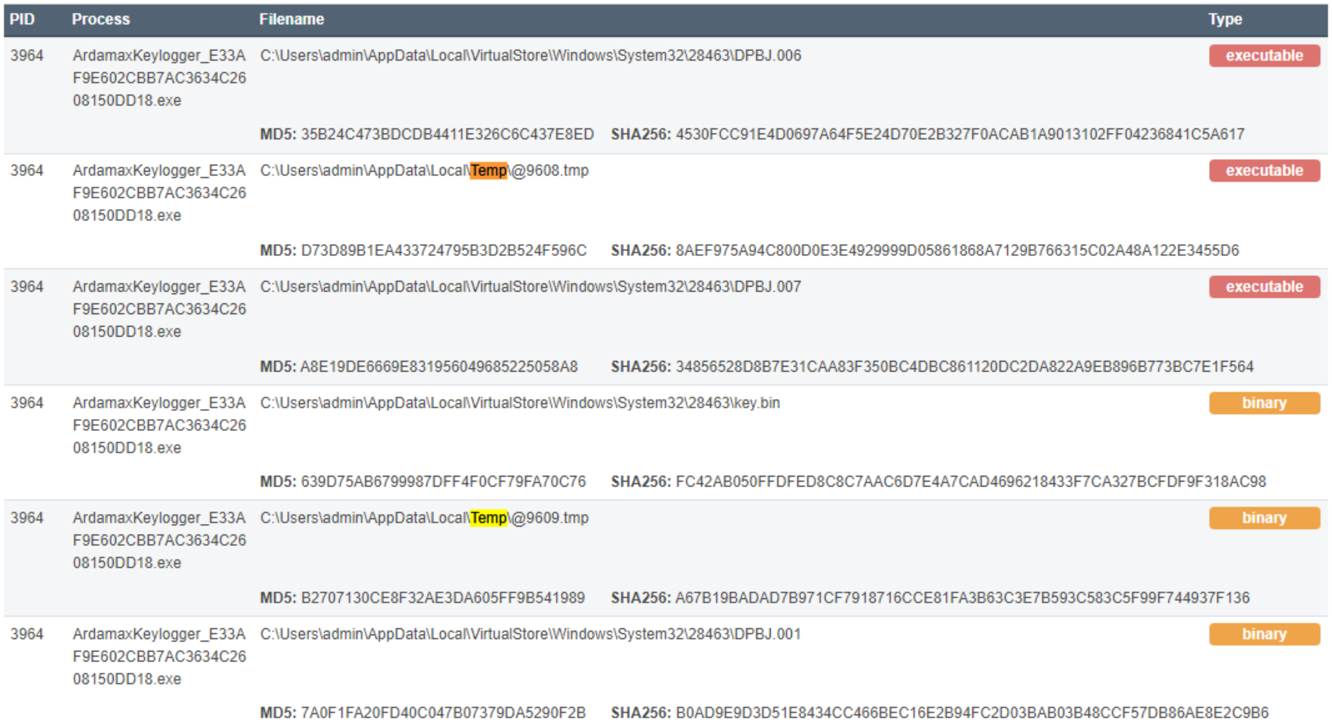
D18.i64 (ArdamaxKeylogger_E33AF9E602CBB7AC3634C2608150DD18) C:\Users\kumudunee\Desktop\IW\Keylogger.Ardamax\ArdamaxKeylogger_E33AF9E602CBB7AC

```
.model flat


; Segment type: Pure code
; Segment permissions: Read/Execute
_text segment para public 'CODE' use32
assume cs:_text
;org 401000h
assume es:nothing, ss:nothing, ds:_data, fs:nothing, gs:nothing



sub_401000 proc near
push    esi
mov     esi, ecx
push    dword ptr [esi+8] ; lpLibFileName
call    ds:LoadLibraryW
mov     [esi+10h], eax
test    eax, eax
jz      short loc_401024
```

```
push    offset ProcName ; "sfx_main"
push    eax             ; hModule
call    ds:GetProcAddress
push    esi
call    eax
pop     esi
retn
```

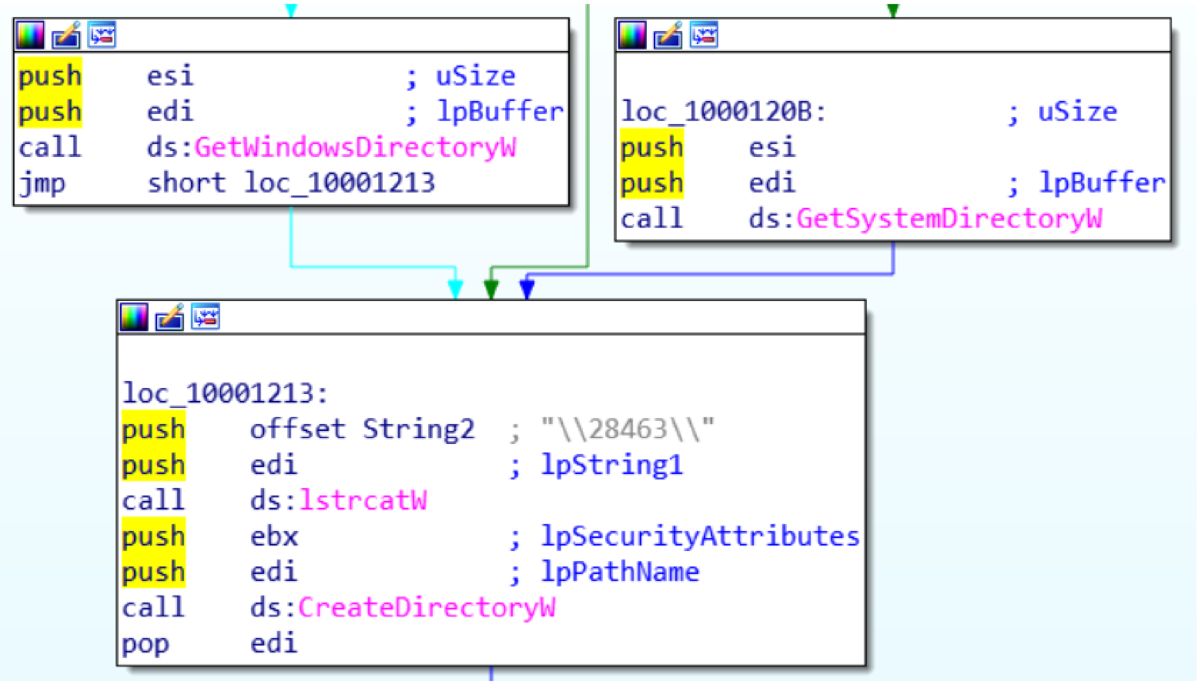
```
loc_401024:
push    0FFFFFF9Fh
pop     eax
pop     esi
retn
sub_401000 endp
```

Figure 24: sfx_main



PID	Process	Filename	Type
3964	ArdamaxKeylogger_E33AF9E602CBB7AC3634C2608150DD18.exe	C:\Users\admin\AppData\Local\VirtualStore\Windows\System32\28463\DPBJ.006 **MD5:** 35B24C473BDCDB4411E326C6C437E8ED **SHA256:** 4530FCC91E4D0697A64F5E24D70E2B327F0ACAB1A9013102FF04236841C5A617	executable
3964	ArdamaxKeylogger_E33AF9E602CBB7AC3634C2608150DD18.exe	C:\Users\admin\AppData\Local\Temp\@9608.tmp **MD5:** D73D89B1EA433724795B3D2B524F596C **SHA256:** 8AEF975A94C800D0E3E4929999D05861868A7129B766315C02A48A122E3455D6	executable
3964	ArdamaxKeylogger_E33AF9E602CBB7AC3634C2608150DD18.exe	C:\Users\admin\AppData\Local\VirtualStore\Windows\System32\28463\DPBJ.007 **MD5:** A8E19DE6669E831956049685225058A8 **SHA256:** 34856528D8B7E31CAA83F350BC4DBC861120DC2DA822A9EB896B773BC7E1F564	executable
3964	ArdamaxKeylogger_E33AF9E602CBB7AC3634C2608150DD18.exe	C:\Users\admin\AppData\Local\VirtualStore\Windows\System32\28463\key.bin **MD5:** 639D75AB6799987DFF4F0CF79FA70C76 **SHA256:** FC42AB050FFDFED8C8C7AAC6D7E4A7CAD4696218433F7CA327BCFDF9F318AC98	binary
3964	ArdamaxKeylogger_E33AF9E602CBB7AC3634C2608150DD18.exe	C:\Users\admin\AppData\Local\Temp\@9609.tmp **MD5:** B2707130CE8F32AE3DA605FF9B541989 **SHA256:** A67B19BADAD7B971CF7918716CCE81FA3B63C3E7B593C583C5F99F744937F136	binary
3964	ArdamaxKeylogger_E33AF9E602CBB7AC3634C2608150DD18.exe	C:\Users\admin\AppData\Local\VirtualStore\Windows\System32\28463\DPBJ.001 **MD5:** 7A0F1FA20FD40C047B07379DA5290F2B **SHA256:** B0AD9E9D3D51E8434CC466BEC16E2B94FC2D03BAB03B48CCF57DB86AE8E2C9B6	binary

Figure 25: Dropped Files



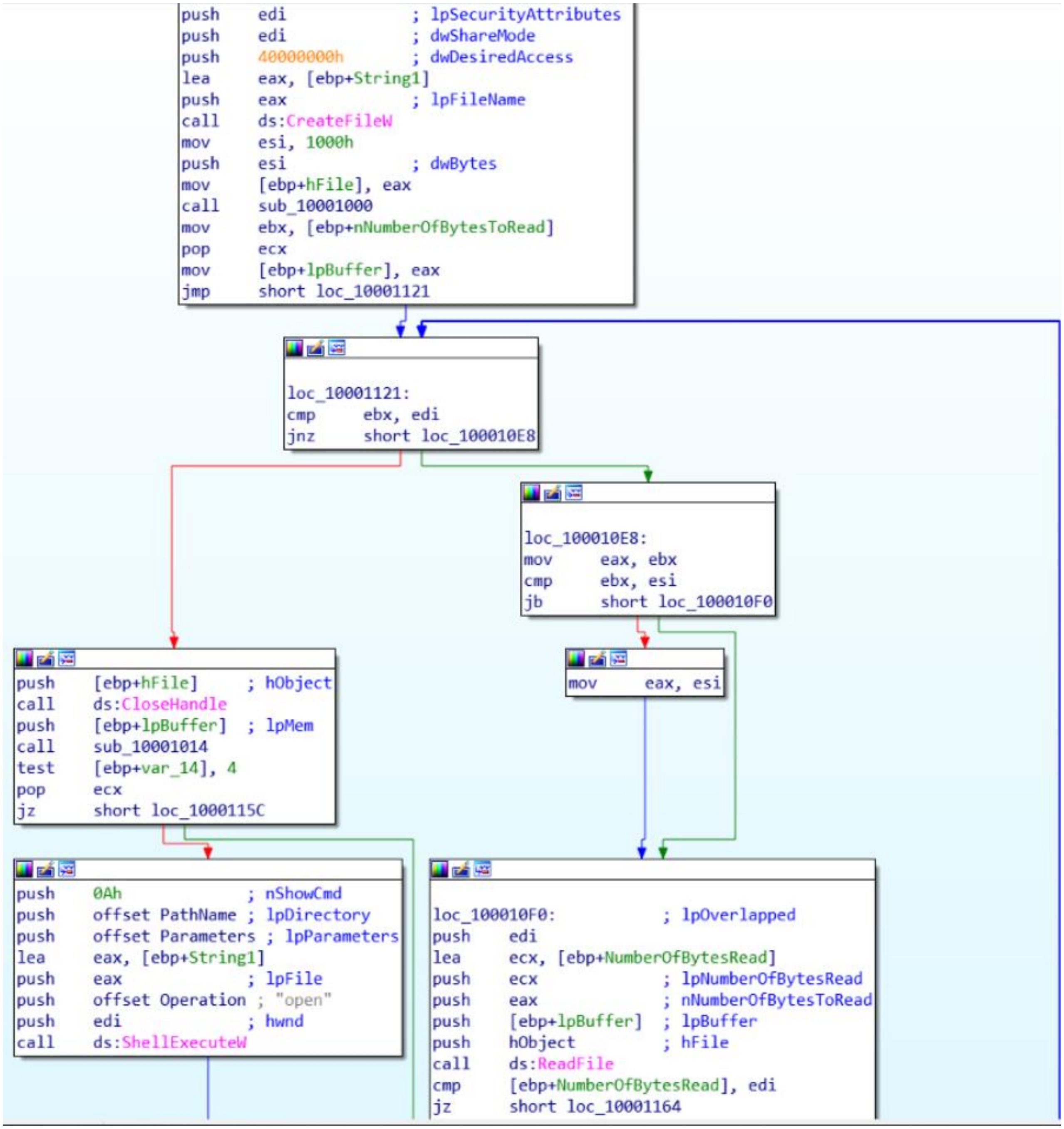
```
push    esi                 ; uSize
push    edi                 ; lpBuffer
call    ds:GetWindowsDirectoryW
jmp     short loc_10001213
```

```
loc_1000120B:               ; uSize
push    esi
push    edi                 ; lpBuffer
call    ds:GetSystemDirectoryW
```

```
loc_10001213:
push    offset String2  ; "\\28463\\"
push    edi             ; lpString1
call    ds:lstrcatW
push    ebx             ; lpSecurityAttributes
push    edi             ; lpPathName
call    ds:CreateDirectoryW
pop     edi
```

Figure 26: creating Hidden folders within the system folder

After copying all files to the specified folder, it’s main program, DPBJ.exe, get executed with the ShellExecuteW.



```
push    edi             ; lpSecurityAttributes
push    edi             ; dwShareMode
push    40000000h       ; dwDesiredAccess
lea     eax, [ebp+String1]
push    eax             ; lpFileName
call    ds:CreateFileW
mov     esi, 1000h
push    esi             ; dwBytes
mov     [ebp+hFile], eax
call    sub_10001000
mov     ebx, [ebp+nNumberOfBytesToRead]
pop     ecx
mov     [ebp+lpBuffer], eax
jmp     short loc_10001121
```

```
loc_10001121:
cmp     ebx, edi
jnz     short loc_100010E8
```

```
loc_100010E8:
mov     eax, ebx
cmp     ebx, esi
jb      short loc_100010F0
```

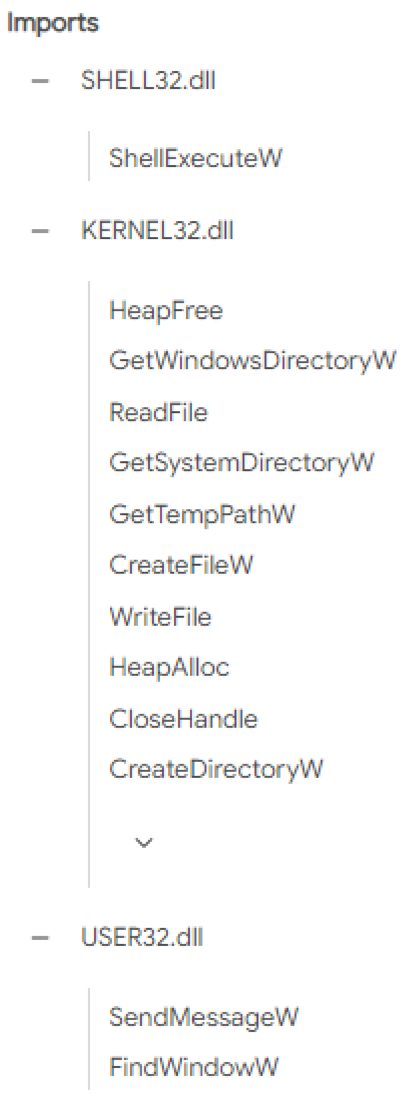
```
push    [ebp+hFile]     ; hObject
call    ds:CloseHandle
push    [ebp+lpBuffer]  ; lpMem
call    sub_10001014
test    [ebp+var_14], 4
pop     ecx
jz      short loc_1000115C
```

```
mov     eax, esi
```

```
push    0Ah             ; nShowCmd
push    offset PathName ; lpDirectory
push    offset Parameters ; lpParameters
lea     eax, [ebp+String1]
push    eax             ; lpFile
push    offset Operation ; "open"
push    edi             ; hwnd
call    ds:ShellExecuteW
```

```
loc_100010F0:                   ; lpOverlapped
push    edi
lea     ecx, [ebp+NumberOfBytesRead]
push    ecx                     ; lpNumberOfBytesRead
push    eax                     ; nNumberOfBytesToRead
push    [ebp+lpBuffer]          ; lpBuffer
push    hObject                 ; hFile
call    ds:ReadFile
cmp     [ebp+NumberOfBytesRead], edi
jz      short loc_10001164
```

Figure 27: Numerous files are dropped into the concealed folder, and the keylogger's activation starts.



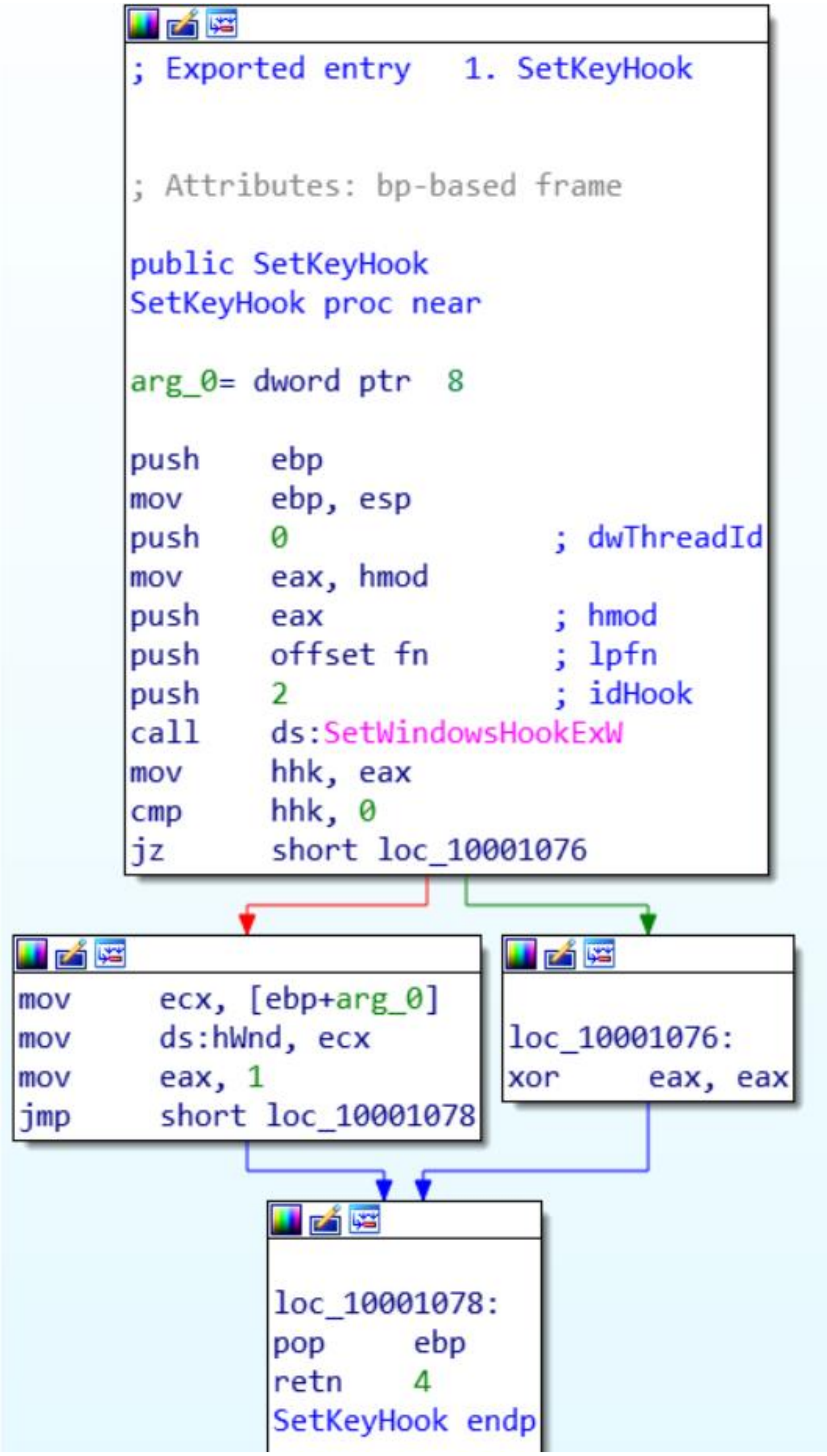
Imports

- SHELL32.dll
  - ShellExecuteW
- KERNEL32.dll
  - HeapFree
  - GetWindowsDirectoryW
  - ReadFile
  - GetSystemDirectoryW
  - GetTempPathW
  - CreateFileW
  - WriteFile
  - HeapAlloc
  - CloseHandle
  - CreateDirectoryW
- USER32.dll
  - SendMessageW
  - FindWindowW

Figure 28: Temp file imports

Execution of Keylogger

The SetWindowsHookEx function is used in the following procedure with an idHook of 2 (WH KEYBOARD) that handles keystroke events and consequently logs them:



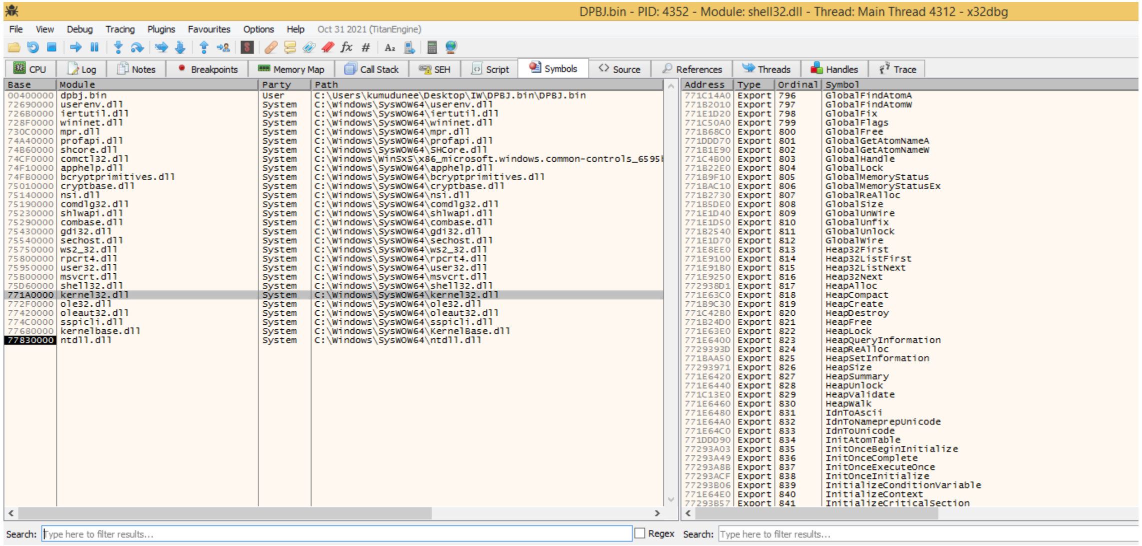
```
; Exported entry   1. SetKeyHook


; Attributes: bp-based frame

public SetKeyHook
SetKeyHook proc near

arg_0= dword ptr  8

push    ebp
mov     ebp, esp
push    0               ; dwThreadId
mov     eax, hmod
push    eax             ; hmod
push    offset fn       ; lpfn
push    2               ; idHook
call    ds:SetWindowsHookExW
mov     hhk, eax
cmp     hhk, 0
jz      short loc_10001076
```

```
mov     ecx, [ebp+arg_0]
mov     ds:hWnd, ecx
mov     eax, 1
jmp     short loc_10001078
```

```

loc_10001076:
xor     eax, eax
```

```

loc_10001078:
pop     ebp
retn    4
SetKeyHook endp
```

Figure 29: SetKeyHook subroutine



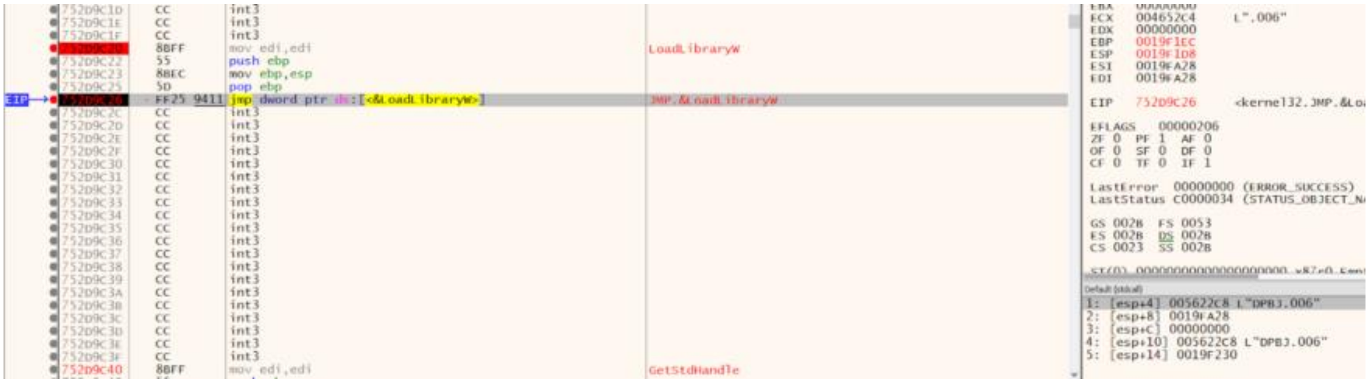
DPBJ.bin - PID: 4352 - Module: shell32.dll - Thread: Main Thread 4312 - x32dbg
File View Debug Tracing Plugins Favourites Options Help Oct 31 2021 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace

```
Base     Module                 Party   Path
00400000 dpbj.bin               User    C:\Users\kumudunee\Desktop\IW\DPBJ.bin\DPBJ.bin
72690000 userenv.dll            System  C:\Windows\SysWOW64\userenv.dll
726B0000 iertutil.dll           System  C:\Windows\SysWOW64\iertutil.dll
728F0000 wininet.dll            System  C:\Windows\SysWOW64\wininet.dll
730C0000 mpr.dll                System  C:\Windows\SysWOW64\mpr.dll
74A40000 profapi.dll            System  C:\Windows\SysWOW64\profapi.dll
74B60000 shcore.dll             System  C:\Windows\SysWOW64\SHCore.dll
74CF0000 comctl32.dll           System  C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595
74F10000 apphelp.dll            System  C:\Windows\SysWOW64\apphelp.dll
74FB0000 bcryptprimitives.dll   System  C:\Windows\SysWOW64\bcryptprimitives.dll
75010000 cryptbase.dll          System  C:\Windows\SysWOW64\cryptbase.dll
75140000 nsi.dll                System  C:\Windows\SysWOW64\nsi.dll
75190000 comdlg32.dll           System  C:\Windows\SysWOW64\comdlg32.dll
75230000 shlwapi.dll            System  C:\Windows\SysWOW64\shlwapi.dll
75290000 combase.dll            System  C:\Windows\SysWOW64\combase.dll
75430000 gdi32.dll              System  C:\Windows\SysWOW64\gdi32.dll
75540000 sechost.dll            System  C:\Windows\SysWOW64\sechost.dll
75750000 ws2_32.dll             System  C:\Windows\SysWOW64\ws2_32.dll
75800000 rpcrt4.dll             System  C:\Windows\SysWOW64\rpcrt4.dll
75950000 user32.dll             System  C:\Windows\SysWOW64\user32.dll
75B00000 msvcrt.dll             System  C:\Windows\SysWOW64\msvcrt.dll
75D60000 shell32.dll            System  C:\Windows\SysWOW64\shell32.dll
771A0000 kernel32.dll           System  C:\Windows\SysWOW64\kernel32.dll
772F0000 ole32.dll              System  C:\Windows\SysWOW64\ole32.dll
77420000 oleaut32.dll           System  C:\Windows\SysWOW64\oleaut32.dll
774C0000 sspicli.dll            System  C:\Windows\SysWOW64\sspicli.dll
77680000 kernelbase.dll         System  C:\Windows\SysWOW64\KernelBase.dll
77830000 ntdll.dll              System  C:\Windows\SysWOW64\ntdll.dll
```

```
Address  Type   Ordinal Symbol
771C14A0 Export 796     GlobalFindAtomA
771B2010 Export 797     GlobalFindAtomW
771E1D20 Export 798     GlobalFix
771C50A0 Export 799     GlobalFlags
771B68C0 Export 800     GlobalFree
771DDD70 Export 801     GlobalGetAtomNameA
771B1E90 Export 802     GlobalGetAtomNameW
771C4B00 Export 803     GlobalHandle
771B22E0 Export 804     GlobalLock
771B9F10 Export 805     GlobalMemoryStatus
771BAC10 Export 806     GlobalMemoryStatusEx
771B2730 Export 807     GlobalReAlloc
771B5DE0 Export 808     GlobalSize
771E1D40 Export 809     GlobalUnWire
771E1D50 Export 810     GlobalUnfix
771B2540 Export 811     GlobalUnlock
771E1D70 Export 812     GlobalWire
771E8EE0 Export 813     Heap32First
771E9100 Export 814     Heap32ListFirst
771E91B0 Export 815     Heap32ListNext
771E9250 Export 816     Heap32Next
772938D1 Export 817     HeapAlloc
771E63C0 Export 818     HeapCompact
771B9C30 Export 819     HeapCreate
771C42B0 Export 820     HeapDestroy
771B24D0 Export 821     HeapFree
771E63E0 Export 822     HeapLock
771E6400 Export 823     HeapQueryInformation
7729393D Export 824     HeapReAlloc
771BAA50 Export 825     HeapSetInformation
77293971 Export 826     HeapSize
771E6420 Export 827     HeapSummary
771E6440 Export 828     HeapUnlock
771C13E0 Export 829     HeapValidate
771E6460 Export 830     HeapWalk
771E6480 Export 831     IdnToAscii
771E64A0 Export 832     IdnToNameprepUnicode
771E64C0 Export 833     IdnToUnicode
771DDD90 Export 834     InitAtomTable
77293A03 Export 835     InitOnceBeginInitialize
77293A49 Export 836     InitOnceComplete
77293A8B Export 837     InitOnceExecuteOnce
77293ACF Export 838     InitOnceInitialize
77293B06 Export 839     InitializeConditionVariable
771E64E0 Export 840     InitializeContext
77293B57 Export 841     InitializeCriticalSection
```

Search: Type here to filter results...
☐ Regex
Search: Type here to filter results...

Figure 30: Using x32dbg



```
     752D9C1D  CC         int3
     752D9C1E  CC         int3
     752D9C1F  CC         int3
     752D9C20  8BFF       mov edi,edi                               LoadLibraryW
     752D9C22  55         push ebp
     752D9C23  8BEC       mov ebp,esp
     752D9C25  5D         pop ebp
EIP→ 752D9C26  FF25 9411  jmp dword ptr ds:[<&LoadLibraryW>]        JMP.&LoadLibraryW
     752D9C2C  CC         int3
     752D9C2D  CC         int3
     752D9C2E  CC         int3
     752D9C2F  CC         int3
     752D9C30  CC         int3
     752D9C31  CC         int3
     752D9C32  CC         int3
     752D9C33  CC         int3
     752D9C34  CC         int3
     752D9C35  CC         int3
     752D9C36  CC         int3
     752D9C37  CC         int3
     752D9C38  CC         int3
     752D9C39  CC         int3
     752D9C3A  CC         int3
     752D9C3B  CC         int3
     752D9C3C  CC         int3
     752D9C3D  CC         int3
     752D9C3E  CC         int3
     752D9C3F  CC         int3
     752D9C40  8BFF       mov edi,edi                               GetStdHandle
```

```
ECX   004652C4      L".006"
EDX   00000000
EBP   0019F1EC
ESP   0019F1D8
ESI   0019FA28
EDI   0019FA28

EIP   752D9C26      <kernel32.JMP.&Lo

EFLAGS   00000206
ZF 0  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError  00000000 (ERROR_SUCCESS)
LastStatus C0000034 (STATUS_OBJECT_N

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

Default (stdcall)
1: [esp+4] 005622C8 L"DPBJ.006"
2: [esp+8] 0019FA28
3: [esp+C] 00000000
4: [esp+10] 005622C8 L"DPBJ.006"
5: [esp+14] 0019F230
```

Figure 31: LoadLibraryW

The loss of validation in the LoadLibraryW call provides a potential backdoor for the built executable. This permits a DLL to be loaded just based on its name, therefore any third-party attacker takes advantage of this method simply creating his own malicious DLL and replacing it with the exact name ("DPBJ.006," in this example). Finally, when DPBJ.exe is invoked, it will load the forged DLL of the substituted attacker.

FINDINGS 03

d1f3b9372a6be9c02430b6e4526202974179a674ce94fe22028d7212ae6be9e7

Labels

Trojan agent, backdoor agent

Basic Details

Name: INETSVC.EXE

File Type: Win32 EXE

File Size: 204.00 KB

MD5: c6f78ad187c365d117cacbee140f6230

SHA-1: 5116f281c61639b48fd58caaed60018bafdefe7a

SHA-256: d1f3b9372a6be9c02430b6e4526202974179a674ce94fe22028d7212ae6be9e7

Vhash: 025046651d6d1048z45uz137z

SHA-512:

41698e5ca4579b369372e3e3a7e5e05004e25eb9965e650df30b98ba7ec2182a374c7560c1d5f1e06a9b282aa864153d6c4b1d6ed04300b6a8d359aec4a117df

SSDEEP:

1536:X86D0r4QxG5+XCFpaG7+esyzktLYUwnZ7hUOKYUwnZ7hUOaeYUwnZ7hUOKYUwnZr:X8O0IgCvH7+UzktMxzxgRxzx9

Magic PE32 executable for MS Windows (GUI) Intel 80386 32-bit

TrID: Win32 Executable MS Visual C++ (generic) (38.8%)

TrID: Microsoft Visual C++ compiled executable (generic) (20.5%)

TrID: Win64 Executable (generic) (13%)

TrID: Win32 Dynamic Link Library (generic) (8.1%)

TrID: Win16 NE executable (generic) (6.2%)

Target Machine: Intel 386 or later processors and compatible processors

Entropy: 7.711

File Signature Verification

File is not signed

Anti-Virus

AhnLab-V3: Backdoor/Win32.Akdoor.R176413

ALYac: Trojan.Agent.45056A

Portable Executable Information

Compilation Timestamp: 2016-02-07 03:17:51

PE Sections

Table 2: PE Section

Name	Raw Size	Entropy	MD5
.text	53248	6.51	08112b571663ff5ed42e331a00ccce0c
.rdata	8192	4.57	ca61927558a4dfe9305eb037a5432960
.data	139264	6.94	bb49b2fb00c1ae88ad440971914711a7
.sxdata	4096	0.18	c58b62cf949e8636ebd5c75f482207c3

Imports

ADVAPI32.dll

SSLEAY32.dll

KERNEL32.dll

WS2_32.dll

LIBEAY32.dll

Packers

Name: Microsoft Visual C++ ver 5.0/6.0 - no sec. Cab.7z.Zip - 2016-02-07

Unpacker: Big sec. 3 .data , Not packed , try www.ollydbg.de or x64 debug v0025 www.x64dbg.com

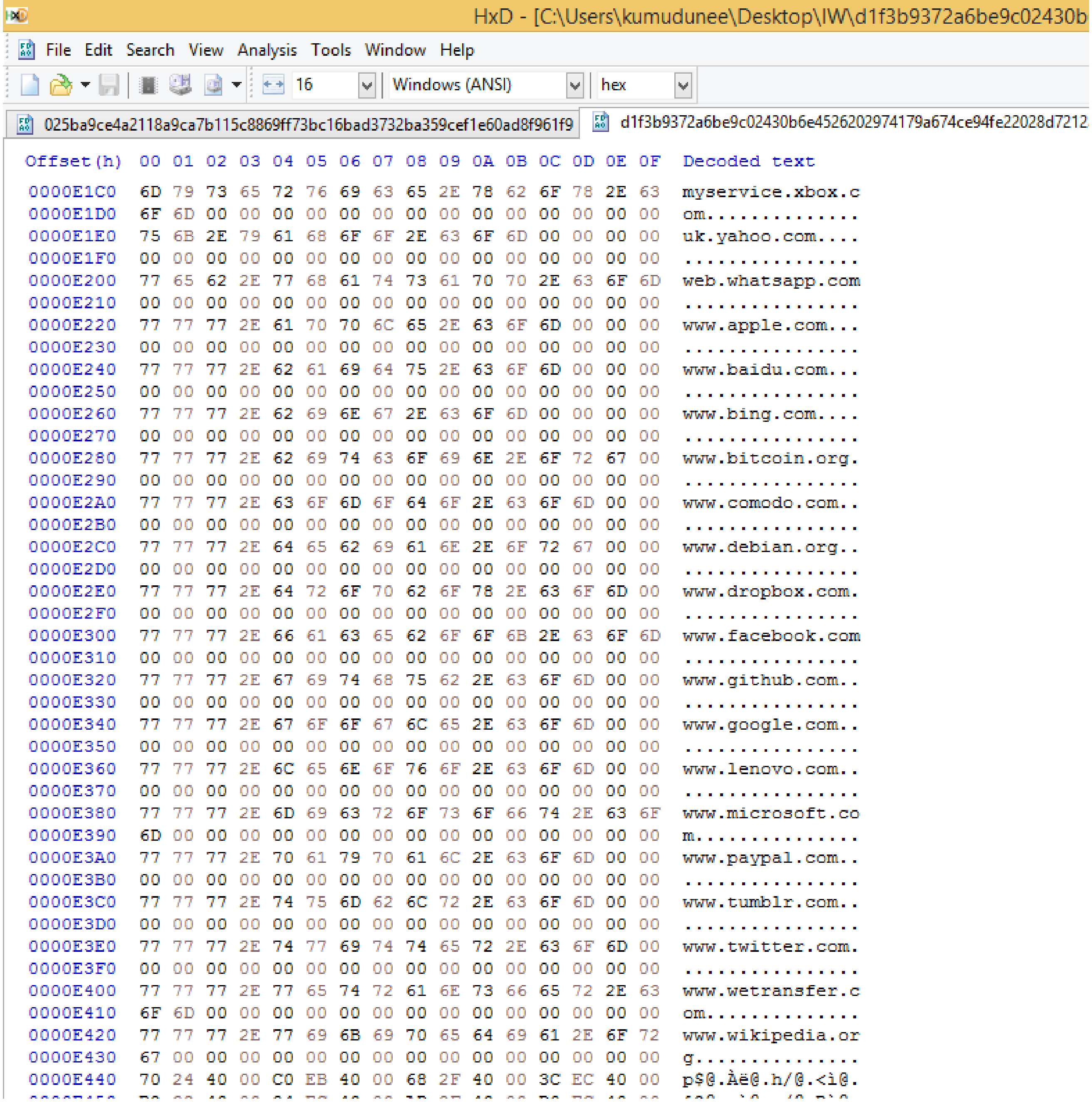
Description

It is a malicious Windows 32-bit executable. This application appears to be intended to enable an infected system to act as a proxy server, according to the analysis. When the virus is run, it connects to the infected system's port 8000 and listens for incoming connections. It may read the windows installation date.

```
3376 rundll32.exe (1)
2952 rundll32.exe (1)
3056 rundll32.exe (1)
Operation: READ
Name: INSTALLDATE
Value:
Key:HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION
TypeValue: REG_DWORD
```

Also, it has the ability to modify the phishing filter for Internet Explorer and also change the internet zones settings.

The domains for which the virus has public SSL certificates, which are used to initiate "FAKE TLS" sessions are shown in the Figure 10.

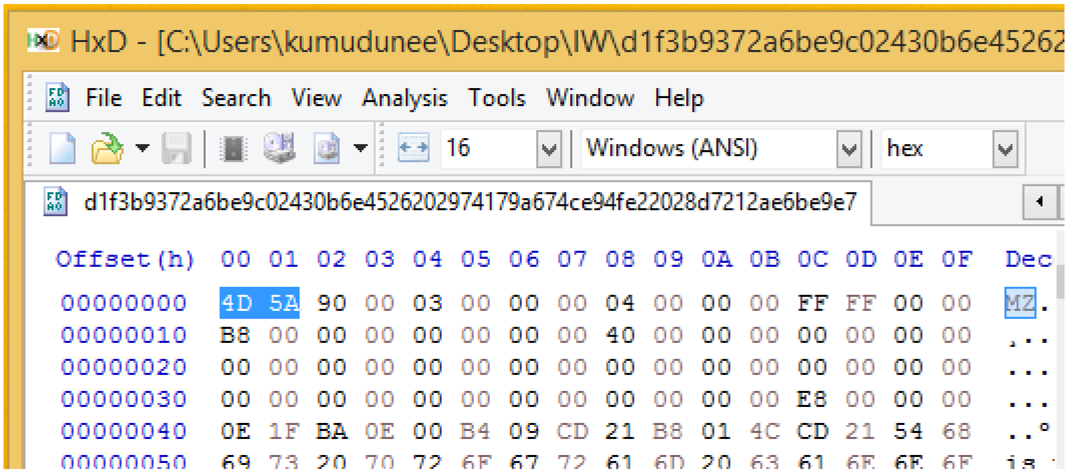

HxD - [C:\Users\kumudunee\Desktop\IW\d1f3b9372a6be9c02430b
File
Edit
Search
View
Analysis
Tools
Window
Help
16
Windows (ANSI)
hex
025ba9ce4a2118a9ca7b115c8869ff73bc16bad3732ba359cef1e60ad8f961f9
d1f3b9372a6be9c02430b6e4526202974179a674ce94fe22028d7212

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

0000E1C0  6D 79 73 65 72 76 69 63 65 2E 78 62 6F 78 2E 63  myservice.xbox.c
0000E1D0  6F 6D 00 00 00 00 00 00 00 00 00 00 00 00 00 00  om..............
0000E1E0  75 6B 2E 79 61 68 6F 6F 2E 63 6F 6D 00 00 00 00  uk.yahoo.com....
0000E1F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000E200  77 65 62 2E 77 68 61 74 73 61 70 70 2E 63 6F 6D  web.whatsapp.com
0000E210  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000E220  77 77 77 2E 61 70 70 6C 65 2E 63 6F 6D 00 00 00  www.apple.com...
0000E230  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000E240  77 77 77 2E 62 61 69 64 75 2E 63 6F 6D 00 00 00  www.baidu.com...
0000E250  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000E260  77 77 77 2E 62 69 6E 67 2E 63 6F 6D 00 00 00 00  www.bing.com....
0000E270  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000E280  77 77 77 2E 62 69 74 63 6F 69 6E 2E 6F 72 67 00  www.bitcoin.org.
0000E290  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000E2A0  77 77 77 2E 63 6F 6D 6F 64 6F 2E 63 6F 6D 00 00  www.comodo.com..
0000E2B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000E2C0  77 77 77 2E 64 65 62 69 61 6E 2E 6F 72 67 00 00  www.debian.org..
0000E2D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000E2E0  77 77 77 2E 64 72 6F 70 62 6F 78 2E 63 6F 6D 00  www.dropbox.com.
0000E2F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000E300  77 77 77 2E 66 61 63 65 62 6F 6F 6B 2E 63 6F 6D  www.facebook.com
0000E310  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000E320  77 77 77 2E 67 69 74 68 75 62 2E 63 6F 6D 00 00  www.github.com..
0000E330  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000E340  77 77 77 2E 67 6F 6F 67 6C 65 2E 63 6F 6D 00 00  www.google.com..
0000E350  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000E360  77 77 77 2E 6C 65 6E 6F 76 6F 2E 63 6F 6D 00 00  www.lenovo.com..
0000E370  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000E380  77 77 77 2E 6D 69 63 72 6F 73 6F 66 74 2E 63 6F  www.microsoft.co
0000E390  6D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  m...............
0000E3A0  77 77 77 2E 70 61 79 70 61 6C 2E 63 6F 6D 00 00  www.paypal.com..
0000E3B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000E3C0  77 77 77 2E 74 75 6D 62 6C 72 2E 63 6F 6D 00 00  www.tumblr.com..
0000E3D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000E3E0  77 77 77 2E 74 77 69 74 74 65 72 2E 63 6F 6D 00  www.twitter.com.
0000E3F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000E400  77 77 77 2E 77 65 74 72 61 6E 73 66 65 72 2E 63  www.wetransfer.c
0000E410  6F 6D 00 00 00 00 00 00 00 00 00 00 00 00 00 00  om..............
0000E420  77 77 77 2E 77 69 6B 69 70 65 64 69 61 2E 6F 72  www.wikipedia.or
0000E430  67 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  g...............
0000E440  70 24 40 00 C0 EB 40 00 68 2F 40 00 3C EC 40 00  p$@.Àë@.h/@.<ì@.
```

Figure 32: SSL cert list

Analysis Process

File type is identified with the use of hex editor.



HxD - [C:\Users\kumudunee\Desktop\IW\d1f3b9372a6be9c02430b6e45262

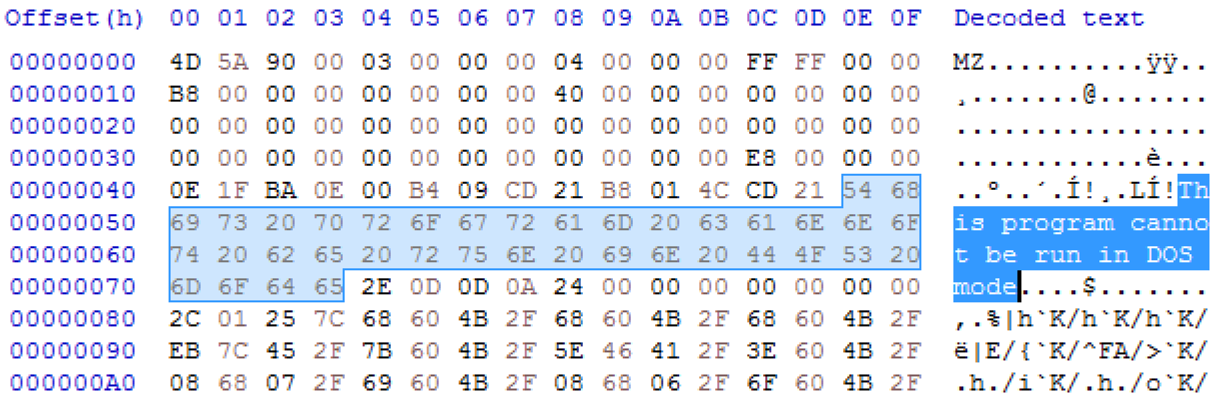
16 | Windows (ANSI) | hex

d1f3b9372a6be9c02430b6e4526202974179a674ce94fe22028d7212ae6be9e7

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Dec
00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ.
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸..
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...
00000030  00 00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00  ...
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º
00000050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is 
```

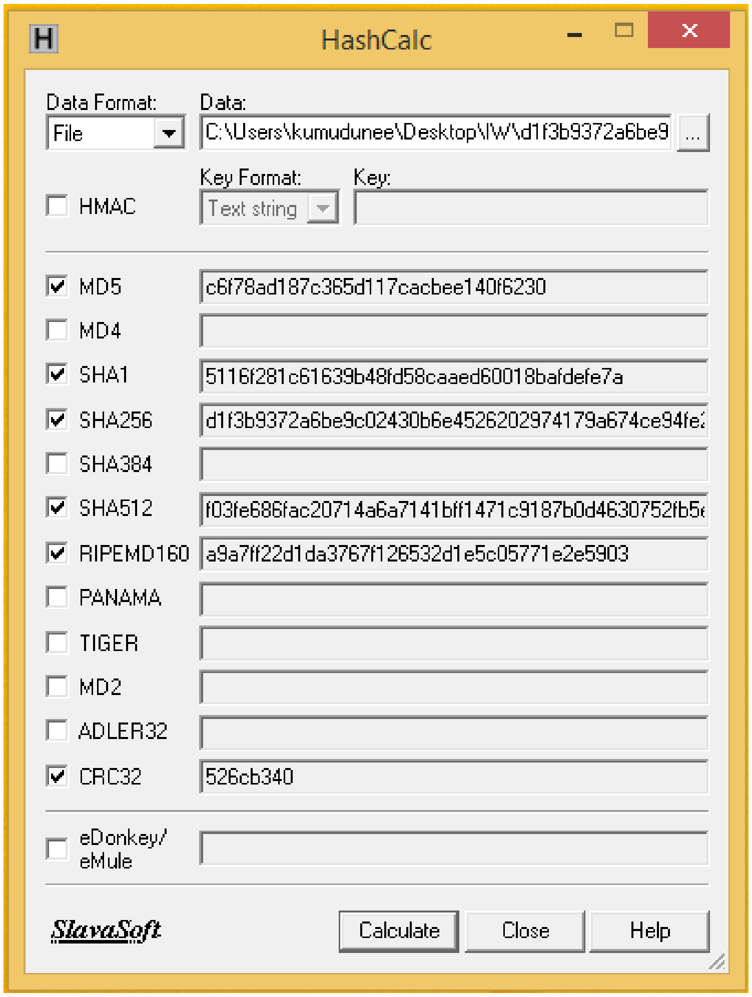
Figure 33: File Type identification

MZ stands for Portable Executable. There is a clear indication of that the program can not run in DOS mode. Which means the program does not compatible with oldish system. Portable Executables can be in formats such as exe, dll etc. In order to identify the file, type the file signature should be analyzed. We use this technique to avoid the false positives caused because of the double extension. In the first two bytes of a PE file, the file signature is represented by the hexadecimal numbers 4D, 5A, or MZ.



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00  ............è...
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
00000050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
00000060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
00000070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
00000080  2C 01 25 7C 68 60 4B 2F 68 60 4B 2F 68 60 4B 2F  ,.%|h`K/h`K/h`K/
00000090  EB 7C 45 2F 7B 60 4B 2F 5E 46 41 2F 3E 60 4B 2F  ë|E/{`K/^FA/>`K/
000000A0  08 68 07 2F 69 60 4B 2F 08 68 06 2F 6F 60 4B 2F  .h./i`K/.h./o`K/
```

Figure 34: HxD



HashCalc

Data Format: File

Data: C:\Users\kumudunee\Desktop\IW\d1f3b9372a6be9

Key Format: Text string

Key:

☐ HMAC

☑ MD5 c6f78ad187c365d117cacbee140f6230

☐ MD4

☑ SHA1 5116f281c61639b48fd58caaed60018bafdefe7a

☑ SHA256 d1f3b9372a6be9c02430b6e4526202974179a674ce94fe

☐ SHA384

☑ SHA512 f03fe686fac20714a6a7141bff1471c9187b0d4630752fb5

☑ RIPEMD160 a9a7ff22d1da3767f126532d1e5c05771e2e5903

☐ PANAMA

☐ TIGER

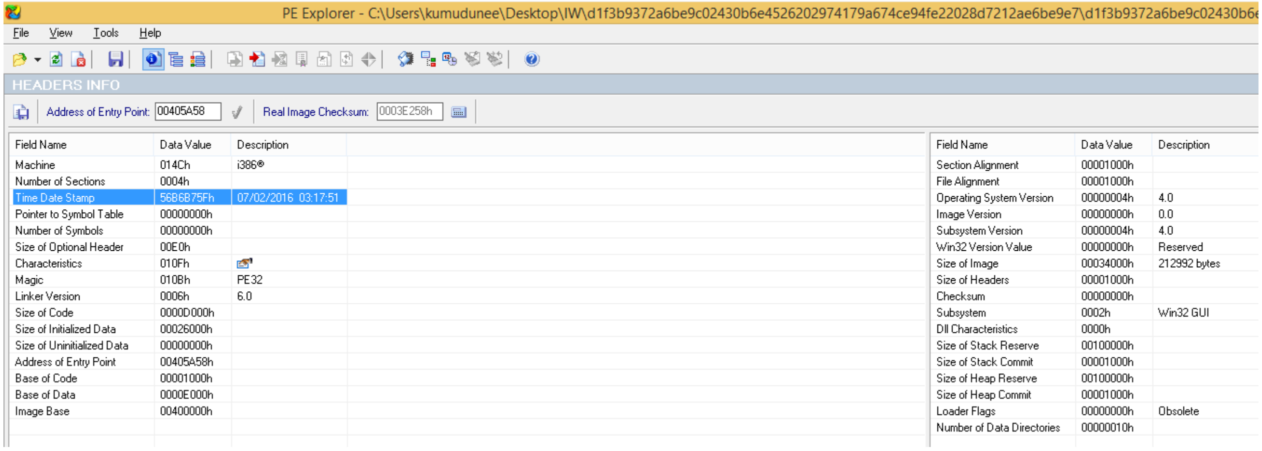
☐ MD2

☐ ADLER32

☑ CRC32 526cb340

☐ eDonkey/ eMule

Figure 35: Hash Calculation



PE Explorer - C:\Users\kumudunee\Desktop\IW\d1f3b9372a6be9c02430b6e4526202974179a674ce94fe22028d7212ae6be9e7\d1f3b9372a6be9c02430b6e

Address of Entry Point: 00405A58

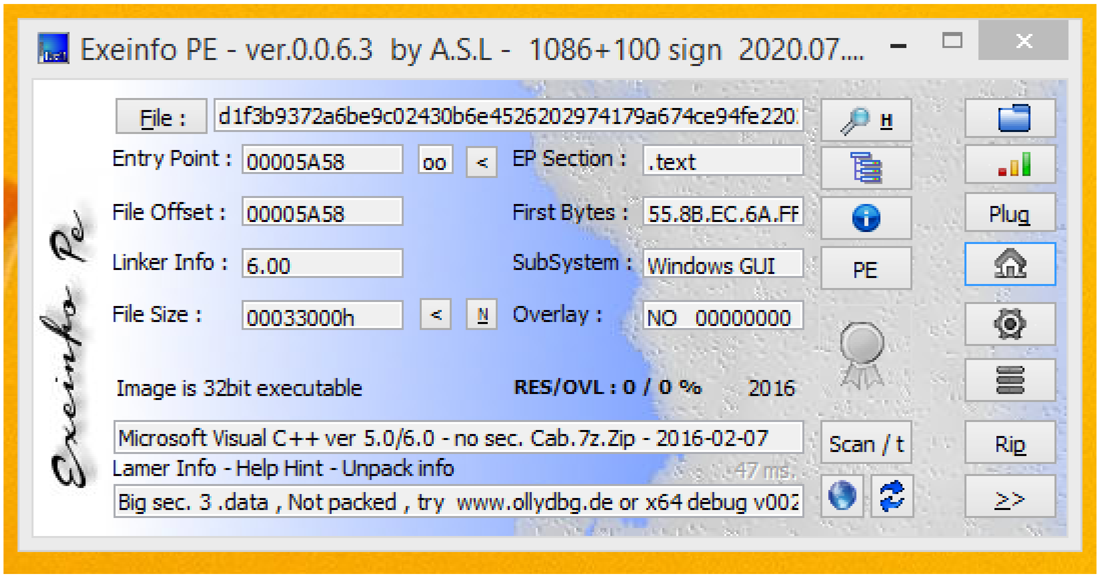
Real Image Checksum: 0003E258h

Field Name	Data Value	Description
Machine	014Ch	i386®
Number of Sections	0004h	
Time Date Stamp	56B6B75Fh	07/02/2016 03:17:51
Pointer to Symbol Table	00000000h	
Number of Symbols	00000000h	
Size of Optional Header	00E0h	
Characteristics	010Fh	
Magic	010Bh	PE32
Linker Version	0006h	6.0
Size of Code	0000D000h	
Size of Initialized Data	00026000h	
Size of Uninitialized Data	00000000h	
Address of Entry Point	00405A58h	
Base of Code	00001000h	
Base of Data	0000E000h	
Image Base	00400000h	

Field Name	Data Value	Description
Section Alignment	00001000h	
File Alignment	00001000h	
Operating System Version	00000004h	4.0
Image Version	00000000h	0.0
Subsystem Version	00000004h	4.0
Win32 Version Value	00000000h	Reserved
Size of Image	00034000h	212992 bytes
Size of Headers	00001000h	
Checksum	00000000h	
Subsystem	0002h	Win32 GUI
Dll Characteristics	0000h	
Size of Stack Reserve	00100000h	
Size of Stack Commit	00001000h	
Size of Heap Reserve	00100000h	
Size of Heap Commit	00001000h	
Loader Flags	00000000h	Obsolete
Number of Data Directories	00000010h	

Figure 36: Compilation Timestamp

Figure 13 shows the compilation timestamp.



Exeinfo PE - ver.0.0.6.3 by A.S.L - 1086+100 sign 2020.07....

File : d1f3b9372a6be9c02430b6e4526202974179a674ce94fe220

Entry Point : 00005A58 oo < EP Section : .text

File Offset : 00005A58 First Bytes : 55.8B.EC.6A.FF

Linker Info : 6.00 SubSystem : Windows GUI

File Size : 00033000h < N Overlay : NO 00000000

Image is 32bit executable RES/OVL : 0 / 0 % 2016

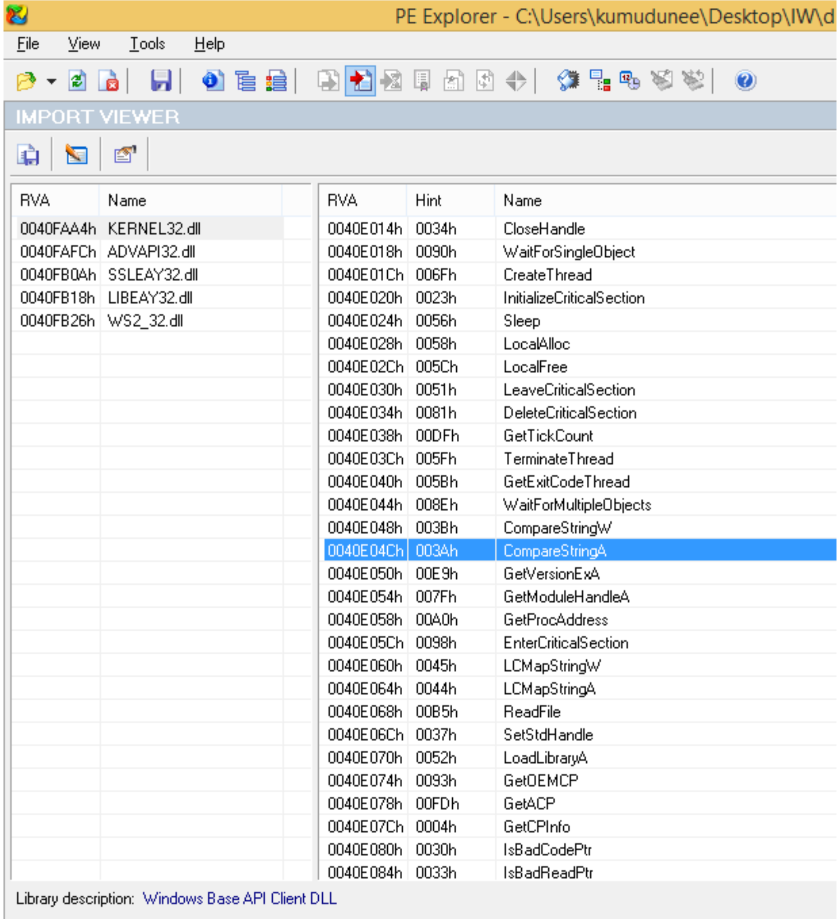
Microsoft Visual C++ ver 5.0/6.0 - no sec. Cab.7z.Zip - 2016-02-07

Lamer Info - Help Hint - Unpack info 47 ms.

Big sec. 3 .data , Not packed , try www.ollydbg.de or x64 debug v002

Figure 37: Using Exeinfo PE

With the use of Exeinfo PE tool we could found that the packer Microsoft Visual C++ is used to pack the malware and the version is 6.0.

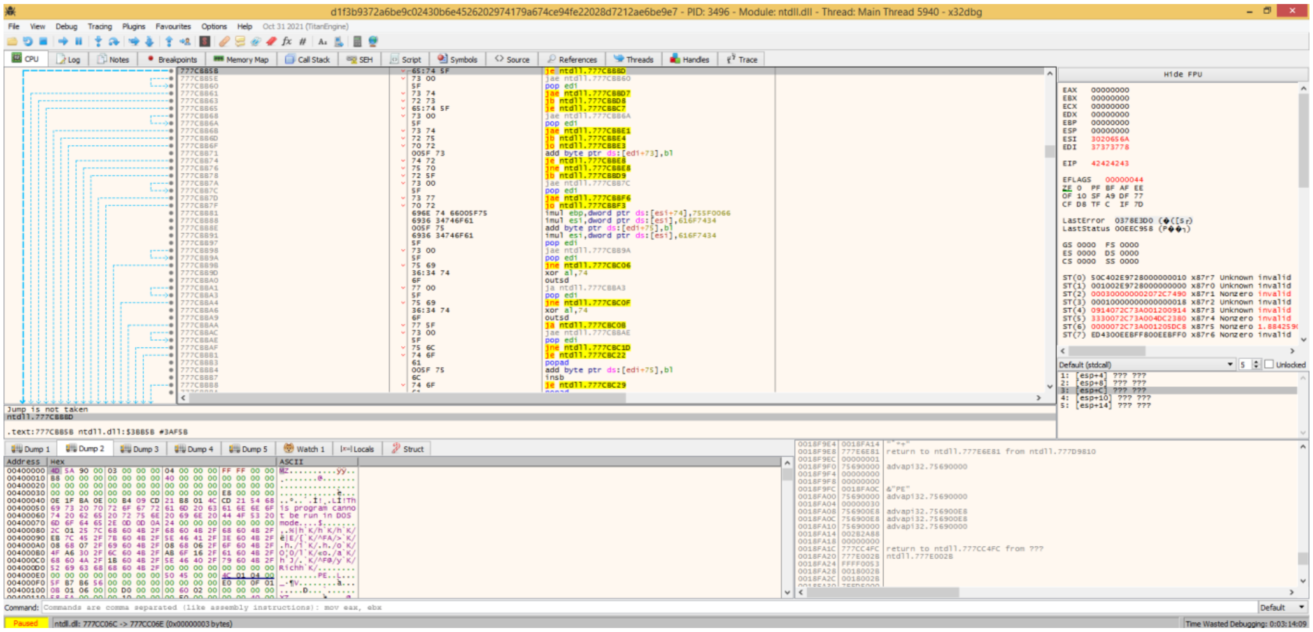


RVA	Name
0040FAA4h	KERNEL32.dll
0040FAFCh	ADVAPI32.dll
0040FB0Ah	SSLEAY32.dll
0040FB18h	LIBEAY32.dll
0040FB26h	WS2_32.dll

RVA	Hint	Name
0040E014h	0034h	CloseHandle
0040E018h	0090h	WaitForSingleObject
0040E01Ch	006Fh	CreateThread
0040E020h	0023h	InitializeCriticalSection
0040E024h	0056h	Sleep
0040E028h	0058h	LocalAlloc
0040E02Ch	005Ch	LocalFree
0040E030h	0051h	LeaveCriticalSection
0040E034h	0081h	DeleteCriticalSection
0040E038h	00DFh	GetTickCount
0040E03Ch	005Fh	TerminateThread
0040E040h	005Bh	GetExitCodeThread
0040E044h	008Eh	WaitForMultipleObjects
0040E048h	003Bh	CompareStringW
0040E04Ch	003Ah	CompareStringA
0040E050h	00E9h	GetVersionExA
0040E054h	007Fh	GetModuleHandleA
0040E058h	00A0h	GetProcAddress
0040E05Ch	0098h	EnterCriticalSection
0040E060h	0045h	LCMapStringW
0040E064h	0044h	LCMapStringA
0040E068h	00B5h	ReadFile
0040E06Ch	0037h	SetStdHandle
0040E070h	0052h	LoadLibraryA
0040E074h	0093h	GetOEMCP
0040E078h	00FDh	GetACP
0040E07Ch	0004h	GetCPInfo
0040E080h	0030h	IsBadCodePtr
0040E084h	0033h	IsBadReadPtr

Library description: Windows Base API Client DLL

Figure 38: Using PE Explorer



d1f3b9372a6be9c02430b6e4526202974179a674ce94fe22028d7212ae6be9e7 - PID: 3496 - Module: ntdll.dll - Thread: Main Thread 5940 - x32dbg
File View Debug Tracing Plugins Favourites Options Help Oct 31 2021 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
Hide FPU
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct
Default (stdcall) 5 □ Unlocked
Default

```
777CBB58  65:74 5F           je ntdll.777CBBBD
777CBB5E  73 00              jae ntdll.777CBB60
777CBB60  5F                 pop edi
777CBB61  73 74              jae ntdll.777CBBD7
777CBB63  72 73              jb ntdll.777CBBD8
777CBB65  65:74 5F           je ntdll.777CBBC7
777CBB68  73 00              jae ntdll.777CBB6A
777CBB6A  5F                 pop edi
777CBB6B  73 74              jae ntdll.777CBBE1
777CBB6D  72 75              jb ntdll.777CBBE4
777CBB6F  70 72              jo ntdll.777CBBE3
777CBB71  005F 73            add byte ptr ds:[edi+73],bl
777CBB74  74 72              je ntdll.777CBBE8
777CBB76  75 70              jne ntdll.777CBBE8
777CBB78  72 5F              jb ntdll.777CBBD9
777CBB7A  73 00              jae ntdll.777CBB7C
777CBB7C  5F                 pop edi
777CBB7D  73 77              jae ntdll.777CBBF6
777CBB7F  70 72              jo ntdll.777CBBF3
777CBB81  696E 74 66005F75   imul ebp,dword ptr ds:[esi+74],755F0066
777CBB88  6936 34746F61      imul esi,dword ptr ds:[esi],616F7434
777CBB8E  005F 75            add byte ptr ds:[edi+75],bl
777CBB91  6936 34746F61      imul esi,dword ptr ds:[esi],616F7434
777CBB97  5F                 pop edi
777CBB98  73 00              jae ntdll.777CBB9A
777CBB9A  5F                 pop edi
777CBB9B  75 69              jne ntdll.777CBC06
777CBB9D  36:34 74           xor al,74
777CBBA0  6F                 outsd
777CBBA1  77 00              ja ntdll.777CBBA3
777CBBA3  5F                 pop edi
777CBBA4  75 69              jne ntdll.777CBC0F
777CBBA6  36:34 74           xor al,74
777CBBA9  6F                 outsd
777CBBAA  77 5F              ja ntdll.777CBC0B
777CBBAC  73 00              jae ntdll.777CBBAE
777CBBAE  5F                 pop edi
777CBBAF  75 6C              jne ntdll.777CBC1D
777CBBB1  74 6F              je ntdll.777CBC22
777CBBB3  61                 popad
777CBBB4  005F 75            add byte ptr ds:[edi+75],bl
777CBBB7  6C                 insb
777CBBB8  74 6F              je ntdll.777CBC29

Jump is not taken
ntdll.777CBBBD

.text:777CBB58 ntdll.dll:$3BB58 #3AF58
```

```
EAX   00000000
EBX   00000000
ECX   00000000
EDX   00000000
EBP   00000000
ESP   00000000
ESI   3020656A
EDI   37373778

EIP   42424243

EFLAGS   00000044
ZF 0  PF BF  AF EE
OF 10 SF A9  DF 77
CF D8 TF C   IF 7D

LastError  0378E3D0 (�([sr)
LastStatus 00EEC958 (P��┐)

GS 0000  FS 0000
ES 0000  DS 0000
CS 0000  SS 0000

ST(0) 50C402E9728000000010 x87r7 Unknown invalid
ST(1) 001002E9728000000000 x87r0 Unknown invalid
ST(2) 000300000002072C7490 x87r1 Nonzero invalid
ST(3) 00010000000000000018 x87r2 Unknown invalid
ST(4) 0914072C73A001200914 x87r3 Unknown invalid
ST(5) 3330072C73A004DC2380 x87r4 Nonzero invalid
ST(6) 0000072C73A001205DC8 x87r5 Nonzero 1.884259
ST(7) ED4300EEBFF800EEBFF0 x87r6 Nonzero invalid

1: [esp+4] ??? ???
2: [esp+8] ??? ???
3: [esp+C] ??? ???
4: [esp+10] ??? ???
5: [esp+14] ??? ???
```

```
Address   Hex                                              ASCII
00400000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
00400010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ,.......@.......
00400020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00400030  00 00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00  ............è...
00400040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
00400050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
00400060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
00400070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
00400080  2C 01 25 7C 68 60 4B 2F 68 60 4B 2F 68 60 4B 2F  ,.%|h`K/h`K/h`K/
00400090  EB 7C 45 2F 7B 60 4B 2F 5E 46 41 2F 3E 60 4B 2F  ë|E/{`K/^FA/>`K/
004000A0  08 68 07 2F 69 60 4B 2F 08 68 06 2F 6F 60 4B 2F  .h./i`K/.h./o`K/
004000B0  4F A6 30 2F 6C 60 4B 2F AB 6F 16 2F 61 60 4B 2F  O¦0/l`K/«o./a`K/
004000C0  68 60 4A 2F 1B 60 4B 2F 5E 46 40 2F 79 60 4B 2F  h`J/.`K/^F@/y`K/
004000D0  52 69 63 68 68 60 4B 2F 00 00 00 00 00 00 00 00  Richh`K/........
004000E0  00 00 00 00 00 00 00 00 50 45 00 00 4C 01 04 00  ........PE..L...
004000F0  5F B7 B6 56 00 00 00 00 00 00 00 00 E0 00 0F 01  _·¶V........à...
00400100  0B 01 06 00 00 D0 00 00 00 60 02 00 00 00 00 00  .....Ð...`......
```

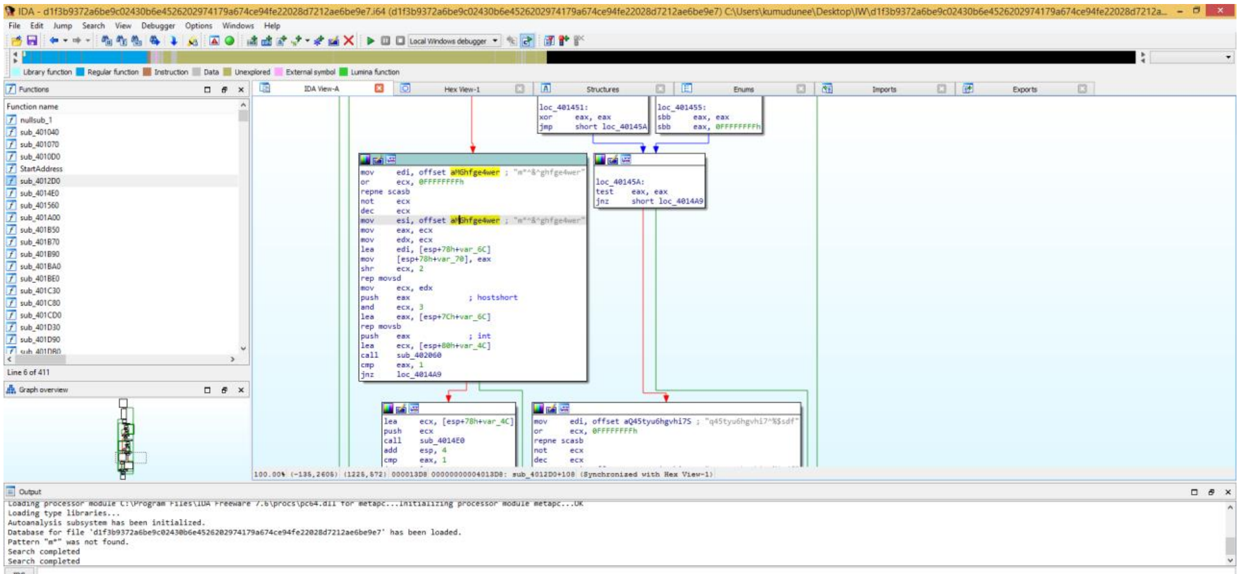
```
0018F9E4  0018FA14  ""*+"
0018F9E8  777E6E81  return to ntdll.777E6E81 from ntdll.777D9810
0018F9EC  00000001
0018F9F0  75690000  advapi32.75690000
0018F9F4  00000000
0018F9F8  00000000
0018F9FC  0018FA0C  &"PE"
0018FA00  75690000  advapi32.75690000
0018FA04  00000030
0018FA08  756900E8  advapi32.756900E8
0018FA0C  756900E8  advapi32.756900E8
0018FA10  75690000  advapi32.75690000
0018FA14  00282A88
0018FA18  00000000
0018FA1C  777CC4FC  return to ntdll.777CC4FC from ???
0018FA20  777E002B  ntdll.777E002B
0018FA24  FFFF0053
0018FA28  0018002B
0018FA2C  0018002B
```

Command: Commands are comma separated (like assembly instructions): mov eax, ebx

Paused ntdll.dll: 777CC06C -> 777CC06E (0x00000003 bytes)

Time Wasted Debugging: 0:03:14:09

Figure 39: Using x32 dgb



IDA - d1f3b9372a6be9c02430b6e4526202974179a674ce94fe22028d7212ae6be9e7.i64 (d1f3b9372a6be9c02430b6e4526202974179a674ce94fe22028d7212ae6be9e7) C:\Users\kumudunee\Desktop\IW\d1f3b9372a6be9c02430b6e4526202974179a674ce94fe22028d7212a...

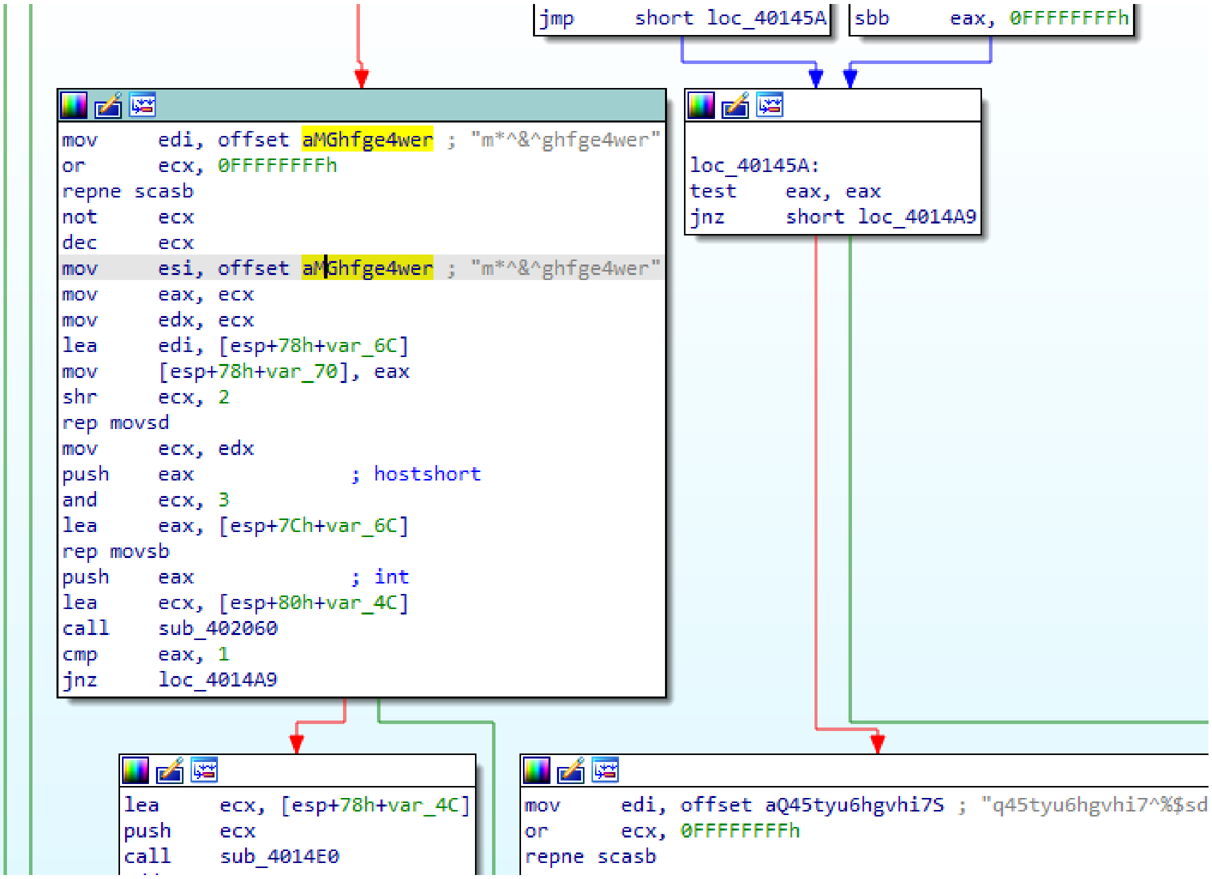
```
Function name
nullsub_1
sub_401040
sub_401070
sub_4010D0
StartAddress
sub_4012D0
sub_4014E0
sub_401560
sub_401A00
sub_401B50
sub_401B70
sub_401B90
sub_401BA0
sub_401BE0
sub_401C30
sub_401C80
sub_401CD0
sub_401D30
sub_401D90
sub_401DB0
Line 6 of 411
```

```
loc_401451:
xor     eax, eax
jmp     short loc_40145A

loc_401455:
sbb     eax, eax
sbb     eax, 0FFFFFFFFh

mov     edi, offset aMGhfge4wer ; "m*^&^ghfge4wer"
or      ecx, 0FFFFFFFFh
repne scasb
not     ecx
dec     ecx
mov     esi, offset aMGhfge4wer ; "m*^&^ghfge4wer"
mov     eax, ecx
mov     edx, ecx
lea     edi, [esp+78h+var_6C]
mov     [esp+78h+var_70], eax
shr     ecx, 2
rep movsd
mov     ecx, edx
push    eax             ; hostshort
and     ecx, 3
lea     eax, [esp+7Ch+var_6C]
rep movsb
push    eax             ; int
lea     ecx, [esp+80h+var_4C]
call    sub_402060
cmp     eax, 1
jnz     loc_4014A9

loc_40145A:
test    eax, eax
jnz     short loc_4014A9

lea     ecx, [esp+78h+var_4C]
push    ecx
call    sub_4014E0
add     esp, 4
cmp     eax, 1

mov     edi, offset aQ45tyu6hgvhi7S ; "q45tyu6hgvhi7^%$sdf"
or      ecx, 0FFFFFFFFh
repne scasb
not     ecx
dec     ecx
```

```
100.00% (-135,2605) (1225,572) 000013D8 00000000004013D8: sub_4012D0+108 (Synchronized with Hex View-1)
```

```
Loading processor module C:\Program Files\IDA Freeware 7.6\procs\pc64.dll for metapc...Initializing processor module metapc...OK
Loading type libraries...
Autoanalysis subsystem has been initialized.
Database for file 'd1f3b9372a6be9c02430b6e4526202974179a674ce94fe22028d7212ae6be9e7' has been loaded.
Pattern "m*" was not found.
Search completed
Search completed
```

Figure 40: Using IDA



```
jmp     short loc_40145A
sbb     eax, 0FFFFFFFFh

mov     edi, offset aMGhfge4wer ; "m*^&^ghfge4wer"
or      ecx, 0FFFFFFFFh
repne scasb
not     ecx
dec     ecx
mov     esi, offset aMGhfge4wer ; "m*^&^ghfge4wer"
mov     eax, ecx
mov     edx, ecx
lea     edi, [esp+78h+var_6C]
mov     [esp+78h+var_70], eax
shr     ecx, 2
rep movsd
mov     ecx, edx
push    eax             ; hostshort
and     ecx, 3
lea     eax, [esp+7Ch+var_6C]
rep movsb
push    eax             ; int
lea     ecx, [esp+80h+var_4C]
call    sub_402060
cmp     eax, 1
jnz     loc_4014A9

loc_40145A:
test    eax, eax
jnz     short loc_4014A9

lea     ecx, [esp+78h+var_4C]
push    ecx
call    sub_4014E0

mov     edi, offset aQ45tyu6hgvhi7S ; "q45tyu6hgvhi7^%$sd
or      ecx, 0FFFFFFFFh
repne scasb
```

Figure 41: Malware is checking to see if the command "m&ghfge4wer" was received from the proxy target.*

GLOSSARY

Table 3: Glossary

HxD	The software which is used to view and modify binary files.
HashCalc	A quick and simple generator for calculating message digests, checksums, and HMACs as well as text and hex strings.
PE Studio	A free tool which helps the user to conduct an initial malware evaluation without affection the system or analyzing the code.
PdfStreamDumper	A tool which is used to analyze malicious PDFs.
Exeinfo PE	This tool allows the user to verify the executable file and inspect it's properties.
X32 dbg	It is a debugger which compatible with 32 bits.
X64 dbg	It is a debugger compatible with 64 bits.
IDA Pro	This program is well-known within malware investigators, reverse engineers, and vulnerability testers. This allows for interactive disassembly.
VirusTotal	Malicious file can be submitted and verified using a variety of anti-virus tools, using the results indicating whether the signature is present. For the scanning process URLs can also be included.
Any.run	It can be defined as a malware analyzing sandbox.

Virtual Machine	Virtual machines enable users to execute an os in an application window on ones desktop that acts like a full-fledged pc.
PE Explorer	This application, like PE View, has functionality like the ability to unpack folders packaged by malware packers like UPX and Ns Packs.
PEiD	A program that assists in the identification of complicated malwares. And it uses a signature-based identification method with almost 600 malware fingerprints.
Hybrid Analysis	A sophisticated security program that analyzes uploaded malware files and the URLs. It necessitates a more in-depth understanding of windows and programing languages.

SUMMARY

This malware analysis report for stark industries has illustrated the many kinds of tools and techniques for analyzing a specific threat. In this brief study, we provided a technical description of three kinds of malwares, as well as additional functionality added to the malware intensify the damage it inflicts on the businesses the malware target. The malwares identified by Stark Industries' security team require fast action to prevent massive financial losses and reputational damage.

We strongly advise that the controls be installed in the following order:

Document Management System -

Install the latest Power Systems firmware (version FW920.30) to solve the CVE-2018-12384 Common Vulnerabilities and Exposures vulnerability, as well as the McAfee NSP intrusion prevention system. Immediate action is required.

Work Force Management System –

Need to be updated with the new versions supplied by the vendor. Immediate actions are not required.

REFERENCE

[1] Stark Industries - https://marvel-movies.fandom.com/wiki/Stark_Industries

[2] Stark Industries - https://marvelcinematicuniverse.fandom.com/wiki/Stark_Industries

[3] Stark Tower - https://en.wikipedia.org/wiki/Stark_Tower

[4] https://patchlinks.com/ardamax-keylogger-crack/

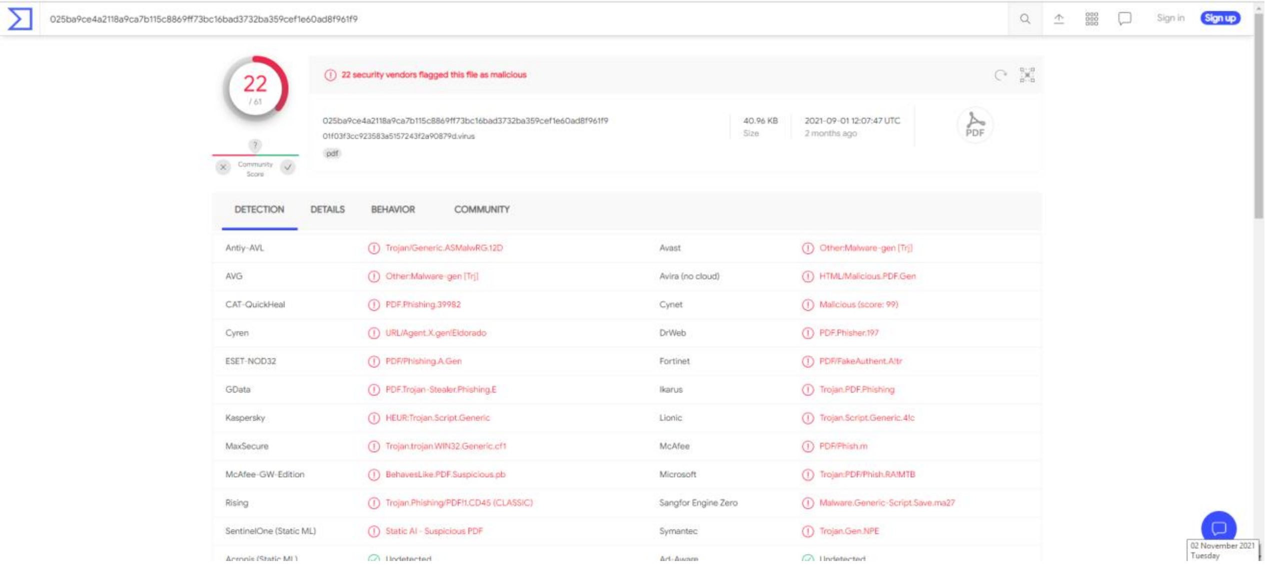
[5] Bhojani, Nirav. (2014). Malware Analysis. 10.13140/2.1.4750.6889.

[6] Datta, Arkajit & Anil Kumar, Kakelli & D, Aju. (2021). An Emerging Malware Analysis Techniques and Tools: A Comparative Analysis.

APPENDICES

Appendix A

025ba9ce4a2118a9ca7b115c8869ff73bc16bad3732ba359cef1e60ad8f961f9



025ba9ce4a2118a9ca7b115c8869ff73bc16bad3732ba359cef1e60ad8f961f9

22 security vendors flagged this file as malicious

025ba9ce4a2118a9ca7b115c8869ff73bc16bad3732ba359cef1e60ad8f961f9
01f03f3cc923583a5157243f2a90879d.virus
pdf

40.96 KB
Size

2021-09-01 12:07:47 UTC
2 months ago

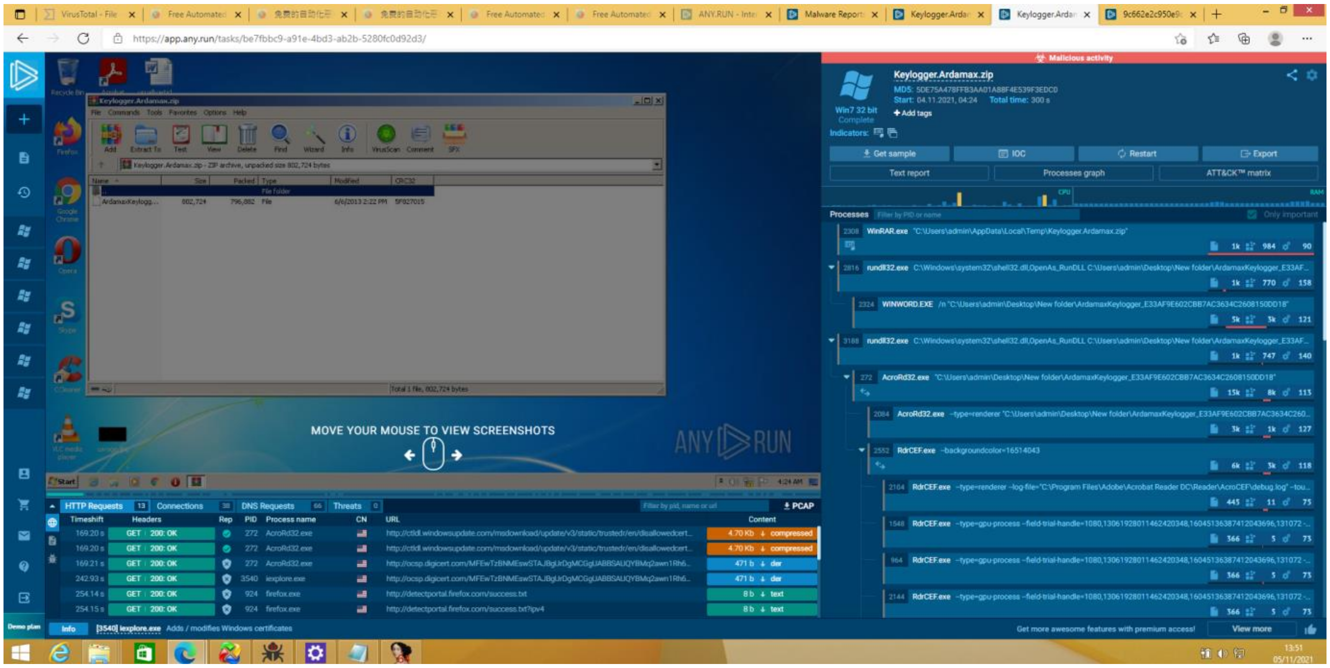
DETECTION | DETAILS | BEHAVIOR | COMMUNITY

Antiy-AVL	Trojan/Generic.ASMalwRG.12D	Avast	Other:Malware-gen [Trj]
AVG	Other:Malware-gen [Trj]	Avira (no cloud)	HTML/Malicious.PDF.Gen
CAT-QuickHeal	PDF.Phishing.39982	Cynet	Malicious (score: 99)
Cyren	URL/Agent.X.gen!Eldorado	DrWeb	PDF.Phisher.197
ESET-NOD32	PDF/Phishing.A.Gen	Fortinet	PDF/FakeAuthent.A!tr
GData	PDF.Trojan-Stealer.Phishing.E	Ikarus	Trojan.PDF.Phishing
Kaspersky	HEUR:Trojan.Script.Generic	Lionic	Trojan.Script.Generic.4!c
MaxSecure	Trojan.trojan.WIN32.Generic.cf1	McAfee	PDF/Phish.m
McAfee-GW-Edition	BehavesLike.PDF.Suspicious.pb	Microsoft	Trojan:PDF/Phish.RA!MTB
Rising	Trojan.Phishing/PDF!1.CD45 (CLASSIC)	Sangfor Engine Zero	Malware.Generic-Script.Save.ma27
SentinelOne (Static ML)	Static AI - Suspicious PDF	Symantec	Trojan.Gen.NPE
Acronis (Static ML)	✓ Undetected	Ad-Aware	✓ Undetected

Figure 42: Virus Total Report

Appendix B

Ardamax Keylogger



https://app.any.run/tasks/be7fbbc9-a91e-4bd3-ab2b-5280fc0d92d3/

Keylogger.Ardamax.zip - ZIP archive, unpacked size 802,724 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
ArdamaxKeylogg...	802,724	796,882	File	6/6/2013 2:22 PM	5F827015

Total 1 file, 802,724 bytes

Keylogger.Ardamax.zip
MD5: 5DE75A478FFB3AA01A88F4E539F3EDCD
Start: 04.11.2021, 04:24 Total time: 300 s
+ Add tags

```
2308 WinRAR.exe "C:\Users\admin\AppData\Local\Temp\Keylogger.Ardamax.zip"        1k  984  90
2816 rundll32.exe C:\Windows\system32\shell32.dll,OpenAs_RunDLL C:\Users\admin\Desktop\New folder\ArdamaxKeylogger_E33AF...        1k  770  158
  2324 WINWORD.EXE /n "C:\Users\admin\Desktop\New folder\ArdamaxKeylogger_E33AF9E602CBB7AC3634C2608150DD18"        5k  3k  121
3188 rundll32.exe C:\Windows\system32\shell32.dll,OpenAs_RunDLL C:\Users\admin\Desktop\New folder\ArdamaxKeylogger_E33AF...        1k  747  140
  272 AcroRd32.exe "C:\Users\admin\Desktop\New folder\ArdamaxKeylogger_E33AF9E602CBB7AC3634C2608150DD18"        15k  8k  113
    2084 AcroRd32.exe --type=renderer "C:\Users\admin\Desktop\New folder\ArdamaxKeylogger_E33AF9E602CBB7AC3634C260...        3k  1k  127
    2552 RdrCEF.exe --backgroundcolor=16514043        6k  3k  118
      2104 RdrCEF.exe --type=renderer --log-file="C:\Program Files\Adobe\Acrobat Reader DC\Reader\AcroCEF\debug.log" --tou...        445  11  75
      1548 RdrCEF.exe --type=gpu-process --field-trial-handle=1080,13061928011462420348,16045136387412043696,131072 -...        366  5  73
      964 RdrCEF.exe --type=gpu-process --field-trial-handle=1080,13061928011462420348,16045136387412043696,131072 -...        366  5  73
      2144 RdrCEF.exe --type=gpu-process --field-trial-handle=1080,13061928011462420348,16045136387412043696,131072 -...        366  5  73
```

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
169.20 s	GET 200: OK	✓	272	AcroRd32.exe	🇺🇸	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcert...	4.70 Kb compressed
169.20 s	GET 200: OK	✓	272	AcroRd32.exe	🇺🇸	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcert...	4.70 Kb compressed
169.21 s	GET 200: OK	⛨	272	AcroRd32.exe	🇺🇸	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6...	471 b der
242.93 s	GET 200: OK	⛨	3540	iexplore.exe	🇺🇸	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6...	471 b der
254.14 s	GET 200: OK	⛨	924	firefox.exe	🇺🇸	http://detectportal.firefox.com/success.txt	8 b text
254.15 s	GET 200: OK	⛨	924	firefox.exe	🇺🇸	http://detectportal.firefox.com/success.txt?ipv4	8 b text

[3540] iexplore.exe Adds / modifies Windows certificates

Figure 43: Any Run report

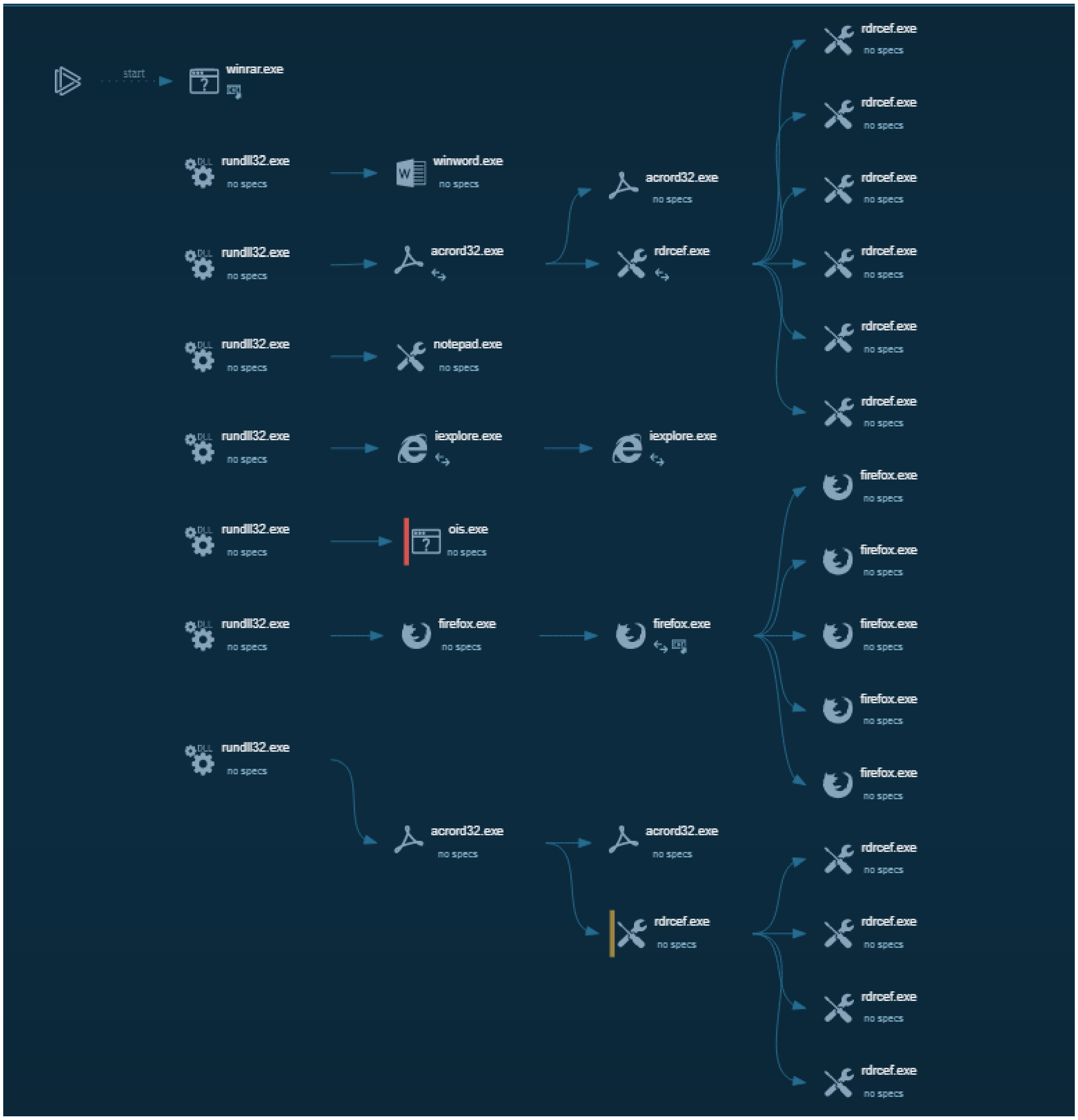
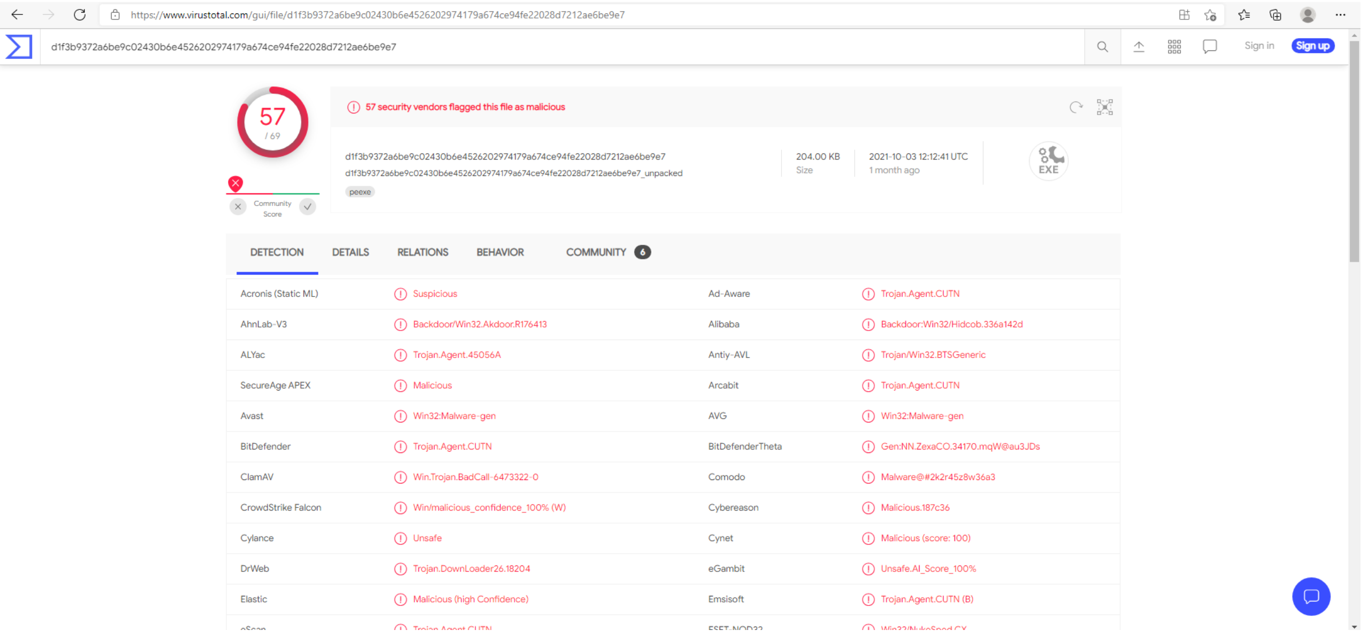


Figure 44: Process graph of keylogger

Appendix C

d1f3b9372a6be9c02430b6e4526202974179a674ce94fe22028d7212ae6be9e7



https://www.virustotal.com/gui/file/d1f3b9372a6be9c02430b6e4526202974179a674ce94fe22028d7212ae6be9e7

d1f3b9372a6be9c02430b6e4526202974179a674ce94fe22028d7212ae6be9e7

57 / 69

Community Score

57 security vendors flagged this file as malicious

d1f3b9372a6be9c02430b6e4526202974179a674ce94fe22028d7212ae6be9e7
d1f3b9372a6be9c02430b6e4526202974179a674ce94fe22028d7212ae6be9e7_unpacked
peexe

204.00 KB
Size

2021-10-03 12:12:41 UTC
1 month ago

EXE

Acronis (Static ML)	Suspicious	Ad-Aware	Trojan.Agent.CUTN
AhnLab-V3	Backdoor/Win32.Akdoor.R176413	Alibaba	Backdoor:Win32/Hidcob.336a142d
ALYac	Trojan.Agent.45056A	Antiy-AVL	Trojan/Win32.BTSGeneric
SecureAge APEX	Malicious	Arcabit	Trojan.Agent.CUTN
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
BitDefender	Trojan.Agent.CUTN	BitDefenderTheta	Gen:NN.ZexaCO.34170.mqW@au3JDs
ClamAV	Win.Trojan.BadCall-6473322-0	Comodo	Malware@#2k2r45z8w36a3
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cybereason	Malicious.187c36
Cylance	Unsafe	Cynet	Malicious (score: 100)
DrWeb	Trojan.DownLoader26.18204	eGambit	Unsafe.AI_Score_100%
Elastic	Malicious (high Confidence)	Emsisoft	Trojan.Agent.CUTN (B)
eScan	Trojan.Agent.CUTN	ESET-NOD32	Win32/NukeSped.CX

Figure 45: Virus Total report

d1f3b9372a6be9c02430b6e4526202974179a674ce94fe22028d7212ae6be9e7 - Notepad

```
MZ └    ┘    ÿÿ          @                                  è    ┌º┌     Í!  └Í!This program cannot be run in DOS mod
$         ,  %|h`K/h`K/h`K/ë|E/{`K/^FA/>`K/gh•/1`K/gh-/o`K/O¦0/1`K/«O┬/a`K/h`J/÷`K/^F®/y`K/Rîchh`K/                     PE    L
```

Figure 46: Executed Malware