ID: 532884
Sample Name: Unpoetical.exe
Cookbook: default.jbs
Time: 19:22:16
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

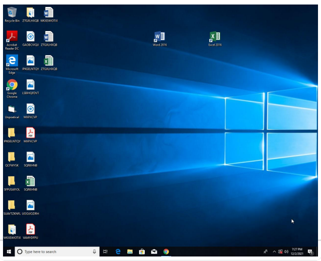
Windows Analysis Report Unpoetical.exe

Overview

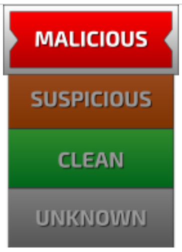
General Information

Sample Name:	Unpoetical.exe
Analysis ID:	532884
MD5:	72a83ab4f94c308.
SHA1:	541adced7fdeaab.
SHA256:	5de06140579c23..
Infos:	

Most interesting Screenshot:



Detection



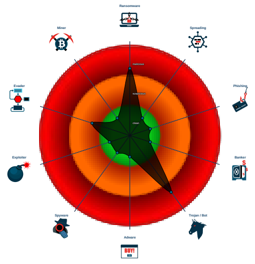
GuLoader

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Potential malicious icon found
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- PE file contains strange resources
- Contains functionality to read the PEB
- Uses code obfuscation techniques (…
- Detected potential crypto function
- PE / OLE file has an invalid certificate
- Contains functionality to call native f…

Classification



Process Tree

- **System is w10x64**
- Unpoetical.exe (PID: 7144 cmdline: "C:\Users\user\Desktop\Unpoetical.exe" MD5: 72A83AB4F94C308D77E166E299B70420)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=do"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.875035981.00000000020E0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Potential malicious icon found

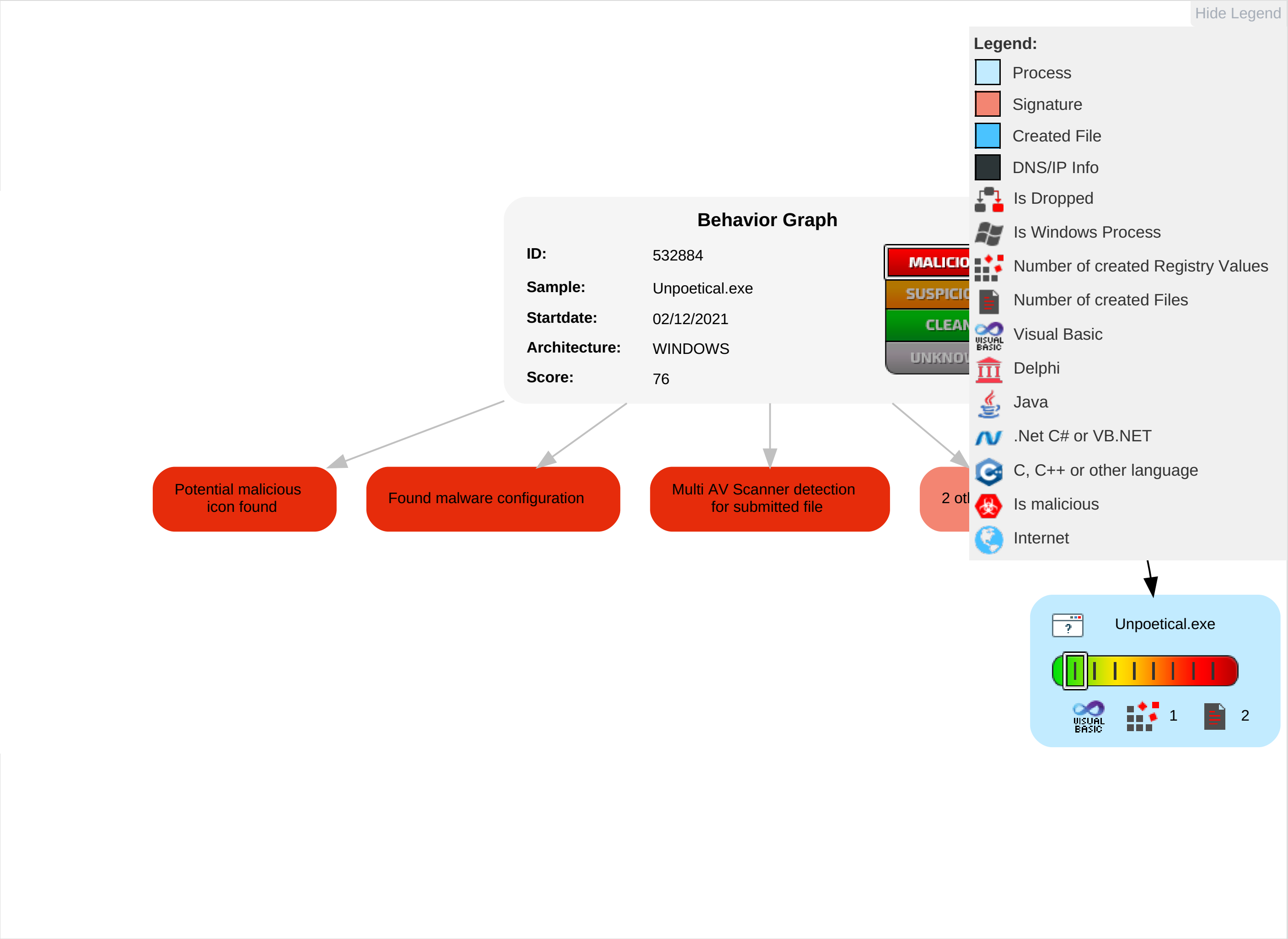
Data Obfuscation:

Yara detected GuLoader

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	In
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M Sy Pa
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	System Information Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D

Behavior Graph



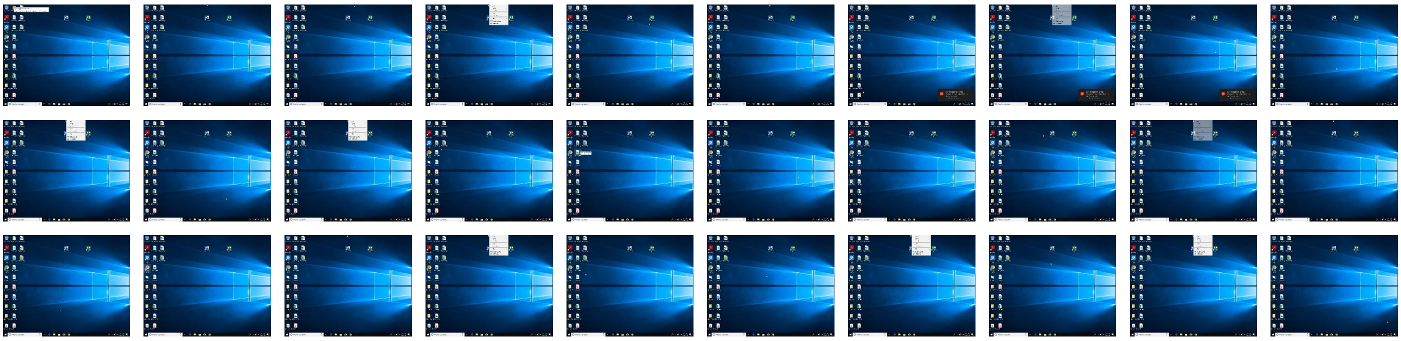
Behavior Graph

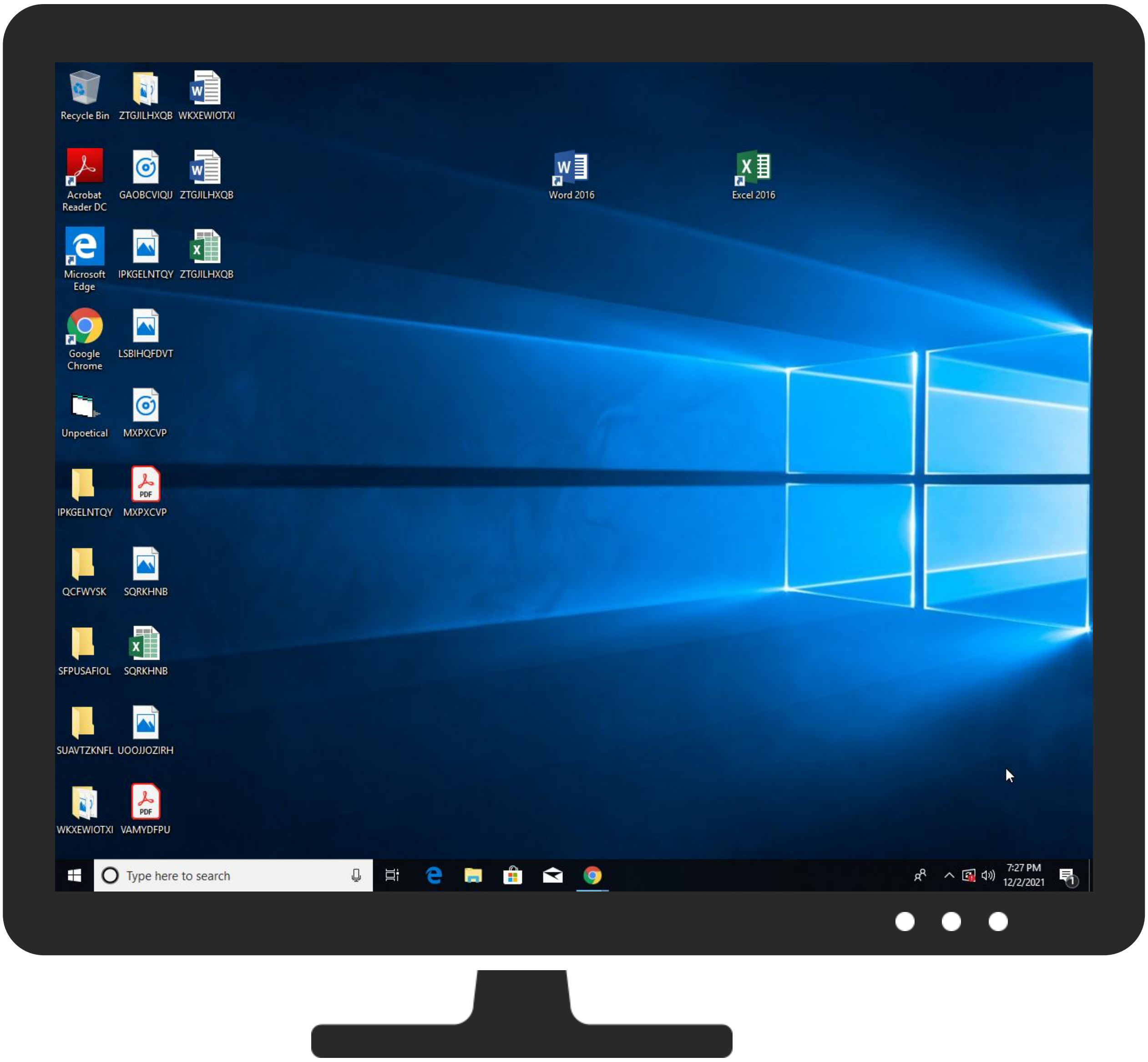
ID:	532884
Sample:	Unpoetical.exe
Startdate:	02/12/2021
Architecture:	WINDOWS
Score:	76

Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Unpoetical.exe	45%	Virustotal		Browse
Unpoetical.exe	61%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.Unpoetical.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1140082		Download File
0.2.Unpoetical.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1140082		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532884
Start date:	02.12.2021
Start time:	19:22:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Unpoetical.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.rans.troj.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 44.3% (good quality ratio 26.5%) • Quality average: 34.2% • Quality standard deviation: 30.2%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

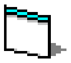
No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.202099583182856
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Unpoetical.exe
File size:	152736
MD5:	72a83ab4f94c308d77e166e299b70420
SHA1:	541adced7fdeaab8977935628ec837a9dbd69e15
SHA256:	5de06140579c23eadb8f4f353255feb83711314b0752ca4 fdfdf432d4bbc92c6
SHA512:	e4ecea7d95c76bde906d961d27841f2c54bbf5e1c11adb8 9120fea2450872cbfa1bf3f0c66d563299f2b79091174f6b 2985011b4c94621e876aa47200e42705b
SSDEEP:	1536:TrQyUE6l7U/oor5sLOQrFLeUdqz8Ts/zEn9YRXAI P6mzywp:ME6l7UQoraOQrRbMz8TKc92XNPBn
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$.......O........... ....D.......=.......Rich............PE..L.....(L..................... 0............... ....@................

File Icon



Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401888
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4C289BDE [Mon Jun 28 12:55:58 2010 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	b209c8634733456633136bfedc71877a

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=cirkusartisterne@Sunburned5.SKR, CN=sjlstilstandene, OU=Bladhandlerens2, O=CRYSTALED, L=Receptivitetens9, S=Creeping, C=FJ
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 12/1/2021 4:21:52 AM 12/1/2022 4:21:52 AM
Subject Chain	• E=cirkusartisterne@Sunburned5.SKR, CN=sjlstilstandene, OU=Bladhandlerens2, O=CRYSTALED, L=Receptivitetens9, S=Creeping, C=FJ
Version:	3
Thumbprint MD5:	5BC3698C2C97D0BE2CF19994B3762274
Thumbprint SHA-1:	91A263642EA14B669A5EDD51F5BA2FDE156D47D8
Thumbprint SHA-256:	7888FBC9BE284740E820C1A153B4CE8C0DC18EEB46FF96E29301BEEF2C8EDC46
Serial:	00

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x20b34	0x21000	False	0.365093809186	data	5.28140779308	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x22000	0x122c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x24000	0x968	0x1000	False	0.175048828125	data	2.06079043208	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
Chinese	Taiwan	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: Unpoetical.exe PID: 7144 Parent PID: 5712

General

Start time:	19:23:30
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\Unpoetical.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Unpoetical.exe"
Imagebase:	0x400000
File size:	152736 bytes
MD5 hash:	72A83AB4F94C308D77E166E299B70420
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.875035981.00000000020E0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis