ID: 532884
Sample Name: Unpoetical.exe
Cookbook: default.jbs
Time: 19:30:44
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

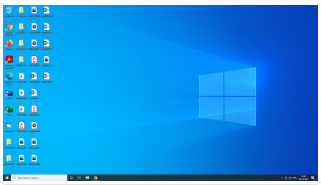
Windows Analysis Report Unpoetical.exe

Overview

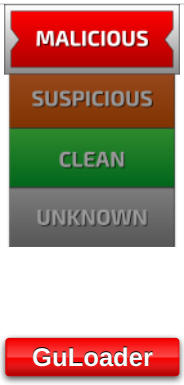
General Information

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

Most interesting Screenshot:



Detection

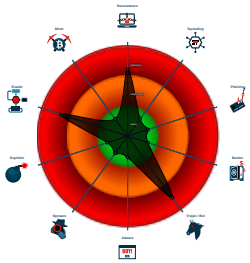


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Potential malicious icon found
- Multi AV Scanner detection for subm…
- GuLoader behavior detected
- Yara detected GuLoader
- Hides threads from debuggers
- Writes to foreign memory regions
- Tries to detect Any.run
- C2 URLs / IPs found in malware con…
- Tries to detect sandboxes and other…
- Uses 32bit PE files
- Found a high number of Window / Us…

Classification



Process Tree

- **System is w10x64native**
- Unpoetical.exe (PID: 644 cmdline: "C:\Users\user\Desktop\Unpoetical.exe" MD5: 72A83AB4F94C308D77E166E299B70420)
  - CasPol.exe (PID: 380 cmdline: "C:\Users\user\Desktop\Unpoetical.exe" MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)
    - conhost.exe (PID: 376 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

Threatname: GuLoader

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

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000000.120841224105.000000000D00000.00000040.00000001.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

Malware Analysis System Evasion:

Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Anti Debugging:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Stealing of Sensitive Information:

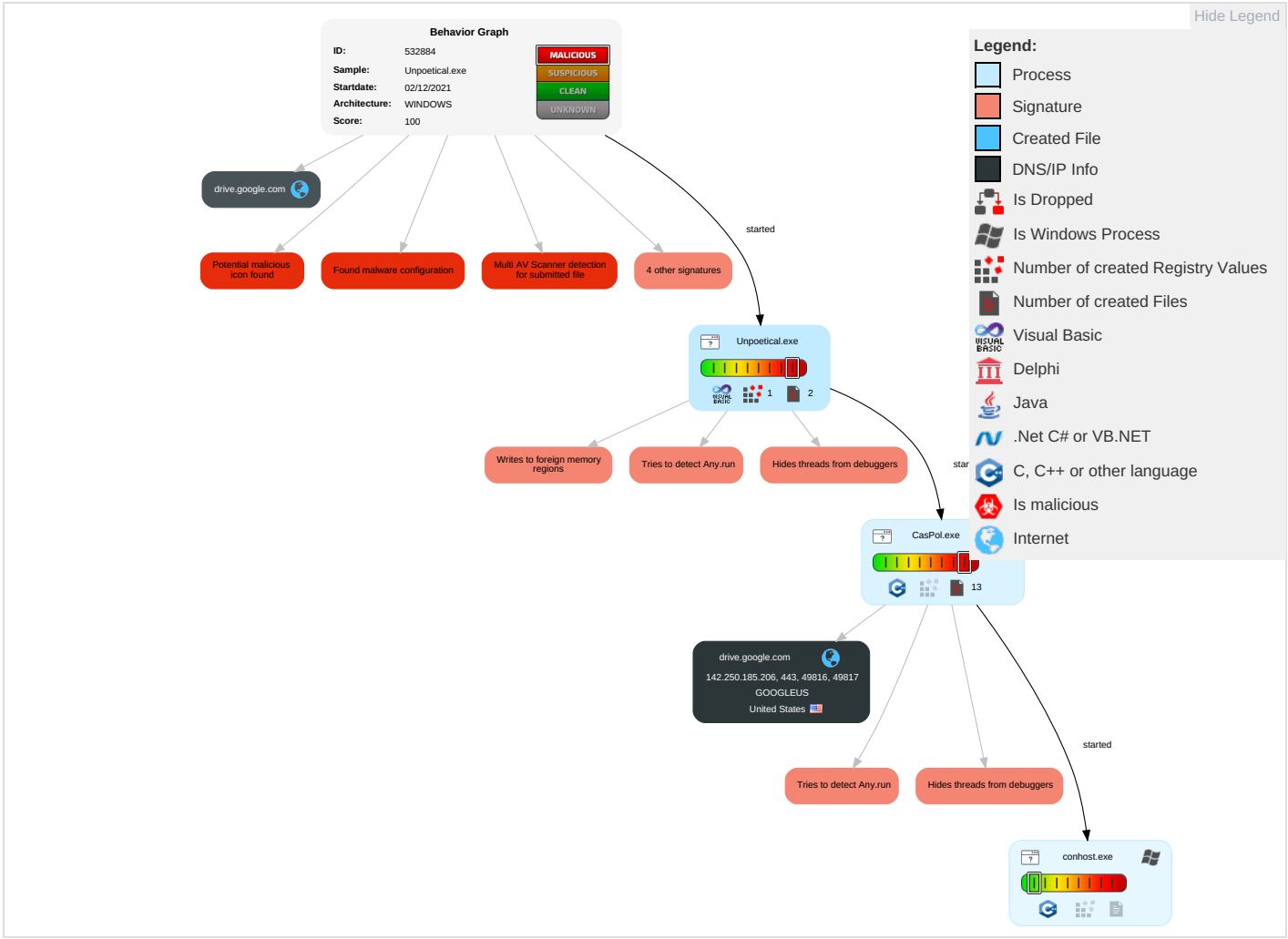
GuLoader behavior detected

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	DLL Side-Loading 1	Process Injection 1 1 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 3 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop or Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Virtualization/Sandbox Evasion 2 2	LSASS Memory	Virtualization/Sandbox Evasion 2 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1 1	Security Account Manager	Application Window Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1 2	Exploit SS7 to Track Device Location

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	DLL Side-Loading 1	NTDS	System Information Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati

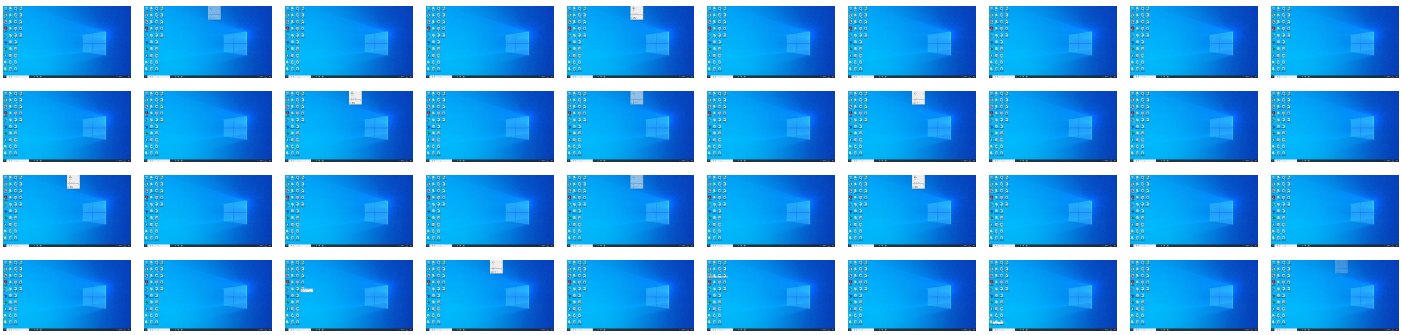
Behavior Graph



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
2.0.Unpoetical.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1140082		Download File
2.2.Unpoetical.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1140082		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://csp.withgoogle.com/csp/report-to/gse_l9ocaq	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
drive.google.com	142.250.185.206	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.185.206	drive.google.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532884
Start date:	02.12.2021
Start time:	19:30:44
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 58s
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 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	23
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:	mal100.rans.troj.evad.winEXE@4/0@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:34:20	API Interceptor	1188x Sleep call for process: CasPol.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	CTvjbMY3DK.dll	Get hash	malicious	Browse	• 142.250.185.206
	FT A75619637369.vbs	Get hash	malicious	Browse	• 142.250.185.206
	OSJlMxel05.exe	Get hash	malicious	Browse	• 142.250.185.206
	fel.com.html	Get hash	malicious	Browse	• 142.250.185.206
	S6RqSs1LsE.exe	Get hash	malicious	Browse	• 142.250.185.206
	4RXRHeZIG8.exe	Get hash	malicious	Browse	• 142.250.185.206
	kEwILWnlG5.exe	Get hash	malicious	Browse	• 142.250.185.206
	kEwILWnlG5.exe	Get hash	malicious	Browse	• 142.250.185.206
	SecuriteInfo.com.W32.AIDetect.malware2.32340.exe	Get hash	malicious	Browse	• 142.250.185.206
	mUYEdn5OC0.exe	Get hash	malicious	Browse	• 142.250.185.206
	new offers885111832.docx	Get hash	malicious	Browse	• 142.250.185.206
	_0.html	Get hash	malicious	Browse	• 142.250.185.206
	lifehacks_6582318243.docx	Get hash	malicious	Browse	• 142.250.185.206
	counter-1248368226.xls	Get hash	malicious	Browse	• 142.250.185.206
	counter-1248368226.xls	Get hash	malicious	Browse	• 142.250.185.206
	ukmxWblFcs.exe	Get hash	malicious	Browse	• 142.250.185.206
	Narudzba.0953635637.PDF.exe	Get hash	malicious	Browse	• 142.250.185.206
	Orden de compra.exe	Get hash	malicious	Browse	• 142.250.185.206
	EmployeeAssessment.html	Get hash	malicious	Browse	• 142.250.185.206
	bUSzS84fr4.dll	Get hash	malicious	Browse	• 142.250.185.206

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:	5de06140579c23eadb8f4f353255feb83711314b0752ca4fdfdf432d4bbc92c6
SHA512:	e4ecea7d95c76bde906d961d27841f2c54bbf5e1c11adb89120fea2450872cbfa1bf3f0c66d563299f2b79091174f6b2985011b4c94621e876aa47200e42705b
SSDEEP:	1536:TrQyUE6l7U/oor5sLOQrFLeUdqz8Ts/zEn9YRXAIP6mzywp:ME6l7UQoraOQrRbMz8TKc92XNPBn
File Content Preview:	MZ.....@.....!..L.!This 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

General

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	• 01/12/2021 12:21:52 01/12/2022 12:21:52
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

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 19:34:20.947186947 CET	192.168.11.20	1.1.1.1	0x9f36	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 19:34:20.956871986 CET	1.1.1.1	192.168.11.20	0x9f36	No error (0)	drive.google.com		142.250.185.206	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Unpoetical.exe PID: 644 Parent PID: 7732

General

Start time:	19:32:34
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
Reputation:	low

File Activities

Show Windows behavior

File Created

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: CasPol.exe PID: 380 Parent PID: 644

General

Start time:	19:32:49
Start date:	02/12/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe

Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Unpoetical.exe"
Imagebase:	0x900000
File size:	106496 bytes
MD5 hash:	7BAE06CBE364BB42B8C34FCFB90E3EBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000004.00000000.120841224105.0000000000D00000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

File Created

Analysis Process: conhost.exe PID: 376 Parent PID: 380

General

Start time:	19:32:49
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff707230000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Disassembly

Code Analysis