ID: 531747
Sample Name: draft_inv dec21.exe
Cookbook: default.jbs
Time: 10:21:21
Date: 01/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

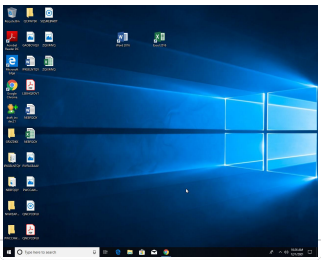
Windows Analysis Report draft_inv dec21.exe

Overview

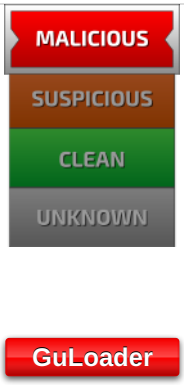
General Information

Sample Name:	draft_inv dec21.exe
Analysis ID:	531747
MD5:	89a584acaeb2f9e.
SHA1:	263ff0b238d57cf…
SHA256:	59ae017767f6a56.
Infos:	

Most interesting Screenshot:



Detection

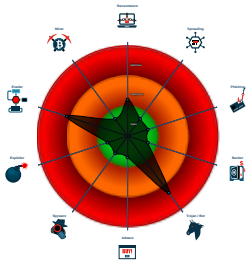


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Found potential dummy code loops (…
- Uses 32bit PE files
- Sample file is different than original …
- PE file contains strange resources
- Contains functionality to read the PEB
- Uses code obfuscation techniques (…
- Detected potential crypto function
- Monitors certain registry keys / valu…

Classification



Process Tree

- **System is w10x64**
- draft_inv dec21.exe (PID: 6976 cmdline: "C:\Users\user\Desktop\draft_inv dec21.exe" MD5: 89A584ACAEB2F9E8BAF46714EB7D3550)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://statuswar.info/GHDFR/bin_rOlFDOAa61.bin"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.1200998777.0000000002CA0000.00000040.00000001.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

Data Obfuscation:

Yara detected GuLoader

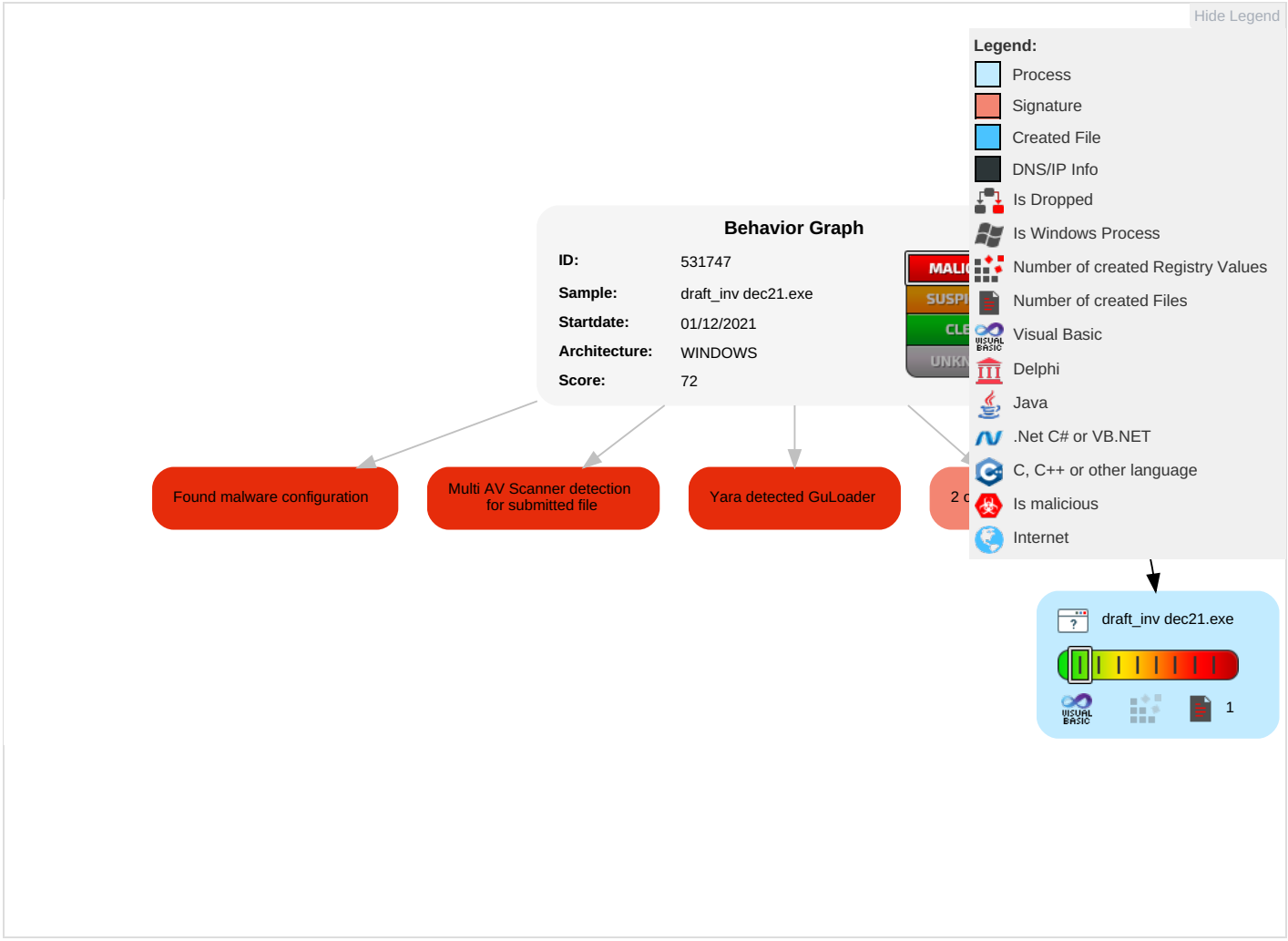
Anti Debugging:

Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	R T W A
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	R W W A
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Virtualization/Sandbox Evasion 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	O D C B
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Information Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

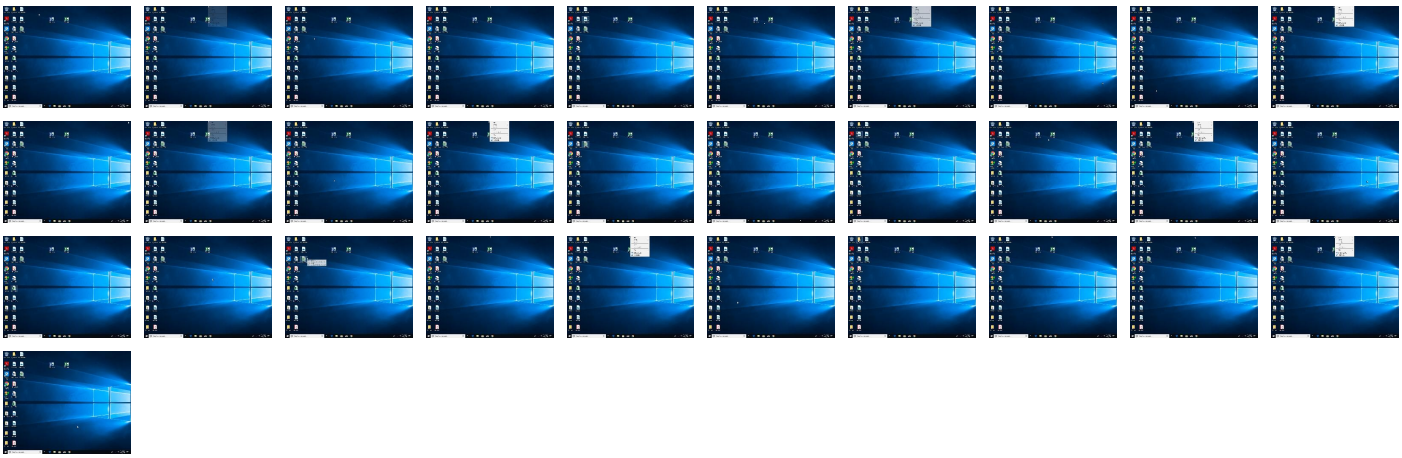
Behavior Graph



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
draft_inv dec21.exe	20%	Metadefender		Browse
draft_inv dec21.exe	18%	ReversingLabs	Win32.Trojan.GuLoader	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://statuswar.info/GHDFR/bin_rOlFDOAa61.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://statuswar.info/GHDFR/bin_rOlFDOAa61.bin	true	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	531747
Start date:	01.12.2021
Start time:	10:21:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	draft_inv dec21.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:	13
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:	mal72.troj.evad.winEXE@1/1@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 33.8% (good quality ratio 11.7%) • Quality average: 20.8% • Quality standard deviation: 32.3%
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

C:\Users\user\AppData\Local\Temp\~DF91089FF9233BF8CB.TMP	
Process:	C:\Users\user\Desktop\draft_inv dec21.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.6374754921163319
Encrypted:	false
SSDEEP:	12:rl3lKFQCb77z4cl9ZgFLGVwtn4+jbxO/37X6XMRZnAX3CqFZlUoz:r8JloFP1jbxOfLhlAX3CAZlj
MD5:	26F4DF069A76EC44D3497157CFC2A7FF
SHA1:	4FFDEDEB83278CA75D0AAE246C6451342C6A763F
SHA-256:	B83265C7FB0E0239E55E32B503B9D73689FC800BCF26E8670284B2BCF805841B
SHA-512:	161E06993EE630FC83DD0A17D0B2370FF69173EAD77E385A4396E5E921C2037A2547FBEF7CD3B9E605ABE1960C928C158CB9D6C6479A4BD232F5790574AD029
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.94335884500492
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:	draft_inv dec21.exe
File size:	135168

General

MD5:	89a584acaeb2f9e8baf46714eb7d3550
SHA1:	263ff0b238d57cfc30492f8801530b9986dcae38
SHA256:	59ae017767f6a56eba79abdad1343cba3643744f4668b320c30fda283abdedf2
SHA512:	299b531915221fd0003e2f526c7ac529d948524a065dde767c4d638f4121cd62d3a70e67bca3c013baf79cf98f67d9f84b5097327dfdba2d4ffd4b10dc571241
SSDEEP:	3072:9U8lySFndx820q1KtKiNaoLbi/gRN1bmwADH:9UkSFd22j1KvfEgHJO
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7b..s...s...s.....r...<!..v...E%..r...Richs.....PE..L...W.aL.....0.....h.....@

File Icon

Icon Hash:	98989c98b8787c00

Static PE Info

General

Entrypoint:	0x401668
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4C61B357 [Tue Aug 10 20:15:19 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:	a7de590cc5b951bdfc15c3f8afbf7326

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1d570	0x1e000	False	0.558390299479	data	6.27464824978	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1f000	0x1a18	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x21000	0x750	0x1000	False	0.18310546875	data	1.93536831113	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

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: draft_inv dec21.exe PID: 6976 Parent PID: 1556

General

Start time:	10:22:22
Start date:	01/12/2021
Path:	C:\Users\user\Desktop\draft_inv dec21.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\draft_inv dec21.exe"
Imagebase:	0x400000
File size:	135168 bytes
MD5 hash:	89A584ACAEB2F9E8BAF46714EB7D3550
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.1200998777.0000000002CA0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis