ID: 530423
Sample Name: Scanned Payment Copy00024.scr.exe
Cookbook: default.jbs
Time: 15:42:52
Date: 29/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

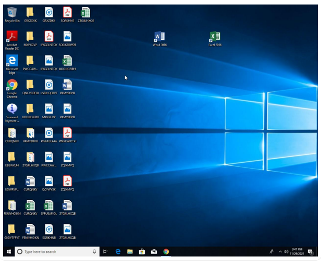
Windows Analysis Report Scanned Payment Copy00024…

Overview

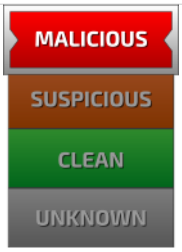
General Information

Sample Name:	Scanned Payment Copy00024.scr.exe
Analysis ID:	530423
MD5:	9ebaab853c410a..
SHA1:	67c221c5f132982..
SHA256:	b24869692ba4efa..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



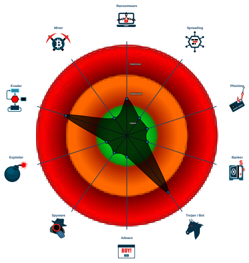
GuLoader

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Initial sample is a PE file and has a …
- Tries to detect virtualization through…
- Executable has a suspicious name (…
- C2 URLs / IPs found in malware con…
- 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
- Sample execution stops while proce…

Classification



Process Tree

- **System is w10x64**
- Scanned Payment Copy00024.scr.exe (PID: 7052 cmdline: "C:\Users\user\Desktop\Scanned Payment Copy00024.scr.exe" MD5: 9EBAAB853C410A3C6EF16ECF45739E8B)
  - conhost.exe (PID: 7116 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?expo"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.870438121.0000000002210000.00000040.00000001.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:

Initial sample is a PE file and has a suspicious name

Executable has a suspicious name (potential lure to open the executable)

Data Obfuscation:

Yara detected GuLoader

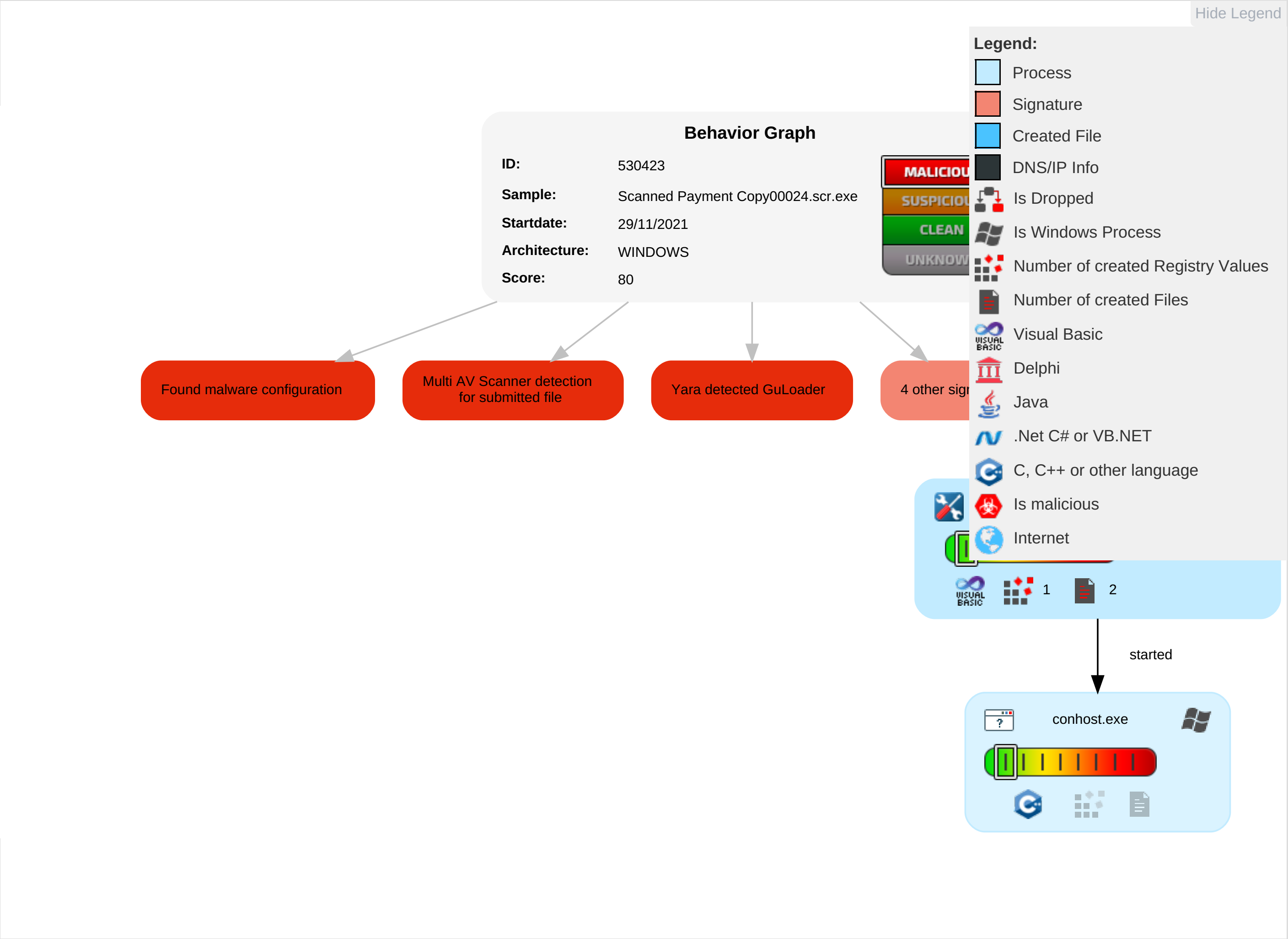
Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

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 2	Process Injection 2	OS Credential Dumping	Security Software Discovery 1 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 S P
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information 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 L
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	System Information Discovery 1 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: 530423

Sample: Scanned Payment Copy00024.scr.exe

Startdate: 29/11/2021

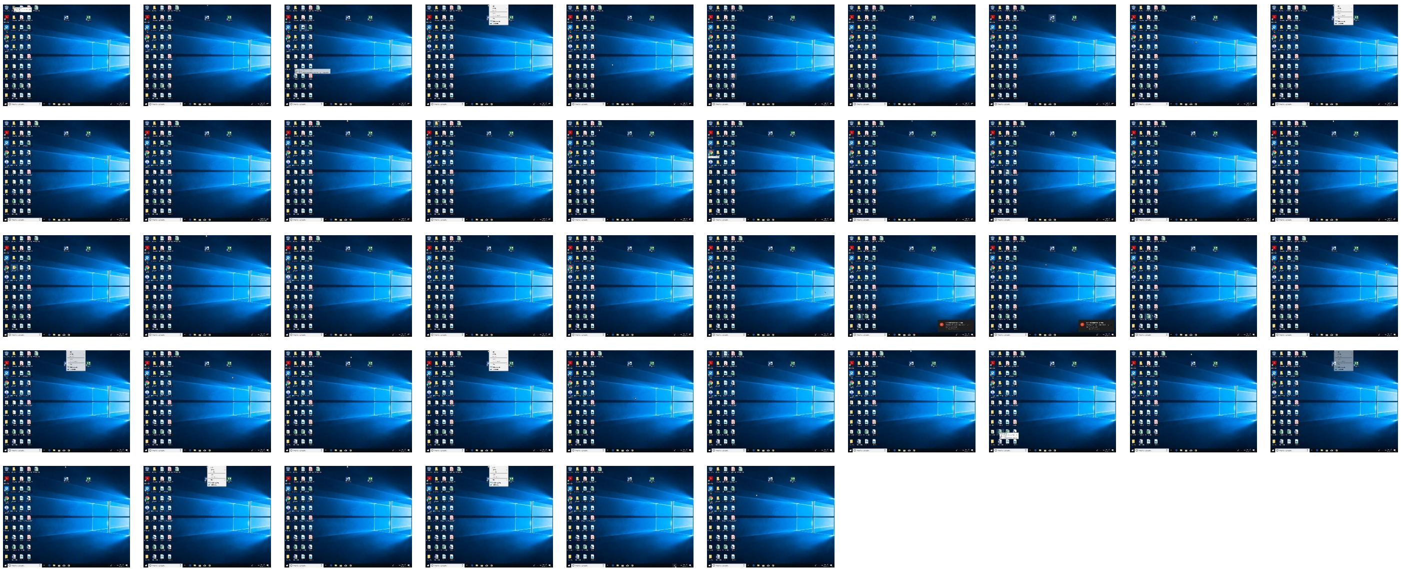
Architecture: WINDOWS

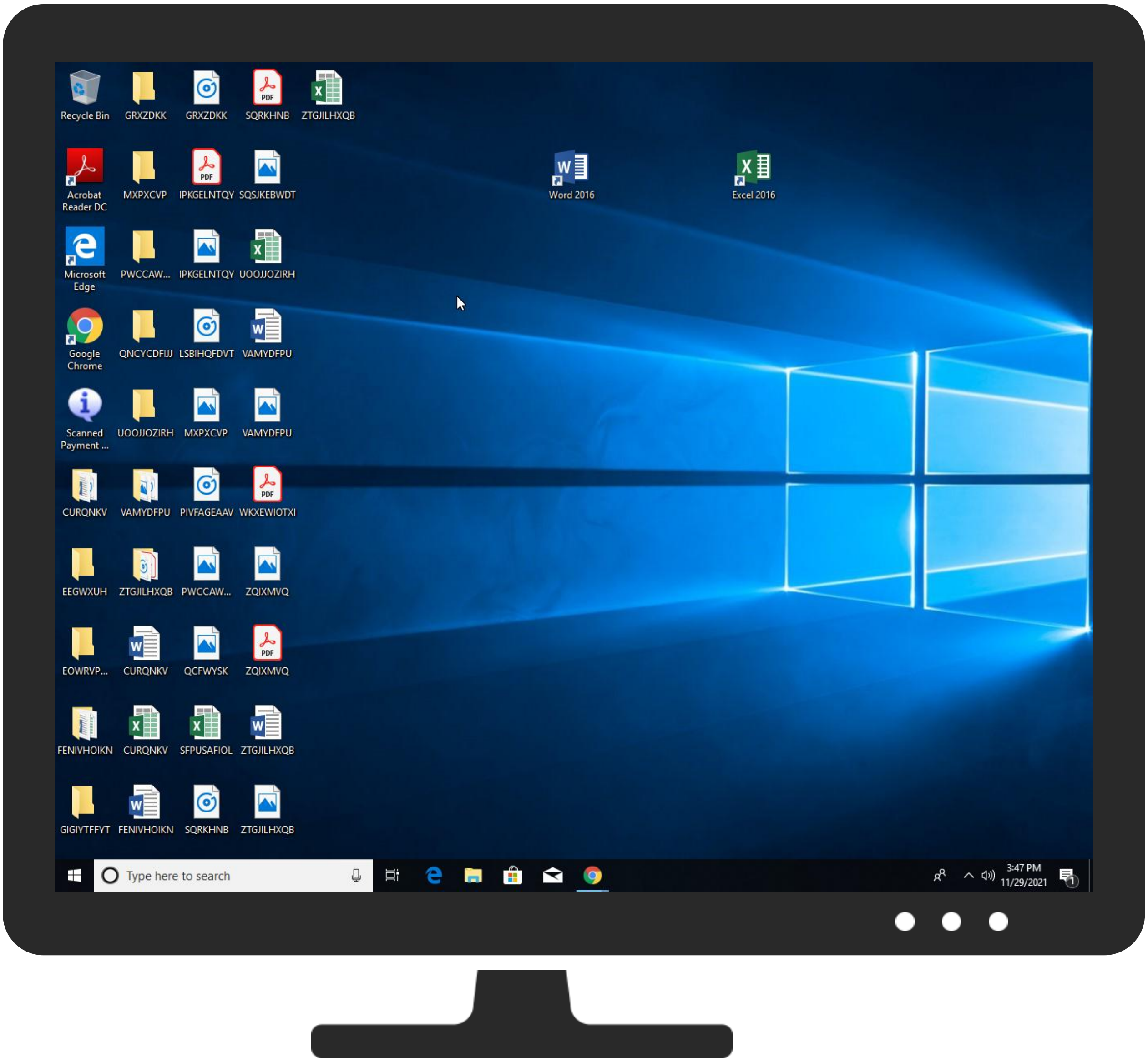
Score: 80

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
Scanned Payment Copy00024.scr.exe	33%	ReversingLabs	Win32.Worm.GenericML	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

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:	530423
Start date:	29.11.2021
Start time:	15:42:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Scanned Payment Copy00024.scr.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:	22
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:	mal80.troj.evad.winEXE@2/1@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 16.9% (good quality ratio 11.1%) • Quality average: 35.1% • Quality standard deviation: 32%
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\~DF25FB0965A4D91BCD.TMP	
Process:	C:\Users\user\Desktop\Scanned Payment Copy00024.scr.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.9866006611106688
Encrypted:	false
SSDEEP:	96:jWpahLKAycVxc4LlvnffSIPW0wLzzj1ylDHn3Rs:KMhLKCxV5vnffI0wIdHBs
MD5:	A256BBA112F7FA34FE9E19ED07D0DF83
SHA1:	3E86ADD7C0890C55E8F22334A3E26134D7AB1EE8
SHA-256:	AB9F6744C55428A62F4696BC1779409A30420D0983EDD5536A0D280DF5EE7FE0
SHA-512:	9E762DFE82611778602E8BF19439E48AF7278D3D9399FF44666EB8A196206F4B1B50B9B623710B138BD7A7E9C1E0A05BE85CE6FB7B0F208C9664669297C416EA
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....................>... ....

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.028365197002993
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:	Scanned Payment Copy00024.scr.exe
File size:	155648
MD5:	9ebaab853c410a3c6ef16ecf45739e8b
SHA1:	67c221c5f1329829d7a808791dc030bf1288d2d7
SHA256:	b24869692ba4efa8bb957cb2334ac798b570277c038db867db5a177a0e9a54ec
SHA512:	c0945c9b720ee31b8d2651ec584a02ca4373692dd1712fb09f4f87692c141bb86fd2f84b6b9dfa17f4bda49a7014682bdf7a0430b627381c6515ea679b9dabc3

General

SSDEEP:	1536:flfJffvxToSdAB/6lUUyaNTAETxEvZ0swq+A6T++DqfJffpfJff:9fJff9oKM/6ljyK5adwXqfJffpfJff
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......O......................D.......=.......Rich............PE..L...i.xT.....................P............... ....@................

File Icon

Icon Hash:	70ecccaececc71e2

Static PE Info

General

Entrypoint:	0x4015a8
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:	0x5478D769 [Fri Nov 28 20:13:29 2014 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:	458ac857eb15a6ebaad7748f2f663dae

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x20838	0x21000	False	0.353278882576	data	5.18913238109	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x22000	0x1250	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x24000	0x2f2c	0x3000	False	0.232584635417	data	4.20201309343	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
English	United States	

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

💡 Click to jump to process

System Behavior

Analysis Process: Scanned Payment Copy00024.scr.exe PID: 7052 Parent PID: 5288

General

Start time:	15:43:51
Start date:	29/11/2021
Path:	C:\Users\user\Desktop\Scanned Payment Copy00024.scr.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Scanned Payment Copy00024.scr.exe"
Imagebase:	0x400000
File size:	155648 bytes
MD5 hash:	9EBAAB853C410A3C6EF16ECF45739E8B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.870438121.0000000002210000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: conhost.exe PID: 7116 Parent PID: 7052

General

Start time:	15:43:51
Start date:	29/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis