ID: 528205
Sample Name: Hong Tak Engineering SB Payment Receipt 241121_PDF.exe
Cookbook: default.jbs
Time: 21:02:08
Date: 24/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

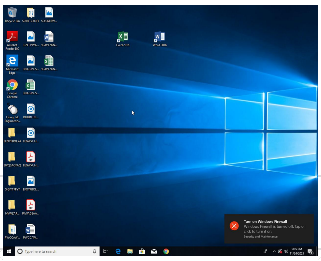
Windows Analysis Report Hong Tak Engineering SB Pa…

Overview

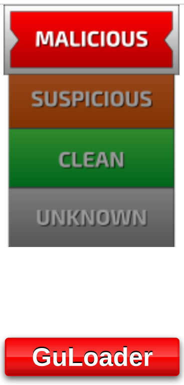
General Information

Sample Name:	Hong Tak Engineering SB Payment Receipt 241121_PDF.exe
Analysis ID:	528205
MD5:	b2e24bc0f1f55f2…
SHA1:	4a20778acf6d512.
SHA256:	d5ace58c68d1ff7..
Tags:	exe signed
Infos:	

Most interesting Screenshot:



Detection

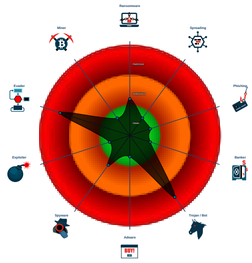


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- GuLoader behavior detected
- Yara detected GuLoader
- Hides threads from debuggers
- Initial sample is a PE file and has a …
- Writes to foreign memory regions
- Tries to detect Any.run
- Executable has a suspicious name (…
- C2 URLs / IPs found in malware con…
- Tries to detect sandboxes and other…
- Found potential dummy code loops (…

Classification



Process Tree

- **System is w10x64**
- Hong Tak Engineering SB Payment Receipt 241121_PDF.exe (PID: 6132 cmdline: "C:\Users\user\Desktop\Hong Tak Engineering SB Payment Receipt 241121_PDF.exe" MD5: B2E24BC0F1F55F2AC9D8034098DFE32F)
  - ieinstal.exe (PID: 6676 cmdline: "C:\Users\user\Desktop\Hong Tak Engineering SB Payment Receipt 241121_PDF.exe" MD5: DAD17AB737E680C47C8A44CBB95EE67E)
  - ieinstal.exe (PID: 672 cmdline: "C:\Users\user\Desktop\Hong Tak Engineering SB Payment Receipt 241121_PDF.exe" MD5: DAD17AB737E680C47C8A44CBB95EE67E)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://onedrive.live.com/download?cid=7FA6B3"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.520378272.0000000000750000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000006.00000000.377067642.0000000000560000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000006.00000002.564225292.0000000000560000.00000040.00000001.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 Any.run

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

Anti Debugging:

Hides threads from debuggers

Found potential dummy code loops (likely to delay analysis)

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Stealing of Sensitive Information:

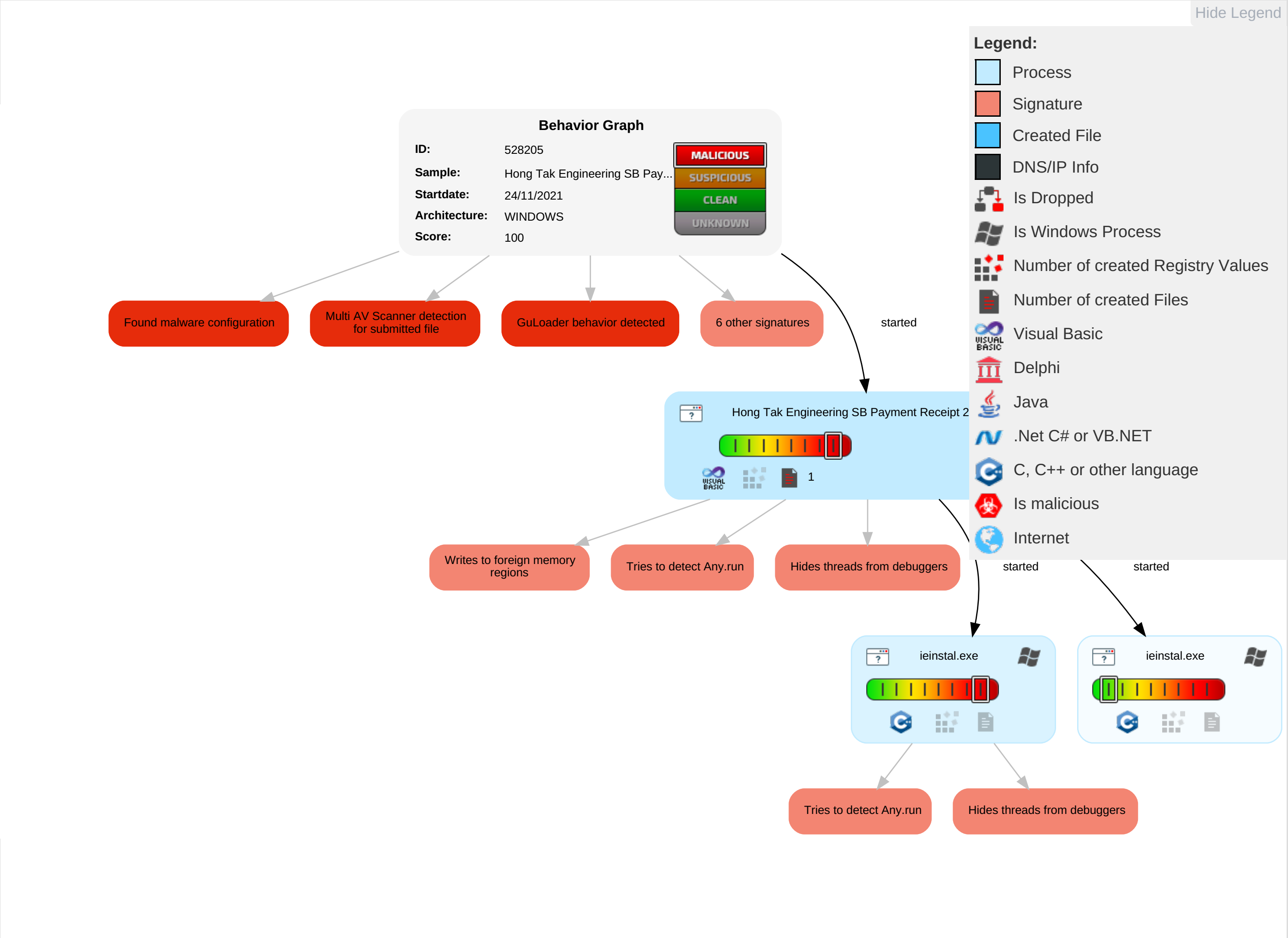
GuLoader behavior detected

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	Path Interception	Process Injection 1 1 2	Virtualization/Sandbox Evasion 3 1	Input Capture 1	Security Software Discovery 4 1 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicati

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 1 2	LSASS Memory	Virtualization/Sandbox Evasion 3 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap

Behavior Graph



ID: 528205

Sample: Hong Tak Engineering SB Pay...

Startdate: 24/11/2021

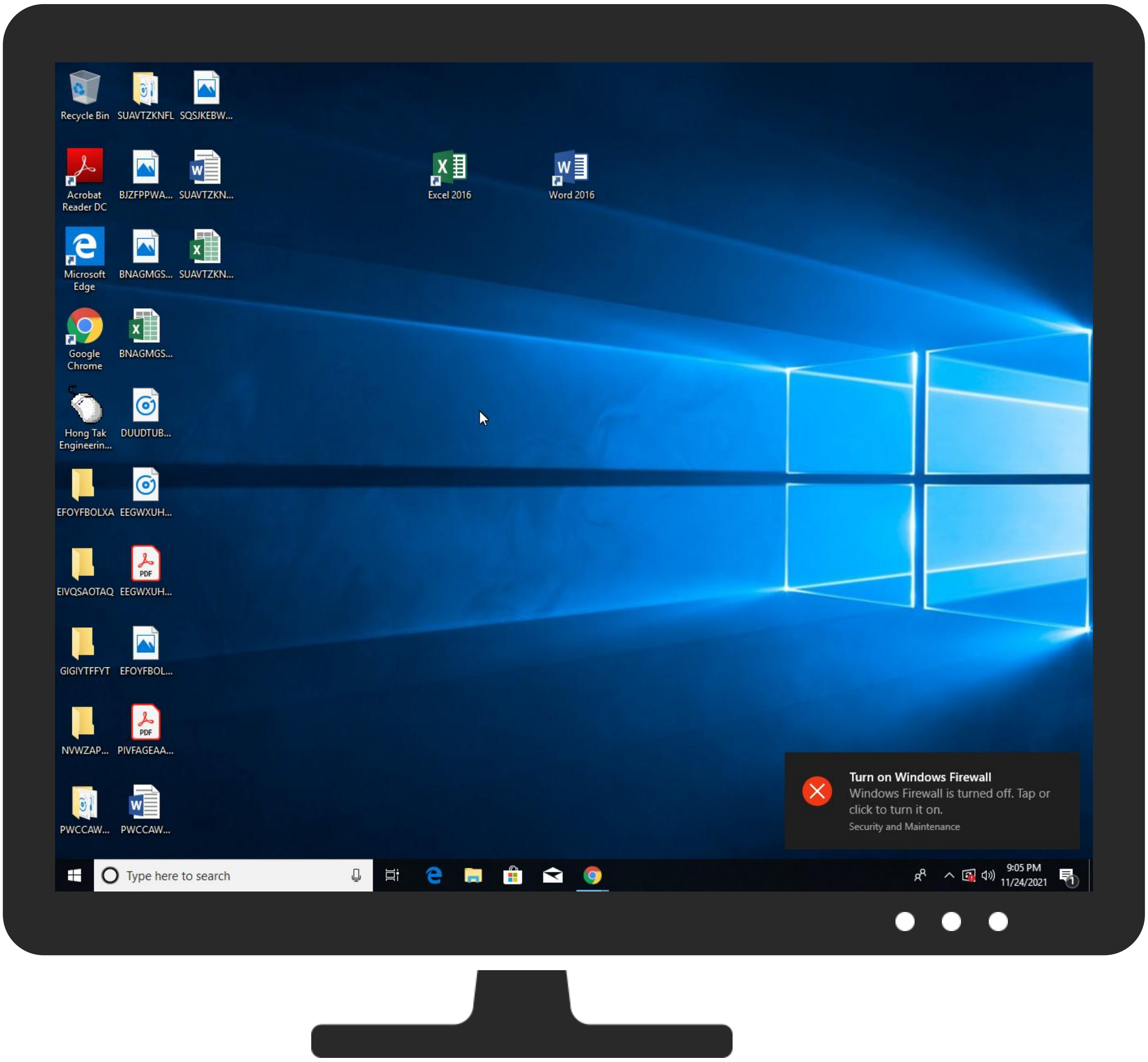
Architecture: WINDOWS

Score: 100

Screenshots

Thumbnails

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



Turn on Windows Firewall
Windows Firewall is turned off. Tap or click to turn it on.
Security and Maintenance

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Hong Tak Engineering SB Payment Receipt 241121_PDF.exe	40%	Virustotal		Browse
Hong Tak Engineering SB Payment Receipt 241121_PDF.exe	27%	ReversingLabs	Win32.Downloader.GuLoader	

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 URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://onedrive.live.com/download?cid=7FA6B3	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528205
Start date:	24.11.2021
Start time:	21:02:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Hong Tak Engineering SB Payment Receipt 241121_PDF.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:	mal100.troj.evad.winEXE@5/1@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 13.3% (good quality ratio 5.8%) • Quality average: 28.9% • Quality standard deviation: 36.3%
HCA Information:	• Successful, ratio: 80% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
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\~DFEBA196672956C021.TMP	
Process:	C:\Users\user\Desktop\Hong Tak Engineering SB Payment Receipt 241121_PDF.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.3863194741075688
Encrypted:	false
SSDEEP:	96:GaabmG8CL3uSTdfPBeQaabmG8CL3uSTdf:i93jJBeU93j
MD5:	B3A27F74C52AC98DDE14EA7A804ECFD6
SHA1:	5F6D3F7644E0973D8A059AC228042EA60C507836
SHA-256:	F6C6736ACA8B6A743732E216DBB62B59B65DCBB0B6308B2B28D67706ABBC7F0C
SHA-512:	F7129070C7133C63C57BE7724B322B2A8F3FB6624F35B7A4E730DECD418E488CBF53292E845255DEDCFBA1502A0332D7DB17EF29D0E2A2A4DD345F87EECB36 E
Malicious:	false
Reputation:	low
Preview:	......................>... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.999498053134024

General

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:	Hong Tak Engineering SB Payment Receipt 241121_PDF.exe
File size:	128816
MD5:	b2e24bc0f1f55f2ac9d8034098dfe32f
SHA1:	4a20778acf6d512792077dc339f23acfbdf22875
SHA256:	d5ace58c68d1ff767b284deb172b5ce0550e96023a509a1 71fa7b34f0929b8e0
SHA512:	01dbc321743acf74ef5557f9429d26aa5892b196c695a5e 4ed0342d626c4e98a650d01729975d20812653edaf5295 dc7484a43949738d9de5effdb1dcb7b896
SSDEEP:	1536:I+3sCKWgen7J84YCrMYpNxXeBwodguvRZkVT7yaBOJzFHKAgYX5:I1PX0JLHrJNvoPvoVT58JzFh5
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$..........u...&...&...&T..&...&...&...&...&...&Rich...&................PE..L......V.. ....`...... ....@........

File Icon

Icon Hash:	42b97ce4f0e1f2e4

Static PE Info

General

Entrypoint:	0x401320
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:	0x56BC1AFE [Thu Feb 11 05:24:14 2016 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:	995d60149de3040b4890e5871343f4eb

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=dykkerklokkeado@LOKALITET.Sk, CN=godkendelsesmil, OU=Iroquoianspri1, O=Klarissenobie, L=KEDECHRYSLEROVEREF, S=AFSPADSERING, C=SC
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	• 11/23/2021 8:20:15 PM 11/23/2022 8:20:15 PM
Subject Chain	• E=dykkerklokkeado@LOKALITET.Sk, CN=godkendelsesmil, OU=Iroquoianspri1, O=Klarissenobie, L=KEDECHRYSLEROVEREF, S=AFSPADSERING, C=SC
Version:	3
Thumbprint MD5:	8ACCDE5BD3D9438F5ED6CE6C1979787E
Thumbprint SHA-1:	E6BE6E4C60B6588F4C337C033C6165C6914F3249
Thumbprint SHA-256:	A2E6DA055CC6C343D9251796595BC0A1882C21EC31DBD14C72A656EC419A4096
Serial:	00

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x18728	0x19000	False	0.47935546875	data	6.37312654175	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1a000	0x1a94	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1c000	0x373c	0x4000	False	0.217163085938	data	3.71594095347	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	
Chinese	Taiwan	

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Hong Tak Engineering SB Payment Receipt 241121_PDF.exe PID: 6132 Parent PID: 5256

General

Start time:	21:03:03
Start date:	24/11/2021
Path:	C:\Users\user\Desktop\Hong Tak Engineering SB Payment Receipt 241121_PDF.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Hong Tak Engineering SB Payment Receipt 241121_PDF.exe"
Imagebase:	0x400000
File size:	128816 bytes
MD5 hash:	B2E24BC0F1F55F2AC9D8034098DFE32F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.520378272.0000000000750000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: ieinstal.exe PID: 6676 Parent PID: 6132

General

Start time:	21:03:44
Start date:	24/11/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\Hong Tak Engineering SB Payment Receipt 241121_PDF.exe"
Imagebase:	0xe80000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: 672 Parent PID: 6132

General

Start time:	21:03:45
Start date:	24/11/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Hong Tak Engineering SB Payment Receipt 241121_PDF.exe"
Imagebase:	0xe80000
File size:	480256 bytes
MD5 hash:	DAD17AB737E680C47C8A44CBB95EE67E
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: 00000006.00000000.377067642.0000000000560000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000006.00000002.564225292.0000000000560000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

Disassembly

Code Analysis

Joe Sandbox Cloud Basic 34.0.0 Boulder Opal