JoeSandbox Cloud BASIC

ID: 528205
Sample Name: Hong Tak Engineering SB Payment Receipt 241121_PDF.exe
Cookbook: default.jbs
Time: 21:11:59
Date: 24/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

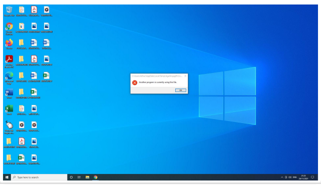
Windows Analysis Report Hong Tak Engineering SB Pa…

Overview

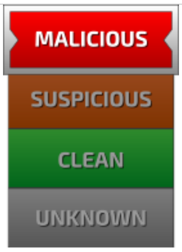
General Information

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

Most interesting Screenshot:



Detection



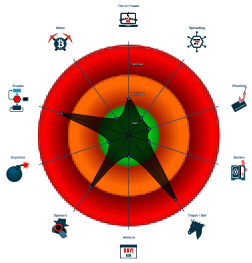
GuLoader Remcos

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Remcos RAT
- Multi AV Scanner detection for dropp…
- Yara detected GuLoader
- Hides threads from debuggers
- Installs a global keyboard hook
- Initial sample is a PE file and has a …
- Writes to foreign memory regions
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Executable has a suspicious name (…

Classification



Process Tree

- **System is w10x64native**
- Hong Tak Engineering SB Payment Receipt 241121_PDF.exe (PID: 3648 cmdline: "C:\Users\user\Desktop\Hong Tak Engineering SB Payment Receipt 241121_PDF.exe" MD5: B2E24BC0F1F55F2AC9D8034098DFE32F)
  - ieinstal.exe (PID: 5020 cmdline: "C:\Users\user\Desktop\Hong Tak Engineering SB Payment Receipt 241121_PDF.exe" MD5: 7871873BABCEA94FBA13900B561C7C55)
- **cleanup**

Malware Configuration

Threatname: GuLoader

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

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000002.5679272163.00000000030 2B000.00000004.00000020.sdmp	JoeSecurity_Remcos	Yara detected Remcos RAT	Joe Security	
00000003.00000002.1038188324.00000000022 D0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
0000000F.00000000.759017370.0000000002CE 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
Process Memory Space: ieinstal.exe PID: 5020	JoeSecurity_Remcos	Yara detected Remcos RAT	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

Yara detected Remcos RAT

Multi AV Scanner detection for dropped file

Networking:

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

E-Banking Fraud:

Yara detected Remcos RAT

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

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Remcos RAT

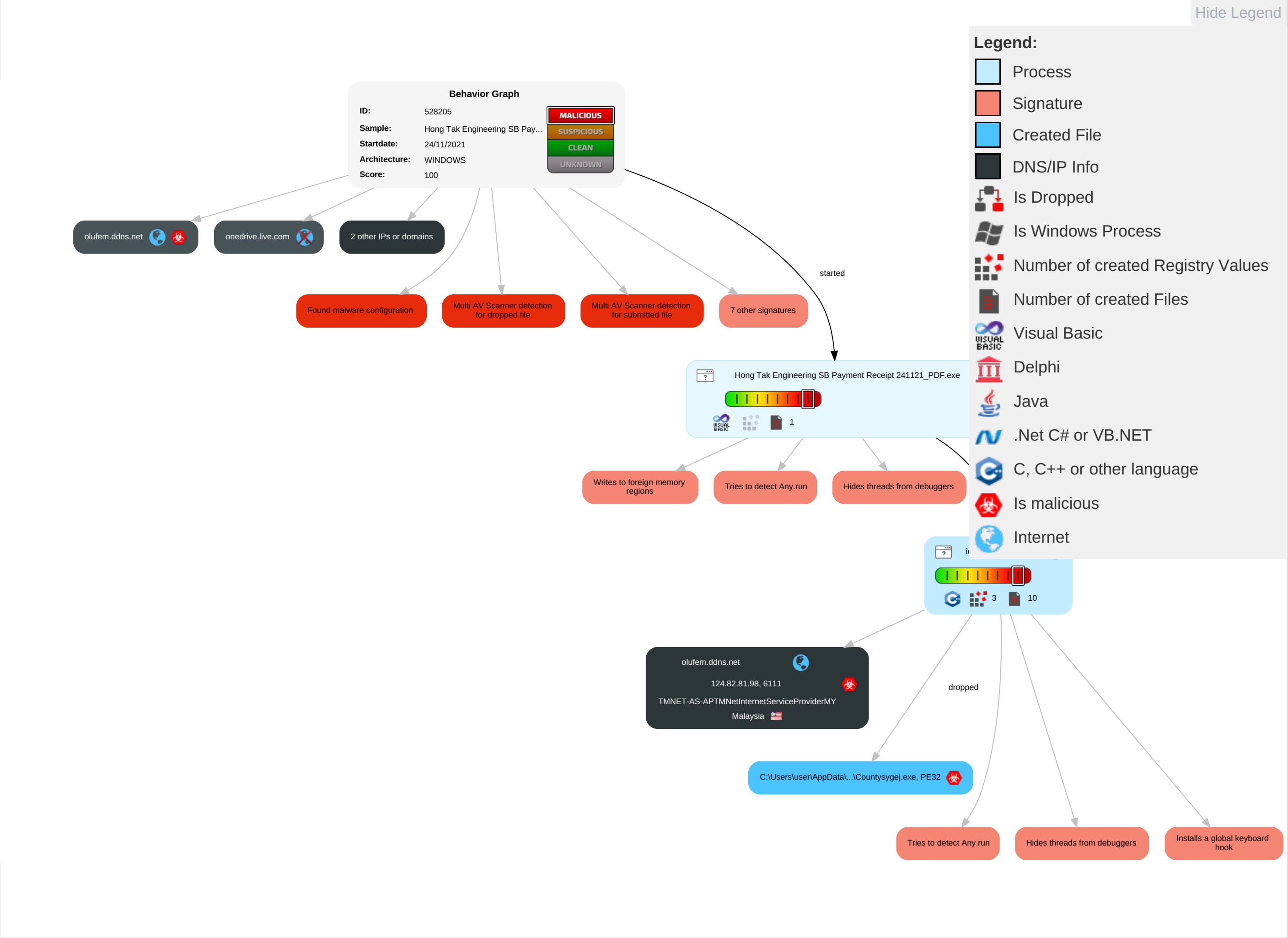
Remote Access Functionality:

Yara detected Remcos RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Windows Management Instrumentation	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	Masquerading 1	Input Capture 1 1	Security Software Discovery 4 2 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesd Insecur Networl Commu
Default Accounts	Scheduled Task/Job	DLL Side-Loading 1	Registry Run Keys / Startup Folder 1	Virtualization/Sandbox Evasion 2 3	LSASS Memory	Virtualization/Sandbox Evasion 2 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit Redirec Calls/SI
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Process Injection 1 1 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 1	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	System Information Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Commu

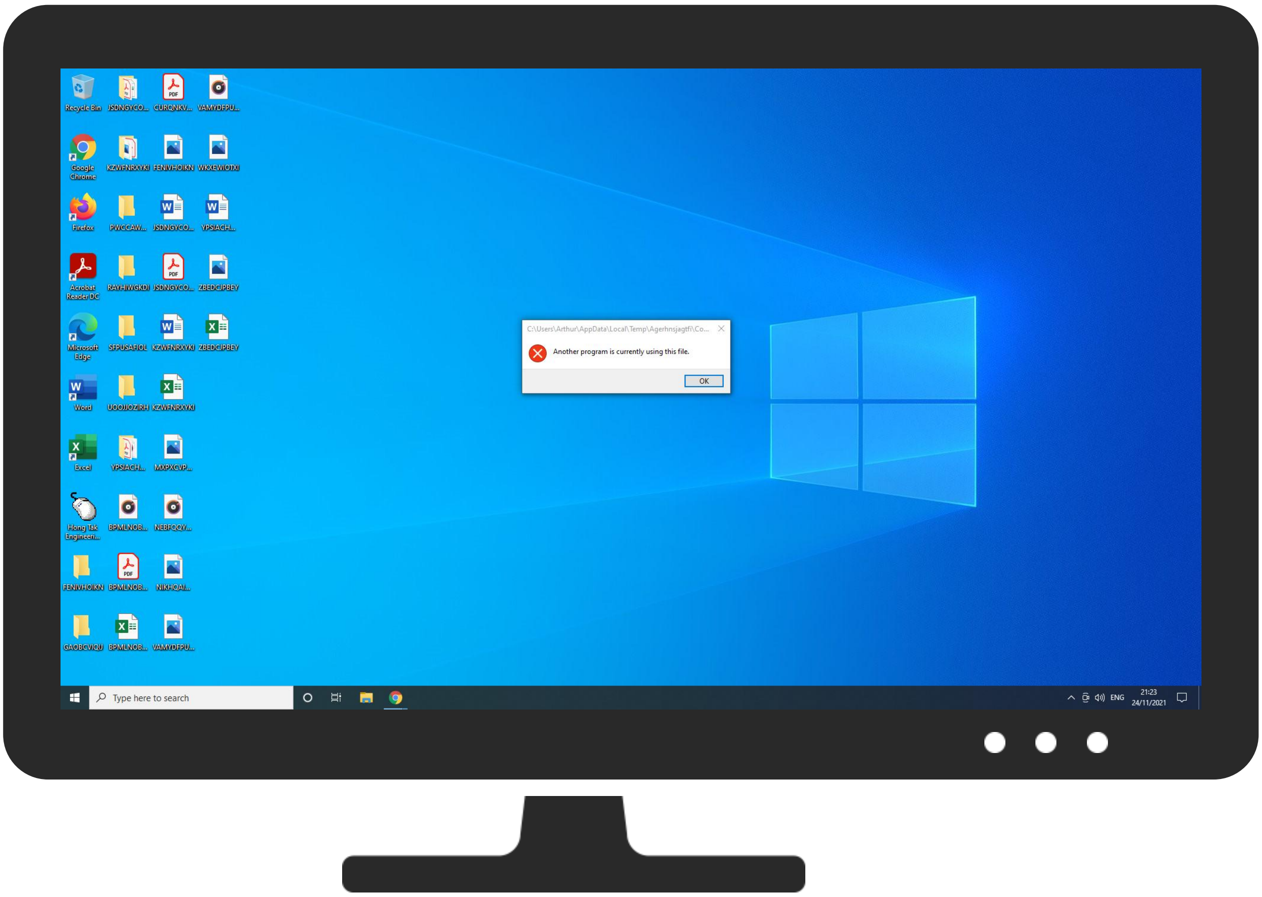
Behavior Graph



Screenshots

Thumbnails

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



C:\Users\Arthur\AppData\Local\Temp\Agerhnsjagtfi\Co...

Another program is currently using this file.

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

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

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Agerhnsjagtfi\Countysygej.exe	40%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\Agerhnsjagtfi\Countysygej.exe	27%	ReversingLabs	Win32.Downloader.GuLoader	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
olufem.ddns.net	124.82.81.98	true	true		unknown
onedrive.live.com	unknown	unknown	false		high
7ybh4q.bn.files.1drv.com	unknown	unknown	false		high

Contacted URLs

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

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
124.82.81.98	olufem.ddns.net	Malaysia	🇲🇾	4788	TMNET-AS-APTMNetInternetServiceProviderMY	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528205
Start date:	24.11.2021
Start time:	21:11:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 43s
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 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:	41
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.spyw.evad.winEXE@3/3@10/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 75% • 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

Time	Type	Description
21:15:22	Task Scheduler	Run new task: Intel PTT EK Recertification path: "C:\Windows\System32\DriverStore\FileRepository\iclsclient.inf_amd64_75ffca5eec865b4b\lib\IntelPTTEKRecertification.exe"
21:15:54	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Tanadarforurenings C:\Users\user\AppData\Local\Temp\Agerhnsjagtfi\Countysygej.exe
21:16:02	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Tanadarforurenings C:\Users\user\AppData\Local\Temp\Agerhnsjagtfi\Countysygej.exe

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
olufem.ddns.net	EASTWAY COMNAGA SB PAYMENT BANK IN SLIP 250521_PDF.exe	Get hash	malicious	Browse	• 192.253.242.6

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TMNET-AS-APTMNetInternetServiceProviderMY	8WJ1mWaBwN	Get hash	malicious	Browse	• 60.49.58.145
	j9ZfvcmyKN	Get hash	malicious	Browse	• 1.32.15.223
	jJE7aD1zME	Get hash	malicious	Browse	• 219.93.31.44
	SSIuSyaBAF	Get hash	malicious	Browse	• 210.187.51.227
	arm-20211121-1750	Get hash	malicious	Browse	• 175.145.81.50

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Z4GtdTRjuR	Get hash	malicious	Browse	- 175.139.103.110
	4ljC16LtGD	Get hash	malicious	Browse	- 60.51.38.70
	n3586AtaJ2	Get hash	malicious	Browse	- 110.159.188.159
	XLKPMXNVFz	Get hash	malicious	Browse	- 60.49.58.145
	uranium.arm	Get hash	malicious	Browse	- 115.133.184.135
	6czmI0PCR3	Get hash	malicious	Browse	- 202.188.38.151
	hlejwF53zt	Get hash	malicious	Browse	- 219.93.199.24
	arm7	Get hash	malicious	Browse	- 175.143.137.156
	arm	Get hash	malicious	Browse	- 219.95.72.247
	TAwWC6sZFE	Get hash	malicious	Browse	- 42.189.114.232
	he7hRoAnnx	Get hash	malicious	Browse	- 175.143.137.179
	mips	Get hash	malicious	Browse	- 115.132.43.74
	0v5QUcQFnC	Get hash	malicious	Browse	- 1.32.134.252
	arm5-20211114-0109	Get hash	malicious	Browse	- 175.139.159.156
	0tCtZXUxNW	Get hash	malicious	Browse	- 118.101.211.234

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\Agerhnsjagtfil\Countysygej.exe	
Process:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	128816
Entropy (8bit):	5.999498053134024
Encrypted:	false
SSDEEP:	1536:I+3sCKWgen7J84YCrMYpNxXeBwodguvRZkVT7yaBOJzFHKAgYX5:I1PX0JLHrJNvoPvoVT58JzFh5
MD5:	B2E24BC0F1F55F2AC9D8034098DFE32F
SHA1:	4A20778ACF6D512792077DC339F23ACFBDF22875
SHA-256:	D5ACE58C68D1FF767B284DEB172B5CE0550E96023A509A171FA7B34F0929B8E0
SHA-512:	01DBC321743ACF74EF5557F9429D26AA5892B196C695A5E4ED0342D626C4E98A650D01729975D20812653EDAF5295FDC7484A43949738D9DE5EFFDB1DCB7B89
Malicious:	**true**
Antivirus:	- Antivirus: Virustotal, Detection: 40%, Browse - Antivirus: ReversingLabs, Detection: 27%
Reputation:	low
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$..........u..&..&..&T.&..&..&..&..&..&Rich..&................PE..L......V................ .....`...... .............@..................................A.......................................d...(.......<7..............0..................................................0... ....................................text...(.......................... ..` .data...............................@....rsrc...<7.......@..................@..@..^............MSVBVM60.DLL.. ....

C:\Users\user\AppData\Local\Temp\~DFDA925A6B9EAC6C8F.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

C:\Users\user\AppData\Local\Temp\~DFDA925A6B9EAC6C8F.TMP

SHA1:	5F6D3F7644E0973D8A059AC228042EA60C507836
SHA-256:	F6C6736ACA8B6A743732E216DBB62B59B65DCBB0B6308B2B28D67706ABBC7F0C
SHA-512:	F7129070C7133C63C57BE7724B322B2A8F3FB6624F35B7A4E730DECD418E488CBF53292E845255DEDCFBA1502A0332D7DB17EF29D0E2A2A4DD345F87EECB36 E
Malicious:	false
Reputation:	low
Preview:	.....................>.. ....

C:\Users\user\AppData\Roaming\wifitskl\logs.dat

Process:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
File Type:	data
Category:	dropped
Size (bytes):	144
Entropy (8bit):	3.3458058208756873
Encrypted:	false
SSDEEP:	3:rklKlFlUef4qClDl5JWRal2Jl+7R0DAlBG45klovDl6v:IlKPlPf4qCb5YcIeeDAlOWAv
MD5:	15929DC814DA0FBE525987A12E1802A8
SHA1:	AF68046542D879732F3D447B3046FD02D5B5EFC1
SHA-256:	3D48A06F43C9DC735B6174D4019EFBF866D9F11946A8D2F691CA7DF33460823F
SHA-512:	74C074F001B04538BE027C1E8FCE6F1CBC5A36D01083B3AB455DFDA14DC61850E12B816C5A4E9C7D3A22422E223E866306D874293DB157415B0C70DF3A1A8C3
Malicious:	false
Reputation:	low
Preview:	....[.2.0.2.1./.1.1./.2.4. .2.1.:.1.6.:.0.3. .O.f.f.l.i.n.e. .K.e.y.l.o.g.g.e.r. .S.t.a.r.t.e.d.].........[.P.r.o.g.r.a.m. .M.a.n.a.g.e.r.].....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.999498053134024
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.!Th is 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	• 24/11/2021 04:20:15 24/11/2022 04:20:15
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	

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/24/21-21:16:03.943231	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54993	1.1.1.1	192.168.11.20
11/24/21-21:17:10.219978	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61388	1.1.1.1	192.168.11.20
11/24/21-21:18:16.486809	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56392	1.1.1.1	192.168.11.20
11/24/21-21:19:22.754077	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53851	1.1.1.1	192.168.11.20
11/24/21-21:20:29.035139	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57069	1.1.1.1	192.168.11.20
11/24/21-21:21:35.301983	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50763	1.1.1.1	192.168.11.20
11/24/21-21:22:41.570485	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	62805	1.1.1.1	192.168.11.20
11/24/21-21:23:47.834671	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	63500	1.1.1.1	192.168.11.20

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 24, 2021 21:15:56.838493109 CET	192.168.11.20	1.1.1.1	0x7c5f	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Nov 24, 2021 21:15:57.603185892 CET	192.168.11.20	1.1.1.1	0xb6f5	Standard query (0)	7ybh4q.bn.files.1drv.com	A (IP address)	IN (0x0001)
Nov 24, 2021 21:16:03.931648970 CET	192.168.11.20	1.1.1.1	0xcd2c	Standard query (0)	olufem.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 21:17:10.207977057 CET	192.168.11.20	1.1.1.1	0xf8f8	Standard query (0)	olufem.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 21:18:16.474395037 CET	192.168.11.20	1.1.1.1	0x77ac	Standard query (0)	olufem.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 21:19:22.741189957 CET	192.168.11.20	1.1.1.1	0x6f48	Standard query (0)	olufem.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 21:20:29.023251057 CET	192.168.11.20	1.1.1.1	0x5463	Standard query (0)	olufem.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 21:21:35.289797068 CET	192.168.11.20	1.1.1.1	0x2889	Standard query (0)	olufem.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 21:22:41.556521893 CET	192.168.11.20	1.1.1.1	0xdd45	Standard query (0)	olufem.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 21:23:47.822930098 CET	192.168.11.20	1.1.1.1	0x4b0f	Standard query (0)	olufem.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 24, 2021 21:15:56.848558903 CET	1.1.1.1	192.168.11.20	0x7c5f	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 24, 2021 21:15:57.780812979 CET	1.1.1.1	192.168.11.20	0xb6f5	No error (0)	7ybh4q.bn.files.1drv.com	bn-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Nov 24, 2021 21:15:57.780812979 CET	1.1.1.1	192.168.11.20	0xb6f5	No error (0)	bn-files.fe.1drv.com	odc-bn-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Nov 24, 2021 21:16:03.943231106 CET	1.1.1.1	192.168.11.20	0xcd2c	No error (0)	olufem.ddns.net		124.82.81.98	A (IP address)	IN (0x0001)
Nov 24, 2021 21:17:10.219978094 CET	1.1.1.1	192.168.11.20	0xf8f8	No error (0)	olufem.ddns.net		124.82.81.98	A (IP address)	IN (0x0001)
Nov 24, 2021 21:18:16.486809015 CET	1.1.1.1	192.168.11.20	0x77ac	No error (0)	olufem.ddns.net		124.82.81.98	A (IP address)	IN (0x0001)
Nov 24, 2021 21:19:22.754076958 CET	1.1.1.1	192.168.11.20	0x6f48	No error (0)	olufem.ddns.net		124.82.81.98	A (IP address)	IN (0x0001)
Nov 24, 2021 21:20:29.035139084 CET	1.1.1.1	192.168.11.20	0x5463	No error (0)	olufem.ddns.net		124.82.81.98	A (IP address)	IN (0x0001)
Nov 24, 2021 21:21:35.301983118 CET	1.1.1.1	192.168.11.20	0x2889	No error (0)	olufem.ddns.net		124.82.81.98	A (IP address)	IN (0x0001)
Nov 24, 2021 21:22:41.570485115 CET	1.1.1.1	192.168.11.20	0xdd45	No error (0)	olufem.ddns.net		124.82.81.98	A (IP address)	IN (0x0001)
Nov 24, 2021 21:23:47.834671021 CET	1.1.1.1	192.168.11.20	0x4b0f	No error (0)	olufem.ddns.net		124.82.81.98	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Hong Tak Engineering SB Payment Receipt 241121_PDF.exe PID: 3648 Parent PID: 8652

General

Start time:	21:15:22
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: 00000003.00000002.1038188324.00000000022D0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: ieinstal.exe PID: 5020 Parent PID: 3648

General

Start time:	21:15:37
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:	0xc60000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	- Rule: JoeSecurity_Remcos, Description: Yara detected Remcos RAT, Source: 0000000F.00000002.5679272163.000000000302B000.00000004.00000020.sdmp, Author: Joe Security - Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000F.00000000.759017370.0000000002CE0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis

Joe Sandbox Cloud Basic 34.0.0 Boulder Opal