ID: 540990
Sample Name:
PKO_TRANS_DETAILS_20211216_0809521.exe
Cookbook: default.jbs
Time: 13:10:15
Date: 16/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

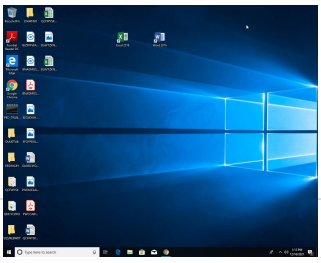
Windows Analysis Report PKO_TRANS_DETAILS_2021…

Overview

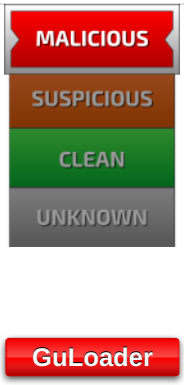
General Information

Sample Name:	PKO_TRANS_DETAILS_20211216_0809521.exe
Analysis ID:	540990
MD5:	1823b507e96d81..
SHA1:	e5d7884da7d17b..
SHA256:	99b81b452d1739..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



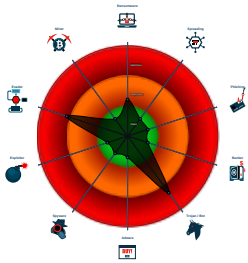
GuLoader

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
- Contains functionality to call native f…

Classification



Process Tree

- **System is w10x64**
- PKO_TRANS_DETAILS_20211216_0809521.exe (PID: 6972 cmdline: "C:\Users\user\Desktop\PKO_TRANS_DETAILS_20211216_0809521.exe" MD5: 1823B507E96D8138BADA7C65D424ABCC)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=1bySt7nT"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.805543754.0000000004C80000.00000040.00000001.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

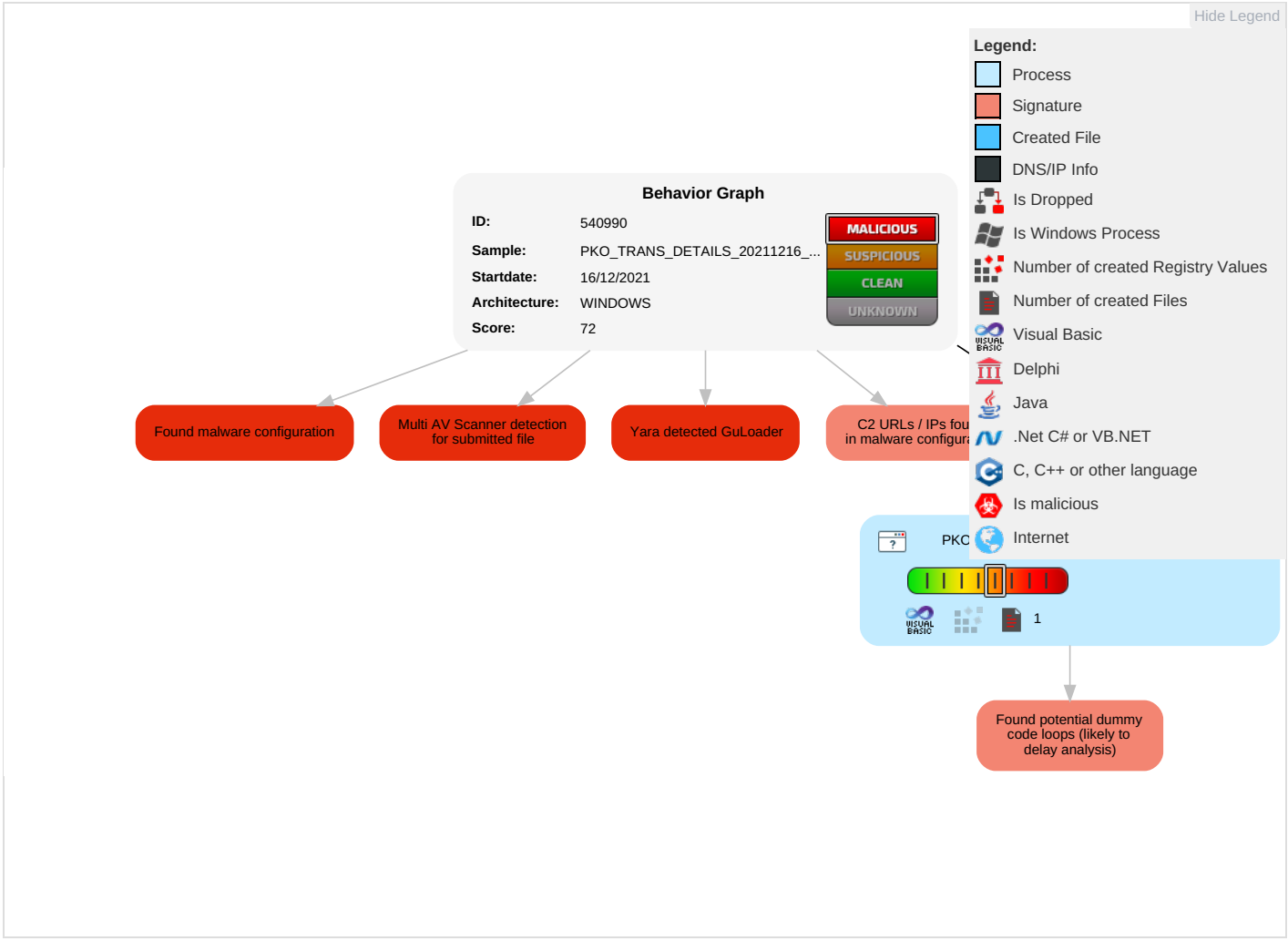
Anti Debugging:

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	Security Software Discovery 1 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	Software Packing 1	LSASS Memory	Virtualization/Sandbox Evasion 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)	Process Injection 1	Security Account Manager	Process Discovery 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)	Obfuscated Files or Information 2	NTDS	System Information Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

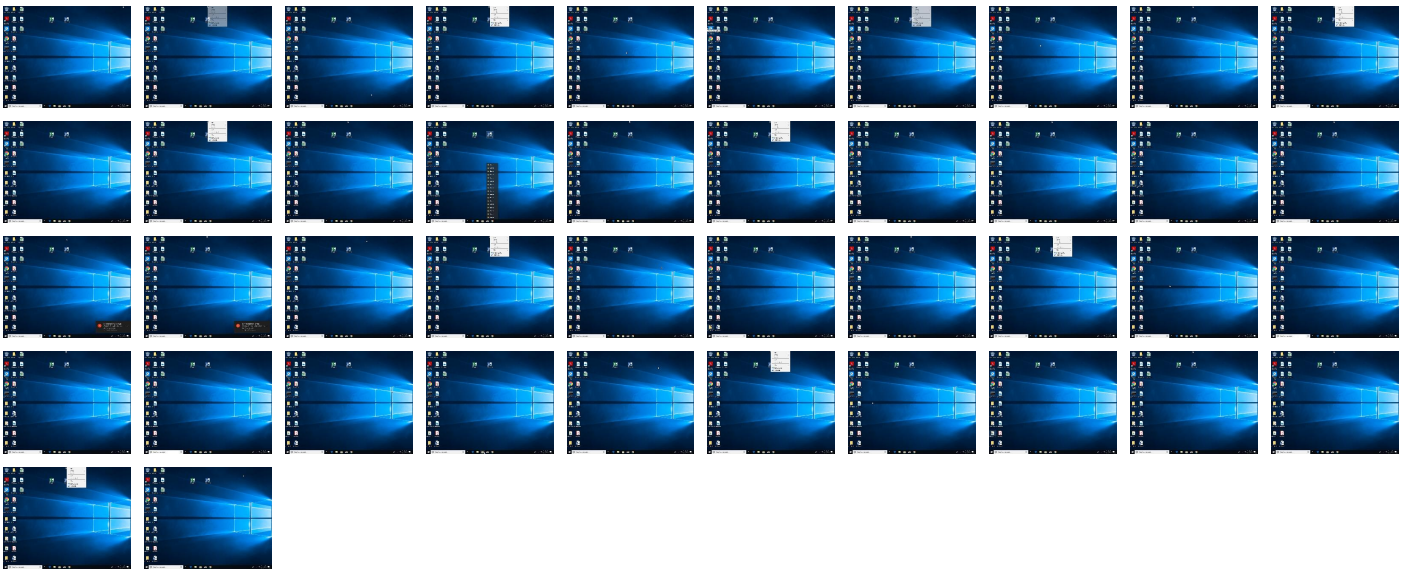
Behavior Graph



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
PKO_TRANS_DETAILS_20211216_0809521.exe	21%	Virustotal		Browse

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:	540990
Start date:	16.12.2021
Start time:	13:10:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PKO_TRANS_DETAILS_20211216_0809521.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:	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:	mal72.troj.evad.winEXE@1/1@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 26.3% (good quality ratio 16%) • Quality average: 36.8% • Quality standard deviation: 37%
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\~DF4AE55F204BB0FB8A.TMP	
Process:	C:\Users\user\Desktop\PKO_TRANS_DETAILS_20211216_0809521.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	2.45010052865662
Encrypted:	false
SSDEEP:	96:jaGu8uY05xb30uxH+iMa9eHC2K4veMC47+crGNa:jtjReMC49rAa
MD5:	9635DCB06D1E14BE1BB3D7D4B4CEA9F0
SHA1:	CCE17243F4FDB2A218D4185E75715E67AE7E219C
SHA-256:	D40FDC94A7E2F1C30434803A370E8881BF493D506000C27178A79CF02ECAB2D6
SHA-512:	D75D3149FFE0F772CE6E99E239E72EADCCB1F2CE55F05ABBF1C687A3991C0DAD6905DA85D0F1CDD8C5FCC91F533E1C0799F04BB2EAC9CD91CB61C480EAA 7F3
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.690014470947888
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:	PKO_TRANS_DETAILS_20211216_0809521.exe
File size:	147456
MD5:	1823b507e96d8138bada7c65d424abcc
SHA1:	e5d7884da7d17ba0ae592ff787e84ae665e21c3a
SHA256:	99b81b452d173986229ed512383e05214f35c819aa9da4 c2a972bb05c880d536

General

SHA512:	66c962308ad08bf950dfd738de5585e79aa91a28379fe59ccfd78a578a7e629ff123b63d8509d3f0366089f3cca65e932bee3dee5d8a1744e1f3d8eca340d852
SSDEEP:	3072:U4PvIBPPFoSfth9WGq8Av35lbUTv9/alVVPx:U4PAsGU5+BaxPx
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W.x.....\.....%.....Rich.....PE..L.....U.....`.....$.....@

File Icon

Icon Hash:	bc546d7f6f130982

Static PE Info

General

Entrypoint:	0x401524
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:	0x55BBDCC8 [Fri Jul 31 20:38:32 2015 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:	7d340e80350d9e6231e6392a24967d10

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1faf0	0x20000	False	0.557975769043	data	6.98717798783	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x21000	0x36b4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x25000	0x1956	0x2000	False	0.317504882812	data	4.27344211058	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

System Behavior

Analysis Process: PKO_TRANS_DETAILS_20211216_0809521.exe PID: 6972 Parent PID: 2464

General

Start time:	13:11:06
Start date:	16/12/2021
Path:	C:\Users\user\Desktop\PKO_TRANS_DETAILS_20211216_0809521.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\PKO_TRANS_DETAILS_20211216_0809521.exe"
Imagebase:	0x400000
File size:	147456 bytes
MD5 hash:	1823B507E96D8138BADA7C65D424ABCC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.805543754.0000000004C80000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis