

JOeSandbox Cloud BASIC



ID: 339384

Sample Name: SPPG contract
9200355_Acma Engineers SP
Power_Contract No
9200355.exe

Cookbook: default.jbs

Time: 22:01:10

Date: 13/01/2021

Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents	2
Analysis Report SPPG contract 9200355_Acma Engineers SP	
Power_Contract No 9200355.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Yara Overview	4
Memory Dumps	4
Sigma Overview	4
Signature Overview	5
Data Obfuscation:	5
Malware Analysis System Evasion:	5
Anti Debugging:	5
Mitre Att&ck Matrix	5
Behavior Graph	6
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	7
Domains	7
URLs	7
Domains and IPs	8
Contacted Domains	8
Contacted IPs	8
General Information	8
Simulations	8
Behavior and APIs	9
Joe Sandbox View / Context	9
IPs	9
Domains	9
ASN	9
JA3 Fingerprints	9
Dropped Files	9
Created / dropped Files	9
Static File Info	9
General	9
File Icon	10
Static PE Info	10
General	10
Entrypoint Preview	10
Data Directories	11
Sections	11
Resources	11
Imports	11
Version Infos	11
Possible Origin	12
Network Behavior	12
Code Manipulations	12
Statistics	12

System Behavior	12
Analysis Process: SPPG contract 9200355_Acma Engineers SP Power_Contract No 9200355.exe PID: 6072	
Parent PID: 5648	12
General	12
File Activities	12
Disassembly	13
Code Analysis	13

Analysis Report SPPG contract 9200355_Acma Enginee...

Overview

General Information

Sample Name:

SPPG contract 9200355_Acma Engineers SP Power_Contract No 9200355.exe

Analysis ID:

339384

MD5:

276d1a6d58cc96...

SHA1:

c918ee3a14f5fe8..

SHA256:

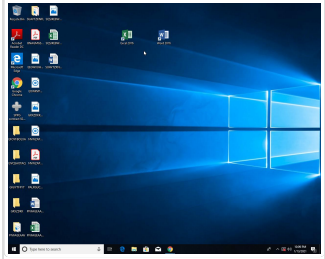
ef89d342ca08bb2.

Tags:

exe

GuLoader

Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

GuLoader

Score:

76

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Yara detected GuLoader

Contains functionality to detect hard...

Detected RDTSC dummy instruction...

Found potential dummy code loops (...)

Potential time zone aware malware

Tries to detect sandboxes and other...

Tries to detect virtualization through...

Yara detected VB6 Downloader Gen...

Abnormal high CPU Usage

Contains functionality for execution ...

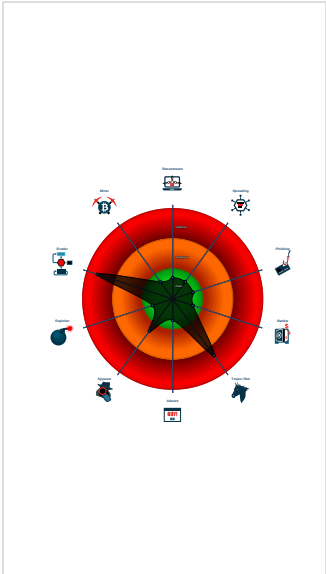
Contains functionality to query CPU ...

Contains functionality to read the PEB

Creates a DirectInput object (often fo...

PE file contains strange resources

Classification



Startup

- System is w10x64
- [SPPG contract 9200355_Acma Engineers SP Power_Contract No 9200355.exe](#) (PID: 6072 cmdline: 'C:\Users\user\Desktop\SPPG contract 9200355_Acma Engineers SP Power_Contract No 9200355.exe' MD5: 276D1A6D58CC96BEC4CCF5F19D395170)
- cleanup

Malware Configuration

No configs have been found

Yara Overview

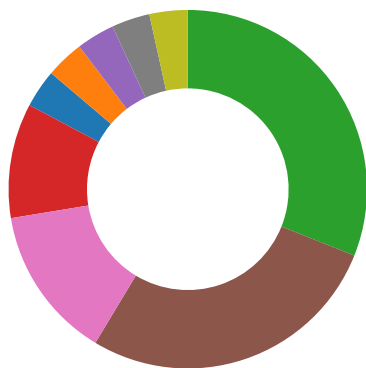
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: SPPG contract 9200355_Acma Engineers SP Power_Contract No 9200355.exe PID: 6072	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: SPPG contract 9200355_Acma Engineers SP Power_Contract No 9200355.exe PID: 6072	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- Compliance
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

Data Obfuscation:



Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:



Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Potential time zone aware malware

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

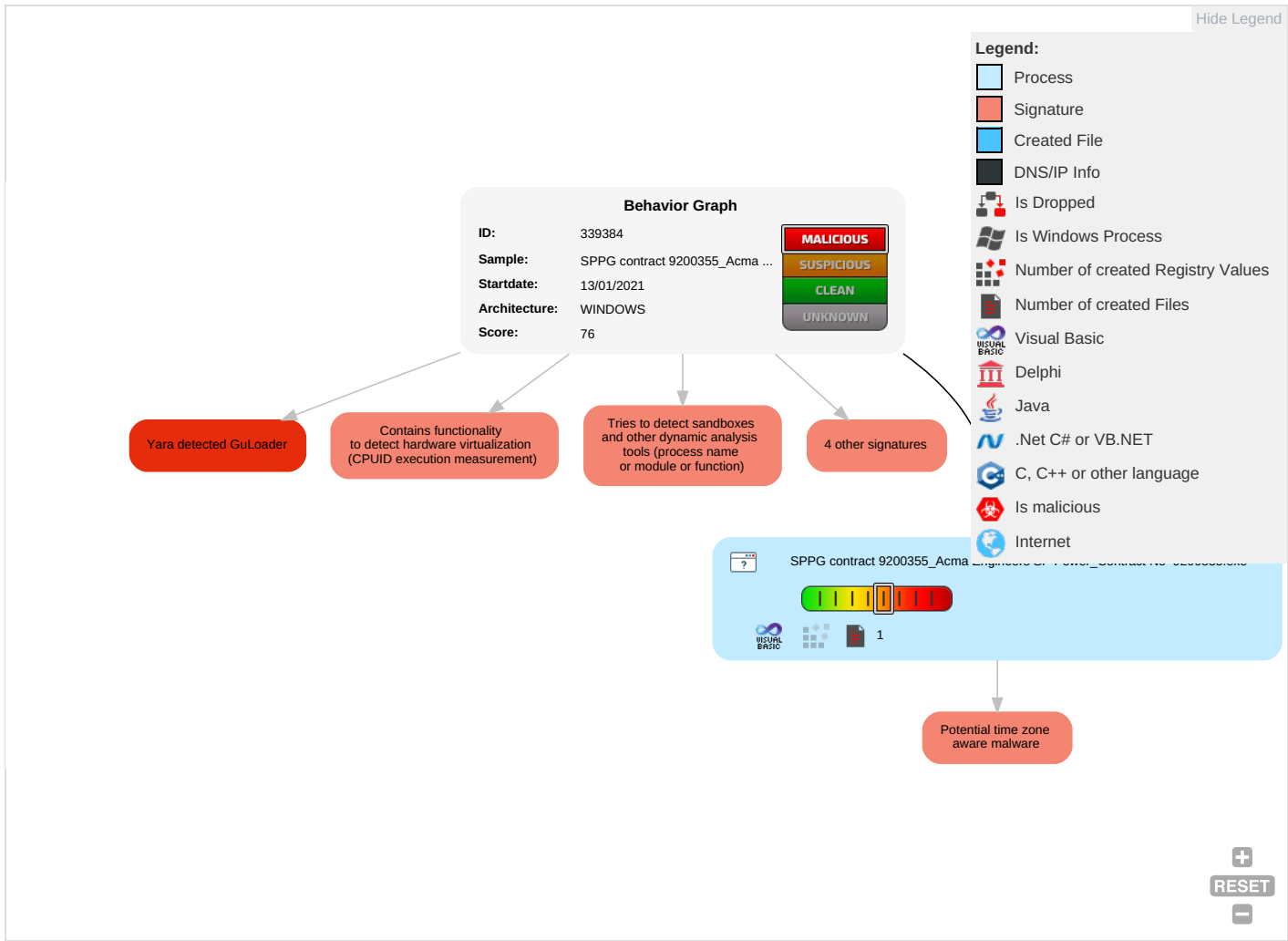


Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Recovery
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Recovery
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Security Software Discovery 5 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Recovery
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	Recovery
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	Recovery
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Information Discovery 3 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	Recovery

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
SPPG contract 9200355_Acma Engineers SP Power_Contract No 9200355.exe	0%	ReversingLabs		

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:	31.0.0 Red Diamond
Analysis ID:	339384
Start date:	13.01.2021
Start time:	22:01:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SPPG contract 9200355_Acma Engineers SP Power_Contract No 9200355.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:	37
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:	<ul style="list-style-type: none">• HCA enabled• EGA enabled• HDC enabled• AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal76.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none">• Successful, ratio: 31.6% (good quality ratio 17.9%)• Quality average: 33.3%• Quality standard deviation: 33.6%
HCA Information:	Failed
Cookbook Comments:	<ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• Exclude process from analysis (whitelisted): MpCmdRun.exe, RuntimeBroker.exe, backgroundTaskHost.exe, Usoclient.exe, audiodg.exe, BackgroundTransferHost.exe, HxTsr.exe, WMIADAP.exe, MusNotifIcon.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe• VT rate limit hit for: /opt/package/joesandbox/database/analysis/339384/sample/SPPG contract 9200355_Acma Engineers SP Power_Contract No 9200355.exe

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

No created / dropped files found

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.138928852734773
TrID:	<ul style="list-style-type: none">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:	SPPG contract 9200355_Acma Engineers SP Power_Contract No 9200355.exe
File size:	65536
MD5:	276d1a6d58cc96bec4ccf5f19d395170
SHA1:	c918ee3a14f5fe894ae66322a8c577b4cf5a90b3
SHA256:	ef89d342ca08bb27526ec176d4a359bb99e406ccccfc16a9f704d706574e215f
SHA512:	35969877df3943fd1571cb3815d4d62b5b20a386c213c5fde1449bf63fa2e71c29899e6b40938b603ac267c7866dc8125c49c48771946c52081069450cecc94b
SSDEEP:	768:XC1qT3P0XKiCra7AltYI5Pmkd22DRnizxXstAjQKWCCmUY:y4f0dCKnDRizRBT
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode...\$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L.... TW.....0.....@.....

File Icon



Icon Hash:

f030f0c6f030b100

Static PE Info

General

Entrypoint:	0x401200
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:	0x57541720 [Sun Jun 5 12:12:16 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:	e4e19abc2b8b3cdf6beeb846e51c393a2

Entrypoint Preview

Instruction

```
push 00401E68h
call 00007FA4E4FAD605h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ebp+7Eh], dh
adc ecx, esi
adc eax, 814B7AD7h
lds edi, dword ptr [esi+69h]
out 11h, eax
pop edi
dec ecx
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
inc edx
outsd
jc 00007FA4E4FAD676h
jc 00007FA4E4FAD663h
jc 00007FA4E4FAD681h
push 00000065h
arpl word ptr [ecx+esi+00h], si
or eax, 7061430Ah
je 00007FA4E4FAD67Bh
add byte ptr [eax], al
add byte ptr [eax], al
```

Instruction
dec esp
xor dword ptr [eax], eax
add ebp, dword ptr [edx-7712EC60h]
xchg ebx, ecx
dec edi
cwde
aad 57h
push es
jl 00007FA4E4FAD5BAh
xchg eax, esp
je 00007FA4E4FAD5C9h
add dl, byte ptr [esi-40h]
lds edx, edi
imul ecx, dword ptr [edx-7Ch], 28h
mov bl, 82h
mov ah, DDh
into

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd244	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x10000	0x8a8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0xc4	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xc5e8	0xd000	False	0.522047776442	data	5.84101863969	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0xe000	0x1158	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x10000	0x8a8	0x1000	False	0.135498046875	data	1.28818251933	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x10340	0x568	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x1032c	0x14	data		
RT_VERSION	0x100f0	0x23c	data	English	United States


Imports

DLL	Import
MSVBVM60.DLL	__vbaCyForInit, __Clicos, __adj_fptan, __vbaFreeVar, __vbaEnd, __adj_fdiv_m64, __adj_fprem1, __vbaStrCat, __vbaHresultCheckObj, __adj_fdiv_m32, __vbaObjSet, __adj_fdiv_m16i, __adj_fdivr_m16i, __vbaVarTstLt, __Clsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaCyl2, __vbaStrCmp, __vbaCyl4, __adj_fpatan, EVENT_SINK_Release, __CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptionHandler, __adj_fprem, __adj_fdivr_m64, __vbaFPException, __vbaCyForNext, __Cilog, __vbaNew2, __adj_fdiv_m32i, __adj_fdivr_m32i, __vbaI4Str, __vbaFreeStrList, __adj_fdivr_m32, __adj_fdiv_r, __Clatan, __vbaStrMove, __allmul, __Cltan, __Clexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0409 0x04b0
InternalName	Iranske
FileVersion	2.00
CompanyName	Axis Corp
Comments	Axis Corp
ProductName	Project1
ProductVersion	2.00
OriginalFilename	Iranske.exe

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: SPPG contract 9200355_Acma Engineers SP Power_Contract No 9200355.exe PID: 6072 Parent PID: 5648

General

Start time:	22:02:04
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\SPPG contract 9200355_Acma Engineers SP Power_Contract No 9200355.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SPPG contract 9200355_Acma Engineers SP Power_Contract No 9200355.exe'
Imagebase:	0x400000
File size:	65536 bytes
MD5 hash:	276D1A6D58CC96BEC4CCF5F19D395170
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

Disassembly

Code Analysis