ID: 358442
Sample Name: Product Order 2070121_SN-WS.scr
Cookbook: default.jbs
Time: 16:13:14
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

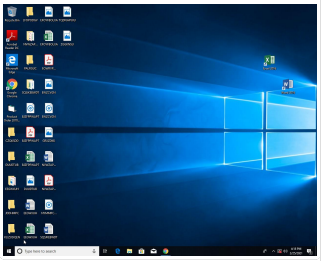
Analysis Report Product Order 2070121_SN-WS.scr

Overview

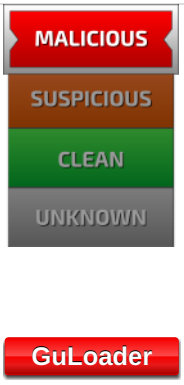
General Information

Sample Name:	Product Order 2070121_SN-WS.scr (renamed file extension from scr to exe)
Analysis ID:	358442
MD5:	1c6aec49b015d3..
SHA1:	9cfbd68f389d410..
SHA256:	e1fdbaebafc61e8..
Tags:	GuLoader scr
Infos:	

Most interesting Screenshot:



Detection

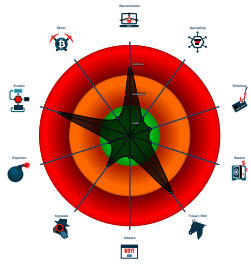


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Potential malicious icon found
- Yara detected GuLoader
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Initial sample is a PE file and has a …
- 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 read the PEB
- Creates a DirectInput object (often fo…
- Detected potential crypto function
- PE file contains strange resources

Classification



Startup

- **System is w10x64**
- Product Order 2070121_SN-WS.exe (PID: 6336 cmdline: 'C:\Users\user\Desktop\Product Order 2070121_SN-WS.exe' MD5: 1C6AEC49B015D3AE4BEE86B84BB37A42)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

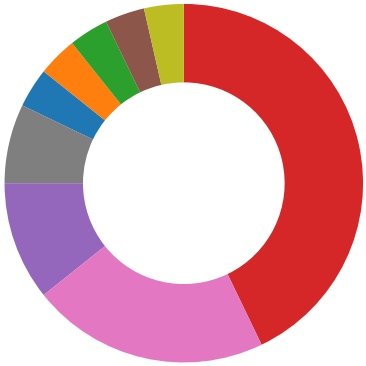
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: Product Order 2070121_SN-WS.exe PID: 6336	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: Product Order 2070121_SN-WS.exe PID: 6336	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- 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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Compliance:

Uses 32bit PE files

System Summary:

Potential malicious icon found

Initial sample is a PE file and has a suspicious name

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)

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

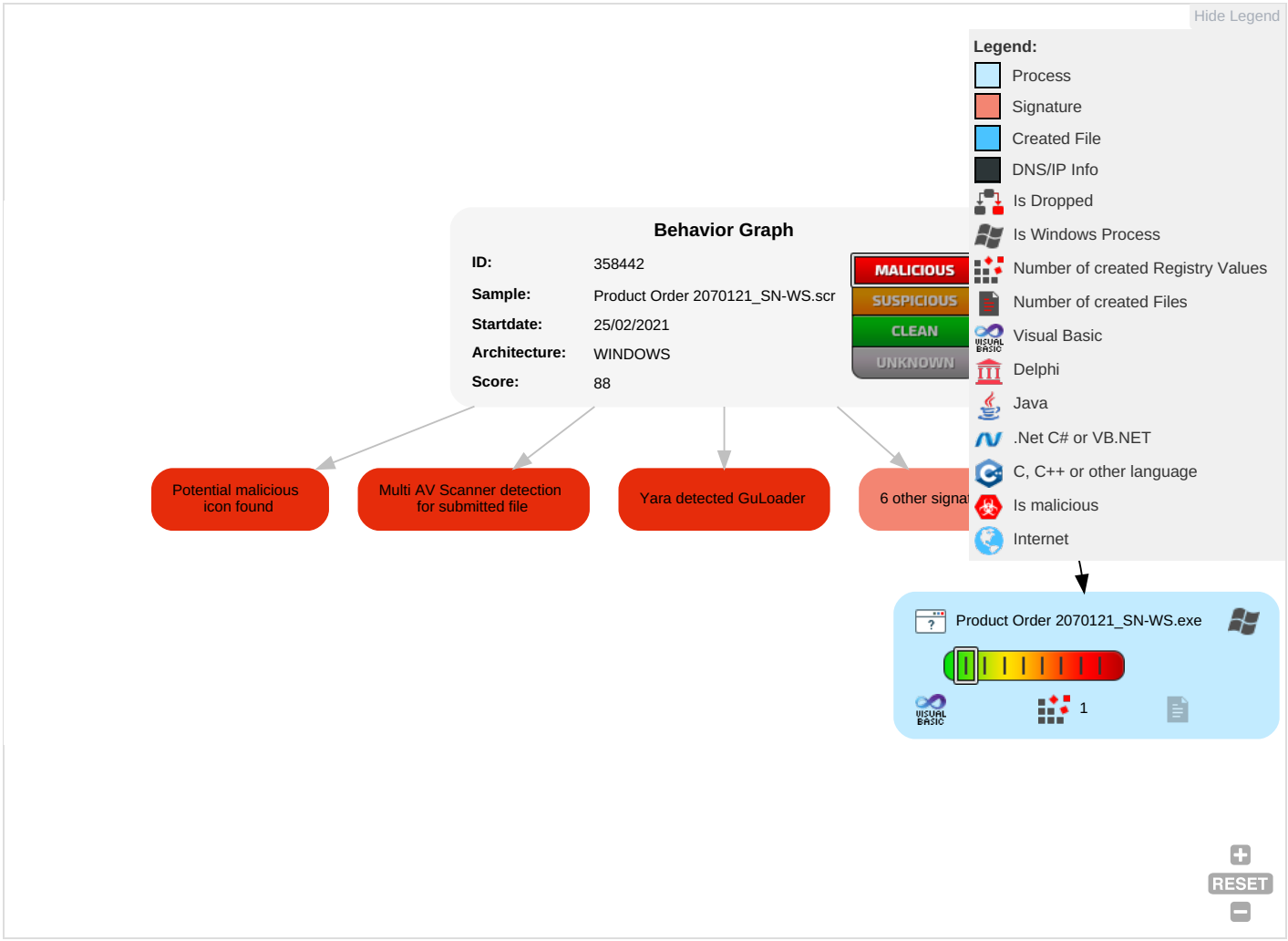
Tries to detect virtualization through RDTSC time measurements

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
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Process Injection 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 Communication	Remotely Track Device Without Authorization
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	Archive Collected Data 1	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	System Information Discovery 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups

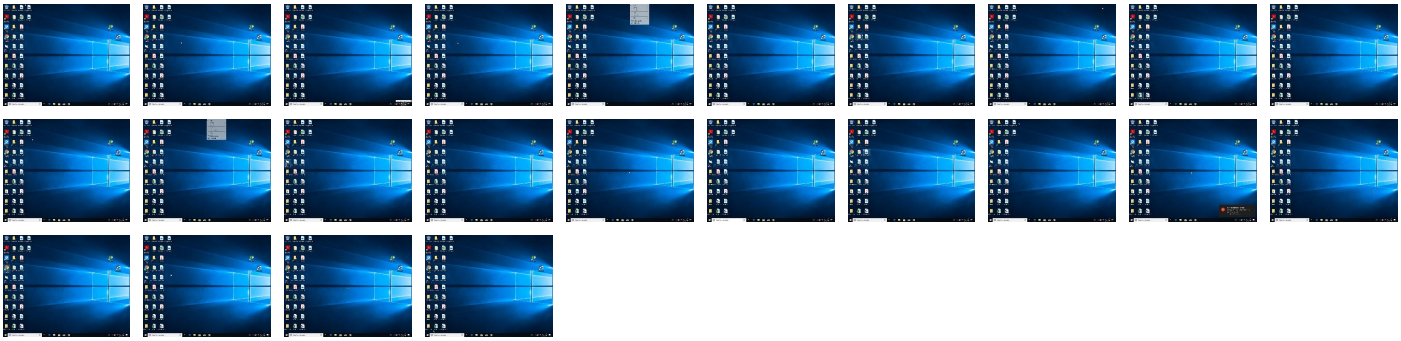
Behavior Graph



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
Product Order 2070121_SN-WS.exe	35%	Virustotal		Browse
Product Order 2070121_SN-WS.exe	13%	ReversingLabs	Win32.Trojan.Generic	

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 Emerald
Analysis ID:	358442
Start date:	25.02.2021
Start time:	16:13:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Product Order 2070121_SN-WS.scr (renamed file extension from scr to 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:	27
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:	mal88.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 43.7% (good quality ratio 17.3%) • Quality average: 24.4% • Quality standard deviation: 31.8%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Report size exceeded maximum capacity and may have missing disassembly code.

Simulations

Behavior and APIs

No simulations
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):	5.963684213640259
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:	Product Order 2070121_SN-WS.exe
File size:	86016
MD5:	1c6aec49b015d3ae4bee86b84bb37a42
SHA1:	9cfbd68f389d4106557b7daea67bb95b8c51eea7
SHA256:	e1fdbaebafc61e8a7d21913134e3c83104805f2bdb932525108da2f3c35176ee
SHA512:	7748c9a652985fe0ebc938d0e005e4df308f780f1c24aa050f1de7a1d0bdcf6fd5c64eef6e964b3482d5ce5f263891e03280e708b8ce8fe76a8cd480c421e686
SSDEEP:	768:4GKC47Ovmr1ITWNFq22edVGTaExG7iTho+FW99+oeKDklyVdbTD3PtrkwXTX0fRC:5whVFq2fVKxuic9fLLxk4AfRtQ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L.....7`..... ...0.....0....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x4014bc
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:	0x6037868D [Thu Feb 25 11:14:21 2021 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:	3a6673b23cf9b03cd6b926c02ab84460

Entrypoint Preview

Instruction
push 00401778h
call 00007FFB20570A83h
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 [eax-74h], ah
fisttp word ptr [edx-76h]
cmove ecx, dword ptr [edx-44h]
inc edi
push esp
add al, 7Bh
mov ebp, 0000EEFFh
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
and byte ptr [6C432220h], bh
dec esp
popad
jns 00007FFB20570AF6h
insb
outsd
arpl word ptr [ebx+00h], bp
or al, byte ptr [ebx+6Ch]
imul esp, dword ptr [ebp+6Eh], 00000000h
dec esp
xor dword ptr [eax], eax
or esi, dword ptr [ebp-6E6D277Bh]
aam 81h
dec ebp

Instruction
test dword ptr [ecx+1492B737h], esp
mov cl, A1h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x125c4	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x15000	0xa48	.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	0x120	.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	0x11ad0	0x12000	False	0.453830295139	data	6.50011548254	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x13000	0x11bc	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x15000	0xa48	0x1000	False	0.18896484375	data	2.2831350237	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x15918	0x130	data		
RT_ICON	0x15630	0x2e8	data		
RT_ICON	0x15508	0x128	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x154d8	0x30	data		
RT_VERSION	0x15150	0x388	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, __vbaLenBstrB, _adj_fdiv_m32, __vbaAryDestruct, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, _adj_fdivr_m16i, __vbaVarTstLt, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, __vbaVarTstEq, _adj_fpatan, __vbaLateIdCallLd, __vbaRedim, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaI2Str, __vbaFPException, __vbaInStrVar, _CIlog, __vbaNew2, __vbaR8Str, __vbaInStr, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, __vbaDerefAry1, _adj_fdivr_m32, _adj_fdiv_r, __vbaI4Var, __vbaVarAdd, __vbaLateMemCall, __vbaVarDup, __vbaFpI4, _CIatan, __vbaStrMove, __vbaCastObj, _allmul, __vbaLateIdSt, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0409 0x04b0
LegalCopyright	Copyright 2016-2021 Proton Clear
InternalName	Reselects1
FileVersion	1.00
CompanyName	Proton Clear Inc.
LegalTrademarks	Copyright 2016-2021 Proton Clear
Comments	Proton Clear
ProductName	Proton Clear
ProductVersion	1.00
FileDescription	ProtonClear

Description	Data
OriginalFilename	Reselects1.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: Product Order 2070121_SN-WS.exe PID: 6336 Parent PID: 5640

General

Start time:	16:14:01
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\Product Order 2070121_SN-WS.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Product Order 2070121_SN-WS.exe'
Imagebase:	0x400000
File size:	86016 bytes
MD5 hash:	1C6AEC49B015D3AE4BEE86B84BB37A42
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\VB and VBA Program Settings	success or wait	1	660E2872	RegCreateKeyW
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\VAGTPOSTERS	success or wait	1	660E2872	RegCreateKeyW
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\VAGTPOSTERS\Taylorismens	success or wait	1	660E2872	RegCreateKeyW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\VAGTPOSTERS\Taylorismens	Forsrget	unicode	Vareprves4	success or wait	1	660E2183	RegSetValueExW

Disassembly

Code Analysis