

JoeSandbox Cloud BASIC



**ID:** 434933

**Sample Name:** PRICE-  
(BPS).exe

**Cookbook:** default.jbs

**Time:** 16:54:29

**Date:** 15/06/2021

**Version:** 32.0.0 Black Diamond


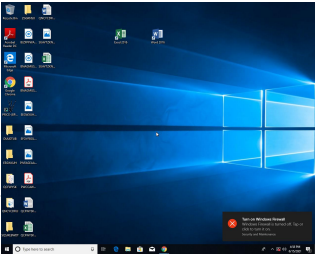
## Table of Contents

Table of Contents	2
Windows Analysis Report PRICE-(BPS).exe	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Threatname: GuLoader	3
Yara Overview	3
Initial Sample	3
Memory Dumps	3
Unpacked PEs	3
Sigma Overview	4
Signature Overview	4
AV Detection:	4
Networking:	4
Data Obfuscation:	4
Malware Analysis System Evasion:	4
Anti Debugging:	4
Mitre Att&ck Matrix	4
Behavior Graph	5
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	6
Domains	6
URLs	6
Domains and IPs	6
Contacted Domains	7
Contacted URLs	7
Contacted IPs	7
General Information	7
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	8
IPs	8
Domains	8
ASN	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	8
General	8
File Icon	8
Static PE Info	8
General	9
Entrypoint Preview	9
Data Directories	9
Sections	9
Resources	9
Imports	9
Version Infos	9
Possible Origin	9
Network Behavior	9
Code Manipulations	9
Statistics	9
System Behavior	10
Analysis Process: PRICE-(BPS).exe PID: 632 Parent PID: 5548	10
General	10
File Activities	10
Disassembly	10
Code Analysis	10

# Windows Analysis Report PRICE-(BPS).exe

## Overview

### General Information

Sample Name:	PRICE-(BPS).exe
Analysis ID:	434933
MD5:	a75c6c6953a362..
SHA1:	36c2485f9bec118..
SHA256:	19a93cf55d422bf..
Tags:	exe
Infos:	
Most interesting Screenshot:	
	

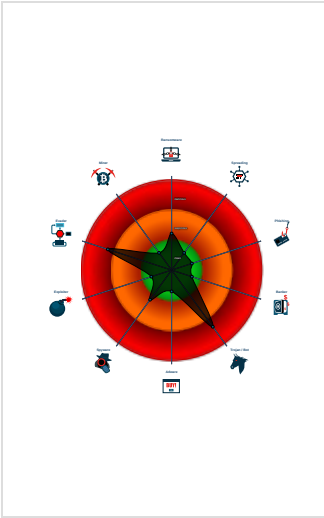
### Detection

<div><div>MALICIOUS</div><div>SUSPICIOUS</div><div>CLEAN</div><div>UNKNOWN</div></div>	
<div>GuLoader</div>	
Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

### Signatures

Found malware configuration
Yara detected GuLoader
C2 URLs / IPs found in malware con...
Contains functionality to detect hard...
Found potential dummy code loops (...)
Abnormal high CPU Usage
Contains functionality for execution ...
Contains functionality to call native f...
Contains functionality to query CPU ...
Contains functionality to read the PEB
Detected potential crypto function
PE file contains strange resources

### Classification



## Process Tree

System is w10x64
 PRICE-(BPS).exe (PID: 632 cmdline: 'C:\Users\user\Desktop\PRICE-(BPS).exe' MD5: A75C6C6953A362788C54B36EC7F8DBF2)
cleanup

## Malware Configuration

### Threatname: GuLoader

<pre>{   "Payload URL": "https://onedrive.live.com/download?cid=4775355831E91CD1&amp;resid=4775355831E91CD1%215798&amp;authkey=ADoN1Lkq2uILQT4Z" }</pre>
--

## Yara Overview

### Initial Sample

Source	Rule	Description	Author	Strings
PRICE-(BPS).exe	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

### Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.201011246.0000000000040 1000.00000020.00020000.sdmp	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	
00000000.00000002.580142915.0000000000040 1000.00000020.00020000.sdmp	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

### Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.PRICE-(BPS).exe.400000.0.unpack	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	
0.2.PRICE-(BPS).exe.400000.0.unpack	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

## Sigma Overview

No Sigma rule has matched

## Signature Overview



Click to jump to signature section

### AV Detection:



Found malware configuration

### Networking:



C2 URLs / IPs found in malware configuration

### Data Obfuscation:



Yara detected GuLoader

### Malware Analysis System Evasion:



Contains functionality to detect hardware virtualization (CPUID execution measurement)

### Anti Debugging:

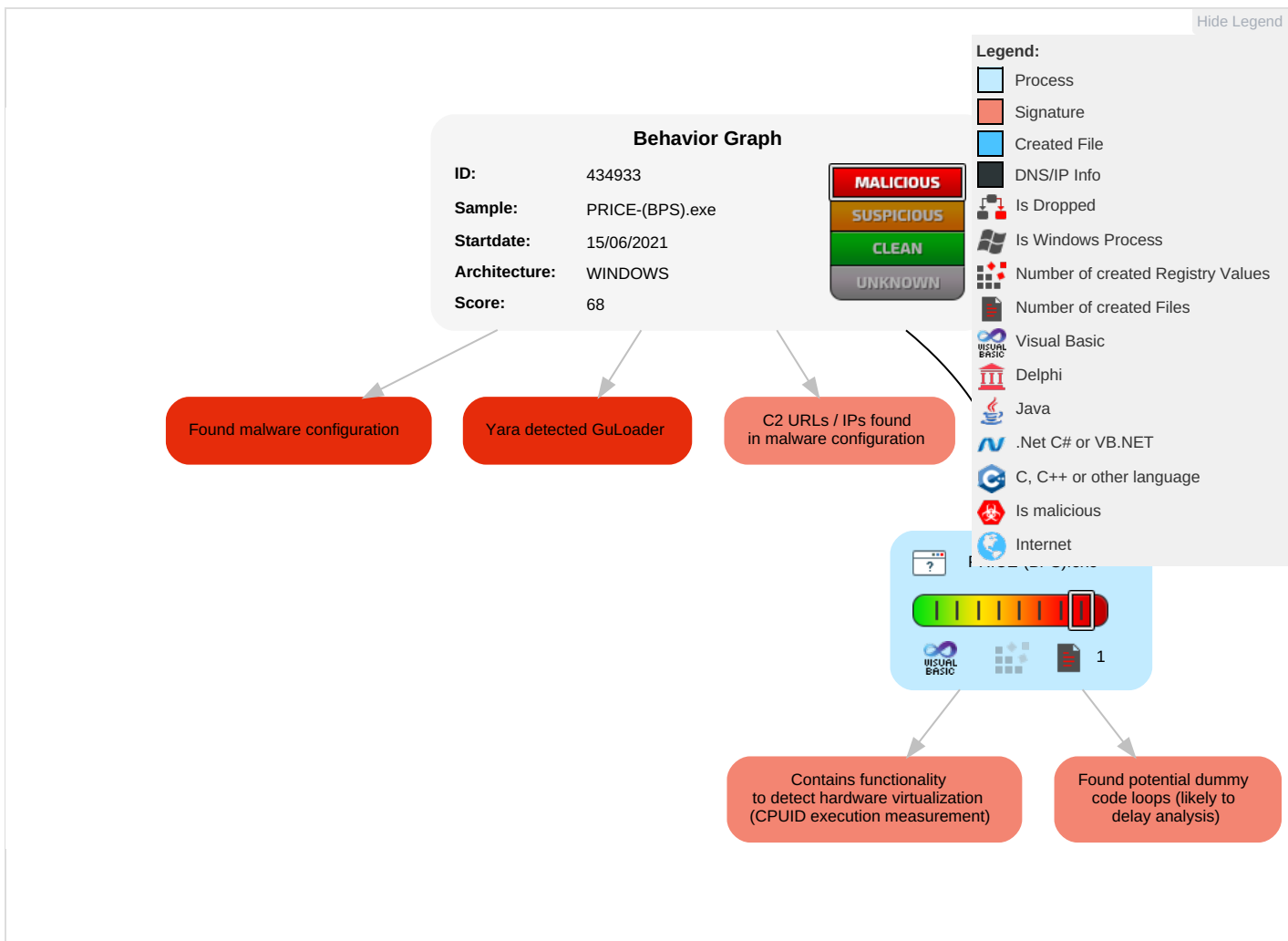


Found potential dummy code loops (likely to delay analysis)

## 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	OS Credential Dumping	Security Software Discovery 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	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	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	Recovery
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 to Track Device Location	Recovery
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 1 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	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

No Antivirus matches

### 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=4775355831E91CD1&resid=4775355831E91CD1%215798&authkey=ADoN1Lkq2uilQT4Z	false		high

## Contacted IPs

No contacted IP infos

## General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	434933
Start date:	15.06.2021
Start time:	16:54:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PRICE-(BPS).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:	30
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"><li>• HCA enabled</li><li>• EGA enabled</li><li>• HDC enabled</li><li>• AMSI enabled</li></ul>
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	Failed
Cookbook Comments:	<ul style="list-style-type: none"><li>• Adjust boot time</li><li>• Enable AMSI</li><li>• Found application associated with file extension: .exe</li><li>• Override analysis time to 240s for sample files taking high CPU consumption</li></ul>
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

No created / dropped files found

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.944349649221438
TrID:	<ul style="list-style-type: none"><li>Win32 Executable (generic) a (10002005/4) 99.15%</li><li>Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81%</li><li>Generic Win/DOS Executable (2004/3) 0.02%</li><li>DOS Executable Generic (2002/1) 0.02%</li><li>Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%</li></ul>
File name:	PRICE-(BPS).exe
File size:	270336
MD5:	a75c6c6953a362788c54b36ec7f8dbf2
SHA1:	36c2485f9bec118660d3dcfb60e4b184c01c5d61
SHA256:	19a93cf55d422bf9dcca2ece46b98704248641f86ca7ed2a21d903c724c79a53
SHA512:	f46923ff9169e4339462c589eebc6cc4f2f3523331c6b929a25f9bb1d85fdcc893ce613a2184cbe716e599c706e8eafa931e0546e70afe2fe5d166834c41a5f
SSDEEP:	3072:goQ3J7Mb+bnPdajl+dJrODGqrK9+p7r2qrFx0fi0XdtaHS2Jp:M1aO+eDdrw+pXpxU73l
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode...\$......c.S..... .....&.....\$.Rich.....PE..L...w@WJ..... .....0.....(.....@.....

File Icon

	
Icon Hash:	6828bae9d2777576

Static PE Info



<b>General</b>		
Entrypoint:		0x402894
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:		0x4A574077 [Fri Jul 10 13:21:59 2009 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:		adaafa2c180ecb7addf1201d12c8322

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x3e68c	0x3f000	False	0.293794177827	data	6.07796755742	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x40000	0x1be8	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x42000	0x9d0	0x1000	False	0.225830078125	data	2.1244697174	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: PRICE-(BPS).exe PID: 632 Parent PID: 5548

### General

Start time:	16:55:17
Start date:	15/06/2021
Path:	C:\Users\user\Desktop\PRICE-(BPS).exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PRICE-(BPS).exe'
Imagebase:	0x400000
File size:	270336 bytes
MD5 hash:	A75C6C6953A362788C54B36EC7F8DBF2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	<ul style="list-style-type: none"><li>Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000000.00000000.201011246.0000000000401000.00000020.00020000.sdmp, Author: Joe Security</li><li>Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000000.00000002.580142915.0000000000401000.00000020.00020000.sdmp, Author: Joe Security</li></ul>
Reputation:	low

### File Activities

Show Windows behavior

## Disassembly

### Code Analysis