

JoeSandbox Cloud BASIC



**ID:** 458355

**Sample Name:** Fec9qUX4at.exe

**Cookbook:** default.jbs

**Time:** 09:40:10

**Date:** 03/08/2021

**Version:** 33.0.0 White Diamond


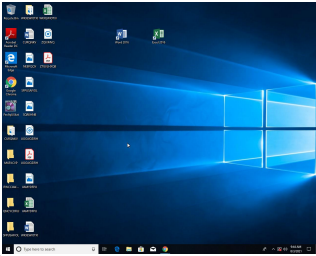
## Table of Contents

Table of Contents	2
Windows Analysis Report Fec9qUX4at.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
Memory Dumps	3
Sigma Overview	3
Jbx 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	4
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	7
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	9
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	10
System Behavior	10
Analysis Process: Fec9qUX4at.exe PID: 6536 Parent PID: 5808	10
General	10
File Activities	10
Disassembly	10
Code Analysis	10

# Windows Analysis Report Fec9qUX4at.exe

## Overview

### General Information

Sample Name:	Fec9qUX4at.exe
Analysis ID:	458355
MD5:	2046b941817392..
SHA1:	843d243a71131b..
SHA256:	c0d3da1cefd1a97..
Tags:	exe
Infos:	
Most interesting Screenshot:	
	

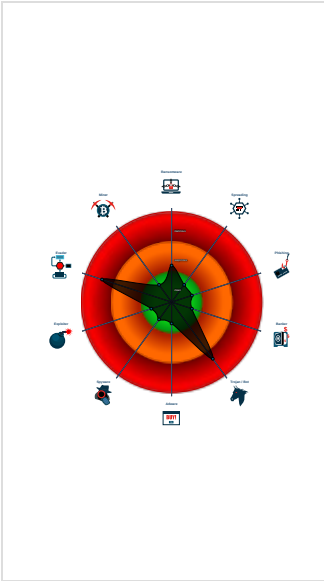
### Detection

<div><div>MALICIOUS</div><div>SUSPICIOUS</div><div>CLEAN</div><div>UNKNOWN</div></div> <div>GuLoader</div>	
Score:	88
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...
Contains functionality to detect hard...
Detected RDTSC dummy instruction...
Found potential dummy code loops (...)
Machine Learning detection for samp...
Tries to detect virtualization through...
Abnormal high CPU Usage
Contains functionality for execution ...
Contains functionality to call native f...
Contains functionality to read the PEB
Detected potential crypto function

### Classification



## Process Tree

- System is w10x64
-  Fec9qUX4at.exe (PID: 6536 cmdline: 'C:\Users\user\Desktop\Fec9qUX4at.exe' MD5: 2046B941817392E3815535FCCB1F39DC)
- cleanup

## Malware Configuration

### Threatname: GuLoader

```
{
  "Payload URL": "http://101.99.94.119/WEALTH_fkHgIQyCX0188.bin"
}
```

## Yara Overview

### Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.1174329957.0000000002B 20000.00000040.00000001.sdmf	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

Machine Learning detection for sample

### 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)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect virtualization through RDTSC time measurements

### Anti Debugging:

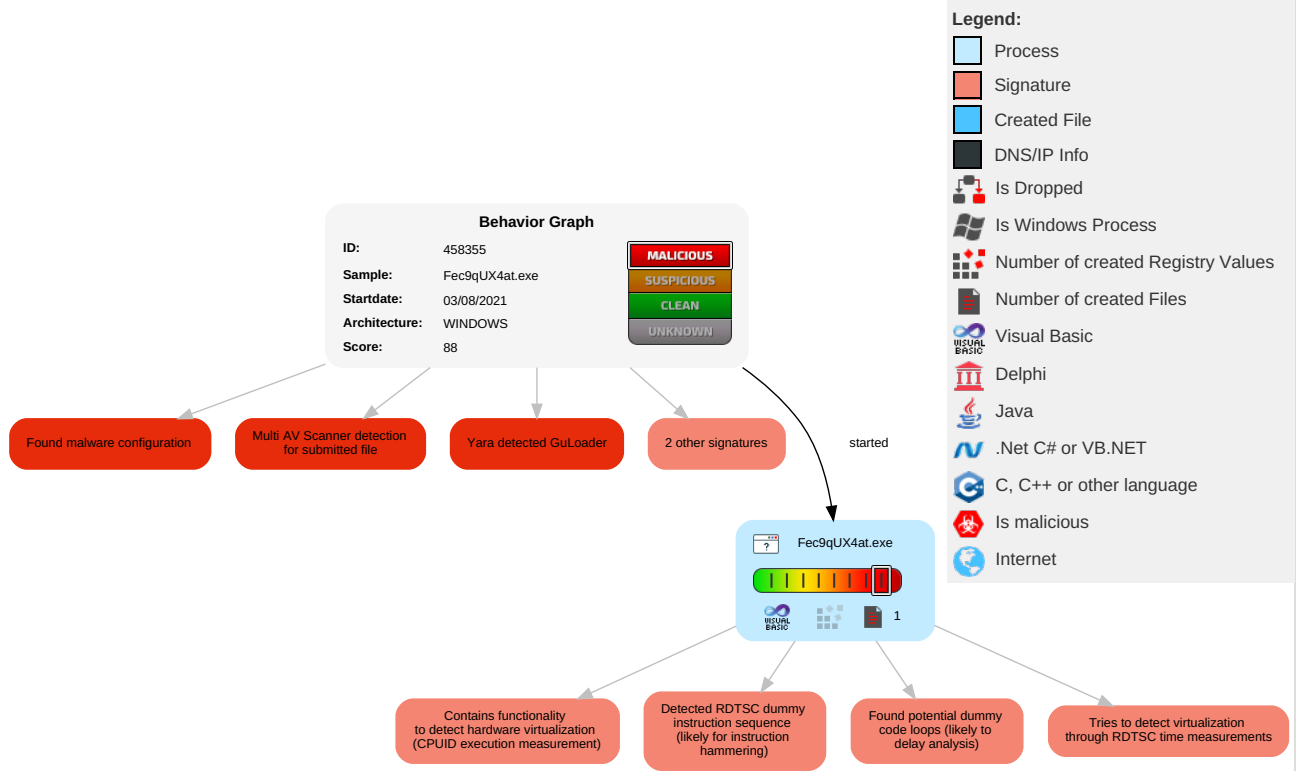


Found potential dummy code loops (likely to delay analysis)

## Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Reputation
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 4 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Reputation
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	Reputation
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	Reputation
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	System Information Discovery 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Reputation

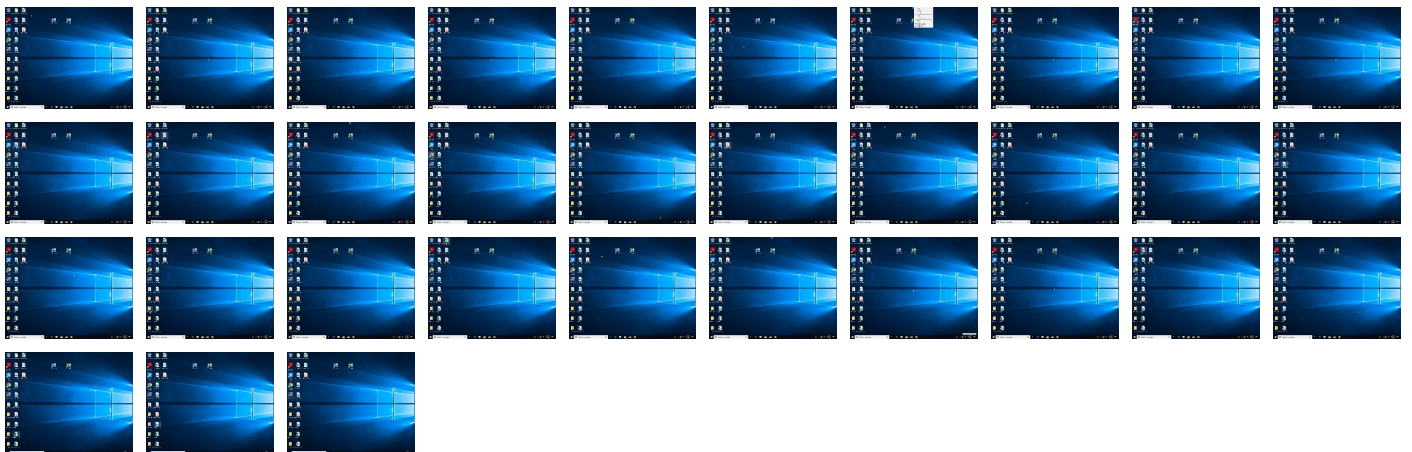
## Behavior Graph



## 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
Fec9qUX4at.exe	29%	Virustotal		<a href="#">Browse</a>
Fec9qUX4at.exe	13%	ReversingLabs	Win32.Trojan.Vebzenpak	
Fec9qUX4at.exe	100%	Joe Sandbox ML		

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

Source	Detection	Scanner	Label	Link
<a href="http://101.99.94.119/WEALTH_fkWglQyCXO188.bin">http://101.99.94.119/WEALTH_fkWglQyCXO188.bin</a>	0%	Avira URL Cloud	safe	

## Domains and IPs

### Contacted Domains

No contacted domains info

### Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://101.99.94.119/WEALTH_fkWglQyCXO188.bin	true	<ul style="list-style-type: none"><li>Avira URL Cloud: safe</li></ul>	unknown

### Contacted IPs

No contacted IP infos

## General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458355
Start date:	03.08.2021
Start time:	09:40:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Fec9qUX4at.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:	16
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:	mal88.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none"><li>Successful, ratio: 26% (good quality ratio 9.9%)</li><li>Quality average: 22.4%</li><li>Quality standard deviation: 33.9%</li></ul>
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):	6.638949072783339
TrID:	<ul style="list-style-type: none"><li>Win32 Executable (generic) a (10002005/4) 99.96%</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:	Fec9qUX4at.exe
File size:	114688
MD5:	2046b941817392e3815535fccb1f39dc
SHA1:	843d243a71131baf9fbe0fc4ba129f51ee74c8f
SHA256:	c0d3da1cefd1a979c8b8ce102fd5d3ff090779f72f4d1098eb383cbbb3480bee
SHA512:	ecf0b711c41619dcf9073f1cd4c769cc106b04aaec40881fc11cbf8686989da512a9c2ee2683a90b99dddb1f4a762cf4df512663519bc9035bbc6d0fd90f9571
SSDEEP:	1536:BUS3/zw2m3c39SYeXvmgU2sIMfWub4cL51tY4SQmiPYElZ943ckw2mUS3:/BT/zM3c3bcBSIMfQuDaSZS3ckYT/
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.....(U.....@.....D.....P....@.....

File Icon





Icon Hash:

d5d5959595959595

Static PE Info

General

Entrypoint:	0x401144
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:	0x558D28E4 [Fri Jun 26 10:26:44 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:	5565993a5a9f2bfb76f28ab304be6bc1

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x13de4	0x14000	False	0.648803710938	data	7.05513425915	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x15000	0x115c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x17000	0x5b92	0x6000	False	0.545776367188	data	6.0293757353	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
Chinese	Taiwan	

Network Behavior

No network behavior found

Code Manipulations

## Statistics

## System Behavior

Analysis Process: Fec9qUX4at.exe PID: 6536 Parent PID: 5808

### General

Start time:	09:40:59
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Fec9qUX4at.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Fec9qUX4at.exe'
Imagebase:	0x400000
File size:	114688 bytes
MD5 hash:	2046B941817392E3815535FCCB1F39DC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	<ul style="list-style-type: none"><li>Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.1174329957.0000000002B20000.00000040.00000001.sdmp, Author: Joe Security</li></ul>
Reputation:	low

### File Activities

Show Windows behavior

## Disassembly

### Code Analysis