ID: 531949
Sample Name: K5hW6I5xeA
Cookbook: default.jbs
Time: 15:23:16
Date: 01/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

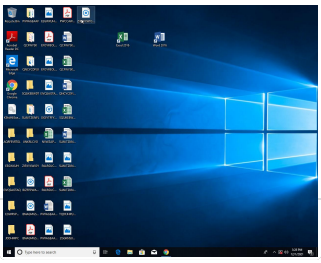
Windows Analysis Report K5hW6I5xeA

Overview

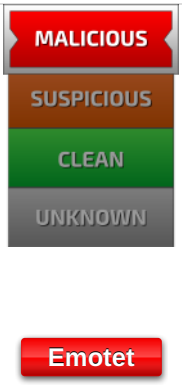
General Information

Sample Name:	K5hW6I5xeA (renamed file extension from none to dll)
Analysis ID:	531949
MD5:	d89375ecbc2638..
SHA1:	d9cd4340910bd1..
SHA256:	e523b545ce399c..
Tags:	32 dll exe trojan
Infos:	

Most interesting Screenshot:



Detection

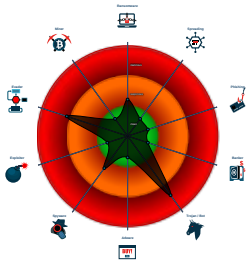


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Emotet
- Multi AV Scanner detection for subm…
- Tries to detect virtualization through…
- Creates a DirectInput object (often fo…
- Uses 32bit PE files
- Contains functionality to check if a d…
- Contains functionality to read the PEB
- Uses code obfuscation techniques (…
- Detected potential crypto function
- Contains functionality to query CPU …
- Uses Microsoft's Enhanced Cryptog…
- Contains functionality which may be…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6692 cmdline: loaddll32.exe "C:\Users\user\Desktop\K5hW6I5xeA.dll" MD5: 72FCD8FB0ADC38ED9050569AD673650E)
  - cmd.exe (PID: 4592 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\K5hW6I5xeA.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5880 cmdline: rundll32.exe "C:\Users\user\Desktop\K5hW6I5xeA.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 4344 cmdline: rundll32.exe C:\Users\user\Desktop\K5hW6I5xeA.dll,Control_RunDLL MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6376 cmdline: rundll32.exe C:\Users\user\Desktop\K5hW6I5xeA.dll,ewjabexomfikq MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6752 cmdline: rundll32.exe C:\Users\user\Desktop\K5hW6I5xeA.dll,fkehpgdsrju MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.914221138.0000000004D30000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000009.00000002.914221138.0000000004D30000.00000040.00000001.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.rundll32.exe.4d30000.0.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
9.2.rundll32.exe.4d30000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
9.2.rundll32.exe.4d30000.0.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
9.2.rundll32.exe.4d30000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

E-Banking Fraud:

Yara detected Emotet

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

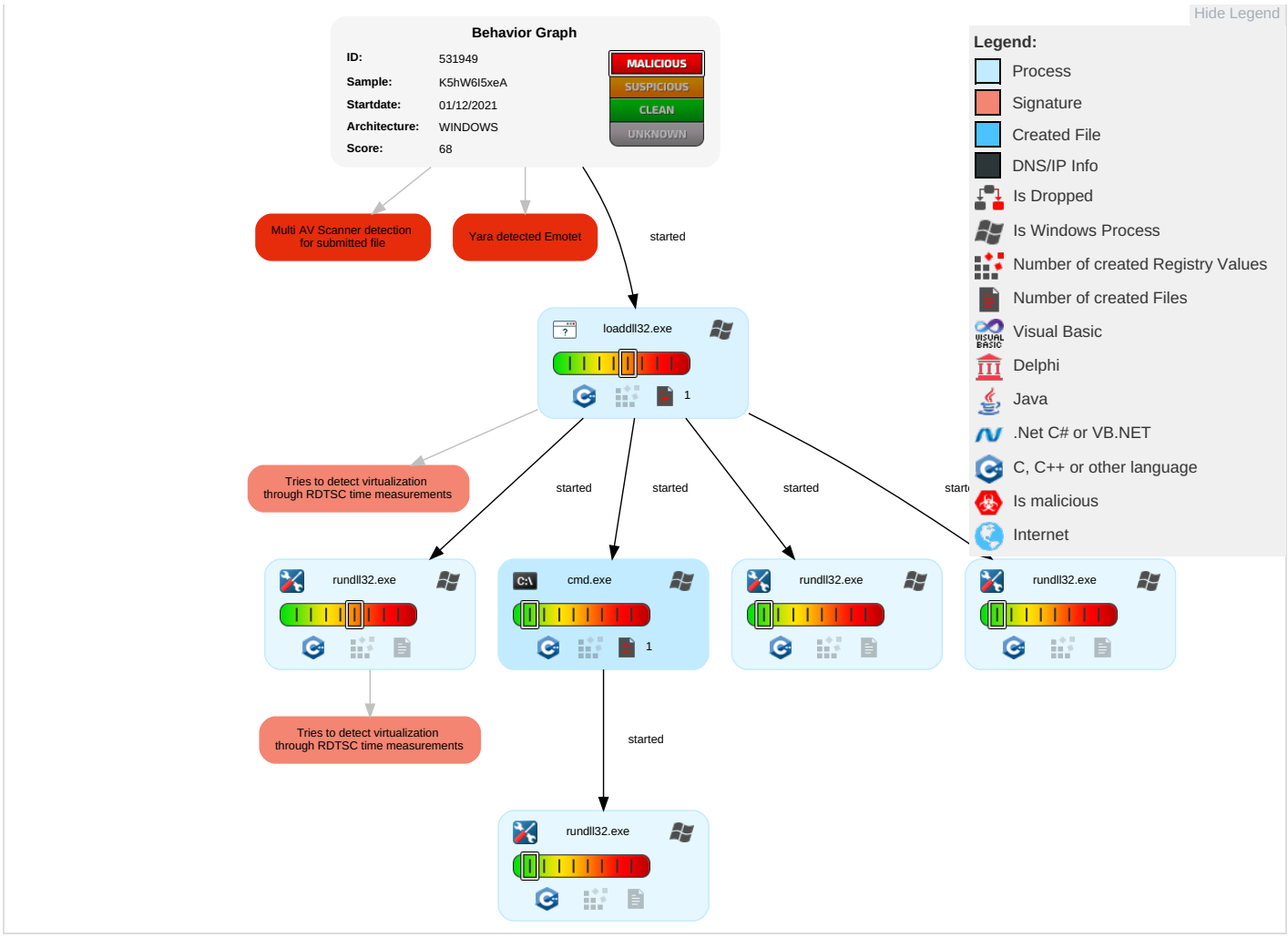
Stealing of Sensitive Information:

Yara detected Emotet

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 2	Rundll32 1	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Dev Without Authorizati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Security Software Discovery 1 3	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizati
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	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

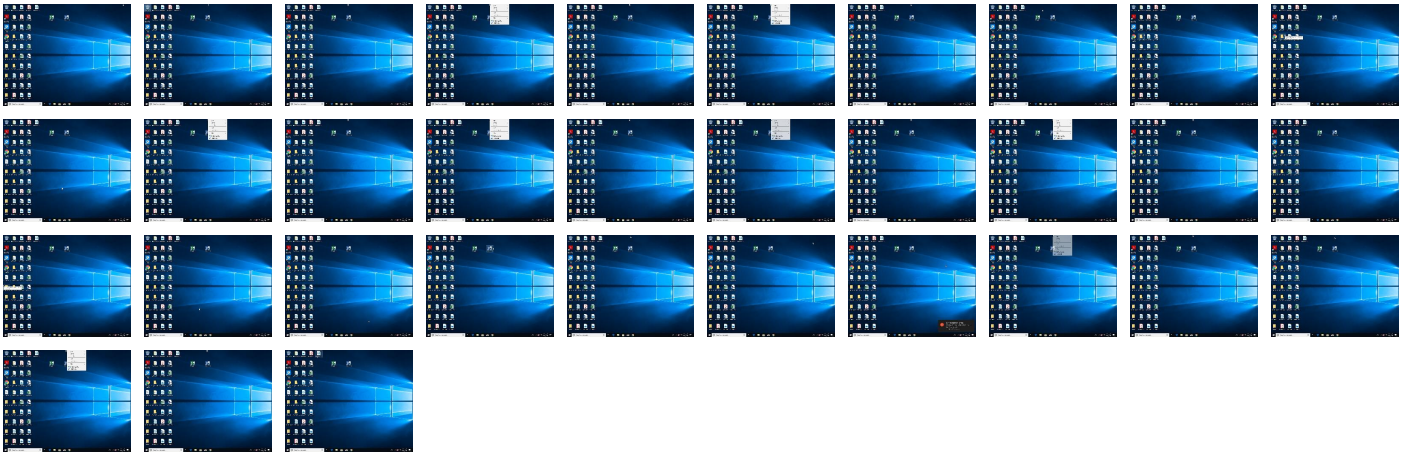
Behavior Graph



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
K5hW6I5xeA.dll	28%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.2.rundll32.exe.4d30000.0.unpack	100%	Avira	HEUR/AGEN.1110387		Download File

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:	531949
Start date:	01.12.2021
Start time:	15:23:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	K5hW6I5xeA (renamed file extension from none to dll)
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:	17
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:	mal68.troj.evad.winDLL@11/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 89.5%) • Quality average: 75.8% • Quality standard deviation: 32.9%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32
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 (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.673697209310638
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	K5hW6I5xeA.dll
File size:	273920
MD5:	d89375ecbc2638d71f6cc446947adb71
SHA1:	d9cd4340910bd1dd2f3d576fd7ea5fdfd6671060
SHA256:	e523b545ce399ceb37ba1fb400ba5e7a285e6d4c1e3ae5bbd5607ce538b64ac7
SHA512:	46a132edd6e8765b11d14a2dd995617fcffe04c081a028b7339f06db7653ec2ea91870fc123bc21cab39c84bbecf70c6a08a6e1e72705835697790a813773ba0
SSDEEP:	6144:I+/WjBDXCrZukVAAYCcVwnmU3PbnvOWRPyrLzP:lWGACc2PlRKrLzP
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....}.`d9..79..79..7J..63..7J..6...7J..6+..7k..6%..7k..66..7k..6+..7J..6:..79..7k..7...60..7...68..7...78..7...68..7Rich9..7.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10003583
Entrypoint Section:	.text

General

Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61A7688F [Wed Dec 1 12:20:31 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	3bc41ab907dcf32970630360a7a2019f

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xc387	0xc400	False	0.582011320153	data	6.66250995052	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xe000	0x34b56	0x34c00	False	0.730320645735	data	6.21371435728	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x43000	0x30d0	0x800	False	0.16357421875	data	2.04808247088	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x47000	0xf8	0x200	False	0.3359375	data	2.52739185048	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x48000	0xea4	0x1000	False	0.763671875	data	6.28630296444	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6692 Parent PID: 5724

General

Start time:	15:24:09
Start date:	01/12/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\K5hW6I5xeA.dll"
Imagebase:	0x240000
File size:	893440 bytes
MD5 hash:	72FCD8FB0ADC38ED9050569AD673650E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 4592 Parent PID: 6692

General

Start time:	15:24:09
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\K5hW6I5xeA.dll",#1
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 4344 Parent PID: 6692

General

Start time:	15:24:10
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\K5hW6I5xeA.dll,Control_RunDLL
Imagebase:	0x80000

File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 5880 Parent PID: 4592

General

Start time:	15:24:10
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\K5hW6I5xeA.dll",#1
Imagebase:	0x80000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 6376 Parent PID: 6692

General

Start time:	15:24:14
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\K5hW6I5xeA.dll,ewjabexomfikq
Imagebase:	0x80000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 6752 Parent PID: 6692

General

Start time:	15:24:18
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\K5hW6I5xeA.dll,fkehpgdsrju
Imagebase:	0x80000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000009.00000002.914221138.0000000004D30000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000009.00000002.914221138.0000000004D30000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Disassembly

Code Analysis