ID: 448941
Sample Name: 6ZV65nCMYQ
Cookbook: default.jbs
Time: 21:05:32
Date: 14/07/2021
Version: 33.0.0 White Diamond

Table of Contents

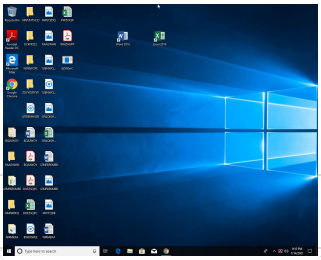
Windows Analysis Report 6ZV65nCMYQ

Overview

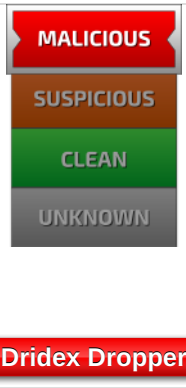
General Information

Sample Name:	6ZV65nCMYQ (renamed file extension from none to exe)
Analysis ID:	448941
MD5:	622f4aa2d5e8243.
SHA1:	b486db47021575..
SHA256:	277089cb78a9c4..
Tags:	32 exe
Infos:	

Most interesting Screenshot:



Detection



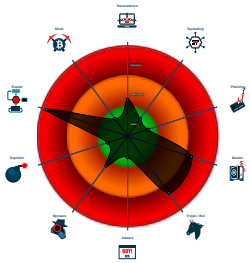
Dridex Dropper

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

Signatures

- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Dridex dropper found
- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Dridex unpacked file
- C2 URLs / IPs found in malware con…
- Found potential dummy code loops (…
- Machine Learning detection for samp…
- Tries to delay execution (extensive O…
- Tries to detect sandboxes / dynamic…
- Tries to detect virtualization through…

Classification



Process Tree

- **System is w10x64**
- 6ZV65nCMYQ.exe (PID: 6632 cmdline: 'C:\Users\user\Desktop\6ZV65nCMYQ.exe' MD5: 622F4AA2D5E82438F3A40A35AB4902D5)
- **cleanup**

Malware Configuration

Threatname: Dridex


```
{
  "Version": 22202,
  "C2 list": [
    "202.29.60.34:443",
    "66.175.217.172:13786",
    "78.46.78.42:9043"
  ],
  "RC4 keys": [
    "RQTJGOuDHeSyUCWzdNRZi3fWMitWY9aTc",
    "2UMW8pusQXiNJDgmuPITkf4TmrOt3Y13lRDWnjBuu16JkzjIG6gNuckQDkiut9pzQHVGfFdlT"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.1172561248.0000000010001000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.6ZV65nCMYQ.exe.10000000.0.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	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

Compliance:

Detected unpacking (overwrites its own PE header)

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Dridex dropper found

Yara detected Dridex unpacked file

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

Malware Analysis System Evasion:

Tries to delay execution (extensive OutputDebugStringW loop)

Tries to detect sandboxes / dynamic malware analysis system (file name check)

Tries to detect virtualization through RDTSC time measurements

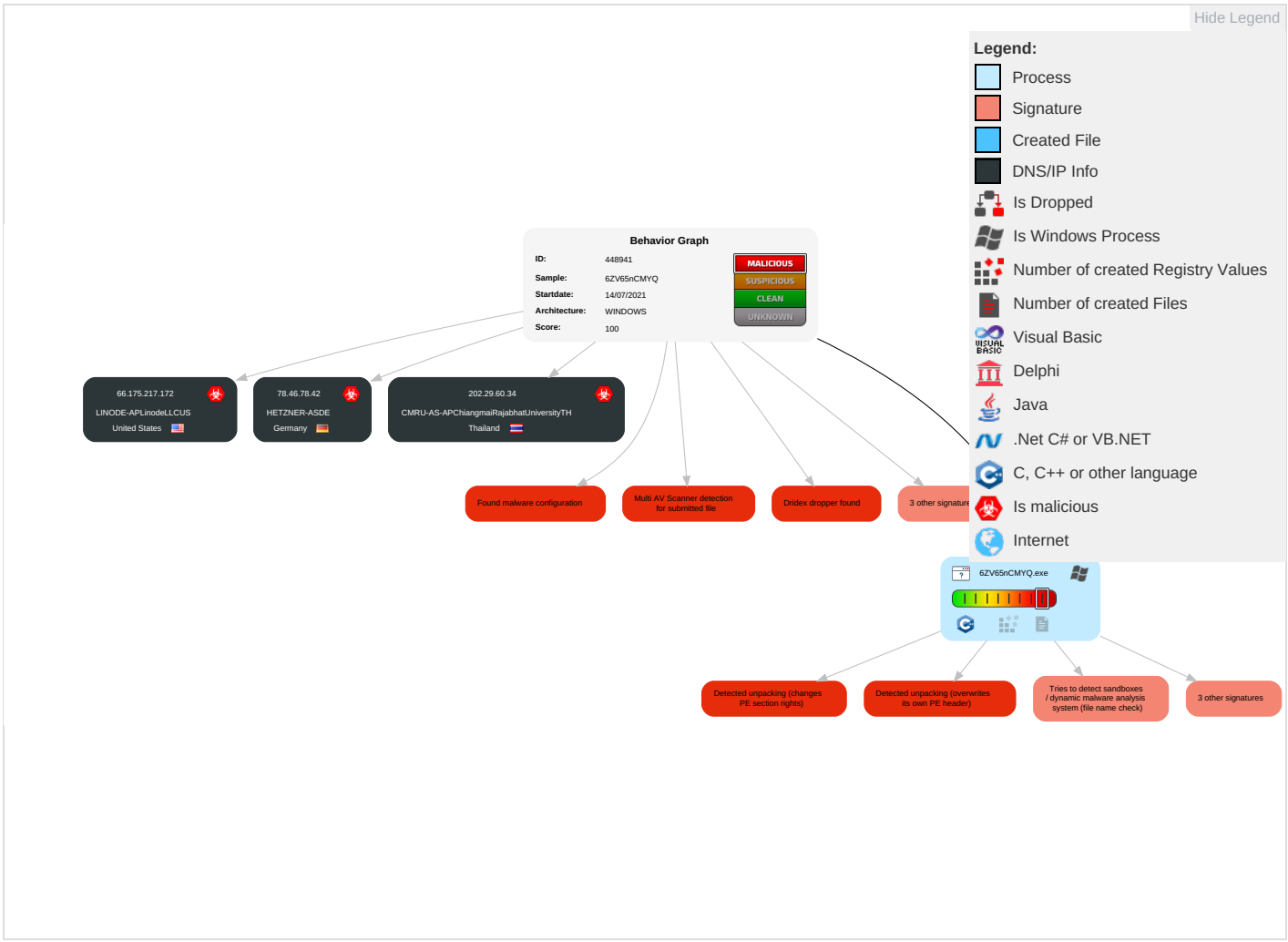
Anti Debugging:

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
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 3 1 1	OS Credential Dumping	Security Software Discovery 3 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Virtualization/Sandbox Evasion 3 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2 3	NTDS	Application Window 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	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

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
6ZV65nCMYQ.exe	30%	Virustotal		Browse
6ZV65nCMYQ.exe	35%	ReversingLabs	Win32.Trojan.Generic	
6ZV65nCMYQ.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.6ZV65nCMYQ.exe.10000000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
78.46.78.42	unknown	Germany		24940	HETZNER-ASDE	true
202.29.60.34	unknown	Thailand		24344	CMRU-AS-APChiangmaiRajabhatUniversityTH	true
66.175.217.172	unknown	United States		63949	LINODE-APLinodeLLCUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	448941
Start date:	14.07.2021
Start time:	21:05:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	6ZV65nCMYQ (renamed file extension from none 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:	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:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal100.bank.troj.evad.winEXE@1/0@0/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 99.6% (good quality ratio 98.3%) • Quality average: 80.9% • Quality standard deviation: 24%
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

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
78.46.78.42	nrQXlgp21m.exe	Get hash	malicious	Browse	
	m3d2gsRm5Q.exe	Get hash	malicious	Browse	
	4TWEQh2HJb.xls	Get hash	malicious	Browse	
	ldE25Snd1f.exe	Get hash	malicious	Browse	
	Receipt-6218387.xls	Get hash	malicious	Browse	
	BhAJLvq0c7.xls	Get hash	malicious	Browse	
	PFx3G8Snzk.exe	Get hash	malicious	Browse	
	9EP6Gxzv6F.xls	Get hash	malicious	Browse	
	2ejCKSIjIV.exe	Get hash	malicious	Browse	
	bQWApID6av.xls	Get hash	malicious	Browse	
202.29.60.34	nrQXlgp21m.exe	Get hash	malicious	Browse	
	m3d2gsRm5Q.exe	Get hash	malicious	Browse	
	4TWEQh2HJb.xls	Get hash	malicious	Browse	
	ldE25Snd1f.exe	Get hash	malicious	Browse	
	Receipt-6218387.xls	Get hash	malicious	Browse	
	BhAJLvq0c7.xls	Get hash	malicious	Browse	
	PFx3G8Snzk.exe	Get hash	malicious	Browse	
	9EP6Gxzv6F.xls	Get hash	malicious	Browse	
	2ejCKSIjIV.exe	Get hash	malicious	Browse	
	bQWApID6av.xls	Get hash	malicious	Browse	
66.175.217.172	nrQXlgp21m.exe	Get hash	malicious	Browse	
	m3d2gsRm5Q.exe	Get hash	malicious	Browse	
	4TWEQh2HJb.xls	Get hash	malicious	Browse	
	ldE25Snd1f.exe	Get hash	malicious	Browse	
	Receipt-6218387.xls	Get hash	malicious	Browse	
	BhAJLvq0c7.xls	Get hash	malicious	Browse	
	PFx3G8Snzk.exe	Get hash	malicious	Browse	
	9EP6Gxzv6F.xls	Get hash	malicious	Browse	
	2ejCKSIjIV.exe	Get hash	malicious	Browse	
	bQWApID6av.xls	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CMRU-AS-APChiangmaiRajabhatUniversityTH	nrQXlgp21m.exe	Get hash	malicious	Browse	• 202.29.60.34
	m3d2gsRm5Q.exe	Get hash	malicious	Browse	• 202.29.60.34
	4TWEQh2HJb.xls	Get hash	malicious	Browse	• 202.29.60.34
	ldE25Snd1f.exe	Get hash	malicious	Browse	• 202.29.60.34
	Receipt-6218387.xls	Get hash	malicious	Browse	• 202.29.60.34
	BhAJLvq0c7.xls	Get hash	malicious	Browse	• 202.29.60.34
	PFx3G8Snzk.exe	Get hash	malicious	Browse	• 202.29.60.34
	9EP6Gxzv6F.xls	Get hash	malicious	Browse	• 202.29.60.34
	2ejCKSIjIV.exe	Get hash	malicious	Browse	• 202.29.60.34
	bQWApID6av.xls	Get hash	malicious	Browse	• 202.29.60.34
HETZNER-ASDE	Bear_Vpn.exe	Get hash	malicious	Browse	• 88.99.66.31
	MiiefP6Jj7.exe	Get hash	malicious	Browse	• 88.99.66.31
	MWTUoiKKLz.exe	Get hash	malicious	Browse	• 88.99.66.31
	qwxiR5lxRE.exe	Get hash	malicious	Browse	• 88.99.66.31
	QaFzP2AOXH.exe	Get hash	malicious	Browse	• 88.99.66.31
	nrQXlgp21m.exe	Get hash	malicious	Browse	• 78.46.78.42
	1z0OH1ed7P.exe	Get hash	malicious	Browse	• 88.99.66.31
	m3d2gsRm5Q.exe	Get hash	malicious	Browse	• 78.46.78.42
	4TWEQh2HJb.xls	Get hash	malicious	Browse	• 78.46.78.42
	ldE25Snd1f.exe	Get hash	malicious	Browse	• 78.46.78.42
	2aJ9QdIdFE.exe	Get hash	malicious	Browse	• 195.201.225.248
	EA4LughYnY.exe	Get hash	malicious	Browse	• 195.201.225.248
	Receipt-6218387.xls	Get hash	malicious	Browse	• 78.46.78.42
	etSPaoVcAD.exe	Get hash	malicious	Browse	• 195.201.225.248
	VwC7ZwYCLH.exe	Get hash	malicious	Browse	• 195.201.225.248
	BhAJLvq0c7.xls	Get hash	malicious	Browse	• 78.46.78.42
	kxQkjkU9DO.exe	Get hash	malicious	Browse	• 195.201.225.248
	PFx3G8Snzk.exe	Get hash	malicious	Browse	• 78.46.78.42
	9CMjcYFBxo.exe	Get hash	malicious	Browse	• 195.201.225.248
	jDnYtpTxyZ.exe	Get hash	malicious	Browse	• 88.99.66.31
LINODE-APLinodeLLCUS	zYObZhfFz0.dll	Get hash	malicious	Browse	• 176.58.123.25
	nrQXlgp21m.exe	Get hash	malicious	Browse	• 66.175.217.172
	m3d2gsRm5Q.exe	Get hash	malicious	Browse	• 66.175.217.172
	4TWEQh2HJb.xls	Get hash	malicious	Browse	• 66.175.217.172
	6kZeSToEoa.dll	Get hash	malicious	Browse	• 176.58.123.25
	ldE25Snd1f.exe	Get hash	malicious	Browse	• 66.175.217.172
	Receipt-6218387.xls	Get hash	malicious	Browse	• 66.175.217.172
	BhAJLvq0c7.xls	Get hash	malicious	Browse	• 66.175.217.172
	PFx3G8Snzk.exe	Get hash	malicious	Browse	• 66.175.217.172
	9EP6Gxzv6F.xls	Get hash	malicious	Browse	• 66.175.217.172
	2ejCKSIjIV.exe	Get hash	malicious	Browse	• 66.175.217.172
	bQWApID6av.xls	Get hash	malicious	Browse	• 66.175.217.172
	sddA9XYpsF.exe	Get hash	malicious	Browse	• 66.175.211.144
	3F9E.dll	Get hash	malicious	Browse	• 176.58.123.25
	5pyLvJBYld.dll	Get hash	malicious	Browse	• 176.58.123.25
	triage_dropped_file.dll	Get hash	malicious	Browse	• 176.58.123.25
	TeMdJqNMM0.exe	Get hash	malicious	Browse	• 45.33.2.79
	RzLicilE0b.exe	Get hash	malicious	Browse	• 172.104.157.41
	C0TEsC936Q.exe	Get hash	malicious	Browse	• 178.79.153.56
	zizy3.dll	Get hash	malicious	Browse	• 176.58.123.25

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):	7.49405680509504
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • 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:	6ZV65nCMYQ.exe
File size:	167936
MD5:	622f4aa2d5e82438f3a40a35ab4902d5
SHA1:	b486db47021575c47e7b130bed1ad70b8bf6a719
SHA256:	277089cb78a9c493cecd8f5fbe70df0577d4f9557fb8b55ff5f7c2505308ca3a
SHA512:	2526c4ddad898208f5c3884e869beb35955a85ed92b628e1f7622daaf84d1f5e14071e6ab6984b8431eb9d127ae0e32c927699a40ef448169f81f74023df3446
SSDEEP:	3072:4WiJzQu5JD9ko9WY1wzxWrPAYNF7L5cWlvsRwmhnxONgkf:4LquAkPAYnX5WncNgk
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....x.....Rich.....PE..L...!`.`.....@...P.....>.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x10013ef0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60FE6021 [Mon Jul 26 07:11:29 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	e9cbee8358b331a128409a4d26e3e347

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1357c	0x14000	False	0.893872070313	data	7.824574037	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x15000	0x9d8	0x1000	False	0.346923828125	data	3.66891935244	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x16000	0x119ca	0x11000	False	0.947150735294	data	7.84923846168	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x28000	0x420	0x1000	False	0.115478515625	data	1.09655664129	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x29000	0x120	0x1000	False	0.076904296875	data	0.698725432618	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: 6ZV65nCMYQ.exe PID: 6632 Parent PID: 6044

General

Start time:	21:06:20
Start date:	14/07/2021
Path:	C:\Users\user\Desktop\6ZV65nCMYQ.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\6ZV65nCMYQ.exe'
Imagebase:	0x10000000
File size:	167936 bytes
MD5 hash:	622F4AA2D5E82438F3A40A35AB4902D5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000000.00000002.1172561248.0000000010001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities | Show Windows behavior

File Read

Disassembly

Code Analysis