

JoeSandbox Cloud BASIC



ID: 452434

Sample Name:

SecuriteInfo.com.Variant.Zusy.394472.15672.20727

Cookbook: default.jbs

Time: 10:48:07

Date: 22/07/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report SecuriteInfo.com.Variant.Zusy.394472.15672.20727	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Threatname: FormBook	3
Yara Overview	4
Memory Dumps	4
Unpacked PEs	5
Sigma Overview	6
Jbx Signature Overview	6
AV Detection:	6
Networking:	6
E-Banking Fraud:	6
System Summary:	6
Data Obfuscation:	6
Malware Analysis System Evasion:	6
HIPS / PFW / Operating System Protection Evasion:	6
Stealing of Sensitive Information:	6
Remote Access Functionality:	6
Mitre Att&ck Matrix	6
Behavior Graph	7
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	9
URLs	9
Domains and IPs	9
Contacted Domains	9
Contacted URLs	9
Contacted IPs	9
General Information	9
Simulations	10
Behavior and APIs	10
Joe Sandbox View / Context	10
IPs	10
Domains	10
ASN	10
JA3 Fingerprints	10
Dropped Files	10
Created / dropped Files	10
Static File Info	10
General	10
File Icon	11
Static PE Info	11
General	11
Entrypoint Preview	11
Rich Headers	11
Data Directories	11
Sections	11
Imports	11
Network Behavior	11
Code Manipulations	11
Statistics	12
Behavior	12
System Behavior	12
Analysis Process: SecuriteInfo.com.Variant.Zusy.394472.15672.exe PID: 6496 Parent PID: 5828	12
General	12
File Activities	12
Analysis Process: SecuriteInfo.com.Variant.Zusy.394472.15672.exe PID: 6568 Parent PID: 6496	12
General	12
File Activities	13
File Read	13
Disassembly	13
Code Analysis	13

Windows Analysis Report SecuriteInfo.com.Variant.Zus...

Overview

General Information

Sample Name:

SecuriteInfo.com.Variant.Zusy.394472.15672.20727 (renamed file extension from 20727 to exe)

Analysis ID:

452434

MD5:

89cfb542cda6a42...

SHA1:

9a0606c633ffe5a..




SHA256:

b663fea76aadb5..

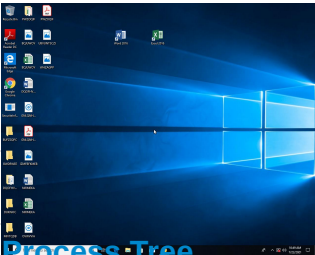
Tags:

exe

Infos:

Most interesting Screenshot:



Process Tree

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

FormBook

Score:

100

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Antivirus detection for URL or domain

Detected unpacking (changes PE se...

Found malware configuration

Malicious sample detected (through ...

Multi AV Scanner detection for doma...

Multi AV Scanner detection for subm...

Yara detected FormBook

C2 URLs / IPs found in malware con...

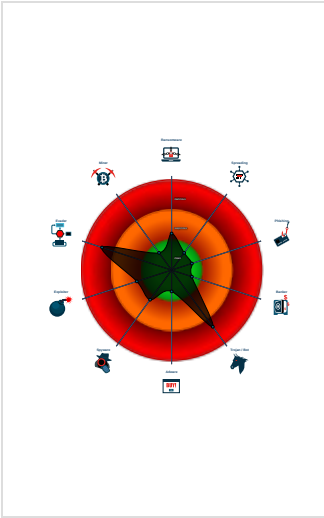
Machine Learning detection for samp...



Maps a DLL or memory area into an...

Tries to detect virtualization through...

Antivirus or Machine Learning detec...

Classification



- System is w10x64
-  SecuriteInfo.com.Variant.Zusy.394472.15672.exe (PID: 6496 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Zusy.394472.15672.exe' MD5: 89CFB542CDA6A428CC5C02FEAF3C55F8)
 -  SecuriteInfo.com.Variant.Zusy.394472.15672.exe (PID: 6568 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Zusy.394472.15672.exe' MD5: 89CFB542CDA6A428CC5C02FEAF3C55F8)
- cleanup

Malware Configuration

Threatname: FormBook

```

{
  "C2 list": [
    "www.yjhlgg.com/grve/"
  ],
  "decoy": [
    "jrvinganimalexterminator.com",
    "smallsyalls.com",
    "poic3.com",
    "mencg.com",
    "aussieenjoyment.today",
    "espace22.com",
    "aanmelding-desk.info",
    "gallopshoes.com",
    "nftsexy.com",
    "ricosdulcesmexicanos.com",
    "riseswift.com",
    "thechicthirty.com",
    "matdcg.com",
    "alternet.today",
    "creativehuesdesigns.com",
    "rjkcrafts.com",
    "lowdosemortgage.com",
    "adoptahanster.com",
    "wellness-sense.com",
    "jacardcapital.com",
    "pastiindonesia.com",
    "lindsaynathan2021.com",
    "brisbanemagicians.com",
    "tvglanz.com",
    "388384.com",
    "mitgrin.com",
    "endoneiatrading.com",
    "political.singles",
    "ganjegirls.com",
    "democratscancelled.com",
    "ytzhubao.com",
    "roiskylands.com",
    "zamlgroup.com",
    "winstonsalemathleticclub.com",
    "62qtz2.com",
    "caddyys.com",
    "ecorarte.com",
    "coonier.com",
    "cbgmanhattan-hub.com",
    "givanon.com",
    "tionis11.com",
    "variceselite.com",
    "tasaciona.com",
    "hiphopeconomicdevelopment.com",
    "citrixfile.com",
    "piebuilder.com",
    "drmetalpublishing.com",
    "themesthatyoulike.com",
    "vinhomes-phanhung.info",
    "ardecentro.com",
    "gameshowsatwork.com",
    "go-rillathebrand.com",
    "virtualppo.com",
    "nogodbeforeme.net",
    "fabrezeairpurifiers.com",
    "roorisor.com",
    "elaraberentcar.com",
    "rugpat.com",
    "renewalbyheather.com",
    "innocox.com",
    "ztsj10086.com",
    "channelarmor.info",
    "thecarbonbox.store",
    "edicionesvita.com"
  ]
}

```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000001.644193470.0000000000400000.0000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000001.644193470.0000000000400000.0000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	<ul style="list-style-type: none"> 0x98e8:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x9b52:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x15675:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x15161:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x15777:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x158ef:\$sequence_4: 5D C3 8D 50 7C 80 FA 07 0xa56a:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 0x143dc:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0xb263:\$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x1b317:\$sequence_8: 3C 54 74 04 3C 74 75 F4 0x1c31a:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000001.644193470.0000000000400000.0000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	<ul style="list-style-type: none"> 0x183f9:\$sqlite3step: 68 34 1C 7B E1 0x1850c:\$sqlite3step: 68 34 1C 7B E1 0x18428:\$sqlite3text: 68 38 2A 90 C5 0x1854d:\$sqlite3text: 68 38 2A 90 C5 0x1843b:\$sqlite3blob: 68 53 D8 7F 8C 0x18563:\$sqlite3blob: 68 53 D8 7F 8C
00000001.00000002.644964411.0000000000600000.0000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.644964411.0000000000600000.0000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	<ul style="list-style-type: none"> 0x98e8:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x9b52:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x15675:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x15161:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x15777:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x158ef:\$sequence_4: 5D C3 8D 50 7C 80 FA 07 0xa56a:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 0x143dc:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0xb263:\$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x1b317:\$sequence_8: 3C 54 74 04 3C 74 75 F4 0x1c31a:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 4 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.SecuriteInfo.com.Variant.Zusy.394472.15672.exe .600000.3.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.SecuriteInfo.com.Variant.Zusy.394472.15672.exe .600000.3.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	<ul style="list-style-type: none"> 0x8ae8:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x8d52:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x14875:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x14361:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x14977:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x14aef:\$sequence_4: 5D C3 8D 50 7C 80 FA 07 0x976a:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 0x135dc:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0xa463:\$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x1a517:\$sequence_8: 3C 54 74 04 3C 74 75 F4 0x1b51a:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.SecuriteInfo.com.Variant.Zusy.394472.15672.exe .600000.3.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	<ul style="list-style-type: none"> 0x175f9:\$sqlite3step: 68 34 1C 7B E1 0x1770c:\$sqlite3step: 68 34 1C 7B E1 0x17628:\$sqlite3text: 68 38 2A 90 C5 0x1774d:\$sqlite3text: 68 38 2A 90 C5 0x1763b:\$sqlite3blob: 68 53 D8 7F 8C 0x17763:\$sqlite3blob: 68 53 D8 7F 8C
3.2.SecuriteInfo.com.Variant.Zusy.394472.15672.exe .400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.SecuriteInfo.com.Variant.Zusy.394472.15672.exe .400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	<ul style="list-style-type: none"> 0x8ae8:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x8d52:\$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x14875:\$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x14361:\$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x14977:\$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x14aef:\$sequence_4: 5D C3 8D 50 7C 80 FA 07 0x976a:\$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 0x135dc:\$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0xa463:\$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x1a517:\$sequence_8: 3C 54 74 04 3C 74 75 F4 0x1b51a:\$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview



Click to jump to signature section

AV Detection:



Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:



C2 URLs / IPs found in malware configuration

E-Banking Fraud:



Yara detected FormBook

System Summary:



Malicious sample detected (through community Yara rule)

Data Obfuscation:



Detected unpacking (changes PE section rights)

Malware Analysis System Evasion:



Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:



Maps a DLL or memory area into another process

Stealing of Sensitive Information:



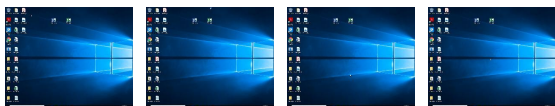
Yara detected FormBook

Remote Access Functionality:



Yara detected FormBook

Mitre Att&ck Matrix



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.Variant.Zusy.394472.15672.exe	51%	Virustotal		Browse
SecuriteInfo.com.Variant.Zusy.394472.15672.exe	23%	Metadefender		Browse
SecuriteInfo.com.Variant.Zusy.394472.15672.exe	61%	ReversingLabs	Win32.Trojan.VirRansom	
SecuriteInfo.com.Variant.Zusy.394472.15672.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.SecuriteInfo.com.Variant.Zusy.394472.15672.exe.600000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.SecuriteInfo.com.Variant.Zusy.394472.15672.exe.5c0000.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
3.2.SecuriteInfo.com.Variant.Zusy.394472.15672.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.1.SecuriteInfo.com.Variant.Zusy.394472.15672.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.yjhlgg.com/grve/	9%	Virustotal		Browse
www.yjhlgg.com/grve/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.yjhlgg.com/grve/	true	<ul style="list-style-type: none">9%, Virustotal, BrowseAvira URL Cloud: malware	low

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452434
Start date:	22.07.2021
Start time:	10:48:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Variant.Zusy.394472.15672.20727 (renamed file extension from 20727 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:	6
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">HCA enabledEGA enabledHDC enabledAMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@3/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none">Successful, ratio: 37.8% (good quality ratio 34.8%)Quality average: 67.9%Quality standard deviation: 32%
HCA Information:	<ul style="list-style-type: none">Successful, ratio: 100%Number of executed functions: 0Number of non-executed functions: 0

Cookbook Comments:	<ul style="list-style-type: none">Adjust boot timeEnable AMSIStop behavior analysis, all processes terminated
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):	7.972672862174758
TrID:	<ul style="list-style-type: none">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:	SecuriteInfo.com.Variant.Zusy.394472.15672.exe
File size:	198124
MD5:	89cfb542cda6a428cc5c02feaf3c55f8
SHA1:	9a0606c633ffe5ae4b6dcb7dcfba57b7e22cb05d
SHA256:	b663fea76aadbf574e5bb9f704ad689ec10f0d720b0b9641e70b27494fe4cc17

General		
SHA512:		22fd691c761ec2ac5be4b3a9b682daf53abb3de05787d07474bc0e41a8c7bf001a10783f3eea6d7d70528dae1da13506e4370b16f3c02b7d92db9e6ffb2ac79b
SSDEEP:		3072:p5y2zSw5QFZ5h8gOgXN15tm4Inoll4wegWYXzb+f3ilvwDrqvHDlkNBKrD9CafOn:Dy2OVbFvLKzTwePi+nQrU8+fLBcMQ
File Content Preview:		MZ.....@.....!..L.!Th is program cannot be run in DOS mode....\$......WullI9& II9&II9&@..&BI9&II8&UI9&@..&HI9&@..&HI9&RichII9&..PE..L.....\.....0....@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x401000
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x60F8A6D1 [Wed Jul 21 22:59:29 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:	ad7593902351b94d30c5d42690419916

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1248	0x1400	False	0.470703125	data	4.74743195609	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x3000	0x3ae	0x400	False	0.53515625	data	4.4688660684	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Imports


Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

 Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.Variant.Zusy.394472.15672.exe PID: 6496 Parent PID: 5828

General

Start time:	10:48:51
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Zusy.394472.15672.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Zusy.394472.15672.exe'
Imagebase:	0x400000
File size:	198124 bytes
MD5 hash:	89CFB542CDA6A428CC5C02FEAF3C55F8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	<ul style="list-style-type: none">Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.644964411.0000000000600000.00000040.00000001.sdmp, Author: Joe SecurityRule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.644964411.0000000000600000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot comRule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.644964411.0000000000600000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: SecuriteInfo.com.Variant.Zusy.394472.15672.exe PID: 6568 Parent PID: 6496

General

Start time:	10:48:51
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Zusy.394472.15672.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Variant.Zusy.394472.15672.exe'
Imagebase:	0x400000
File size:	198124 bytes
MD5 hash:	89CFB542CDA6A428CC5C02FEAF3C55F8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	<ul style="list-style-type: none">• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000001.644193470.000000000400000.00000040.00020000.sdmp, Author: Joe Security• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000001.644193470.000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com• Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000001.644193470.000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.646633088.000000000400000.00000040.00000001.sdmp, Author: Joe Security• Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.646633088.000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com• Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.646633088.000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

[File Activities](#)

Show Windows behavior

File Read

Disassembly

Code Analysis