ID: 679627
Sample Name: w9J4jyf7oY
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 07:13:57
Date: 06/08/2022
Version: 35.0.0 Citrine

Table of Contents

Linux Analysis Report

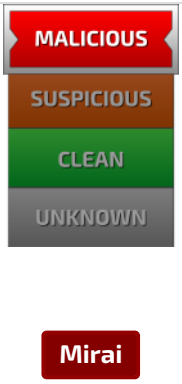
w9J4jyf7oY

Overview

General Information

Sample Name:	w9J4jyf7oY
Analysis ID:	679627
MD5:	bb2f72c63c8c04…
SHA1:	035b12d2be4f11..
SHA256:	2e717964f7f88a6.
Tags:	32 elf mirai motorola
Infos:	

Detection

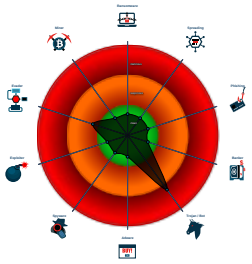


Score:	64
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Yara signature match
- Sample contains strings that are po…
- Sample has stripped symbol table
- Uses the "uname" system call to qu…
- Enumerates processes within the "p…
- Sample listens on a socket
- Sample contains strings indicative o…

Classification



Analysis Advice

Static ELF header machine description suggests that the sample might not execute correctly on this machine.

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679627
Start date and time: 06/08/202207:13:57	2022-08-06 07:13:57 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	w9J4jyf7oY
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 20.04 x64 (Kernel 5.4.0-72, Firefox 91.0, Evince Document Viewer 3.36.10, LibreOffice 6.4.7.2, OpenJDK 11.0.11)
Analysis Mode:	default
Detection:	MAL
Classification:	mal64.troj.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/w9J4jyf7oY
PID:	6219
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- w9J4jyf7oY (PID: 6219, Parent: 6125, MD5: cd177594338c77b895ae27c33f8f86cc) Arguments: /tmp/w9J4jyf7oY
  - w9J4jyf7oY New Fork (PID: 6221, Parent: 6219)
  - w9J4jyf7oY New Fork (PID: 6222, Parent: 6219)
  - w9J4jyf7oY New Fork (PID: 6224, Parent: 6219)
    - w9J4jyf7oY New Fork (PID: 6227, Parent: 6224)
    - w9J4jyf7oY New Fork (PID: 6228, Parent: 6224)
    - w9J4jyf7oY New Fork (PID: 6229, Parent: 6224)
    - w9J4jyf7oY New Fork (PID: 6230, Parent: 6224)
    - w9J4jyf7oY New Fork (PID: 6231, Parent: 6224)
    - w9J4jyf7oY New Fork (PID: 6237, Parent: 6224)
    - w9J4jyf7oY New Fork (PID: 6238, Parent: 6224)
    - w9J4jyf7oY New Fork (PID: 6243, Parent: 6224)
    - w9J4jyf7oY New Fork (PID: 6245, Parent: 6224)
    - w9J4jyf7oY New Fork (PID: 6246, Parent: 6224)
    - w9J4jyf7oY New Fork (PID: 6248, Parent: 6224)
    - w9J4jyf7oY New Fork (PID: 6249, Parent: 6224)
    - w9J4jyf7oY New Fork (PID: 6252, Parent: 6224)
    - w9J4jyf7oY New Fork (PID: 6254, Parent: 6224)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
w9J4jyf7oY	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	• 0x1c112:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1c182:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1c1f2:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1c261:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1c2d0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1c538:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1c58b:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1c5de:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1c631:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1c685:$xo1: oMXKNNC\x0D\x17\x0C\x12
w9J4jyf7oY	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
6222.1.00007fac24021000.00007fac24022000.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	• 0x584:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x5f8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x66c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x6e0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x754:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x9d4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xa2c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xa84:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xadc:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xb34:$xo1: oMXKNNC\x0D\x17\x0C\x12
6219.1.00007fac2401f000.00007fac24021000.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	• 0x112:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x182:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1f2:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x261:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x2d0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x538:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x58b:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x5de:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x631:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x685:$xo1: oMXKNNC\x0D\x17\x0C\x12

Source	Rule	Description	Author	Strings
6222.1.00007fac2401f000.00007fac24021000.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	• 0x112:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x182:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1f2:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x261:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x2d0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x538:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x58b:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x5de:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x631:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x685:$xo1: oMXKNNC\x0D\x17\x0C\x12
6219.1.00007fac24021000.00007fac24022000.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	• 0x584:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x5f8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x66c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x6e0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x754:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x9d4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xa2c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xa84:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xadc:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xb34:$xo1: oMXKNNC\x0D\x17\x0C\x12
6222.1.00007fac24001000.00007fac2401e000.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious single byte XORed keyword \'Mozilla/5.0\' - it uses yara\'s XOR modifier and therefore cannot print the XOR key. You can use the CyberChef recipe linked in the reference field to brute force the used key.	Florian Roth	• 0x1c112:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1c182:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1c1f2:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1c261:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1c2d0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1c538:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1c58b:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1c5de:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1c631:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1c685:$xo1: oMXKNNC\x0D\x17\x0C\x12
Click to see the 3 entries				

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

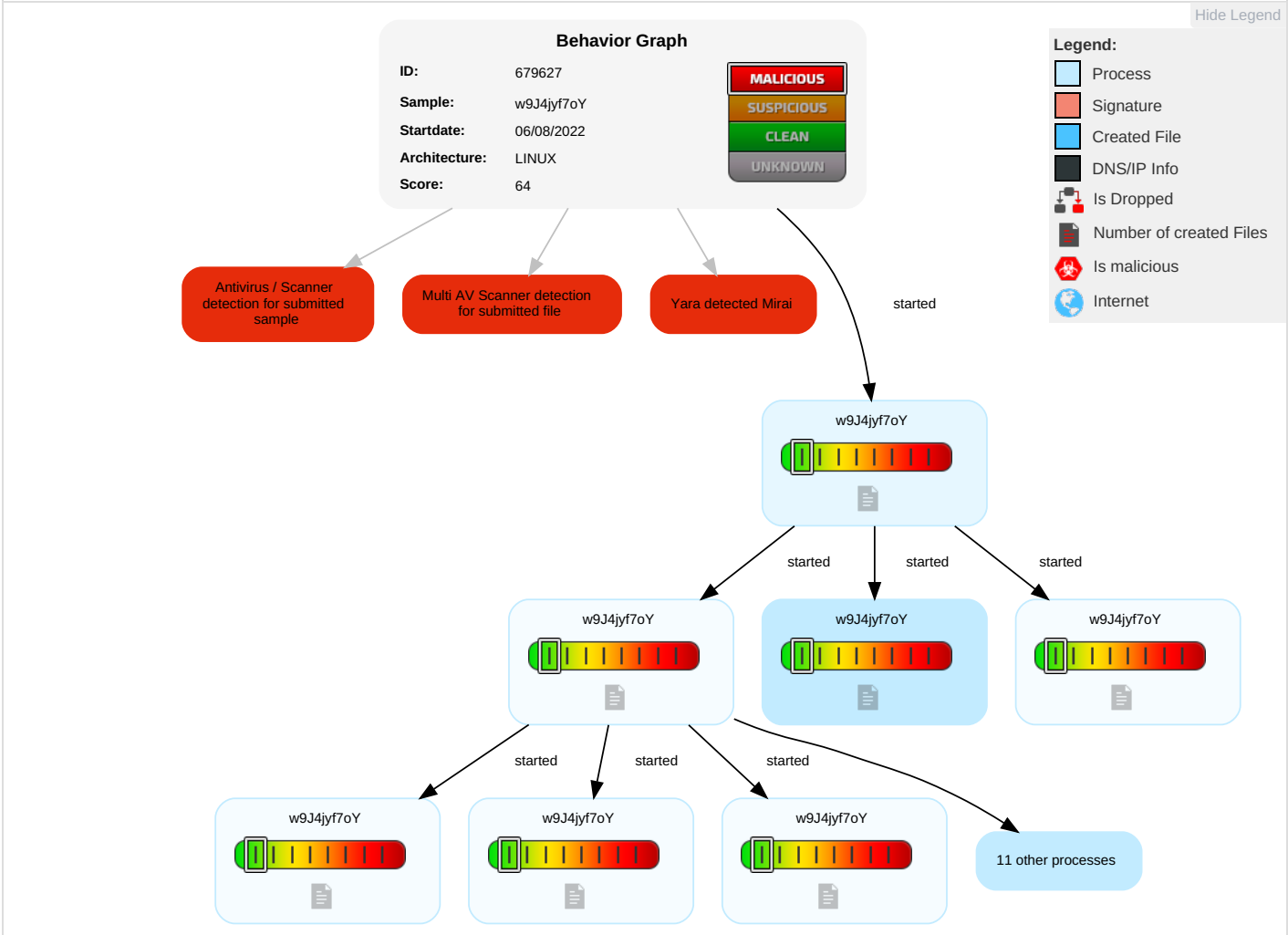
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Command and Scripting Interpreter	Path Interception	Path Interception	Direct Volume Access	1 OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
w9J4jyf7oY	58%	Virustotal		Browse
w9J4jyf7oY	62%	ReversingLabs	Linux.Trojan.Mirai	

Source	Detection	Scanner	Label	Link
w9J4jyf7oY	100%	Avira	LINUX/Mirai.bonb	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://46.23.109.47/Cloud/Gpon.sh	19%	Virustotal		Browse
http://46.23.109.47/Cloud/Gpon.sh	100%	Avira URL Cloud	malware	
http://46.23.109.47/Cloud/Cloud.x86	18%	Virustotal		Browse
http://46.23.109.47/Cloud/Cloud.x86	100%	Avira URL Cloud	malware	
http://46.23.109.47/Cloud/Comtrend.sh%20-O%20-%3E%20/tmp/jno;sh%20/tmp/jno%27/&sessionKey=1039230114	100%	Avira URL Cloud	malware	
http://46.23.109.47/Cloud/Netlink.sh%20-O%20-%3E%20/tmp/jno;sh%20/tmp/jno%27/&waninf=1_INTERNET_R_VI	100%	Avira URL Cloud	malware	
http://46.23.109.47/Cloud/Cloud.mpsl;chmod	100%	Avira URL Cloud	malware	
http://46.23.109.47/Cloud/Cloud.mips;	100%	Avira URL Cloud	malware	
http://purenetworks.com/HNAP1/	0%	URL Reputation	safe	
http://0.0.0.0/Cloud/Cloud.x86	0%	Avira URL Cloud	safe	
http://46.23.109.47/Cloud/Dlink.sh%20-O%20-%3E%20/tmp/kh;sh%20/tmp/kh%27$	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

World Map of Contacted IPs

No contacted IP infos

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	ELF 32-bit MSB executable, Motorola m68k, 68020, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.536123197703782
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	w9J4jyf7oY
File size:	119516
MD5:	bb2f72c63c8c0427d31a757dfa190260
SHA1:	035b12d2be4f11e9ebe390aadab1205a599c6432
SHA256:	2e717964f7f88a60459e708ac92be181d0c3899fd3ce6b60c34624b0402f78a0
SHA512:	af8b0ae4bdb1016c6b65adb1b697b334e3bb38f7a855501fed7cc5727d56f7df93eec6544255ffbee0530c766e1a495375a59bdc3c4e9e3b96043e3697861920
SSDEEP:	3072:Wf75AB1k77IgffdHma8pdPUoPSHLP+E8f:e75AB1k77IgffVma8pdPUzT+EI
TLSH:	DFC38ED5A8115F3CFADB9AB582334B0CA82192040FE30F57FA67EC977D73195AA06C46
File Content Preview:	.ELF.....D...4...L.....4. ...(.....l...l..... .....p...p...p.....t..... .dt.Q.....NV..a....da.....N^NuNV..J9....f>"y.... QJ.g.X.#.....N."y.... QJ.f.A.....J.g.Hy...lN.X.....N^NuNV..N^NuN

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	MC68000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x80000144
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	119116
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x80000094	0x94	0x14	0x0	0x6	AX	0	0	2
.text	PROGBITS	0x800000a8	0xa8	0x1a3ee	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x8001a496	0x1a496	0xe	0x0	0x6	AX	0	0	2
.rodata	PROGBITS	0x8001a4a4	0x1a4a4	0x29c8	0x0	0x2	A	0	0	2

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
.ctors	PROGBITS	0x8001ee70	0x1ce70	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x8001ee78	0x1ce78	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x8001ee84	0x1ce84	0x288	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x8001f10c	0x1d10c	0x8d8	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x1d10c	0x3e	0x0	0x0		0	0	1

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x80000000	0x80000000	0x1ce6c	0x1ce6c	6.5552	0x5	R E	0x2000		.init .text .fini .rodata
LOAD	0x1ce70	0x8001ee70	0x8001ee70	0x29c	0xb74	3.0075	0x6	RW	0x2000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

No network behavior found

System Behavior

Analysis Process: w9J4jyf7oY PID: 6219, Parent PID: 6125

General

Start time:	07:14:41
Start date:	06/08/2022
Path:	/tmp/w9J4jyf7oY
Arguments:	/tmp/w9J4jyf7oY
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Analysis Process: w9J4jyf7oY PID: 6221, Parent PID: 6219

General

Start time:	07:14:41
Start date:	06/08/2022
Path:	/tmp/w9J4jyf7oY
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Directory Enumerated

Analysis Process: w9J4jyf7oY PID: 6222, Parent PID: 6219

General

Start time:	07:14:41
Start date:	06/08/2022
Path:	/tmp/w9J4jyf7oY
Arguments:	n/a

File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: w9J4jyf7oY PID: **6224**, Parent PID: **6219**

General

Start time:	07:14:41
Start date:	06/08/2022
Path:	/tmp/w9J4jyf7oY
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: w9J4jyf7oY PID: **6227**, Parent PID: **6224**

General

Start time:	07:14:41
Start date:	06/08/2022
Path:	/tmp/w9J4jyf7oY
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: w9J4jyf7oY PID: **6228**, Parent PID: **6224**

General

Start time:	07:14:41
Start date:	06/08/2022
Path:	/tmp/w9J4jyf7oY
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: w9J4jyf7oY PID: **6229**, Parent PID: **6224**

General

Start time:	07:14:41
Start date:	06/08/2022
Path:	/tmp/w9J4jyf7oY
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: w9J4jyf7oY PID: **6230**, Parent PID: **6224**

General

Start time:	07:14:41
Start date:	06/08/2022
Path:	/tmp/w9J4jyf7oY
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: w9J4jyf7oY PID: **6231**, Parent PID: **6224**

General

Start time:	07:14:41
Start date:	06/08/2022
Path:	/tmp/w9J4jyf7oY
Arguments:	n/a

File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: w9J4jyf7oY PID: **6237**, Parent PID: **6224**

General

Start time:	07:14:41
Start date:	06/08/2022
Path:	/tmp/w9J4jyf7oY
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: w9J4jyf7oY PID: **6238**, Parent PID: **6224**

General

Start time:	07:14:41
Start date:	06/08/2022
Path:	/tmp/w9J4jyf7oY
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: w9J4jyf7oY PID: **6243**, Parent PID: **6224**

General

Start time:	07:14:42
Start date:	06/08/2022
Path:	/tmp/w9J4jyf7oY
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: w9J4jyf7oY PID: **6245**, Parent PID: **6224**

General

Start time:	07:14:42
Start date:	06/08/2022
Path:	/tmp/w9J4jyf7oY
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: w9J4jyf7oY PID: **6246**, Parent PID: **6224**

General

Start time:	07:14:42
Start date:	06/08/2022
Path:	/tmp/w9J4jyf7oY
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: w9J4jyf7oY PID: **6248**, Parent PID: **6224**

General

Start time:	07:14:42
Start date:	06/08/2022
Path:	/tmp/w9J4jyf7oY
Arguments:	n/a

File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: w9J4jyf7oY PID: **6249**, Parent PID: **6224**

General

Start time:	07:14:42
Start date:	06/08/2022
Path:	/tmp/w9J4jyf7oY
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: w9J4jyf7oY PID: **6252**, Parent PID: **6224**

General

Start time:	07:14:42
Start date:	06/08/2022
Path:	/tmp/w9J4jyf7oY
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: w9J4jyf7oY PID: **6254**, Parent PID: **6224**

General

Start time:	07:14:42
Start date:	06/08/2022
Path:	/tmp/w9J4jyf7oY
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc