ID: 679619
Sample Name: 4wiwmAupak
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 06:42:39
Date: 06/08/2022
Version: 35.0.0 Citrine

Table of Contents

Linux Analysis Report

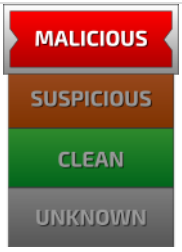
4wiwmAupak

Overview

General Information

Sample Name:	4wiwmAupak
Analysis ID:	679619
MD5:	234f833a57b262..
SHA1:	81915b94e27f54..
SHA256:	4738edac99f86b..
Tags:	32 elf mips mirai
Infos:	

Detection



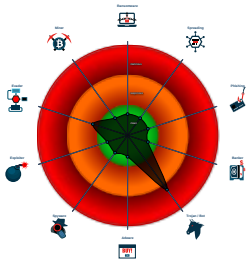
Mirai

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 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.

Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures.

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679619
Start date and time: 06/08/202206:42:39	2022-08-06 06:42:39 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	4wiwmAupak
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/4wiwmAupak
PID:	6233
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- 4wiwmAupak (PID: 6233, Parent: 6127, MD5: 0083f1f0e77be34ad27f849842bbb00c) Arguments: /tmp/4wiwmAupak
  - 4wiwmAupak New Fork (PID: 6235, Parent: 6233)
  - 4wiwmAupak New Fork (PID: 6236, Parent: 6233)
  - 4wiwmAupak New Fork (PID: 6238, Parent: 6233)
    - 4wiwmAupak New Fork (PID: 6241, Parent: 6238)
    - 4wiwmAupak New Fork (PID: 6242, Parent: 6238)
    - 4wiwmAupak New Fork (PID: 6243, Parent: 6238)
    - 4wiwmAupak New Fork (PID: 6244, Parent: 6238)
    - 4wiwmAupak New Fork (PID: 6245, Parent: 6238)
    - 4wiwmAupak New Fork (PID: 6251, Parent: 6238)
    - 4wiwmAupak New Fork (PID: 6252, Parent: 6238)
    - 4wiwmAupak New Fork (PID: 6253, Parent: 6238)
    - 4wiwmAupak New Fork (PID: 6258, Parent: 6238)
    - 4wiwmAupak New Fork (PID: 6259, Parent: 6238)
    - 4wiwmAupak New Fork (PID: 6262, Parent: 6238)
    - 4wiwmAupak New Fork (PID: 6265, Parent: 6238)
    - 4wiwmAupak New Fork (PID: 6266, Parent: 6238)
    - 4wiwmAupak New Fork (PID: 6268, Parent: 6238)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
4wiwmAupak	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	0x223c4:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x22434:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x224a4:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x22514:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x22584:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x227f4:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x22848:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x2289c:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x228f0:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x22944:$xo1: oMXKNNC\x0D\x17\x0C\x12
4wiwmAupak	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
6233.1.00007fd554464000.00007fd554466000.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	0x1584:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x15f8:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x166c:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x16e0:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1754:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x19d4:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1a2c:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1a84:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1adc:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1b34:$xo1: oMXKNNC\x0D\x17\x0C\x12
6236.1.00007fd554464000.00007fd554466000.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	0x1584:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x15f8:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x166c:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x16e0:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1754:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x19d4:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1a2c:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1a84:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1adc:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1b34:$xo1: oMXKNNC\x0D\x17\x0C\x12

Source	Rule	Description	Author	Strings
6233.1.00007fd554400000.00007fd554424000.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	• 0x223c4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x22434:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x224a4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x22514:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x22584:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x227f4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x22848:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x2289c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x228f0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x22944:$xo1: oMXKNNC\x0D\x17\x0C\x12
6233.1.00007fd554400000.00007fd554424000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6236.1.00007fd554400000.00007fd554424000.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	• 0x223c4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x22434:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x224a4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x22514:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x22584:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x227f4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x22848:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x2289c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x228f0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x22944:$xo1: oMXKNNC\x0D\x17\x0C\x12
Click to see the 1 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

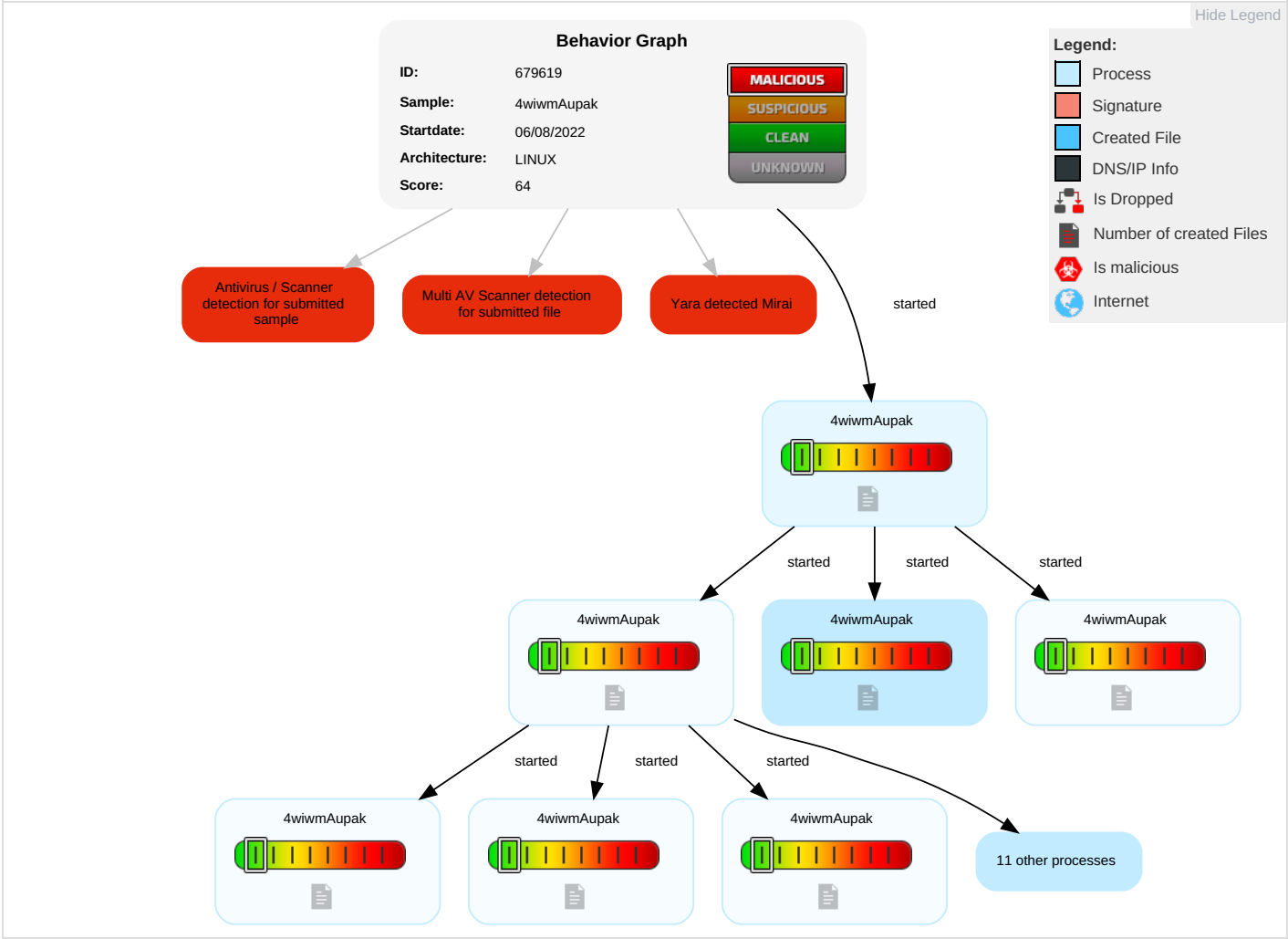
Mitre Att&ck Matrix

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	Windows Management Instrumentation	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
4wiwmAupak	61%	Virustotal		Browse
4wiwmAupak	31%	Metadefender		Browse
4wiwmAupak	63%	ReversingLabs	Linux.Trojan.Mirai	
4wiwmAupak	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, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
Entropy (8bit):	5.710060818234627
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	4wiwmAupak
File size:	147164
MD5:	234f833a57b2626dbd7992faf3c2a149
SHA1:	81915b94e27f542c1f8331a1f6b3317d82624805
SHA256:	4738edac99f86b857032b8c7fb640b6fe5cf4109ae0c3a6e56deb84b0a76d936
SHA512:	73d07c52a01e8beeab7d78443a5102e9f4eac12f54e93c5bef4a021c235f37e03affdaaddc236d1d9a9bc79ca6a3bb24425cddb2b8fc3c93e87575ee0024a91d
SSDEEP:	3072:4rgHjxhR7/ZbV0yb6bZZeySx0eOn6WoexbY1wAhMwwRaeL:e0FXrnszehxWoubY1wwwl
TLSH:	D5E3B50D3E219F7DF7ACC23447B78A255258339A32E0D5C5D15CE9016EA028E786FF9A
File Content Preview:	.ELF.....@.`...4..<.....4. ...(.....@...@....3...3.....3..F3..F3....t...4.....dt.Q.....<...'.....!'.....<...'.....!... ....'9... ..... <...'.....!.....'9.

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	MIPS R3000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x400260
Flags:	0x1007
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	146604
Section Header Size:	40
Number of Section Headers:	14
Header String Table Index:	13

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x400094	0x94	0x8c	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x400120	0x120	0x20450	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x420570	0x20570	0x5c	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x4205d0	0x205d0	0x2e00	0x0	0x2	A	0	0	16
.ctors	PROGBITS	0x4633d4	0x233d4	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x4633dc	0x233dc	0x8	0x0	0x3	WA	0	0	4
.data.rel.ro	PROGBITS	0x4633e8	0x233e8	0x10	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x463400	0x23400	0x2c0	0x0	0x3	WA	0	0	16
.got	PROGBITS	0x4636c0	0x236c0	0x588	0x4	0x10000003	WAp	0	0	16
.sbss	NOBITS	0x463c48	0x23c48	0x24	0x0	0x10000003	WAp	0	0	4
.bss	NOBITS	0x463c70	0x23c48	0xa98	0x0	0x3	WA	0	0	16
.mdebug.abi32	PROGBITS	0x84c	0x23c48	0x0	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x23c48	0x64	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	0x400000	0x400000	0x233d0	0x233d0	5.7229	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x233d4	0x4633d4	0x4633d4	0x874	0x1334	3.9409	0x6	RW	0x10000		.ctors .dtors .data.rel.ro .data .got .sbss .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

No network behavior found

System Behavior

Analysis Process: 4wiwmAupak PID: 6233, Parent PID: 6127

General

Start time:	06:43:23
Start date:	06/08/2022
Path:	/tmp/4wiwmAupak
Arguments:	/tmp/4wiwmAupak
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Analysis Process: 4wiwmAupak PID: 6235, Parent PID: 6233

General

Start time:	06:43:23
Start date:	06/08/2022
Path:	/tmp/4wiwmAupak
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

File Activities

File Read

Directory Enumerated

Analysis Process: 4wiwmAupak PID: 6236, Parent PID: 6233

General

Start time:	06:43:23
Start date:	06/08/2022
Path:	/tmp/4wiwmAupak
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: 4wiwmAupak PID: 6238, Parent PID: 6233

General

Start time:	06:43:23

Start date:	06/08/2022
Path:	/tmp/4wiwmAupak
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: 4wiwmAupak PID: **6241**, Parent PID: **6238**

General

Start time:	06:43:23
Start date:	06/08/2022
Path:	/tmp/4wiwmAupak
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: 4wiwmAupak PID: **6242**, Parent PID: **6238**

General

Start time:	06:43:23
Start date:	06/08/2022
Path:	/tmp/4wiwmAupak
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: 4wiwmAupak PID: **6243**, Parent PID: **6238**

General

Start time:	06:43:23
Start date:	06/08/2022
Path:	/tmp/4wiwmAupak
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: 4wiwmAupak PID: **6244**, Parent PID: **6238**

General

Start time:	06:43:23
Start date:	06/08/2022
Path:	/tmp/4wiwmAupak
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: 4wiwmAupak PID: **6245**, Parent PID: **6238**

General

Start time:	06:43:23
Start date:	06/08/2022
Path:	/tmp/4wiwmAupak
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: 4wiwmAupak PID: **6251**, Parent PID: **6238**

General

Start time:	06:43:23

Start date:	06/08/2022
Path:	/tmp/4wiwmAupak
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: 4wiwmAupak PID: **6252**, Parent PID: **6238**

General

Start time:	06:43:23
Start date:	06/08/2022
Path:	/tmp/4wiwmAupak
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: 4wiwmAupak PID: **6253**, Parent PID: **6238**

General

Start time:	06:43:24
Start date:	06/08/2022
Path:	/tmp/4wiwmAupak
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: 4wiwmAupak PID: **6258**, Parent PID: **6238**

General

Start time:	06:43:24
Start date:	06/08/2022
Path:	/tmp/4wiwmAupak
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: 4wiwmAupak PID: **6259**, Parent PID: **6238**

General

Start time:	06:43:24
Start date:	06/08/2022
Path:	/tmp/4wiwmAupak
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: 4wiwmAupak PID: **6262**, Parent PID: **6238**

General

Start time:	06:43:24
Start date:	06/08/2022
Path:	/tmp/4wiwmAupak
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: 4wiwmAupak PID: **6265**, Parent PID: **6238**

General

Start time:	06:43:24

Start date:	06/08/2022
Path:	/tmp/4wiwmAupak
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: 4wiwmAupak PID: **6266**, Parent PID: **6238**

General

Start time:	06:43:24
Start date:	06/08/2022
Path:	/tmp/4wiwmAupak
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c

Analysis Process: 4wiwmAupak PID: **6268**, Parent PID: **6238**

General

Start time:	06:43:24
Start date:	06/08/2022
Path:	/tmp/4wiwmAupak
Arguments:	n/a
File size:	5777432 bytes
MD5 hash:	0083f1f0e77be34ad27f849842bbb00c