ID: 679624
Sample Name: Kr9mYMyujR
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 07:00:30
Date: 06/08/2022
Version: 35.0.0 Citrine

Table of Contents

Copyright Joe Security LLC 2022

Copyright Joe Security LLC 2022

Linux Analysis Report

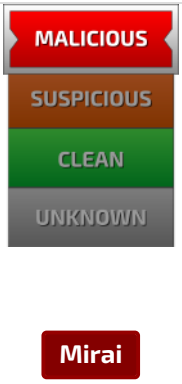
Kr9mYMyujR

Overview

General Information

Sample Name:	Kr9mYMyujR
Analysis ID:	679624
MD5:	8b9b5682e14d09.
SHA1:	d843aa17a4843b.
SHA256:	4531055787bdf4..
Tags:	32 arm elf mirai
Infos:	

Detection

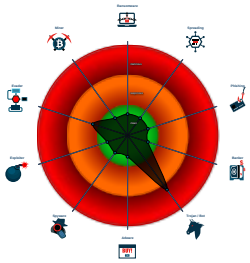


Score:	64
Range:	0 - 100
Whitelisted:	false

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.

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:	679624
Start date and time: 06/08/202207:00:30	2022-08-06 07:00:30 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Kr9mYMyujR
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/Kr9mYMyujR
PID:	6228
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Copyright Joe Security LLC 2022

Process Tree

- **system is lnxubuntu20**
- Kr9mYMyujR (PID: 6228, Parent: 6123, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/Kr9mYMyujR
  - Kr9mYMyujR New Fork (PID: 6230, Parent: 6228)
  - Kr9mYMyujR New Fork (PID: 6231, Parent: 6228)
  - Kr9mYMyujR New Fork (PID: 6232, Parent: 6228)
    - Kr9mYMyujR New Fork (PID: 6236, Parent: 6232)
    - Kr9mYMyujR New Fork (PID: 6237, Parent: 6232)
    - Kr9mYMyujR New Fork (PID: 6240, Parent: 6232)
    - Kr9mYMyujR New Fork (PID: 6242, Parent: 6232)
    - Kr9mYMyujR New Fork (PID: 6243, Parent: 6232)
    - Kr9mYMyujR New Fork (PID: 6246, Parent: 6232)
    - Kr9mYMyujR New Fork (PID: 6247, Parent: 6232)
    - Kr9mYMyujR New Fork (PID: 6250, Parent: 6232)
    - Kr9mYMyujR New Fork (PID: 6251, Parent: 6232)
    - Kr9mYMyujR New Fork (PID: 6252, Parent: 6232)
    - Kr9mYMyujR New Fork (PID: 6254, Parent: 6232)
    - Kr9mYMyujR New Fork (PID: 6255, Parent: 6232)
    - Kr9mYMyujR New Fork (PID: 6260, Parent: 6232)
    - Kr9mYMyujR New Fork (PID: 6261, Parent: 6232)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
Kr9mYMyujR	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	0x1be30:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1bea0:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1bf10:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1bf80:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1bff0:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1c260:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1c2b4:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1c308:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1c35c:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1c3b0:$xo1: oMXKNNC\x0D\x17\x0C\x12
Kr9mYMyujR	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
6228.1.00007f925803d000.00007f925803e000.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
6228.1.00007f9258017000.00007f9258034000.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	0x1be30:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1bea0:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1bf10:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1bf80:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1bff0:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1c260:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1c2b4:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1c308:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1c35c:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1c3b0:$xo1: oMXKNNC\x0D\x17\x0C\x12

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
6228.1.00007f9258017000.00007f9258034000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6231.1.00007f9258017000.00007f9258034000.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	• 0x1be30:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1bea0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1bf10:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1bf80:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1bff0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1c260:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1c2b4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1c308:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1c35c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1c3b0:$xo1: oMXKNNC\x0D\x17\x0C\x12
6231.1.00007f9258017000.00007f9258034000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
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

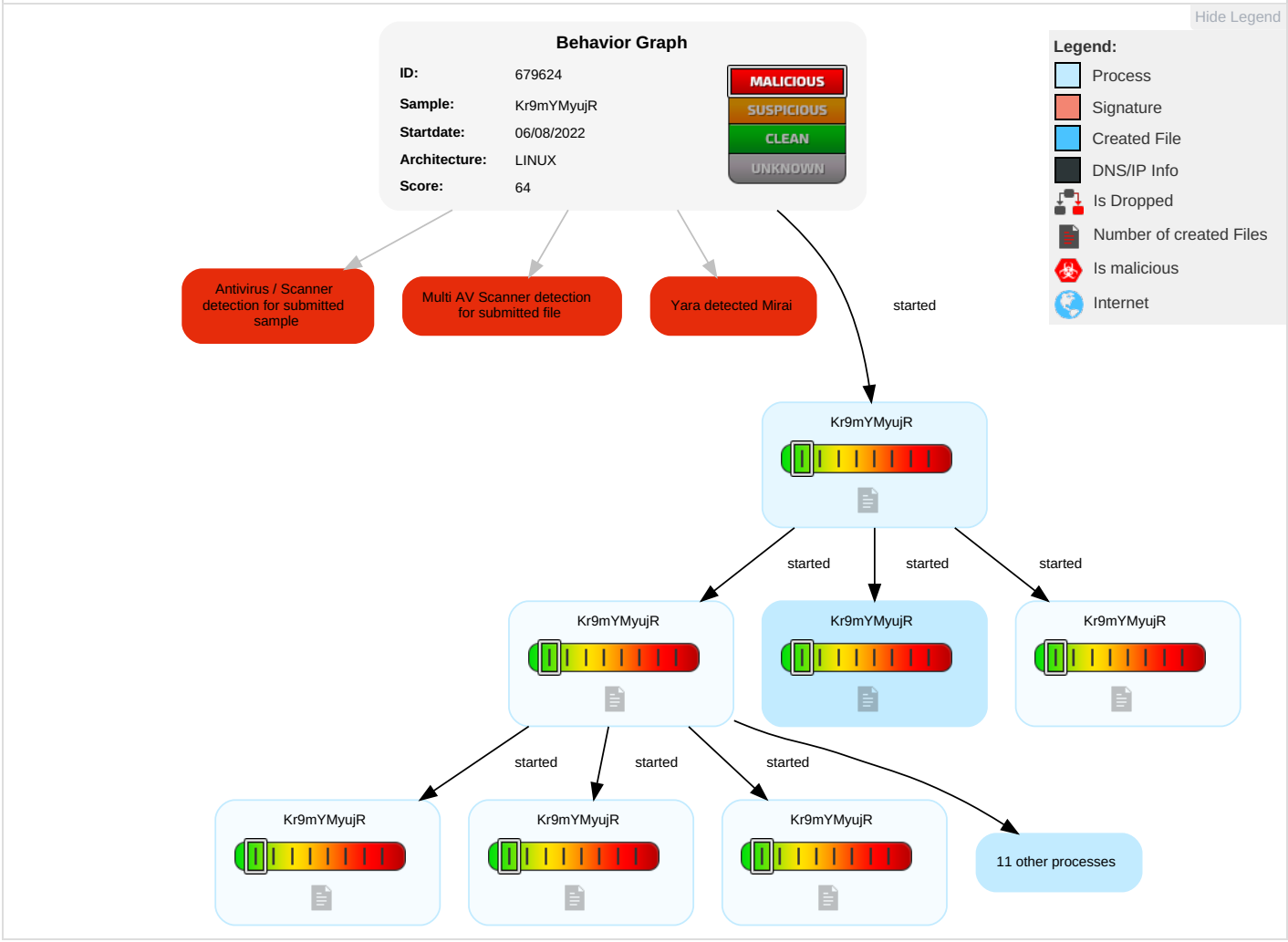
Mitre Att&ck Matrix

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	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
Kr9mYMyujR	62%	Virustotal		Browse
Kr9mYMyujR	34%	Metadefender		Browse
Kr9mYMyujR	69%	ReversingLabs	Linux.Trojan.Mirai	
Kr9mYMyujR	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

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
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 LSB executable, ARM, version 1 (ARM), statically linked, stripped
Entropy (8bit):	6.254459794987672
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	Kr9mYMyujR
File size:	119920
MD5:	8b9b5682e14d09f74ef586ebd9c2023a
SHA1:	d843aa17a4843b19a9bb67839e0a6a565dc8c99b
SHA256:	4531055787bdf40bc227b678922785a5f8e3994bf3efd2f611cc50d408a0f8dc
SHA512:	c3d6b447c9d91c0abe8a03396f9a104dd226ebfc759db2fd8116dd79d951e2d7860d6c6e3e2e9007acb968bc1dd630e4057e99cece3839df101d8efc5e07ee33
SSDEEP:	3072:aiNnGlqUjjaP1AKl0Py/tYaGKJ5NctVRa:BnGlq/0st3
TLSH:	E8C33B86AC91D925CBC223B7FA2F108D331593DCD2EA72439D281F6836CB55E1E37646
File Content Preview:	.ELF...a.....(.....4.....4. ...(.....Q.td.....-...L."....g.....0@-.\P...0....S.0...P@...0... ....R.....0...0.....0... ....R..... 0....S

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	ARM - ABI
ABI Version:	0
Entry Point Address:	0x8190
Flags:	0x202
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	119520
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	0x8094	0x94	0x18	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x80b0	0xb0	0x19ffc	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x220ac	0x1a0ac	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x220c0	0x1a0c0	0x2ae0	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x2d000	0x1d000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x2d008	0x1d008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x2d014	0x1d014	0x28c	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x2d2a0	0x1d2a0	0xa70	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x1d2a0	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	0x8000	0x8000	0x1cba0	0x1cba0	6.3025	0x5	R E	0x8000		.init .text .fini .rodata
LOAD	0x1d000	0x2d000	0x2d000	0x2a0	0xd10	2.8807	0x6	RW	0x8000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Copyright Joe Security LLC 2022

Network Behavior

No network behavior found

System Behavior

Analysis Process: Kr9mYMyujR PID: 6228, Parent PID: 6123

General

Start time:	07:01:16
Start date:	06/08/2022
Path:	/tmp/Kr9mYMyujR
Arguments:	/tmp/Kr9mYMyujR
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: Kr9mYMyujR PID: 6230, Parent PID: 6228

General

Start time:	07:01:16
Start date:	06/08/2022
Path:	/tmp/Kr9mYMyujR
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: Kr9mYMyujR PID: 6231, Parent PID: 6228

General

Start time:	07:01:16
Start date:	06/08/2022
Path:	/tmp/Kr9mYMyujR
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: Kr9mYMyujR PID: 6232, Parent PID: 6228

General

Start time:	07:01:16
Start date:	06/08/2022
Path:	/tmp/Kr9mYMyujR
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: Kr9mYMyujR PID: 6236, Parent PID: 6232

General

Start time:	07:01:16

Copyright Joe Security LLC 2022

Start date:	06/08/2022
Path:	/tmp/Kr9mYMyujR
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: Kr9mYMyujR PID: **6237**, Parent PID: **6232**

General

Start time:	07:01:16
Start date:	06/08/2022
Path:	/tmp/Kr9mYMyujR
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: Kr9mYMyujR PID: **6240**, Parent PID: **6232**

General

Start time:	07:01:16
Start date:	06/08/2022
Path:	/tmp/Kr9mYMyujR
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: Kr9mYMyujR PID: **6242**, Parent PID: **6232**

General

Start time:	07:01:16
Start date:	06/08/2022
Path:	/tmp/Kr9mYMyujR
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: Kr9mYMyujR PID: **6243**, Parent PID: **6232**

General

Start time:	07:01:16
Start date:	06/08/2022
Path:	/tmp/Kr9mYMyujR
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: Kr9mYMyujR PID: **6246**, Parent PID: **6232**

General

Start time:	07:01:16
Start date:	06/08/2022
Path:	/tmp/Kr9mYMyujR
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: Kr9mYMyujR PID: **6247**, Parent PID: **6232**

General

Start time:	07:01:16

Copyright Joe Security LLC 2022

Start date:	06/08/2022
Path:	/tmp/Kr9mYMyujR
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: Kr9mYMyujR PID: **6250**, Parent PID: **6232**

General

Start time:	07:01:16
Start date:	06/08/2022
Path:	/tmp/Kr9mYMyujR
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: Kr9mYMyujR PID: **6251**, Parent PID: **6232**

General

Start time:	07:01:16
Start date:	06/08/2022
Path:	/tmp/Kr9mYMyujR
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: Kr9mYMyujR PID: **6252**, Parent PID: **6232**

General

Start time:	07:01:16
Start date:	06/08/2022
Path:	/tmp/Kr9mYMyujR
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: Kr9mYMyujR PID: **6254**, Parent PID: **6232**

General

Start time:	07:01:16
Start date:	06/08/2022
Path:	/tmp/Kr9mYMyujR
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: Kr9mYMyujR PID: **6255**, Parent PID: **6232**

General

Start time:	07:01:16
Start date:	06/08/2022
Path:	/tmp/Kr9mYMyujR
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: Kr9mYMyujR PID: **6260**, Parent PID: **6232**

General

Start time:	07:01:16

Copyright Joe Security LLC 2022

Start date:	06/08/2022
Path:	/tmp/Kr9mYMyujR
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: Kr9mYMyujR PID: **6261**, Parent PID: **6232**

General

Start time:	07:01:16
Start date:	06/08/2022
Path:	/tmp/Kr9mYMyujR
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Copyright Joe Security LLC 2022