ID: 679630
Sample Name: tknjinyyHK
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 07:26:25
Date: 06/08/2022
Version: 35.0.0 Citrine

Table of Contents

Linux Analysis Report

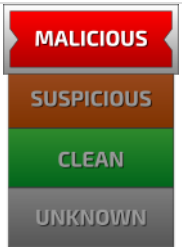
tknjinyyHK

Overview

General Information

Sample Name:	tknjinyyHK
Analysis ID:	679630
MD5:	207b92b6ce447a..
SHA1:	a2b8c7518f370a..
SHA256:	7274ee8cc094cd..
Tags:	32 elf intel mirai
Infos:	

Detection



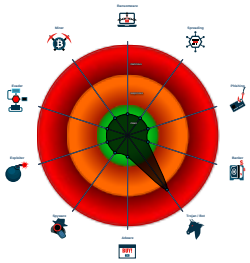
Mirai

Score:	76
Range:	0 - 100
Whitelisted:	false

Signatures

- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Yara detected Mirai
- Machine Learning detection for sam…
- Enumerates processes within the "p…
- Yara signature match
- Sample contains strings that are po…
- Sample has stripped symbol table
- Sample contains strings indicative o…

Classification



General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679630
Start date and time: 06/08/202207:26:25	2022-08-06 07:26:25 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	tknjinyyHK
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:	mal76.troj.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/tknjinyyHK
PID:	6235
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Process Tree

- **system is lnxubuntu20**

- tknjinyyHK (PID: 6235, Parent: 6126, MD5: 207b92b6ce447a8be88fee4f5ab257d6) Arguments: /tmp/tknjinyyHK
  - tknjinyyHK New Fork (PID: 6236, Parent: 6235)
  - tknjinyyHK New Fork (PID: 6237, Parent: 6235)
  - tknjinyyHK New Fork (PID: 6238, Parent: 6235)
    - tknjinyyHK New Fork (PID: 6239, Parent: 6238)
    - tknjinyyHK New Fork (PID: 6240, Parent: 6238)
    - tknjinyyHK New Fork (PID: 6242, Parent: 6238)
    - tknjinyyHK New Fork (PID: 6243, Parent: 6238)
    - tknjinyyHK New Fork (PID: 6244, Parent: 6238)
    - tknjinyyHK New Fork (PID: 6245, Parent: 6238)
    - tknjinyyHK New Fork (PID: 6246, Parent: 6238)
    - tknjinyyHK New Fork (PID: 6247, Parent: 6238)
    - tknjinyyHK New Fork (PID: 6248, Parent: 6238)
    - tknjinyyHK New Fork (PID: 6249, Parent: 6238)
    - tknjinyyHK New Fork (PID: 6250, Parent: 6238)
    - tknjinyyHK New Fork (PID: 6251, Parent: 6238)
    - tknjinyyHK New Fork (PID: 6252, Parent: 6238)
    - tknjinyyHK New Fork (PID: 6253, Parent: 6238)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
tknjinyyHK	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	0x18b9c:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x18c0c:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x18c7c:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x18cec:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x18d5c:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x18fcc:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x19020:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x19074:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x190c8:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x1911c:$xo1: oMXKNNC\x0D\x17\x0C\x12
tknjinyyHK	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
tknjinyyHK	Linux_Trojan_Mirai_fa3ad9d0	unknown	unknown	0x3b2a:$a: CB 08 C1 CB 10 66 C1 CB 08 31 C9 8A 4F 1 4 D3 E8 01 D8 66 C1
tknjinyyHK	Linux_Trojan_Mirai_b14f4c5d	unknown	unknown	0x5970:$a: 53 31 DB 8B 4C 24 0C 8B 54 24 08 83 F9 01 76 15 66 8B 02 83 E9 02 25 FF FF 00 00 83 C2 02 01 C3 83 F9 01 77 EB 49 75 05 0F BE 02 01 C3
tknjinyyHK	Linux_Trojan_Mirai_93fc3657	unknown	unknown	0x3bb5:$a: 00 00 00 89 44 24 60 89 D1 31 C0 8B 7C 24 28 FC F3 AB 89 D1 8B 7C

Click to see the 8 entries

Memory Dumps

Source	Rule	Description	Author	Strings
6235.1.000000000905c000.000000000905d000.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	0x740:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x7b8:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x830:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x8a8:$xo1: oMXKNNC\x0D\x17\x0C\x12 0x920:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xbb0:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xc08:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xc60:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xcb8:$xo1: oMXKNNC\x0D\x17\x0C\x12 0xd10:$xo1: oMXKNNC\x0D\x17\x0C\x12

Source	Rule	Description	Author	Strings
6237.1.000000000905c000.000000000905d000.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	• 0x740:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x7b8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x830:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x8a8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x920:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xbb0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xc08:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xc60:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xcb8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xd10:$xo1: oMXKNNC\x0D\x17\x0C\x12
6235.1.0000000008062000.0000000008063000.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	• 0x20:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x74:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xc8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11c:$xo1: oMXKNNC\x0D\x17\x0C\x12
6237.1.0000000008062000.0000000008063000.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	• 0x20:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x74:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0xc8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x11c:$xo1: oMXKNNC\x0D\x17\x0C\x12
6235.1.0000000008048000.0000000008062000.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	• 0x18b9c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x18c0c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x18c7c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x18cec:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x18d5c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x18fcc:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x19020:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x19074:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x190c8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x1911c:$xo1: oMXKNNC\x0D\x17\x0C\x12
Click to see the 25 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

Machine Learning detection for sample

System Summary

Malicious sample detected (through community Yara rule)

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

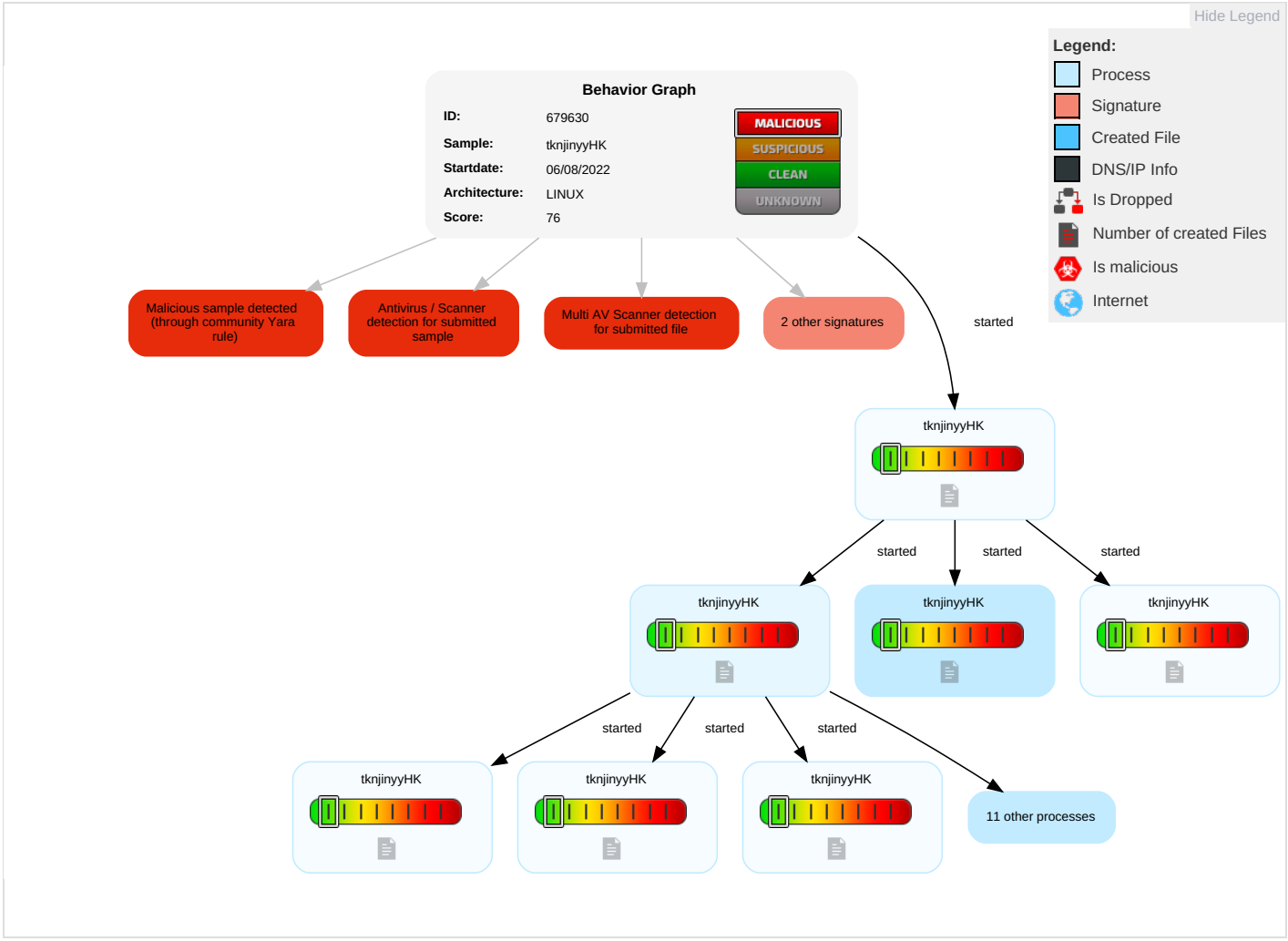
Mitre Att&ck Matrix

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	System Service 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
tknjinyyHK	56%	Virustotal		Browse
tknjinyyHK	37%	Metadefender		Browse
tknjinyyHK	69%	ReversingLabs	Linux.Trojan.Mirai	
tknjinyyHK	100%	Avira	LINUX/Mirai.haqdn	
tknjinyyHK	100%	Joe Sandbox ML		

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	

Source	Detection	Scanner	Label	Link
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, Intel 80386, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.581459410183035

TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	tknjinyyHK
File size:	106256
MD5:	207b92b6ce447a8be88fee4f5ab257d6
SHA1:	a2b8c7518f370a978dda19ade031c9d1885acb5e
SHA256:	7274ee8cc094cdfcab48b23978837b12d01bd426202f34d7191e0f6fc3ae18d3
SHA512:	7fc6f244884ccad21fb96a9a08062255d00f81a25e380d6d0ac5a591d836510d3d8cd0ae8886c59f6a9c3b7f2d394245634f46594c46a76f3fbfad7f119a9280
SSDEEP:	3072:LTPT78lIJrWP9qJsSNJQ7RJndlfbpkxTWY25eeJBDcpPY:bwGVWPYVNqNJPpksJJ0
TLSH:	51A33AC9E693E0F6DC005ABC306BAF329D73E93F6126DAD6E3E45C73A54550181072AE
File Content Preview:	.ELF.....d...4.....4. ...(..... ... .$...$+..$+.....Q.td.....U..S.....h.....m..[]...$.....U.....=@- ...t..5....d+.....d+.....u.....t....h .....

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	Intel 80386
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x8048164
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	105856
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	0x8048094	0x94	0x1c	0x0	0x6	AX	0	0	1
.text	PROGBITS	0x80480b0	0xb0	0x16db6	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x805ee66	0x16e66	0x17	0x0	0x6	AX	0	0	1
.rodata	PROGBITS	0x805ee80	0x16e80	0x2ca0	0x0	0x2	A	0	0	32
.ctors	PROGBITS	0x8062b24	0x19b24	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x8062b2c	0x19b2c	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x8062b60	0x19b60	0x1e0	0x0	0x3	WA	0	0	32
.bss	NOBITS	0x8062d40	0x19d40	0xe80	0x0	0x3	WA	0	0	32
.shstrtab	STRTAB	0x0	0x19d40	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	0x8048000	0x8048000	0x19b20	0x19b20	6.5992	0x5	R E	0x1000		.init .text .fini .rodata
LOAD	0x19b24	0x8062b24	0x8062b24	0x21c	0x109c	3.4802	0x6	RW	0x1000		.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: tknjinyyHK PID: 6235, Parent PID: 6126

General

Start time:	07:27:10
Start date:	06/08/2022
Path:	/tmp/tknjinyyHK
Arguments:	/tmp/tknjinyyHK
File size:	106256 bytes
MD5 hash:	207b92b6ce447a8be88fee4f5ab257d6

Analysis Process: tknjinyyHK PID: 6236, Parent PID: 6235

General

Start time:	07:27:10
Start date:	06/08/2022
Path:	/tmp/tknjinyyHK
Arguments:	n/a
File size:	106256 bytes
MD5 hash:	207b92b6ce447a8be88fee4f5ab257d6

File Activities

File Read

Directory Enumerated

Analysis Process: tknjinyyHK PID: 6237, Parent PID: 6235

General

Start time:	07:27:10
Start date:	06/08/2022
Path:	/tmp/tknjinyyHK
Arguments:	n/a
File size:	106256 bytes
MD5 hash:	207b92b6ce447a8be88fee4f5ab257d6

Analysis Process: tknjinyyHK PID: 6238, Parent PID: 6235

General

Start time:	07:27:10
Start date:	06/08/2022
Path:	/tmp/tknjinyyHK
Arguments:	n/a
File size:	106256 bytes
MD5 hash:	207b92b6ce447a8be88fee4f5ab257d6

Analysis Process: tknjinyyHK PID: 6239, Parent PID: 6238

General

Start time:	07:27:10
Start date:	06/08/2022
Path:	/tmp/tknjinyyHK
Arguments:	n/a
File size:	106256 bytes
MD5 hash:	207b92b6ce447a8be88fee4f5ab257d6

Analysis Process: tknjinyyHK PID: **6240**, Parent PID: **6238**

General

Start time:	07:27:10
Start date:	06/08/2022
Path:	/tmp/tknjinyyHK
Arguments:	n/a
File size:	106256 bytes
MD5 hash:	207b92b6ce447a8be88fee4f5ab257d6

Analysis Process: tknjinyyHK PID: **6242**, Parent PID: **6238**

General

Start time:	07:27:10
Start date:	06/08/2022
Path:	/tmp/tknjinyyHK
Arguments:	n/a
File size:	106256 bytes
MD5 hash:	207b92b6ce447a8be88fee4f5ab257d6

Analysis Process: tknjinyyHK PID: **6243**, Parent PID: **6238**

General

Start time:	07:27:10
Start date:	06/08/2022
Path:	/tmp/tknjinyyHK
Arguments:	n/a
File size:	106256 bytes
MD5 hash:	207b92b6ce447a8be88fee4f5ab257d6

Analysis Process: tknjinyyHK PID: **6244**, Parent PID: **6238**

General

Start time:	07:27:10
Start date:	06/08/2022
Path:	/tmp/tknjinyyHK
Arguments:	n/a
File size:	106256 bytes
MD5 hash:	207b92b6ce447a8be88fee4f5ab257d6

Analysis Process: tknjinyyHK PID: **6245**, Parent PID: **6238**

General

Start time:	07:27:10
Start date:	06/08/2022
Path:	/tmp/tknjinyyHK
Arguments:	n/a
File size:	106256 bytes
MD5 hash:	207b92b6ce447a8be88fee4f5ab257d6

Analysis Process: tknjinyyHK PID: **6246**, Parent PID: **6238**

General

Start time:	07:27:10
Start date:	06/08/2022
Path:	/tmp/tknjinyyHK
Arguments:	n/a
File size:	106256 bytes
MD5 hash:	207b92b6ce447a8be88fee4f5ab257d6

Analysis Process: tknjinyyHK PID: **6247**, Parent PID: **6238**

General

Start time:	07:27:10
Start date:	06/08/2022
Path:	/tmp/tknjinyyHK
Arguments:	n/a
File size:	106256 bytes
MD5 hash:	207b92b6ce447a8be88fee4f5ab257d6

Analysis Process: tknjinyyHK PID: **6248**, Parent PID: **6238**

General

Start time:	07:27:10
Start date:	06/08/2022
Path:	/tmp/tknjinyyHK
Arguments:	n/a
File size:	106256 bytes
MD5 hash:	207b92b6ce447a8be88fee4f5ab257d6

Analysis Process: tknjinyyHK PID: **6249**, Parent PID: **6238**

General

Start time:	07:27:10
Start date:	06/08/2022
Path:	/tmp/tknjinyyHK
Arguments:	n/a
File size:	106256 bytes
MD5 hash:	207b92b6ce447a8be88fee4f5ab257d6

Analysis Process: tknjinyyHK PID: **6250**, Parent PID: **6238**

General

Start time:	07:27:10
Start date:	06/08/2022
Path:	/tmp/tknjinyyHK
Arguments:	n/a
File size:	106256 bytes
MD5 hash:	207b92b6ce447a8be88fee4f5ab257d6

Analysis Process: tknjinyyHK PID: **6251**, Parent PID: **6238**

General

Start time:	07:27:10
Start date:	06/08/2022
Path:	/tmp/tknjinyyHK
Arguments:	n/a
File size:	106256 bytes
MD5 hash:	207b92b6ce447a8be88fee4f5ab257d6

Analysis Process: tknjinyyHK PID: **6252**, Parent PID: **6238**

General

Start time:	07:27:10
Start date:	06/08/2022
Path:	/tmp/tknjinyyHK
Arguments:	n/a
File size:	106256 bytes
MD5 hash:	207b92b6ce447a8be88fee4f5ab257d6

Analysis Process: tknjinyyHK PID: **6253**, Parent PID: **6238**

General

Start time:	07:27:10
Start date:	06/08/2022
Path:	/tmp/tknjinyyHK
Arguments:	n/a
File size:	106256 bytes
MD5 hash:	207b92b6ce447a8be88fee4f5ab257d6