

JoeSandbox Cloud BASIC



ID: 756333

Sample Name: KezTmruoNx.elf

Cookbook:

defaultlinuxfilecookbook.jbs

Time: 01:53:31

Date: 30/11/2022

Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents	2
Linux Analysis Report KezTmruoNx.elf	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Analysis Advice	4
General Information	4
Runtime Messages	4
Process Tree	5
Yara Signatures	5
Initial Sample	5
Memory Dumps	6
Snort Signatures	7
Joe Sandbox Signatures	7
AV Detection	7
System Summary	7
Stealing of Sensitive Information	7
Remote Access Functionality	7
Mitre Att&ck Matrix	8
Malware Configuration	8
Behavior Graph	8
Screenshots	9
Thumbnails	9
Antivirus, Machine Learning and Genetic Malware Detection	9
Initial Sample	9
Dropped Files	9
Domains	9
URLs	10
Domains and IPs	10
Contacted Domains	10
World Map of Contacted IPs	10
Public IPs	10
Joe Sandbox View / Context	10
IPs	10
Domains	10
ASNs	11
JA3 Fingerprints	11
Dropped Files	11
Created / dropped Files	11
Static File Info	11
General	11
Static ELF Info	11
ELF header	11
Sections	12
Program Segments	12
Network Behavior	12
Network Port Distribution	12
TCP Packets	12
System Behavior	12
Analysis Process: KezTmruoNx.elf PID: 6230, Parent PID: 6123	12
General	12
File Activities	13
File Read	13
Analysis Process: KezTmruoNx.elf PID: 6232, Parent PID: 6230	13
General	13
File Activities	13
File Read	13
Directory Enumerated	13
Analysis Process: KezTmruoNx.elf PID: 6233, Parent PID: 6230	13
General	13
Analysis Process: KezTmruoNx.elf PID: 6234, Parent PID: 6230	13
General	13
Analysis Process: xfce4-panel PID: 6242, Parent PID: 2063	13
General	13
Analysis Process: wrapper-2.0 PID: 6242, Parent PID: 2063	13
General	13
File Activities	13
File Read	13
Analysis Process: xfce4-panel PID: 6243, Parent PID: 2063	14
General	14
Analysis Process: wrapper-2.0 PID: 6243, Parent PID: 2063	14
General	14
File Activities	14
File Read	14

Analysis Process: xfce4-panel PID: 6244, Parent PID: 2063	14
General	14
Analysis Process: wrapper-2.0 PID: 6244, Parent PID: 2063	14
General	14
File Activities	14
File Read	14
Analysis Process: xfce4-panel PID: 6245, Parent PID: 2063	14
General	14
Analysis Process: wrapper-2.0 PID: 6245, Parent PID: 2063	14
General	15
File Activities	15
File Read	15
Analysis Process: xfce4-panel PID: 6246, Parent PID: 2063	15
General	15
Analysis Process: wrapper-2.0 PID: 6246, Parent PID: 2063	15
General	15
File Activities	15
File Read	15
Analysis Process: xfce4-panel PID: 6247, Parent PID: 2063	15
General	15
Analysis Process: wrapper-2.0 PID: 6247, Parent PID: 2063	15
General	15
File Activities	15
File Read	15

Linux Analysis Report

KezTmruoNx.elf

Overview

General Information

Sample Name:

KezTmruoNx.elf

Analysis ID:

756333

MD5:

e7c14f0a444293..

SHA1:

e71ef6d9a269ae..

SHA256:

6544527833a0cf..

Tags:

32

elf

mirai

renesas

Infos:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Mirai

Score:

68

Range:

0 - 100

Whitelisted:

false

Signatures

Malicious sample detected (through...

Yara detected Mirai

Multi AV Scanner detection for subm...

Sample tries to kill multiple process...

Yara signature match

Sample has stripped symbol table

Uses the "uname" system call to qu...

Enumerates processes within the "p...

Tries to connect to HTTP servers, b...

Detected TCP or UDP traffic on non...

Sample tries to kill a process (SIGK...

Classification

Analysis Advice

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

All HTTP servers contacted by the sample do not answer. The sample is likely an old dropper which does no longer work.

General Information	
Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756333
Start date and time:	2022-11-30 01:53:31 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	KezTmruoNx.elf
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:	mal68.spre.troj.linELF@0/0@0/0

Runtime Messages	
Command:	/tmp/KezTmruoNx.elf
PID:	6230
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	lzrd cock fest"/proc"/exe
Standard Error:	

Copyright Joe Security LLC 2022

Page 4 of 15

Process Tree

- **system is Inxubuntu20**
- **KezTmruoNx.elf** (PID: 6230, Parent: 6123, MD5: 8943e5f8f8c280467b4472c15ae93ba9) Arguments: /tmp/KezTmruoNx.elf
 - **KezTmruoNx.elf** New Fork (PID: 6232, Parent: 6230)
 - **KezTmruoNx.elf** New Fork (PID: 6233, Parent: 6230)
 - **KezTmruoNx.elf** New Fork (PID: 6234, Parent: 6230)
- **xfce4-panel** New Fork (PID: 6242, Parent: 2063)
- **wrapper-2.0** (PID: 6242, Parent: 2063, MD5: ac0b8a906f359a8ae102244738682e76) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libsystray.so 6 12582920 systray "Notification Area" "Area where notification icons appear"
- **xfce4-panel** New Fork (PID: 6243, Parent: 2063)
- **wrapper-2.0** (PID: 6243, Parent: 2063, MD5: ac0b8a906f359a8ae102244738682e76) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libstatusnotifier.so 7 12582921 statusnotifier "Status Notifier Plugin" "Provides a panel area for status notifier items (application indicators)"
- **xfce4-panel** New Fork (PID: 6244, Parent: 2063)
- **wrapper-2.0** (PID: 6244, Parent: 2063, MD5: ac0b8a906f359a8ae102244738682e76) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libpulseaudio-plugin.so 8 12582922 pulseaudio "PulseAudio Plugin" "Adjust the audio volume of the PulseAudio sound system"
- **xfce4-panel** New Fork (PID: 6245, Parent: 2063)
- **wrapper-2.0** (PID: 6245, Parent: 2063, MD5: ac0b8a906f359a8ae102244738682e76) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libxfce4powermanager.so 9 12582923 power-manager-plugin "Power Manager Plugin" "Display the battery levels of your devices and control the brightness of your display"
- **xfce4-panel** New Fork (PID: 6246, Parent: 2063)
- **wrapper-2.0** (PID: 6246, Parent: 2063, MD5: ac0b8a906f359a8ae102244738682e76) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libnotification-plugin.so 10 12582924 notification-plugin "Notification Plugin" "Notification plugin for the Xfce panel"
- **xfce4-panel** New Fork (PID: 6247, Parent: 2063)
- **wrapper-2.0** (PID: 6247, Parent: 2063, MD5: ac0b8a906f359a8ae102244738682e76) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libactions.so 14 12582925 actions "Action Buttons" "Log out, lock or other system actions"
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
KezTmruoNx.elf	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
KezTmruoNx.elf	Linux_Trojan_Gafigyt_28a2fe0c	unknown	unknown	● 0xab04:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F ● 0xab18:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F ● 0xab2c:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F ● 0xab40:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F ● 0xab54:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F ● 0xab68:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F ● 0xab7c:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F ● 0xab90:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F ● 0xaba4:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F ● 0xabb8:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F ● 0xabcc:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F ● 0xabe0:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F ● 0xabf4:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F ● 0xac08:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F ● 0xac1c:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F ● 0xac30:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F ● 0xac44:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F ● 0xac58:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F ● 0xac6c:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F ● 0xac80:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F ● 0xac94:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
KezTmruoNx.elf	Linux_Trojan_Gafigyt_ea92cca8	unknown	unknown	● 0xb05c:\$a: 53 65 6C 66 20 52 65 70 20 46 75 63 6B 69 6 E 67 20 4E 65 54 69 53 20 61 6E 64

Memory Dumps				
Source	Rule	Description	Author	Strings
6234.1.00007f20b0400000.00007f20b040c000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6234.1.00007f20b0400000.00007f20b040c000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0xab04:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xab18:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xab2c:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xab40:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xab54:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xab68:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xab7c:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xab90:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xaba4:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xabb8:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xabcc:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xabe0:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xabf4:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xac08:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xac1c:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xac30:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xac44:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xac58:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xac6c:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xac80:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xac94:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
6234.1.00007f20b0400000.00007f20b040c000.r-x.sdmp	Linux_Trojan_Gafgyt_ea92cca8	unknown	unknown	• 0xb05c:\$a: 53 65 6C 66 20 52 65 70 20 46 75 63 6B 69 6 E 67 20 4E 65 54 69 53 20 61 6E 64
6233.1.00007f20b0400000.00007f20b040c000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
6233.1.00007f20b0400000.00007f20b040c000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	0xab04:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0xab18:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0xab2c:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0xab40:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0xab54:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0xab68:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0xab7c:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0xab90:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0xaba4:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0xabb8:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0xabcc:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0xabe0:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0xabf4:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0xac08:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0xac1c:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0xac30:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0xac44:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0xac58:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0xac6c:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0xac80:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F 0xac94:\$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 4 9 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
Click to see the 10 entries				

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

System Summary

Malicious sample detected (through community Yara rule)

Sample tries to kill multiple processes (SIGKILL)

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

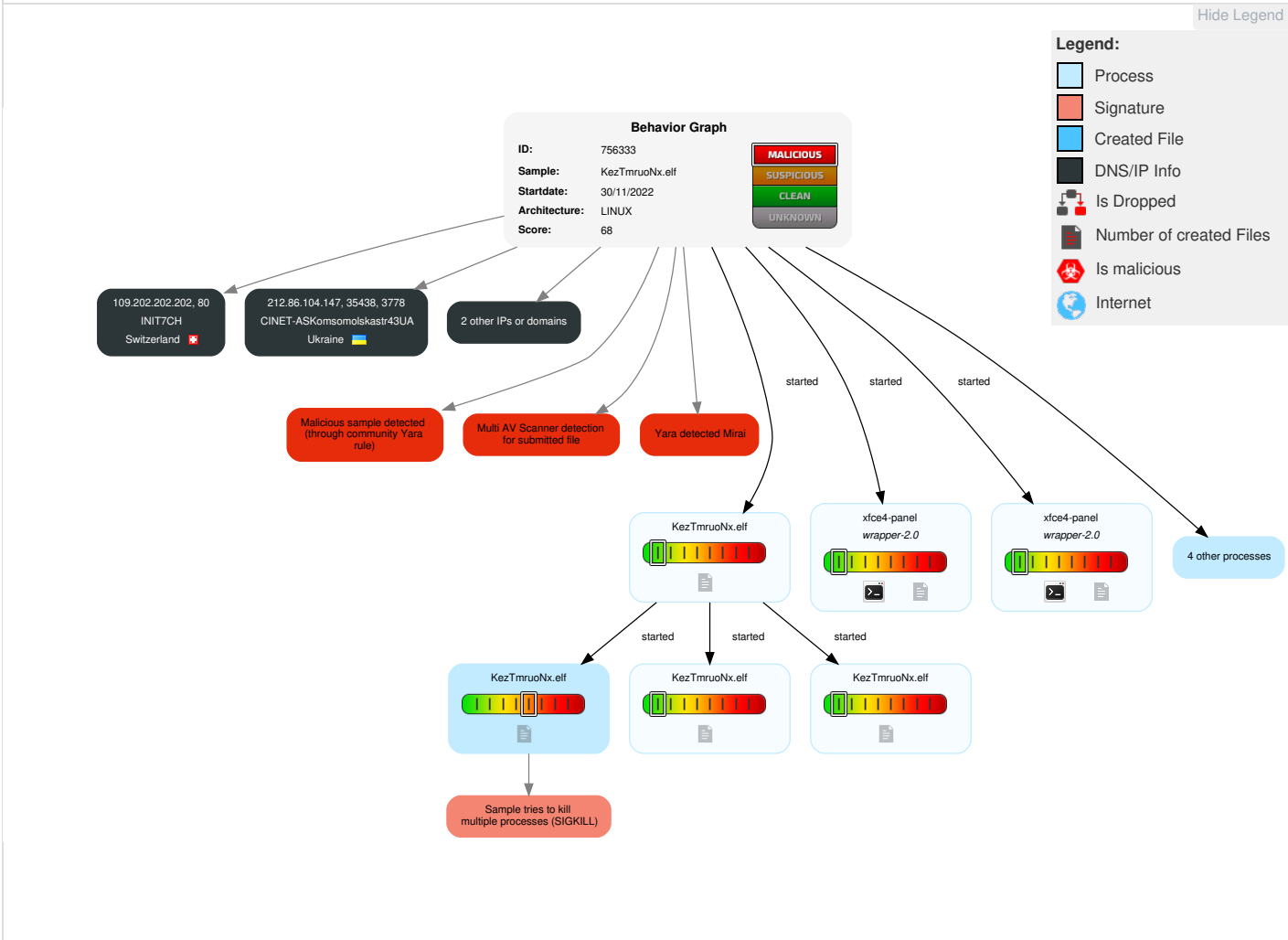
Mitre Att&ck Matrix

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	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Service Stop
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Malware Configuration

No configs have been found

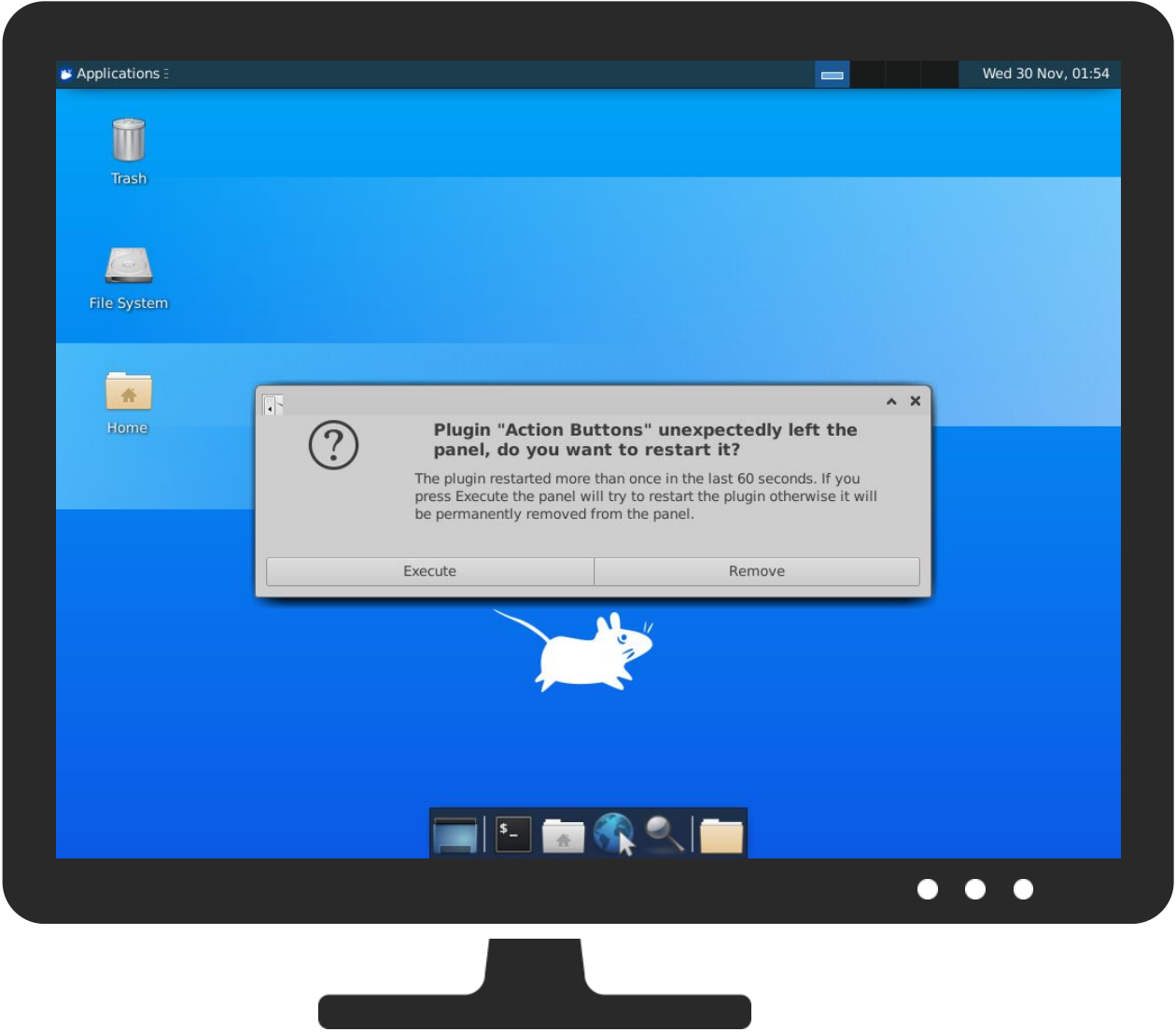
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
KezTmruoNx.elf	62%	ReversingLabs	Linux.Trojan.Mirai	
KezTmruoNx.elf	62%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

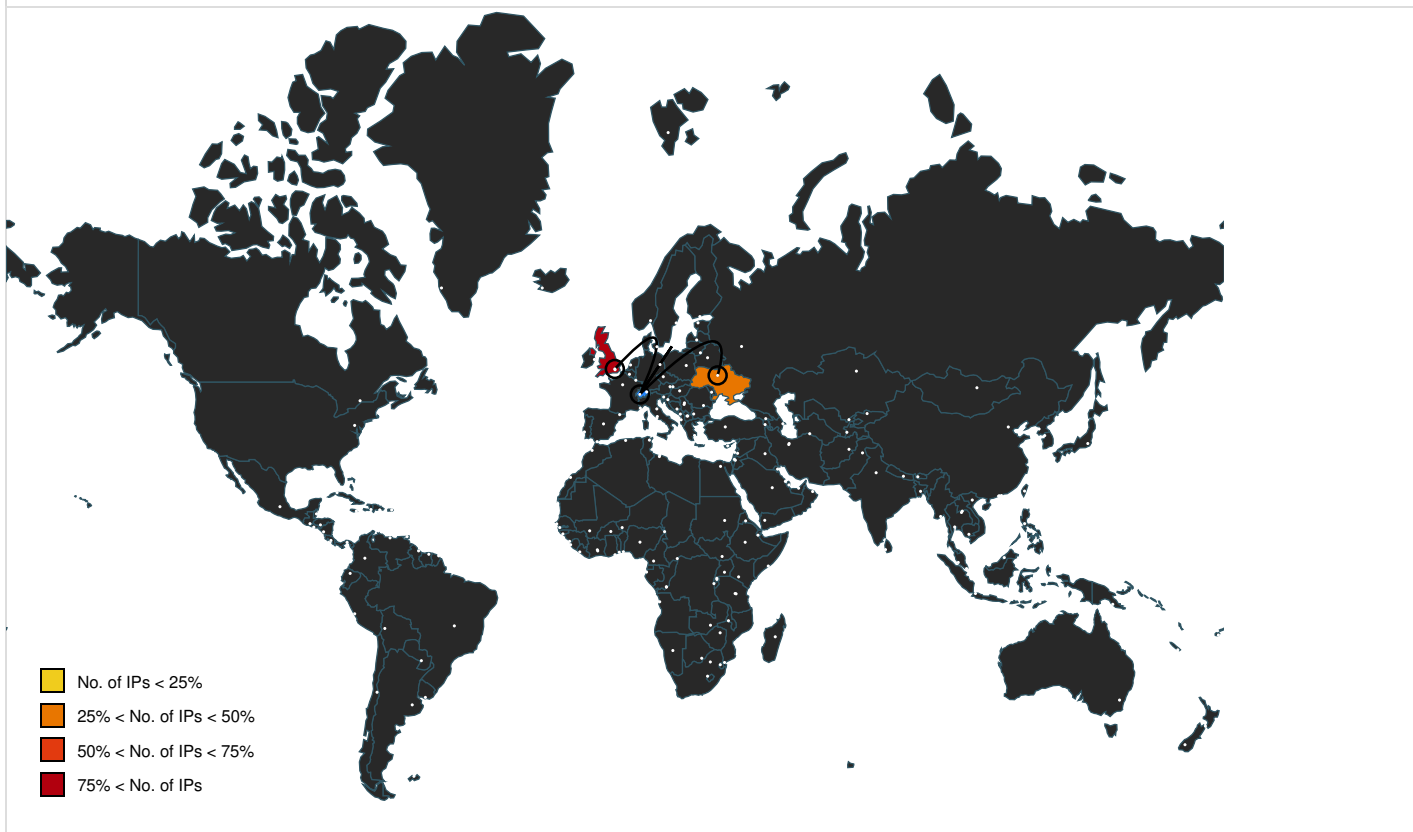
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
212.86.104.147	unknown	Ukraine		12792	CINET-ASKomsomolskastr43UA	false
109.202.202.202	unknown	Switzerland		13030	INIT7CH	false
91.189.91.43	unknown	United Kingdom		41231	CANONICAL-ASGB	false
91.189.91.42	unknown	United Kingdom		41231	CANONICAL-ASGB	false

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, Renesas SH, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.73460472712052
TrID:	ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	KezTmruoNx.elf
File size:	50168
MD5:	e7c14f0a444293a097925250df033d1d
SHA1:	e71ef6d9a269aeb59cb643720a2b6d88da44ff42
SHA256:	6544527833a0cfaf1a9e0cc9718033e55bac47b2f242f90864849ca2f4726263
SHA512:	d47561571ca58f4206aa9ad987ff57c7a56adf2a3ad8cd61373b3add373da797959e35909d8bcfe32c4313e679d970c92de4634620f37404a164326026757428
SSDEEP:	768:Oa2vU7eng2qGJert7LrLMU6fgatQh+YbT/9+m3CZQoV/bnmCozw:Oa4U7G7SvT6ftBTm3KVrmCo8
TLSH:	96336C36E029DED0C6560134A4E88F751F03F1C883536EBB2AE546B2645396CFA19FF4
File Content Preview:	.ELF.....*.....@.4...h.....4. ...(.@.....@...@.....A...A.(...<.....Q.td...../."O.n.....#. *@.....#. *@.....o&O.n...l...../.../a"O.l...n...a.b("...q.

Static ELF Info

ELF header

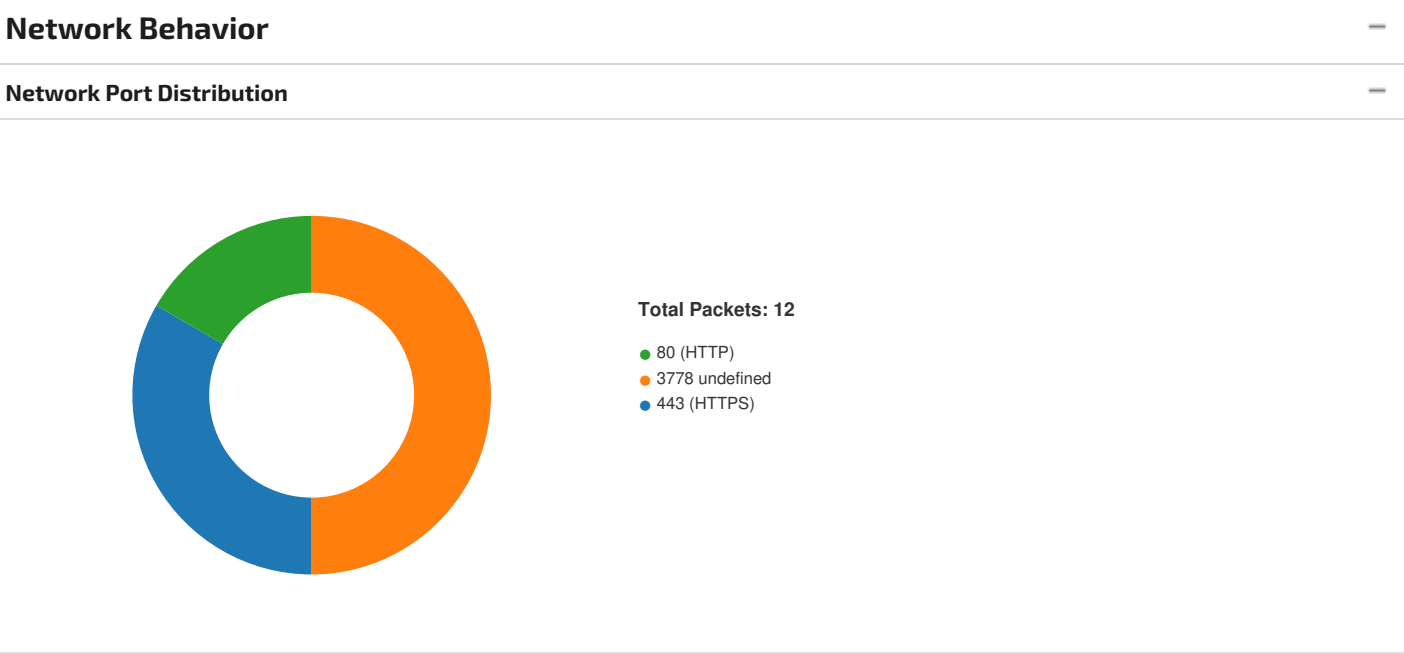
Class:	
Data:	
Version:	
Machine:	
Version Number:	
Type:	
OS/ABI:	
ABI Version:	
Entry Point Address:	
Flags:	
ELF Header Size:	
Program Header Offset:	
Program Header Size:	
Number of Program Headers:	
Section Header Offset:	
Section Header Size:	
Number of Section Headers:	
Header String Table Index:	

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	0x30	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x4000e0	0xe0	0xaa00	0x0	0x6	AX	0	0	32
.fini	PROGBITS	0x40aae0	0xaae0	0x24	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x40ab04	0xab04	0x113c	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x41c000	0xc000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x41c008	0xc008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x41c014	0xc014	0x214	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x41c228	0xc228	0x314	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0xc228	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	0x400000	0x400000	0xbc40	0xbc40	6.8560	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0xc000	0x41c000	0x41c000	0x228	0x53c	3.0262	0x6	RW	0x10000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		



TCP Packets

System Behavior

Analysis Process: KezTmruoNx.elf PID: 6230, Parent PID: 6123

General	
Start time:	01:54:17
Start date:	30/11/2022
Path:	/tmp/KezTmruoNx.elf
Arguments:	/tmp/KezTmruoNx.elf
File size:	4139976 bytes
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9

File Activities		—
File Read		▼
Analysis Process: KezTmruoNx.elf PID: 6232, Parent PID: 6230		—
General		—
Start time:	01:54:17	
Start date:	30/11/2022	
Path:	/tmp/KezTmruoNx.elf	
Arguments:	n/a	
File size:	4139976 bytes	
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9	

File Activities		—
File Read		▼
Directory Enumerated		▼

Analysis Process: KezTmruoNx.elf PID: 6233, Parent PID: 6230		—
General		—
Start time:	01:54:17	
Start date:	30/11/2022	
Path:	/tmp/KezTmruoNx.elf	
Arguments:	n/a	
File size:	4139976 bytes	
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9	

Analysis Process: KezTmruoNx.elf PID: 6234, Parent PID: 6230		—
General		—
Start time:	01:54:17	
Start date:	30/11/2022	
Path:	/tmp/KezTmruoNx.elf	
Arguments:	n/a	
File size:	4139976 bytes	
MD5 hash:	8943e5f8f8c280467b4472c15ae93ba9	

Analysis Process: xfce4-panel PID: 6242, Parent PID: 2063		—
General		—
Start time:	01:54:22	
Start date:	30/11/2022	
Path:	/usr/bin/xfce4-panel	
Arguments:	n/a	
File size:	375768 bytes	
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784	

Analysis Process: wrapper-2.0 PID: 6242, Parent PID: 2063		—
General		—
Start time:	01:54:22	
Start date:	30/11/2022	
Path:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0	
Arguments:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libsystray.so 6 12582920 systray "Notification Area" "Area where notification icons appear"	
File size:	35136 bytes	
MD5 hash:	ac0b8a906f359a8ae102244738682e76	

File Activities		—
File Read		▼

Analysis Process: xfce4-panel PID: 6243, Parent PID: 2063	
General	
Start time:	01:54:22
Start date:	30/11/2022
Path:	/usr/bin/xfce4-panel
Arguments:	n/a
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: 6243, Parent PID: 2063	
General	
Start time:	01:54:22
Start date:	30/11/2022
Path:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
Arguments:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libstatusnotifier.so 7 12582921 statusnotifier "Status Notifier Plugin" "Provides a panel area for status notifier items (application indicators)"
File size:	35136 bytes
MD5 hash:	ac0b8a906f359a8ae102244738682e76

File Activities	
File Read	

Analysis Process: xfce4-panel PID: 6244, Parent PID: 2063	
General	
Start time:	01:54:22
Start date:	30/11/2022
Path:	/usr/bin/xfce4-panel
Arguments:	n/a
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: 6244, Parent PID: 2063	
General	
Start time:	01:54:22
Start date:	30/11/2022
Path:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
Arguments:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libpulseaudio-plugin.so 8 12582922 pulseaudio "PulseAudio Plugin" "Adjust the audio volume of the PulseAudio sound system"
File size:	35136 bytes
MD5 hash:	ac0b8a906f359a8ae102244738682e76

File Activities	
File Read	

Analysis Process: xfce4-panel PID: 6245, Parent PID: 2063	
General	
Start time:	01:54:22
Start date:	30/11/2022
Path:	/usr/bin/xfce4-panel
Arguments:	n/a
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: 6245, Parent PID: 2063	
---	--

General	
Start time:	01:54:22
Start date:	30/11/2022
Path:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
Arguments:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libxfce4powermanager.so 9 12582923 power-manager-plugin "Power Manager Plugin" "Display the battery levels of your devices and control the brightness of your display"
File size:	35136 bytes
MD5 hash:	ac0b8a906f359a8ae102244738682e76

File Activities	
File Read	

Analysis Process: xfce4-panel PID: 6246, Parent PID: 2063

General	
Start time:	01:54:23
Start date:	30/11/2022
Path:	/usr/bin/xfce4-panel
Arguments:	n/a
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: 6246, Parent PID: 2063

General	
Start time:	01:54:23
Start date:	30/11/2022
Path:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
Arguments:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libnotification-plugin.so 10 12582924 notification-plugin "Notification Plugin" "Notification plugin for the Xfce panel"
File size:	35136 bytes
MD5 hash:	ac0b8a906f359a8ae102244738682e76

File Activities	
File Read	

Analysis Process: xfce4-panel PID: 6247, Parent PID: 2063

General	
Start time:	01:54:23
Start date:	30/11/2022
Path:	/usr/bin/xfce4-panel
Arguments:	n/a
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: 6247, Parent PID: 2063

General	
Start time:	01:54:23
Start date:	30/11/2022
Path:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
Arguments:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0 /usr/lib/x86_64-linux-gnu/xfce4/panel/plugins/libactions.so 14 12582925 actions "Action Buttons" "Log out, lock or other system actions"
File size:	35136 bytes
MD5 hash:	ac0b8a906f359a8ae102244738682e76

File Activities	
File Read	