ID: 683525
Sample Name: TvhJo1pOSe
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 17:34:54
Date: 13/08/2022
Version: 35.0.0 Citrine

Table of Contents

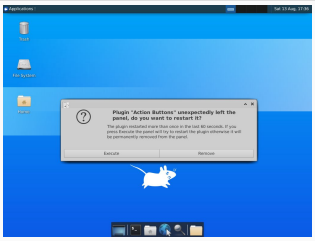
Linux Analysis Report

TvhJo1pOSe

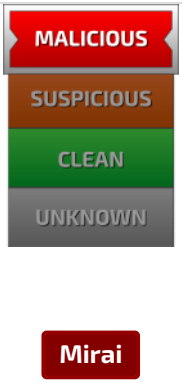
Overview

General Information

Sample Name:	TvhJo1pOSe
Analysis ID:	683525
MD5:	9dd6dd5bd57722.
SHA1:	8a50040db7ce0f..
SHA256:	95685ce485e3e8..
Tags:	32 arm elf mirai
Infos:	



Detection



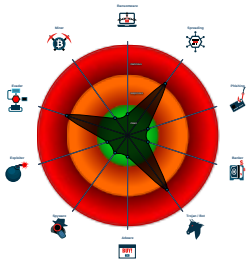
Mirai

Score:	72
Range:	0 - 100
Whitelisted:	false

Signatures

- Malicious sample detected (through…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Sample is packed with UPX
- Sample tries to kill multiple process…
- Sample contains only a LOAD segm…
- Yara signature match
- Creates hidden files and/or directorie…
- Uses the "uname" system call to qu…
- Enumerates processes within the "p…
- Tries to connect to HTTP servers, b…

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.

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:	683525
Start date and time:	2022-08-13 17:34:54 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TvhJo1pOSe
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:	mal72.spre.troj.evad.lin@0/0@0/0

Runtime Messages

Command:	/tmp/TvhJo1pOSe
PID:	6230
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	lzrd cock fest"/proc/"/exe
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- TvhJo1pOSe (PID: 6230, Parent: 6126, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/TvhJo1pOSe
  - TvhJo1pOSe New Fork (PID: 6233, Parent: 6230)
  - TvhJo1pOSe New Fork (PID: 6234, Parent: 6230)
  - TvhJo1pOSe New Fork (PID: 6236, Parent: 6230)
- 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/libsystray.so 6 12582920 systray "Notification Area" "Area where notification icons appear"
- 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/libstatusnotifier.so 7 12582921 statusnotifier "Status Notifier Plugin" "Provides a panel area for status notifier items (application indicators)"
- 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"
  - wrapper-2.0 New Fork (PID: 6268, Parent: 6245)
  - xfpm-power-backlight-helper (PID: 6268, Parent: 6245, MD5: 3d221ad23f28ca3259f599b1664e2427) Arguments: /usr/sbin/xfpm-power-backlight-helper --get-max-brightness
- 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/libpulseaudio-plugin.so 8 12582922 pulseaudio "PulseAudio Plugin" "Adjust the audio volume of the PulseAudio sound system"
- 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/libnotification-plugin.so 10 12582924 notification-plugin "Notification Plugin" "Notification plugin for the Xfce panel"
- xfce4-panel New Fork (PID: 6248, Parent: 2063)
- wrapper-2.0 (PID: 6248, 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"
- dbus-daemon New Fork (PID: 6267, Parent: 6266)
- xfconfd (PID: 6267, Parent: 6266, MD5: 4c7a0d6d258bb970905b19b84abcd8e9) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/xfconf/xfconfd
- systemd New Fork (PID: 6277, Parent: 1860)
- xfce4-notifyd (PID: 6277, Parent: 1860, MD5: eee956f1b227c1d5031f9c61223255d1) Arguments: /usr/lib/x86_64-linux-gnu/xfce4/notifyd/xfce4-notifyd
- **cleanup**

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
6236.1.00007fe1f8017000.00007fe1f8025000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
6236.1.00007fe1f8017000.00007fe1f8025000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0xc624:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc638:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc64c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc660:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc674:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc688:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc69c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc6b0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc6c4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc6d8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc6ec:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc700:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc714:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc728:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc73c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc750:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc764:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc778:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc78c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc7a0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc7b4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
6236.1.00007fe1f8017000.00007fe1f8025000.r-x.sdmp	Linux_Trojan_Gafgyt_ea92cca8	unknown	unknown	• 0xcb7c:$a: 53 65 6C 66 20 52 65 70 20 46 75 63 6B 69 6E 67 20 4E 65 54 69 53 20 61 6E 64
6230.1.00007fe1f8017000.00007fe1f8025000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
6230.1.00007fe1f8017000.00007fe1f8025000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0xc624:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc638:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc64c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc660:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc674:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc688:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc69c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc6b0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc6c4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc6d8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc6ec:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc700:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc714:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc728:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc73c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc750:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc764:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc778:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc78c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc7a0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xc7b4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 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)

Data Obfuscation

Sample is packed with UPX

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

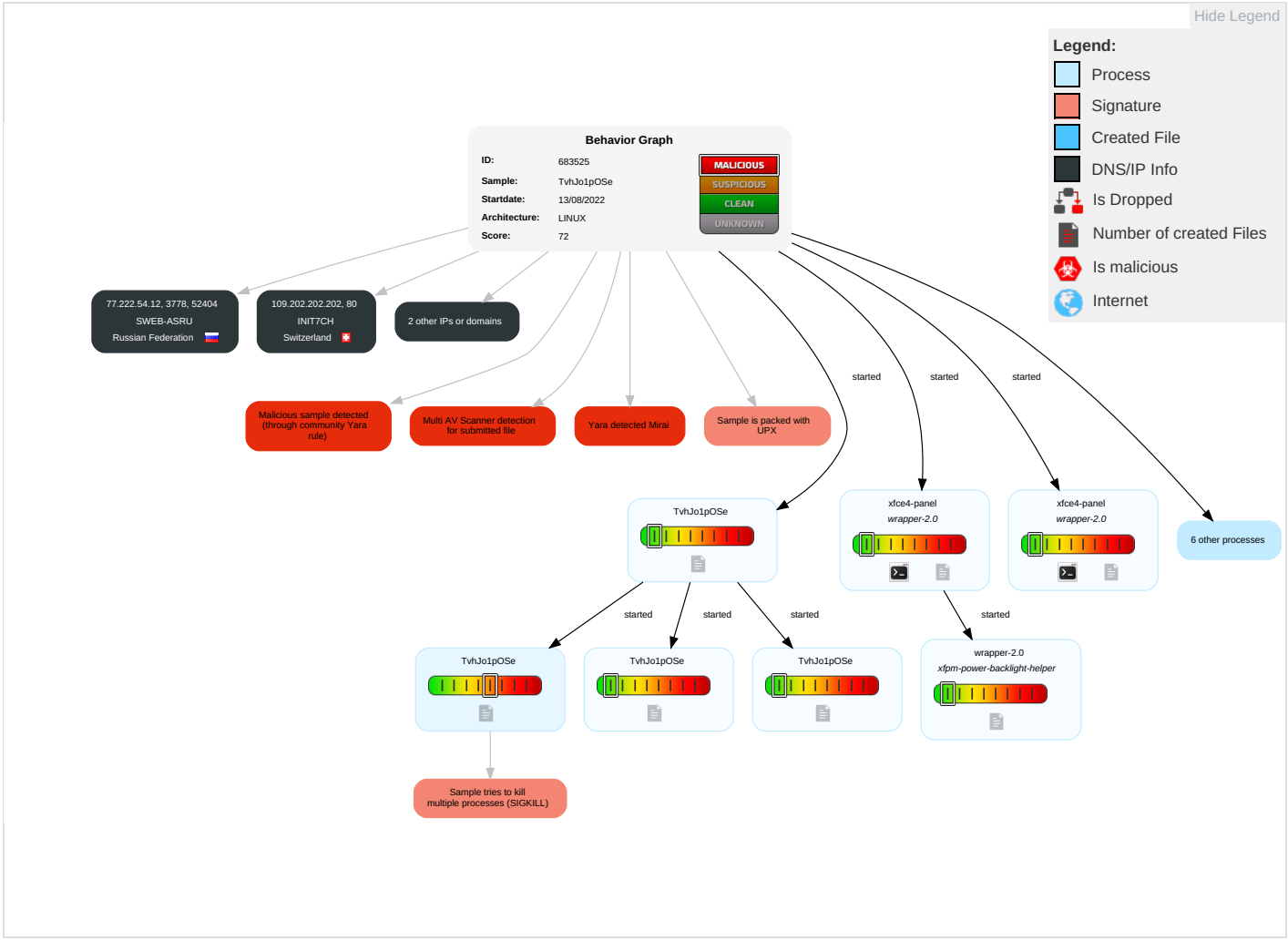
Mitre Att&ck Matrix

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	1 Hidden Files and Directories	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	1 1 Obfuscated Files or Information	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

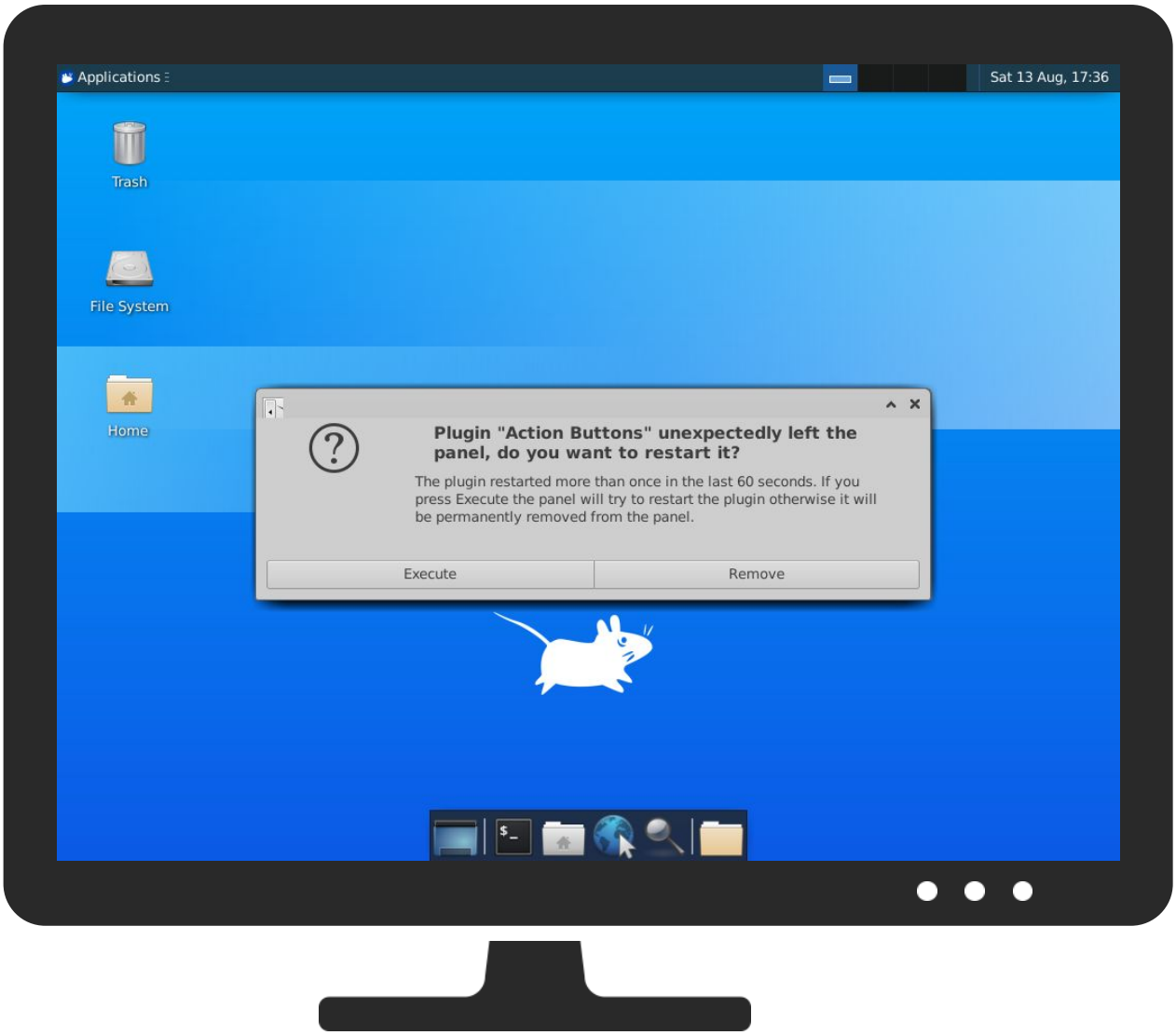
Behavior Graph



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
TvhJo1pOSe	44%	Virustotal		Browse
TvhJo1pOSe	42%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

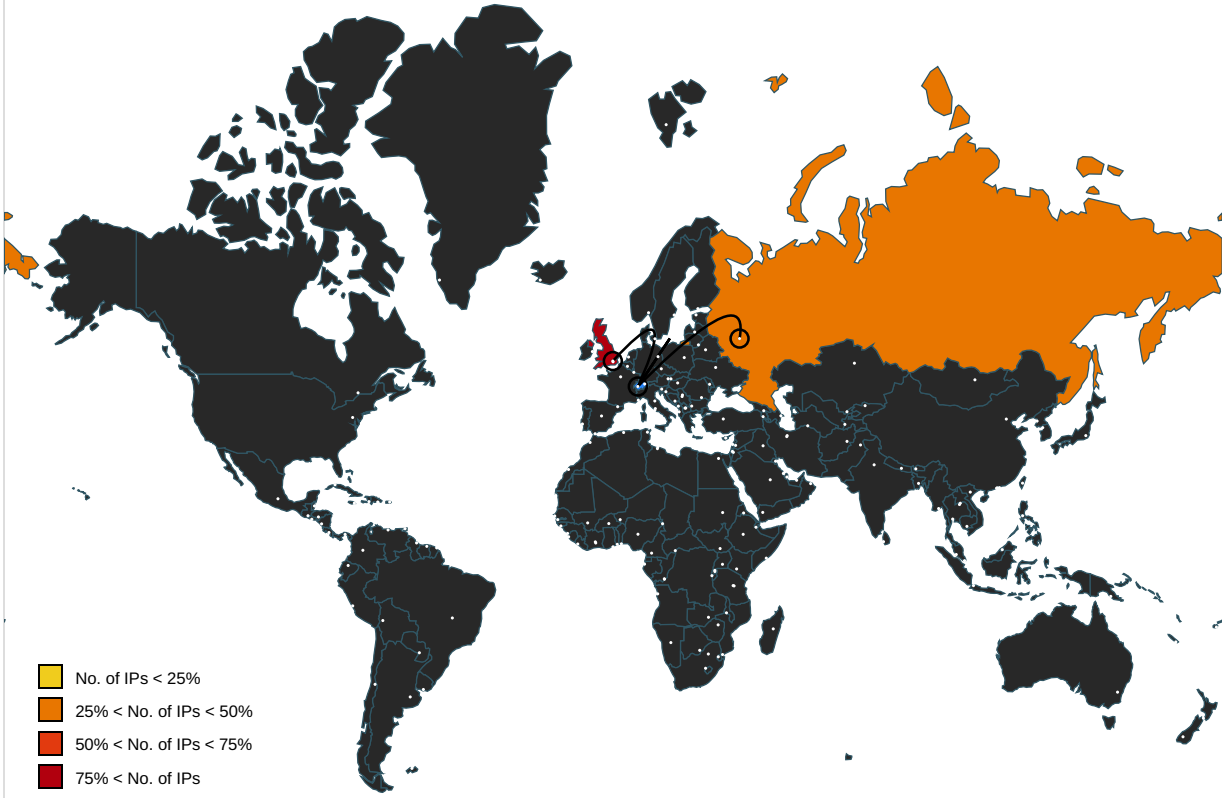
Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
77.222.54.12	unknown	Russian Federation		44112	SWEB-ASRU	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, ARM, version 1 (ARM), statically linked, stripped
Entropy (8bit):	7.914978210323174
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	TvhJo1pOSe
File size:	22160
MD5:	9dd6dd5bd577226323ba207c5e1127e2
SHA1:	8a50040db7ce0ffa37934be58174d7ef2cd32197
SHA256:	95685ce485e3e87f4cc24923a9407c061012c195b6f2c8d9340d1756405a12da
SHA512:	47a523536eb815df2214d7f35e1e62a9c614352aa80713f27422b7aaba6251b3f732ec3a0cee78ec0e2d8774c7a2ec51a20054e6280c8e86965508aefbfe4fdb
SSDEEP:	384:xvtIoZxrSniaXs+qx+bwqPX+VOcFd5fHq52lxjehymdGUop5h7:xvQn4j+ZO5fKAlx6s3Uozx
TLSH:	DBA2E01176A32D65E3ED2C3DC96EC327F9661BFC90F532B579402620C94D24A3E38A4B
File Content Preview:	.ELF...a.....(.....4.....4. ...(.....U...U.....\.....Q.td.....CvUPX!.....`...`.....Q.....?.E.h;.}...^.....f@.,v.. (fw....&.x:.E....|.....y]8J.r.F.O.v

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:	0xc3f8
Flags:	0x202
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

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	0x55a7	0x55a7	7.9190	0x5	R E	0x8000		
LOAD	0x5ca4	0x1dca4	0x1dca4	0x0	0x0	0.0000	0x6	RW	0x8000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution

Total Packets: 12

- 3778 undefined
- 80 (HTTP)
- 443 (HTTPS)

TCP Packets

System Behavior

Analysis Process: TvhJo1pOSe PID: 6230, Parent PID: 6126

General

Start time:	17:35:41
Start date:	13/08/2022
Path:	/tmp/TvhJo1pOSe
Arguments:	/tmp/TvhJo1pOSe
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: TvhJo1pOSe PID: 6233, Parent PID: 6230

General

Start time:	17:35:41
Start date:	13/08/2022
Path:	/tmp/TvhJo1pOSe
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: TvhJo1pOSe PID: 6234, Parent PID: 6230

General

Start time:	17:35:41
Start date:	13/08/2022
Path:	/tmp/TvhJo1pOSe
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: TvhJo1pOSe PID: **6236**, Parent PID: **6230**

General

Start time:	17:35:41
Start date:	13/08/2022
Path:	/tmp/TvhJo1pOSe
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: xfce4-panel PID: **6243**, Parent PID: **2063**

General

Start time:	17:35:46
Start date:	13/08/2022
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:	17:35:46
Start date:	13/08/2022
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

Directory Enumerated

Analysis Process: xfce4-panel PID: **6244**, Parent PID: **2063**

General

Start time:	17:35:46
Start date:	13/08/2022
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:	17:35:46
Start date:	13/08/2022
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

Directory Enumerated

Analysis Process: xfce4-panel PID: **6245**, Parent PID: **2063**

General

Start time:	17:35:47
Start date:	13/08/2022
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:	17:35:47
Start date:	13/08/2022
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

Directory Enumerated

Analysis Process: wrapper-2.0 PID: **6268**, Parent PID: **6245**

General

Start time:	17:35:55
Start date:	13/08/2022
Path:	/usr/lib/x86_64-linux-gnu/xfce4/panel/wrapper-2.0
Arguments:	n/a
File size:	35136 bytes
MD5 hash:	ac0b8a906f359a8ae102244738682e76

File Activities

Directory Enumerated

Analysis Process: xfpm-power-backlight-helper PID: **6268**, Parent PID: **6245**

General

Start time:	17:35:55
Start date:	13/08/2022
Path:	/usr/sbin/xfpm-power-backlight-helper
Arguments:	/usr/sbin/xfpm-power-backlight-helper --get-max-brightness
File size:	14656 bytes
MD5 hash:	3d221ad23f28ca3259f599b1664e2427

File Activities

File Read

Directory Enumerated

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

General

Start time:	17:35:47
Start date:	13/08/2022
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:	17:35:47
Start date:	13/08/2022
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

Directory Enumerated

Directory Created

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

General

Start time:	17:35:47
Start date:	13/08/2022
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:	17:35:47
Start date:	13/08/2022
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

Directory Enumerated

Directory Created

Analysis Process: xfce4-panel PID: **6248**, Parent PID: **2063**

General

Start time:	17:35:47
Start date:	13/08/2022
Path:	/usr/bin/xfce4-panel
Arguments:	n/a
File size:	375768 bytes
MD5 hash:	a15b657c7d54ac1385f1f15004ea6784

Analysis Process: wrapper-2.0 PID: **6248**, Parent PID: **2063**

General

Start time:	17:35:47
Start date:	13/08/2022

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

Directory Enumerated

Analysis Process: dbus-daemon PID: **6267**, Parent PID: **6266**

General

Start time:	17:35:55
Start date:	13/08/2022
Path:	/usr/bin/dbus-daemon
Arguments:	n/a
File size:	249032 bytes
MD5 hash:	3089d47e3f3ab84cd81c48fd406d7a8c

Analysis Process: xfconfd PID: **6267**, Parent PID: **6266**

General

Start time:	17:35:55
Start date:	13/08/2022
Path:	/usr/lib/x86_64-linux-gnu/xfce4/xfconf/xfconfd
Arguments:	/usr/lib/x86_64-linux-gnu/xfce4/xfconf/xfconfd
File size:	112880 bytes
MD5 hash:	4c7a0d6d258bb970905b19b84abcd8e9

File Activities

File Read

Directory Created

Analysis Process: systemd PID: **6277**, Parent PID: **1860**

General

Start time:	17:35:59
Start date:	13/08/2022
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: xfce4-notifyd PID: **6277**, Parent PID: **1860**

General

Start time:	17:35:59
Start date:	13/08/2022
Path:	/usr/lib/x86_64-linux-gnu/xfce4/notifyd/xfce4-notifyd
Arguments:	/usr/lib/x86_64-linux-gnu/xfce4/notifyd/xfce4-notifyd
File size:	112872 bytes
MD5 hash:	eee956f1b227c1d5031f9c61223255d1

File Activities

File Read