



ID: 756339
Sample Name: 5Qnr6x5Dqv.elf
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 02:10:50
Date: 30/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Linux Analysis Report 5Qnr6x5Dqv.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
Memory Dumps 5
Snort Signatures 6
Joe Sandbox Signatures 6
AV Detection 6
System Summary 6
Data Obfuscation 6
Stealing of Sensitive Information 7
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Malware Configuration 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 10
World Map of Contacted IPs 10
Public IPs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASNs 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 11
Static File Info 11
General 11
Static ELF Info 11
ELF header 11
Program Segments 11
Network Behavior 11
Network Port Distribution 11
TCP Packets 12
System Behavior 12
Analysis Process: 5Qnr6x5Dqv.elf PID: 6225, Parent PID: 6124 12
General 12
File Activities 12
File Read 12
Analysis Process: 5Qnr6x5Dqv.elf PID: 6227, Parent PID: 6225 12
General 12
File Activities 12
File Read 12
Directory Enumerated 12
Analysis Process: 5Qnr6x5Dqv.elf PID: 6228, Parent PID: 6225 12
General 12
Analysis Process: 5Qnr6x5Dqv.elf PID: 6230, Parent PID: 6225 13
General 13
Analysis Process: xfce4-panel PID: 6238, Parent PID: 2063 13
General 13
Analysis Process: wrapper-2.0 PID: 6238, Parent PID: 2063 13
General 13
File Activities 13
File Read 13
Analysis Process: xfce4-panel PID: 6239, Parent PID: 2063 13
General 13
Analysis Process: wrapper-2.0 PID: 6239, Parent PID: 2063 13
General 13
File Activities 13

File Read 13
Analysis Process: xfce4-panel PID: 6240, Parent PID: 2063 13
General 14
Analysis Process: wrapper-2.0 PID: 6240, Parent PID: 2063 14
General 14
File Activities 14
File Read 14
Analysis Process: xfce4-panel PID: 6241, Parent PID: 2063 14
General 14
Analysis Process: wrapper-2.0 PID: 6241, Parent PID: 2063 14
General 14
File Activities 14
File Read 14
Analysis Process: xfce4-panel PID: 6242, Parent PID: 2063 14
General 14
Analysis Process: wrapper-2.0 PID: 6242, Parent PID: 2063 14
General 14
File Activities 15
File Read 15
Analysis Process: xfce4-panel PID: 6243, Parent PID: 2063 15
General 15
Analysis Process: wrapper-2.0 PID: 6243, Parent PID: 2063 15
General 15
File Activities 15
File Read 15

Copyright Joe Security LLC 2022

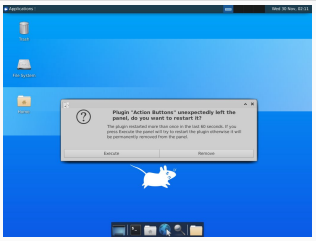
Linux Analysis Report

5Qnr6x5Dqv.elf

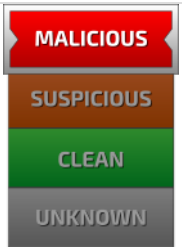
Overview

General Information

Sample Name:	5Qnr6x5Dqv.elf
Analysis ID:	756339
MD5:	cbc93213240219..
SHA1:	f6b7f08e879e3d1..
SHA256:	a0adda466b7e22..
Tags:	32 arm elf mirai
Infos:	



Detection



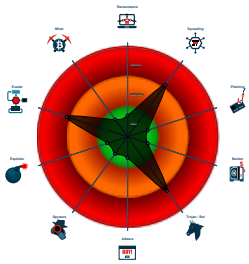
Mirai

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
- 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…

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:	36.0.0 Rainbow Opal
Analysis ID:	756339
Start date and time:	2022-11-30 02:10:50 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	5Qnr6x5Dqv.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:	mal72.spre.troj.evad.linELF@0/0@0/0

Runtime Messages

Command:	/tmp/5Qnr6x5Dqv.elf
PID:	6225
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	lzrd cock fest"/proc/"/exe
Standard Error:	

Copyright Joe Security LLC 2022

Process Tree

- **system is lnxubuntu20**
- 5Qnr6x5Dqv.elf (PID: 6225, Parent: 6124, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/5Qnr6x5Dqv.elf
  - 5Qnr6x5Dqv.elf New Fork (PID: 6227, Parent: 6225)
  - 5Qnr6x5Dqv.elf New Fork (PID: 6228, Parent: 6225)
  - 5Qnr6x5Dqv.elf New Fork (PID: 6230, Parent: 6225)
- xfce4-panel New Fork (PID: 6238, Parent: 2063)
- wrapper-2.0 (PID: 6238, 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: 6239, Parent: 2063)
- wrapper-2.0 (PID: 6239, 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: 6240, Parent: 2063)
- wrapper-2.0 (PID: 6240, 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: 6241, Parent: 2063)
- wrapper-2.0 (PID: 6241, 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: 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/libnotification-plugin.so 10 12582924 notification-plugin "Notification Plugin" "Notification plugin for the Xfce panel"
- 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/libactions.so 14 12582925 actions "Action Buttons" "Log out, lock or other system actions"
- **cleanup**

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
6230.1.00007fd0bc017000.00007fd0bc025000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6230.1.00007fd0bc017000.00007fd0bc025000.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:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
6230.1.00007fd0bc017000.00007fd0bc025000.r-x.sdmp	Linux_Trojan_Gafgyt_ea92cca8	unknown	unknown	• 0xcb7c:$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

Source	Rule	Description	Author	Strings
6225.1.00007fd0bc017000.00007fd0bc025000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
6225.1.00007fd0bc017000.00007fd0bc025000.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 6 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

Copyright Joe Security LLC 2022

Stealing of Sensitive Information



Yara detected Mirai

Remote Access Functionality



Yara detected Mirai

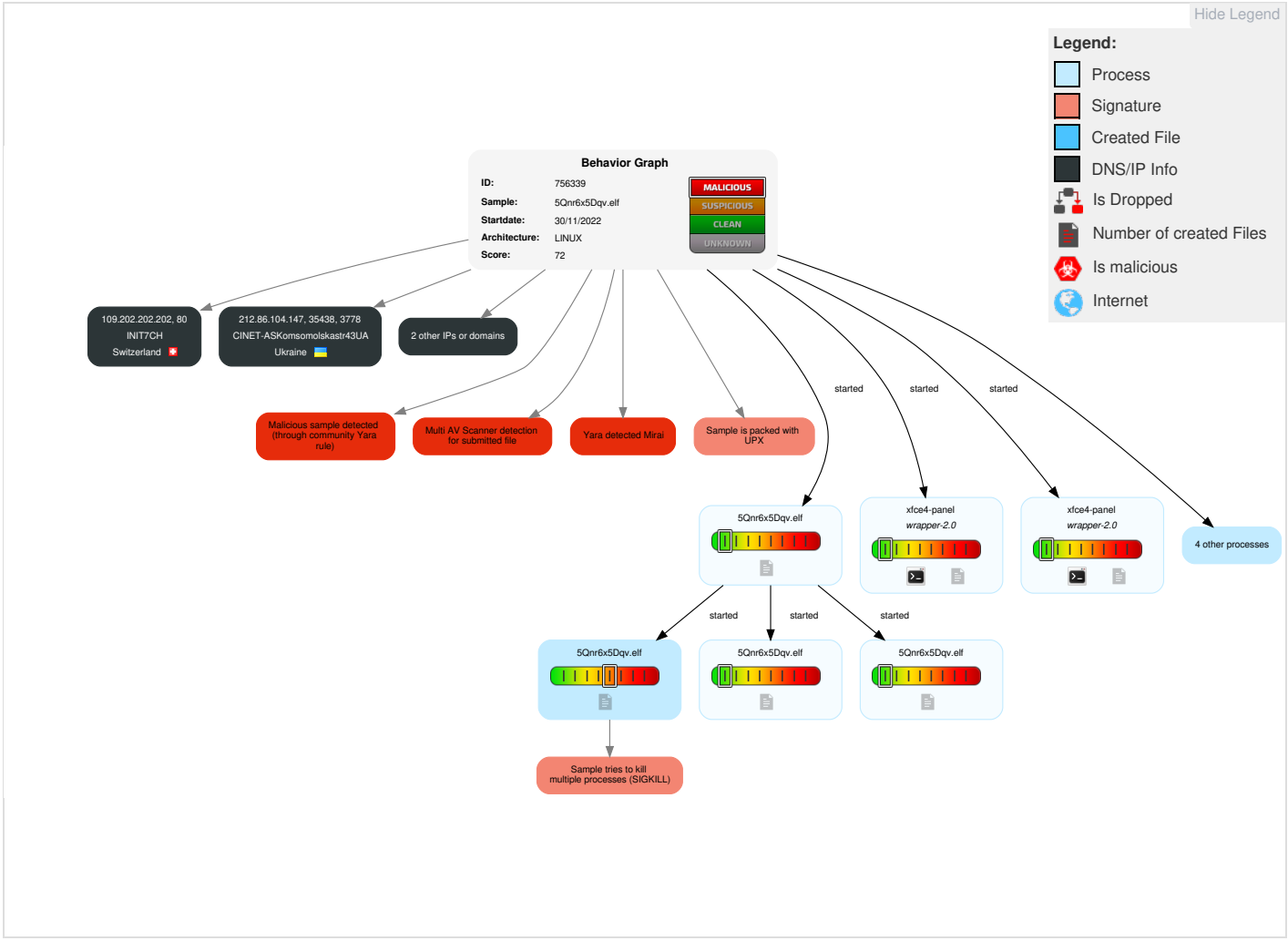
Mitre Att&ck Matrix

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 1 Obfuscated Files or Information	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

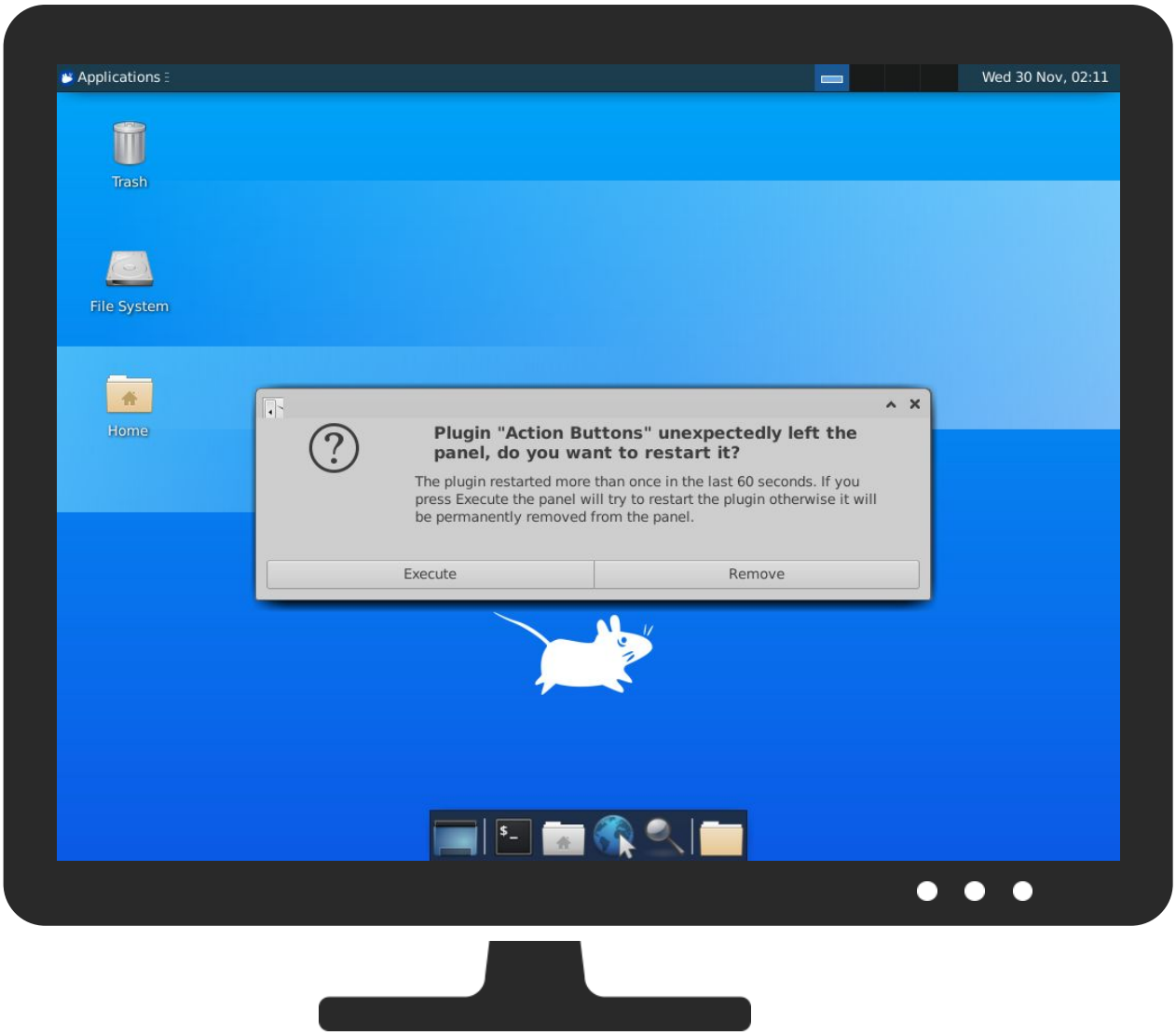


Screenshots

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
5Qnr6x5Dqv.elf	44%	ReversingLabs	Linux.Trojan.Mirai	
5Qnr6x5Dqv.elf	46%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

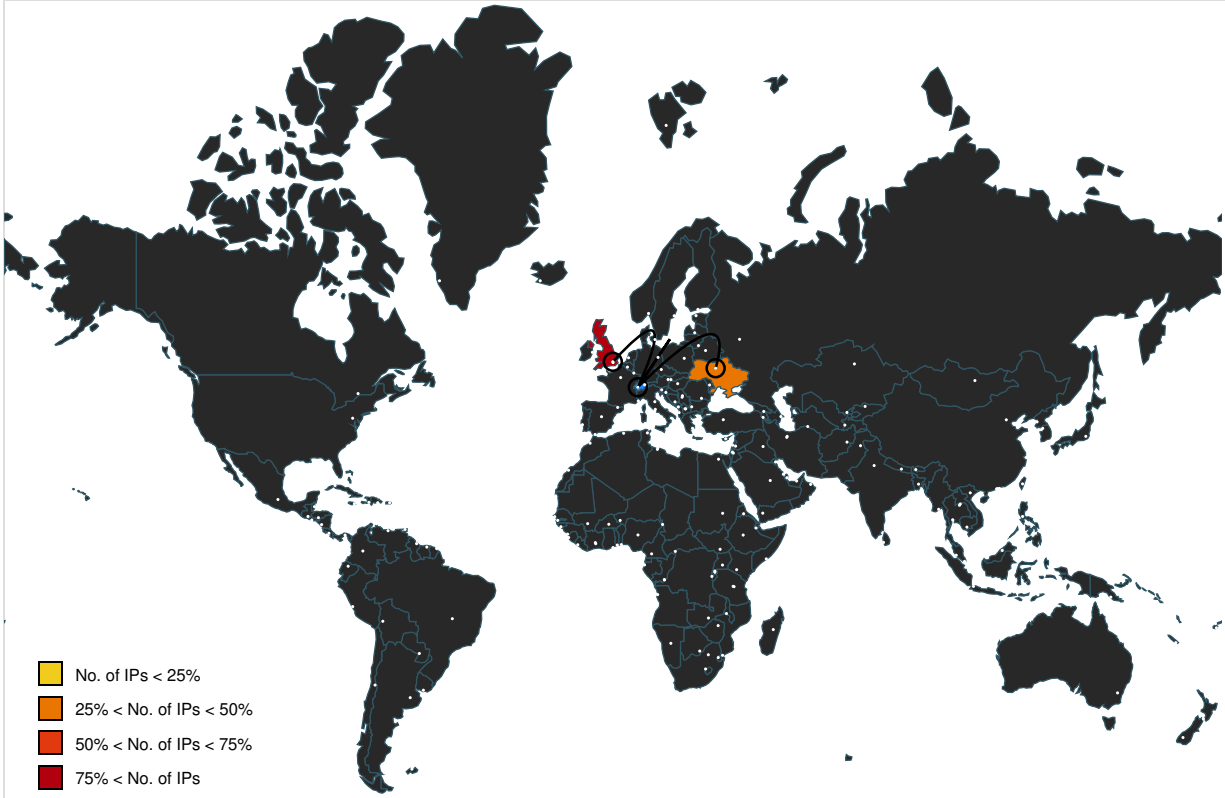
Contacted Domains

No contacted domains info

Copyright Joe Security LLC 2022

URLs from Memory and Binaries

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

Copyright Joe Security LLC 2022

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, no section header
Entropy (8bit):	7.915509796998442
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	5Qnr6x5Dqv.elf
File size:	22160
MD5:	cbc93213240219bbd4bd14ff9974137d
SHA1:	f6b7f08e879e3d1584b269af2c731e96b3a90bcb
SHA256:	a0adda466b7e22810c1c05b1ce28a8e4237d2a43fcb4d2562c8f18f56c21f697
SHA512:	c16966830e35f70b1fc8443029b08fb89f5ea5c49b9f872dd122bc85fd59e0cd9f2f4776f0b07a4d6aa1a4f48d184c2492904210fcb474232f5fda2268adcf62
SSDEEP:	384:vvtIoZxrSniaXs+qx+bwqPX+VOcFd5fHq52lxj7xrBhymdGUop5h+:vvQn4j+ZO5fKAlxXxrBs3Uozw
TLSH:	1FA2E11572A32D65F2ED1C3CC86A835BF9671BFC90F6327669446620C94D24A3E38A4B
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:	
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:	

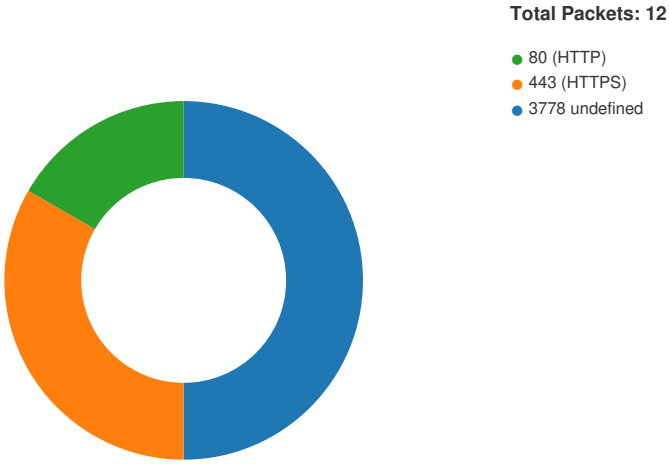
Program Segments

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	7.9197	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

Copyright Joe Security LLC 2022



TCP Packets

System Behavior

Analysis Process: 5Qnr6x5Dqv.elf PID: 6225, Parent PID: 6124

General

Start time:	02:11:36
Start date:	30/11/2022
Path:	/tmp/5Qnr6x5Dqv.elf
Arguments:	/tmp/5Qnr6x5Dqv.elf
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: 5Qnr6x5Dqv.elf PID: 6227, Parent PID: 6225

General

Start time:	02:11:36
Start date:	30/11/2022
Path:	/tmp/5Qnr6x5Dqv.elf
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: 5Qnr6x5Dqv.elf PID: 6228, Parent PID: 6225

General

Start time:	02:11:36
Start date:	30/11/2022
Path:	/tmp/5Qnr6x5Dqv.elf
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Copyright Joe Security LLC 2022

Analysis Process: 5Qnr6x5Dqv.elf PID: **6230**, Parent PID: **6225**

General

Start time:	02:11:36
Start date:	30/11/2022
Path:	/tmp/5Qnr6x5Dqv.elf
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: xfce4-panel PID: **6238**, Parent PID: **2063**

General

Start time:	02:11:42
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: **6238**, Parent PID: **2063**

General

Start time:	02:11:42
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: **6239**, Parent PID: **2063**

General

Start time:	02:11:42
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: **6239**, Parent PID: **2063**

General

Start time:	02:11:42
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: **6240**, Parent PID: **2063**

Copyright Joe Security LLC 2022

General	
Start time:	02:11:42
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: **6240**, Parent PID: **2063**

General	
Start time:	02:11:42
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: **6241**, Parent PID: **2063**

General	
Start time:	02:11:42
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: **6241**, Parent PID: **2063**

General	
Start time:	02:11:42
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: **6242**, Parent PID: **2063**

General	
Start time:	02:11:42
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:	02:11:42

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: **6243**, Parent PID: **2063**

General

Start time:	02:11:42
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:	02:11:42
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

Copyright Joe Security LLC 2022