ID: 780227
Sample Name: yNGgbod6dt.elf
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 16:30:07
Date: 08/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

Linux Analysis Report

yNGgbod6dt.elf

Overview

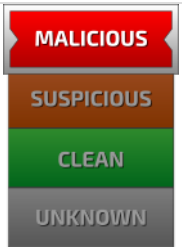
General Information

Sample Name:	yNGgbod6dt.elf
Analysis ID:	780227
MD5:	62f1db29777c38..
SHA1:	0adc886845b8a3..
SHA256:	2b68e82dada6e7..
Tags:	32 elf gafgyt Mirai
Infos:	

Errors

⚠ No process behavior to analyse as no analysis process or sample was found

Detection



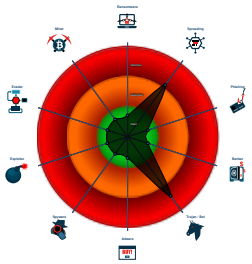
Mirai

Score:	76
Range:	0 - 100
Whitelisted:	false

Signatures

- Malicious sample detected (through…
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Found strings indicative of a multi-p…
- Yara signature match
- Sample contains strings that are po…
- Sample has stripped symbol table
- Tries to connect to HTTP servers, b…
- Sample contains strings indicative o…

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.

Non-zero exit code suggests an error during the execution. Lookup the error code for hints.

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	780227
Start date and time:	2023-01-08 16:30:07 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	yNGgbod6dt.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:	mal76.spre.troj.linELF@0/0@0/0

Errors

Runtime Messages

Command:	/tmp/yNGgbod6dt.elf
PID:	6230
Exit Code:	255
Exit Code Info:	
Killed:	False
Standard Output:	

Standard Error:	

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
yNGgbod6dt.elf	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	• 0x1b2f8:$xo1: \x96\xB4\xA1\xB2\xB7\xB7\xBA\xF4\xEE\xF5\xEB • 0x1b3cc:$xo1: \x96\xB4\xA1\xB2\xB7\xB7\xBA\xF4\xEE\xF5\xEB • 0x1b454:$xo1: \x96\xB4\xA1\xB2\xB7\xB7\xBA\xF4\xEE\xF5\xEB • 0x1b4d0:$xo1: \x96\xB4\xA1\xB2\xB7\xB7\xBA\xF4\xEE\xF5\xEB
yNGgbod6dt.elf	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
yNGgbod6dt.elf	JoeSecurity_Mirai_4	Yara detected Mirai	Joe Security	
yNGgbod6dt.elf	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0x18ec8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x18edc:$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 • 0x18ef0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x18f04:$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 • 0x18f18:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x18f2c:$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 • 0x18f40:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x18f54:$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 • 0x18f68:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x18f7c:$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 • 0x18f90:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x18fa4:$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 • 0x18fb8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x18fcc:$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 • 0x18fe0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x18ff4:$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 • 0x19008:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x1901c:$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 • 0x19030:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x19044:$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 • 0x19058:$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

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Spreading

Found strings indicative of a multi-platform dropper

System Summary

Malicious sample detected (through community Yara rule)

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

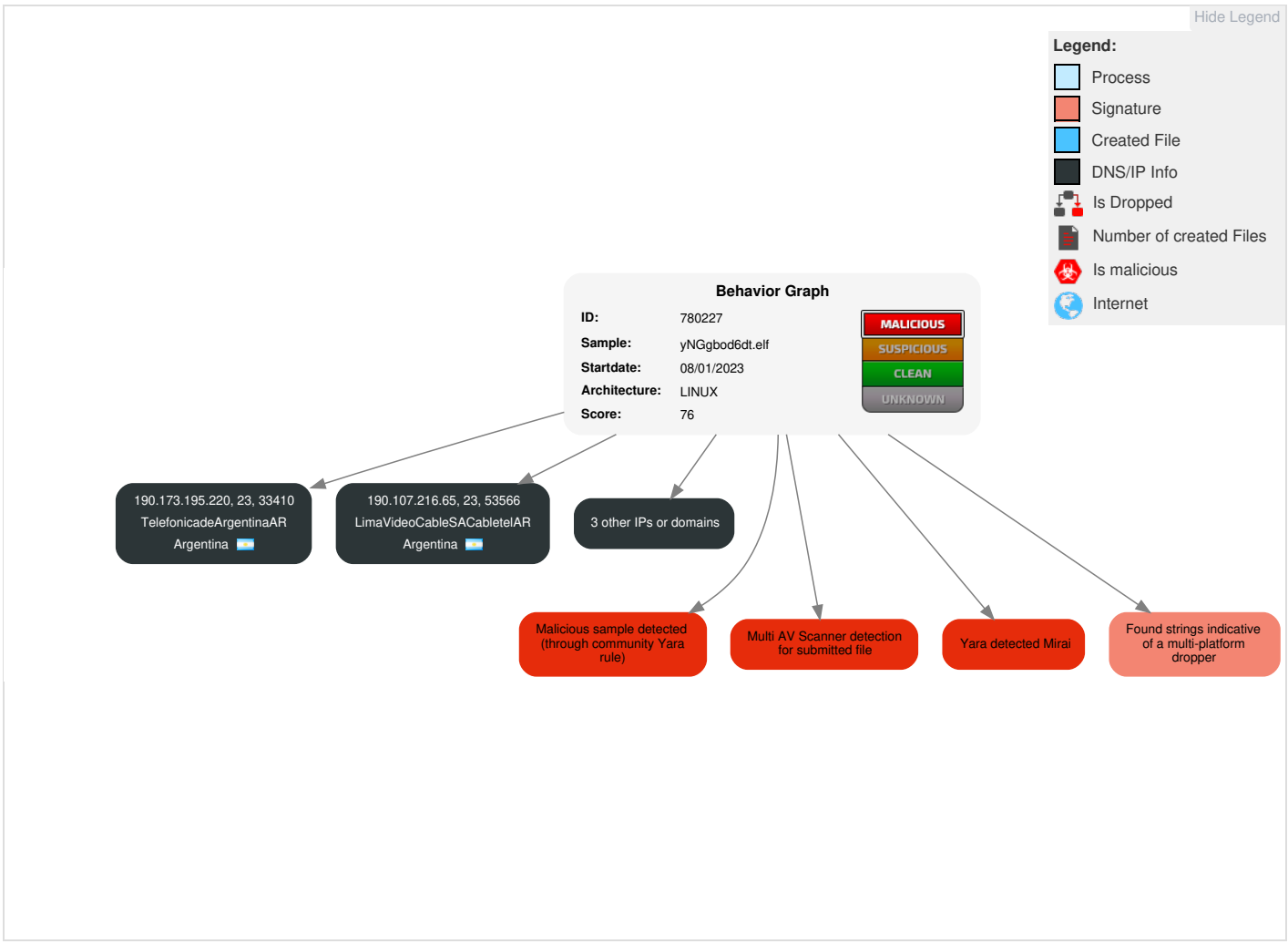
Mitre Att&ck Matrix

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	1 Scripting	OS Credential Dumping	System Service 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	Modify System Partition
Default Accounts	1 Scripting	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 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
yNGgbod6dt.elf	41%	ReversingLabs	Linux.Trojan.Gafgyt	
yNGgbod6dt.elf	49%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://purenetworks.com/HNAP1/	0%	URL Reputation	safe	

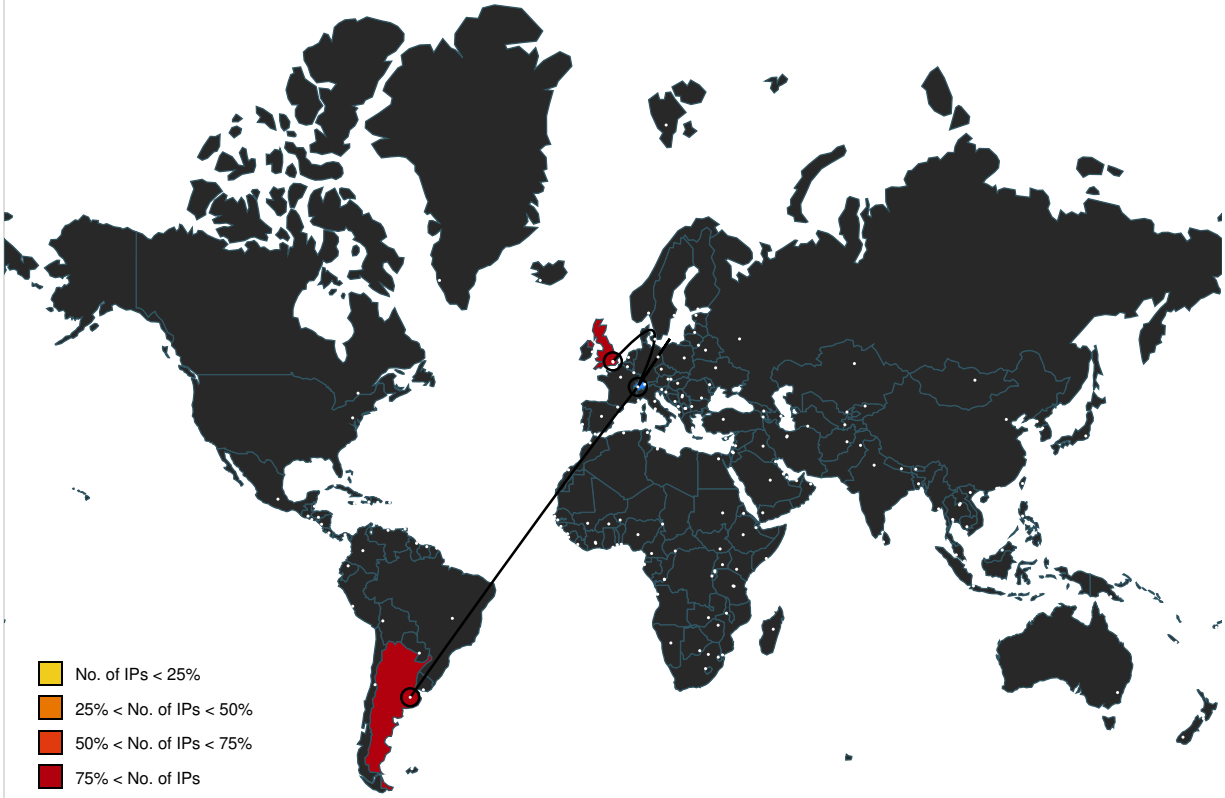
Domains and IPs

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
190.173.195.220	unknown	Argentina		22927	TelefonicadeArgentinaAR	false
190.107.216.65	unknown	Argentina		52339	LimaVideoCableSACabletelAR	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, Synopsys ARCompact ARC700 cores, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.653518843178181
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	yNGgbod6dt.elf
File size:	148972
MD5:	62f1db29777c386f59a4836a2578e635
SHA1:	0adc886845b8a3a549b6d41a16c7e1644ec15908
SHA256:	2b68e82dada6e7bfa17c1ef77c4f03920d5644e34686a6e8a6ea5b809de70c1a
SHA512:	0d90e81a94196dd02191e85f9fc2aaffbc46960b33f650ea03cb879bdf7ab9bc5d628d97543c0a990049910d0aa8ae0d4a747d6da74f75a05f3cd995f5a4c009
SSDEEP:	3072:+BamDuoiU+jxgl30itMkPdWh8jIOs2GvLP54gaKuq:+BmozEtiUXuKuq
TLSH:	8FE3BEABBB8F0250C45702F40BCF5BAE6E6321509DAFC5E3AE39723B443A5C76516760
File Content Preview:	.ELF.....]........4....C.....4. ...(.....0...0..... .....?..._..._..D...4A..... .....?..._..._.....Q.td.....

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	0x10114	0x114	0x22	0x0	0x6	AX	0	0	1
.text	PROGBITS	0x10138	0x138	0x1840c	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x28544	0x18544	0x16	0x0	0x6	AX	0	0	1
.rodata	PROGBITS	0x2855c	0x1855c	0xaaa4	0x0	0x2	A	0	0	4
.tbss	NOBITS	0x35fe0	0x23fe0	0x8	0x0	0x403	WAT	0	0	4
.fini_array	FINI_ARRAY	0x35fe0	0x23fe0	0x4	0x4	0x3	WA	0	0	4
.ctors	PROGBITS	0x35fe4	0x23fe4	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x35fec	0x23fec	0x8	0x0	0x3	WA	0	0	4

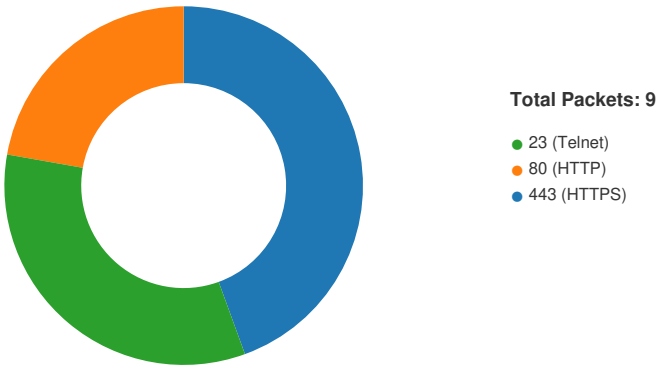
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
.got	PROGBITS	0x35ff4	0x23ff4	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x36008	0x24008	0x31c	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x36324	0x24324	0x3df0	0x0	0x3	WA	0	0	4
.ARC.attributes	<unknown>	0x0	0x24324	0x32	0x0	0x0		0	0	1
.shstrtab	STRTAB	0x0	0x24356	0x65	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	0x10000	0x10000	0x23000	0x23000	6.7860	0x5	R E	0x2000		.init .text .fini .rodata
LOAD	0x23fe0	0x35fe0	0x35fe0	0x344	0x4134	4.1946	0x6	RW	0x2000		.tbss .fini_array .ctors .dtors .got .data .bss
NOTE	0x0	0x0	0x0	0x0	0x0	0.0000	0x4	R	0x4		
TLS	0x23fe0	0x35fe0	0x35fe0	0x0	0x8	0.0000	0x4	R	0x4		.tbss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior