ID: 635081
Sample Name: ogWpjtLcso
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 12:40:37
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

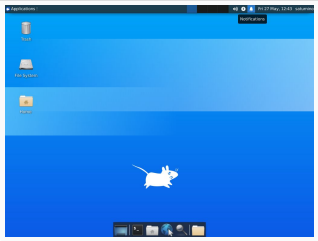
Linux Analysis Report

ogWpjtLcso

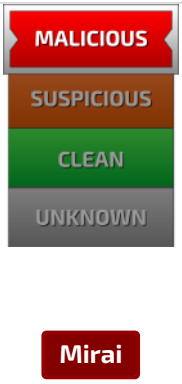
Overview

General Information

Sample Name:	ogWpjtLcso
Analysis ID:	635081
MD5:	e2501a4bed62e1.
SHA1:	5ed9286b1b9d36.
SHA256:	f207c0abf680d78..
Tags:	32 arm elf mirai
Infos:	



Detection

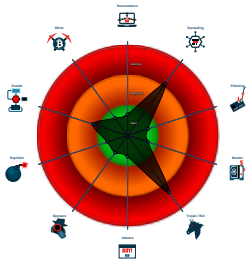


Score:	72
Range:	0 - 100
Whitelisted:	false

Signatures

- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic
- Uses known network protocols on n…
- Sample tries to kill multiple process…
- Sample has stripped symbol table
- HTTP GET or POST without a user …
- Uses the "uname" system call to qu…
- Enumerates processes within the "p…
- 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.

Some HTTP requests failed (404). It is likely that the sample will exhibit less behavior.

Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures.

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635081
Start date and time: 27/05/202212:40:37	2022-05-27 12:40:37 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ogWpjtLcso
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.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/ogWpjtLcso
PID:	6230
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Infected By Cult

Standard Error:	

Process Tree

- **system is lnxubuntu20**
- ogWpjtLcso (PID: 6230, Parent: 6124, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/ogWpjtLcso
  - ogWpjtLcso New Fork (PID: 6232, Parent: 6230)
  - ogWpjtLcso New Fork (PID: 6233, Parent: 6230)
  - ogWpjtLcso New Fork (PID: 6235, Parent: 6230)
    - ogWpjtLcso New Fork (PID: 6238, Parent: 6235)
    - ogWpjtLcso New Fork (PID: 6239, Parent: 6235)
    - ogWpjtLcso New Fork (PID: 6240, Parent: 6235)
    - ogWpjtLcso New Fork (PID: 6241, Parent: 6235)
    - ogWpjtLcso New Fork (PID: 6246, Parent: 6235)
    - ogWpjtLcso New Fork (PID: 6247, Parent: 6235)
    - ogWpjtLcso New Fork (PID: 6304, Parent: 6235)
      - ogWpjtLcso New Fork (PID: 6306, Parent: 6304)
- **cleanup**

Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Mirai_12	Yara detected Mirai	Joe Security	

Snort Signatures

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.97.189.182

Timestamp:	192.168.2.2395.97.189.18244088802839471 05/27/22-12:41:26.233242
SID:	2839471
Source Port:	44088
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.52.93.58

Timestamp:	192.168.2.2395.52.93.5847304802839471 05/27/22-12:41:47.290211
SID:	2839471
Source Port:	47304
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.247.172.2

Timestamp:	192.168.2.2388.247.172.235136802839471 05/27/22-12:41:48.711474
SID:	2839471
Source Port:	35136
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.101.93.99

Timestamp:	192.168.2.2395.101.93.9954318802839471 05/27/22-12:41:37.698966
SID:	2839471
Source Port:	54318
Destination Port:	80
Protocol:	TCP

Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.80.177.176

Timestamp:	192.168.2.2388.80.177.17638888802839471 05/27/22-12:41:41.709523
SID:	2839471
Source Port:	38888
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.68.46.214

Timestamp:	192.168.2.2395.68.46.21445714802839471 05/27/22-12:41:31.584015
SID:	2839471
Source Port:	45714
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.72.100.0

Timestamp:	192.168.2.2388.72.100.054594802839471 05/27/22-12:41:33.759271
SID:	2839471
Source Port:	54594
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.163.124.245

Timestamp:	192.168.2.2395.163.124.24551614802839471 05/27/22-12:41:37.748726
SID:	2839471
Source Port:	51614
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.85.72.114

Timestamp:	192.168.2.2395.85.72.11444518802839471 05/27/22-12:41:31.577298
SID:	2839471
Source Port:	44518
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 95.156.226.69

Timestamp:	192.168.2.2395.156.226.6949982802839471 05/27/22-12:41:31.554788
SID:	2839471
Source Port:	49982
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 112.137.60.74

Timestamp:	192.168.2.23112.137.60.7443984802839471 05/27/22-12:41:35.303316
SID:	2839471
Source Port:	43984
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215) - Source IP: 192.168.2.23 - Destination IP: 197.246.192.108

Timestamp:	192.168.2.23197.246.192.10853320372152835222 05/27/22-12:41:42.355128

SID:	2835222
Source Port:	53320
Destination Port:	37215
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.103.220.242

Timestamp:	192.168.2.2388.103.220.24237162802839471 05/27/22-12:41:45.955319
SID:	2839471
Source Port:	37162
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

ETPRO TROJAN Mirai Variant User-Agent (Outbound) - Source IP: 192.168.2.23 - Destination IP: 88.221.228.201

Timestamp:	192.168.2.2388.221.228.20151072802839471 05/27/22-12:41:43.825767
SID:	2839471
Source Port:	51072
Destination Port:	80
Protocol:	TCP
Classtype:	Web Application Attack

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Networking

Snort IDS alert for network traffic

Uses known network protocols on non-standard ports

System Summary

Sample tries to kill multiple processes (SIGKILL)

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

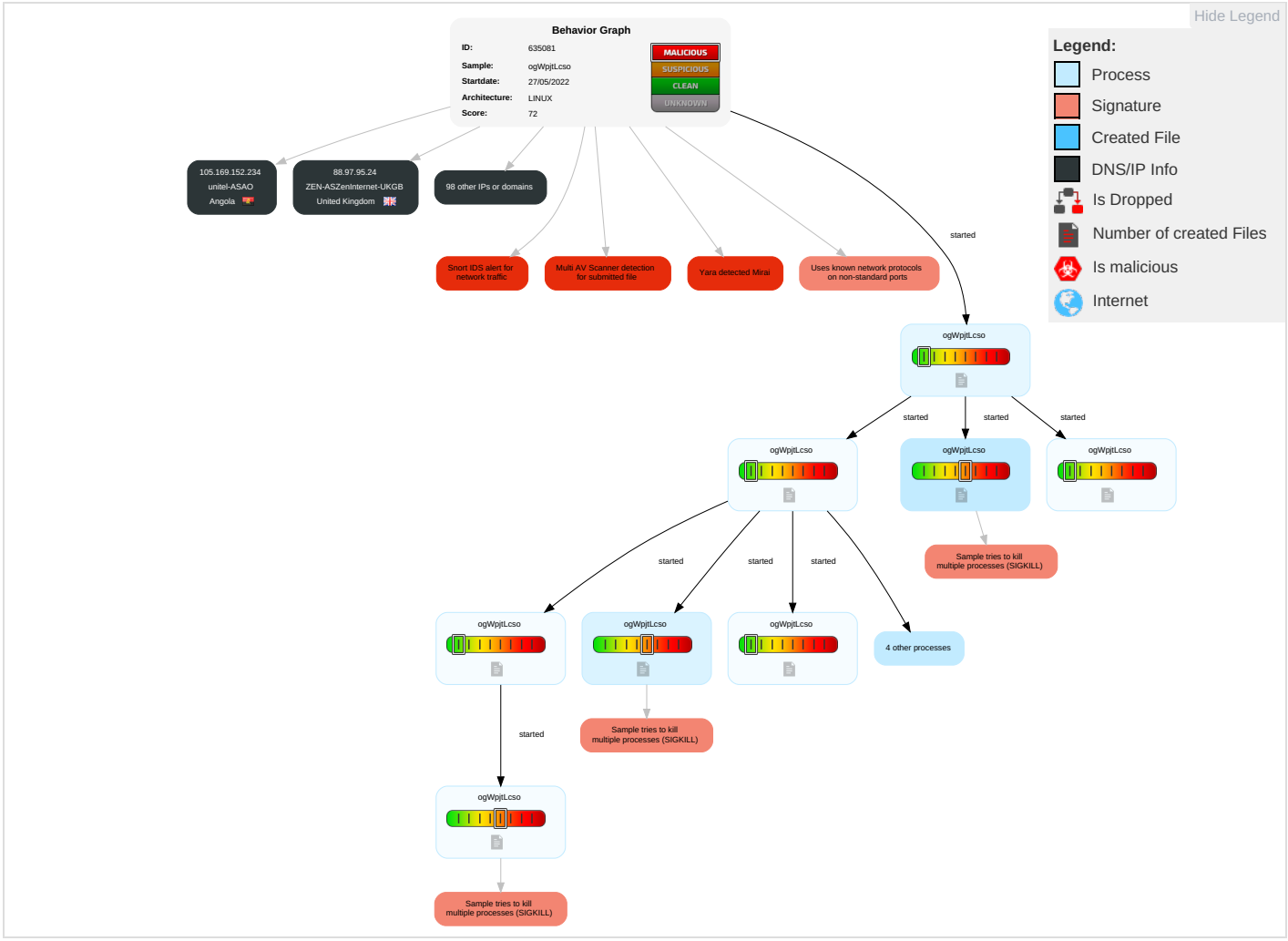
Mitre Att&ck Matrix

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	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 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	4 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	5 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	4 Ingress Tool Transfer	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Malware Configuration

No configs have been found

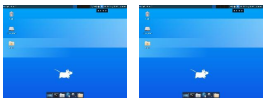
Behavior Graph

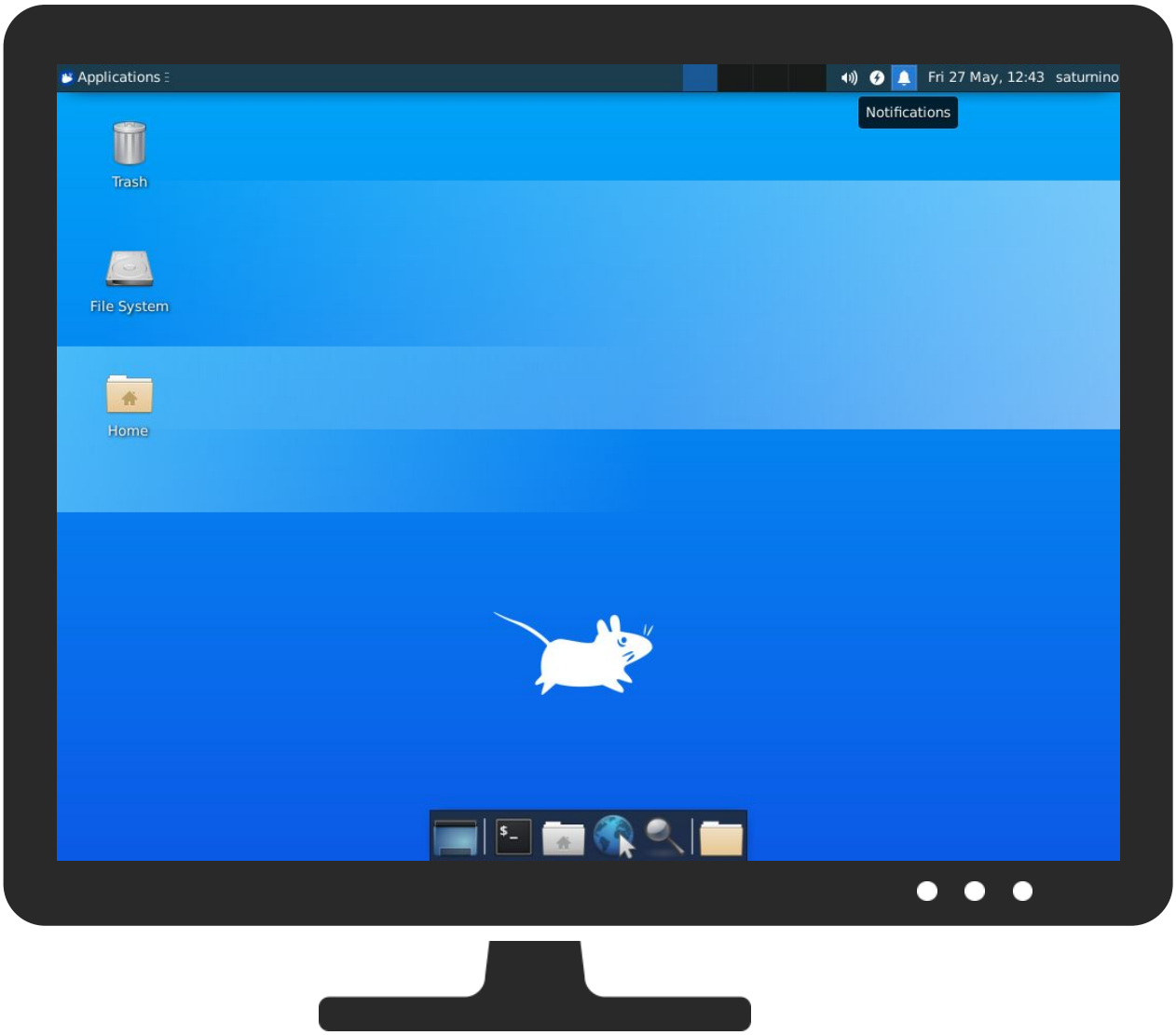


Screenshots

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
ogWpjtLcso	58%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://45.95.55.16/bins/x86	100%	Avira URL Cloud	malware	
http://45.95.55.16/8UsA.sh;	100%	Avira URL Cloud	malware	
http://192.168.0.14:80/cgi-bin/ViewLog.asp	0%	Virustotal		Browse
http://192.168.0.14:80/cgi-bin/ViewLog.asp	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

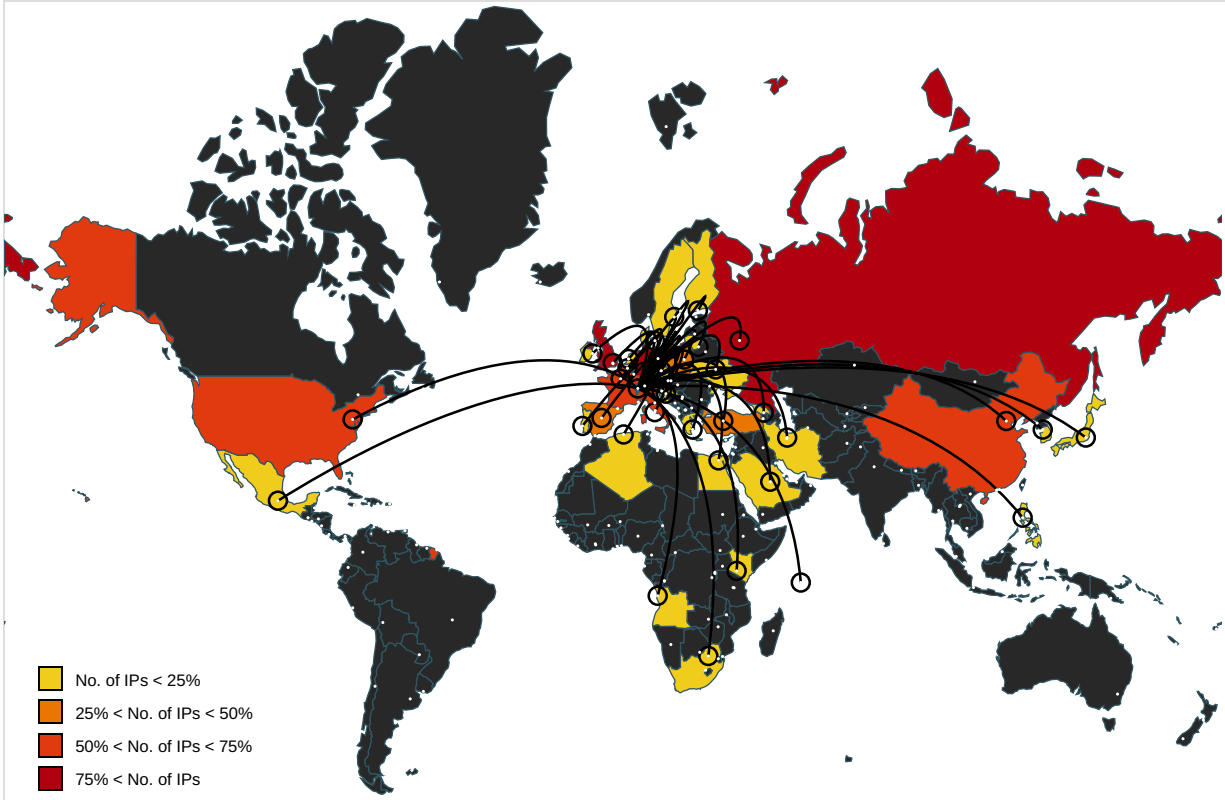
No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://192.168.0.14:80/cgi-bin/ViewLog.asp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
8.32.88.7	unknown	United States		3356	LEVEL3US	false
85.112.35.43	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
31.13.174.150	unknown	Germany		196819	TWK-KL-ASDE	false
31.199.232.18	unknown	Italy		3269	ASN-IBSNAZIT	false
88.97.95.24	unknown	United Kingdom		13037	ZEN-ASZenInternet-UKGB	false
62.42.192.125	unknown	Spain		6739	ONO-ASCableuropa-ONOES	false
95.87.151.85	unknown	Slovenia		2107	ARNES-NETAcademicandResearchNetworkofSloveniaSI	false
62.74.130.49	unknown	Greece		12361	PANAFONET-ASAthensGreeceGR	false
197.177.27.43	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
197.33.61.23	unknown	Egypt		8452	TE-ASTE-ASEG	false
95.53.226.225	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
112.148.254.212	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
31.2.120.64	unknown	Poland		21243	PLUSNETPlusGSMtransitcorenetworkPL	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
120.31.205.9	unknown	China		38372	CNNIC-RJNET-APFoShanRuiJiangScienceandTechLtdCN	false
94.42.225.63	unknown	Poland		5588	GTSCEGTSCentralEuropeAntelGermanyCZ	false
31.199.232.14	unknown	Italy		3269	ASN-IBSNAZIT	false
94.253.223.144	unknown	Croatia (LOCAL Name: Hrvatska)		31012	DCM-ASVipnetdooHR	false
85.50.194.180	unknown	Spain		12479	UNI2-ASES	false
94.132.45.235	unknown	Portugal		2860	NOS_COMUNICACOESPT	false
62.138.132.147	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	false
85.168.96.22	unknown	France		21502	ASN-NUMERICABLEFR	false
85.18.200.242	unknown	Italy		12874	FASTWEBIT	false
156.228.228.22	unknown	Seychelles		328608	Africa-on-Cloud-ASZA	false
62.182.204.139	unknown	Russian Federation		44391	ESD-ASRU	false
94.99.181.112	unknown	Saudi Arabia		25019	SAUDINETSTC-ASSA	false
85.141.148.214	unknown	Russian Federation		8359	MTSRU	false
41.114.147.134	unknown	South Africa		16637	MTNNS-ASZA	false
150.134.68.160	unknown	United States		30499	YSU-ASUS	false
31.67.116.124	unknown	United Kingdom		12576	EELtdGB	false
31.54.228.179	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
94.13.20.89	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
220.234.178.127	unknown	China		9812	CNNIC-CN-COLNETOrientalCableNetworkCoLtdCN	false
95.158.119.70	unknown	Poland		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
62.1.242.66	unknown	Greece		1241	FORTHNET-GRForthnetEU	false
31.41.10.10	unknown	Russian Federation		197658	LEVEL-NETRU	false
41.149.186.105	unknown	South Africa		5713	SAIX-NETZA	false
101.64.115.3	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
131.248.46.246	unknown	Japan		2497	IIJInternetInitiativeJapanIncJP	false
62.23.59.139	unknown	United Kingdom		8220	COLTCOLTTechnologyServicesGroupLimitedGB	false
31.100.145.29	unknown	United Kingdom		12576	EELtdGB	false
85.156.52.97	unknown	Finland		719	ELISA-ASHelsinkiFinlandEU	false
112.97.88.159	unknown	China		17623	CNCGROUP-SZChinaUnicomShenzennetworkCN	false
95.24.169.219	unknown	Russian Federation		8402	CORBINA-ASOJSCVimpelcomRU	false
94.122.78.60	unknown	Turkey		12978	DOGAN-ONLINETR	false
197.143.201.46	unknown	Algeria		36891	ICOSNET-ASDZ	false
62.110.253.242	unknown	Italy		3269	ASN-IBSNAZIT	false
95.100.100.197	unknown	European Union		20940	AKAMAI-ASN1EU	false
95.123.15.181	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
95.30.255.95	unknown	Russian Federation		3216	SOVAM-ASRU	false
95.183.142.114	unknown	Turkey		8517	ULAKNETTR	false
95.166.18.171	unknown	Denmark		3292	TDCTDCASDK	false
94.61.24.253	unknown	Portugal		12353	VODAFONE-PTVodafonePortugalPT	false
93.175.217.118	unknown	Ukraine		47359	CITYNET-ZP-ASUA	false
206.94.128.234	unknown	United States		3549	LVLT-3549US	false
85.146.193.149	unknown	Netherlands		33915	TNF-ASNL	false
83.185.2.163	unknown	Sweden		1257	TELE2EU	false
120.37.0.107	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
207.71.80.134	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
85.111.154.177	unknown	Turkey		9121	TTNETTR	false
95.255.225.252	unknown	Italy		3269	ASN-IBSNAZIT	false
157.162.207.112	unknown	Germany		22192	SSHENETUS	false
88.223.59.11	unknown	Lithuania		39354	INIT-MGNT-LT	false
31.41.10.25	unknown	Russian Federation		197658	LEVEL-NETRU	false
31.51.147.186	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
94.253.22.168	unknown	Russian Federation		21453	FLEX-ASRU	false
86.226.130.43	unknown	France		3215	FranceTelecom-OrangeFR	false
62.129.56.79	unknown	Czech Republic		30764	PODA-ASCZ	false
31.97.71.16	unknown	United Kingdom		12576	EELtdGB	false
95.225.107.124	unknown	Italy		3269	ASN-IBSNAZIT	false
85.90.55.64	unknown	United Kingdom		39116	TELEHOUSEGB	false
94.137.178.78	unknown	Georgia		16010	MAGTICOMASCaucasus-OnlineGE	false
94.178.33.195	unknown	Ukraine		6849	UKRTELNETUA	false
158.178.70.0	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
112.66.68.236	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
95.126.182.156	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
95.33.71.195	unknown	Germany		9145	EWETELCloppenburgerStrasse310DE	false
85.69.64.147	unknown	France		21502	ASN-NUMERICABLEFR	false
95.170.40.13	unknown	France		12684	SES-LUX-ASLU	false
187.246.50.58	unknown	Mexico		13999	MegaCableSAdeCVMX	false
95.33.71.197	unknown	Germany		9145	EWETELCloppenburgerStrasse310DE	false
105.169.152.234	unknown	Angola		37119	unitel-ASAO	false
95.48.117.187	unknown	Poland		5617	TPNETPL	false
108.110.174.174	unknown	United States		10507	SPCSUS	false
31.121.171.216	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
62.138.132.174	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	false
94.104.120.112	unknown	Belgium		47377	ORANGE_BELGIUM_SAKPNBelgiumBusinessNVhasbeenacquired	false
94.225.132.65	unknown	Belgium		6848	TELENET-ASBE	false
157.78.133.58	unknown	Japan		4725	ODNSoftBankMobileCorpJP	false
95.170.75.158	unknown	Netherlands		20857	TRANSIP-ASAmsterdamtheNetherlandsNL	false
95.124.218.225	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
85.203.114.11	unknown	France		30801	OZONE53avenuedelapierrevalleeFR	false
31.104.86.105	unknown	United Kingdom		12576	EELtdGB	false
85.183.86.125	unknown	Germany		6805	TDDE-ASN1DE	false
31.238.72.26	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
157.136.166.2	unknown	France		2200	FR-RENATERReseauNationaldetelecommunicationspourlaTec	false
95.118.119.239	unknown	Germany		6805	TDDE-ASN1DE	false
112.198.197.35	unknown	Philippines		132199	GLOBE-MOBILE-5TH-GEN-ASGlobeTelecomIncPH	false
37.202.175.34	unknown	Iran (ISLAMIC Republic Of)		31549	RASANAIR	false
62.222.185.78	unknown	Ireland		8918	CARRIER1-ASIE	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
95.165.157.37	unknown	Russian Federation		25513	ASN-MGTS-USPDRU	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):	6.056111413251654
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	ogWpjtLcso
File size:	72168
MD5:	e2501a4bed62e15c3cf59b781b2ab698
SHA1:	5ed9286b1b9d36a06dceac8bd0da8ba739ed68e9
SHA256:	f207c0abf680d783ddeb59dc245c4b4e84e471e44c4bb7703019bc2486fdd5d3
SHA512:	445da2858925baecc1bf643f3c93fed12e2bc059ced49caf8223d066230ca56778ce5ccf571b871099d4040669a071f2f2dd7c2101e834df8b82234cef35962c
SSDEEP:	1536:161Uv/15au1m7+tlVp5fm5tyWpRT0fN6cahWMUiU4g5X9/e35GZjOk:16+tRRYN6vhT9gi3Gj
TLSH:	256308967CC19A22C6E423BBF96E01CD332563A8D2DF321B9D212F5477CA81F0D67652
File Content Preview:	.ELF...a.....(.....4...X.....4. ...(.....(...D.....Q.td.....-...L."...vB.....0@-.\P...0....S.0...P@...0... ....R.....0...0.....0... ....R..... 0....S

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM

ELF header	
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	ARM - ABI
ABI Version:	0
Entry Point Address:	0x8190
Flags:	0x202
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	71768
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	0x8094	0x94	0x18	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x80b0	0xb0	0x10a10	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x18ac0	0x10ac0	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x18ad4	0x10ad4	0xb18	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x215f0	0x115f0	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x215f8	0x115f8	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x21604	0x11604	0x214	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x21818	0x11818	0x31c	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x11818	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	0x8000	0x8000	0x115ec	0x115ec	3.2370	0x5	R E	0x8000		.init .text .fini .rodata
LOAD	0x115f0	0x215f0	0x215f0	0x228	0x544	1.6315	0x6	RW	0x8000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2395.97.189.18244088802839471 05/27/22-12:41:26.233242	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	44088	80	192.168.2.23	95.97.189.182
192.168.2.2395.52.93.5847304802839471 05/27/22-12:41:47.290211	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	47304	80	192.168.2.23	95.52.93.58
192.168.2.2388.247.172.235136802839471 05/27/22-12:41:48.711474	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	35136	80	192.168.2.23	88.247.172.2
192.168.2.2395.101.93.9954318802839471 05/27/22-12:41:37.698966	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	54318	80	192.168.2.23	95.101.93.99

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2388.80.177.17638888802839471 05/27/22-12:41:41.709523	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	38888	80	192.168.2.23	88.80.177.176
192.168.2.2395.68.46.21445714802839471 05/27/22-12:41:31.584015	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	45714	80	192.168.2.23	95.68.46.214
192.168.2.2388.72.100.054594802839471 05/27/22-12:41:33.759271	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	54594	80	192.168.2.23	88.72.100.0
192.168.2.2395.163.124.24551614802839471 05/27/22-12:41:37.748726	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	51614	80	192.168.2.23	95.163.124.245
192.168.2.2395.85.72.11444518802839471 05/27/22-12:41:31.577298	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	44518	80	192.168.2.23	95.85.72.114
192.168.2.2395.156.226.6949982802839471 05/27/22-12:41:31.554788	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	49982	80	192.168.2.23	95.156.226.69
192.168.2.23112.137.60.7443984802839471 05/27/22-12:41:35.303316	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	43984	80	192.168.2.23	112.137.60.74
192.168.2.23197.246.192.10853320372152835222 05/27/22-12:41:42.355128	TCP	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	53320	37215	192.168.2.23	197.246.192.108
192.168.2.2388.103.220.24237162802839471 05/27/22-12:41:45.955319	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	37162	80	192.168.2.23	88.103.220.242
192.168.2.2388.221.228.20151072802839471 05/27/22-12:41:43.825767	TCP	2839471	ETPRO TROJAN Mirai Variant User-Agent (Outbound)	51072	80	192.168.2.23	88.221.228.201

TCP Packets

HTTP Request Dependency Graph

- 192.168.0.14:80

System Behavior

Analysis Process: ogWpjtLcso PID: **6230**, Parent PID: **6124**

General

Start time:	12:41:23
Start date:	27/05/2022
Path:	/tmp/ogWpjtLcso
Arguments:	/tmp/ogWpjtLcso
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: ogWpjtLcso PID: **6232**, Parent PID: **6230**

General	
Start time:	12:41:23
Start date:	27/05/2022
Path:	/tmp/ogWpjtLcso
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: ogWpjtLcso PID: **6233**, Parent PID: **6230**

General	
Start time:	12:41:23
Start date:	27/05/2022
Path:	/tmp/ogWpjtLcso
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: ogWpjtLcso PID: **6235**, Parent PID: **6230**

General	
Start time:	12:41:23
Start date:	27/05/2022
Path:	/tmp/ogWpjtLcso
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: ogWpjtLcso PID: **6238**, Parent PID: **6235**

General	
Start time:	12:41:23
Start date:	27/05/2022
Path:	/tmp/ogWpjtLcso
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: ogWpjtLcso PID: **6239**, Parent PID: **6235**

General	
Start time:	12:41:23
Start date:	27/05/2022
Path:	/tmp/ogWpjtLcso
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: ogWpjtLcso PID: **6240**, Parent PID: **6235**

General	
Start time:	12:41:23
Start date:	27/05/2022
Path:	/tmp/ogWpjtLcso
Arguments:	n/a
File size:	4956856 bytes

MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: ogWpjtLcso PID: **6241**, Parent PID: **6235**

General

Start time:	12:41:23
Start date:	27/05/2022
Path:	/tmp/ogWpjtLcso
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: ogWpjtLcso PID: **6246**, Parent PID: **6235**

General

Start time:	12:41:23
Start date:	27/05/2022
Path:	/tmp/ogWpjtLcso
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: ogWpjtLcso PID: **6247**, Parent PID: **6235**

General

Start time:	12:41:23
Start date:	27/05/2022
Path:	/tmp/ogWpjtLcso
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: ogWpjtLcso PID: **6304**, Parent PID: **6235**

General

Start time:	12:43:12
Start date:	27/05/2022
Path:	/tmp/ogWpjtLcso
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: ogWpjtLcso PID: **6306**, Parent PID: **6304**

General

Start time:	12:43:12
Start date:	27/05/2022
Path:	/tmp/ogWpjtLcso
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1