ID: 513311
Sample Name: MePwVTNRoA
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 02:17:41
Date: 02/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

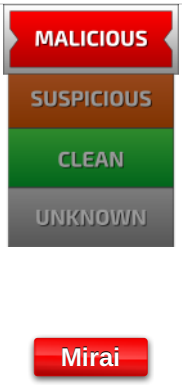
Linux Analysis Report MePwVTNRoA

Overview

General Information

Sample Name:	MePwVTNRoA
Analysis ID:	513311
MD5:	9084c57fbabbee4.
SHA1:	f0e374caec84c85..
SHA256:	514cfc468b96cb8..
Tags:	32 elf mirai powerpc
Infos:	

Detection

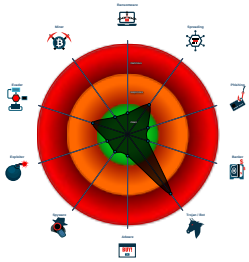


Score:	72
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Uses known network protocols on no...
- Connects to many ports of the same...
- Sample has stripped symbol table
- HTTP GET or POST without a user ...
- 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 listens on a socket

Classification



Analysis Advice

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

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	513311
Start date:	02.11.2021
Start time:	02:17:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	MePwVTNRoA
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.troj.lin@0/2@0/0
Warnings:	Show All

Process Tree

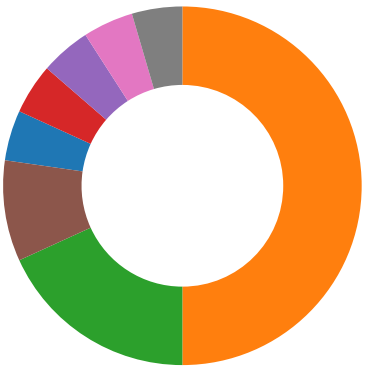
- **system is lnxubuntu20**
- MePwVTNRoA (PID: 5238, Parent: 5118, MD5: ae65271c943d3451b7f026d1fadccea6) Arguments: /tmp/MePwVTNRoA
  - MePwVTNRoA New Fork (PID: 5240, Parent: 5238)
    - MePwVTNRoA New Fork (PID: 5394, Parent: 5240)
    - MePwVTNRoA New Fork (PID: 5395, Parent: 5240)
      - MePwVTNRoA New Fork (PID: 5398, Parent: 5395)
        - MePwVTNRoA New Fork (PID: 5413, Parent: 5398)
        - MePwVTNRoA New Fork (PID: 5415, Parent: 5398)
        - MePwVTNRoA New Fork (PID: 5417, Parent: 5398)
        - MePwVTNRoA New Fork (PID: 5418, Parent: 5398)
      - MePwVTNRoA New Fork (PID: 5400, Parent: 5395)
      - MePwVTNRoA New Fork (PID: 5401, Parent: 5395)
      - MePwVTNRoA New Fork (PID: 5403, Parent: 5395)
      - MePwVTNRoA New Fork (PID: 5406, Parent: 5395)
  - MePwVTNRoA New Fork (PID: 5241, Parent: 5238)
  - MePwVTNRoA New Fork (PID: 5243, Parent: 5238)
    - MePwVTNRoA New Fork (PID: 5246, Parent: 5243)
      - MePwVTNRoA New Fork (PID: 5386, Parent: 5246)
      - MePwVTNRoA New Fork (PID: 5387, Parent: 5246)
      - MePwVTNRoA New Fork (PID: 5390, Parent: 5246)
      - MePwVTNRoA New Fork (PID: 5391, Parent: 5246)
    - MePwVTNRoA New Fork (PID: 5248, Parent: 5243)
    - MePwVTNRoA New Fork (PID: 5249, Parent: 5243)
    - MePwVTNRoA New Fork (PID: 5250, Parent: 5243)
    - MePwVTNRoA New Fork (PID: 5251, Parent: 5243)
- systemd New Fork (PID: 5285, Parent: 1)
- sshd (PID: 5285, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5286, Parent: 1)
- sshd (PID: 5286, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- **cleanup**

Yara Overview

PCAP (Network Traffic)

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

Jbx Signature Overview



- AV Detection
- Networking
- System Summary
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Uses known network protocols on non-standard ports

Connects to many ports of the same IP (likely port scanning)

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

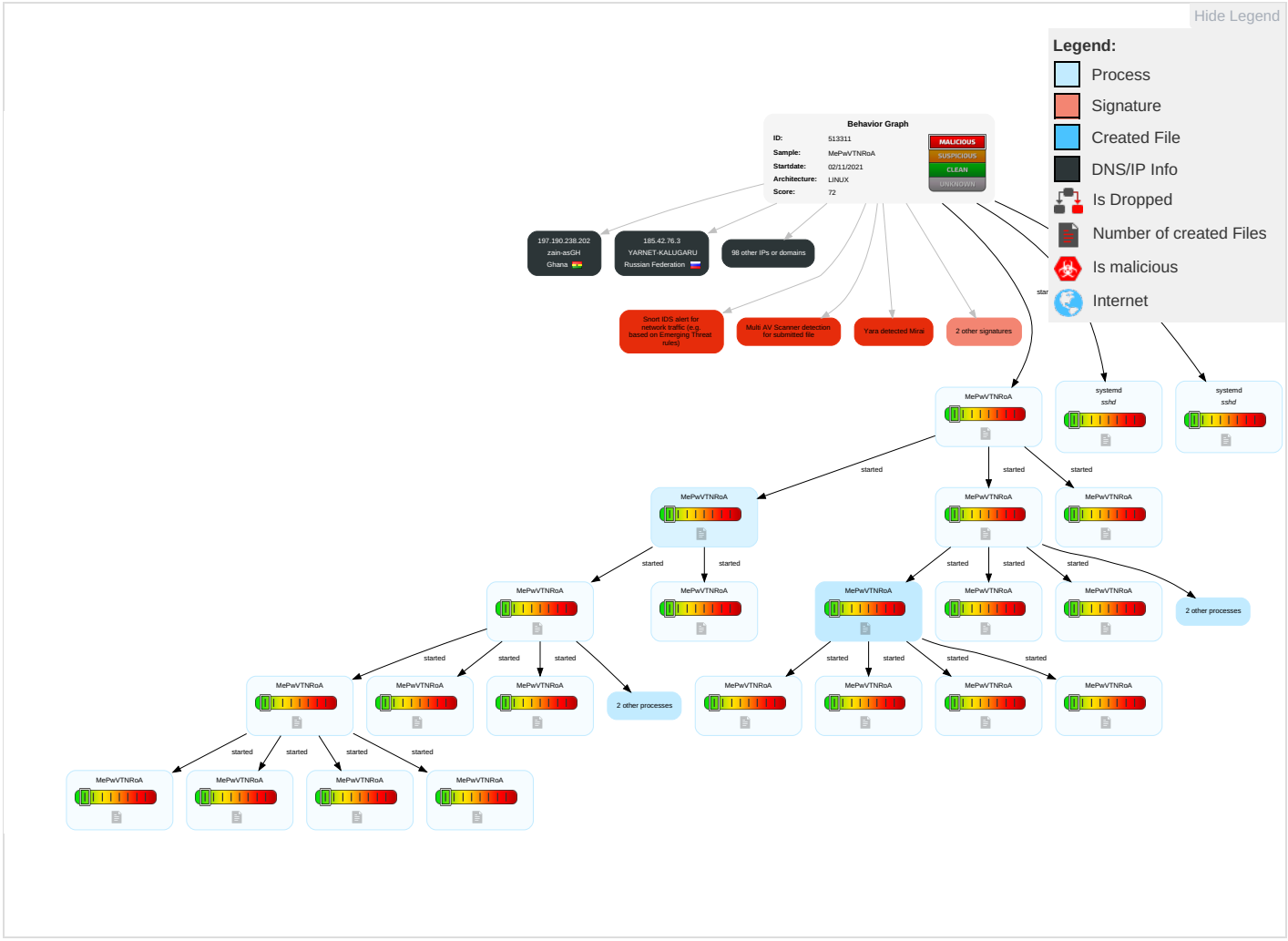
Mitre Att&ck Matrix

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	OS Credential Dumping 1	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partitio
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	Non-Standard Port 1 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockou
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	Non-Application Layer Protocol 1	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	Application Layer Protocol 2	SIM Card Swap		Carrier Billing Fraud

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
MePwVTNRoA	52%	Virustotal		Browse
MePwVTNRoA	64%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:52869/picdesc.xml	0%	Virustotal		Browse
http://127.0.0.1:52869/picdesc.xml	0%	Avira URL Cloud	safe	
http://37.0.9.202/bins/Hilix.mips	9%	Virustotal		Browse
http://37.0.9.202/bins/Hilix.mips	100%	Avira URL Cloud	malware	
http://127.0.0.1:52869/wanipcn.xml	0%	Virustotal		Browse
http://127.0.0.1:52869/wanipcn.xml	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:52869/picdesc.xml	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://127.0.0.1:52869/wanipcn.xml	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.243.89.38	unknown	Egypt		24863	LINKdotNET-ASEG	false
91.204.193.218	unknown	Austria		48151	REDBULL-ASA-5330FuschlamSeeAustriaAT	false
185.42.227.13	unknown	Iran (ISLAMIC Republic Of)		49847	RAYAZMA-ASIR	false
117.35.167.223	unknown	China		4835	CHINANET-IDC-SNChinaTelecomGroupCN	false
197.33.61.28	unknown	Egypt		8452	TE-ASTE-ASEG	false
45.205.88.163	unknown	Seychelles		54600	PEGTECHINCUS	false
185.78.232.36	unknown	Czech Republic		39248	SIVASH-ASRU	false
197.55.123.210	unknown	Egypt		8452	TE-ASTE-ASEG	false
156.0.172.150	unknown	South Africa		328112	Linux-Based-Systems-Design-ASZA	false
185.15.125.85	unknown	Denmark		208237	AS_NKKOMDK	false
45.109.69.103	unknown	Egypt		37069	MOBINILEG	false
41.145.255.174	unknown	South Africa		5713	SAIX-NETZA	false
41.76.191.220	unknown	Kenya		37225	NETWIDEZA	false
185.149.136.59	unknown	Luxembourg		2602	RESTENAReseauTeleinformatiquedelEducationNationaleLU	false
197.190.238.202	unknown	Ghana		37140	zain-asGH	false
206.22.75.132	unknown	United States		7270	NET2PHONEUS	false
91.178.113.240	unknown	Belgium		5432	PROXIMUS-ISP-ASBE	false
197.46.166.212	unknown	Egypt		8452	TE-ASTE-ASEG	false
91.105.34.51	unknown	Latvia		12578	APOLLO-ASLatviaLV	false
185.21.137.213	unknown	Iraq		209565	ALSARDFIBERIQ	false
177.236.160.6	unknown	Mexico		28538	CablemasTelecomunicacionesSAdeCVMX	false
45.50.203.136	unknown	United States		20001	TWC-20001-PACWESTUS	false
190.158.31.107	unknown	Colombia		10620	TelmexColombiaSACO	false
185.6.84.240	unknown	Netherlands		61428	FOXNL	false
45.25.228.56	unknown	United States		7018	ATT-INTERNET4US	false
185.6.84.242	unknown	Netherlands		61428	FOXNL	false
91.174.31.96	unknown	France		12322	PROXADFR	false
197.222.170.141	unknown	Egypt		37069	MOBINILEG	false
185.138.105.230	unknown	France		39405	FULLSAVE-ASFR	false
206.99.173.182	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
185.114.210.160	unknown	Switzerland		199366	TTNETDCTR	false
45.97.239.127	unknown	Egypt		37069	MOBINILEG	false
156.249.107.22	unknown	Seychelles		139086	ONL-HKOCEANNETWORKLIMITEDHK	false
45.239.81.172	unknown	Brazil		268384	JCTELECOMBR	false
123.227.0.185	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
91.57.203.202	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
185.166.97.82	unknown	Switzerland		8758	IWAYCH	false
185.35.202.43	unknown	Norway		50304	BLIXNO	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
41.76.191.231	unknown	Kenya		37225	NETWIDEZA	false
45.219.30.100	unknown	Morocco		36925	ASMediMA	false
41.169.50.119	unknown	South Africa		36937	Neotel-ASZA	false
185.204.41.57	unknown	France		205862	FEDERAL-SERVICE-ARKEAFR	false
45.75.48.156	unknown	Japan		38628	WINK-NETHIMEJICABLETELEVISIONCORPORATIONJP	false
156.223.50.230	unknown	Egypt		8452	TE-ASTE-ASEG	false
91.246.237.126	unknown	Slovenia		34779	T-2-ASASsetpropagatedbyT-2dooSI	false
91.74.73.93	unknown	United Arab Emirates		15802	DU-AS1AE	false
38.57.141.98	unknown	United States		174	COGENT-174US	false
109.195.122.89	unknown	Russian Federation		51819	YAR-ASRU	false
41.102.136.85	unknown	Algeria		36947	ALGTEL-ASDZ	false
41.101.160.215	unknown	Algeria		36947	ALGTEL-ASDZ	false
190.59.122.107	unknown	Trinidad and Tobago		5639	TelecommunicationServicesofTrinidadandTobagoTT	false
91.214.40.160	unknown	Russian Federation		60684	BNEDV-NETRU	false
91.163.145.86	unknown	France		12322	PROXADFR	false
72.248.51.187	unknown	United States		7029	WINDSTREAMUS	false
140.75.84.137	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
45.237.182.84	unknown	Brazil		268283	NETWORKFIBERCOMERCIOESERVICOSDECOMUNICACAOBR	false
45.25.228.70	unknown	United States		7018	ATT-INTERNET4US	false
45.237.182.85	unknown	Brazil		268283	NETWORKFIBERCOMERCIOESERVICOSDECOMUNICACAOBR	false
91.83.150.44	unknown	Hungary		12301	INVITECHHU	false
32.123.173.14	unknown	United States		7018	ATT-INTERNET4US	false
91.74.182.160	unknown	United Arab Emirates		15802	DU-AS1AE	false
74.140.211.191	unknown	United States		10796	TWC-10796-MIDWESTUS	false
45.109.110.136	unknown	Egypt		37069	MOBINILEG	false
197.26.6.242	unknown	Tunisia		37492	ORANGE-TN	false
91.72.131.123	unknown	United Arab Emirates		15802	DU-AS1AE	false
151.108.112.187	unknown	United States		1218	NCUBE-BELMONT-ASUS	false
70.131.38.114	unknown	United States		7018	ATT-INTERNET4US	false
91.100.152.109	unknown	Denmark		15516	DK-DANSKKABELTVDK	false
45.12.189.160	unknown	United Kingdom		35085	ACORSOFR	false
91.147.188.126	unknown	Saudi Arabia		43775	DSP-ASSA	false
156.176.96.231	unknown	Egypt		36992	ETISALAT-MISREG	false
185.42.76.3	unknown	Russian Federation		60172	YARNET-KALUGARU	false
103.30.88.246	unknown	Indonesia		18103	NEUVIZ-AS-ID-APNeuvizNetID	false
41.169.74.18	unknown	South Africa		36937	Neotel-ASZA	false
185.110.36.93	unknown	Guernsey		8680	SURE-INTERNATIONAL-LIMITEDGB	false
45.104.148.60	unknown	Egypt		37069	MOBINILEG	false
45.243.89.20	unknown	Egypt		24863	LINKdotNET-ASEG	false
197.175.223.201	unknown	South Africa		37168	CELL-CZA	false
185.26.182.191	unknown	Norway		39832	NO-OPERANO	false
41.145.154.83	unknown	South Africa		5713	SAIX-NETZA	false
91.98.40.97	unknown	Iran (ISLAMIC Republic Of)		16322	PARSONLINETehran-IRANIR	false
91.167.86.187	unknown	France		12322	PROXADFR	false
45.145.30.172	unknown	Turkey		197328	INETLTDTR	false
185.38.220.182	unknown	Poland		56523	AMELEKTRONIKPL	false
222.97.213.124	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
154.155.93.111	unknown	Kenya		36926	CKL1-ASNKE	false
45.32.45.171	unknown	United States		20473	AS-CHOOPAUS	false
62.112.56.7	unknown	Germany		13157	GOPAS-ASSchellerdamm16DE	false
120.170.161.63	unknown	Indonesia		4761	INDOSAT-INP-APINDOSATInternetNetworkProviderID	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.70.46.30	unknown	Belgium		57948	COBALTIPWorksBE	false
120.87.94.128	unknown	China		17623	CNCGROUP-SZChinaUnicomShenzennetworkCN	false
156.49.135.54	unknown	Sweden		29975	VODACOM-ZA	false
50.131.192.78	unknown	United States		7922	COMCAST-7922US	false
185.154.90.70	unknown	Italy		47406	RLNET-ASIT	false
45.135.40.230	unknown	Netherlands		4785	XTOM-AS-JPxTomJP	false
45.127.206.165	unknown	Indonesia		55699	STARNET-AS-IDPTCemerlangMultimediaID	false
134.233.80.19	unknown	United States		531	DNIC-AS-00531US	false
91.163.145.28	unknown	France		12322	PROXADFR	false
38.202.83.253	unknown	United States		9009	M247GB	false
91.251.11.8	unknown	Iran (ISLAMIC Republic Of)		197207	MCCI-ASIR	false

Runtime Messages

Command:	/tmp/MePwVTNRoA
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
197.46.166.212	arm7	Get hash	malicious	Browse	
41.76.191.220	Sht1aYGDIX	Get hash	malicious	Browse	
185.149.136.59	QUqBgpQj3B	Get hash	malicious	Browse	
197.222.170.141	x86.light	Get hash	malicious	Browse	
	djRl6t3Lqh	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
REDBULL-ASA-5330FuschlamSeeAustriaAT	arm7-20211101-1513	Get hash	malicious	Browse	• 91.204.193.254
	Ebex99Bzzw	Get hash	malicious	Browse	• 91.204.193.246
CHINANET-IDC-SNChinaTelecomGroupCN	b3astmode.x86	Get hash	malicious	Browse	• 117.34.26.57
	z3hir.x86	Get hash	malicious	Browse	• 117.35.77.205
	RkH17dHLZt	Get hash	malicious	Browse	• 120.134.45.4
	ckYh27IjHJ	Get hash	malicious	Browse	• 211.152.112.119
	cu8KB5if2T	Get hash	malicious	Browse	• 210.77.134.79
	lessie.arm7	Get hash	malicious	Browse	• 117.34.51.239
	7ylx6ZIBpI	Get hash	malicious	Browse	• 117.35.167.200
	8UoSNa8TSm	Get hash	malicious	Browse	• 120.135.246.189
	xd.arm	Get hash	malicious	Browse	• 117.34.63.42
	4czqYWTUq8	Get hash	malicious	Browse	• 218.30.14.14
	mipsel	Get hash	malicious	Browse	• 117.34.51.240
	rCCMU7CF4h	Get hash	malicious	Browse	• 124.115.177.23
	YnicivLZV8	Get hash	malicious	Browse	• 124.115.189.28

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	E38HvGUw3W	Get hash	malicious	Browse	• 124.115.165.42
	loligang.arm7	Get hash	malicious	Browse	• 120.134.94.82
	sora.x86	Get hash	malicious	Browse	• 117.35.219.181
	arm7	Get hash	malicious	Browse	• 117.35.219.196
	7NuxE5BCX7	Get hash	malicious	Browse	• 120.135.246.162
	IS4scKXqIr	Get hash	malicious	Browse	• 120.134.45.6
	5tmxDvVI5V	Get hash	malicious	Browse	• 117.35.120.218
LINKdotNET-ASEG	MkyxPXGeTq	Get hash	malicious	Browse	• 45.242.108.14
	TlhOKlVSwf	Get hash	malicious	Browse	• 41.179.6.194
	eFsSvDKams	Get hash	malicious	Browse	• 45.242.133.14
	KHSQ48GkGn	Get hash	malicious	Browse	• 197.160.66.227
	Hilix.arm	Get hash	malicious	Browse	• 45.242.108.39
	Hilix.arm7	Get hash	malicious	Browse	• 45.243.89.42
	Hilix.x86	Get hash	malicious	Browse	• 45.244.195.29
	o6aMoZKsIK	Get hash	malicious	Browse	• 41.179.108.44
	8VANaS473t	Get hash	malicious	Browse	• 41.178.243.106
	t7WU0JjLAR	Get hash	malicious	Browse	• 197.160.192.236
	Antisocial.x86	Get hash	malicious	Browse	• 45.244.195.57
	Antisocial.arm	Get hash	malicious	Browse	• 45.244.195.50
	w66OTKGVFv	Get hash	malicious	Browse	• 41.196.116.155
	swOGb2sZYt	Get hash	malicious	Browse	• 41.196.201.5
	ydZLm6GD56	Get hash	malicious	Browse	• 45.247.65.109
	BitmCvTrdO	Get hash	malicious	Browse	• 197.166.142.80
	UQnO4DB8Z1	Get hash	malicious	Browse	• 197.166.142.60
	OhUy3woBmb	Get hash	malicious	Browse	• 45.242.108.19
	mP1pg0ryFA	Get hash	malicious	Browse	• 197.166.142.55
	yxD7DmfG2j	Get hash	malicious	Browse	• 41.179.108.56
RAYAZMA-ASIR	IdR7xl9k9N	Get hash	malicious	Browse	• 185.42.227.116

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/proc/5286/oom_score_adj	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped
Size (bytes):	6
Entropy (8bit):	1.7924812503605778
Encrypted:	false
SSDEEP:	3:ptn:Dn
MD5:	CBF282CC55ED0792C33D10003D1F760A
SHA1:	007DD8BD75468E6B7ABA4285E9B267202C7EAEED
SHA-256:	FCDBAB99FCC0F4409E5F9D7D6FC497780288B4C441698126BB62832412774D22
SHA-512:	4643A8675D213C7DA35CC0C2BFB3B6F20324F9C48AEA7BA79F470615698C9A0CEFDA45CAA1957FC29110EE746BC8458AB8AB1E43EB513912A5E1E8858812CC0
Malicious:	false
Reputation:	high, very likely benign file
Preview:	-1000.

/run/sshd.pid	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped

/run/sshd.pid	
Size (bytes):	5
Entropy (8bit):	2.321928094887362
Encrypted:	false
SSDEEP:	3:CJ:CJ
MD5:	FD7D13D8915168E1FA59546966B246A8
SHA1:	BFD7D9D37901150D43877320C27E87289DCF5329
SHA-256:	7A3A168A74320D3AF5EC954E29A61CA032A01BEB82D1F1763AFFE8A019E451F3
SHA-512:	9B265063A8F7B46298B915E8710F24EB506F2730726F9B9D98C0F687A03C16CA30147D1BCD1C9E84330F0C85D8D9E32F2EA8C526B4CC32719C8812206749BCF1
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	5286.

Static File Info

General

File type:	ELF 32-bit MSB executable, PowerPC or cisco 4500, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.297947375560919
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	MePwVTNRoA
File size:	58456
MD5:	9084c57fbabbee4ccef6bc105869d070
SHA1:	f0e374caec84c854f3462733c0d8222aad591620
SHA256:	514cfc468b96cb8732a5c04796b683b9c5dd957e050611a631ad747b6351b598
SHA512:	e2492e98722861f44f14efdef1cec4d358b1e11173ad6951140518b0b07ddbc99a22f6d48ef32f799dd5a5ad967ad56b8adfe30252bdb5a658d891318b25bbba
SSDEEP:	1536:EAyte19QO0+lQZMoNrXnafkfiLWNIUFK53mS:YHO0ufoNjafkf5NIUbS
File Content Preview:	.ELF.....4...x....4. ...(.....l...l.....,.....dt.Q.....!..|.....$H...H.....$8!. |...N.. .!..|.....?...../...@..\?.....+../...A..$8...})......N..

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	PowerPC
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x100001f0
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	57976
Section Header Size:	40
Number of Section Headers:	12
Header String Table Index:	11

Sections

Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x10000094	0x94	0x24	0x0	0x6	AX	0	0	4

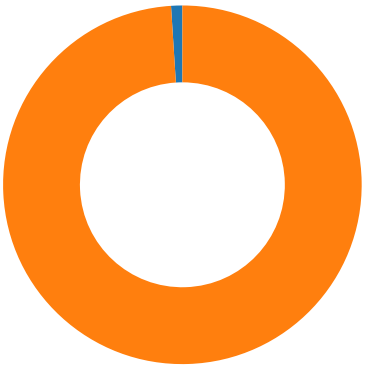
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
.text	PROGBITS	0x100000b8	0xb8	0xcc5c	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x1000cd14	0xcd14	0x20	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x1000cd34	0xcd34	0x1138	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x1001e000	0xe000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x1001e008	0xe008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x1001e018	0xe018	0x1f4	0x0	0x3	WA	0	0	8
.sdata	PROGBITS	0x1001e20c	0xe20c	0x20	0x0	0x3	WA	0	0	4
.sbss	NOBITS	0x1001e22c	0xe22c	0x8c	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x1001e2b8	0xe22c	0x25c	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0xe22c	0x4b	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	0x10000000	0x10000000	0xde6c	0xde6c	4.2988	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0xe000	0x1001e000	0x1001e000	0x22c	0x514	1.6790	0x6	RW	0x10000		.ctors .dtors .data .sdata .sbss .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



Total Packets: 99

- 37215 undefined
- 45 undefined

TCP Packets

HTTP Request Dependency Graph

- 127.0.0.1:52869

System Behavior

Analysis Process: MePwVTNRoA PID: 5238 Parent PID: 5118

General

Start time:	02:18:24

Start date:	02/11/2021
Path:	/tmp/MePwVTNRoA
Arguments:	/tmp/MePwVTNRoA
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

File Activities

File Read

Analysis Process: MePwVTNRoA PID: 5240 Parent PID: 5238

General

Start time:	02:18:24
Start date:	02/11/2021
Path:	/tmp/MePwVTNRoA
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

File Activities

File Read

Directory Enumerated

Analysis Process: MePwVTNRoA PID: 5394 Parent PID: 5240

General

Start time:	02:21:27
Start date:	02/11/2021
Path:	/tmp/MePwVTNRoA
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: MePwVTNRoA PID: 5395 Parent PID: 5240

General

Start time:	02:21:27
Start date:	02/11/2021
Path:	/tmp/MePwVTNRoA
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: MePwVTNRoA PID: 5398 Parent PID: 5395

General

Start time:	02:21:27

Start date:	02/11/2021
Path:	/tmp/MePwVTNRoA
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: MePwVTNRoA PID: 5413 Parent PID: 5398

General

Start time:	02:21:32
Start date:	02/11/2021
Path:	/tmp/MePwVTNRoA
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: MePwVTNRoA PID: 5415 Parent PID: 5398

General

Start time:	02:21:32
Start date:	02/11/2021
Path:	/tmp/MePwVTNRoA
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: MePwVTNRoA PID: 5417 Parent PID: 5398

General

Start time:	02:21:32
Start date:	02/11/2021
Path:	/tmp/MePwVTNRoA
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: MePwVTNRoA PID: 5418 Parent PID: 5398

General

Start time:	02:21:32
Start date:	02/11/2021
Path:	/tmp/MePwVTNRoA
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: MePwVTNRoA PID: 5400 Parent PID: 5395

General

Start time:	02:21:27
Start date:	02/11/2021
Path:	/tmp/MePwVTNRoA
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: MePwVTNRoA PID: 5401 Parent PID: 5395

General

Start time:	02:21:27
Start date:	02/11/2021
Path:	/tmp/MePwVTNRoA
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: MePwVTNRoA PID: 5403 Parent PID: 5395

General

Start time:	02:21:27
Start date:	02/11/2021
Path:	/tmp/MePwVTNRoA
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: MePwVTNRoA PID: 5406 Parent PID: 5395

General

Start time:	02:21:27
Start date:	02/11/2021
Path:	/tmp/MePwVTNRoA
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: MePwVTNRoA PID: 5241 Parent PID: 5238

General

Start time:	02:18:24
Start date:	02/11/2021
Path:	/tmp/MePwVTNRoA
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: MePwVTNRoA PID: 5243 Parent PID: 5238

General

Start time:	02:18:24
Start date:	02/11/2021
Path:	/tmp/MePwVTNRoA
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: MePwVTNRoA PID: 5246 Parent PID: 5243

General

Start time:	02:18:24
Start date:	02/11/2021
Path:	/tmp/MePwVTNRoA
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

File Activities

File Read

Directory Enumerated

Analysis Process: MePwVTNRoA PID: 5386 Parent PID: 5246

General

Start time:	02:21:27
Start date:	02/11/2021
Path:	/tmp/MePwVTNRoA
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: MePwVTNRoA PID: 5387 Parent PID: 5246

General

Start time:	02:21:27
Start date:	02/11/2021
Path:	/tmp/MePwVTNRoA
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: MePwVTNRoA PID: 5390 Parent PID: 5246

General

Start time:	02:21:27
Start date:	02/11/2021
Path:	/tmp/MePwVTNRoA

Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: MePwVTNRoA PID: 5391 Parent PID: 5246

General

Start time:	02:21:27
Start date:	02/11/2021
Path:	/tmp/MePwVTNRoA
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: MePwVTNRoA PID: 5248 Parent PID: 5243

General

Start time:	02:18:24
Start date:	02/11/2021
Path:	/tmp/MePwVTNRoA
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: MePwVTNRoA PID: 5249 Parent PID: 5243

General

Start time:	02:18:24
Start date:	02/11/2021
Path:	/tmp/MePwVTNRoA
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: MePwVTNRoA PID: 5250 Parent PID: 5243

General

Start time:	02:18:24
Start date:	02/11/2021
Path:	/tmp/MePwVTNRoA
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: MePwVTNRoA PID: 5251 Parent PID: 5243

General

Start time:	02:18:24

Start date:	02/11/2021
Path:	/tmp/MePwVTNRoA
Arguments:	n/a
File size:	5388968 bytes
MD5 hash:	ae65271c943d3451b7f026d1fadccea6

Analysis Process: systemd PID: 5285 Parent PID: 1

General

Start time:	02:18:37
Start date:	02/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5285 Parent PID: 1

General

Start time:	02:18:37
Start date:	02/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -t
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5286 Parent PID: 1

General

Start time:	02:18:38
Start date:	02/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5286 Parent PID: 1

General

Start time:	02:18:38
Start date:	02/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -D
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

File Written

Directory Enumerated