ID: 512016
Sample Name: x86_64
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 21:36:10
Date: 29/10/2021
Version: 34.0.0 Boulder Opal

Table of Contents

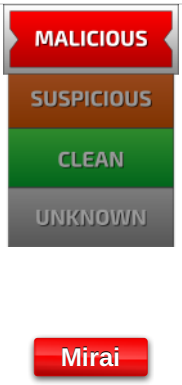
Linux Analysis Report x86_64

Overview

General Information

Sample Name:	x86_64
Analysis ID:	512016
MD5:	7a40533ae23c9a..
SHA1:	1be1d20769e6d3..
SHA256:	edc6930b30ecad..
Tags:	elf
Infos:	

Detection

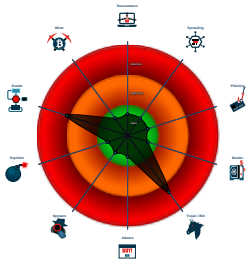


Score:	76
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Sample deletes itself
- Uses known network protocols on no...
- Machine Learning detection for samp...
- Yara signature match
- Sample has stripped symbol table
- Tries to connect to HTTP servers, b...
- Detected TCP or UDP traffic on non...

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	512016
Start date:	29.10.2021
Start time:	21:36:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	x86_64
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.troj.evad.lin@0/0@1/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
  - x86_64 (PID: 5247, Parent: 5116, MD5: 7a40533ae23c9ad78f62854030cae373) Arguments: /tmp/x86_64
    - x86_64 New Fork (PID: 5248, Parent: 5247)
    - x86_64 New Fork (PID: 5249, Parent: 5247)
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
x86_64	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x12bf8:$xo1: \x19;.=885{azd • 0x12c68:$xo1: \x19;.=885{azd • 0x12ccc:$xo1: \x19;.=885{azd • 0x12d38:$xo1: \x19;.=885{azd • 0x12da4:$xo1: \x19;.=885{azd • 0x12e98:$xo1: \x19;.=885{azd • 0x12f00:$xo1: \x19;.=885{azd • 0x12f70:$xo1: \x19;.=885{azd • 0x12fe0:$xo1: \x19;.=885{azd • 0x13050:$xo1: \x19;.=885{azd • 0x130c0:$xo1: \x19;.=885{azd • 0x131e4:$xo1: \x175 366;uotj • 0x13254:$xo1: \x175 366;uotj • 0x132c4:$xo1: \x175 366;uotj • 0x13334:$xo1: \x175 366;uotj • 0x133a4:$xo1: \x175 366;uotj • 0x1341c:$xo1: \x19;.=885{azd • 0x13460:$xo1: \x19;.=885{azd • 0x134ac:$xo1: \x19;.=885{azd • 0x13508:$xo1: \x19;.=885{azd • 0x13550:$xo1: \x19;.=885{azd

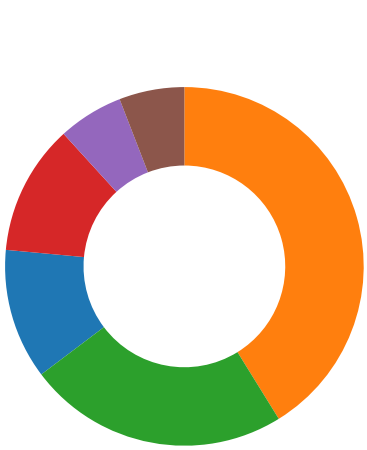
PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
5247.1.00000000c83f63f6.000000005310170b.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x5c8:$xo1: \x175 366;uotj • 0x640:$xo1: \x175 366;uotj • 0x6b8:$xo1: \x175 366;uotj • 0x730:$xo1: \x175 366;uotj • 0x7a8:$xo1: \x175 366;uotj • 0x828:$xo1: \x19;.=885{azd • 0x898:$xo1: \x19;.=885{azd • 0x900:$xo1: \x19;.=885{azd • 0x970:$xo1: \x19;.=885{azd • 0x9e0:$xo1: \x19;.=885{azd • 0xae0:$xo1: \x19;.=885{azd • 0xb98:$xo1: \x19;.=885{azd • 0xbe0:$xo1: \x19;.=885{azd • 0xc30:$xo1: \x19;.=885{azd • 0xc90:$xo1: \x19;.=885{azd • 0xcd8:$xo1: \x19;.=885{azd • 0xcf8:$xo1: \x19;.=885{azd • 0xd48:$xo1: \x19;.=885{azd • 0xd90:$xo1: \x19;.=885{azd • 0xdf0:$xo1: \x19;.=885{azd • 0xe60:$xo1: \x19;.=885{azd
5247.1.000000001a887bdc.000000000b831e49.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x12bf8:$xo1: \x19;.=885{azd • 0x12c68:$xo1: \x19;.=885{azd • 0x12ccc:$xo1: \x19;.=885{azd • 0x12d38:$xo1: \x19;.=885{azd • 0x12da4:$xo1: \x19;.=885{azd • 0x12e98:$xo1: \x19;.=885{azd • 0x12f00:$xo1: \x19;.=885{azd • 0x12f70:$xo1: \x19;.=885{azd • 0x12fe0:$xo1: \x19;.=885{azd • 0x13050:$xo1: \x19;.=885{azd • 0x130c0:$xo1: \x19;.=885{azd • 0x131e4:$xo1: \x175 366;uotj • 0x13254:$xo1: \x175 366;uotj • 0x132c4:$xo1: \x175 366;uotj • 0x13334:$xo1: \x175 366;uotj • 0x133a4:$xo1: \x175 366;uotj • 0x1341c:$xo1: \x19;.=885{azd • 0x13460:$xo1: \x19;.=885{azd • 0x134ac:$xo1: \x19;.=885{azd • 0x13508:$xo1: \x19;.=885{azd • 0x13550:$xo1: \x19;.=885{azd

Jbx Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

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

Uses known network protocols on non-standard ports

Hooking and other Techniques for Hiding and Protection:

Sample deletes itself

Uses known network protocols on non-standard ports

Stealing of Sensitive Information:

Yara detected Mirai

Remote Access Functionality:

Yara detected Mirai

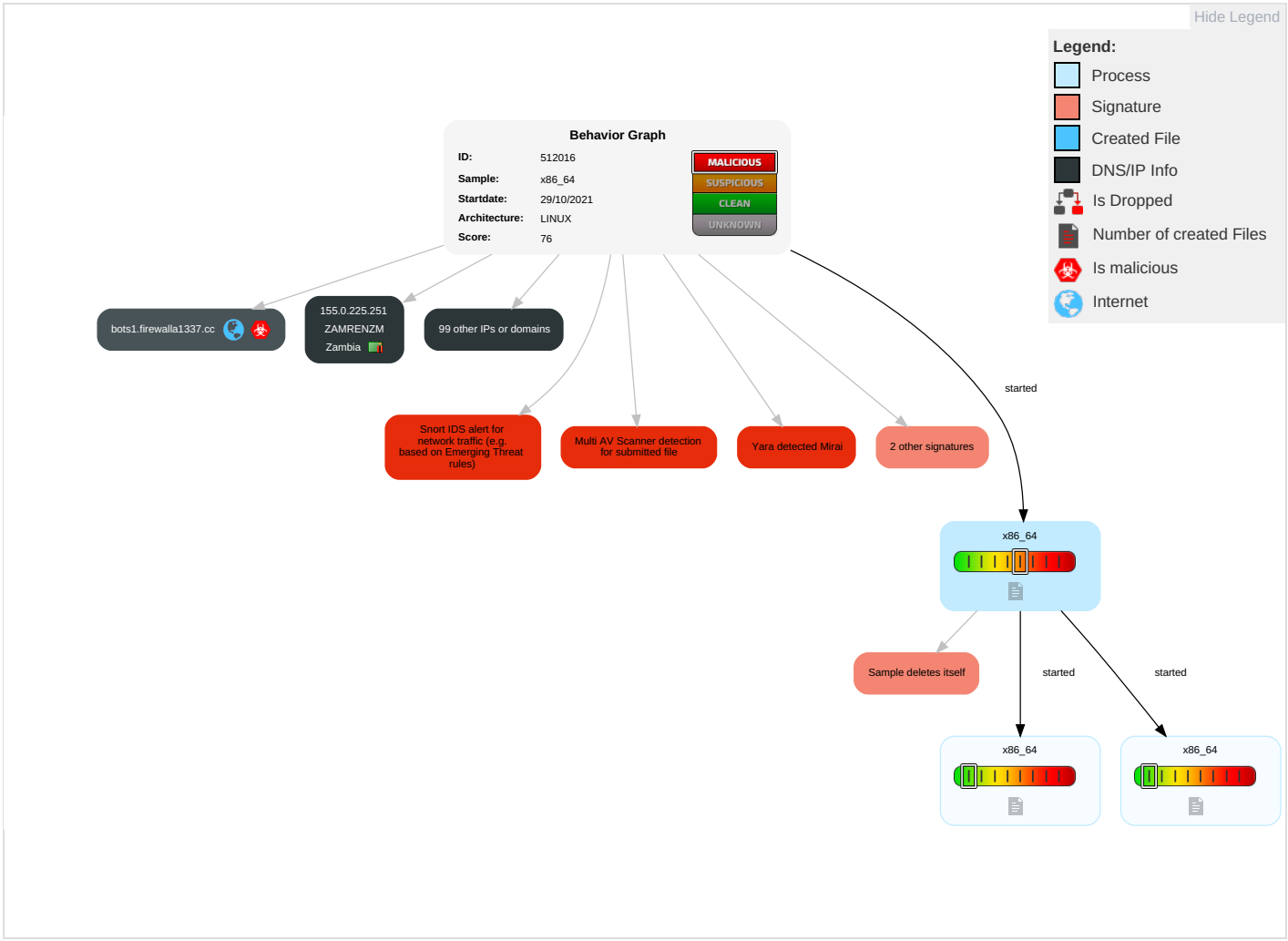
Mitre Att&ck Matrix

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	File Deletion 1	OS Credential Dumping	System Service Discovery	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 Partition
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 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	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
x86_64	51%	Virustotal		Browse
x86_64	56%	ReversingLabs	Linux.Trojan.Mirai	
x86_64	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
bots1.firewalla1337.cc	8%	Virustotal		Browse

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bots1.firewalla1337.cc	107.189.1.185	true	true	• 8%, Virustotal, Browse	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
130.133.232.22	unknown	Germany		680	DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	false
155.0.225.251	unknown	Zambia		37532	ZAMRENZM	false
198.172.66.199	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
82.221.214.204	unknown	Iceland		50613	THORDC-ASIS	false
108.11.242.13	unknown	United States		701	UUNETUS	false
120.244.148.81	unknown	China		56048	CMNET-BEIJING-APChinaMobileCommunicaitonsCorporationCN	false
74.221.73.199	unknown	United States		29979	PWN-ASBLKUS	false
177.75.64.252	unknown	Brazil		53087	TELYLtdaBR	false
176.67.2.102	unknown	Ukraine		25133	MCLAUT-ASUA	false
43.118.71.45	unknown	Japan		4249	LILLY-ASUS	false
157.121.89.74	unknown	United States		2514	INFOSPHERENTTPCCommunicationsIncJP	false
210.47.182.189	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
63.77.90.121	unknown	United States		701	UUNETUS	false
196.37.208.82	unknown	South Africa		3741	ISZA	false
193.11.59.4	unknown	Sweden		1653	SUNETSUNETSwedishUniversityNetworkEU	false
87.17.178.55	unknown	Italy		3269	ASN-IBSNAZIT	false
124.51.222.169	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
57.138.213.131	unknown	Belgium		2686	ATGS-MMD-ASUS	false
13.143.18.135	unknown	United States		7018	ATT-INTERNET4US	false
103.12.43.115	unknown	Pakistan		17557	PKTELECOM-AS-PKPakistanTelecommunicationCompanyLimited	false
174.35.85.209	unknown	United States		36408	CDNETWORKSUS-02US	false
114.69.8.59	unknown	Japan		2519	VECTANTARTERIANetworksCorporationJP	false
96.223.226.155	unknown	United States		7922	COMCAST-7922US	false
115.132.18.46	unknown	Malaysia		4788	TMNET-AS-APTMNetInternetServiceProviderMY	false
154.137.125.103	unknown	Egypt		37069	MOBINILEG	false
136.209.152.247	unknown	United States		1556	DNIC-ASBLK-01550-01601US	false
186.233.176.86	unknown	Brazil		53209	MantiqueiraTecnologiaLtdaBR	false
174.167.169.170	unknown	United States		7922	COMCAST-7922US	false
117.198.255.236	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	false
180.251.193.119	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
78.16.135.24	unknown	Ireland		2110	AS-BTIREBTIrelandwaspreviouslyknownasEsatNetEUnet	false
179.48.52.52	unknown	unknown		3816	COLOMBIATELECOMUNICACIONESSAESPCO	false
71.244.220.141	unknown	United States		701	UUNETUS	false
91.178.161.159	unknown	Belgium		5432	PROXIMUS-ISP-ASBE	false
202.92.242.39	unknown	Australia		18111	NETSPEED-AS-APNetspeedInternetCommunicationsAU	false
206.155.137.28	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
208.80.224.3	unknown	United States		33680	TELEPERFORMANCE-USAUS	false
157.71.232.72	unknown	Japan		131932	JEIS-NETJREastInformationSystemsCompanyJP	false
74.235.184.1	unknown	United States		7018	ATT-INTERNET4US	false
43.226.205.246	unknown	China		133881	RBSPL-AS-APRetracBusinessSolutionsPtyLtdAU	false
145.173.25.109	unknown	Netherlands		59524	KPN-IAASNL	false
136.171.73.191	unknown	United States		2152	CSUNET-NWUS	false
124.100.26.173	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
52.214.28.2	unknown	United States		16509	AMAZON-02US	false
77.18.134.247	unknown	Norway		2119	TELENOR-NEXTELTelenorNorgeASNO	false
74.160.83.161	unknown	United States		10796	TWC-10796-MIDWESTUS	false
198.137.125.185	unknown	United States		292	ESNET-WESTUS	false
17.254.82.69	unknown	United States		714	APPLE-ENGINEERINGUS	false
150.193.183.205	unknown	United States		1479	DNIC-ASBLK-01478-01479US	false
209.62.244.169	unknown	United States		32719	BEPC-ASUS	false
13.53.138.117	unknown	United States		16509	AMAZON-02US	false
150.215.62.48	unknown	United States		3680	NOVELLUS	false
76.226.188.67	unknown	United States		7018	ATT-INTERNET4US	false
191.184.76.41	unknown	Brazil		28573	CLAROSABR	false
213.198.183.242	unknown	Italy		15589	ASN-CLOUDITALIAIT	false
156.99.71.214	unknown	United States		1998	STATE-OF-MNUS	false
105.64.212.1	unknown	Morocco		36884	MAROCCONNECTMA	false
123.148.206.41	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
202.146.173.26	unknown	China		24212	JASNET-AS-IDPTJASNITATELEKOMINDOID	false
191.167.46.134	unknown	Brazil		26615	TIMSABR	false
169.18.199.22	unknown	United States		37611	AfrihostZA	false
193.23.6.28	unknown	Romania		51799	FIDELNET-ASStrIonIrimescuNr307SatSfantullieRO	false
135.47.229.218	unknown	United States		54614	CIKTELECOM-CABLECA	false
142.105.76.151	unknown	United States		12271	TWC-12271-NYCUS	false
193.68.159.5	unknown	Bulgaria		3245	DIGSYS-ASBG	false
37.99.130.185	unknown	Saudi Arabia		47794	ATHEEB-ASSA	false
211.57.156.75	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
141.114.210.100	unknown	United States		557	UMAINE-SYS-ASUS	false
163.185.9.187	unknown	United States		72	SCHLUMBERGER-ASUS	false
183.235.236.244	unknown	China		56040	CMNET-GUANGDONG-APChinaMobilecommunicationscorporation	false
186.106.45.195	unknown	Chile		7418	TELEFONICACHILESACL	false
150.44.223.255	unknown	Japan		9991	SHUDO-UHiroshimaShudoUniversityJP	false
182.80.182.5	unknown	China		23771	SXBCTV-APSXBCTVInternetServiceProviderCN	false
19.125.23.83	unknown	United States		3	MIT-GATEWAYSUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
161.62.8.86	unknown	Switzerland		559	SWITCHPeeringrequestspeeringswitchchEU	false
187.123.195.13	unknown	Brazil		28573	CLAROSABR	false
46.79.34.204	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
159.51.229.171	unknown	Germany		20561	AS20561-INADE	false
51.44.192.155	unknown	United States		2686	ATGS-MMD-ASUS	false
160.40.127.133	unknown	Greece		47616	CERTHGR	false
94.107.201.172	unknown	Belgium		47377	ORANGE_BELGIUM_SAKPNBelgiumBusinessNVhasbeenacquired	false
152.40.102.142	unknown	United States		53785	UNC-GREENSBOROUS	false
96.138.142.23	unknown	United States		7922	COMCAST-7922US	false
108.67.11.143	unknown	United States		7018	ATT-INTERNET4US	false
44.66.151.214	unknown	United States		7377	UCSDUS	false
43.105.198.76	unknown	Japan		4249	LILLY-ASUS	false
98.160.221.119	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
64.154.123.164	unknown	United States		3356	LEVEL3US	false
126.58.120.109	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
159.51.14.151	unknown	Germany		20561	AS20561-INADE	false
129.55.204.176	unknown	United States		63	LL-MIUS	false
179.32.239.38	unknown	Colombia		3816	COLOMBIATELECOMUNICACIONESSAESPCO	false
173.179.156.229	unknown	Canada		5769	VIDEOTRONCA	false
119.13.200.68	unknown	Australia		9723	ISEEK-AS-APiseekCommunicationsPtyLtdAU	false
170.255.199.23	unknown	Belgium		5400	BTGB	false
189.104.135.131	unknown	Brazil		7738	TelemarNorteLesteSABR	false
103.57.39.81	unknown	Indonesia		55699	STARNET-AS-IDPTCemerlangMultimediaID	false
189.181.130.66	unknown	Mexico		8151	UninetSAdeCVMX	false
157.62.205.22	unknown	United States		22192	SSHENETUS	false
2.160.72.2	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false

Runtime Messages

Command:	/tmp/x86_64
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	listening to tun0
Standard Error:	

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
bots1.firewalla1337.cc	jJ6GK5qbZt	Get hash	malicious	Browse	• 107.189.1.185
	KPz4ERtS9a	Get hash	malicious	Browse	• 107.189.1.185
	UNNEIaOxVM	Get hash	malicious	Browse	• 107.189.1.185
	ATc5uxXITp	Get hash	malicious	Browse	• 107.189.1.185
	il32XbklZm	Get hash	malicious	Browse	• 107.189.1.185

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IN7REq0Jv5	Get hash	malicious	Browse	• 107.189.1.185
	HDgtpV43hX	Get hash	malicious	Browse	• 107.189.1.185
	B2WBaqkm8k	Get hash	malicious	Browse	• 107.189.1.185
	7SerHvEAjE	Get hash	malicious	Browse	• 107.189.1.185
	i686	Get hash	malicious	Browse	• 107.189.1.185
	m5DozqUO2t	Get hash	malicious	Browse	• 107.189.1.185
	avxeC9Wssi	Get hash	malicious	Browse	• 107.189.1.185
	ayx5kFWYmZ	Get hash	malicious	Browse	• 107.189.1.185
	p4vXpD0P73	Get hash	malicious	Browse	• 107.189.1.185
	j3LQELTT0m	Get hash	malicious	Browse	• 107.189.1.185
	BLBHEA8knd	Get hash	malicious	Browse	• 107.189.1.185
	mips	Get hash	malicious	Browse	• 107.189.1.185
	x86_64	Get hash	malicious	Browse	• 107.189.1.185
	arm	Get hash	malicious	Browse	• 107.189.1.185
	Ynffczq7m4	Get hash	malicious	Browse	• 107.189.1.185

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DFNVereinzurFoerderungeinesDeutschenForschungsnetzese	vEBWe85OY5	Get hash	malicious	Browse	• 193.174.164.2
	5mLAGfiGBf	Get hash	malicious	Browse	• 141.94.41.5
	Installer.exe	Get hash	malicious	Browse	• 141.94.188.139
	LCgNoeCOl6	Get hash	malicious	Browse	• 141.61.124.247
	yZ7D7o1Z7p	Get hash	malicious	Browse	• 149.222.208.5
	sj2211QUKu	Get hash	malicious	Browse	• 141.65.9.77
	P4ci8kzzCS.exe	Get hash	malicious	Browse	• 141.94.188.138
	dMP72tpVfm.exe	Get hash	malicious	Browse	• 141.94.188.138
	mdyu2wtnR8	Get hash	malicious	Browse	• 188.1.166.66
	GQM8qzLfFs	Get hash	malicious	Browse	• 192.108.25.227
	Installer.exe	Get hash	malicious	Browse	• 141.94.188.139
	KPz4ERtS9a	Get hash	malicious	Browse	• 141.30.26.199
	Cleaner.exe	Get hash	malicious	Browse	• 141.94.188.139
	uK570ZEpyQ	Get hash	malicious	Browse	• 141.9.190.205
	pLpqV3XZ76	Get hash	malicious	Browse	• 141.99.244.214
	b3astmode.x86	Get hash	malicious	Browse	• 141.35.196.152
	JYWllP5wHP	Get hash	malicious	Browse	• 132.199.16 5.171
	uwgXkY20gB	Get hash	malicious	Browse	• 139.21.47.133
	sora.x86	Get hash	malicious	Browse	• 141.99.244.226
	sora.arm7	Get hash	malicious	Browse	• 193.174.61.141
NTT-COMMUNICATIONS-2914US	WnhlYWJ5C5	Get hash	malicious	Browse	• 205.47.168.95
	RVG73cR3DP	Get hash	malicious	Browse	• 205.45.106.28
	2pPPNW1XSo	Get hash	malicious	Browse	• 168.143.4.195
	1b5356SnwB	Get hash	malicious	Browse	• 204.1.128.214
	yZ7D7o1Z7p	Get hash	malicious	Browse	• 198.247.45.180
	arm7	Get hash	malicious	Browse	• 209.69.48.55
	KPz4ERtS9a	Get hash	malicious	Browse	• 198.65.209.238
	db0fa4b8db0333367e9bda3ab68b8042.x86	Get hash	malicious	Browse	• 204.156.18.76
	MjqRJNVy8K	Get hash	malicious	Browse	• 204.141.27.195
	GvPiIhzmX1	Get hash	malicious	Browse	• 161.58.199.139
	gKCq4VLpjL	Get hash	malicious	Browse	• 207.153.20 8.134
	UYnpKcFZ2s	Get hash	malicious	Browse	• 206.54.15.11
	pLpqV3XZ76	Get hash	malicious	Browse	• 198.65.210.163
	b3astmode.arm7	Get hash	malicious	Browse	• 209.238.13 7.106
	arm	Get hash	malicious	Browse	• 104.88.11.46
	FWsCarsq8Q	Get hash	malicious	Browse	• 128.241.223.16
	sora.arm7	Get hash	malicious	Browse	• 209.70.74.37
	PFD33mzc5l	Get hash	malicious	Browse	• 205.47.193.77
	7qvn4qlmi3	Get hash	malicious	Browse	• 206.58.73.143
	JuofJwjQMT	Get hash	malicious	Browse	• 161.58.199.187
ZAMRENZM	2pPPNW1XSo	Get hash	malicious	Browse	• 155.1.97.79

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	S1WMHUXAQU	Get hash	malicious	Browse	• 155.132.115.250
	UYnpKcFZ2s	Get hash	malicious	Browse	• 155.181.232.64
	dAhGa49Lql	Get hash	malicious	Browse	• 155.73.40.76
	kMn6L4fH2T	Get hash	malicious	Browse	• 155.176.102.219
	H9pX0VKTN5	Get hash	malicious	Browse	• 155.180.201.36
	hoho.arm7	Get hash	malicious	Browse	• 155.73.39.82
	jew.x86	Get hash	malicious	Browse	• 155.21.62.219
	7mtKAPnOCb	Get hash	malicious	Browse	• 155.160.190.198
	1WL2kQmrNk	Get hash	malicious	Browse	• 155.67.122.229
	0FPjf8qK5E	Get hash	malicious	Browse	• 155.17.233.118
	fK8cP1dNlv	Get hash	malicious	Browse	• 155.128.185.199
	5yjXpBEf1o	Get hash	malicious	Browse	• 155.21.178.46
	666.arm	Get hash	malicious	Browse	• 155.132.115.244
	hoho.x86	Get hash	malicious	Browse	• 155.67.50.170
	hoho.arm	Get hash	malicious	Browse	• 155.183.159.109
	arm7-20211013-0650	Get hash	malicious	Browse	• 155.176.111.219
	x86	Get hash	malicious	Browse	• 155.160.14.181
	ubr43ro8gn	Get hash	malicious	Browse	• 155.73.27.79
	yE2Dyk0Dcv	Get hash	malicious	Browse	• 155.181.220.25

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, Intel 80386, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.436972842754819
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	x86_64
File size:	82704
MD5:	7a40533ae23c9ad78f62854030cae373
SHA1:	1be1d20769e6d38dce5df729347ec73487d91bc7
SHA256:	edc6930b30ecad1c771ed2297a7633303663bbe49ee1837c57266167d532e4f7
SHA512:	c0c5d3a170a68466ca0a2ab18f4f08639f1f9f2039b0c4909b07f436550d55def8af45e9ab0b5cffd047e0260744b13375925bbaa2db380aecdea96ad18623ae
SSDEEP:	1536:2EnSyw5t+1LeAvKwjPYZEnhuBcnWYfHGutkf/sSX+/ALeAvWlfwhU+yi5+EH:XSypKAvBjPYZsh8cnWYfHGuSsSX+/ALN

General

File Content Preview:	.ELF.....d...4....A.....4. ...(.....;...;..... .....@.....@.....Q.td.....U..S..... w?...h....S...[]...$.....U.....=@....t..5....$.....$.....u.... ....t....h.....

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	Intel 80386
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x8048164
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	82304
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	0x8048094	0x94	0x1c	0x0	0x6	AX	0	0	1
.text	PROGBITS	0x80480b0	0xb0	0x11f76	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x805a026	0x12026	0x17	0x0	0x6	AX	0	0	1
.rodata	PROGBITS	0x805a040	0x12040	0x1b60	0x0	0x2	A	0	0	32
.ctors	PROGBITS	0x805c000	0x14000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x805c008	0x14008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x805c020	0x14020	0x120	0x0	0x3	WA	0	0	32
.bss	NOBITS	0x805c140	0x14140	0x840	0x0	0x3	WA	0	0	32
.shstrtab	STRTAB	0x0	0x14140	0x3e	0x0	0x0		0	0	1

Program Segments

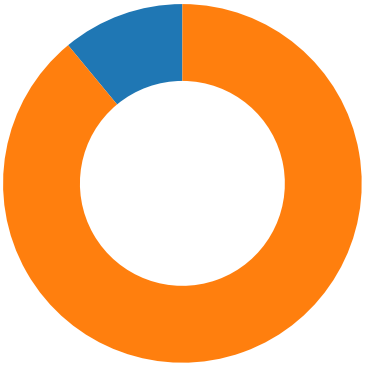
Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8048000	0x8048000	0x13ba0	0x13ba0	3.9183	0x5	R E	0x1000		.init .text .fini .rodata
LOAD	0x14000	0x805c000	0x805c000	0x140	0x980	2.4523	0x6	RW	0x1000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution

Total Packets: 100

- 23 (Telnet)
- 2323 undefined



TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 29, 2021 21:36:54.268131971 CEST	192.168.2.23	1.1.1.1	0xedca	Standard query (0)	bots1.fire walla1337.cc	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 29, 2021 21:36:54.285510063 CEST	1.1.1.1	192.168.2.23	0xedca	No error (0)	bots1.fire walla1337.cc		107.189.1.185	A (IP address)	IN (0x0001)

System Behavior

Analysis Process: x86_64 PID: 5247 Parent PID: 5116

General

Start time:	21:36:53
Start date:	29/10/2021
Path:	/tmp/x86_64
Arguments:	/tmp/x86_64
File size:	82704 bytes
MD5 hash:	7a40533ae23c9ad78f62854030cae373

File Activities

File Deleted

Analysis Process: x86_64 PID: 5248 Parent PID: 5247

General

Start time:	21:36:53
Start date:	29/10/2021
Path:	/tmp/x86_64
Arguments:	n/a

File size:	82704 bytes
MD5 hash:	7a40533ae23c9ad78f62854030cae373

Analysis Process: x86_64 PID: 5249 Parent PID: 5247

General

Start time:	21:36:53
Start date:	29/10/2021
Path:	/tmp/x86_64
Arguments:	n/a
File size:	82704 bytes
MD5 hash:	7a40533ae23c9ad78f62854030cae373