ID: 514272
Sample Name: x86-20211103-0152
Cookbook: defaultlinuxfilecookbook.jbs
Time: 03:26:25
Date: 03/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2021

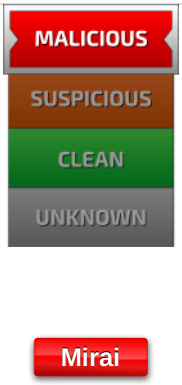
Linux Analysis Report x86-20211103-0152

Overview

General Information

Sample Name:	x86-20211103-0152
Analysis ID:	514272
MD5:	48bfe55d7795f2d..
SHA1:	760d6b9c2779c3..
SHA256:	fa1be914982a111.
Tags:	Mirai
Infos:	

Detection

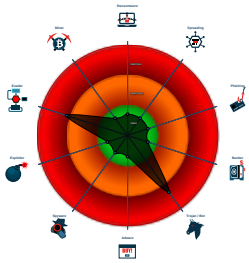


Score:	76
Range:	0 - 100
Whitelisted:	false

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:	514272
Start date:	03.11.2021
Start time:	03:26:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	x86-20211103-0152
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**
  - x86-20211103-0152 (PID: 5237, Parent: 5113, MD5: 48bfe55d7795f2d6905c6cdbea372b9b) Arguments: /tmp/x86-20211103-0152
    - x86-20211103-0152 New Fork (PID: 5238, Parent: 5237)
    - x86-20211103-0152 New Fork (PID: 5239, Parent: 5237)
- **cleanup**

Copyright Joe Security LLC 2021

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
x86-20211103-0152	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x139dc:$xo1: \x19;.=885{azd • 0x13a4c:$xo1: \x19;.=885{azd • 0x13ab0:$xo1: \x19;.=885{azd • 0x13b1c:$xo1: \x19;.=885{azd • 0x13b88:$xo1: \x19;.=885{azd • 0x13c7c:$xo1: \x19;.=885{azd • 0x13ce4:$xo1: \x19;.=885{azd • 0x13d54:$xo1: \x19;.=885{azd • 0x13dc4:$xo1: \x19;.=885{azd • 0x13e34:$xo1: \x19;.=885{azd • 0x13ea4:$xo1: \x19;.=885{azd • 0x13fc8:$xo1: \x175 366;uotj • 0x14038:$xo1: \x175 366;uotj • 0x140a8:$xo1: \x175 366;uotj • 0x14118:$xo1: \x175 366;uotj • 0x14188:$xo1: \x175 366;uotj • 0x14200:$xo1: \x19;.=885{azd • 0x14244:$xo1: \x19;.=885{azd • 0x14290:$xo1: \x19;.=885{azd • 0x142ec:$xo1: \x19;.=885{azd • 0x14334:$xo1: \x19;.=885{azd

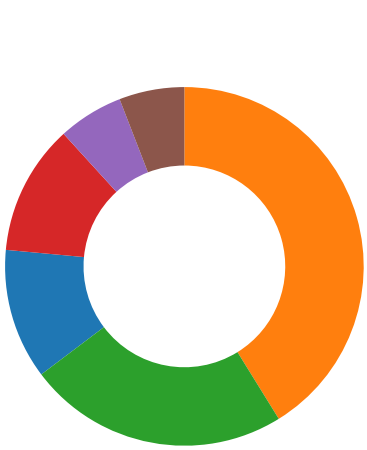
PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
5237.1.00000000c2a55aea.00000000adfd88f2.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x5d0:$xo1: \x175 366;uotj • 0x648:$xo1: \x175 366;uotj • 0x6c0:$xo1: \x175 366;uotj • 0x738:$xo1: \x175 366;uotj • 0x7b0:$xo1: \x175 366;uotj • 0x830:$xo1: \x19;.=885{azd • 0x8a0:$xo1: \x19;.=885{azd • 0x908:$xo1: \x19;.=885{azd • 0x978:$xo1: \x19;.=885{azd • 0x9e8:$xo1: \x19;.=885{azd • 0xae8:$xo1: \x19;.=885{azd • 0xba0:$xo1: \x19;.=885{azd • 0xbe8:$xo1: \x19;.=885{azd • 0xc38:$xo1: \x19;.=885{azd • 0xc98:$xo1: \x19;.=885{azd • 0xce0:$xo1: \x19;.=885{azd • 0xd00:$xo1: \x19;.=885{azd • 0xd50:$xo1: \x19;.=885{azd • 0xd98:$xo1: \x19;.=885{azd • 0xdf8:$xo1: \x19;.=885{azd • 0xe68:$xo1: \x19;.=885{azd
5237.1.000000001a887bdc.00000000531557b5.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x139dc:$xo1: \x19;.=885{azd • 0x13a4c:$xo1: \x19;.=885{azd • 0x13ab0:$xo1: \x19;.=885{azd • 0x13b1c:$xo1: \x19;.=885{azd • 0x13b88:$xo1: \x19;.=885{azd • 0x13c7c:$xo1: \x19;.=885{azd • 0x13ce4:$xo1: \x19;.=885{azd • 0x13d54:$xo1: \x19;.=885{azd • 0x13dc4:$xo1: \x19;.=885{azd • 0x13e34:$xo1: \x19;.=885{azd • 0x13ea4:$xo1: \x19;.=885{azd • 0x13fc8:$xo1: \x175 366;uotj • 0x14038:$xo1: \x175 366;uotj • 0x140a8:$xo1: \x175 366;uotj • 0x14118:$xo1: \x175 366;uotj • 0x14188:$xo1: \x175 366;uotj • 0x14200:$xo1: \x19;.=885{azd • 0x14244:$xo1: \x19;.=885{azd • 0x14290:$xo1: \x19;.=885{azd • 0x142ec:$xo1: \x19;.=885{azd • 0x14334:$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

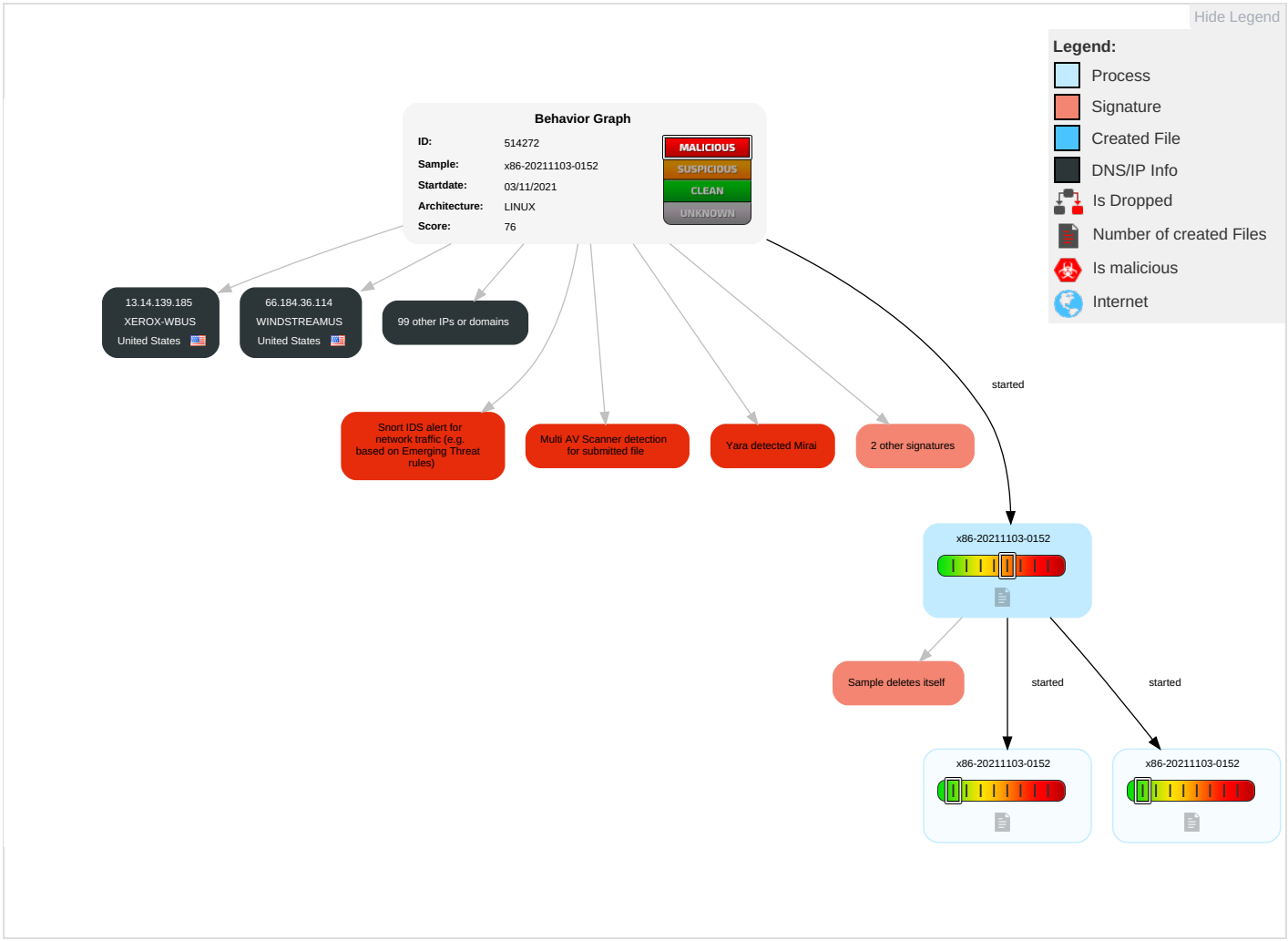
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	File Deletion 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

Copyright Joe Security LLC 2021

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
x86-20211103-0152	49%	Virustotal		Browse
x86-20211103-0152	55%	ReversingLabs	Linux.Trojan.Mirai	
x86-20211103-0152	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bots1.firewalla1337.cc	107.189.1.185	true	false		unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
117.67.217.242	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
142.228.46.212	unknown	Canada		13576	SDNW-13576US	false
70.91.49.232	unknown	United States		7922	COMCAST-7922US	false
45.153.14.15	unknown	Russian Federation		208221	ORIONNET-BRKRU	false
216.57.220.240	unknown	United States		6295	GREENHOUSE-WAUS	false
14.143.23.186	unknown	India		4755	TATACOMM-ASTATACommunicationsformerlyVSNLisLeadingISP	false
148.180.55.76	unknown	United States		6400	CompaniaDominicanadeTelefonosSADO	false
222.202.165.80	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
198.40.41.36	unknown	United States		26854	NYSUS	false
79.213.16.154	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
118.98.129.75	unknown	Indonesia		17974	TELKOMNET-AS2-APPTTelekomunikasiIndonesiaID	false
145.153.116.158	unknown	Netherlands		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
53.225.188.124	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
91.143.209.253	unknown	Serbia		31042	SERBIA-BROADBAND-ASSerbiaBroadBand-SrpskeKablovskemreze	false
70.201.63.234	unknown	United States		22394	CELLCOUS	false
27.215.103.174	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
88.41.34.31	unknown	Italy		3269	ASN-IBSNAZIT	false
134.11.167.68	unknown	United States		6041	DNIC-ASBLK-05800-06055US	false
129.3.48.62	unknown	United States		14433	SUNY-OSWEGO-ASNUS	false
213.241.87.171	unknown	Poland		12741	AS-NETIAWarszawa02-822PL	false
92.193.186.68	unknown	Germany		20676	PLUSNETDE	false
203.169.176.73	unknown	Hong Kong		9293	HKNET-VIPNETNTTComAsiaLimitedHK	false
24.219.213.161	unknown	United States		8092	AMHUS	false
13.14.139.185	unknown	United States		22390	XEROX-WBUS	false
123.72.218.66	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
159.210.217.163	unknown	Italy		131090	CAT-IDC-4BYTENET-AS-APCATTELECOMPublicCompanyLtdCATT	false
98.235.18.108	unknown	United States		7922	COMCAST-7922US	false
53.246.64.7	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false

Copyright Joe Security LLC 2021

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
118.117.187.154	unknown	China		139220	CHINANET-SICHUAN-CHUANXI-IDCSichuanChuanxnIDCCN	false
97.158.142.172	unknown	United States		6167	CELLCO-PARTUS	false
2.170.128.67	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
208.43.199.95	unknown	United States		36351	SOFTLAYERUS	false
92.184.7.55	unknown	France		12479	UNI2-ASES	false
41.240.157.122	unknown	Sudan		36998	SDN-MOBITELSD	false
135.72.175.235	unknown	United States		18676	AVAYAUS	false
217.30.98.102	unknown	Malta		15892	MITTS-NETMT	false
132.232.151.150	unknown	China		45090	CNNIC-TENCENT-NET-APShenzhenTencentComputerSystemsCompa	false
184.172.25.16	unknown	United States		36351	SOFTLAYERUS	false
114.73.237.81	unknown	Australia		4804	MPX-ASMicroplexPTYLTDAU	false
189.206.1.71	unknown	Mexico		11172	AlestraSdeRLdeCVMX	false
116.13.183.182	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
97.163.91.171	unknown	United States		6167	CELLCO-PARTUS	false
182.102.227.102	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
124.108.152.70	unknown	Taiwan; Republic of China (ROC)		9924	TFN-TWTaiwanFixedNetworkTelcoandNetworkServiceProvi	false
47.104.53.185	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
195.107.90.248	unknown	United Kingdom		8437	UTA-ASAT	false
167.109.220.135	unknown	United States		6057	AdministracionNacionaldeTelecomunicacionesUY	false
126.71.91.43	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
5.234.190.62	unknown	Iran (ISLAMIC Republic Of)		58224	TCIIR	false
184.50.149.116	unknown	United States		16625	AKAMAI-ASUS	false
78.218.37.115	unknown	France		12322	PROXADFR	false
113.131.9.25	unknown	Korea Republic of		9697	CJHAEUNDAEGIJANG-AS-KRLGHelloVisionCorpKR	false
80.214.139.42	unknown	France		5410	BOUYGTEL-ISPFR	false
170.206.48.0	unknown	United States		11685	HNBCOL-ASUS	false
148.157.94.104	unknown	United States		18715	NYPAUS	false
122.157.183.89	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
45.201.177.22	unknown	Seychelles		131178	KINGCORP-KHOpenNetISPCambodiaKH	false
200.238.68.126	unknown	Brazil		10938	AGENCIAESTADUALDETECNOLOGIADAINFORMACAO-ATIBR	false
134.88.115.76	unknown	United States		394003	UMASSDUS	false
65.37.3.125	unknown	United States		5650	FRONTIER-FRTRUS	false
212.167.164.209	unknown	European Union		51964	ORANGE-BUSINESS-SERVICES-IPSN-ASNFR	false
149.214.223.243	unknown	Germany		5605	NETUSEDE	false
91.29.31.39	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
93.75.8.89	unknown	Ukraine		25229	VOLIA-ASUA	false
174.100.158.2	unknown	United States		10796	TWC-10796-MIDWESTUS	false
27.206.89.52	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
54.39.101.232	unknown	Canada		16276	OVHFR	false
12.234.177.204	unknown	United States		7018	ATT-INTERNET4US	false
48.102.229.207	unknown	United States		2686	ATGS-MMD-ASUS	false
160.147.196.225	unknown	United States		1503	DNIC-AS-01503US	false
71.173.20.100	unknown	United States		701	UUNETUS	false
44.254.248.7	unknown	United States		16509	AMAZON-02US	false
97.60.167.5	unknown	United States		22394	CELLCOUS	false

Copyright Joe Security LLC 2021

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
18.97.63.27	unknown	United States		3	MIT-GATEWAYSUS	false
171.194.174.190	unknown	United States		10794	BANKAMERICAUS	false
50.192.53.93	unknown	United States		7922	COMCAST-7922US	false
203.157.28.66	unknown	Thailand		9649	MOPH-TH-APInformationTechnologyOfficeSG	false
144.182.0.226	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
221.177.195.70	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
17.123.177.174	unknown	United States		714	APPLE-ENGINEERINGUS	false
207.167.245.229	unknown	Canada		852	ASN852CA	false
13.157.7.65	unknown	United States		7018	ATT-INTERNET4US	false
137.90.157.222	unknown	United States		14977	STATE-OF-WYOMING-ASNUS	false
171.14.155.147	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
43.18.191.129	unknown	Japan		4249	LILLY-ASUS	false
66.184.36.114	unknown	United States		7029	WINDSTREAMUS	false
182.177.155.166	unknown	Pakistan		45595	PKTELECOM-AS-PKPakistanTelecomCompanyLimitedPK	false
14.3.193.10	unknown	Japan		4685	ASAHI-NETAsahiNetJP	false
203.87.148.54	unknown	Philippines		10139	SMARTBRO-PH-APSmartBroadbandIncPH	false
106.61.187.105	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
174.207.156.1	unknown	United States		22394	CELLCOUS	false
156.253.18.34	unknown	Seychelles		137443	ANCHGLOBAL-AS-APAnchnetAsiaLimitedHK	false
138.20.119.49	unknown	United States		11078	BROWNUS	false
60.207.58.5	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
97.61.226.167	unknown	United States		22394	CELLCOUS	false
14.104.194.177	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
60.215.203.221	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
84.81.162.155	unknown	Netherlands		1136	KPNKPNNationalEU	false
158.88.179.153	unknown	United States		20379	NET-BAKERUS	false
116.61.37.183	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false

Runtime Messages

Command:	/tmp/x86-20211103-0152
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	InfectedNight did its job
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
213.241.87.171	7bkrFirKok	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
bots1.firewalla1337.cc	mips-20211103-0152	Get hash	malicious	Browse	• 107.189.1.185
	mipsel	Get hash	malicious	Browse	• 107.189.1.185
	arm	Get hash	malicious	Browse	• 107.189.1.185
	arm7-20211101-1513	Get hash	malicious	Browse	• 107.189.1.185
	mips	Get hash	malicious	Browse	• 107.189.1.185
	Z7QqCH0bak	Get hash	malicious	Browse	• 107.189.1.185
	x86_64	Get hash	malicious	Browse	• 107.189.1.185
	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
	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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SDNW-13576US	sora.x86	Get hash	malicious	Browse	• 142.130.161.15
	Ko84iLip1u	Get hash	malicious	Browse	• 142.212.51.44
	Yoshi.arm	Get hash	malicious	Browse	• 142.200.80.38
	hvYTLlrdRm	Get hash	malicious	Browse	• 142.209.12 2.156
	MPnFvIsvJp	Get hash	malicious	Browse	• 142.212.99.59
	cosvgegE1S	Get hash	malicious	Browse	• 142.130.66.50
	mkRkjGXjDJ	Get hash	malicious	Browse	• 142.10.164.48
	eBQ4XSarFt	Get hash	malicious	Browse	• 142.211.174.27
	BXQb7BRQx7	Get hash	malicious	Browse	• 142.16.131.111
	9aAl5Mt3Jz	Get hash	malicious	Browse	• 142.210.58.123
	QqhaOHWtCU	Get hash	malicious	Browse	• 142.200.79.60
	b3astmode.x86	Get hash	malicious	Browse	• 142.193.243.68
	b3astmode.arm7	Get hash	malicious	Browse	• 142.220.188.39
	KKveTTgaAAsecNNaaaa.x86	Get hash	malicious	Browse	• 142.16.112.47
	KKveTTgaAAsecNNaaaa.arm7	Get hash	malicious	Browse	• 142.212.75.71
	RkH17dHLZt	Get hash	malicious	Browse	• 142.209.69.126
	b3astmode.arm7	Get hash	malicious	Browse	• 142.220.188.50
	z0x3n.x86	Get hash	malicious	Browse	• 66.115.210.166
	b3astmode.arm7-20211011-1850	Get hash	malicious	Browse	• 142.16.178.153
	mips-20211007-1618	Get hash	malicious	Browse	• 142.211.37.187
CHINANET-BACKBONENo31Jin-rongStreetCN	mips-20211103-0152	Get hash	malicious	Browse	• 111.228.229.65
	sora.arm	Get hash	malicious	Browse	• 115.216.10 4.211
	sora.x86	Get hash	malicious	Browse	• 171.209.7.158
	sora.x86	Get hash	malicious	Browse	• 106.6.100.225
	sora.arm	Get hash	malicious	Browse	• 183.4.32.19
	sora.arm7	Get hash	malicious	Browse	• 1.195.66.22
	sora.arm7	Get hash	malicious	Browse	• 115.231.119.54
	sora.x86	Get hash	malicious	Browse	• 220.183.55.54
	sora.arm	Get hash	malicious	Browse	• 183.4.31.124
	RlP4DUwOBH	Get hash	malicious	Browse	• 61.144.58.240
	sora.x86	Get hash	malicious	Browse	• 121.207.26.16
	sora.arm7	Get hash	malicious	Browse	• 125.81.144.7
	WmEErPtdS9	Get hash	malicious	Browse	• 120.38.227.156

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	3Htna329pC	Get hash	malicious	Browse	• 125.113.173.182
	uTGiKHSeyv	Get hash	malicious	Browse	• 110.86.51.222
	sora.x86	Get hash	malicious	Browse	• 110.167.231.74
	sora.arm7	Get hash	malicious	Browse	• 106.63.74.131
	sora.arm	Get hash	malicious	Browse	• 222.185.3.25
	6A9RyJXCd7	Get hash	malicious	Browse	• 117.89.157.112
	mipsel	Get hash	malicious	Browse	• 171.43.62.146

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):	6.426601263779105
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	x86-20211103-0152
File size:	86800
MD5:	48bfe55d7795f2d6905c6cdbea372b9b
SHA1:	760d6b9c2779c3bb8f5eb2c8e1b95824fb8277dc
SHA256:	fa1be914982a111f999fee0ed612d94ba9d0792257ee54c41acba3c2126e35ab
SHA512:	dbf026fc8e0079a91b0829d67596b4d705e7e67ee2956a4b91a29440634c626e182f198366d9c9b4d5d93a42dcf4fb1bd25ff8aa605dfd759fbb09e29ba5dc
SSDEEP:	1536:hNw7TjznqVg1WeAvqwjP1Zr7uuInqYtHsnYkf01hwkq/rnVzWX9yX/miwwEH:fw7vzdrAvhjP1Zr7/InqYtHsnw16kErK
File Content Preview:	.ELF.....d...4....Q.....4. ...(.....I...I.....P.....@.....Q.td.....U..S.....wO...h.....,..[]...$.....U.....=@....t..5....$.....$.....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

Copyright Joe Security LLC 2021

ELF header

Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	86400
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

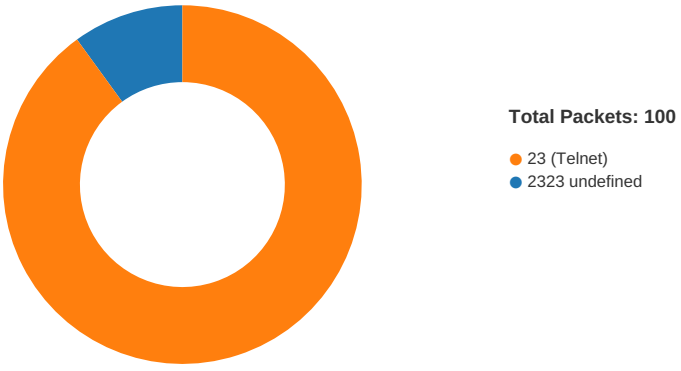
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x8048094	0x94	0x1c	0x0	0x6	AX	0	0	1
.text	PROGBITS	0x80480b0	0xb0	0x12d06	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x805adb6	0x12db6	0x17	0x0	0x6	AX	0	0	1
.rodata	PROGBITS	0x805ade0	0x12de0	0x1ba0	0x0	0x2	A	0	0	32
.ctors	PROGBITS	0x805d000	0x15000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x805d008	0x15008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x805d020	0x15020	0x120	0x0	0x3	WA	0	0	32
.bss	NOBITS	0x805d140	0x15140	0x840	0x0	0x3	WA	0	0	32
.shstrtab	STRTAB	0x0	0x15140	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	0x14980	0x14980	3.9068	0x5	R E	0x1000		.init .text .fini .rodata
LOAD	0x15000	0x805d000	0x805d000	0x140	0x980	2.4783	0x6	RW	0x1000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 3, 2021 03:27:07.472503901 CET	192.168.2.23	1.1.1.1	0xf9bb	Standard query (0)	bots1.firewalla1337.cc	A (IP address)	IN (0x0001)

DNS Answers

Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 3, 2021 03:27:07.490596056 CET	1.1.1.1	192.168.2.23	0xf9bb	No error (0)	bots1.firewalla1337.cc		107.189.1.185	A (IP address)	IN (0x0001)

System Behavior

Analysis Process: x86-20211103-0152 PID: 5237 Parent PID: 5113

General

Start time:	03:27:06
Start date:	03/11/2021
Path:	/tmp/x86-20211103-0152
Arguments:	/tmp/x86-20211103-0152
File size:	86800 bytes
MD5 hash:	48bfe55d7795f2d6905c6cdbea372b9b

File Activities

File Deleted

Analysis Process: x86-20211103-0152 PID: 5238 Parent PID: 5237

General

Start time:	03:27:06
Start date:	03/11/2021
Path:	/tmp/x86-20211103-0152
Arguments:	n/a
File size:	86800 bytes
MD5 hash:	48bfe55d7795f2d6905c6cdbea372b9b

Analysis Process: x86-20211103-0152 PID: 5239 Parent PID: 5237

General

Start time:	03:27:06
Start date:	03/11/2021
Path:	/tmp/x86-20211103-0152
Arguments:	n/a
File size:	86800 bytes
MD5 hash:	48bfe55d7795f2d6905c6cdbea372b9b

Copyright Joe Security LLC 2021