ID: 1537583
Sample Name: la.bot.sparc.elf
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 08:26:33
Date: 19/10/2024
Version: 41.0.0 Charoite

Table of Contents

Linux Analysis Report

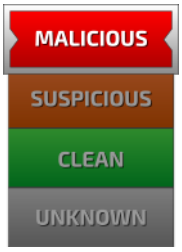
la.bot.sparc.elf

Overview

General Information

Sample name:	la.bot.sparc.elf
Analysis ID:	1537583
MD5:	ae156594e5ef9..
SHA1:	e6b3a0c03e3a…
SHA256:	822f3f8c5b1e8…
Tags:	elf user-abuse_ch
Infos:	

Detection

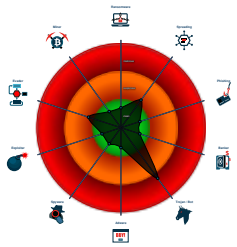


Score:	56
Range:	0 - 100
Whitelisted:	false

Signatures

- Multi AV Scanner detection for subm…
- Connects to many ports of the same…
- Sends malformed DNS queries
- Detected TCP or UDP traffic on non…
- Found strings indicative of a multi-p…
- Sample contains strings indicative o…
- Sample has stripped symbol table
- Sample listens on a socket
- Tries to connect to HTTP servers, b…
- Uses the "uname" system call to qu…

Classification



General Information

Joe Sandbox version:	41.0.0 Charoite
Analysis ID:	1537583
Start date and time:	2024-10-19 08:26:33 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 5m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
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
Sample name:	la.bot.sparc.elf
Detection:	MAL
Classification:	mal56.troj.linELF@0/0@10/0

Warnings

Runtime Messages

Command:	/tmp/la.bot.sparc.elf
PID:	6205
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	thIs wEek on xLaB lEarNs nOthinG xd
Standard Error:	

Process Tree

- **system is lnxubuntu20**
- la.bot.sparc.elf (PID: 6205, Parent: 6126, MD5: 7dc1c0e23cd5e102bb12e5c29403410e) Arguments: /tmp/la.bot.sparc.elf
  - la.bot.sparc.elf New Fork (PID: 6207, Parent: 6205)
  - la.bot.sparc.elf New Fork (PID: 6236, Parent: 6205)
    - la.bot.sparc.elf New Fork (PID: 6239, Parent: 6236)
- **cleanup**

Yara Signatures

No yara matches

Suricata Signatures

No Suricata rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Networking

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

Sends malformed DNS queries

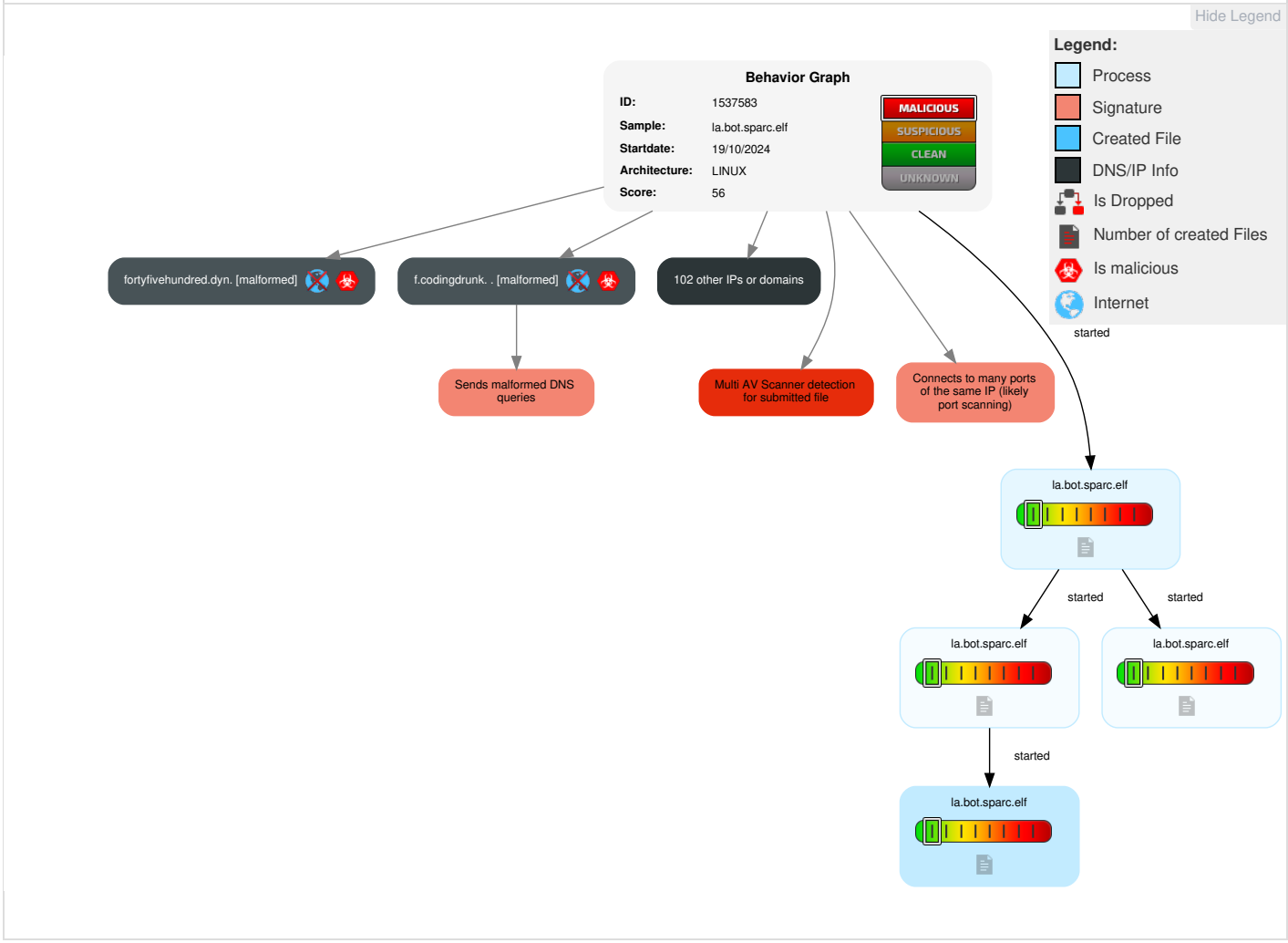
Mitre Att&ck Matrix

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	1 Scripting	Valid Accounts	Windows Management Instrumentation	1 Scripting	Path Interception	Direct Volume Access	OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	1 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	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	1 Non-Standard Port	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	1 Non-Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	Login Hook	Login Hook	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	2 Application Layer Protocol	Traffic Duplication	Data Destruction

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
la.bot.sparc.elf	34%	ReversingLabs	Linux.Backdoor.Miai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

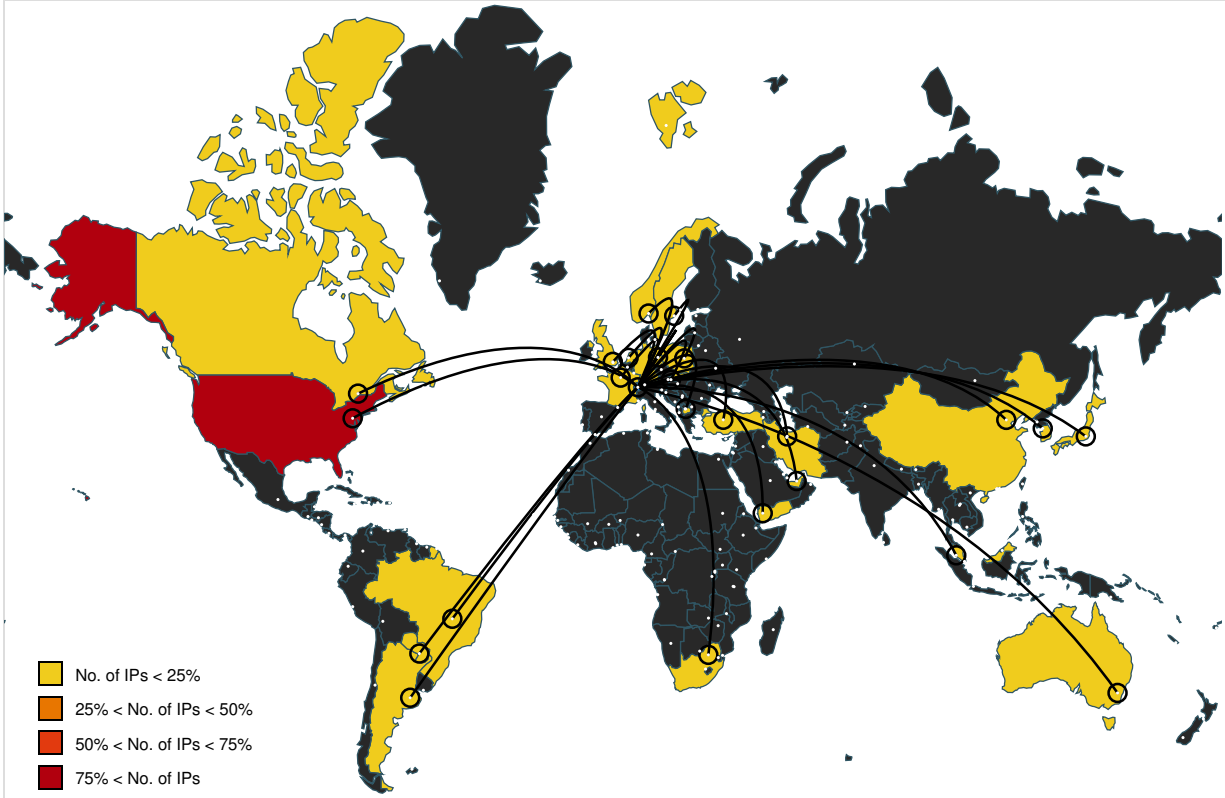
Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
21savage.dyn	156.244.19.135	true	false		unknown
eighteen.pirate. [malformed]	unknown	unknown	true		unknown
fortyfivehundred.dyn. [malformed]	unknown	unknown	true		unknown
f.codingdrunk. . [malformed]	unknown	unknown	true		unknown

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
211.168.94.59	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
42.80.179.1	unknown	China		17638	CHINATELECOM-TJ-AS-APASNforTIANJINProvincialNetofCT	false
216.61.140.14	unknown	United States		7018	ATT-INTERNET4US	false
32.38.104.224	unknown	United States		2686	ATGS-MMD-ASUS	false
153.103.159.78	unknown	United States		1519	DNIC-AS-01519US	false
40.154.161.227	unknown	United States		4249	LILLY-ASUS	false
93.3.135.121	unknown	France		15557	LDCOMNETFR	false
97.175.248.242	unknown	United States		6167	CELLCO-PARTUS	false
190.19.60.246	unknown	Argentina		10318	TelecomArgentinaSAAR	false
67.75.143.134	unknown	United States		3549	LVLT-3549US	false
38.182.55.169	unknown	United States		174	COGENT-174US	false
195.143.26.185	unknown	United Kingdom		8928	INTEROUTE25CanadaSquareCanaryWharf31stFloorGB	false
122.252.150.28	unknown	Australia		17918	AC3-AS-APac3AustralianCentreforAdvancedComputingand	false
205.95.149.25	unknown	United States		647	DNIC-ASBLK-00616-00665US	false
172.64.209.7	unknown	United States		13335	CLOUDFLARENETUS	false
67.97.52.106	unknown	United States		6977	IAC-ASUS	false
179.105.195.253	unknown	Brazil		28573	CLAROSABR	false
43.72.210.0	unknown	Japan		4249	LILLY-ASUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
202.187.175.215	unknown	Malaysia		9930	TTNET-MYTIMEdotComBerhadMY	false
4.17.92.81	unknown	United States		3356	LEVEL3US	false
185.102.172.167	unknown	Netherlands		7922	COMCAST-7922US	false
137.40.151.154	unknown	Japan		721	DNIC-ASBLK-00721-00726US	false
182.40.122.50	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
97.0.183.61	unknown	United States		22394	CELLCOUS	false
177.172.239.110	unknown	Brazil		26599	TELEFONICABRASILSABR	false
202.240.57.130	unknown	Japan		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
60.68.83.129	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
123.7.103.195	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
91.72.131.151	unknown	United Arab Emirates		15802	DU-AS1AE	false
22.204.37.88	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
6.69.199.126	unknown	United States		1479	DNIC-ASBLK-01478-01479US	false
46.217.99.42	unknown	Macedonia		6821	MT-AS-OWNbulOrceNikolovbbMK	false
1.253.60.24	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
67.19.213.165	unknown	United States		36351	SOFTLAYERUS	false
65.90.47.122	unknown	United States		3356	LEVEL3US	false
44.221.119.232	unknown	United States		14618	AMAZON-AESUS	false
90.133.141.31	unknown	Sweden		39651	COMHEM-SWEDENSE	false
179.129.143.179	unknown	Brazil		26599	TELEFONICABRASILSABR	false
197.211.66.58	unknown	South Africa		29918	IMPOL-ASNZA	false
162.212.106.109	unknown	United States		46887	LIGHTOWERUS	false
108.60.223.136	unknown	United States		13354	ZC38-AS1US	false
85.218.82.228	unknown	Switzerland		34781	SIL-CITYCABLE-ASCH	false
77.7.8.13	unknown	Germany		6805	TDDE-ASN1DE	false
163.71.42.69	unknown	France		17816	CHINA169-GZChinaUnicomIPnetworkChina169Guangdongprovi	false
46.81.62.28	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
28.171.133.129	unknown	United States		7922	COMCAST-7922US	false
48.134.243.4	unknown	United States		2686	ATGS-MMD-ASUS	false
18.122.71.167	unknown	United States		3	MIT-GATEWAYSUS	false
102.234.29.246	unknown	unknown		36926	CKL1-ASNKE	false
190.112.213.122	unknown	Paraguay		263228	PLANETSAPY	false
133.34.181.229	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
162.66.100.20	unknown	United States		35893	ACPCA	false
150.167.212.135	unknown	United States		2572	MORENETUS	false
103.170.35.86	unknown	unknown		7575	AARNET-AS-APAustralianAcademicandResearchNetworkAARNe	false
95.217.66.145	unknown	Germany		24940	HETZNER-ASDE	false
196.9.233.51	unknown	South Africa		21491	UGANDA-TELECOMUgandaTelecomUG	false
45.93.168.244	unknown	Iran (ISLAMIC Republic Of)		57497	FARASOSAMANEHPASARGADIR	false
147.107.249.251	unknown	United States		19096	DESALES-NETWORKUS	false
178.105.99.77	unknown	United Kingdom		12576	EELtdGB	false
131.183.22.32	unknown	United States		2025	UTOLEDOUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
51.213.29.139	unknown	United States		2686	ATGS-MMD-ASUS	false
46.169.96.219	unknown	Poland		8374	PLUSNETPlusnetworkoperatorinPolandPL	false
56.170.248.182	unknown	United States		2686	ATGS-MMD-ASUS	false
192.204.218.202	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
84.209.102.235	unknown	Norway		41164	GET-NOGETNorwayNO	false
133.245.237.28	unknown	Japan		2497	IIJInternetInitiativeJapanIncJP	false
166.91.30.33	unknown	United States		33084	DC-NETUS	false
49.73.162.56	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
140.7.152.235	unknown	United States		668	DNIC-AS-00668US	false
25.61.184.25	unknown	United Kingdom		7922	COMCAST-7922US	false
200.103.220.3	unknown	Brazil		8167	BrasilTelecomSA-FilialDistritoFederalBR	false
195.94.17.148	unknown	Yemen		12486	TELEYEMENSanaaYE	false
200.175.108.154	unknown	Brazil		18881	TELEFONICABRASILSABR	false
199.175.181.111	unknown	Canada		852	ASN852CA	false
5.11.138.251	unknown	Turkey		16135	TURKCELL-ASTurkcellASTR	false
68.15.246.60	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
174.15.56.77	unknown	United States		6327	SHAWCA	false
86.21.69.110	unknown	United Kingdom		5089	NTLGB	false
133.3.69.48	unknown	Japan		2504	NCA5KyotoUniversityJP	false
68.12.58.210	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
143.0.200.132	unknown	Brazil		264001	GENESYSNETPROVEDORDEINTERNETLTDAMEBR	false
206.26.161.121	unknown	United States		3561	CENTURYLINK-LEGACY-SAVVISUS	false
194.16.168.72	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
53.50.228.118	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
39.106.194.223	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
191.219.7.134	unknown	Brazil		8167	BrasilTelecomSA-FilialDistritoFederalBR	false
189.112.150.130	unknown	Brazil		16735	ALGARTELECOMSABR	false
193.48.240.31	unknown	France		2200	FR-RENATERReseauNationaldetelecommunicationspourlaTec	false
205.23.44.30	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
115.132.43.44	unknown	Malaysia		4788	TMNET-AS-APTMNetInternetServiceProviderMY	false
96.202.31.14	unknown	United States		7922	COMCAST-7922US	false
85.216.185.176	unknown	Slovakia (SLOVAK Republic)		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
104.108.196.84	unknown	United States		9498	BBIL-APBHARTIAirtelLtdIN	false
214.223.82.71	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
52.161.161.121	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
180.146.247.79	unknown	Japan		17511	OPTAGEOPTAGEIncJP	false
112.229.41.51	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
102.38.52.92	unknown	South Africa		328529	Zoom-NetworksZA	false
64.219.130.100	unknown	United States		7018	ATT-INTERNET4US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
202.120.138.175	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	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 MSB executable, SPARC, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	5.989494135928699
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	la.bot.sparc.elf
File size:	76'024 bytes
MD5:	ae156594e5ef91c243fcc1aeddd238fd
SHA1:	e6b3a0c03e3ab0f8e63148bf3f320ba589d76e22
SHA256:	822f3f8c5b1e8f1a1068783d5b888ac09eee82a2e657784ee47a672538787397
SHA512:	0834aae295ef1b05f3eb69413e504784ddc34524fdca750ba92c2a25b3447465c7a21a58458f95711726cb033262e02134c67ccc547b20c1fc1b6059366f179a
SSDEEP:	1536:748a06AW5bWGJZtRUQLQfzJTnu2dabHM/47nfOiUpdxl4HFsD0:FxTnu44nSd8HI
TLSH:	EA735A267A746D2BC8C8583E61B74776F1F5274A20E8C61F7E321F8EFB60540660B6B4
File Content Preview:	.ELF.....4..'h.....4. ...(.....$8..$8.....$<..$<..$<.....E.....dt.Q.....@..(....@.?.....#.....c(..`.....!..... T..@....."........`.....$ T..T..@.....`....

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)

ELF header	
Machine:	Sparc
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x101a4
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	75624
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

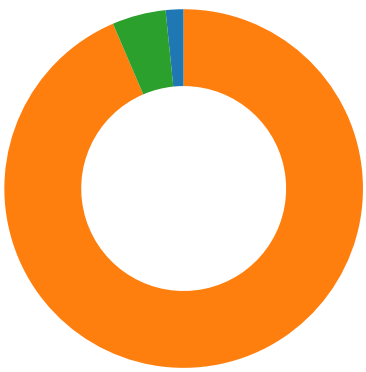
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x10094	0x94	0x1c	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x100b0	0xb0	0xff3c	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x1ffec	0xffec	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x20000	0x10000	0x2438	0x0	0x2	A	0	0	8
.ctors	PROGBITS	0x3243c	0x1243c	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x32444	0x12444	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x32450	0x12450	0x2d8	0x0	0x3	WA	0	0	8
.bss	NOBITS	0x32728	0x12728	0x42a8	0x0	0x3	WA	0	0	8
.shstrtab	STRTAB	0x0	0x12728	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	0x10000	0x10000	0x12438	0x12438	6.0114	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x1243c	0x3243c	0x3243c	0x2ec	0x4594	3.6236	0x6	RW	0x10000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



Total Packets: 62

- 15987 undefined
- 23 (Telnet)
- 443 (HTTPS)

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 19, 2024 08:27:18.770081043 CEST	192.168.2.23	162.243.19.47	0x4c57	Standard query (0)	21savage.dyn	A (IP address)	IN (0x0001)	false
Oct 19, 2024 08:27:29.623320103 CEST	192.168.2.23	130.61.69.123	0x4193	Standard query (0)	eighteen.pirate. [malformed]	256	337	false
Oct 19, 2024 08:27:29.631484032 CEST	192.168.2.23	185.84.81.194	0xc1e5	Standard query (0)	eighteen.pirate. [malformed]	256	337	false
Oct 19, 2024 08:27:29.643656969 CEST	192.168.2.23	130.61.64.122	0x8f2d	Standard query (0)	eighteen.pirate. [malformed]	256	337	false
Oct 19, 2024 08:27:29.651369095 CEST	192.168.2.23	192.3.165.37	0xe566	Standard query (0)	fortyfiveh undred.dyn. [malformed]	256	337	false
Oct 19, 2024 08:27:29.752980947 CEST	192.168.2.23	8.8.8.8	0x45d6	Standard query (0)	f.codingdrunk. . [malformed]	256	337	false
Oct 19, 2024 08:27:29.762204885 CEST	192.168.2.23	8.8.8.8	0x45d6	Standard query (0)	f.codingdrunk. . [malformed]	256	337	false
Oct 19, 2024 08:27:29.770576954 CEST	192.168.2.23	8.8.8.8	0x45d6	Standard query (0)	f.codingdrunk. . [malformed]	256	337	false
Oct 19, 2024 08:27:29.777770042 CEST	192.168.2.23	8.8.8.8	0x45d6	Standard query (0)	f.codingdrunk. . [malformed]	256	337	false
Oct 19, 2024 08:27:29.784892082 CEST	192.168.2.23	8.8.8.8	0x45d6	Standard query (0)	f.codingdrunk. . [malformed]	256	337	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 19, 2024 08:27:18.865411043 CEST	162.243.19.47	192.168.2.23	0x4c57	No error (0)	21savage.dyn		156.244.19.135	A (IP address)	IN (0x0001)	false
Oct 19, 2024 08:27:18.865411043 CEST	162.243.19.47	192.168.2.23	0x4c57	No error (0)	21savage.dyn		103.253.147.242	A (IP address)	IN (0x0001)	false

System Behavior

Analysis Process: la.bot.sparc.elf PID: **6205**, Parent PID: **6126**

General

Start time (UTC):	06:27:18
Start date (UTC):	19/10/2024
Path:	/tmp/la.bot.sparc.elf
Arguments:	/tmp/la.bot.sparc.elf
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

File Activities

- File Read
- File Moved
- Directory Enumerated

Analysis Process: la.bot.sparc.elf PID: **6207**, Parent PID: **6205**

General

Start time (UTC):	06:27:18
Start date (UTC):	19/10/2024
Path:	/tmp/la.bot.sparc.elf
Arguments:	-

File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

File Activities

Directory Enumerated

Analysis Process: la.bot.sparc.elf PID: **6236**, Parent PID: **6205**

General

Start time (UTC):	06:27:18
Start date (UTC):	19/10/2024
Path:	/tmp/la.bot.sparc.elf
Arguments:	-
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: la.bot.sparc.elf PID: **6239**, Parent PID: **6236**

General

Start time (UTC):	06:27:18
Start date (UTC):	19/10/2024
Path:	/tmp/la.bot.sparc.elf
Arguments:	-
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e