ID: 1575489
Sample Name: bot.m68k.elf
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 19:32:45
Date: 15/12/2024
Version: 41.0.0 Charoite

Table of Contents

Linux Analysis Report

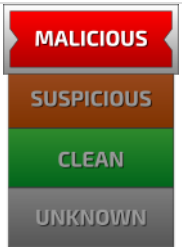
bot.m68k.elf

Overview

General Information

Sample name:	bot.m68k.elf
Analysis ID:	1575489
MD5:	7193e673ff416…
SHA1:	b965c035e807…
SHA256:	7bd3e39acf671…
Tags:	elf user-abuse_ch
Infos:	

Detection



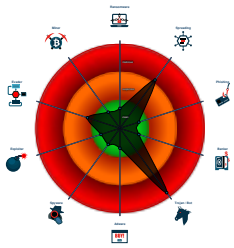
Mirai

Score:	100
Range:	0 - 100
Whitelisted:	false

Signatures

- Antivirus / Scanner detection for sub…
- Detected Mirai
- Malicious sample detected (through…
- Multi AV Scanner detection for subm…
- Suricata IDS alerts for network traffic
- Yara detected Mirai
- Connects to many ports of the same…
- Sample tries to kill multiple process…
- Uses known network protocols on n…
- Detected TCP or UDP traffic on non…
- Enumerates processes within the "p…

Classification



General Information

Joe Sandbox version:	41.0.0 Charoite
Analysis ID:	1575489
Start date and time:	2024-12-15 19:32:45 +01:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 6m 41s
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:	bot.m68k.elf
Detection:	MAL
Classification:	mal100.spre.troj.linELF@0/0@2/0

Warnings

Runtime Messages

Command:	/tmp/bot.m68k.elf
PID:	5497
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Infected By Cult
Standard Error:	

Process Tree

- **system is lnxubuntu20**

- bot.m68k.elf (PID: 5497, Parent: 5415, MD5: cd177594338c77b895ae27c33f8f86cc) Arguments: /tmp/bot.m68k.elf
  - bot.m68k.elf New Fork (PID: 5499, Parent: 5497)
  - bot.m68k.elf New Fork (PID: 5500, Parent: 5497)
  - bot.m68k.elf New Fork (PID: 5503, Parent: 5497)
    - bot.m68k.elf New Fork (PID: 5505, Parent: 5503)
    - bot.m68k.elf New Fork (PID: 5510, Parent: 5503)
    - bot.m68k.elf New Fork (PID: 5512, Parent: 5503)
    - bot.m68k.elf New Fork (PID: 5514, Parent: 5503)
    - bot.m68k.elf New Fork (PID: 5517, Parent: 5503)
    - bot.m68k.elf New Fork (PID: 5519, Parent: 5503)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Mirai	Mirai is one of the first significant botnets targeting exposed networking devices running Linux. Found in August 2016 by MalwareMustDie, its name means "future" in Japanese. Nowadays it targets a wide range of networked embedded devices such as IP cameras, home routers (many vendors involved), and other IoT devices. Since the source code was published on "Hack Forums" many variants of the Mirai family appeared, infecting mostly home networks all around the world.	No Attribution	http://osint.bambenekconsulting.com/feeds/http://www.simonroses.com/2016/10/mirai-ddos-botnet-source-code-binary-analysis/https://blog.malwaremustdie.org/2020/02/mmd-0065-2021-linuxmirai-fbot-re.htmlhttps://blog.netlab.360.com/another-lilin-dvr-0-day-being-used-to-spread-mirai-en/https://blog.netlab.360.com/mirai_ptea-botnet-is-exploiting-undisclosed-kguard-dvr-vulnerability-en/	http://https://malpedia.caad.fkie.fraunhofer.de/details/elf.mirai

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
bot.m68k.elf	JoeSecurity_Mirai_6	Yara detected Mirai	Joe Security	
bot.m68k.elf	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
bot.m68k.elf	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0xff5c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xff70:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xff84:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xff98:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xffac:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xffc0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xffd4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xffe8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xfffc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x10010:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x10024:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x10038:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x1004c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x10060:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x10074:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x10088:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x1009c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x100b0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x100c4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x100d8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x100ec:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
bot.m68k.elf	Linux_Trojan_Gafgyt_ea92cca8	unknown	unknown	• 0x104ad:$a: 53 65 6C 66 20 52 65 70 20 46 75 63 6B 69 6E 67 20 4E 65 54 69 53 20 61 6E 64

Memory Dumps

Source	Rule	Description	Author	Strings
5512.1.00007f3644001000.00007f3644013000.r-x.sdmp	JoeSecurity_Mirai_6	Yara detected Mirai	Joe Security	
5512.1.00007f3644001000.00007f3644013000.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

Source	Rule	Description	Author	Strings
5512.1.00007f3644001000.00007f3644013000.r-x.sdmp	Linux_Trojan_Gafgyt_28a2fe0c	unknown	unknown	• 0xff5c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xff70:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xff84:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xff98:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xffac:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xffc0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xffd4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xffe8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0xfffc:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x10010:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x10024:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x10038:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x1004c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x10060:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x10074:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x10088:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x1009c:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x100b0:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x100c4:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x100d8:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F • 0x100ec:$a: 2F 78 33 38 2F 78 46 4A 2F 78 39 33 2F 78 49 44 2F 78 39 41 2F 78 33 38 2F 78 46 4A 2F
5512.1.00007f3644001000.00007f3644013000.r-x.sdmp	Linux_Trojan_Gafgyt_ea92cca8	unknown	unknown	• 0x104ad:$a: 53 65 6C 66 20 52 65 70 20 46 75 63 6B 69 6E 67 20 4E 65 54 69 53 20 61 6E 64
5517.1.00007f3644001000.00007f3644013000.r-x.sdmp	JoeSecurity_Mirai_6	Yara detected Mirai	Joe Security	
Click to see the 44 entries				

Suricata Signatures

ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-15T19:33:43.940354+0100	2835222	1	A Network Trojan was detected	192.168.2.14	38910	197.92.216.123	37215	TCP
2024-12-15T19:33:45.061182+0100	2835222	1	A Network Trojan was detected	192.168.2.14	39760	157.15.140.45	37215	TCP
2024-12-15T19:33:49.505977+0100	2835222	1	A Network Trojan was detected	192.168.2.14	43954	197.5.116.175	37215	TCP

ETPRO MALWARE ELF/Mirai User-Agent Observed (Outbound)

Timestamp	SID	Severity	Classtype	Source IP	Source Port	Destination IP	Destination Port	Protocol
2024-12-15T19:33:45.800709+0100	2841377	1	Attempted Administrator Privilege Gain	192.168.2.14	51384	95.234.5.99	80	TCP
2024-12-15T19:33:46.873102+0100	2841377	1	Attempted Administrator Privilege Gain	192.168.2.14	60390	112.178.50.2	80	TCP

Joe Sandbox Signatures

AV Detection

- Antivirus / Scanner detection for submitted sample
- Multi AV Scanner detection for submitted file

Networking

- Suricata IDS alerts for network traffic
- Connects to many ports of the same IP (likely port scanning)
- Uses known network protocols on non-standard ports

System Summary

- Malicious sample detected (through community Yara rule)
- Sample tries to kill multiple processes (SIGKILL)

Hooking and other Techniques for Hiding and Protection

- Uses known network protocols on non-standard ports

Stealing of Sensitive Information

- Yara detected Mirai

Remote Access Functionality

- Detected Mirai
- Yara detected Mirai

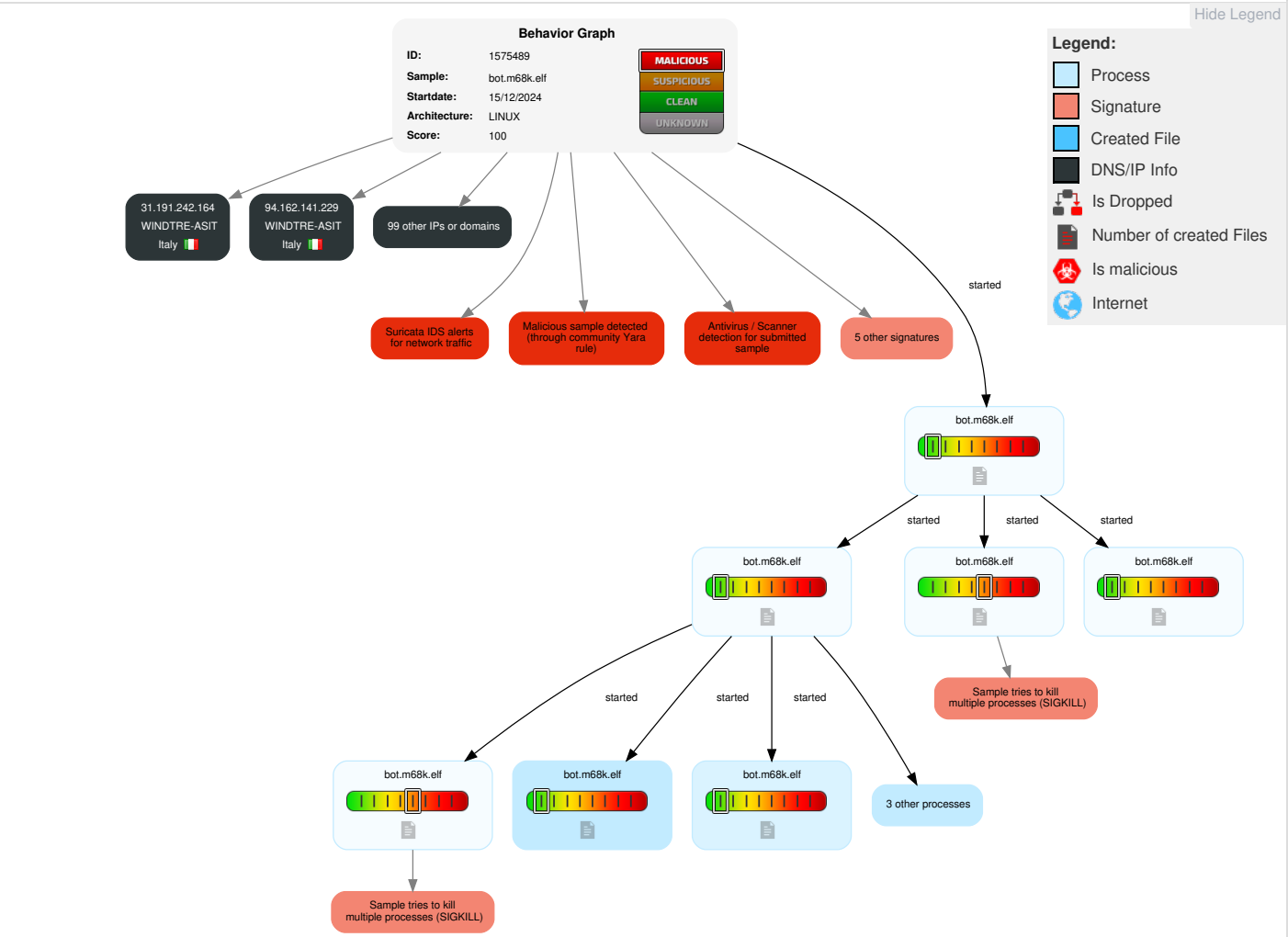
Mitre Att&ck Matrix

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	Acquire Infrastructure	Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Direct Volume Access	1 OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	1 Encrypted Channel	Exfiltration Over Other Network Medium	1 Service Stop
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 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	3 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	4 Application Layer Protocol	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Internet Connection Discovery	SSH	Keylogging	1 Ingress Tool Transfer	Scheduled Transfer	Data Encrypted for Impact

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
bot.m68k.elf	66%	ReversingLabs	Linux.Backdoor.Mirai	
bot.m68k.elf	100%	Avira	EXP/ELF.Mirai.Botnet.o	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://152.42.234.215/bns/x86	0%	Avira URL Cloud	safe	
http://152.42.234.215/zyxel.sh;	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

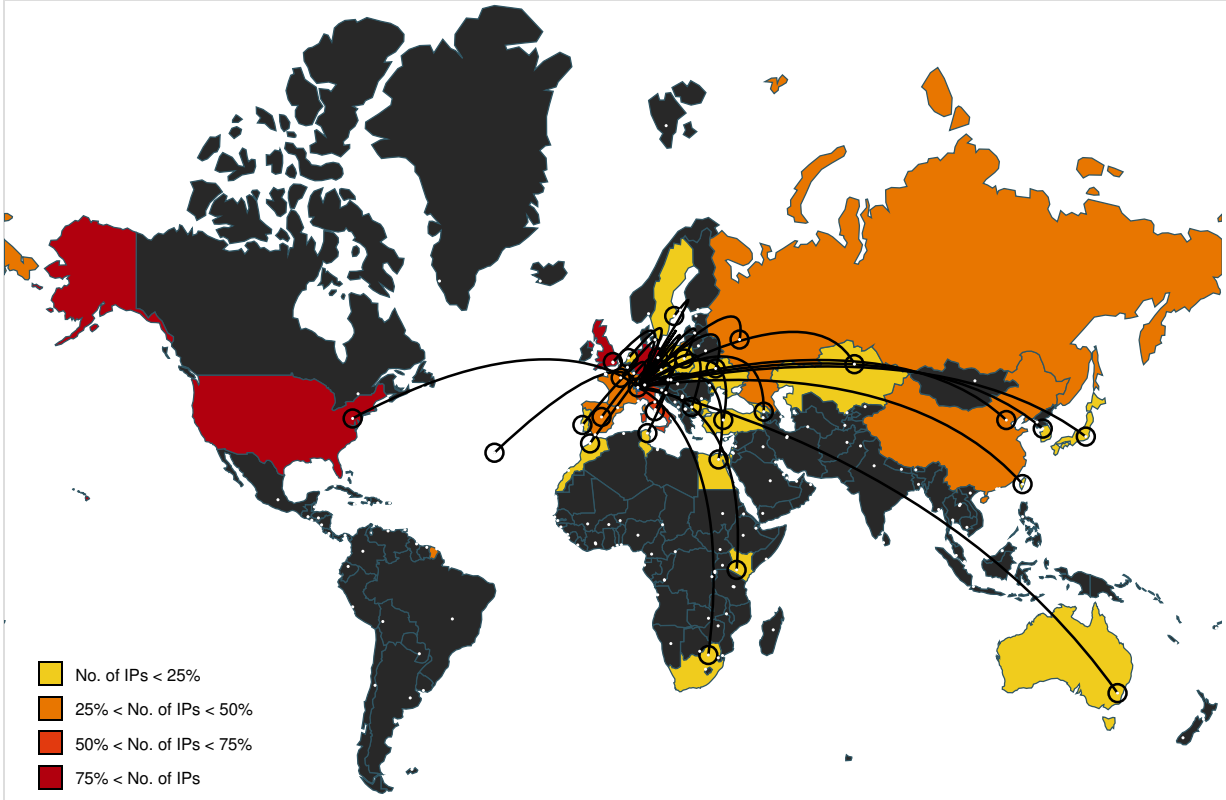
Name	IP	Active	Malicious	Antivirus Detection	Reputation
daisy.ubuntu.com	162.213.35.25	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://192.168.0.14:80/cgi-bin/ViewLog.asp	false		high

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
112.11.173.213	unknown	China		56041	CMNET-ZHEJIANG-APChinaMobilecommunicationscorporationC	false
122.47.48.252	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
94.178.33.185	unknown	Ukraine		6849	UKRTELNETUA	false
216.137.217.141	unknown	United States		11090	MTAONLINE-ASUS	false
112.160.76.180	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
82.210.46.21	unknown	France		34177	CELESTE-ASCELESTE-InternetservicesproviderFR	false
112.125.213.14	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
202.216.32.75	unknown	Japan		4704	SANNETRakutenMobileIncJP	false
94.232.145.11	unknown	Poland		39893	NETSYSTEM_TP-ASNPL	false
62.213.110.14	unknown	Russian Federation		25227	ASN-AVANTEL-MSKLocatedinMoscowRussiaRU	false
31.210.249.112	unknown	Sweden		35706	NAOSE	false
41.165.218.84	unknown	South Africa		36937	Neotel-ASZA	false
62.53.240.219	unknown	Germany		6805	TDDE-ASN1DE	false
31.191.242.164	unknown	Italy		24608	WINDTRE-ASIT	false
62.224.49.12	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
31.86.186.163	unknown	United Kingdom		12576	EELtdGB	false
95.225.107.101	unknown	Italy		3269	ASN-IBSNAZIT	false
48.43.93.222	unknown	United States		2686	ATGS-MMD-ASUS	false
85.2.39.204	unknown	Switzerland		3303	SWISSCOMSwisscomSwitzerlandLtdCH	false
98.236.235.248	unknown	United States		7922	COMCAST-7922US	false
62.219.245.6	unknown	Israel		8551	BEZEQ-INTERNATIONAL-ASBezeqintInternetBackboneIL	false
41.143.104.40	unknown	Morocco		36903	MT-MPLSMA	false
31.186.168.36	unknown	Netherlands		60781	LEASEWEB-NL-AMS-01NetherlandsNL	false
62.132.39.137	unknown	Germany		286	KPNNL	false
149.225.203.5	unknown	Germany		702	UUNETUS	false
130.29.222.114	unknown	United States		367	DNIC-ASBLK-00306-00371US	false
13.213.91.161	unknown	United States		16509	AMAZON-02US	false
118.8.252.56	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
95.57.49.122	unknown	Kazakhstan		9198	KAZTELECOM-ASKZ	false
94.11.75.120	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
78.36.212.16	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
71.46.110.185	unknown	United States		33363	BHN-33363US	false
62.132.39.166	unknown	Germany		286	KPNNL	false
62.182.204.108	unknown	Russian Federation		44391	ESD-ASRU	false
62.96.134.109	unknown	United Kingdom		8220	COLTCOLTTechnologyServicesGroupLimitedGB	false
148.15.121.118	unknown	United States		394673	9408US	false
62.52.13.75	unknown	Germany		6805	TDDE-ASN1DE	false
95.109.203.209	unknown	Ukraine		34610	RIKSNETSE	false
94.193.8.115	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
42.206.177.67	unknown	China		7641	CHINABTNChinaBroadcastingTVNetCN	false
95.111.20.230	unknown	Bulgaria		35141	MEGALANBG	false
62.28.37.205	unknown	Portugal		15525	MEO-EMPRESASPT	false
85.2.39.227	unknown	Switzerland		3303	SWISSCOMSwisscomSwitzerlandLtdCH	false
31.121.27.3	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
107.42.122.118	unknown	United States		16567	NETRIX-16567US	false
221.223.2.42	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
88.189.183.18	unknown	France		12322	PROXADFR	false
95.14.46.196	unknown	Turkey		9121	TTNETTR	false
152.157.227.174	unknown	United States		10430	WA-K20US	false
85.114.235.174	unknown	Georgia		16010	MAGTICOMASCaucasus-OnlineGE	false
31.118.153.226	unknown	United Kingdom		12576	EELtdGB	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
211.78.171.116	unknown	Taiwan; Republic of China (ROC)		9919	NCIC-TWNewCenturyInfoCommTechCoLtdTW	false
95.215.48.50	unknown	Ukraine		48882	OPTIMA-SHID-ASUA	false
62.10.234.152	unknown	Italy		8612	TISCALI-IT	false
85.215.233.4	unknown	Germany		6724	STRATOSTRATOAGDE	false
95.240.28.23	unknown	Italy		3269	ASN-IBSNAZIT	false
37.206.89.185	unknown	Italy		3269	ASN-IBSNAZIT	false
85.84.200.62	unknown	Spain		12338	EUSKALTELES	false
197.26.6.253	unknown	Tunisia		37492	ORANGE-TN	false
31.77.234.49	unknown	United Kingdom		12576	EELtdGB	false
31.247.60.247	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
150.64.159.135	unknown	Japan		6400	CompaniaDominicanadeTelefonosSADO	false
62.167.11.194	unknown	Switzerland		6730	SUNRISECH	false
195.104.188.124	unknown	United Kingdom		8437	UTA-ASAT	false
94.162.141.229	unknown	Italy		24608	WINDTRE-ASIT	false
95.212.118.93	unknown	Egypt		51167	CONTABODE	false
62.147.6.201	unknown	France		12322	PROXADFR	false
85.25.248.167	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	false
85.21.71.62	unknown	Russian Federation		8402	CORBINA-ASOJSCVimpelcomRU	false
95.89.255.123	unknown	Germany		31334	KABELDEUTSCHLAND-ASDE	false
85.59.172.97	unknown	Spain		12479	UNI2-ASES	false
41.122.114.205	unknown	South Africa		16637	MTNNS-ASZA	false
112.141.118.203	unknown	Australia		9443	VOCUS-RETAIL-AUVocusRetailAU	false
31.125.242.103	unknown	United Kingdom		6871	PLUSNETUKInternetServiceProviderGB	false
95.167.9.128	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
95.152.245.213	unknown	United Kingdom		8190	MDNXGB	false
112.146.29.238	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
112.33.55.168	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
17.209.40.24	unknown	United States		714	APPLE-ENGINEERINGUS	false
41.139.156.190	unknown	Kenya		37061	SafaricomKE	false
85.183.86.199	unknown	Germany		6805	TDDE-ASN1DE	false
41.73.35.0	unknown	South Africa		37105	NEOLOGY-ASZA	false
218.167.76.209	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
95.170.15.89	unknown	France		25540	ALPHALINK-ASFR	false
85.218.82.252	unknown	Switzerland		34781	SIL-CITYCABLE-ASCH	false
76.244.63.0	unknown	United States		7018	ATT-INTERNET4US	false
62.81.143.70	unknown	Spain		6739	ONO-ASCableuropa-ONOES	false
94.90.206.13	unknown	Italy		3269	ASN-IBSNAZIT	false
31.122.161.114	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
94.84.106.240	unknown	Italy		3269	ASN-IBSNAZIT	false
95.22.141.8	unknown	Spain		12479	UNI2-ASES	false
95.158.144.48	unknown	Bulgaria		61071	NETBOX-ASBG	false
198.61.201.94	unknown	United States		33070	RMH-14US	false
31.61.177.127	unknown	Poland		5617	TPNETPL	false
31.179.155.97	unknown	Poland		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
31.70.134.110	unknown	United Kingdom		12576	EELtdGB	false
85.0.181.48	unknown	Switzerland		3303	SWISSCOMSwisscomSwitzerlandLtdCH	false
88.125.239.251	unknown	France		12322	PROXADFR	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
161.162.59.218	unknown	United States		3257	GTT-BACKBONEGTTDE	false
85.71.136.97	unknown	Czech Republic		5610	O2-CZECH-REPUBLICCZ	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, Motorola m68k, 68020, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.37646226493113
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	bot.m68k.elf
File size:	72'336 bytes
MD5:	7193e673ff416c51aba3a37b63bb0c36
SHA1:	b965c035e8073b961d237c007614144fbdbc1508
SHA256:	7bd3e39acf6713b62fc8e6e431916fb436ec40531ca2aa08dba93e8ca6eb6727
SHA512:	25ddaefa096c3c6a5e6f61d63c1b3be062dfee8c328839f3c59a805314d134cac612689945dcc3d3a3777d3bb090a34332aded628afd5a8c53b6ce840bfbfc65
SSDEEP:	1536:AOegDyBkWJ1eIE00zIm8Ok/z452nPSVf+47E:AOegDzWf1E00kP/RPk+3
TLSH:	9D633995F4029F3CF88BD6BA90170E05B92163C157C30F2BA6A6FDE37DB2164AE25D41
File Content Preview:	.ELF.....D...4.....4. ...(..... .....6...6....$..... .dt.Q.....NV..a....da....|N^NuNV..J9..8.f>"y..6. QJ.g.X.#...6.N."y..6. QJ.f.A.....J.g.Hy....N.X.....8.N^NuNV..N^NuN

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	MC68000

ELF header	
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x80000144
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	71936
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	0x80000094	0x94	0x14	0x0	0x6	AX	0	0	2
.text	PROGBITS	0x800000a8	0xa8	0xfea6	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x8000ff4e	0xff4e	0xe	0x0	0x6	AX	0	0	2
.rodata	PROGBITS	0x8000ff5c	0xff5c	0x173a	0x0	0x2	A	0	0	2
.ctors	PROGBITS	0x8001369c	0x1169c	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x800136a4	0x116a4	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x800136b0	0x116b0	0x210	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x800138c0	0x118c0	0x2d8	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x118c0	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	0x80000000	0x80000000	0x11696	0x11696	6.4040	0x5	R E	0x2000		.init .text .fini .rodata
LOAD	0x1169c	0x8001369c	0x8001369c	0x224	0x4fc	3.0647	0x6	RW	0x2000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Suricata IDS Alerts

Timestamp	SID	Signature	Severity	Source IP	Source Port	Dest IP	Dest Port	Protocol
2024-12-15T19:33:43.940354+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	38910	197.92.216.123	37215	TCP
2024-12-15T19:33:45.061182+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	39760	157.15.140.45	37215	TCP
2024-12-15T19:33:45.800709+0100	2841377	ETPRO MALWARE ELF/Mirai User-Agent Observed (Outbound)	1	192.168.2.14	51384	95.234.5.99	80	TCP
2024-12-15T19:33:46.873102+0100	2841377	ETPRO MALWARE ELF/Mirai User-Agent Observed (Outbound)	1	192.168.2.14	60390	112.178.50.2	80	TCP
2024-12-15T19:33:49.505977+0100	2835222	ETPRO EXPLOIT Huawei Remote Command Execution - Outbound (CVE-2017-17215)	1	192.168.2.14	43954	197.5.116.175	37215	TCP

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Dec 15, 2024 19:36:22.252645969 CET	192.168.2.14	8.8.8.8	0xe02c	Standard query (0)	daisy.ubuntu.com	A (IP address)	IN (0x0001)	false
Dec 15, 2024 19:36:22.252687931 CET	192.168.2.14	8.8.8.8	0x863c	Standard query (0)	daisy.ubuntu.com	28	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Dec 15, 2024 19:36:22.378483057 CET	8.8.8.8	192.168.2.14	0xe02c	No error (0)	daisy.ubuntu.com		162.213.35.25	A (IP address)	IN (0x0001)	false
Dec 15, 2024 19:36:22.378483057 CET	8.8.8.8	192.168.2.14	0xe02c	No error (0)	daisy.ubuntu.com		162.213.35.24	A (IP address)	IN (0x0001)	false

System Behavior

Analysis Process: bot.m68k.elf PID: **5497**, Parent PID: **5415**

General

Start time (UTC):	18:33:38
Start date (UTC):	15/12/2024
Path:	/tmp/bot.m68k.elf
Arguments:	/tmp/bot.m68k.elf
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Analysis Process: bot.m68k.elf PID: **5499**, Parent PID: **5497**

General

Start time (UTC):	18:33:38
Start date (UTC):	15/12/2024
Path:	/tmp/bot.m68k.elf
Arguments:	-
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Directory Enumerated

Analysis Process: bot.m68k.elf PID: **5500**, Parent PID: **5497**

General

Start time (UTC):	18:33:38
Start date (UTC):	15/12/2024
Path:	/tmp/bot.m68k.elf
Arguments:	-
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: bot.m68k.elf PID: **5503**, Parent PID: **5497**

General	
Start time (UTC):	18:33:38
Start date (UTC):	15/12/2024
Path:	/tmp/bot.m68k.elf
Arguments:	-
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: bot.m68k.elf PID: 5505, Parent PID: 5503

General	
Start time (UTC):	18:33:38
Start date (UTC):	15/12/2024
Path:	/tmp/bot.m68k.elf
Arguments:	-
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: bot.m68k.elf PID: 5510, Parent PID: 5503

General	
Start time (UTC):	18:33:38
Start date (UTC):	15/12/2024
Path:	/tmp/bot.m68k.elf
Arguments:	-
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: bot.m68k.elf PID: 5512, Parent PID: 5503

General	
Start time (UTC):	18:33:38
Start date (UTC):	15/12/2024
Path:	/tmp/bot.m68k.elf
Arguments:	-
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: bot.m68k.elf PID: 5514, Parent PID: 5503

General	
Start time (UTC):	18:33:38
Start date (UTC):	15/12/2024
Path:	/tmp/bot.m68k.elf
Arguments:	-
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

- File Read
- Directory Enumerated

Analysis Process: bot.m68k.elf PID: 5517, Parent PID: 5503

General	
Start time (UTC):	18:33:38
Start date (UTC):	15/12/2024
Path:	/tmp/bot.m68k.elf
Arguments:	-
File size:	4463432 bytes

MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: bot.m68k.elf PID: **5519**, Parent PID: **5503**

General

Start time (UTC):	18:33:38
Start date (UTC):	15/12/2024
Path:	/tmp/bot.m68k.elf
Arguments:	-
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc