ID: 635401
Sample Name: XXJn52htu2
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 21:07:46
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Linux Analysis Report

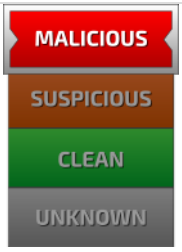
XXJn52htu2

Overview

General Information

Sample Name:	XXJn52htu2
Analysis ID:	635401
MD5:	214bc7a1112014..
SHA1:	bc997a8ce1456d..
SHA256:	ff54b59b11d8a63.
Tags:	32 arm elf mirai
Infos:	

Detection



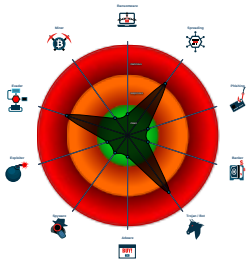
Mirai

Score:	68
Range:	0 - 100
Whitelisted:	false

Signatures

- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Sample is packed with UPX
- Uses known network protocols on n…
- Sample tries to kill multiple process…
- Sample contains only a LOAD segm…
- Yara signature match
- Uses the "uname" system call to qu…
- Enumerates processes within the "p…
- Tries to connect to HTTP servers, b…
- Detected TCP or UDP traffic on non…

Classification



Analysis Advice

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

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

Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures.

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635401
Start date and time: 27/05/202221:07:46	2022-05-27 21:07:46 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	XXJn52htu2
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:	mal68.spre.troj.evad.lin@0/0@0/0

Warnings

Runtime Messages

Command:	/tmp/XXJn52htu2
PID:	6225
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Infected

Standard Error:	

Process Tree

- **system is lnxubuntu20**
- XXJn52htu2 (PID: 6225, Parent: 6123, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/XXJn52htu2
  - XXJn52htu2 New Fork (PID: 6227, Parent: 6225)
  - XXJn52htu2 New Fork (PID: 6228, Parent: 6225)
    - XXJn52htu2 New Fork (PID: 6232, Parent: 6228)
    - XXJn52htu2 New Fork (PID: 6235, Parent: 6228)
      - XXJn52htu2 New Fork (PID: 6237, Parent: 6235)
- **cleanup**

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
XXJn52htu2	SUSP_ELF_LNX_UPX_Compressed_File	Detects a suspicious ELF binary with UPX compression	Florian Roth	• 0x8e60:$s1: PROT_EXEC\|PROT_WRITE failed. • 0x8ecf:$s2: $Id: UPX • 0x8e80:$s3: $Info: This file is packed with the UPX executable packer

PCAP (Network Traffic)

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

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Networking

Uses known network protocols on non-standard ports

System Summary

Sample tries to kill multiple processes (SIGKILL)

Data Obfuscation

Sample is packed with UPX

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

Stealing of Sensitive Information

Yara detected Mirai

Remote Access Functionality

Yara detected Mirai

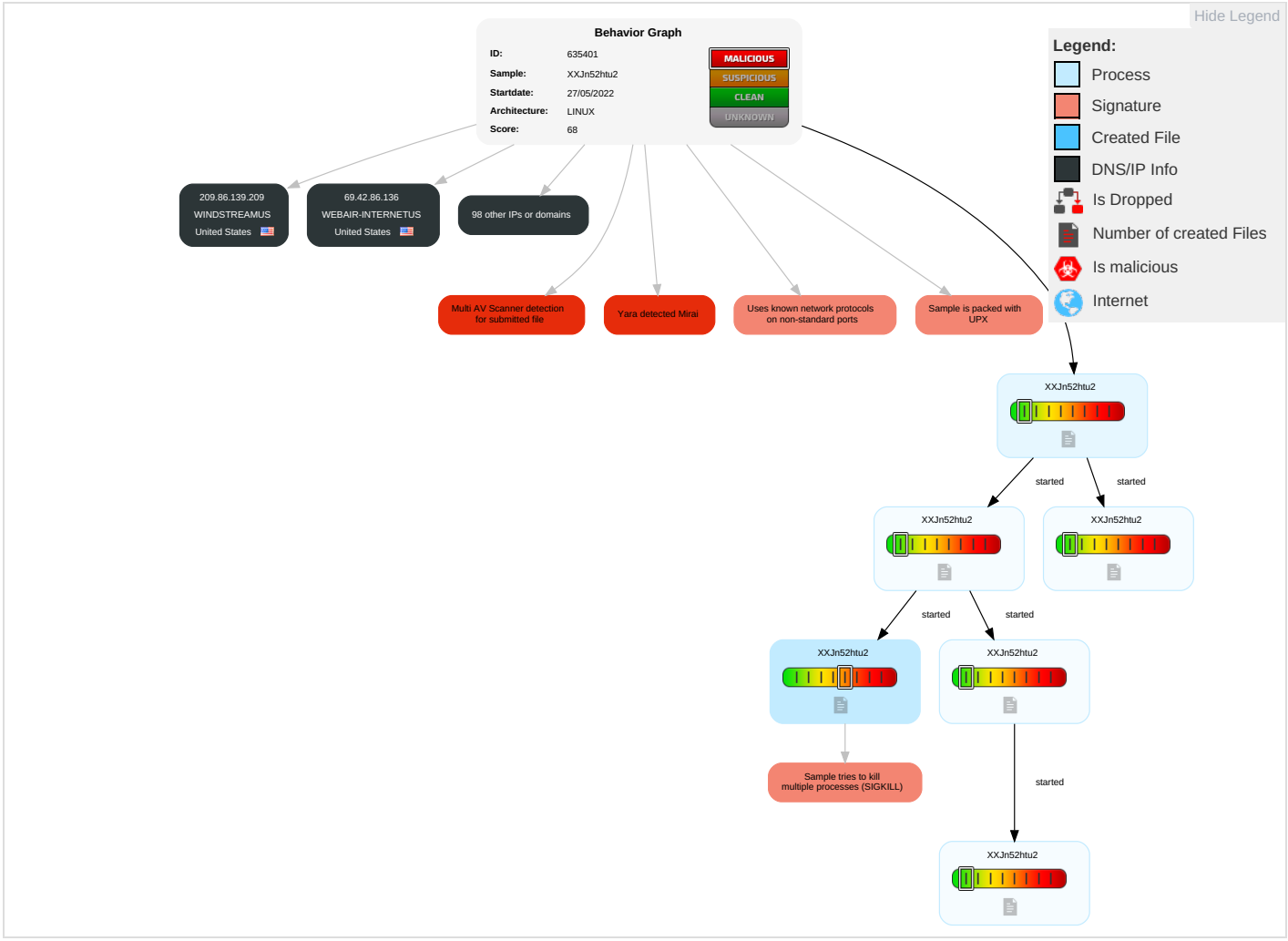
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	1 Obfuscated Files or Information	1 OS Credential Dumping	1 1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 Service Stop
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	1 1 Non-Standard Port	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	1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
XXJn52htu2	17%	Virustotal		Browse
XXJn52htu2	20%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

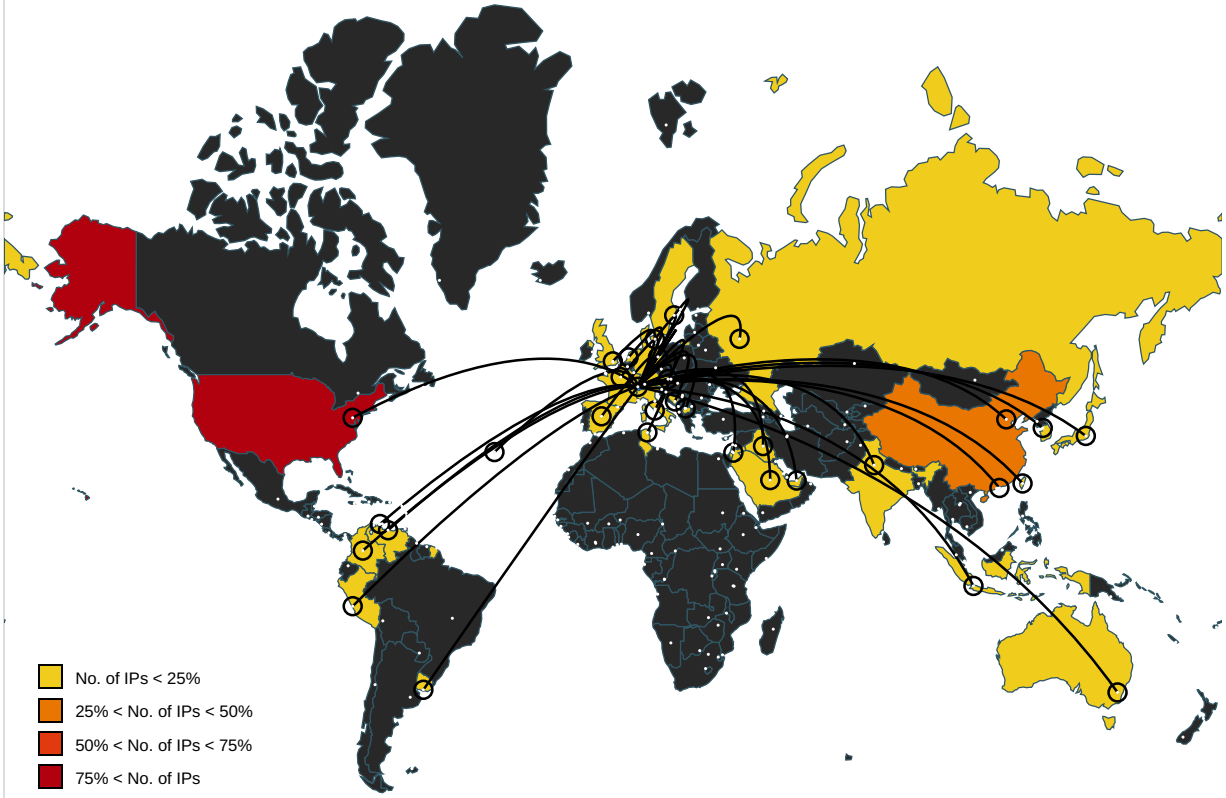
Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
51.223.227.122	unknown	Saudi Arabia		25019	SAUDINETSTC-ASSA	false
50.240.247.180	unknown	United States		7922	COMCAST-7922US	false
119.49.253.58	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
208.122.171.23	unknown	United States		46476	TTUHSCUS	false
246.246.200.243	unknown	Reserved		unknown	unknown	false
206.126.23.139	unknown	United States		23265	POCKETINETUS	false
181.136.190.145	unknown	Colombia		13489	EPMTelecomunicacionesSAESPCO	false
98.252.105.154	unknown	United States		7922	COMCAST-7922US	false
203.85.146.105	unknown	Hong Kong		4058	CITICTEL-CPC-AS4058CITICTelecomInternationalCPCLimited	false
186.49.156.123	unknown	Uruguay		6057	AdministracionNacionaldeTelecomunicacionesUY	false
185.21.137.210	unknown	Iraq		209565	ALSARDFIBERIQ	false
243.14.153.5	unknown	Reserved		unknown	unknown	false
88.214.61.218	unknown	Bosnia and Herzegowina		47959	TELINEABA	false
48.151.193.96	unknown	United States		2686	ATGS-MMD-ASUS	false
209.86.139.209	unknown	United States		7029	WINDSTREAMUS	false
71.207.148.144	unknown	United States		7922	COMCAST-7922US	false
124.2.228.15	unknown	Korea Republic of		18302	SKG_NW-AS-KRSKTelecomKR	false
192.70.138.77	unknown	United States		2200	FR-RENATERReseauNationaldetelecommunicationspourlaTec	false
55.26.142.22	unknown	United States		319	DNIC-ASBLK-00306-00371US	false
138.207.110.63	unknown	United States		396368	TETHERVIEWUS	false
69.42.86.136	unknown	United States		27257	WEBAIR-INTERNETUS	false
131.109.171.204	unknown	United States		14464	RINETUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.29.80.111	unknown	United States		1239	SPRINTLINKUS	false
200.6.57.233	unknown	Curacao		11081	UnitedTelecommunicationServicesUTSCW	false
46.208.236.8	unknown	United Kingdom		6871	PLUSNETUKInternetServiceProviderGB	false
73.215.212.60	unknown	United States		7922	COMCAST-7922US	false
198.11.206.99	unknown	United States		36351	SOFTLAYERUS	false
151.32.206.187	unknown	Italy		1267	ASN-WINDTREIUNETEU	false
117.161.54.243	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
222.13.19.27	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
110.244.101.149	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
52.246.95.187	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
217.165.155.168	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	false
21.75.220.138	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
78.64.186.144	unknown	Sweden		3301	TELIANET-SWEDENTeliaCompanySE	false
212.143.81.73	unknown	Israel		1680	NV-ASNCELLCOMltdIL	false
176.29.233.108	unknown	Jordan		20773	GODADDYDE	false
139.63.130.160	unknown	Netherlands		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
195.82.203.156	unknown	Denmark		9158	TELENOR_DANMARK_ASDK	false
7.103.157.233	unknown	United States		3356	LEVEL3US	false
101.209.22.32	unknown	India		58519	CHINATELECOM-CTCLOUDCloudComputingCorporationCN	false
73.90.89.90	unknown	United States		7922	COMCAST-7922US	false
197.26.6.244	unknown	Tunisia		37492	ORANGE-TN	false
60.168.15.60	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
161.32.117.152	unknown	United States		14340	SALESFORCEUS	false
191.104.108.95	unknown	Colombia		61317	ASDETUKhttpwwwheficedcomGB	false
111.55.29.14	unknown	China		56042	CMNET-SHANXI-APChinaMobilecommunicationscorporationCN	false
98.61.107.114	unknown	United States		7922	COMCAST-7922US	false
245.240.114.75	unknown	Reserved		unknown	unknown	false
190.117.210.173	unknown	Peru		12252	AmericaMovilPeruSACPE	false
46.217.76.226	unknown	Macedonia		6821	MT-AS-OWNbulOrceNikolovbbMK	false
79.179.215.246	unknown	Israel		8551	BEZEQ-INTERNATIONAL-ASBezeqintInternetBackboneIL	false
202.249.239.93	unknown	Japan		2506	SUPERCSINTTWESTCHUGOKUCORPORATIONJP	false
114.55.242.143	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
48.142.166.161	unknown	United States		2686	ATGS-MMD-ASUS	false
108.77.188.45	unknown	United States		7018	ATT-INTERNET4US	false
151.86.44.179	unknown	Italy		8217	ASN-ENIIT	false
27.161.81.28	unknown	Korea Republic of		9644	SKTELECOM-NET-ASSKTelecomKR	false
28.169.115.88	unknown	United States		7922	COMCAST-7922US	false
73.43.54.233	unknown	United States		7922	COMCAST-7922US	false
183.87.69.237	unknown	India		45194	SIPL-ASSysconInfowayPvtLtdIN	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
240.240.180.215	unknown	Reserved		unknown	unknown	false
153.10.223.13	unknown	United States		22063	UNASSIGNED	false
128.222.21.6	unknown	United States		5723	JHUUS	false
88.10.111.96	unknown	Spain		3352	TELEFONICA_DE_ESPANAES	false
138.83.39.54	unknown	United States		58611	CDU-AS-APCharlesDarwinUniversityAU	false
212.203.107.179	unknown	Switzerland		8220	COLTCOLTTechnologyServicesGroupLimitedGB	false
1.31.84.172	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
223.23.20.175	unknown	Taiwan; Republic of China (ROC)		17709	APTAsiaPacificTelecomTW	false
246.92.208.130	unknown	Reserved		unknown	unknown	false
92.162.65.172	unknown	France		3215	FranceTelecom-OrangeFR	false
59.73.212.81	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
32.88.158.219	unknown	United States		2686	ATGS-MMD-ASUS	false
112.192.74.37	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
203.14.225.221	unknown	Australia		7546	DREAMTILT-APDreamtiltServiceProviderGladstoneAU	false
39.148.239.5	unknown	China		24445	CMNET-V4HENAN-AS-APHenanMobileCommunicationsCoLtdCN	false
86.160.170.246	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetworkGB	false
203.108.203.190	unknown	Australia		703	UUNETUS	false
161.39.253.184	unknown	United States		33039	EDMC-INTERNETUS	false
99.189.112.208	unknown	United States		7018	ATT-INTERNET4US	false
42.30.66.54	unknown	Korea Republic of		9644	SKTELECOM-NET-ASSKTelecomKR	false
49.93.214.49	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
136.45.143.198	unknown	United States		16591	GOOGLE-FIBERUS	false
194.195.203.136	unknown	Germany		6659	NEXINTO-DE	false
86.33.220.221	unknown	Austria		5089	NTLGB	false
157.141.165.146	unknown	United States		27064	DNIC-ASBLK-27032-27159US	false
163.49.121.212	unknown	Japan		2497	IIJInternetInitiativeJapanIncJP	false
12.215.219.28	unknown	United States		7018	ATT-INTERNET4US	false
188.194.192.24	unknown	Germany		31334	KABELDEUTSCHLAND-ASDE	false
175.94.80.103	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
180.131.146.88	unknown	Indonesia		45719	NAWALA-AS-IDNawalaProject-DNSFilteringProjectID	false
252.70.145.142	unknown	Reserved		unknown	unknown	false
24.167.176.22	unknown	United States		11426	TWC-11426-CAROLINASUS	false
42.12.204.143	unknown	Korea Republic of		4249	LILLY-ASUS	false
28.108.249.218	unknown	United States		7922	COMCAST-7922US	false
190.39.145.49	unknown	Venezuela		8048	CANTVServiciosVenezuelaVE	false
188.0.171.238	unknown	Russian Federation		49724	VAINAHTELECOM-ASRU	false
46.242.31.24	unknown	Russian Federation		42610	NCNET-ASRU	false
130.200.191.155	unknown	United States		137	ASGARRConsortiumGARREU	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
153.206.128.250	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	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 LSB executable, ARM, version 1 (ARM), statically linked, stripped
Entropy (8bit):	7.966088580361416
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	XXJn52htu2
File size:	38440
MD5:	214bc7a11120145241f962afdb35bab1
SHA1:	bc997a8ce1456d17b56bbf3eede98a160d4b42f0
SHA256:	ff54b59b11d8a639c26411d069a74c6f9493bcff1226b0c7785f092c489fa7fe
SHA512:	a587cbd681ee8f5a280c68092db35721572398a10dd43d3b418e7a7a3008fee3b628ffecf1f58f7b02ee94c285784ebb2c73947820414cba32ae72c6ebebd6ce
SSDEEP:	768:kufCsecOTPyhmevGNpBJy2OZAXsGOjtoR5JwEzus3UozV:NCtcKBevGNpPy2OZAXsGKOR5JwuTzV
TLSH:	FC03F224DB827D12CE705B35E616CB46E7F51AE4E4E9B37C2691E098E0C391E4D3530A
File Content Preview:	.ELF...a.....(.....4.....4. ... (.....?...?.....Q.td.....UPX!.....:..:.....S.....?.E.h;.}...^.....e..G....I..u.].r...fqk.w..j6.7...c;.....N....f

Static ELF Info

ELF header

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

ELF header	
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	ARM - ABI
ABI Version:	0
Entry Point Address:	0x10390
Flags:	0x2
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8000	0x8000	0x953f	0x953f	4.0189	0x5	R E	0x8000		
LOAD	0x1c00	0x29c00	0x29c00	0x0	0x0	0.0000	0x6	RW	0x8000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

TCP Packets

System Behavior

Analysis Process: XXJn52htu2 PID: **6225**, Parent PID: **6123**

General

Start time:	21:08:30
Start date:	27/05/2022
Path:	/tmp/XXJn52htu2
Arguments:	/tmp/XXJn52htu2
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: XXJn52htu2 PID: **6227**, Parent PID: **6225**

General

Start time:	21:08:31
Start date:	27/05/2022
Path:	/tmp/XXJn52htu2
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: XXJn52htu2 PID: **6228**, Parent PID: **6225**

General	
Start time:	21:08:31
Start date:	27/05/2022
Path:	/tmp/XXJn52htu2
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: XXJn52htu2 PID: **6232**, Parent PID: **6228**

General	
Start time:	21:08:31
Start date:	27/05/2022
Path:	/tmp/XXJn52htu2
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: XXJn52htu2 PID: **6235**, Parent PID: **6228**

General	
Start time:	21:08:31
Start date:	27/05/2022
Path:	/tmp/XXJn52htu2
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: XXJn52htu2 PID: **6237**, Parent PID: **6235**

General	
Start time:	21:08:31
Start date:	27/05/2022
Path:	/tmp/XXJn52htu2
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1