ID: 512619
Sample Name: z0x3n.x86
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 08:54:01
Date: 01/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

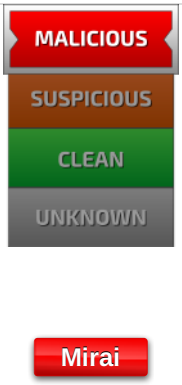
Linux Analysis Report z0x3n.x86

Overview

General Information

Sample Name:	z0x3n.x86
Analysis ID:	512619
MD5:	c2c1c54bbc5f372..
SHA1:	2c9ebbad068ea0..
SHA256:	dd9c8a7d71f944d.
Infos:	

Detection

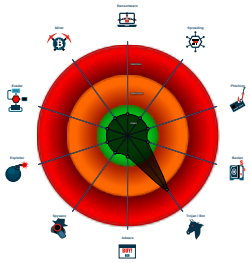


Score:	68
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Machine Learning detection for samp...
- Yara signature match
- Sample has stripped symbol table
- Enumerates processes within the "p...
- 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:	512619
Start date:	01.11.2021
Start time:	08:54:01
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	z0x3n.x86
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.troj.linX86@0/0@1/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- z0x3n.x86 (PID: 5231, Parent: 5116, MD5: c2c1c54bbc5f372df082aebc0d983716) Arguments: /tmp/z0x3n.x86
  - z0x3n.x86 New Fork (PID: 5232, Parent: 5231)
  - z0x3n.x86 New Fork (PID: 5233, Parent: 5231)
    - z0x3n.x86 New Fork (PID: 5234, Parent: 5233)
    - z0x3n.x86 New Fork (PID: 5235, Parent: 5233)
    - z0x3n.x86 New Fork (PID: 5236, Parent: 5233)
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
z0x3n.x86	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0xedc8:$xo1: Dfs`eeh&<'9 • 0xee40:$xo1: Dfs`eeh&<'9 • 0xeeb4:$xo1: Dfs`eeh&<'9 • 0xef24:$xo1: Dfs`eeh&<'9 • 0xef70:$xo1: Dfs`eeh&<'9

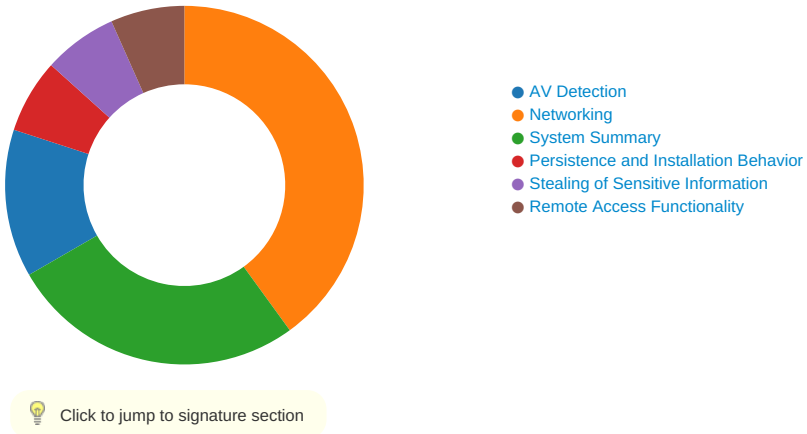
PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
5231.1.0000000019671de5.00000000c7254e12.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x6d0:$xo1: Dfs`eeh&<'9 • 0x750:$xo1: Dfs`eeh&<'9 • 0x7c8:$xo1: Dfs`eeh&<'9 • 0x840:$xo1: Dfs`eeh&<'9 • 0x890:$xo1: Dfs`eeh&<'9
5234.1.0000000019671de5.00000000c7254e12.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x6d0:$xo1: Dfs`eeh&<'9 • 0x750:$xo1: Dfs`eeh&<'9 • 0x7c8:$xo1: Dfs`eeh&<'9 • 0x840:$xo1: Dfs`eeh&<'9 • 0x890:$xo1: Dfs`eeh&<'9
5232.1.0000000019671de5.00000000c7254e12.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x6d0:$xo1: Dfs`eeh&<'9 • 0x750:$xo1: Dfs`eeh&<'9 • 0x7c8:$xo1: Dfs`eeh&<'9 • 0x840:$xo1: Dfs`eeh&<'9 • 0x890:$xo1: Dfs`eeh&<'9
5232.1.000000001a887bdc.00000000328ec990.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0xedc8:$xo1: Dfs`eeh&<'9 • 0xee40:$xo1: Dfs`eeh&<'9 • 0xeeb4:$xo1: Dfs`eeh&<'9 • 0xef24:$xo1: Dfs`eeh&<'9 • 0xef70:$xo1: Dfs`eeh&<'9
5231.1.000000001a887bdc.00000000328ec990.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0xedc8:$xo1: Dfs`eeh&<'9 • 0xee40:$xo1: Dfs`eeh&<'9 • 0xeeb4:$xo1: Dfs`eeh&<'9 • 0xef24:$xo1: Dfs`eeh&<'9 • 0xef70:$xo1: Dfs`eeh&<'9
Click to see the 1 entries				

Jbx Signature Overview



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)

Stealing of Sensitive Information:

Yara detected Mirai

Remote Access Functionality:

Yara detected Mirai

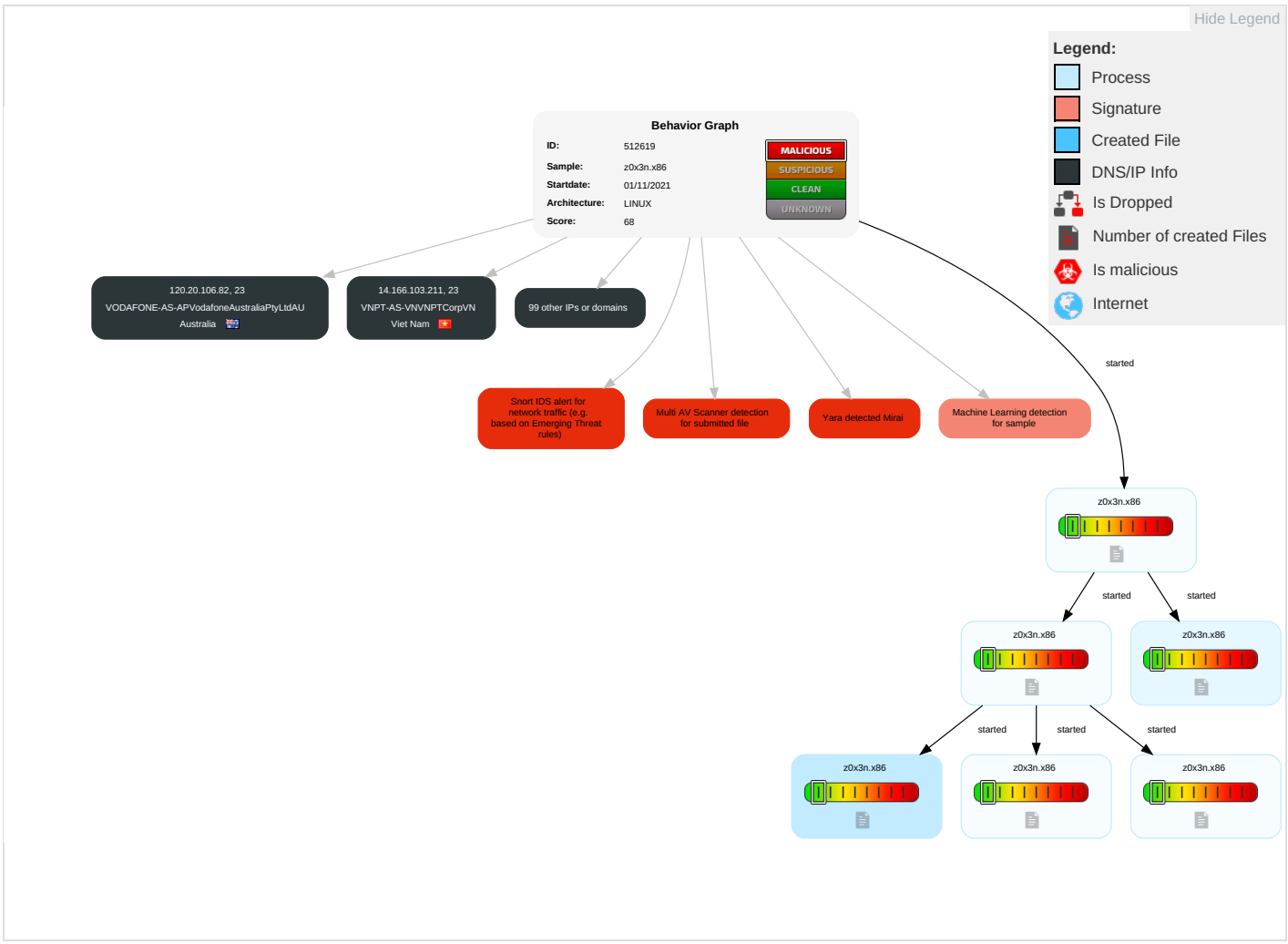
Mitre Att&ck Matrix

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	Direct Volume Access	OS Credential Dumping 1	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	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
z0x3n.x86	42%	Virustotal		Browse
z0x3n.x86	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
z0x3n.cf	37.0.10.67	true	false		unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
111.12.128.239	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
8.102.49.78	unknown	United States		3356	LEVEL3US	false
192.77.169.162	unknown	United States		394008	DBI-ASUS	false
57.111.236.183	unknown	Belgium		51964	ORANGE-BUSINESS-SERVICES-IPSN-ASNFR	false
191.255.128.161	unknown	Brazil		27699	TELEFONICABRASILSABR	false
178.22.52.188	unknown	Russian Federation		44943	RAMNET-ASInternetServiceProviderRamNetRU	false
91.156.163.171	unknown	Finland		719	ELISA-ASHelsinkiFinlandEU	false
179.67.250.16	unknown	Brazil		7738	TelemarNorteLesteSABR	false
113.133.36.115	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
195.89.233.144	unknown	United Kingdom		1273	CWVodafoneGroupPLCEU	false
130.223.218.209	unknown	Switzerland		559	SWITCHPeeringrequestspeeringswitchchEU	false
106.44.67.176	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
181.28.71.103	unknown	Argentina		10318	TelecomArgentinaSAAR	false
112.246.77.240	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
73.180.82.168	unknown	United States		7922	COMCAST-7922US	false
213.202.53.40	unknown	Switzerland		21466	ASQUICKNETKabelfernsehnBoedeliinInterlakenSwitzerland	false
146.190.146.173	unknown	United States		702	UUNETUS	false
89.27.99.244	unknown	Finland		16086	DNAFI	false
20.73.200.192	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
169.64.152.199	unknown	United States		37611	AfrihostZA	false
210.200.107.2	unknown	Taiwan; Republic of China (ROC)		9311	HITRON-AS-APHITRONTECHNOLOGYINCTW	false
200.64.54.219	unknown	Mexico		8151	UninetSAdeCVMX	false
173.225.75.100	unknown	United States		26878	TWRS-NYCUS	false
94.43.140.207	unknown	Georgia		35805	SILKNET-ASGE	false
111.253.7.151	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
1.81.74.63	unknown	China		134768	CHINANET-SHAANXI-CLOUD-BASECHINANETSHAANXIprovinceCloud	false
98.225.187.150	unknown	United States		7922	COMCAST-7922US	false
183.91.246.58	unknown	Korea Republic of		9976	ICNDP-AS-KRNamincheonBrodcastingCoLtdKR	false
200.98.94.223	unknown	Brazil		7162	UniversoOnlineSABR	false
177.247.199.47	unknown	Mexico		13999	MegaCableSAdeCVMX	false
125.51.30.130	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
185.151.99.5	unknown	Iran (ISLAMIC Republic Of)		62153	PANAIR	false
42.68.109.132	unknown	Taiwan; Republic of China (ROC)		4249	LILLY-ASUS	false
76.0.12.143	unknown	United States		18494	CENTURYLINK-LEGACY-EMBARQ-WRBGUS	false
83.80.167.254	unknown	Netherlands		33915	TNF-ASNL	false
120.20.106.82	unknown	Australia		133612	VODAFONE-AS-APVodafoneAustraliaPtyLtdAU	false
82.76.185.25	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	false
205.194.107.171	unknown	Canada		3356	LEVEL3US	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
119.63.255.29	unknown	Korea Republic of		17577	GIGAPASS-AS-KRLGHelloVisionCorpKR	false
95.19.35.69	unknown	Spain		12479	UNI2-ASES	false
169.144.15.17	unknown	United States		158	ERI-ASUS	false
8.55.105.60	unknown	United States		3356	LEVEL3US	false
107.209.55.138	unknown	United States		7018	ATT-INTERNET4US	false
202.102.100.47	unknown	China		137702	CHINATELECOM-JIANGSU-NANJING-IDCNanjingJiangsuProvince	false
161.152.120.87	unknown	Australia		9328	DATACOM-AUDATACOMSYSTEMSAUPTYLTDAU	false
54.21.179.8	unknown	United States		14618	AMAZON-AESUS	false
12.101.24.89	unknown	United States		7018	ATT-INTERNET4US	false
170.12.117.113	unknown	United States		27283	RJF-INTERNETUS	false
88.58.19.233	unknown	Italy		3269	ASN-IBSNAZIT	false
125.48.186.209	unknown	Japan		2516	KDDIKDDICORPORATIONJP	false
140.234.210.128	unknown	United States		6932	EBSCOPUBUS	false
165.245.232.222	unknown	United States		4668	LGNET-AS-KRLGCNSKR	false
171.253.42.137	unknown	Viet Nam		7552	VIETEL-AS-APViettelGroupVN	false
200.7.36.227	unknown	Sint Maarten		27734	NewTechnologiesGroupNVSX	false
156.186.86.117	unknown	Egypt		36992	ETISALAT-MISREG	false
195.135.1.151	unknown	France		8399	SEWAN-FR	false
207.197.1.26	unknown	United States		3851	NSHE-NEVADANETUS	false
186.58.217.66	unknown	Argentina		22927	TelefonicadeArgentinaAR	false
154.56.2.191	unknown	United States		174	COGENT-174US	false
62.212.29.71	unknown	Italy		9026	ULI-MAINULIIT	false
97.121.96.184	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
68.89.131.171	unknown	United States		7018	ATT-INTERNET4US	false
116.17.39.25	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
14.166.103.211	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
150.227.240.141	unknown	Sweden		3246	TDCSONGTele2BusinessTDCSwedenSE	false
91.113.151.22	unknown	Austria		8447	TELEKOM-ATA1TelekomAustriaAGAT	false
4.44.24.55	unknown	United States		3356	LEVEL3US	false
156.169.238.165	unknown	Egypt		36992	ETISALAT-MISREG	false
163.141.21.203	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
93.120.179.216	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
47.0.120.15	unknown	United States		34533	ESAMARA-ASRU	false
114.170.2.111	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
66.212.66.237	unknown	United States		21525	AS-SPLUS	false
196.80.15.132	unknown	Morocco		6713	IAM-ASMA	false
23.253.210.18	unknown	United States		19994	RACKSPACEUS	false
151.226.142.75	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
101.7.232.251	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
117.176.199.169	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
185.92.209.62	unknown	Switzerland		200879	SWISSBROTHERSCH	false
160.172.146.38	unknown	Morocco		6713	IAM-ASMA	false
39.89.15.205	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
219.17.70.121	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
168.154.89.155	unknown	Korea Republic of		10049	SKNET-ASSKCoKR	false
40.71.135.48	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
212.22.221.83	unknown	Ukraine		31148	FREENET_LLCUA	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
202.238.46.90	unknown	Japan		10001	MICSNETMicsNetworkCorporationJP	false
152.11.76.235	unknown	United States		81	NCRENUS	false
81.222.210.53	unknown	Russian Federation		20597	ELTEL-ASRU	false
192.30.221.157	unknown	United States		23275	LM-USAUS	false
74.140.211.129	unknown	United States		10796	TWC-10796-MIDWESTUS	false
97.78.71.158	unknown	United States		33363	BHN-33363US	false
184.142.114.154	unknown	United States		5778	CENTURYLINK-LEGACY-EMBARQ-RCMTUS	false
93.32.193.143	unknown	Italy		12874	FASTWEBIT	false
93.50.106.246	unknown	Italy		12874	FASTWEBIT	false
45.143.235.203	unknown	Estonia		39855	MOD-EUNL	false
72.59.167.134	unknown	United States		10507	SPCSUS	false
38.200.160.186	unknown	United States		174	COGENT-174US	false
70.131.55.48	unknown	United States		7018	ATT-INTERNET4US	false
24.194.248.225	unknown	United States		11351	TWC-11351-NORTHEASTUS	false
8.166.90.215	unknown	Singapore		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false

Runtime Messages

Command:	/tmp/z0x3n.x86
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	0G0dn3t Got To Ya!
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
20.73.200.192	x86	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ORANGE-BUSINESS-SERVICES-IPSN-ASNFR	gbk4XWulUo	Get hash	malicious	Browse	• 212.167.164.218
	Tsunami.arm	Get hash	malicious	Browse	• 156.134.58.72
	x86	Get hash	malicious	Browse	• 57.111.44.42
	ivImhRZqGa	Get hash	malicious	Browse	• 57.111.19.90
	07xBxVsvEn	Get hash	malicious	Browse	• 57.79.150.70
	wTFR3LK4Mo	Get hash	malicious	Browse	• 57.92.163.149
	bKHI9UT0D1	Get hash	malicious	Browse	• 57.127.117.170
	eNrYzJWFvB	Get hash	malicious	Browse	• 200.240.115.57
	GQM8qzLfFs	Get hash	malicious	Browse	• 57.105.13.102
	sora.arm	Get hash	malicious	Browse	• 57.70.235.20
	Tf9ATzpdKR	Get hash	malicious	Browse	• 200.226.197.191
	b3astmode.arm	Get hash	malicious	Browse	• 57.74.72.11
	yFbmGHoONE	Get hash	malicious	Browse	• 156.134.58.77

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	FWsCarsq8Q	Get hash	malicious	Browse	• 156.135.155.197
	buiodawbdawbuiopdw.x86	Get hash	malicious	Browse	• 62.229.123.252
	arm7	Get hash	malicious	Browse	• 57.99.202.79
	arm	Get hash	malicious	Browse	• 57.86.239.254
	arm7	Get hash	malicious	Browse	• 156.134.58.88
	arm	Get hash	malicious	Browse	• 57.84.148.190
	sora.arm	Get hash	malicious	Browse	• 57.117.171.166
LEVEL3US	z0x3n.arm	Get hash	malicious	Browse	• 4.77.193.187
	jGVlUAzDbQ	Get hash	malicious	Browse	• 138.12.216.235
	ev1JsPbdMA	Get hash	malicious	Browse	• 138.12.216.253
	QZ2CN6CUyv	Get hash	malicious	Browse	• 9.162.77.202
	Xs0PMn85CN	Get hash	malicious	Browse	• 4.7.177.40
	x86	Get hash	malicious	Browse	• 216.141.213.58
	KXAJjgoH22	Get hash	malicious	Browse	• 4.45.235.181
	Z7QqCH0bak	Get hash	malicious	Browse	• 157.199.162.106
	zouBbQwUTb	Get hash	malicious	Browse	• 9.44.191.61
	x86_64	Get hash	malicious	Browse	• 64.154.123.164
	U1WRbn3wOa	Get hash	malicious	Browse	• 9.152.52.161
	RVG73cR3DP	Get hash	malicious	Browse	• 4.136.211.76
	9QPGr9LMaq	Get hash	malicious	Browse	• 206.33.161.35
	32UX3eB2m0	Get hash	malicious	Browse	• 9.169.60.90
	jJ6GK5qbZt	Get hash	malicious	Browse	• 4.125.80.128
	x86	Get hash	malicious	Browse	• 166.90.237.153
	hvYTLlrdRm	Get hash	malicious	Browse	• 4.204.173.89
	1b5356SnwB	Get hash	malicious	Browse	• 75.103.49.235
	vEBWe85OY5	Get hash	malicious	Browse	• 8.196.29.107
	S1WMHUXAQU	Get hash	malicious	Browse	• 4.234.132.186
CMNET-GDGuangdongMobileCommunicationCoLtdCN	QZ2CN6CUyv	Get hash	malicious	Browse	• 183.224.188.131
	x86	Get hash	malicious	Browse	• 183.255.19.37
	ivImhRZqGa	Get hash	malicious	Browse	• 117.139.191.41
	Z7QqCH0bak	Get hash	malicious	Browse	• 36.175.118.55
	PpZvxl4DJg	Get hash	malicious	Browse	• 36.164.147.131
	arm7	Get hash	malicious	Browse	• 117.187.200.202
	U1WRbn3wOa	Get hash	malicious	Browse	• 112.47.118.185
	RVG73cR3DP	Get hash	malicious	Browse	• 39.131.235.1
	hvYTLlrdRm	Get hash	malicious	Browse	• 123.82.185.223
	2pPPNW1XSo	Get hash	malicious	Browse	• 112.50.147.80
	S1WMHUXAQU	Get hash	malicious	Browse	• 117.150.97.40
	st2AAeCXsR	Get hash	malicious	Browse	• 112.31.237.169
	OklOTajM3X.exe	Get hash	malicious	Browse	• 111.12.28.24
	mdyu2wtnR8	Get hash	malicious	Browse	• 36.167.38.135
	egd7wSpaw2	Get hash	malicious	Browse	• 39.133.46.94
	KfvEoN0wlw	Get hash	malicious	Browse	• 223.75.114.193
	Xb1sM3W7BK	Get hash	malicious	Browse	• 111.28.163.155
	txwaNf62fv	Get hash	malicious	Browse	• 122.77.200.46
	nLfUJu0kEA	Get hash	malicious	Browse	• 223.82.2.220
	K1fia4oWep	Get hash	malicious	Browse	• 111.60.197.135

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):	6.455104594575481
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	z0x3n.x86
File size:	63664
MD5:	c2c1c54bbc5f372df082aebc0d983716
SHA1:	2c9ebbad068ea09d2fcf7cfff48608a8abdf4337
SHA256:	dd9c8a7d71f944ded984394fcc021043403e3a39ef424d70d2a3a18c3b58b69d
SHA512:	dfd1c9ad3a1da9d190717f77e407774d2b9bd68986fdeb3fd7dff3bd7d8852311d5df9eb1d0f350e4d221d9b494f00afc128e3a2ef3f96e67456020e6f73dfa2
SSDEEP:	1536:WuIDGwqmkZxXP5XM4wCadEzKC18HqmPWJBus0eD/OQAy9T:PIDsbZxf5XM4wCq0zCHqpEs5/22
File Content Preview:	.ELF.....d...4... .....4. ...(.....\...\.....Q.td.....U..S.....h.....[]...$.....U.....=.....t..5.....u.....t....h.u.....

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:	63264
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

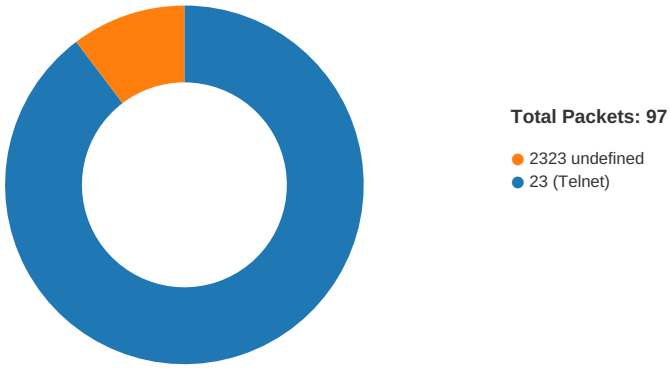
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x8048094	0x94	0x1c	0x0	0x6	AX	0	0	1
.text	PROGBITS	0x80480b0	0xb0	0xe636	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x80566e6	0xe6e6	0x17	0x0	0x6	AX	0	0	1
.rodata	PROGBITS	0x8056700	0xe700	0xe80	0x0	0x2	A	0	0	32
.ctors	PROGBITS	0x8058584	0xf584	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x805858c	0xf58c	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x80585c0	0xf5c0	0x120	0x0	0x3	WA	0	0	32
.bss	NOBITS	0x80586e0	0xf6e0	0x800	0x0	0x3	WA	0	0	32
.shstrtab	STRTAB	0x0	0xf6e0	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	0xf580	0xf580	3.7842	0x5	R E	0x1000		.init .text .fini .rodata
LOAD	0xf584	0x8058584	0x8058584	0x15c	0x95c	2.4470	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 1, 2021 08:54:44.484302044 CET	192.168.2.23	8.8.8.8	0xee26	Standard query (0)	z0x3n.cf	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 1, 2021 08:54:44.512578011 CET	8.8.8.8	192.168.2.23	0xee26	No error (0)	z0x3n.cf		37.0.10.67	A (IP address)	IN (0x0001)

System Behavior

Analysis Process: z0x3n.x86 PID: 5231 Parent PID: 5116

General

Start time:	08:54:44
Start date:	01/11/2021
Path:	/tmp/z0x3n.x86
Arguments:	/tmp/z0x3n.x86
File size:	63664 bytes
MD5 hash:	c2c1c54bbc5f372df082aebc0d983716

Analysis Process: z0x3n.x86 PID: 5232 Parent PID: 5231

General

Start time:	08:54:44
Start date:	01/11/2021
Path:	/tmp/z0x3n.x86
Arguments:	n/a
File size:	63664 bytes
MD5 hash:	c2c1c54bbc5f372df082aebc0d983716

Analysis Process: z0x3n.x86 PID: 5233 Parent PID: 5231

General

Start time:	08:54:44
Start date:	01/11/2021
Path:	/tmp/z0x3n.x86
Arguments:	n/a
File size:	63664 bytes
MD5 hash:	c2c1c54bbc5f372df082aebc0d983716

Analysis Process: z0x3n.x86 PID: 5234 Parent PID: 5233

General

Start time:	08:54:44
Start date:	01/11/2021
Path:	/tmp/z0x3n.x86
Arguments:	n/a
File size:	63664 bytes
MD5 hash:	c2c1c54bbc5f372df082aebc0d983716

Analysis Process: z0x3n.x86 PID: 5235 Parent PID: 5233

General

Start time:	08:54:44
Start date:	01/11/2021
Path:	/tmp/z0x3n.x86
Arguments:	n/a
File size:	63664 bytes
MD5 hash:	c2c1c54bbc5f372df082aebc0d983716

File Activities

File Read

Directory Enumerated

Analysis Process: z0x3n.x86 PID: 5236 Parent PID: 5233

General

Start time:	08:54:44

Start date:	01/11/2021
Path:	/tmp/z0x3n.x86
Arguments:	n/a
File size:	63664 bytes
MD5 hash:	c2c1c54bbc5f372df082aebc0d983716