ID: 511504
Sample Name: iksM5QEg2j
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 08:33:41
Date: 29/10/2021
Version: 34.0.0 Boulder Opal

Table of Contents

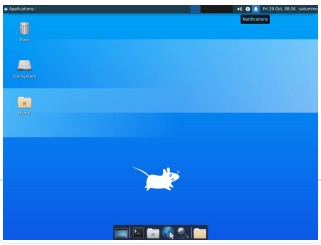
Linux Analysis Report iksM5QEg2j

Overview

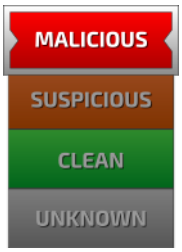
General Information

Sample Name:	iksM5QEg2j
Analysis ID:	511504
MD5:	d5f7312f62ca02a..
SHA1:	d157216923829b..
SHA256:	752b21a8ab77df1.
Tags:	32 elf intel
Infos:	

Most interesting Screenshot:



Detection

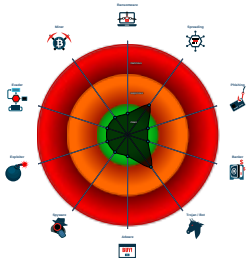


Score:	52
Range:	0 - 100
Whitelisted:	false

Signatures

- Multi AV Scanner detection for subm…
- Machine Learning detection for samp…
- Enumerates processes within the "p…
- Tries to connect to HTTP servers, b…
- Detected TCP or UDP traffic on non…
- Sample tries to kill a process (SIGK…
- Sample has stripped symbol table

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:	511504
Start date:	29.10.2021
Start time:	08:33:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	iksM5QEg2j
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:	mal52.lin@0/0@0/0

Process Tree

- **system is lnxubuntu20**
- iksM5QEg2j (PID: 5236, Parent: 5112, MD5: d5f7312f62ca02ad0873bdd213dd71be) Arguments: /tmp/iksM5QEg2j
  - iksM5QEg2j New Fork (PID: 5237, Parent: 5236)
    - iksM5QEg2j New Fork (PID: 5238, Parent: 5237)
- **cleanup**

Yara Overview

No yara matches

Jbx Signature Overview

- AV Detection
- Networking
- System Summary
- Persistence and Installation Behavior

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

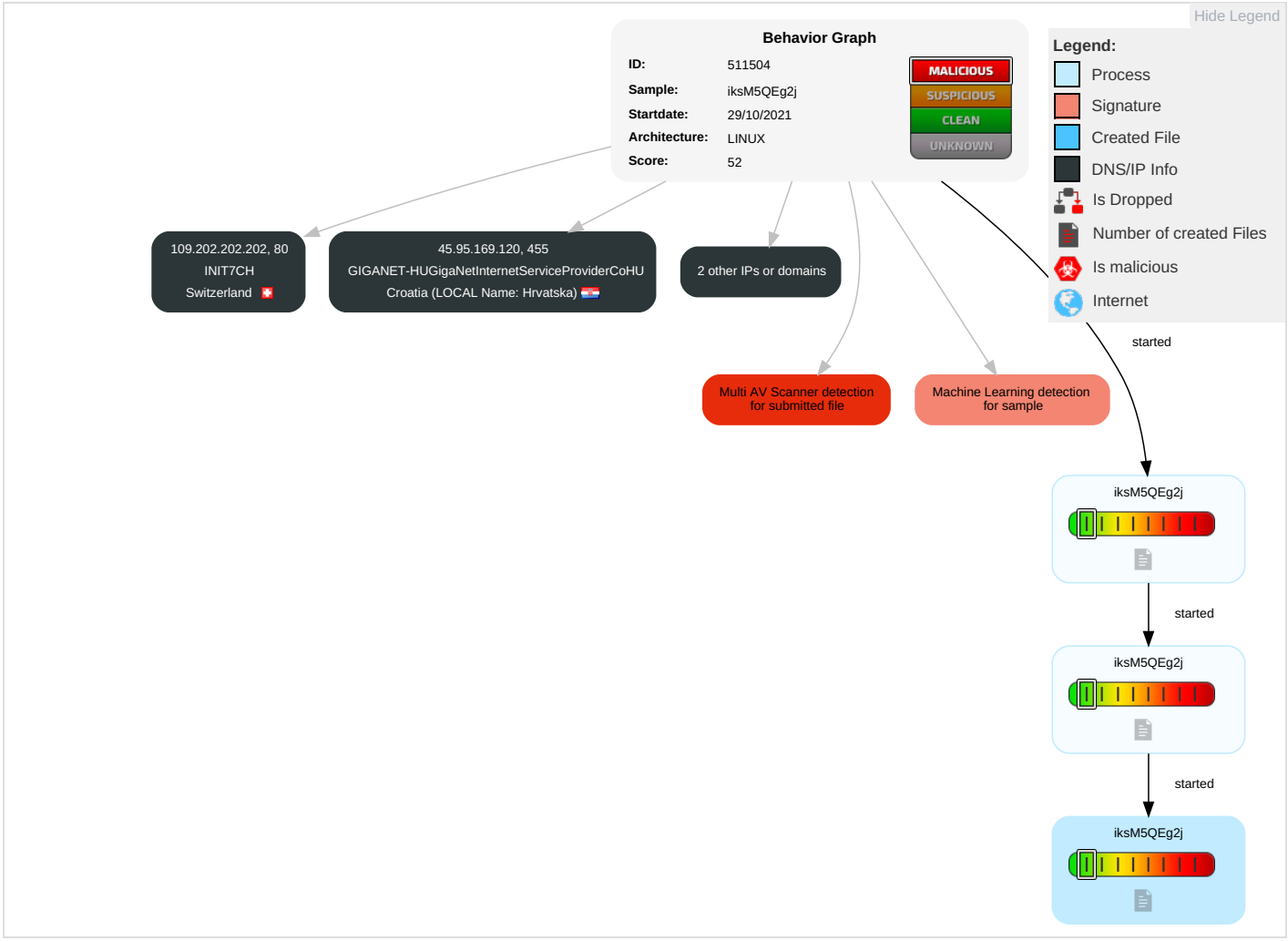
Mitre Att&ck Matrix

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	Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Malware Configuration

No configs have been found

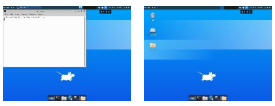
Behavior Graph

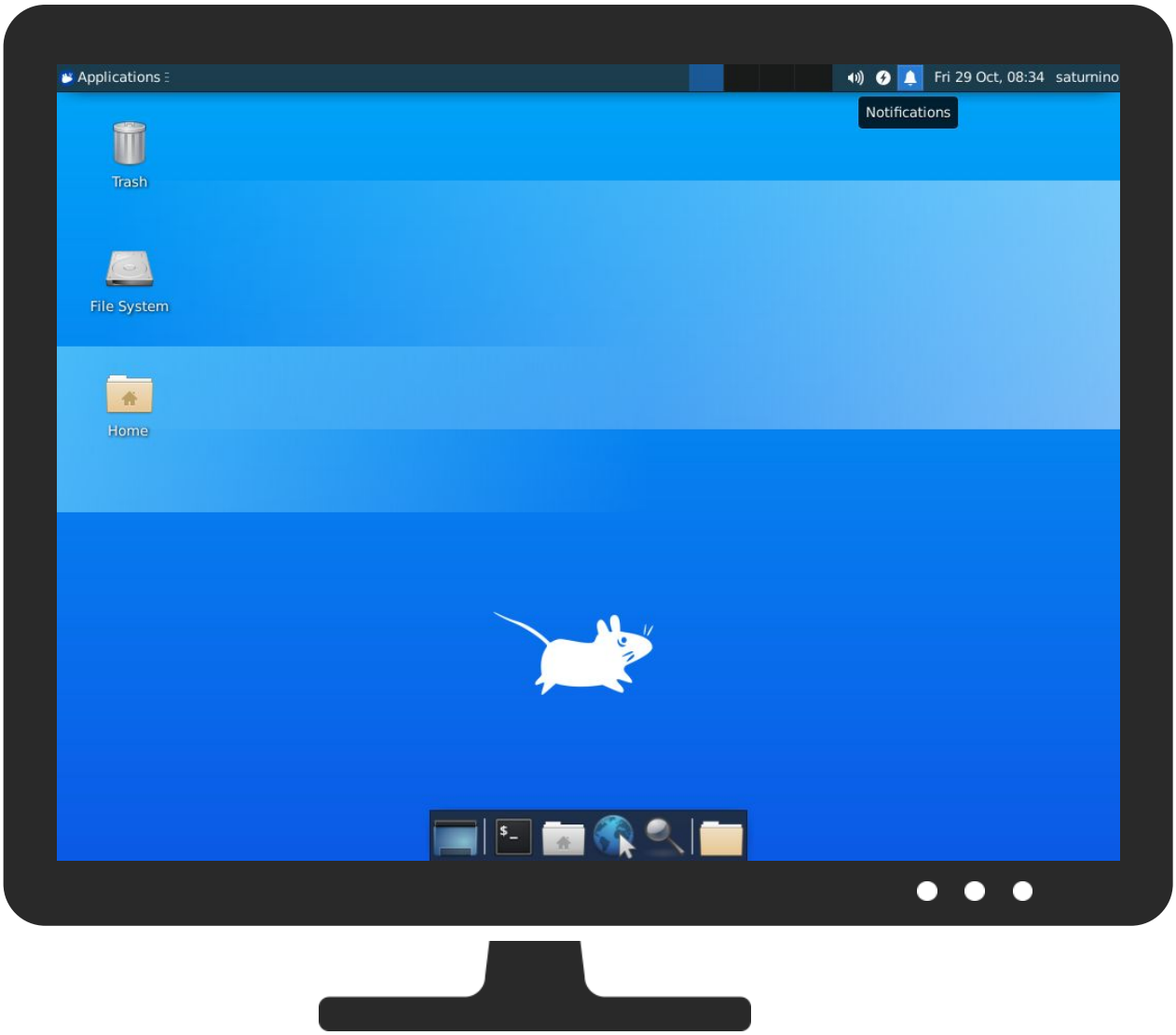


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
iksM5QEg2j	27%	Virustotal		Browse
iksM5QEg2j	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.95.169.120	unknown	Croatia (LOCAL Name: Hrvatska)		42864	GIGANET-HUGigaNetInternetServiceProviderCoHU	false
109.202.202.202	unknown	Switzerland		13030	INIT7CH	false
91.189.91.43	unknown	United Kingdom		41231	CANONICAL-ASGB	false
91.189.91.42	unknown	United Kingdom		41231	CANONICAL-ASGB	false

Runtime Messages

Command:	/tmp/iksM5QEg2j
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
109.202.202.202	lGJEkz80oe	Get hash	malicious	Browse	
	roV7kGaVr1	Get hash	malicious	Browse	
	SecuriteInfo.com.Linux.Siggen.4218.298.3210	Get hash	malicious	Browse	
	uPOWBxniTA	Get hash	malicious	Browse	
	qy5unieRgR	Get hash	malicious	Browse	
	sAzPpn6mKZ	Get hash	malicious	Browse	
	AxadDC89j9	Get hash	malicious	Browse	
	ZErnXU2XR1	Get hash	malicious	Browse	
	sTHJvS5LPJ	Get hash	malicious	Browse	
	THzHjYQ4z6	Get hash	malicious	Browse	
	jC0B6sMh1d	Get hash	malicious	Browse	
	JoLmvC65B7	Get hash	malicious	Browse	
	AOaKSm1cij	Get hash	malicious	Browse	
	Mozi.a	Get hash	malicious	Browse	
	ggbMKQDdG2	Get hash	malicious	Browse	
	SecuriteInfo.com.Linux.Siggen.4218.31606.9155	Get hash	malicious	Browse	
	AbriuSDkeL	Get hash	malicious	Browse	
	xjmPNreY8I	Get hash	malicious	Browse	
	u7kjf23xQc	Get hash	malicious	Browse	
	nrT4coM180	Get hash	malicious	Browse	
91.189.91.43	lGJEkz80oe	Get hash	malicious	Browse	
	roV7kGaVr1	Get hash	malicious	Browse	
	SecuriteInfo.com.Linux.Siggen.4218.298.3210	Get hash	malicious	Browse	
	uPOWBxniTA	Get hash	malicious	Browse	
	qy5unieRgR	Get hash	malicious	Browse	
	sAzPpn6mKZ	Get hash	malicious	Browse	
	AxadDC89j9	Get hash	malicious	Browse	
	ZErnXU2XR1	Get hash	malicious	Browse	
	sTHJvS5LPJ	Get hash	malicious	Browse	
	THzHjYQ4z6	Get hash	malicious	Browse	
	jC0B6sMh1d	Get hash	malicious	Browse	
	JoLmvC65B7	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	AOaKSm1cij	Get hash	malicious	Browse	
	Mozi.a	Get hash	malicious	Browse	
	ggbMKQDdG2	Get hash	malicious	Browse	
	SecuriteInfo.com.Linux.Siggen.4218.31606.9155	Get hash	malicious	Browse	
	AbriuSDkeL	Get hash	malicious	Browse	
	xjmPNreY8l	Get hash	malicious	Browse	
	u7kjf23xQc	Get hash	malicious	Browse	
	nrT4coM180	Get hash	malicious	Browse	
91.189.91.42	lGJEkz80oe	Get hash	malicious	Browse	
	roV7kGaVr1	Get hash	malicious	Browse	
	SecuriteInfo.com.Linux.Siggen.4218.298.3210	Get hash	malicious	Browse	
	uPOWBxniTA	Get hash	malicious	Browse	
	qy5unieRgR	Get hash	malicious	Browse	
	sAzPpn6mKZ	Get hash	malicious	Browse	
	AxadDC89j9	Get hash	malicious	Browse	
	ZErnXU2XR1	Get hash	malicious	Browse	
	sTHJvS5LPJ	Get hash	malicious	Browse	
	THzHjYQ4z6	Get hash	malicious	Browse	
	jC0B6sMh1d	Get hash	malicious	Browse	
	JoLmvC65B7	Get hash	malicious	Browse	
	AOaKSm1cij	Get hash	malicious	Browse	
	Mozi.a	Get hash	malicious	Browse	
	ggbMKQDdG2	Get hash	malicious	Browse	
	SecuriteInfo.com.Linux.Siggen.4218.31606.9155	Get hash	malicious	Browse	
	AbriuSDkeL	Get hash	malicious	Browse	
	xjmPNreY8l	Get hash	malicious	Browse	
	u7kjf23xQc	Get hash	malicious	Browse	
	nrT4coM180	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CANONICAL-ASGB	lGJEkz80oe	Get hash	malicious	Browse	• 91.189.91.42
	roV7kGaVr1	Get hash	malicious	Browse	• 91.189.91.42
	SecuriteInfo.com.Linux.Siggen.4218.298.3210	Get hash	malicious	Browse	• 91.189.91.42
	uPOWBxniTA	Get hash	malicious	Browse	• 91.189.91.42
	qy5unieRgR	Get hash	malicious	Browse	• 91.189.91.42
	sAzPpn6mKZ	Get hash	malicious	Browse	• 91.189.91.42
	AxadDC89j9	Get hash	malicious	Browse	• 91.189.91.42
	ZErnXU2XR1	Get hash	malicious	Browse	• 91.189.91.42
	sTHJvS5LPJ	Get hash	malicious	Browse	• 91.189.91.42
	THzHjYQ4z6	Get hash	malicious	Browse	• 91.189.91.42
	jC0B6sMh1d	Get hash	malicious	Browse	• 91.189.91.42
	JoLmvC65B7	Get hash	malicious	Browse	• 91.189.91.42
	AOaKSm1cij	Get hash	malicious	Browse	• 91.189.91.42
	Mozi.a	Get hash	malicious	Browse	• 91.189.91.42
	ggbMKQDdG2	Get hash	malicious	Browse	• 91.189.91.42
	SecuriteInfo.com.Linux.Siggen.4218.31606.9155	Get hash	malicious	Browse	• 91.189.91.42
	AbriuSDkeL	Get hash	malicious	Browse	• 91.189.91.42
	xjmPNreY8l	Get hash	malicious	Browse	• 91.189.91.42
	u7kjf23xQc	Get hash	malicious	Browse	• 91.189.91.42
	nrT4coM180	Get hash	malicious	Browse	• 91.189.91.42
GIGANET-HUGigaNetInternetServiceProviderCoHU	RicwIfIHLK	Get hash	malicious	Browse	• 45.95.169.115
	aIY7AxjUMc	Get hash	malicious	Browse	• 45.95.169.115
	DtJmFQxtNC	Get hash	malicious	Browse	• 45.95.169.115
	Wm4CzOCmNY	Get hash	malicious	Browse	• 45.95.169.115
	vunWUzXJvC	Get hash	malicious	Browse	• 45.95.169.115
	52xhBHy9Wz	Get hash	malicious	Browse	• 45.95.169.115
	YGvwG0iCDE	Get hash	malicious	Browse	• 45.95.169.115
	dbd5O0RUTq	Get hash	malicious	Browse	• 45.95.169.115

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	fHVDVj0pzO	Get hash	malicious	Browse	• 45.95.169.115
	eZPk7Fg5w7	Get hash	malicious	Browse	• 45.95.169.115
	ph5PjoFBpj	Get hash	malicious	Browse	• 45.95.169.115
	xugAk5haat	Get hash	malicious	Browse	• 45.95.169.115
	0jEbWQtzs0	Get hash	malicious	Browse	• 45.95.169.115
	8g3tc5SWwB	Get hash	malicious	Browse	• 92.52.211.220
	7okgnZjK06	Get hash	malicious	Browse	• 45.95.169.115
	D9efs9TYvN	Get hash	malicious	Browse	• 45.95.169.115
	LlE7nUUjmA	Get hash	malicious	Browse	• 45.95.169.115
	3HwsuWd7at	Get hash	malicious	Browse	• 45.95.169.115
	XOg0GKdALN	Get hash	malicious	Browse	• 45.95.169.115
	2VSJDSxulv	Get hash	malicious	Browse	• 45.95.169.115
INIT7CH	lGJEkz80oe	Get hash	malicious	Browse	• 109.202.202.202
	roV7kGaVr1	Get hash	malicious	Browse	• 109.202.202.202
	SecuriteInfo.com.Linux.Siggen.4218.298.3210	Get hash	malicious	Browse	• 109.202.202.202
	uPOWBxniTA	Get hash	malicious	Browse	• 109.202.202.202
	qy5unieRgR	Get hash	malicious	Browse	• 109.202.202.202
	sAzPpn6mKZ	Get hash	malicious	Browse	• 109.202.202.202
	AxadDC89j9	Get hash	malicious	Browse	• 109.202.202.202
	ZErnXU2XR1	Get hash	malicious	Browse	• 109.202.202.202
	sTHJvS5LPJ	Get hash	malicious	Browse	• 109.202.202.202
	THzHjYQ4z6	Get hash	malicious	Browse	• 109.202.202.202
	jC0B6sMh1d	Get hash	malicious	Browse	• 109.202.202.202
	JoLmvC65B7	Get hash	malicious	Browse	• 109.202.202.202
	AOaKSm1cij	Get hash	malicious	Browse	• 109.202.202.202
	Mozi.a	Get hash	malicious	Browse	• 109.202.202.202
	ggbMKQDdG2	Get hash	malicious	Browse	• 109.202.202.202
	SecuriteInfo.com.Linux.Siggen.4218.31606.9155	Get hash	malicious	Browse	• 109.202.202.202
	AbriuSDkeL	Get hash	malicious	Browse	• 109.202.202.202
	xjmPNreY8l	Get hash	malicious	Browse	• 109.202.202.202
	u7kjf23xQc	Get hash	malicious	Browse	• 109.202.202.202
	nrT4coM180	Get hash	malicious	Browse	• 109.202.202.202

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):	6.216846948570903
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	iksM5QEg2j
File size:	34032
MD5:	d5f7312f62ca02ad0873bdd213dd71be
SHA1:	d157216923829b73f69c4db6cf6d6bf80edd4962
SHA256:	752b21a8ab77df1640dade907ad8268990665e0b00a3909b1bf19a23ef8c0770
SHA512:	b047436a6b9a89b3126e5d95ff6ace8d42985780620d0a7ee2b65e53590de0db5a06f33f2a0cc7fc5d6fd8ce929e16b56134509a1fec59bc1bd46da714673ed0
SSDEEP:	384:fXxT87+xyCCy/hGAzz9H/wm1h9+Ezq7H8OOhPWMq:/xT87+M0Xfwm0EzqD8OkOl
File Content Preview:	.ELF.....d...4...`.....4. ...(.....h...h.....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
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	33632
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	0x6046	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x804e0f6	0x60f6	0x17	0x0	0x6	AX	0	0	1
.rodata	PROGBITS	0x804e120	0x6120	0x760	0x0	0x2	A	0	0	32
.ctors	PROGBITS	0x804f000	0x7000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x804f008	0x7008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x804f020	0x7020	0x1300	0x0	0x3	WA	0	0	32
.bss	NOBITS	0x8050320	0x8320	0x1580	0x0	0x3	WA	0	0	32
.shstrtab	STRTAB	0x0	0x8320	0x3e	0x0	0x0		0	0	1

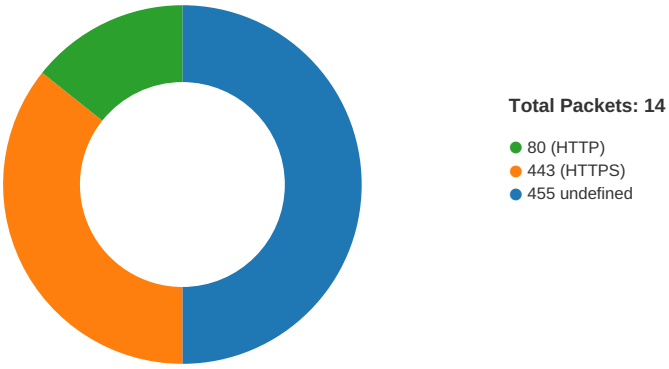
Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8048000	0x8048000	0x6880	0x6880	3.8450	0x5	R E	0x1000		.init .text .fini .rodata
LOAD	0x7000	0x804f000	0x804f000	0x1320	0x28a0	1.7047	0x6	RW	0x1000		.ctors .dtors .data .bss

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



TCP Packets

System Behavior

Analysis Process: iksM5QEg2j PID: 5236 Parent PID: 5112

General

Start time:	08:34:26
Start date:	29/10/2021
Path:	/tmp/iksM5QEg2j
Arguments:	/tmp/iksM5QEg2j
File size:	34032 bytes
MD5 hash:	d5f7312f62ca02ad0873bdd213dd71be

Analysis Process: iksM5QEg2j PID: 5237 Parent PID: 5236

General

Start time:	08:34:26
Start date:	29/10/2021
Path:	/tmp/iksM5QEg2j
Arguments:	n/a
File size:	34032 bytes
MD5 hash:	d5f7312f62ca02ad0873bdd213dd71be

Analysis Process: iksM5QEg2j PID: 5238 Parent PID: 5237

General

Start time:	08:34:26
Start date:	29/10/2021
Path:	/tmp/iksM5QEg2j
Arguments:	n/a
File size:	34032 bytes
MD5 hash:	d5f7312f62ca02ad0873bdd213dd71be

File Activities

File Read

Directory Enumerated