ID: 533079
Sample Name: beamer.x86-20211202-2350
Cookbook: defaultlinuxfilecookbook.jbs
Time: 01:01:18
Date: 03/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

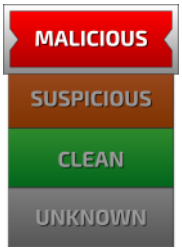
Linux Analysis Report beamer.x86-20211202-2350

Overview

General Information

Sample Name:	beamer.x86-20211202-2350
Analysis ID:	533079
MD5:	04e178a6fe92b38.
SHA1:	ba0e9885d26309..
SHA256:	1000ab055531e0..
Infos:	

Detection

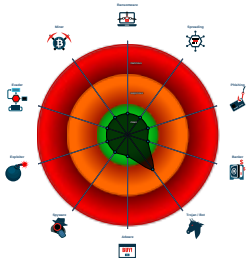


Score:	52
Range:	0 - 100
Whitelisted:	false

Signatures

- Multi AV Scanner detection for subm…
- Machine Learning detection for samp…
- Tries to connect to HTTP servers, b…
- Detected TCP or UDP traffic on non…
- Executes the "rm" command used to…
- Sample has stripped symbol table
- Sample contains strings indicative o…

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:	533079
Start date:	03.12.2021
Start time:	01:01:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	beamer.x86-20211202-2350
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.linX86-20211202-2350@0/0@0/0

Process Tree

- **system is lnxubuntu20**
- beamer.x86-20211202-2350 (PID: 5212, Parent: 5115, MD5: 04e178a6fe92b38222e03a4c2e2303e0) Arguments: /tmp/beamer.x86-20211202-2350
  - beamer.x86-20211202-2350 New Fork (PID: 5213, Parent: 5212)
  - beamer.x86-20211202-2350 New Fork (PID: 5214, Parent: 5212)
  - beamer.x86-20211202-2350 New Fork (PID: 5215, Parent: 5212)
- dash New Fork (PID: 5253, Parent: 4331)
- rm (PID: 5253, Parent: 4331, MD5: aa2b5496fdbfd88e38791ab81f90b95b) Arguments: rm -f /tmp/tmp.AlKkHgaC4m /tmp/tmp.GpcnZvv7fC /tmp/tmp.zmqkJtmHaS
- **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

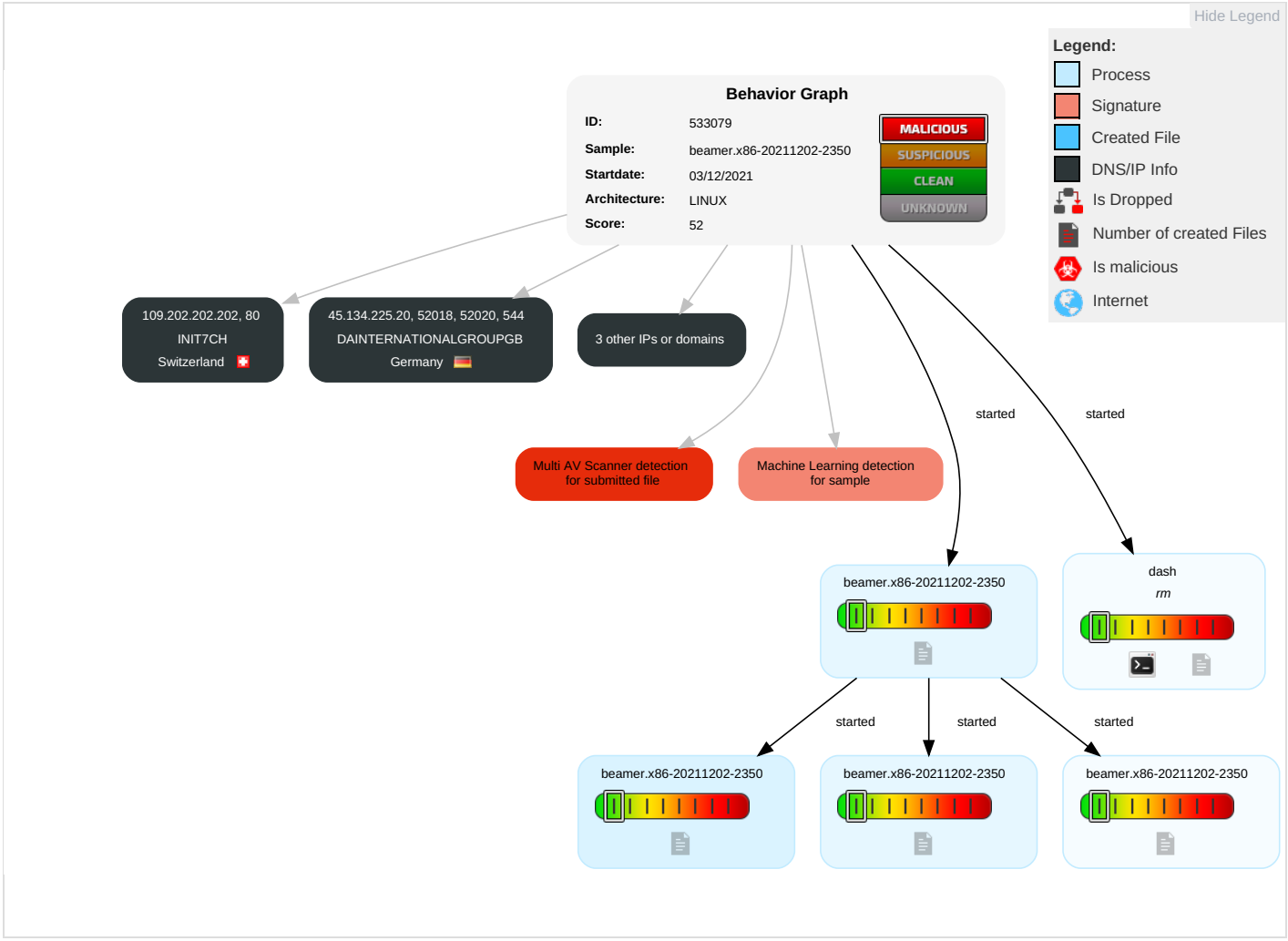
Mitre Att&ck Matrix

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	File Deletion 1	OS Credential Dumping	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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
beamer.x86-20211202-2350	24%	Virustotal		Browse
beamer.x86-20211202-2350	31%	ReversingLabs	Linux.Trojan.Mirai	
beamer.x86-20211202-2350	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
45.134.225.20	unknown	Germany		203380	DAINTERNATIONALGROUPGB	false
34.249.145.219	unknown	United States		16509	AMAZON-02US	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/beamer.x86-20211202-2350
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
45.134.225.20	beamer.arm7-20211202-2350	Get hash	malicious	Browse	
	beamer.arm-20211202-2350	Get hash	malicious	Browse	
	fAS1IqIeKJ	Get hash	malicious	Browse	
	q6L054nmNP	Get hash	malicious	Browse	
	rNroDrxDX8	Get hash	malicious	Browse	
	a13lg45BBF	Get hash	malicious	Browse	
	HdxaOdBHLy	Get hash	malicious	Browse	
	SianBf68ns	Get hash	malicious	Browse	
	j22Vry7PQB	Get hash	malicious	Browse	
	jJ1l2W978w	Get hash	malicious	Browse	
	VSE57F94Eu	Get hash	malicious	Browse	
	95dSetGliK	Get hash	malicious	Browse	
	H7MTKzOUnc	Get hash	malicious	Browse	
	z0sDGe1HWt	Get hash	malicious	Browse	
	bx8ZRDTbie	Get hash	malicious	Browse	
	HOi5DIja39	Get hash	malicious	Browse	
	KXcyJaK55a	Get hash	malicious	Browse	
	beamer.x86	Get hash	malicious	Browse	
	beamer.arm	Get hash	malicious	Browse	
34.249.145.219	beamer.arm-20211202-2350	Get hash	malicious	Browse	
	PQPv91RexG	Get hash	malicious	Browse	
	RIE3BrH6X4	Get hash	malicious	Browse	
	tlKkI7uWcu	Get hash	malicious	Browse	
	nbGnA0iX0e	Get hash	malicious	Browse	
	VvUgZxfzqG	Get hash	malicious	Browse	
	Vc90gP8W1b	Get hash	malicious	Browse	
	tJaSWmeCjd	Get hash	malicious	Browse	
	2MzNonluPU	Get hash	malicious	Browse	
	jew.x86-20211122-1350	Get hash	malicious	Browse	
	xwbqdTFD93	Get hash	malicious	Browse	
	i686	Get hash	malicious	Browse	
	sw10l80cO2	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	JTHn81Q2S2	Get hash	malicious	Browse	
	SecuriteInfo.com.Linux.BackDoor.Fgt.3841.14881.20899	Get hash	malicious	Browse	
	6ZIiJTDBft	Get hash	malicious	Browse	
	5vYAnApKPH	Get hash	malicious	Browse	
	ByutK666RH	Get hash	malicious	Browse	
	2m6GYRpRq2	Get hash	malicious	Browse	
	NJY9kuGznp	Get hash	malicious	Browse	
109.202.202.202	beamer.arm7-20211202-2350	Get hash	malicious	Browse	
	beamer.arm-20211202-2350	Get hash	malicious	Browse	
	a-r.m-4.Sakura	Get hash	malicious	Browse	
	a-r.m-5.Sakura	Get hash	malicious	Browse	
	x-8.6-.Sakura	Get hash	malicious	Browse	
	x-3.2-.Sakura	Get hash	malicious	Browse	
	Mo7tMkRLVz	Get hash	malicious	Browse	
	m-p.s-l.Sakura	Get hash	malicious	Browse	
	m-i.p-s.Sakura	Get hash	malicious	Browse	
	mirai.arm7	Get hash	malicious	Browse	
	eh.arm7-20211202-2050	Get hash	malicious	Browse	
	eh.x86-20211202-2050	Get hash	malicious	Browse	
	eh.arm-20211202-2050	Get hash	malicious	Browse	
	mirai.arm	Get hash	malicious	Browse	
	RAyX4iU3dy	Get hash	malicious	Browse	
	oeOZvHnuaU	Get hash	malicious	Browse	
	nYdomnUtHq	Get hash	malicious	Browse	
	peon7hY4z4	Get hash	malicious	Browse	
	y4yhQj9Eff	Get hash	malicious	Browse	
	qHBU9CAlTZ	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAINTERNATIONALGROUPGB	beamer.arm7-20211202-2350	Get hash	malicious	Browse	• 45.134.225.20
	beamer.arm-20211202-2350	Get hash	malicious	Browse	• 45.134.225.20
	fAS1IqIeKJ	Get hash	malicious	Browse	• 45.134.225.20
	q6L054nmNP	Get hash	malicious	Browse	• 45.134.225.20
	rNroDrxDX8	Get hash	malicious	Browse	• 45.134.225.20
	a13lg45BBF	Get hash	malicious	Browse	• 45.134.225.20
	HdxaOdBHLy	Get hash	malicious	Browse	• 45.134.225.20
	SianBf68ns	Get hash	malicious	Browse	• 45.134.225.20
	j22Vry7PQB	Get hash	malicious	Browse	• 45.134.225.20
	jJ1l2W978w	Get hash	malicious	Browse	• 45.134.225.20
	VSE57F94Eu	Get hash	malicious	Browse	• 45.134.225.20
	N6y7A7R9wg.exe	Get hash	malicious	Browse	• 45.134.225.35
	2b0519e3978cea744b220f109077b4b012dc4e9856be8.exe	Get hash	malicious	Browse	• 45.134.225.35
	95dSetGliK	Get hash	malicious	Browse	• 45.134.225.20
	H7MTKzOUnc	Get hash	malicious	Browse	• 45.134.225.20
	z0sDGe1HWt	Get hash	malicious	Browse	• 45.134.225.20
	bx8ZRDTbie	Get hash	malicious	Browse	• 45.134.225.20
	HOi5DIja39	Get hash	malicious	Browse	• 45.134.225.20
	KXcyJaK55a	Get hash	malicious	Browse	• 45.134.225.20
	beamer.x86	Get hash	malicious	Browse	• 45.134.225.20
AMAZON-02US	beamer.arm-20211202-2350	Get hash	malicious	Browse	• 34.249.145.219
	a-r.m-4.Sakura	Get hash	malicious	Browse	• 54.171.230.55
	GenoSec.arm7	Get hash	malicious	Browse	• 176.34.166.240
	S2pmCqOFEf.exe	Get hash	malicious	Browse	• 52.216.166.67
	12.dll	Get hash	malicious	Browse	• 13.225.75.74
	NVTNgwAjOK	Get hash	malicious	Browse	• 54.102.91.74
	lAe63MagsK	Get hash	malicious	Browse	• 13.233.103.244
	GenoSec.x86	Get hash	malicious	Browse	• 198.251.13 7.253

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	HackLoader.exe	Get hash	malicious	Browse	• 52.217.109.12
	mirai.x86	Get hash	malicious	Browse	• 44.224.113.150
	Yoshi.x86-20211202-2050	Get hash	malicious	Browse	• 13.52.72.80
	7009.xlsx	Get hash	malicious	Browse	• 13.250.31.113
	invoice dhl.delivery document and original invoice sign.exe	Get hash	malicious	Browse	• 44.227.76.166
	oeOZvHnuaU	Get hash	malicious	Browse	• 54.171.230.55
	Milleniumbpc.xlsx	Get hash	malicious	Browse	• 44.231.165.140
	PQPv91RexG	Get hash	malicious	Browse	• 34.249.145.219
	WAYBILL 44 7611 9546 - Joao Carlos.exe	Get hash	malicious	Browse	• 75.2.115.196
	HBL No_PZU100035300.xlsx	Get hash	malicious	Browse	• 3.64.163.50
	ufKi6DmWMQCuEb4.exe	Get hash	malicious	Browse	• 3.108.154.143
	yVvATSvedsfMg0l.exe	Get hash	malicious	Browse	• 3.64.163.50

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):	6.469954580077168
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	beamer.x86-20211202-2350
File size:	42164
MD5:	04e178a6fe92b38222e03a4c2e2303e0
SHA1:	ba0e9885d263093c13e955cb79cf6e86039d4177
SHA256:	1000ab055531e011407b62ff66cc2b122334eb14dc01f56f9487023beeb38f59
SHA512:	a698ac1122eeed10d8785d6543bb9fcab3b99a99ead80f69b1a6b04594c9681272d1b8a95d016fc0239b8cc60f1f2633884703bcabbce1c35df6c6816ed5679c
SSDEEP:	768:fDQqegtrUdSHBnMslsWcBUxUBCFJoTR3CjeYnBnCLMiZ8USCIy:7QqegtIdShZIBfBC8DYnJuMiTSC
File Content Preview:	.ELF.....d...4...$.....4. ...(..... ....(.....Q.td.....U..S.....w...h....3...[]...$.....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

ELF header

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:	41764
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

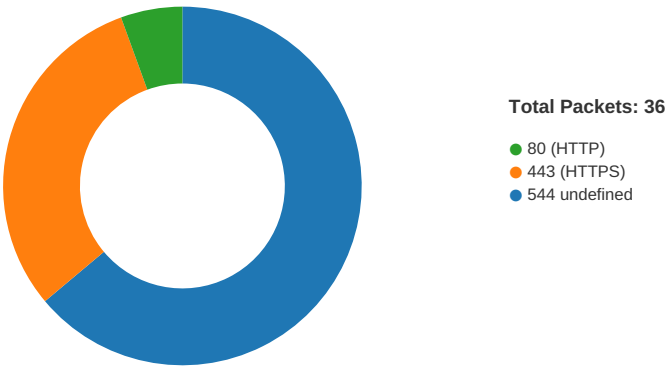
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x8048094	0x94	0x1c	0x0	0x6	AX	0	0	1
.text	PROGBITS	0x80480b0	0xb0	0x8256	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x8050306	0x8306	0x17	0x0	0x6	AX	0	0	1
.rodata	PROGBITS	0x8050320	0x8320	0x19fc	0x0	0x2	A	0	0	32
.ctors	PROGBITS	0x8052000	0xa000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x8052008	0xa008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x8052020	0xa020	0x2c4	0x0	0x3	WA	0	0	32
.bss	NOBITS	0x8052300	0xa2e4	0x25a0	0x0	0x3	WA	0	0	32
.shstrtab	STRTAB	0x0	0xa2e4	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	0x9d1c	0x9d1c	4.1761	0x5	R E	0x1000		.init .text .fini .rodata
LOAD	0xa000	0x8052000	0x8052000	0x2e4	0x28a0	2.6149	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

System Behavior

Analysis Process: beamer.x86-20211202-2350 PID: 5212 Parent PID: 5115

General

Start time:	01:02:02
Start date:	03/12/2021
Path:	/tmp/beamer.x86-20211202-2350
Arguments:	/tmp/beamer.x86-20211202-2350
File size:	42164 bytes
MD5 hash:	04e178a6fe92b38222e03a4c2e2303e0

Analysis Process: beamer.x86-20211202-2350 PID: 5213 Parent PID: 5212

General

Start time:	01:02:02
Start date:	03/12/2021
Path:	/tmp/beamer.x86-20211202-2350
Arguments:	n/a
File size:	42164 bytes
MD5 hash:	04e178a6fe92b38222e03a4c2e2303e0

File Activities

Directory Enumerated

Analysis Process: beamer.x86-20211202-2350 PID: 5214 Parent PID: 5212

General

Start time:	01:02:02
Start date:	03/12/2021
Path:	/tmp/beamer.x86-20211202-2350
Arguments:	n/a
File size:	42164 bytes
MD5 hash:	04e178a6fe92b38222e03a4c2e2303e0

Analysis Process: beamer.x86-20211202-2350 PID: 5215 Parent PID: 5212

General

Start time:	01:02:02
Start date:	03/12/2021
Path:	/tmp/beamer.x86-20211202-2350
Arguments:	n/a
File size:	42164 bytes
MD5 hash:	04e178a6fe92b38222e03a4c2e2303e0

Analysis Process: dash PID: 5253 Parent PID: 4331

General

Start time:	01:03:25
Start date:	03/12/2021

Path:	/usr/bin/dash
Arguments:	n/a
File size:	129816 bytes
MD5 hash:	1e6b1c887c59a315edb7eb9a315fc84c

Analysis Process: rm PID: 5253 Parent PID: 4331

General

Start time:	01:03:25
Start date:	03/12/2021
Path:	/usr/bin/rm
Arguments:	rm -f /tmp/tmp.AlKkHgaC4m /tmp/tmp.GpcnZvv7fC /tmp/tmp.zmqkJtmHaS
File size:	72056 bytes
MD5 hash:	aa2b5496fdbfd88e38791ab81f90b95b

File Activities

File Deleted

File Read