ID: 512691
Sample Name: BitmCvTrdO
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 10:31:21
Date: 01/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

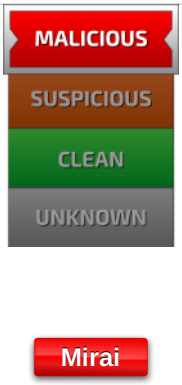
Linux Analysis Report BitmCvTrdO

Overview

General Information

Sample Name:	BitmCvTrdO
Analysis ID:	512691
MD5:	83f51eab5d7a359.
SHA1:	3fa59c483662eff…
SHA256:	9ae7441ecbce9e..
Tags:	32 elf mirai sparc
Infos:	

Detection

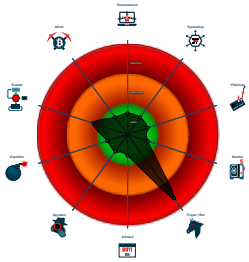


Score:	80
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e….
- Yara detected Mirai
- Multi AV Scanner detection for subm…
- Uses known network protocols on no…
- Connects to many ports of the same…
- Sample has stripped symbol table
- HTTP GET or POST without a user …
- Uses the "uname" system call to qu…
- 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

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	512691
Start date:	01.11.2021
Start time:	10:31:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	BitmCvTrdO
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:	mal80.troj.lin@0/0@0/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- BitmCvTrdO (PID: 5233, Parent: 5112, MD5: 7dc1c0e23cd5e102bb12e5c29403410e) Arguments: /tmp/BitmCvTrdO
  - BitmCvTrdO New Fork (PID: 5235, Parent: 5233)
    - BitmCvTrdO New Fork (PID: 5240, Parent: 5235)
    - BitmCvTrdO New Fork (PID: 5241, Parent: 5235)
      - BitmCvTrdO New Fork (PID: 5246, Parent: 5241)
        - BitmCvTrdO New Fork (PID: 5268, Parent: 5246)
        - BitmCvTrdO New Fork (PID: 5271, Parent: 5246)
        - BitmCvTrdO New Fork (PID: 5272, Parent: 5246)
        - BitmCvTrdO New Fork (PID: 5273, Parent: 5246)
      - BitmCvTrdO New Fork (PID: 5256, Parent: 5241)
      - BitmCvTrdO New Fork (PID: 5269, Parent: 5241)
      - BitmCvTrdO New Fork (PID: 5278, Parent: 5241)
      - BitmCvTrdO New Fork (PID: 5280, Parent: 5241)
  - BitmCvTrdO New Fork (PID: 5236, Parent: 5233)
  - BitmCvTrdO New Fork (PID: 5237, Parent: 5233)
    - BitmCvTrdO New Fork (PID: 5244, Parent: 5237)
      - BitmCvTrdO New Fork (PID: 5260, Parent: 5244)
      - BitmCvTrdO New Fork (PID: 5261, Parent: 5244)
      - BitmCvTrdO New Fork (PID: 5262, Parent: 5244)
      - BitmCvTrdO New Fork (PID: 5264, Parent: 5244)
    - BitmCvTrdO New Fork (PID: 5247, Parent: 5237)
    - BitmCvTrdO New Fork (PID: 5248, Parent: 5237)
    - BitmCvTrdO New Fork (PID: 5251, Parent: 5237)
    - BitmCvTrdO New Fork (PID: 5257, Parent: 5237)
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
BitmCvTrdO	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

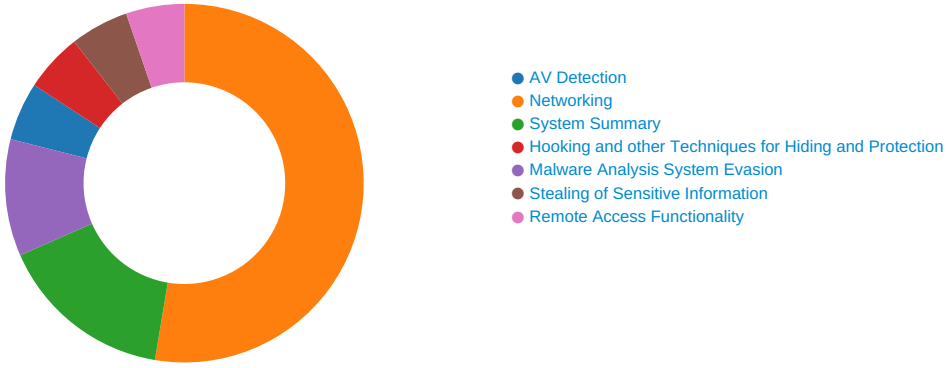
PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
5236.1.00000000a7ecdb85.000000008504b126.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5268.1.00000000a7ecdb85.000000008504b126.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5233.1.00000000a7ecdb85.000000008504b126.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5256.1.00000000a7ecdb85.000000008504b126.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5235.1.00000000a7ecdb85.000000008504b126.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
Click to see the 3 entries				

Jbx Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Uses known network protocols on non-standard ports

Connects to many ports of the same IP (likely port scanning)

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

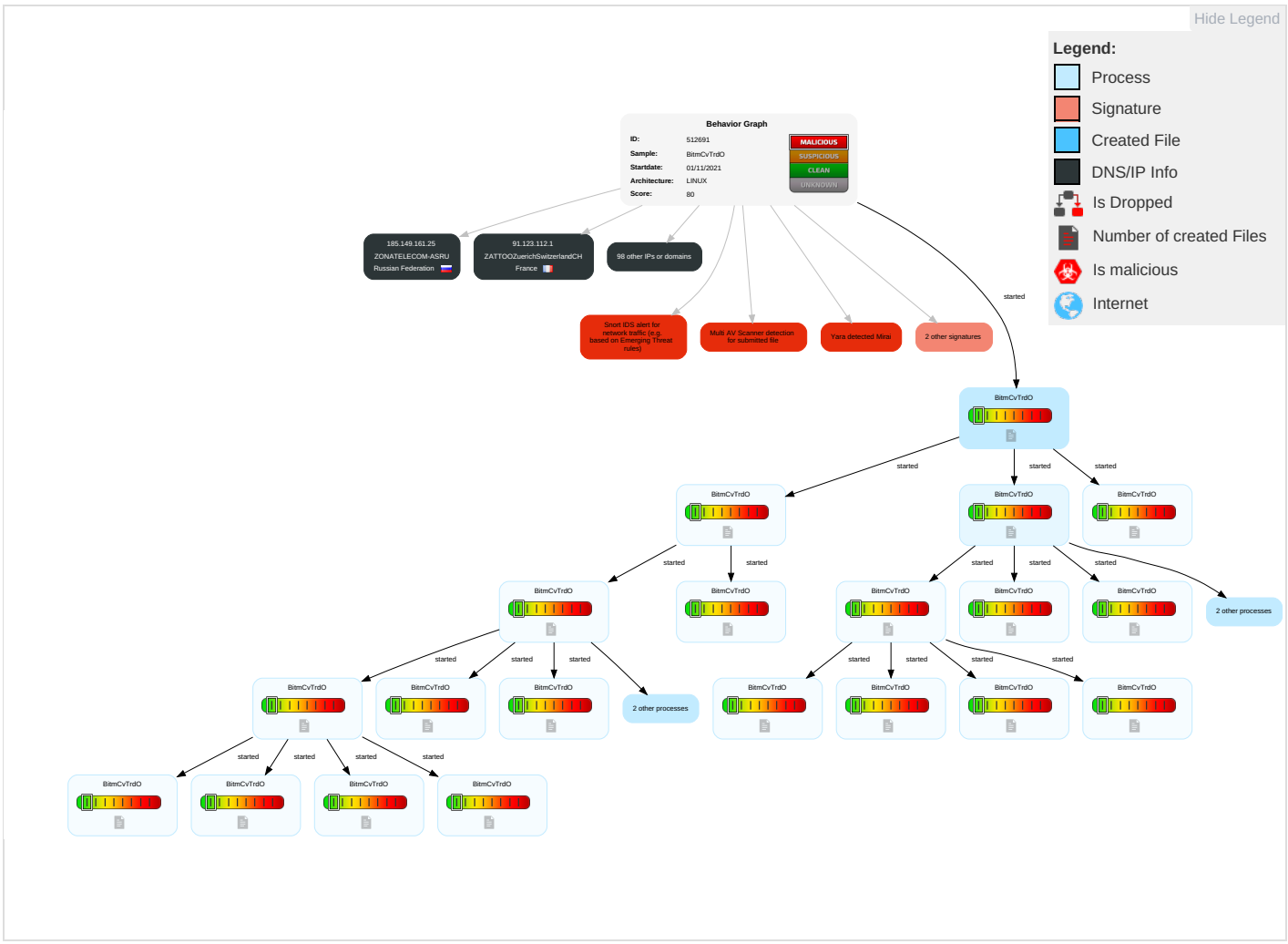
Mitre Att&ck Matrix

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	Direct Volume Access	OS Credential Dumping	Security Software Discovery 1 1	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 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
BitmCvTrdO	54%	Virustotal		Browse

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:52869/picdesc.xml	0%	Virustotal		Browse
http://127.0.0.1:52869/picdesc.xml	0%	Avira URL Cloud	safe	
http://127.0.0.1:52869/wanipcn.xml	0%	Virustotal		Browse
http://127.0.0.1:52869/wanipcn.xml	0%	Avira URL Cloud	safe	
http://194.87.42.3/Anti_Bins/Antisocial.mips	11%	Virustotal		Browse
http://194.87.42.3/Anti_Bins/Antisocial.mips	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:52869/picdesc.xml	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://127.0.0.1:52869/wanipcn.xml	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.49.104.4	unknown	Iran (ISLAMIC Republic Of)		202391	AFRARASAIR	false
45.150.101.140	unknown	Liechtenstein		47987	LOVESERVERSGB	false
45.12.189.19	unknown	United Kingdom		35085	ACORSOFR	false
185.19.109.165	unknown	United Kingdom		17804	LAODC-AS-APLaoDataCenterLA	false
185.58.180.28	unknown	Slovenia		5603	SIOL-NETTelekomSlovenijeddSI	false
45.124.225.9	unknown	India		9381	HKBNES-AS-APHKBNEnterpriseSolutionsHKLimitedHK	false
204.131.144.153	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
147.249.228.28	unknown	United States		6419	IDDUS	false
162.185.219.137	unknown	United States		21928	T-MOBILE-AS21928US	false
87.107.232.225	unknown	Iran (ISLAMIC Republic Of)		41881	FANAVA-ASFanavaGroupCommunicationCoIR	false
45.109.110.157	unknown	Egypt		37069	MOBINILEG	false
185.110.49.220	unknown	Poland		47544	IQPL-ASPL	false
185.69.33.24	unknown	Netherlands		196826	PL-NETTELEKOM-ASNPL	false
91.105.101.232	unknown	Latvia		12578	APOLLO-ASLatviaLV	false
223.88.173.26	unknown	China		24445	CMNET-V4HENAN-AS-APHenanMobileCommunicationsCoLtdCN	false
197.173.155.52	unknown	South Africa		37168	CELL-CZA	false
41.44.233.246	unknown	Egypt		8452	TE-ASTE-ASEG	false
123.210.9.98	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
185.149.161.25	unknown	Russian Federation		61131	ZONATELECOM-ASRU	false
211.6.134.196	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
211.213.138.11	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
128.167.147.23	unknown	United States		1811	CSC-300-AS1810-AS1815US	false
197.166.142.80	unknown	Egypt		24863	LINKdotNET-ASEG	false
45.117.212.38	unknown	India		45194	SIPL-ASSysconInfowayPvtLtdIN	false
185.187.222.154	unknown	Italy		31543	MYNET-ASmyNETgmbhAT	false
138.246.3.225	unknown	Germany		12816	MWN-ASDE	false
45.221.254.25	unknown	Benin		328092	SUD-TELCOM-ASBJ	false
197.4.54.16	unknown	Tunisia		5438	ATI-TN	false
91.90.227.126	unknown	Latvia		24589	TELENETSIA-ASTelenetAUT-NUMpeeringspecificationobject	false
91.52.65.166	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
45.94.158.140	unknown	Ukraine		56851	VPS-UA-ASUA	false
41.24.86.3	unknown	South Africa		36994	Vodacom-VBZA	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.41.19.213	unknown	Norway		199900	ASN-BEDSYSNO	false
91.26.178.48	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
185.69.33.13	unknown	Netherlands		196826	PL-NETTELEKOM-ASNPL	false
202.60.94.153	unknown	Australia		45671	AS45671-NET-AUWholesaleServicesProviderAU	false
45.226.115.240	unknown	Colombia		265861	SISTEMASSATELITALESDECOLOMBIASAESPCO	false
91.11.116.188	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
185.158.165.191	unknown	Netherlands		48635	ASTRALUSNL	false
185.244.103.40	unknown	Estonia		202635	SERVERFARMEE	false
91.179.103.166	unknown	Belgium		5432	PROXIMUS-ISP-ASBE	false
34.181.181.15	unknown	United States		2686	ATGS-MMD-ASUS	false
185.156.114.155	unknown	Norway		8896	XFIBER-ASNO	false
185.50.154.141	unknown	United Kingdom		50203	UK-REYNOLDS-ASNGB	false
45.130.62.156	unknown	Israel		60781	LEASEWEB-NL-AMS-01NetherlandsNL	false
185.69.33.50	unknown	Netherlands		196826	PL-NETTELEKOM-ASNPL	false
197.114.121.159	unknown	Algeria		36947	ALGTEL-ASDZ	false
185.132.166.208	unknown	Spain		29119	SERVIHOSTING-ASAireNetworksES	false
91.26.178.54	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
211.176.210.238	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
91.199.162.51	unknown	Germany		42652	DELUNETDE	false
185.50.154.135	unknown	United Kingdom		50203	UK-REYNOLDS-ASNGB	false
91.197.220.6	unknown	Ukraine		3326	DATAGROUPDatagroupPJSCUA	false
147.89.189.214	unknown	United Kingdom		559	SWITCHPeeringrequestspeeringswitchchEU	false
119.29.176.65	unknown	China		45090	CNNIC-TENCENT-NET-APShenzhenTencentComputerSystemsCompa	false
185.102.172.184	unknown	Netherlands		7922	COMCAST-7922US	false
197.43.51.137	unknown	Egypt		8452	TE-ASTE-ASEG	false
41.157.30.75	unknown	South Africa		37168	CELL-CZA	false
185.203.160.82	unknown	Iran (ISLAMIC Republic Of)		205837	SADADPSP-ASSadadProcessingModernServicesCompanyPJS	false
45.205.88.132	unknown	Seychelles		54600	PEGTECHINCUS	false
51.174.247.85	unknown	Norway		29695	ALTIBOX_ASNorwayNO	false
185.19.109.135	unknown	United Kingdom		17804	LAODC-AS-APLaoDataCenterLA	false
41.219.191.22	unknown	Nigeria		30998	NAL-ASNG	false
216.221.74.30	unknown	Canada		7992	COGECOWAVECA	false
45.205.88.137	unknown	Seychelles		54600	PEGTECHINCUS	false
91.90.227.103	unknown	Latvia		24589	TELENETSIA-ASTelenetAUT-NUMpeeringspecificationobject	false
209.62.244.171	unknown	United States		32719	BEPC-ASUS	false
49.192.247.41	unknown	Australia		4804	MPX-ASMicroplexPTYLTDAU	false
153.239.66.151	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
185.91.208.152	unknown	Azerbaijan		198193	ASN-TCABLEES	false
91.191.194.2	unknown	Azerbaijan		41997	CONNECT-AS-1AZ	false
155.183.159.155	unknown	United States		37532	ZAMRENZM	false
185.199.120.237	unknown	Serbia		42603	PARKING-SERVIS-ASRS	false
45.11.15.113	unknown	Netherlands		395800	GBTCLOUDUS	false
185.75.12.239	unknown	Spain		201942	SOLTIAES	false
185.222.2.236	unknown	Austria		206091	PLANET-DIGITALAT	false
185.56.176.218	unknown	France		35600	ASN-VEDEGEFR	false
156.223.50.219	unknown	Egypt		8452	TE-ASTE-ASEG	false
91.123.112.1	unknown	France		8302	ZATTOOZuerichSwitzerlandCH	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.190.247.32	unknown	Germany		42311	PGHOSTING-DRESDENPGHOSTING-DRESDEN-BACKBONEDE	false
139.120.194.75	unknown	Norway		5619	EVRY-NO	false
185.226.106.149	unknown	Spain		207046	REDSERVICIOES	false
41.21.227.79	unknown	South Africa		36994	Vodacom-VBZA	false
45.167.243.35	unknown	Brazil		268058	REDEMETROPOLITANADETELECOMUNICACOESLTDA-MEBR	false
91.128.130.6	unknown	Austria		1257	TELE2EU	false
54.98.64.93	unknown	United States		16509	AMAZON-02US	false
45.202.220.198	unknown	Seychelles		132839	POWERLINE-AS-APPOWERLINEDATACENTERHK	false
45.202.220.199	unknown	Seychelles		132839	POWERLINE-AS-APPOWERLINEDATACENTERHK	false
45.104.148.75	unknown	Egypt		37069	MOBINILEG	false
185.37.230.227	unknown	Spain		60458	ASN-XTUDIONETES	false
79.112.6.241	unknown	Romania		8708	RCS-RDS73-75DrStaicoviciRO	false
185.50.154.121	unknown	United Kingdom		50203	UK-REYNOLDS-ASNGB	false
91.74.182.143	unknown	United Arab Emirates		15802	DU-AS1AE	false
185.38.220.194	unknown	Poland		56523	AMELEKTRONIKPL	false
91.112.149.164	unknown	Austria		8447	TELEKOM-ATA1TelekomAustriaAGAT	false
223.95.198.29	unknown	China		56041	CMNET-ZHEJIANG-APChinaMobilecommunicationscorporationC	false
185.244.103.203	unknown	Estonia		202635	SERVERFARMEE	false
69.13.247.219	unknown	United States		54489	CORESPACE-DALUS	false
174.100.121.140	unknown	United States		10796	TWC-10796-MIDWESTUS	false
188.245.52.93	unknown	Iran (ISLAMIC Republic Of)		16322	PARSONLINETehran-IRANIR	false

Runtime Messages

Command:	/tmp/BitmCvTrdO
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	C7C - c
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.150.101.140	Hilix.x86	Get hash	malicious	Browse	
197.166.142.80	RiPy3zOdjl	Get hash	malicious	Browse	
45.109.110.157	i01hLg63ev	Get hash	malicious	Browse	
185.19.109.165	BcOfN2cD3e	Get hash	malicious	Browse	
41.44.233.246	x86	Get hash	malicious	Browse	
185.149.161.25	93T511Z3h8	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ACORSOFR	apep.x86	Get hash	malicious	Browse	• 45.12.189.188
	SCahhGpqlT	Get hash	malicious	Browse	• 45.12.189.155
	dBmJXcsqS4	Get hash	malicious	Browse	• 45.12.189.150
	aFxrnP3GU4	Get hash	malicious	Browse	• 45.12.189.145
	Hilix.x86	Get hash	malicious	Browse	• 45.12.189.13
	Hilix.x86	Get hash	malicious	Browse	• 45.12.189.22
	3MlwPT62vR	Get hash	malicious	Browse	• 45.12.189.131
	Antisocial.x86	Get hash	malicious	Browse	• 45.12.189.12
	Antisocial.arm	Get hash	malicious	Browse	• 45.12.189.11
	0iojYwstAE	Get hash	malicious	Browse	• 45.12.189.138
	NMlnVly7uv	Get hash	malicious	Browse	• 45.12.189.139
	bPAMfuy9oa	Get hash	malicious	Browse	• 45.12.189.156
	Md3k7pepaq	Get hash	malicious	Browse	• 45.12.189.134
LOVESERVERSGB	OhUy3woBmb	Get hash	malicious	Browse	• 45.150.101.139
	PO88736446.exe	Get hash	malicious	Browse	• 203.159.80.151
	PO99817581.exe	Get hash	malicious	Browse	• 203.159.80.151
	sora.x86	Get hash	malicious	Browse	• 45.150.101.135
	dTmYFku6X8	Get hash	malicious	Browse	• 45.150.101.191
	tl0W00k1vt	Get hash	malicious	Browse	• 45.150.101.197
	Hilix.arm7	Get hash	malicious	Browse	• 45.150.101.170
	Hilix.x86	Get hash	malicious	Browse	• 45.150.101.174
	Hilix.arm7	Get hash	malicious	Browse	• 45.150.101.196
	Antisocial.x86	Get hash	malicious	Browse	• 45.150.101.165
	frosty.x86	Get hash	malicious	Browse	• 45.150.101.165
	zd9Gd8UT5s	Get hash	malicious	Browse	• 45.150.101.170
	Qz1DSFEgD9.exe	Get hash	malicious	Browse	• 203.159.80.52
	mg2m6hZU0W.exe	Get hash	malicious	Browse	• 203.159.80.18
	p7qsMlfWjt.exe	Get hash	malicious	Browse	• 203.159.80.18
	inquire details & specification.exe	Get hash	malicious	Browse	• 203.159.80.52
	NMlnVly7uv	Get hash	malicious	Browse	• 45.150.101.161
	dark.86_64	Get hash	malicious	Browse	• 45.150.101.150
	PO17904.doc	Get hash	malicious	Browse	• 203.159.80.186
	18.08.2021 Purchase Order.doc	Get hash	malicious	Browse	• 203.159.80.186
AFRARASAIR	17Rom1F3MY	Get hash	malicious	Browse	• 185.49.104.8
	Yx8iF6YZtN	Get hash	malicious	Browse	• 185.49.104.3
	SecuriteInfo.com.Exploit.Siggen3.10048.24657.xls	Get hash	malicious	Browse	• 185.118.15.137
	SecuriteInfo.com.Exploit.Siggen3.10048.14515.xls	Get hash	malicious	Browse	• 185.118.15.137

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, SPARC, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.104929349861386
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	BitmCvTrdO

General

File size:	69072
MD5:	83f51eab5d7a35965c15c15a0966ccc8
SHA1:	3fa59c483662eff85b5b454692eb3dbaa76944ed
SHA256:	9ae7441ecbce9ecf93e8825a4a98b04ec55388a614cbae4baaf8f5e037ee8a76
SHA512:	296eff1fb30310c2ab96631b5dfb20bff582c98d57d4752d98c7a1a397aab77b4f20f97a260223d00988666315238f605ee49df1b4785003c7cc2eb651455162
SSDEEP:	1536:b+lhwhYS5Gbb4O9jtuMzdH9qoKb284k3astY847l:b2el4wztOi5kK9l
File Content Preview:	.ELF.....4...@.....4. ...(.....l..&d.....dt.Q.....@..(....@.9w.....#.....`..`.....l..... ...@.....".....`.....$ ... ...@.....`....

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	Sparc
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x101a4
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	68672
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

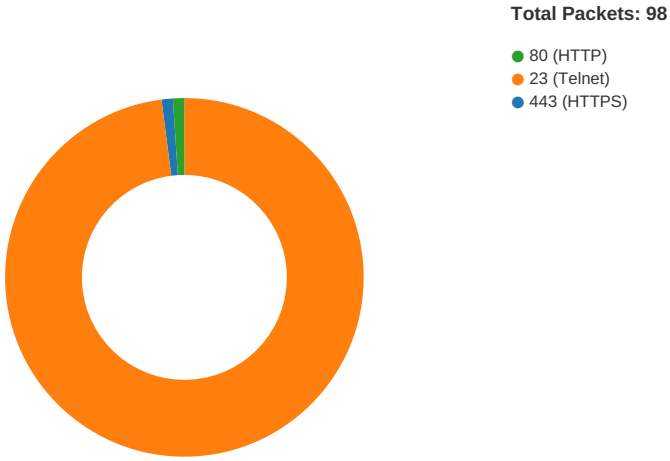
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x10094	0x94	0x1c	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x100b0	0xb0	0xe614	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x1e6c4	0xe6c4	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x1e6d8	0xe6d8	0x21b8	0x0	0x2	A	0	0	8
.ctors	PROGBITS	0x30894	0x10894	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x3089c	0x1089c	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x308a8	0x108a8	0x358	0x0	0x3	WA	0	0	8
.bss	NOBITS	0x30c00	0x10c00	0x22f8	0x0	0x3	WA	0	0	8
.shstrtab	STRTAB	0x0	0x10c00	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	0x10000	0x10000	0x10890	0x10890	3.7025	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x10894	0x30894	0x30894	0x36c	0x2664	1.6618	0x6	RW	0x10000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



TCP Packets

HTTP Request Dependency Graph

- 127.0.0.1:52869

System Behavior

Analysis Process: BitmCvTrdO PID: 5233 Parent PID: 5112

General

Start time:	10:32:06
Start date:	01/11/2021
Path:	/tmp/BitmCvTrdO
Arguments:	/tmp/BitmCvTrdO
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

File Activities

File Read

Analysis Process: BitmCvTrdO PID: 5235 Parent PID: 5233

General

Start time:	10:32:06
Start date:	01/11/2021
Path:	/tmp/BitmCvTrdO
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: BitmCvTrdO PID: 5240 Parent PID: 5235

General

Start time:	10:32:06
Start date:	01/11/2021
Path:	/tmp/BitmCvTrdO
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: BitmCvTrdO PID: 5241 Parent PID: 5235

General

Start time:	10:32:06
Start date:	01/11/2021
Path:	/tmp/BitmCvTrdO
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: BitmCvTrdO PID: 5246 Parent PID: 5241

General

Start time:	10:32:06
Start date:	01/11/2021
Path:	/tmp/BitmCvTrdO
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: BitmCvTrdO PID: 5268 Parent PID: 5246

General

Start time:	10:32:06
Start date:	01/11/2021
Path:	/tmp/BitmCvTrdO
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: BitmCvTrdO PID: 5271 Parent PID: 5246

General

Start time:	10:32:06
Start date:	01/11/2021
Path:	/tmp/BitmCvTrdO
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: BitmCvTrdO PID: 5272 Parent PID: 5246

General

Start time:	10:32:06
Start date:	01/11/2021
Path:	/tmp/BitmCvTrdO
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: BitmCvTrdO PID: 5273 Parent PID: 5246

General

Start time:	10:32:06
Start date:	01/11/2021
Path:	/tmp/BitmCvTrdO
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: BitmCvTrdO PID: 5256 Parent PID: 5241

General

Start time:	10:32:06
Start date:	01/11/2021
Path:	/tmp/BitmCvTrdO
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: BitmCvTrdO PID: 5269 Parent PID: 5241

General

Start time:	10:32:06
Start date:	01/11/2021
Path:	/tmp/BitmCvTrdO
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: BitmCvTrdO PID: 5278 Parent PID: 5241

General

Start time:	10:32:06
Start date:	01/11/2021
Path:	/tmp/BitmCvTrdO
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: BitmCvTrdO PID: 5280 Parent PID: 5241

General

Start time:	10:32:06
Start date:	01/11/2021
Path:	/tmp/BitmCvTrdO
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: BitmCvTrdO PID: 5236 Parent PID: 5233

General

Start time:	10:32:06
Start date:	01/11/2021
Path:	/tmp/BitmCvTrdO
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: BitmCvTrdO PID: 5237 Parent PID: 5233

General

Start time:	10:32:06
Start date:	01/11/2021
Path:	/tmp/BitmCvTrdO
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: BitmCvTrdO PID: 5244 Parent PID: 5237

General

Start time:	10:32:06
Start date:	01/11/2021
Path:	/tmp/BitmCvTrdO
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: BitmCvTrdO PID: 5260 Parent PID: 5244

General

Start time:	10:32:06
Start date:	01/11/2021
Path:	/tmp/BitmCvTrdO
Arguments:	n/a
File size:	4379400 bytes

MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: BitmCvTrdO PID: 5261 Parent PID: 5244

General

Start time:	10:32:06
Start date:	01/11/2021
Path:	/tmp/BitmCvTrdO
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: BitmCvTrdO PID: 5262 Parent PID: 5244

General

Start time:	10:32:06
Start date:	01/11/2021
Path:	/tmp/BitmCvTrdO
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: BitmCvTrdO PID: 5264 Parent PID: 5244

General

Start time:	10:32:06
Start date:	01/11/2021
Path:	/tmp/BitmCvTrdO
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: BitmCvTrdO PID: 5247 Parent PID: 5237

General

Start time:	10:32:06
Start date:	01/11/2021
Path:	/tmp/BitmCvTrdO
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: BitmCvTrdO PID: 5248 Parent PID: 5237

General

Start time:	10:32:06
Start date:	01/11/2021
Path:	/tmp/BitmCvTrdO

Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: BitmCvTrdO PID: 5251 Parent PID: 5237

General

Start time:	10:32:06
Start date:	01/11/2021
Path:	/tmp/BitmCvTrdO
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: BitmCvTrdO PID: 5257 Parent PID: 5237

General

Start time:	10:32:06
Start date:	01/11/2021
Path:	/tmp/BitmCvTrdO
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e