ID: 512832
Sample Name: swOGb2sZYt
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 13:05:33
Date: 01/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

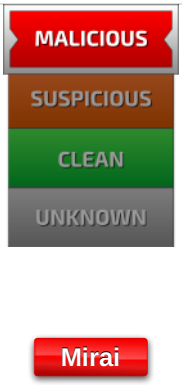
Linux Analysis Report swOGb2sZYt

Overview

General Information

Sample Name:	swOGb2sZYt
Analysis ID:	512832
MD5:	0d987a045736b3..
SHA1:	4c3449d8826b0b..
SHA256:	4704abb6701285..
Tags:	32 elf mirai motorola
Infos:	

Detection

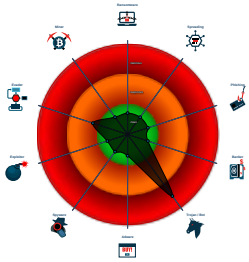


Score:	76
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Uses known network protocols on no...
- 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

Some HTTP requests failed (404). It is likely the sample will exhibit less behavior

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:	512832
Start date:	01.11.2021
Start time:	13:05:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	swOGb2sZYt
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:	mal76.troj.lin@0/0@0/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
  - swOGb2sZYt (PID: 5245, Parent: 5118, MD5: cd177594338c77b895ae27c33f8f86cc) Arguments: /tmp/swOGb2sZYt
    - swOGb2sZYt New Fork (PID: 5247, Parent: 5245)
      - swOGb2sZYt New Fork (PID: 5267, Parent: 5247)
      - swOGb2sZYt New Fork (PID: 5269, Parent: 5247)
        - swOGb2sZYt New Fork (PID: 5271, Parent: 5269)
          - swOGb2sZYt New Fork (PID: 5291, Parent: 5271)
          - swOGb2sZYt New Fork (PID: 5292, Parent: 5271)
          - swOGb2sZYt New Fork (PID: 5295, Parent: 5271)
          - swOGb2sZYt New Fork (PID: 5296, Parent: 5271)
        - swOGb2sZYt New Fork (PID: 5273, Parent: 5269)
        - swOGb2sZYt New Fork (PID: 5275, Parent: 5269)
        - swOGb2sZYt New Fork (PID: 5280, Parent: 5269)
        - swOGb2sZYt New Fork (PID: 5284, Parent: 5269)
    - swOGb2sZYt New Fork (PID: 5248, Parent: 5245)
    - swOGb2sZYt New Fork (PID: 5249, Parent: 5245)
      - swOGb2sZYt New Fork (PID: 5253, Parent: 5249)
        - swOGb2sZYt New Fork (PID: 5276, Parent: 5253)
        - swOGb2sZYt New Fork (PID: 5278, Parent: 5253)
        - swOGb2sZYt New Fork (PID: 5281, Parent: 5253)
        - swOGb2sZYt New Fork (PID: 5283, Parent: 5253)
      - swOGb2sZYt New Fork (PID: 5254, Parent: 5249)
      - swOGb2sZYt New Fork (PID: 5256, Parent: 5249)
      - swOGb2sZYt New Fork (PID: 5259, Parent: 5249)
      - swOGb2sZYt New Fork (PID: 5263, Parent: 5249)
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
swOGb2sZYt	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

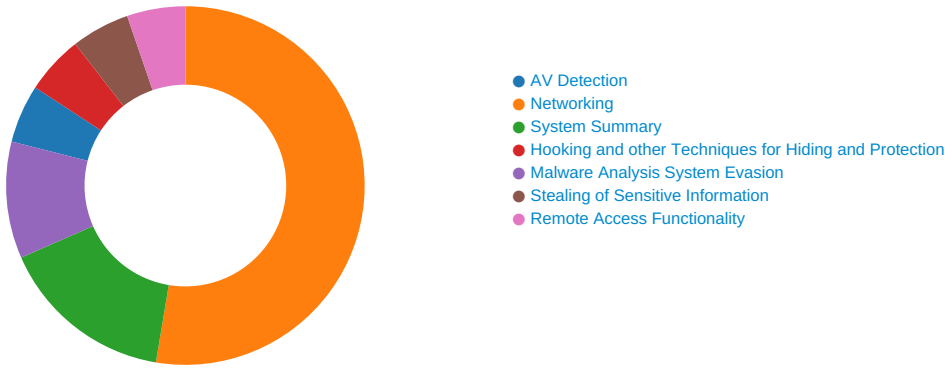
PCAP (Network Traffic)

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

Memory Dumps

Source	Rule	Description	Author	Strings
5267.1.00000000cd92e3cf.00000000eb405220.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5247.1.00000000cd92e3cf.00000000eb405220.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5276.1.00000000cd92e3cf.00000000eb405220.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5248.1.00000000cd92e3cf.00000000eb405220.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
5273.1.00000000cd92e3cf.00000000eb405220.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

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

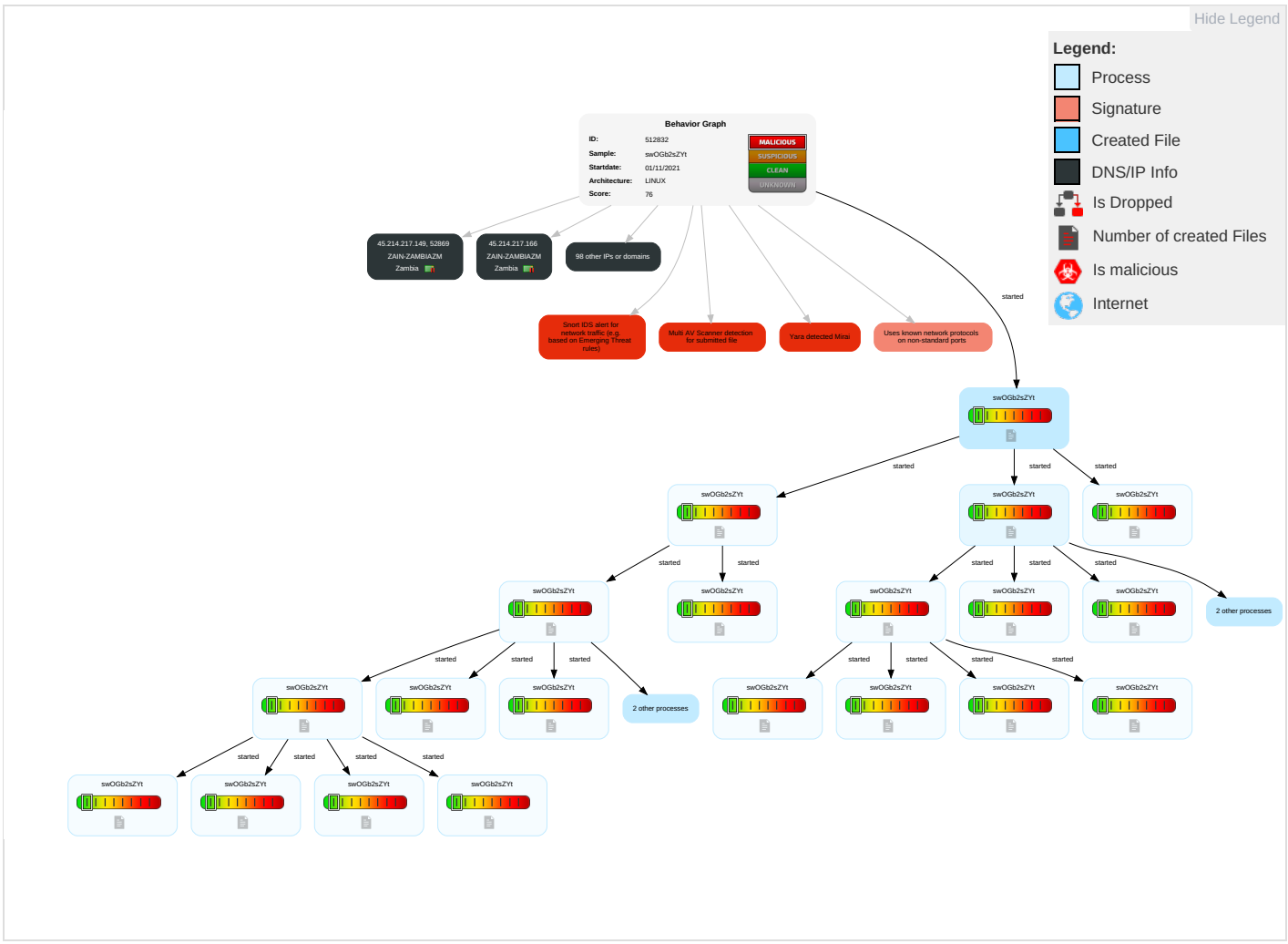
Mitre Att&ck Matrix

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 2	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 3	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Ingress Tool Transfer 2	Manipulate Device Communication		Manipula App Sto Ranking or Ratin

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
swOGb2sZYt	52%	Virustotal		Browse
swOGb2sZYt	51%	ReversingLabs	Linux.Trojan.Mirai	

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
91.30.56.10	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
43.241.39.124	unknown	India		133296	WEBWERKS-AS-INWebWerksIndiaPvtLtdIN	false
91.242.108.4	unknown	Moldova Republic of		35346	ITNSIPtransitandpeeringinfrastructureMD	false
185.204.16.84	unknown	Czech Republic		200918	ORELSOFTCZ	false
41.117.228.133	unknown	South Africa		16637	MTNNS-ASZA	false
213.228.151.224	unknown	Portugal		13156	AS13156PalmelaPT	false
153.72.52.51	unknown	United States		14962	NCR-252US	false
103.49.139.165	unknown	Pakistan		58895	EBONE1-PKEboneNetworkPVTLimitedPK	false
63.184.206.211	unknown	United States		1239	SPRINTLINKUS	false
91.71.83.0	unknown	France		15557	LDCOMNETFR	false
185.78.207.82	unknown	United Kingdom		8426	CLARANET-ASClaraNETLTDGB	false
156.253.18.67	unknown	Seychelles		137443	ANCHGLOBAL-AS-APAnchnetAsiaLimitedHK	false
197.123.112.81	unknown	Egypt		36992	ETISALAT-MISREG	false
195.32.192.103	unknown	Germany		20676	PLUSNETDE	false
197.43.51.159	unknown	Egypt		8452	TE-ASTE-ASEG	false
48.68.113.231	unknown	United States		2686	ATGS-MMD-ASUS	false
91.19.189.222	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
185.220.10.239	unknown	Spain		205390	TECTIQOM-ASDE	false
45.44.104.188	unknown	Canada		54198	VIANETCA	false
138.250.252.45	unknown	United Kingdom		786	JANETJiscServicesLimitedGB	false
41.21.227.49	unknown	South Africa		36994	Vodacom-VBZA	false
113.134.51.34	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
213.42.251.201	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	false
45.50.203.142	unknown	United States		20001	TWC-20001-PACWESTUS	false
45.44.28.205	unknown	Canada		54198	VIANETCA	false
45.30.40.133	unknown	United States		7018	ATT-INTERNET4US	false
141.174.93.129	unknown	United States		29601	UPM-KYMMENE-ASKuusankoskiFinlandFI	false
91.254.204.222	unknown	Italy		1267	ASN-WINDTREIUNETEU	false
185.231.215.248	unknown	Germany		204965	MED360GRADDE	false
45.237.182.85	unknown	Brazil		268283	NETWORKFIBERCOMERCIOESERVICOSDECOMUNICACAOBR	false
201.193.140.237	unknown	Costa Rica		11830	InstitutoCostarricensedeElectricidadyTelecomCR	false
185.132.166.202	unknown	Spain		29119	SERVIHOSTING-ASAireNetworksES	false
91.74.182.161	unknown	United Arab Emirates		15802	DU-AS1AE	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
156.3.253.168	unknown	United States		2920	LACOEUS	false
45.21.146.125	unknown	United States		7018	ATT-INTERNET4US	false
185.231.215.250	unknown	Germany		204965	MED360GRADDE	false
185.56.176.201	unknown	France		35600	ASN-VEDEGEFR	false
185.218.42.205	unknown	Denmark		205452	DIDK	false
69.116.232.196	unknown	United States		6128	CABLE-NET-1US	false
190.37.34.107	unknown	Venezuela		8048	CANTVServiciosVenezuelaVE	false
185.148.4.101	unknown	United Kingdom		203003	MAGNA-CAPAXFI	false
45.150.101.170	unknown	Liechtenstein		47987	LOVESERVERSGB	false
185.102.172.187	unknown	Netherlands		7922	COMCAST-7922US	false
45.93.168.248	unknown	Iran (ISLAMIC Republic Of)		57497	FARASOSAMANEHPASARGADIR	false
180.64.26.212	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	false
45.150.101.157	unknown	Liechtenstein		47987	LOVESERVERSGB	false
156.251.85.211	unknown	Seychelles		26484	IKGUL-26484US	false
185.204.16.97	unknown	Czech Republic		200918	ORELSOFTCZ	false
185.69.33.33	unknown	Netherlands		196826	PL-NETTELEKOM-ASNPL	false
91.72.131.133	unknown	United Arab Emirates		15802	DU-AS1AE	false
162.127.82.93	unknown	United States		11714	NETWORKNEBRASKAUS	false
45.214.217.166	unknown	Zambia		37287	ZAIN-ZAMBIAZM	false
176.237.112.118	unknown	Turkey		16135	TURKCELL-ASTurkcellASTR	false
156.16.3.201	unknown	unknown		29975	VODACOM-ZA	false
91.11.116.182	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
91.19.165.43	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
41.196.116.139	unknown	Egypt		24863	LINKdotNET-ASEG	false
61.27.172.128	unknown	Japan		9824	JTCL-JP-ASJupiterTelecommunicationCoLtdJP	false
91.85.78.212	unknown	United Kingdom		12513	ECLIPSEGB	false
179.249.189.164	unknown	Brazil		26615	TIMSABR	false
45.221.254.50	unknown	Benin		328092	SUD-TELCOM-ASBJ	false
99.55.160.13	unknown	United States		7018	ATT-INTERNET4US	false
152.180.133.25	unknown	United States		701	UUNETUS	false
146.71.165.162	unknown	United States		32904	KAJEET-ARTERRA-OTARRISUS	false
45.20.156.207	unknown	United States		7018	ATT-INTERNET4US	false
156.24.33.228	unknown	United States		29975	VODACOM-ZA	false
185.132.166.226	unknown	Spain		29119	SERVIHOSTING-ASAireNetworksES	false
91.30.186.180	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
197.166.142.27	unknown	Egypt		24863	LINKdotNET-ASEG	false
70.178.160.105	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
166.94.50.202	unknown	United States		3926	FFX-CNTYUS	false
209.143.100.93	unknown	United States		17054	AS17054US	false
197.202.110.242	unknown	Algeria		36947	ALGTEL-ASDZ	false
41.196.201.5	unknown	Egypt		24863	LINKdotNET-ASEG	false
199.58.40.60	unknown	United States		3303	SWISSCOMSwisscomSwitzerlandLtdCH	false
78.17.52.57	unknown	Ireland		2110	AS-BTIREBTIrelandwaspreviouslyknownasEsatNetEUnet	false
185.192.205.96	unknown	Belgium		201050	QBONE-NETBE	false
41.149.186.145	unknown	South Africa		5713	SAIX-NETZA	false
20.112.77.80	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
45.202.220.188	unknown	Seychelles		132839	POWERLINE-AS-APPOWERLINEDATACENTERHK	false
181.159.27.108	unknown	Colombia		26611	COMCELSACO	false
222.147.153.200	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
91.186.75.69	unknown	Norway		56828	NORWEGIANHEALTHNETWORKNO	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
130.221.233.190	unknown	United States		85	AERO-NETUS	false
91.199.162.45	unknown	Germany		42652	DELUNETDE	false
45.214.217.149	unknown	Zambia		37287	ZAIN-ZAMBIAZM	false
8.139.185.129	unknown	Singapore		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
91.184.212.240	unknown	Cyprus		35432	CABLENET-ASCY	false
168.178.38.143	unknown	United States		11663	SUG-1US	false
36.250.29.152	unknown	China		4837	CHINA169-BACKBONECHINAUNICOM China169BackboneCN	false
43.240.13.101	unknown	Hong Kong		55933	CLOUDIE-AS-APCloudieLimitedHK	false
45.44.104.175	unknown	Canada		54198	VIANETCA	false
170.122.117.64	unknown	United States		54314	LHA-2-ASNUS	false
8.113.103.123	unknown	United States		3356	LEVEL3US	false
185.24.218.229	unknown	Poland		59491	LIVENET-PL	false
185.154.90.98	unknown	Italy		47406	RLNET-ASIT	false
91.179.103.124	unknown	Belgium		5432	PROXIMUS-ISP-ASBE	false
45.111.37.194	unknown	Egypt		37069	MOBINILEG	false
45.104.148.96	unknown	Egypt		37069	MOBINILEG	false
45.104.148.98	unknown	Egypt		37069	MOBINILEG	false

Runtime Messages

Command:	/tmp/swOGb2sZYt
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
45.44.28.205	Hilix.arm	Get hash	malicious	Browse	
185.231.215.248	2S8N5fDSRs	Get hash	malicious	Browse	
	h9a1NEWEeR	Get hash	malicious	Browse	
91.30.56.10	QIJ16axero	Get hash	malicious	Browse	
41.117.228.133	Hilix.x86	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DTAGInternetserviceprovideroperationsDE	ydZLm6GD56	Get hash	malicious	Browse	• 91.52.65.175
	BitmCvTrdO	Get hash	malicious	Browse	• 91.26.178.54
	UQnO4DB8Z1	Get hash	malicious	Browse	• 91.19.165.18
	OhUy3woBmb	Get hash	malicious	Browse	• 91.18.128.126
	S8G5z3pdHw	Get hash	malicious	Browse	• 79.225.12.21
	9o6Z1wEokT	Get hash	malicious	Browse	• 31.241.9.128
	00hZyjOhZA	Get hash	malicious	Browse	• 46.86.236.185
	mP1pg0ryFA	Get hash	malicious	Browse	• 37.83.101.87
	a5nulABeSk	Get hash	malicious	Browse	• 79.255.11.184

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	1bL17EUgTk	Get hash	malicious	Browse	• 217.239.211.87
	032k4JmR0U	Get hash	malicious	Browse	• 93.194.49.78
	x86	Get hash	malicious	Browse	• 91.41.111.100
	arm7	Get hash	malicious	Browse	• 91.52.65.199
	yJOZ3EeESV	Get hash	malicious	Browse	• 37.84.16.195
	lYmYPlzghQ	Get hash	malicious	Browse	• 31.248.86.230
	T0uznhDXKw	Get hash	malicious	Browse	• 31.233.207.188
	apep.arm7	Get hash	malicious	Browse	• 31.238.72.59
	QtNnZoNz75	Get hash	malicious	Browse	• 31.225.15.194
	S13B4aCa4E	Get hash	malicious	Browse	• 31.228.35.224
	gbk4XWulUo	Get hash	malicious	Browse	• 31.242.82.129
ITNSIPtransitandpeeringinfrastructureMD	i586-20211007-1619	Get hash	malicious	Browse	• 91.242.108.9
	Antisocial.x86	Get hash	malicious	Browse	• 91.242.108.0
WEBWERKS-AS-INWebWerksIndiaPvtLtdIN	Document MT. MTM MANILA V55.docx	Get hash	malicious	Browse	• 202.148.54.253
	new order 20211029.exe	Get hash	malicious	Browse	• 206.183.111.188
	SOA.exe	Get hash	malicious	Browse	• 206.183.111.188
	x86_64	Get hash	malicious	Browse	• 103.13.111.195
	ppuXvHPso0.dll	Get hash	malicious	Browse	• 103.233.25.228
	ppuXvHPso0.dll	Get hash	malicious	Browse	• 103.233.25.228
	93T511Z3h8	Get hash	malicious	Browse	• 43.241.39.149
	INV.-0456_20210915.xlsm	Get hash	malicious	Browse	• 103.233.25.228
	2rafsvW3VD.xlsm	Get hash	malicious	Browse	• 103.233.25.228
	smierrsy.dll	Get hash	malicious	Browse	• 103.233.25.228
	smierrsy.dll	Get hash	malicious	Browse	• 103.233.25.228
	INV.-44906589_20210915.xlsm	Get hash	malicious	Browse	• 103.233.25.228
	INV.-534912_20210915.xlsm	Get hash	malicious	Browse	• 103.233.25.228
	sbs_iehost.dll	Get hash	malicious	Browse	• 103.233.25.228
	sbs_iehost.dll	Get hash	malicious	Browse	• 103.233.25.228
	INV.-54490_20210915.xlsm	Get hash	malicious	Browse	• 103.233.25.228
	INV.-1381947126_20210915.xlsm	Get hash	malicious	Browse	• 103.233.25.228
	triage_dropped_file.dll	Get hash	malicious	Browse	• 103.233.25.228
	triage_dropped_file.dll	Get hash	malicious	Browse	• 103.233.25.228
	INV.-486898_20210915.xlsm	Get hash	malicious	Browse	• 103.233.25.228

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, Motorola m68k, 68020, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.313602374819329
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	swOGb2sZYt
File size:	67604
MD5:	0d987a045736b3c9164d851d5abf20e7
SHA1:	4c3449d8826b0b8edfaaff4788c762a8c072b759

General

SHA256:	4704abb6701285007a922928f19ae74cee37103046e762e385a0154c2fd899fd
SHA512:	46ee9472fbffb3c440cb3b1e909f2916d6df631ce587f7beac2c38384066a14ec3a843dc6da6c5189834b07fee032daf149620b72a685f117a044247d6181fde
SSDEEP:	1536:AYZnNjddm5fG6pszzsfsJ3918KOyzwjJqSmR7JrlY:AYZNz4fG6WzzRp9WylSAZ
File Content Preview:	.ELF.....D...4.....4. ...(......"..."....`..&..... .dt.Q.....NV..a....da.. ..tN^NuNV..J9..&Df>"y..". QJ.g.X.#...".N."y..". QJ.f.A.....J .g.Hy....N.X.....&DN^NuNV..N^NuN

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, big endian
Version:	1 (current)
Machine:	MC68000
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x80000144
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	67204
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

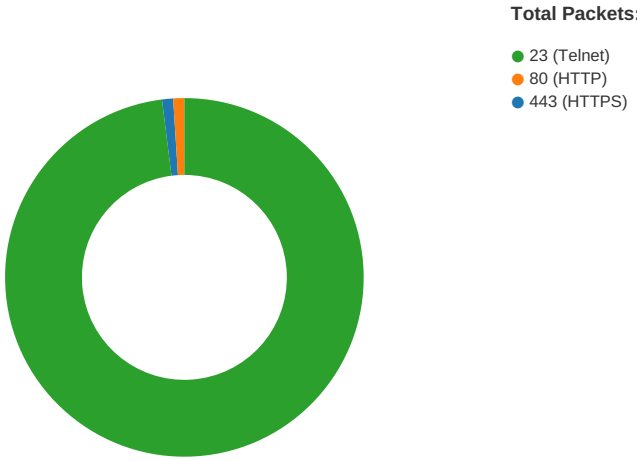
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x80000094	0x94	0x14	0x0	0x6	AX	0	0	2
.text	PROGBITS	0x800000a8	0xa8	0xe79e	0x0	0x6	AX	0	0	4
.fini	PROGBITS	0x8000e846	0xe846	0xe	0x0	0x6	AX	0	0	2
.rodata	PROGBITS	0x8000e854	0xe854	0x1a8c	0x0	0x2	A	0	0	2
.ctors	PROGBITS	0x800122e4	0x102e4	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x800122ec	0x102ec	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x800122f8	0x102f8	0x34c	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x80012644	0x10644	0x22ac	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0x10644	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	0x80000000	0x80000000	0x102e0	0x102e0	4.4356	0x5	R E	0x2000		.init .text .fini .rodata
LOAD	0x102e4	0x800122e4	0x800122e4	0x360	0x260c	1.7129	0x6	RW	0x2000		.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: swOGb2sZYt PID: 5245 Parent PID: 5118

General

Start time:	13:06:17
Start date:	01/11/2021
Path:	/tmp/swOGb2sZYt
Arguments:	/tmp/swOGb2sZYt
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

File Activities

File Read

Analysis Process: swOGb2sZYt PID: 5247 Parent PID: 5245

General

Start time:	13:06:17
Start date:	01/11/2021
Path:	/tmp/swOGb2sZYt
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: swOGb2sZYt PID: 5267 Parent PID: 5247

General

Start time:	13:06:22
Start date:	01/11/2021
Path:	/tmp/swOGb2sZYt
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: swOGb2sZYt PID: 5269 Parent PID: 5247

General

Start time:	13:06:22
Start date:	01/11/2021
Path:	/tmp/swOGb2sZYt
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: swOGb2sZYt PID: 5271 Parent PID: 5269

General

Start time:	13:06:22
Start date:	01/11/2021
Path:	/tmp/swOGb2sZYt
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: swOGb2sZYt PID: 5291 Parent PID: 5271

General

Start time:	13:06:27
Start date:	01/11/2021
Path:	/tmp/swOGb2sZYt
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: swOGb2sZYt PID: 5292 Parent PID: 5271

General

Start time:	13:06:27
Start date:	01/11/2021
Path:	/tmp/swOGb2sZYt
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: swOGb2sZYt PID: 5295 Parent PID: 5271

General

Start time:	13:06:27
Start date:	01/11/2021
Path:	/tmp/swOGb2sZYt
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: swOGb2sZYt PID: 5296 Parent PID: 5271

General

Start time:	13:06:27
Start date:	01/11/2021
Path:	/tmp/swOGb2sZYt
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: swOGb2sZYt PID: 5273 Parent PID: 5269

General

Start time:	13:06:22
Start date:	01/11/2021
Path:	/tmp/swOGb2sZYt
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: swOGb2sZYt PID: 5275 Parent PID: 5269

General

Start time:	13:06:22
Start date:	01/11/2021
Path:	/tmp/swOGb2sZYt
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: swOGb2sZYt PID: 5280 Parent PID: 5269

General

Start time:	13:06:22
Start date:	01/11/2021
Path:	/tmp/swOGb2sZYt
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: swOGb2sZYt PID: 5284 Parent PID: 5269

General

Start time:	13:06:22
Start date:	01/11/2021
Path:	/tmp/swOGb2sZYt
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: swOGb2sZYt PID: 5248 Parent PID: 5245

General

Start time:	13:06:17
Start date:	01/11/2021
Path:	/tmp/swOGb2sZYt
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: swOGb2sZYt PID: 5249 Parent PID: 5245

General

Start time:	13:06:17
Start date:	01/11/2021
Path:	/tmp/swOGb2sZYt
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: swOGb2sZYt PID: 5253 Parent PID: 5249

General

Start time:	13:06:17
Start date:	01/11/2021
Path:	/tmp/swOGb2sZYt
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: swOGb2sZYt PID: 5276 Parent PID: 5253

General

Start time:	13:06:22
Start date:	01/11/2021
Path:	/tmp/swOGb2sZYt
Arguments:	n/a
File size:	4463432 bytes

MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: swOGb2sZYt PID: 5278 Parent PID: 5253

General

Start time:	13:06:22
Start date:	01/11/2021
Path:	/tmp/swOGb2sZYt
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: swOGb2sZYt PID: 5281 Parent PID: 5253

General

Start time:	13:06:22
Start date:	01/11/2021
Path:	/tmp/swOGb2sZYt
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: swOGb2sZYt PID: 5283 Parent PID: 5253

General

Start time:	13:06:22
Start date:	01/11/2021
Path:	/tmp/swOGb2sZYt
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: swOGb2sZYt PID: 5254 Parent PID: 5249

General

Start time:	13:06:17
Start date:	01/11/2021
Path:	/tmp/swOGb2sZYt
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: swOGb2sZYt PID: 5256 Parent PID: 5249

General

Start time:	13:06:17
Start date:	01/11/2021
Path:	/tmp/swOGb2sZYt

Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: swOGb2sZYt PID: 5259 Parent PID: 5249

General

Start time:	13:06:17
Start date:	01/11/2021
Path:	/tmp/swOGb2sZYt
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc

Analysis Process: swOGb2sZYt PID: 5263 Parent PID: 5249

General

Start time:	13:06:17
Start date:	01/11/2021
Path:	/tmp/swOGb2sZYt
Arguments:	n/a
File size:	4463432 bytes
MD5 hash:	cd177594338c77b895ae27c33f8f86cc