ID: 511941
Sample Name: Dy4UCGJRnG
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 20:18:27
Date: 29/10/2021
Version: 34.0.0 Boulder Opal

Table of Contents

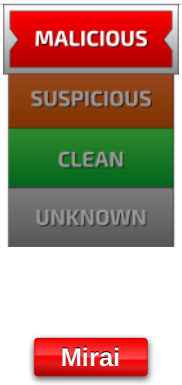
Linux Analysis Report Dy4UCGJRnG

Overview

General Information

Sample Name:	Dy4UCGJRnG
Analysis ID:	511941
MD5:	32167ecd41fd0a0.
SHA1:	b18653a994bfc98.
SHA256:	404afa3c5ce562b..
Tags:	32 elf mirai sparc
Infos:	

Detection

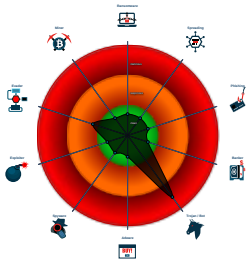


Score:	76
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Uses known network protocols on no...
- Yara signature match
- Sample has stripped symbol table
- HTTP GET or POST without a user ...
- Uses the "uname" system call to qu...
- Detected TCP or UDP traffic on non...
- Sample listens on a socket

Classification



Analysis Advice

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

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:	511941
Start date:	29.10.2021
Start time:	20:18:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Dy4UCGJRnG
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**
- Dy4UCGJRnG (PID: 5239, Parent: 5117, MD5: 7dc1c0e23cd5e102bb12e5c29403410e) Arguments: /tmp/Dy4UCGJRnG
  - Dy4UCGJRnG New Fork (PID: 5241, Parent: 5239)
  - Dy4UCGJRnG New Fork (PID: 5242, Parent: 5239)
    - Dy4UCGJRnG New Fork (PID: 5244, Parent: 5242)
    - Dy4UCGJRnG New Fork (PID: 5246, Parent: 5242)
    - Dy4UCGJRnG New Fork (PID: 5247, Parent: 5242)
    - Dy4UCGJRnG New Fork (PID: 5248, Parent: 5242)
    - Dy4UCGJRnG New Fork (PID: 5252, Parent: 5242)
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
Dy4UCGJRnG	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x12fb8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13028:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13098:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13108:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13178:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x133f8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13450:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x134a8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13500:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13558:$xo1: oMXKNNC\x0D\x17\x0C\x12
Dy4UCGJRnG	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	

PCAP (Network Traffic)

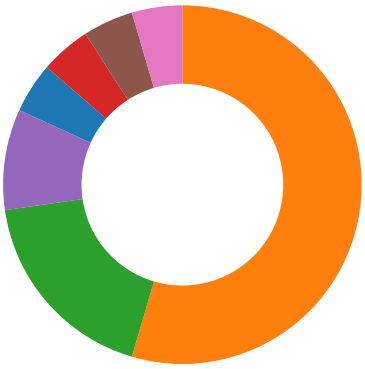
Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Mirai_12	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
5239.1.0000000060226c23.0000000052bc6aaf.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x298:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x30c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x380:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x3f4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x468:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x6e8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x740:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x798:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x7f0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x848:$xo1: oMXKNNC\x0D\x17\x0C\x12
5241.1.0000000060226c23.0000000052bc6aaf.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x298:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x30c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x380:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x3f4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x468:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x6e8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x740:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x798:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x7f0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x848:$xo1: oMXKNNC\x0D\x17\x0C\x12
5248.1.0000000060226c23.0000000052bc6aaf.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x298:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x30c:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x380:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x3f4:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x468:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x6e8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x740:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x798:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x7f0:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x848:$xo1: oMXKNNC\x0D\x17\x0C\x12
5241.1.000000003df39fd4.0000000084fd119a.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x12fb8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13028:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13098:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13108:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13178:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x133f8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13450:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x134a8:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13500:$xo1: oMXKNNC\x0D\x17\x0C\x12 • 0x13558:$xo1: oMXKNNC\x0D\x17\x0C\x12

Source	Rule	Description	Author	Strings
5241.1.000000003df39fd4.0000000084fd119a.r-x.sdmp	JoeSecurity_Mirai_8	Yara detected Mirai	Joe Security	
Click to see the 4 entries				

Jbx Signature Overview



- AV Detection
- Networking
- System Summary
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Stealing of Sensitive Information
- Remote Access Functionality

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

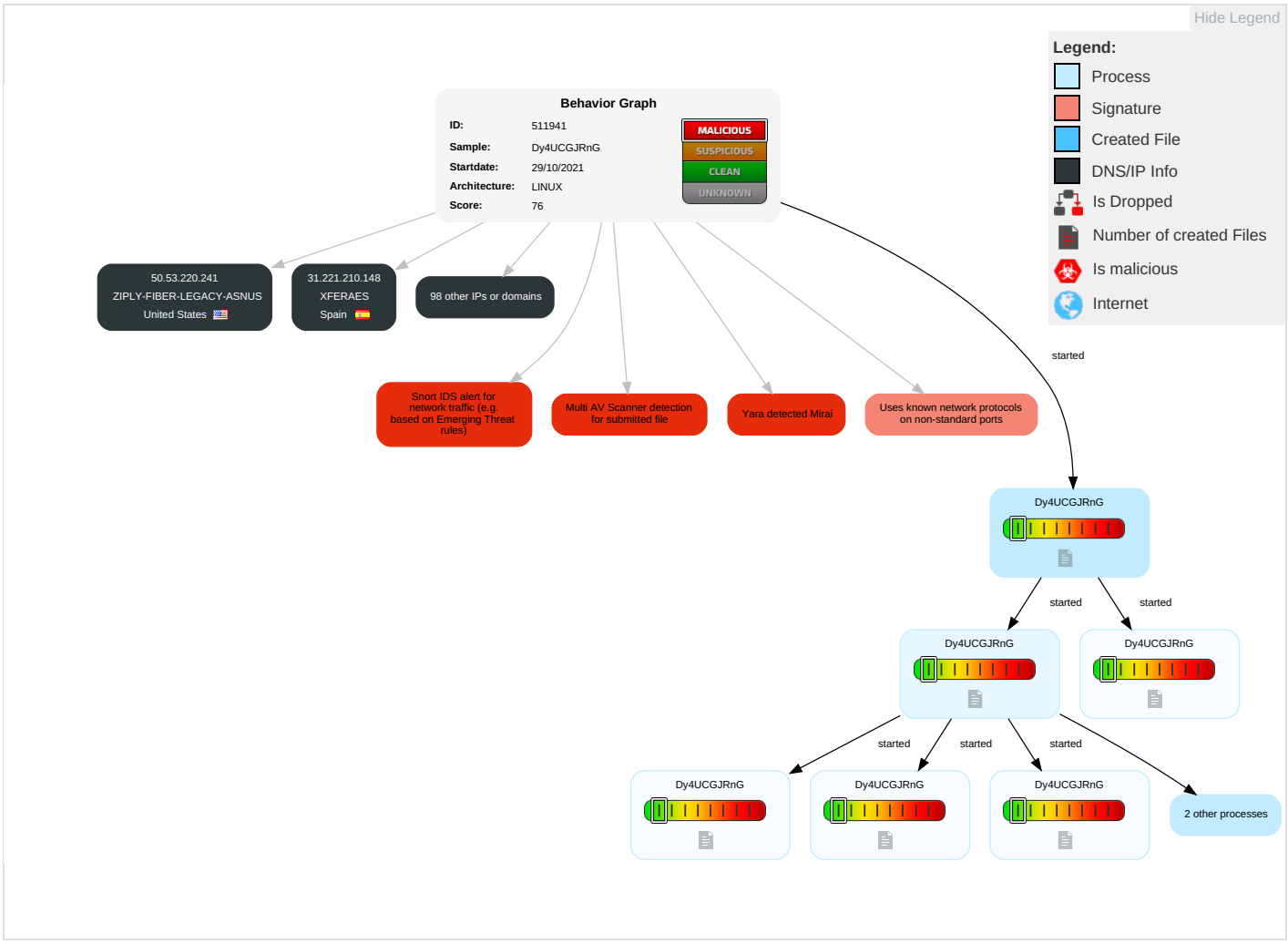
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Direct 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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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 4	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 5	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 4	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
Dy4UCGJRnG	46%	Virustotal		Browse
Dy4UCGJRnG	57%	ReversingLabs	Linux.Trojan.Mirai	

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://209.141.40.100/w.sh;	0%	Avira URL Cloud	safe	
http://209.141.40.100/bins/x86	0%	Avira URL Cloud	safe	
http://192.168.0.14:80/cgi-bin/ViewLog.asp	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://192.168.0.14:80/cgi-bin/ViewLog.asp	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
156.130.158.120	unknown	United States		29975	VODACOM-ZA	false
95.252.144.254	unknown	Italy		3269	ASN-IBSNAZIT	false
2.36.96.219	unknown	Italy		30722	VODAFONE-IT-ASNIT	false
41.108.48.186	unknown	Algeria		36947	ALGTEL-ASDZ	false
95.150.154.175	unknown	United Kingdom		12576	EELtdGB	false
85.33.215.214	unknown	Italy		3269	ASN-IBSNAZIT	false
157.105.247.183	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
62.125.156.10	unknown	United Kingdom		702	UUNETUS	false
62.168.37.195	unknown	Czech Republic		5588	GTSCEGTSCentralEuropeAntelGermanyCZ	false
94.8.166.132	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
85.66.79.209	unknown	Hungary		20845	DIGICABLEHU	false
31.167.93.129	unknown	Saudi Arabia		35819	MOBILY-ASEtihadEtisalatCompanyMobilySA	false
95.181.161.82	unknown	Russian Federation		50214	QWARTARU	false
41.42.142.154	unknown	Egypt		8452	TE-ASTE-ASEG	false
95.28.117.17	unknown	Russian Federation		8402	CORBINA-ASOJSCVimpelcomRU	false
31.58.18.189	unknown	Iran (ISLAMIC Republic Of)		31549	RASANAIR	false
85.142.138.106	unknown	Russian Federation		3267	RUNNETRU	false
62.40.187.71	unknown	Austria		8339	KABSI-ASAT	false
85.38.44.219	unknown	Italy		3269	ASN-IBSNAZIT	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
94.193.8.122	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
31.179.155.54	unknown	Poland		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
94.78.81.208	unknown	Turkey		44558	NETONLINETR	false
95.123.15.156	unknown	Spain		3352	TELEFONICA_DE_ESPANA ES	false
62.242.237.22	unknown	Denmark		3292	TDCTDCASDK	false
95.94.139.70	unknown	Portugal		2860	NOS_COMUNICACOESPT	false
31.122.161.107	unknown	United Kingdom		2856	BT-UK-ASBTnetUKRegionalnetwork GB	false
94.94.61.77	unknown	Italy		3269	ASN-IBSNAZIT	false
41.198.207.251	unknown	South Africa		327693	ECHO-SPZA	false
197.33.36.90	unknown	Egypt		8452	TE-ASTE-ASEG	false
95.236.91.143	unknown	Italy		3269	ASN-IBSNAZIT	false
62.19.15.19	unknown	Italy		16232	ASN-TIMServiceProviderIT	false
88.159.204.76	unknown	Netherlands		1136	KPNKPNNationalEU	false
95.38.211.201	unknown	Iran (ISLAMIC Republic Of)		41881	FANAVA-ASFanavaGroupCommunicationCoIR	false
31.221.210.148	unknown	Spain		16299	XFERAES	false
41.186.122.43	unknown	Rwanda		36890	MTNRW-ASNRW	false
197.92.49.1	unknown	South Africa		10474	OPTINETZA	false
157.47.67.105	unknown	India		55836	RELIANCEJIO-INRelianceJioInfocommLimitedIN	false
85.21.130.14	unknown	Russian Federation		8402	CORBINA-ASOJSCVimpelcomRU	false
94.218.73.2	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
95.52.196.241	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
95.47.59.211	unknown	Czech Republic		51131	SEVEN-ASRU	false
41.57.232.69	unknown	Ghana		37103	BUSYINTERNETGH	false
85.19.149.180	unknown	Norway		25400	TELIA-NORWAY-ASTeliaNorwayCoreNetworksNO	false
157.57.242.34	unknown	United States		3598	MICROSOFT-CORP-ASUS	false
31.142.125.246	unknown	Turkey		16135	TURKCELL-ASTurkcellASTR	false
197.197.89.73	unknown	Egypt		36992	ETISALAT-MISREG	false
90.131.24.64	unknown	Sweden		1257	TELE2EU	false
171.148.60.105	unknown	United States		9874	STARHUB-MOBILEStarHubLtdSG	false
197.59.229.17	unknown	Egypt		8452	TE-ASTE-ASEG	false
95.126.182.162	unknown	Spain		3352	TELEFONICA_DE_ESPANA ES	false
66.113.21.36	unknown	United States		15221	STRATUSIQUS	false
41.144.100.8	unknown	South Africa		5713	SAIX-NETZA	false
95.51.134.79	unknown	Poland		5617	TPNETPL	false
62.118.118.46	unknown	Russian Federation		8359	MTSRU	false
62.16.54.174	unknown	Russian Federation		15640	FPIC-ASRU	false
95.71.223.70	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
31.219.129.239	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternet AE	false
62.65.150.141	unknown	Switzerland		15517	NETSTREAM-CH	false
41.129.126.207	unknown	Egypt		24863	LINKdotNET-ASEG	false
24.130.12.151	unknown	United States		7922	COMCAST-7922US	false
62.92.203.193	unknown	Norway		2119	TELENOR-NEXTELTelenorNorgeASNO	false
66.9.68.14	unknown	United States		18885	M2NGAGE2US	false
134.6.198.59	unknown	United States		16504	GRANITEUS	false
41.252.35.47	unknown	Libyan Arab Jamahiriya		21003	GPTC-ASLY	false
197.202.209.158	unknown	Algeria		36947	ALGTEL-ASDZ	false
157.105.247.142	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
41.187.12.182	unknown	Egypt		20928	NOOR-ASEG	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
31.14.164.59	unknown	Syrian Arab Republic		29256	INT-PDN-STE-ASSTEPDNInternalASSY	false
70.160.227.214	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
62.98.1.199	unknown	Italy		1267	ASN-WINDTREIUNETEU	false
223.199.27.178	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
85.158.231.110	unknown	Austria		8692	BRZAT	false
95.94.141.249	unknown	Portugal		2860	NOS_COMUNICACOESPT	false
95.211.189.192	unknown	Netherlands		60781	LEASEWEB-NL-AMS-01NetherlandsNL	false
31.59.81.131	unknown	Iran (ISLAMIC Republic Of)		31549	RASANAIR	false
112.245.212.135	unknown	China		4837	CHINA169-BACKBONECHINAUNICOM China169BackboneCN	false
62.140.160.229	unknown	Netherlands		28995	ANTHOS-ASAnthosAmsterdamprovidesservicesforseveralint	false
31.61.177.127	unknown	Poland		5617	TPNETPL	false
94.216.58.20	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
95.44.121.88	unknown	Ireland		5466	EIRCOMInternetHouseIE	false
50.53.220.241	unknown	United States		27017	ZIPLY-FIBER-LEGACY-ASNUS	false
31.238.25.176	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
95.20.61.81	unknown	Spain		12479	UNI2-ASES	false
182.63.229.4	unknown	Malaysia		4818	DIGIIX-APDiGiTelecommunicationsSdnBhdMY	false
31.179.180.35	unknown	Poland		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
19.72.216.253	unknown	United States		3	MIT-GATEWAYSUS	false
85.209.47.150	unknown	Ukraine		209825	IBNETUA	false
41.227.43.56	unknown	Tunisia		2609	TN-BB-ASTunisiaBackBoneASTN	false
85.89.121.168	unknown	Russian Federation		5429	IIP-NET-AS5429RU	false
85.170.165.117	unknown	France		21502	ASN-NUMERICABLEFR	false
94.100.58.198	unknown	Serbia		47588	TELCOMMUNICATIONS-ASRS	false
31.142.52.199	unknown	Turkey		16135	TURKCELL-ASTurkcellASTR	false
197.82.0.30	unknown	South Africa		10474	OPTINETZA	false
31.211.62.229	unknown	Russian Federation		47938	FASTNET-ASRU	false
94.60.211.190	unknown	Portugal		12353	VODAFONE-PTVodafonePortugalPT	false
62.96.244.71	unknown	United Kingdom		8220	COLTCOLTTechnologyServicesGroupLimitedGB	false
31.16.255.135	unknown	Germany		31334	KABELDEUTSCHLAND-ASDE	false
94.104.217.4	unknown	Belgium		47377	ORANGE_BELGIUM_SAKPNBelgiumBusinessNVhasbeenacquired	false
19.172.192.200	unknown	United States		3	MIT-GATEWAYSUS	false
62.64.57.93	unknown	France		8362	20rueDenisPapinFR	false

Runtime Messages

Command:	/tmp/Dy4UCGJRnG
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Infected By Cult
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
95.28.117.17	1pXwlJR8QV	Get hash	malicious	Browse	
95.123.15.156	8EddA0qHLY	Get hash	malicious	Browse	
31.122.161.107	DEMONS.x86	Get hash	malicious	Browse	
95.181.161.82	lv2E1Fn8Eo	Get hash	malicious	Browse	
62.125.156.10	UnHAnaAW.x86	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VODACOM-ZA	wTFR3LK4Mo	Get hash	malicious	Browse	• 156.64.215.165
	VdcjZYprbt	Get hash	malicious	Browse	• 156.22.182.31
	apep.arm7	Get hash	malicious	Browse	• 41.30.254.97
	apep.arm	Get hash	malicious	Browse	• 156.133.23 9.108
	yOtRXukeq9	Get hash	malicious	Browse	• 156.49.135.69
	yFbmGHoONE	Get hash	malicious	Browse	• 156.129.36.250
	zju8TB277l	Get hash	malicious	Browse	• 156.2.60.196
	JYWllP5wHP	Get hash	malicious	Browse	• 156.131.22 4.191
	uwgXkY20gB	Get hash	malicious	Browse	• 41.18.99.139
	arm7	Get hash	malicious	Browse	• 156.72.152.79
	arm	Get hash	malicious	Browse	• 156.133.23 9.102
	x86	Get hash	malicious	Browse	• 156.72.152.59
	FWsCarsq8Q	Get hash	malicious	Browse	• 156.7.48.23
	p6j5MzMpDW	Get hash	malicious	Browse	• 156.2.60.187
	BMP4Nk5TTq	Get hash	malicious	Browse	• 156.132.102.5
	B6WwgS8sUq	Get hash	malicious	Browse	• 41.12.183.226
	PFD33mzc5l	Get hash	malicious	Browse	• 156.23.161.115
	tqQd9hibj0	Get hash	malicious	Browse	• 156.49.200.174
	buiodawbdawbuiopdw.x86	Get hash	malicious	Browse	• 156.37.137.189
	buiodawbdawbuiopdw.arm7	Get hash	malicious	Browse	• 156.2.12.217
ASN-IBSNAZIT	nUDLlJvoP4	Get hash	malicious	Browse	• 95.225.107.162
	heHfsavwfJ	Get hash	malicious	Browse	• 95.245.191.253
	RVG73cR3DP	Get hash	malicious	Browse	• 87.8.110.250
	9QPGr9LMaq	Get hash	malicious	Browse	• 31.198.254.110
	dqnskKAmQq	Get hash	malicious	Browse	• 88.45.10.182
	A0Pvsxsjf7	Get hash	malicious	Browse	• 95.225.107.130
	32UX3eB2m0	Get hash	malicious	Browse	• 95.255.148.89
	5odXR1ZmTd	Get hash	malicious	Browse	• 94.84.106.240
	x86	Get hash	malicious	Browse	• 62.110.19.21
	vEBWe85OY5	Get hash	malicious	Browse	• 82.60.20.182
	S1WMHUXAQU	Get hash	malicious	Browse	• 95.236.91.135
	5mLAGfiGBf	Get hash	malicious	Browse	• 5.99.27.231
	st2AAeCXsR	Get hash	malicious	Browse	• 79.21.225.126
	sj2211QUKu	Get hash	malicious	Browse	• 88.61.50.216
	bKHI9UT0D1	Get hash	malicious	Browse	• 151.99.94.9
	eNrYzJWFvB	Get hash	malicious	Browse	• 80.21.131.152
	arm7	Get hash	malicious	Browse	• 79.56.128.228
	x86_64	Get hash	malicious	Browse	• 94.92.80.206
	en94piXmL6	Get hash	malicious	Browse	• 79.1.2.209
	wRmHCEnowl	Get hash	malicious	Browse	• 79.21.137.181

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):	6.132548859394571
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	Dy4UCGJRnG
File size:	82952
MD5:	32167ecd41fd0a0a2cf1cf9db65b9e0e
SHA1:	b18653a994bfc98fbc6df17684cca4ac85a8cda3
SHA256:	404afa3c5ce562b339afd7e02b561168ec15a4baccdca22deb34024e969b6ef2
SHA512:	63855f2b99f9e9eaf1a1a9c2836788453bd5b93fc87eb1c35c6aab69c3fa9d6bc5d2d10bb9df5e3e53b8647a9b25b12ec4c4b983088eea78b882d4902550ea03
SSDEEP:	1536:VhT/5UtCT3Ev/UzSEAMT0PY3TlXNFKFGUDuT+h:vOcGNolRUDum
File Content Preview:	.ELF.....4..Bx.....4. ...(.....<h..<h. .....@...@...@....8...X.....dt.Q..... @..(....@.I.....#.....b8..`.....!..... ...@....."..... `..... $ ... ...@.....`....

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:	82552
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	0x12744	0x0	0x6	AX	0	0	4

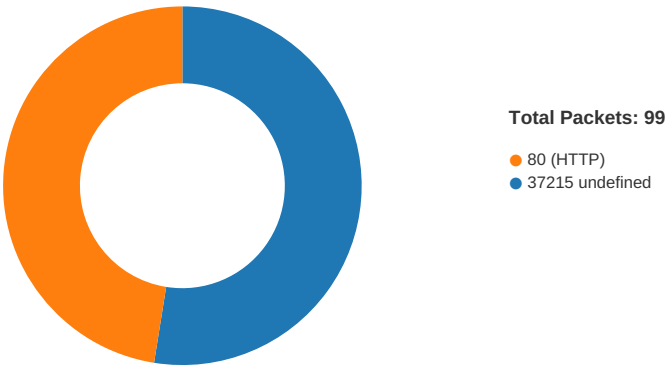
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
.fini	PROGBITS	0x227f4	0x127f4	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x22808	0x12808	0x1460	0x0	0x2	A	0	0	8
.ctors	PROGBITS	0x34000	0x14000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x34008	0x14008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x34018	0x14018	0x220	0x0	0x3	WA	0	0	8
.bss	NOBITS	0x34238	0x14238	0x320	0x0	0x3	WA	0	0	8
.shstrtab	STRTAB	0x0	0x14238	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	0x13c68	0x13c68	3.6697	0x5	R E	0x10000		.init .text .fini .rodata
LOAD	0x14000	0x34000	0x34000	0x238	0x558	1.6811	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

- 192.168.0.14:80

System Behavior

Analysis Process: Dy4UCGJRnG PID: 5239 Parent PID: 5117

General

Start time:	20:19:08
Start date:	29/10/2021
Path:	/tmp/Dy4UCGJRnG
Arguments:	/tmp/Dy4UCGJRnG

File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

File Activities

File Read

Analysis Process: Dy4UCGJRnG PID: 5241 Parent PID: 5239

General

Start time:	20:19:08
Start date:	29/10/2021
Path:	/tmp/Dy4UCGJRnG
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: Dy4UCGJRnG PID: 5242 Parent PID: 5239

General

Start time:	20:19:08
Start date:	29/10/2021
Path:	/tmp/Dy4UCGJRnG
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: Dy4UCGJRnG PID: 5244 Parent PID: 5242

General

Start time:	20:19:08
Start date:	29/10/2021
Path:	/tmp/Dy4UCGJRnG
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: Dy4UCGJRnG PID: 5246 Parent PID: 5242

General

Start time:	20:19:08
Start date:	29/10/2021
Path:	/tmp/Dy4UCGJRnG
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: Dy4UCGJRnG PID: 5247 Parent PID: 5242

General

Start time:	20:19:08
Start date:	29/10/2021
Path:	/tmp/Dy4UCGJRnG
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: Dy4UCGJRnG PID: 5248 Parent PID: 5242

General

Start time:	20:19:08
Start date:	29/10/2021
Path:	/tmp/Dy4UCGJRnG
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e

Analysis Process: Dy4UCGJRnG PID: 5252 Parent PID: 5242

General

Start time:	20:19:08
Start date:	29/10/2021
Path:	/tmp/Dy4UCGJRnG
Arguments:	n/a
File size:	4379400 bytes
MD5 hash:	7dc1c0e23cd5e102bb12e5c29403410e