ID: 491830
Sample Name: mirkatclpb.arm
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 23:50:38
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

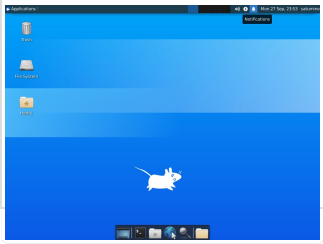
Linux Analysis Report mirkatclpb.arm

Overview

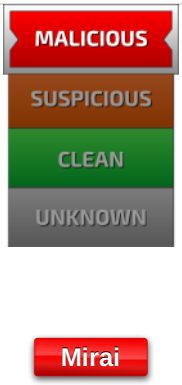
General Information

Sample Name:	mirkatclpb.arm
Analysis ID:	491830
MD5:	f11d4deb3dc1563.
SHA1:	f785ac4c47b9945..
SHA256:	64e0601e1a0a1b..
Infos:	

Most interesting Screenshot:



Detection

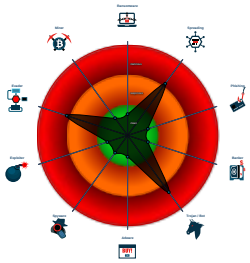


Score:	68
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Sample is packed with UPX
- Uses known network protocols on no...
- Sample tries to kill many processes...
- Sample contains only a LOAD segm...
- Uses the "uname" system call to qu...
- Enumerates processes within the "p...
- Tries to connect to HTTP servers, b...
- Detected TCP or UDP traffic on non...
- Sample listens on a socket
- Sample tries to kill a process (SIGK...

Classification



Analysis Advice

Static ELF header machine description suggests that the sample might only run correctly on MIPS or ARM architectures

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:	33.0.0 White Diamond
Analysis ID:	491830
Start date:	27.09.2021
Start time:	23:50:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	mirkatclpb.arm
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:	mal68.spre.troj.evad.linARM@0/6@0/0
Warnings:	Show All

Process Tree

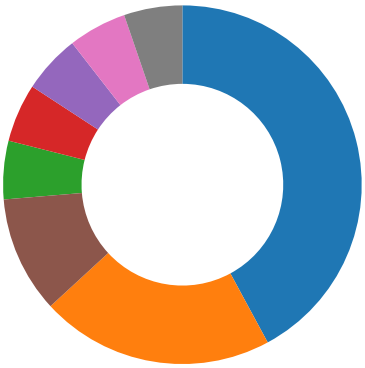
- **system is lnxubuntu20**
- mirkatclpb.arm (PID: 5225, Parent: 5115, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/mirkatclpb.arm
  - mirkatclpb.arm New Fork (PID: 5227, Parent: 5225)
  - mirkatclpb.arm New Fork (PID: 5229, Parent: 5225)
  - mirkatclpb.arm New Fork (PID: 5231, Parent: 5225)
    - mirkatclpb.arm New Fork (PID: 5233, Parent: 5231)
    - mirkatclpb.arm New Fork (PID: 5234, Parent: 5231)
    - mirkatclpb.arm New Fork (PID: 5237, Parent: 5231)
- systemd New Fork (PID: 5261, Parent: 1)
  - sshd (PID: 5261, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5262, Parent: 1)
  - sshd (PID: 5262, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- systemd New Fork (PID: 5356, Parent: 1)
  - sshd (PID: 5356, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5357, Parent: 1)
  - sshd (PID: 5357, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- systemd New Fork (PID: 5358, Parent: 1)
  - sshd (PID: 5358, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5359, Parent: 1)
  - sshd (PID: 5359, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- **cleanup**

Yara Overview

PCAP (Network Traffic)

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

Jbx Signature Overview



- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- 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

Networking:

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

Uses known network protocols on non-standard ports

System Summary:

Sample tries to kill many processes (SIGKILL)

Data Obfuscation:

Sample is packed with UPX

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

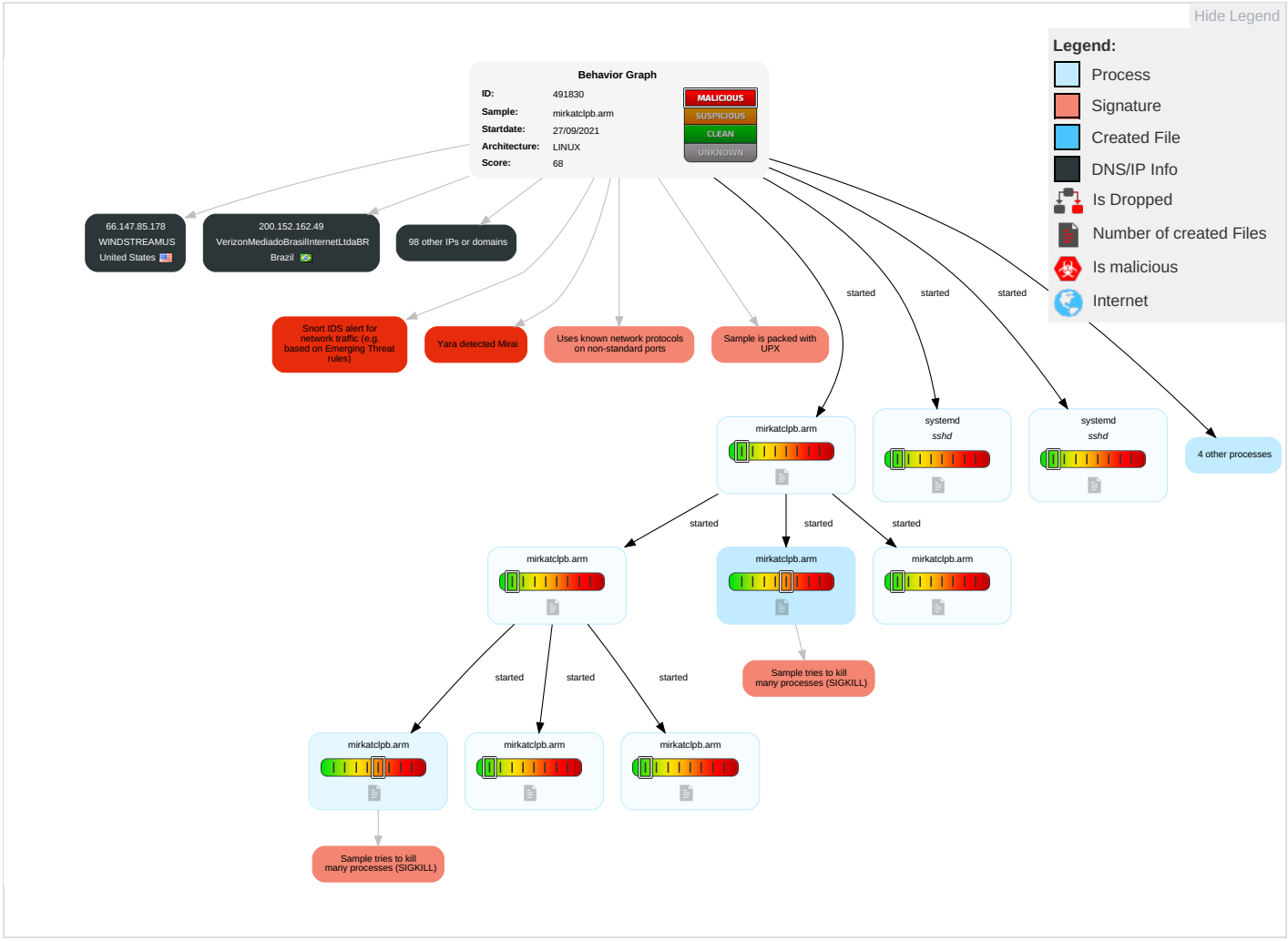
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Obfuscated Files or Information 1	OS Credential Dumping 1	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	Mod Syst Parti
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	Devi Lock
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	Dele Devi Data

Malware Configuration

No configs have been found

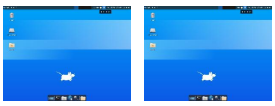
Behavior Graph

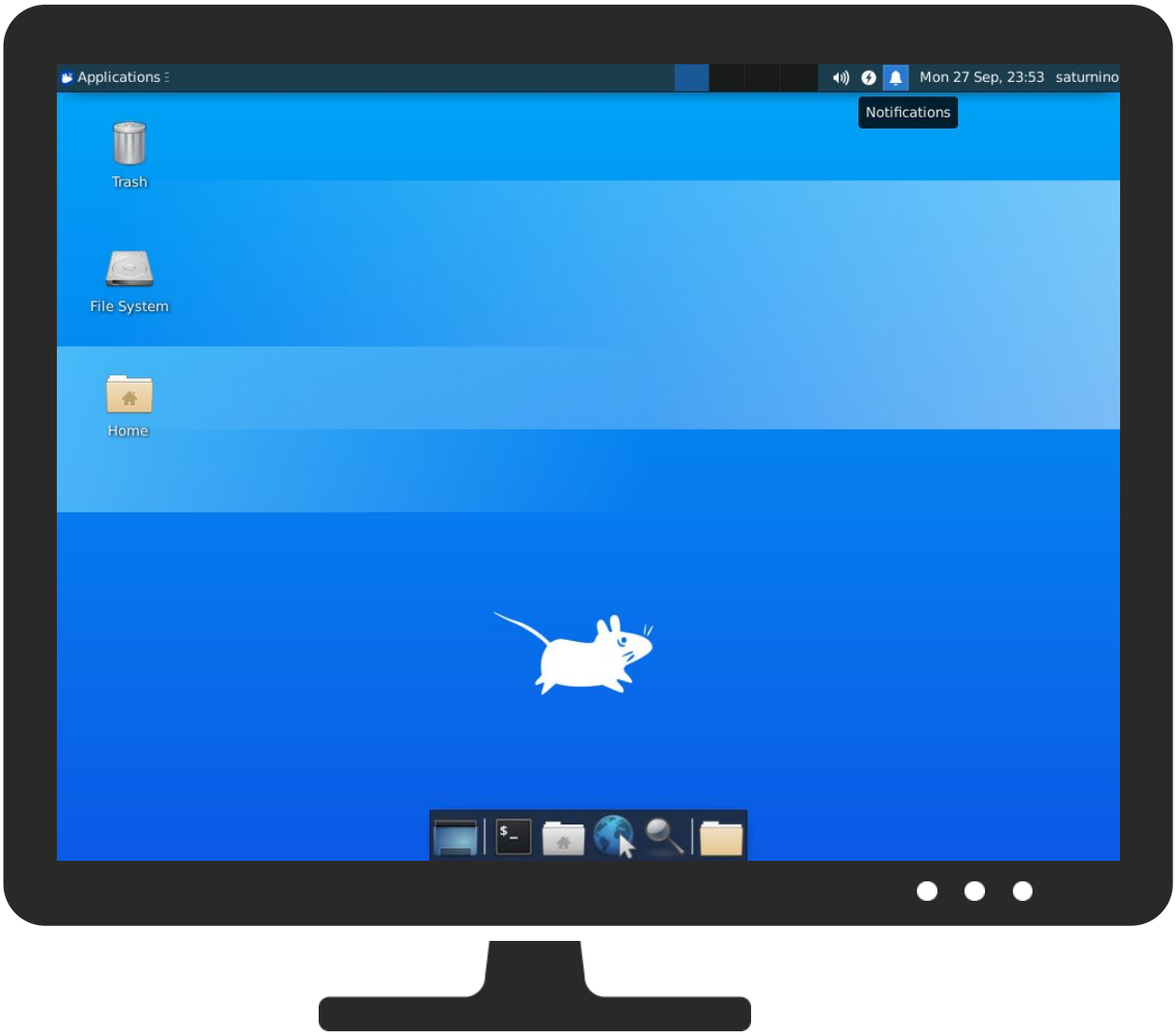


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
213.31.71.244	unknown	Belgium		6871	PLUSNETUKInternetServiceProviderGB	false
166.29.74.82	unknown	United States		206	CSC-IGN-AMERUS	false
14.143.23.189	unknown	India		4755	TATACOMM-ASTATACommunicationsformerlyVSNLisLeadingISP	false
200.152.162.49	unknown	Brazil		28122	VerizonMediadoBrasilInternetLtdaBR	false
206.67.127.12	unknown	United States		701	UUNETUS	false
158.34.190.147	unknown	United States		721	DNIC-ASBLK-00721-00726US	false
247.118.145.156	unknown	Reserved		unknown	unknown	false
23.179.6.168	unknown	Reserved		63297	PACIFIC-SERVERSCA	false
202.236.115.3	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
245.114.66.174	unknown	Reserved		unknown	unknown	false
87.81.175.34	unknown	United Kingdom		5607	BSKYB-BROADBAND-ASGB	false
188.97.180.64	unknown	Germany		3209	VODANETInternationalIP-BackboneofVodafoneDE	false
159.173.54.239	unknown	France		28686	AVECTRIS-ASCH	false
188.248.166.141	unknown	Saudi Arabia		48695	ATHEEB-ASSA	false
253.254.231.181	unknown	Reserved		unknown	unknown	false
102.241.34.87	unknown	Tunisia		36926	CKL1-ASNKE	false
57.67.217.115	unknown	Belgium		51964	ORANGE-BUSINESS-SERVICES-IPSN-ASNFR	false
197.131.99.208	unknown	Morocco		6713	IAM-ASMA	false
14.139.237.177	unknown	India		55824	NKN-CORE-NWNKNCoreNetworkIN	false
173.70.19.51	unknown	United States		701	UUNETUS	false
102.114.79.239	unknown	Mauritius		23889	MauritiusTelecomMU	false
139.196.56.182	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
73.207.81.45	unknown	United States		7922	COMCAST-7922US	false
194.128.173.25	unknown	United Kingdom		702	UUNETUS	false
242.249.209.192	unknown	Reserved		unknown	unknown	false
87.51.208.65	unknown	Denmark		3292	TDCTDCASDK	false
63.148.159.88	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
2.103.215.131	unknown	United Kingdom		13285	OPALTELECOM-ASTalkTalkCommunicationsLimitedGB	false
108.243.173.4	unknown	United States		7018	ATT-INTERNET4US	false
207.90.126.129	unknown	United States		7321	LNET-ASNUS	false
193.245.131.64	unknown	Belgium		3549	LVLT-3549US	false
242.63.95.89	unknown	Reserved		unknown	unknown	false
195.229.184.171	unknown	United Arab Emirates		5384	EMIRATES-INTERNETEmiratesInternetAE	false
180.170.25.215	unknown	China		4812	CHINANET-SH-APChinaTelecomGroupCN	false
174.64.2.29	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
86.52.29.10	unknown	Denmark		197288	STOFANETDK	false
254.91.231.74	unknown	Reserved		unknown	unknown	false
246.141.80.184	unknown	Reserved		unknown	unknown	false
36.90.232.64	unknown	Indonesia		7713	TELKOMNET-AS-APPTTelekomunikasiIndonesiaID	false
135.205.221.76	unknown	United States		6431	ATT-RESEARCHUS	false
250.51.173.213	unknown	Reserved		unknown	unknown	false
84.116.116.140	unknown	Netherlands		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
69.90.190.99	unknown	Canada		13768	COGECO-PEER1CA	false
157.72.178.5	unknown	Japan		131932	JEIS-NETJREastInformationSystemsCompanyJP	false
110.125.97.65	unknown	China		9808	CMNET-GDGuangdongMobileCommunicationCoLtdCN	false
20.21.196.35	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
125.73.254.169	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
1.99.146.64	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
206.9.187.110	unknown	United States		5006	VOYANTUS	false
65.201.108.229	unknown	United States		701	UUNETUS	false
179.48.209.102	unknown	unknown		3816	COLOMBIATELECOMUNICACIONESSAESPCO	false
59.166.150.107	unknown	Japan		9824	JTCL-JP-ASJupiterTelecommunicationCoLtdJP	false
120.161.3.29	unknown	Indonesia		4761	INDOSAT-INP-APINDOSATInternetNetworkProviderID	false
170.73.197.190	unknown	United States		16761	FEDMOG-ASN-01US	false
23.42.205.247	unknown	United States		16625	AKAMAI-ASUS	false
17.103.205.219	unknown	United States		714	APPLE-ENGINEERINGUS	false
66.147.85.178	unknown	United States		7029	WINDSTREAMUS	false
102.74.168.118	unknown	Morocco		6713	IAM-ASMA	false
149.210.199.62	unknown	Netherlands		20857	TRANSIP-ASAmsterdamtheNetherlandsNL	false
221.248.80.1	unknown	Japan		17506	UCOMARTERIANetworksCorporationJP	false
60.16.183.22	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
107.134.158.250	unknown	United States		7018	ATT-INTERNET4US	false
202.200.196.12	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
184.5.225.222	unknown	United States		5778	CENTURYLINK-LEGACY-EMBARQ-RCMTUS	false
151.246.218.21	unknown	Iran (ISLAMIC Republic Of)		31549	RASANAIR	false
117.219.36.68	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	false
220.138.36.103	unknown	Taiwan; Republic of China (ROC)		3462	HINETDataCommunicationBusinessGroupTW	false
16.225.121.0	unknown	United States		unknown	unknown	false
66.12.192.156	unknown	United States		5650	FRONTIER-FRTRUS	false
106.90.12.33	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
216.46.212.245	unknown	United States		19945	GRANBURYISDUS	false
146.123.208.124	unknown	United States		2158	HPESUS	false
250.53.18.17	unknown	Reserved		unknown	unknown	false
159.201.91.21	unknown	United States		1906	NORTHROP-GRUMMANUS	false
165.133.204.80	unknown	Korea Republic of		4961	DISC-AS-KRDaewooInformationSystemsKR	false
31.61.177.115	unknown	Poland		5617	TPNETPL	false
204.233.222.220	unknown	United States		2914	NTT-COMMUNICATIONS-2914US	false
47.90.213.32	unknown	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	false
12.50.93.239	unknown	United States		7018	ATT-INTERNET4US	false
140.220.168.137	unknown	United States		600	OARNET-ASUS	false
221.87.174.160	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
217.202.195.230	unknown	Italy		16232	ASN-TIMServiceProviderIT	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
173.80.22.227	unknown	United States		19108	SUDDENLINK-COMMUNICATIONSUS	false
1.146.71.43	unknown	Australia		1221	ASN-TELSTRATelstraCorporationLtdAU	false
217.95.63.172	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
114.253.135.30	unknown	China		4808	CHINA169-BJChinaUnicomBeijingProvinceNetworkCN	false
243.220.176.106	unknown	Reserved		unknown	unknown	false
38.49.227.144	unknown	United States		174	COGENT-174US	false
254.89.164.115	unknown	Reserved		unknown	unknown	false
175.248.208.227	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
95.27.203.251	unknown	Russian Federation		8402	CORBINA-ASOJSCVimpelcomRU	false
61.32.110.154	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	false
87.4.93.209	unknown	Italy		3269	ASN-IBSNAZIT	false
158.214.59.15	unknown	Japan		2907	SINET-ASResearchOrganizationofInformationandSystemsN	false
192.248.174.124	unknown	France		20473	AS-CHOOPAUS	false
9.35.128.167	unknown	United States		3356	LEVEL3US	false
143.236.35.245	unknown	United States		3128	BRUWS-AS3128US	false
252.4.195.138	unknown	Reserved		unknown	unknown	false
173.197.253.115	unknown	United States		10796	TWC-10796-MIDWESTUS	false
216.224.227.28	unknown	United States		39948	INIT-PHXUS	false

Runtime Messages

Command:	/tmp/mirkatclpb.arm
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	Connected To CNC
Standard Error:	

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CSC-IGN-AMERUS	soramrk.arm7	Get hash	malicious	Browse	• 166.18.138.122
	4czqYWTUq8	Get hash	malicious	Browse	• 166.28.2.6
	dark.x86	Get hash	malicious	Browse	• 166.24.237.116
	sora.x86	Get hash	malicious	Browse	• 20.137.104.111
	jew.x86	Get hash	malicious	Browse	• 166.26.105.225
	RIkJg4Hr71	Get hash	malicious	Browse	• 166.25.76.134
	sora.x86	Get hash	malicious	Browse	• 20.132.107.100
	sora.arm	Get hash	malicious	Browse	• 166.25.76.133
	ayx5kFWYmZ	Get hash	malicious	Browse	• 20.137.104.115

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	x86_64	Get hash	malicious	Browse	• 166.29.182.33
	4nLik56DrD	Get hash	malicious	Browse	• 166.26.55.116
	b3astmode.arm7	Get hash	malicious	Browse	• 166.26.55.112
	x86	Get hash	malicious	Browse	• 166.17.196.159
	K6s3wEt8Ua	Get hash	malicious	Browse	• 166.26.55.100
	r6ZMm6XiWc	Get hash	malicious	Browse	• 166.18.138.185
	M2hPt9E5Fk	Get hash	malicious	Browse	• 166.28.244.239
	RYlggrmClJ	Get hash	malicious	Browse	• 166.29.98.78
	vWV3GzP3vR	Get hash	malicious	Browse	• 166.24.102.124
	vHVNRpNhIs	Get hash	malicious	Browse	• 20.132.231.166
	1isequal9.x86	Get hash	malicious	Browse	• 166.29.121.84
PLUSNETUKInternetServiceProviderGB	8LdKQlRfZG	Get hash	malicious	Browse	• 91.125.96.99
	soramrk.arm7	Get hash	malicious	Browse	• 195.213.49.51
	R4j2V50iCQ	Get hash	malicious	Browse	• 81.141.31.72
	VRVgDYWUED	Get hash	malicious	Browse	• 84.92.157.60
	PNv1wwpUow	Get hash	malicious	Browse	• 80.229.218.105
	sora.x86	Get hash	malicious	Browse	• 209.93.111.137
	UnHAnaAW.x86	Get hash	malicious	Browse	• 31.185.55.182
	TsHIdFKafF	Get hash	malicious	Browse	• 84.92.108.96
	l6l48v5NQD	Get hash	malicious	Browse	• 81.141.79.14
	BLBHEA8knd	Get hash	malicious	Browse	• 84.92.157.59
	Wrg7vnHm5A	Get hash	malicious	Browse	• 195.166.145.100
	uxHuQqDuZc	Get hash	malicious	Browse	• 195.99.43.175
	b3astmode.arm	Get hash	malicious	Browse	• 84.93.18.172
	aXyZQ9O8iB	Get hash	malicious	Browse	• 80.229.86.18
	AJK7j832D2	Get hash	malicious	Browse	• 81.140.202.98
	x86	Get hash	malicious	Browse	• 195.166.145.114
	arm5	Get hash	malicious	Browse	• 80.229.2.221
	dark.sh4	Get hash	malicious	Browse	• 80.229.2.247
	tW7pu9B8A0	Get hash	malicious	Browse	• 84.93.0.213
	77QZ81W0pZ	Get hash	malicious	Browse	• 81.141.55.50

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/proc/5262/oom_score_adj	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped
Size (bytes):	6
Entropy (8bit):	1.7924812503605778
Encrypted:	false
SSDEEP:	3:ptn:Dn
MD5:	CBF282CC55ED0792C33D10003D1F760A
SHA1:	007DD8BD75468E6B7ABA4285E9B267202C7EAEED
SHA-256:	FCDBAB99FCC0F4409E5F9D7D6FC497780288B4C441698126BB62832412774D22
SHA-512:	4643A8675D213C7DA35CC0C2BFB3B6F20324F9C48AEA7BA79F470615698C9A0CEFDA45CAA1957FC29110EE746BC8458AB8AB1E43EB513912A5E1E8858812CC0
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	-1000.

/proc/5357/oom_score_adj	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped
Size (bytes):	6
Entropy (8bit):	1.7924812503605778
Encrypted:	false
SSDEEP:	3:ptn:Dn
MD5:	CBF282CC55ED0792C33D10003D1F760A
SHA1:	007DD8BD75468E6B7ABA4285E9B267202C7EAEED
SHA-256:	FCDBAB99FCC0F4409E5F9D7D6FC497780288B4C441698126BB62832412774D22
SHA-512:	4643A8675D213C7DA35CC0C2BFB3B6F20324F9C48AEA7BA79F470615698C9A0CEFDA45CAA1957FC29110EE746BC8458AB8AB1E43EB513912A5E1E8858812CC 0
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	 -1000.

/proc/5359/oom_score_adj	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped
Size (bytes):	6
Entropy (8bit):	1.7924812503605778
Encrypted:	false
SSDEEP:	3:ptn:Dn
MD5:	CBF282CC55ED0792C33D10003D1F760A
SHA1:	007DD8BD75468E6B7ABA4285E9B267202C7EAEED
SHA-256:	FCDBAB99FCC0F4409E5F9D7D6FC497780288B4C441698126BB62832412774D22
SHA-512:	4643A8675D213C7DA35CC0C2BFB3B6F20324F9C48AEA7BA79F470615698C9A0CEFDA45CAA1957FC29110EE746BC8458AB8AB1E43EB513912A5E1E8858812CC 0
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	 -1000.

/run/sshd.pid	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	1.9219280948873623
Encrypted:	false
SSDEEP:	3:DQe:t
MD5:	D58EE3FB1678D38519A28E681026FE91
SHA1:	DA5269859F42E02B8C6E870022B15E6656B7C425
SHA-256:	E42E7906AE58FC4C8B70F912EC415D0FB2A49A3F54C9FB9D84C66731A1ED0DE6
SHA-512:	DDEA99F3C15931102CF7EAF551FEED190B762F7B597DEF5329CCA576ADD6F5E59885BAAE14D7483BE141B24DBD5D05E2C877DE1C5F978AF60276C28CAC3EB FAC
Malicious:	false
Reputation:	low
Preview:	 5359.

Static File Info

General

File type:	ELF 32-bit LSB executable, ARM, version 1 (ARM), s tatically linked, stripped
Entropy (8bit):	7.929079875154064
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	mirkatclpb.arm
File size:	25004
MD5:	f11d4deb3dc156310b53b21e22c5663a

General	
SHA1:	f785ac4c47b99459a8ce236aa76df115af76dd7f
SHA256:	64e0601e1a0a1bb7f8f170ea14efa55b1f17aaefad94edf0b96cfdbebeb689e8
SHA512:	158581447fc598aa5139b8d93c96b09b82b0b442f6704a4a2fbbe816e8df57e10471899ac9f38d3d34e23d637723d1462e44857db1208b9c57bc507564db18d6
SSDEEP:	768:QX9nxn8o9wnBoWzEQf2EjKb3pWz9s3Uoz2:Qtn+o9wjfBAZWcz2
File Content Preview:	.ELF...a.....(.....4.....4. ...(.....`...`.....^.....Q.td.....CvUPX!.....0...0.....R.....?.E.h;.}...^.....f.Z.6..(fw....&.x:.E.....oe.`.S..T.....n..

Static ELF Info

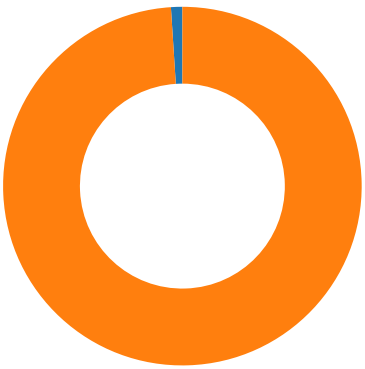
ELF header	
Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	ARM
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	ARM - ABI
ABI Version:	0
Entry Point Address:	0xcf10
Flags:	0x202
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	0
Section Header Size:	40
Number of Section Headers:	0
Header String Table Index:	0

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8000	0x8000	0x60bf	0x60bf	4.0477	0x5	R E	0x8000		
LOAD	0x5ee0	0x1dee0	0x1dee0	0x0	0x0	0.0000	0x6	RW	0x8000		
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

Network Port Distribution



Total Packets: 98

- 23 (Telnet)
- 1312 undefined

TCP Packets

System Behavior

Analysis Process: mirkatclpb.arm PID: 5225 Parent PID: 5115

General

Start time:	23:51:24
Start date:	27/09/2021
Path:	/tmp/mirkatclpb.arm
Arguments:	/tmp/mirkatclpb.arm
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: mirkatclpb.arm PID: 5227 Parent PID: 5225

General

Start time:	23:51:25
Start date:	27/09/2021
Path:	/tmp/mirkatclpb.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: mirkatclpb.arm PID: 5229 Parent PID: 5225

General

Start time:	23:51:25
Start date:	27/09/2021
Path:	/tmp/mirkatclpb.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: mirkatclpb.arm PID: 5231 Parent PID: 5225

General

Start time:	23:51:25
Start date:	27/09/2021
Path:	/tmp/mirkatclpb.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: mirkatclpb.arm PID: 5233 Parent PID: 5231

General

Start time:	23:51:25
Start date:	27/09/2021
Path:	/tmp/mirkatclpb.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: mirkatclpb.arm PID: 5234 Parent PID: 5231

General

Start time:	23:51:25
Start date:	27/09/2021
Path:	/tmp/mirkatclpb.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: mirkatclpb.arm PID: 5237 Parent PID: 5231

General

Start time:	23:51:25
Start date:	27/09/2021
Path:	/tmp/mirkatclpb.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: systemd PID: 5261 Parent PID: 1

General

Start time:	23:51:40
Start date:	27/09/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes

MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5261 Parent PID: 1

General

Start time:	23:51:40
Start date:	27/09/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -t
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5262 Parent PID: 1

General

Start time:	23:51:42
Start date:	27/09/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5262 Parent PID: 1

General

Start time:	23:51:42
Start date:	27/09/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -D
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: systemd PID: 5356 Parent PID: 1

General

Start time:	23:54:23

Start date:	27/09/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5356 Parent PID: 1

General

Start time:	23:54:23
Start date:	27/09/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -t
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5357 Parent PID: 1

General

Start time:	23:54:24
Start date:	27/09/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5357 Parent PID: 1

General

Start time:	23:54:24
Start date:	27/09/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -D
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

File Written

Directory Enumerated

Analysis Process: systemd PID: 5358 Parent PID: 1

General

Start time:	23:54:26
Start date:	27/09/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5358 Parent PID: 1

General

Start time:	23:54:26
Start date:	27/09/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -t
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

Directory Enumerated

Analysis Process: systemd PID: 5359 Parent PID: 1

General

Start time:	23:54:26
Start date:	27/09/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5359 Parent PID: 1

General

Start time:	23:54:26
Start date:	27/09/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -D
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

File Written

Directory Enumerated