ID: 513293
Sample Name: Hilix.arm
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 01:45:33
Date: 02/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

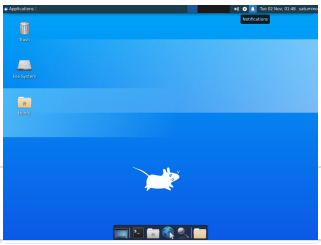
Linux Analysis Report Hilix.arm

Overview

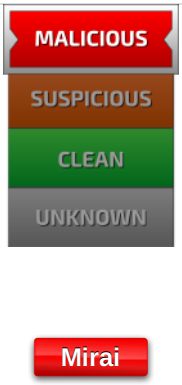
General Information

Sample Name:	Hilix.arm
Analysis ID:	513293
MD5:	9653f94dca32a23.
SHA1:	a7037a2353ddf06.
SHA256:	dcd35159cd640f9..
Tags:	Mirai
Infos:	

Most interesting Screenshot:



Detection

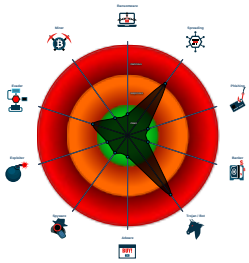


Score:	76
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Uses known network protocols on no...
- Sample tries to kill many processes...
- 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...
- Enumerates processes within the "p...
- Tries to connect to HTTP servers, b...
- Detected TCP or UDP traffic on non...

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:	34.0.0 Boulder Opal
Analysis ID:	513293
Start date:	02.11.2021
Start time:	01:45:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Hilix.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:	mal76.spre.troj.linARM@0/6@0/0
Warnings:	Show All

Process Tree

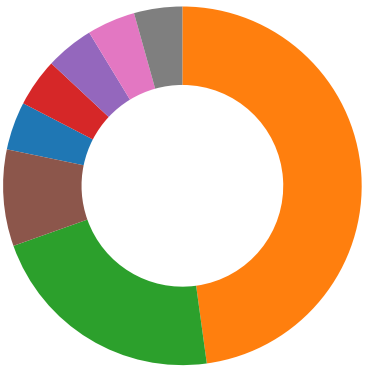
- **system is lnxubuntu20**
- Hilix.arm (PID: 5244, Parent: 5115, MD5: 5ebfcae4fe2471fcc5695c2394773ff1) Arguments: /tmp/Hilix.arm
  - Hilix.arm New Fork (PID: 5246, Parent: 5244)
  - Hilix.arm New Fork (PID: 5247, Parent: 5244)
  - Hilix.arm New Fork (PID: 5248, Parent: 5244)
    - Hilix.arm New Fork (PID: 5252, Parent: 5248)
    - Hilix.arm New Fork (PID: 5253, Parent: 5248)
    - Hilix.arm New Fork (PID: 5255, Parent: 5248)
    - Hilix.arm New Fork (PID: 5257, Parent: 5248)
    - Hilix.arm New Fork (PID: 5260, Parent: 5248)
- systemd New Fork (PID: 5289, Parent: 1)
  - sshd (PID: 5289, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5290, Parent: 1)
  - sshd (PID: 5290, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- systemd New Fork (PID: 5404, Parent: 1)
  - sshd (PID: 5404, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5405, Parent: 1)
  - sshd (PID: 5405, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -D
- systemd New Fork (PID: 5408, Parent: 1)
  - sshd (PID: 5408, Parent: 1, MD5: dbca7a6bbf7bf57fedac243d4b2cb340) Arguments: /usr/sbin/sshd -t
- systemd New Fork (PID: 5409, Parent: 1)
  - sshd (PID: 5409, 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



- AV Detection
- Networking
- System Summary
- 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

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)

System Summary:

Sample tries to kill many processes (SIGKILL)

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

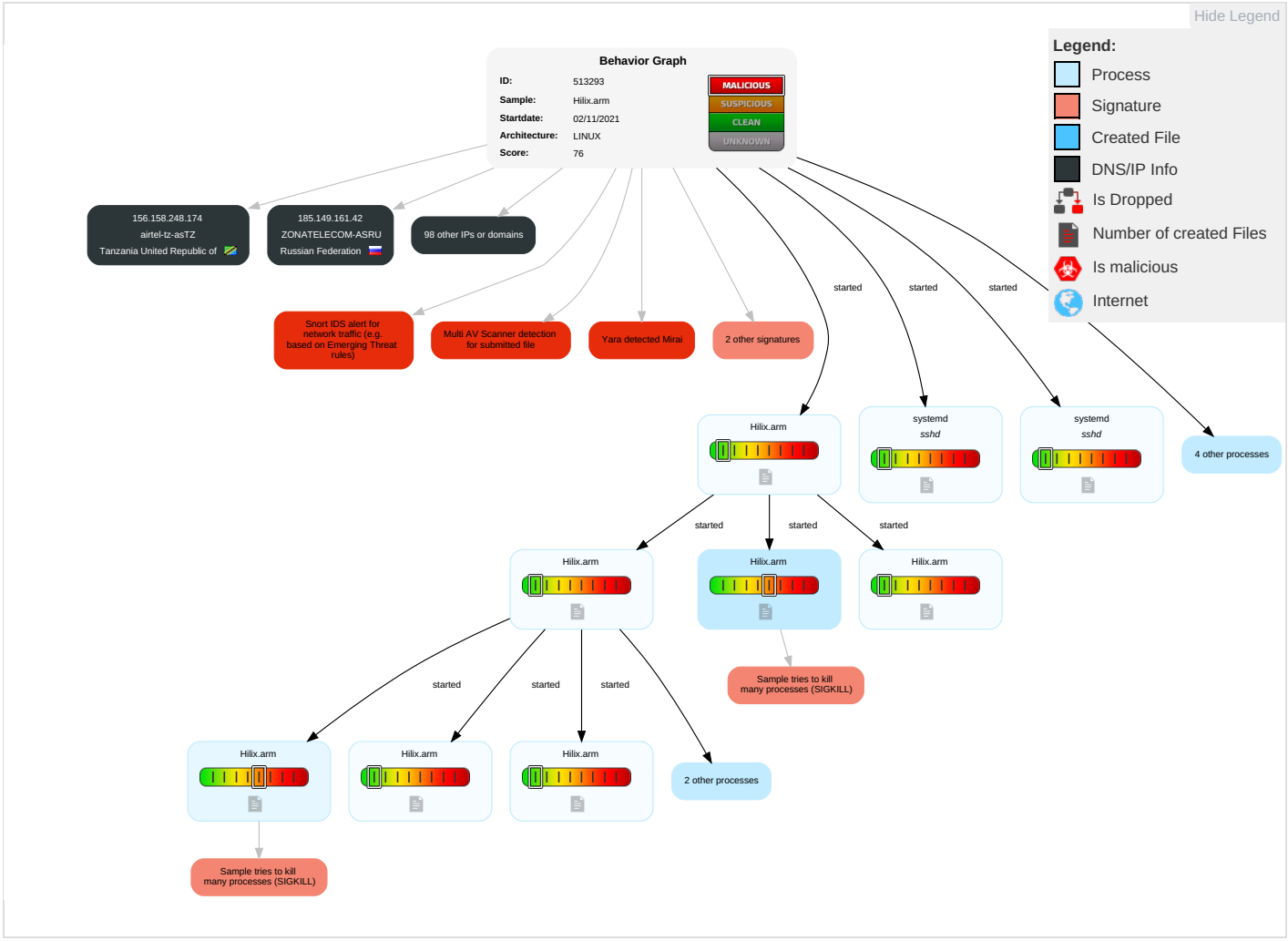
Mitre Att&ck Matrix

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 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	Modify System Partitio
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 Lockou
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

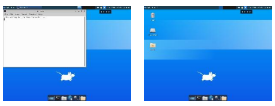
Behavior Graph

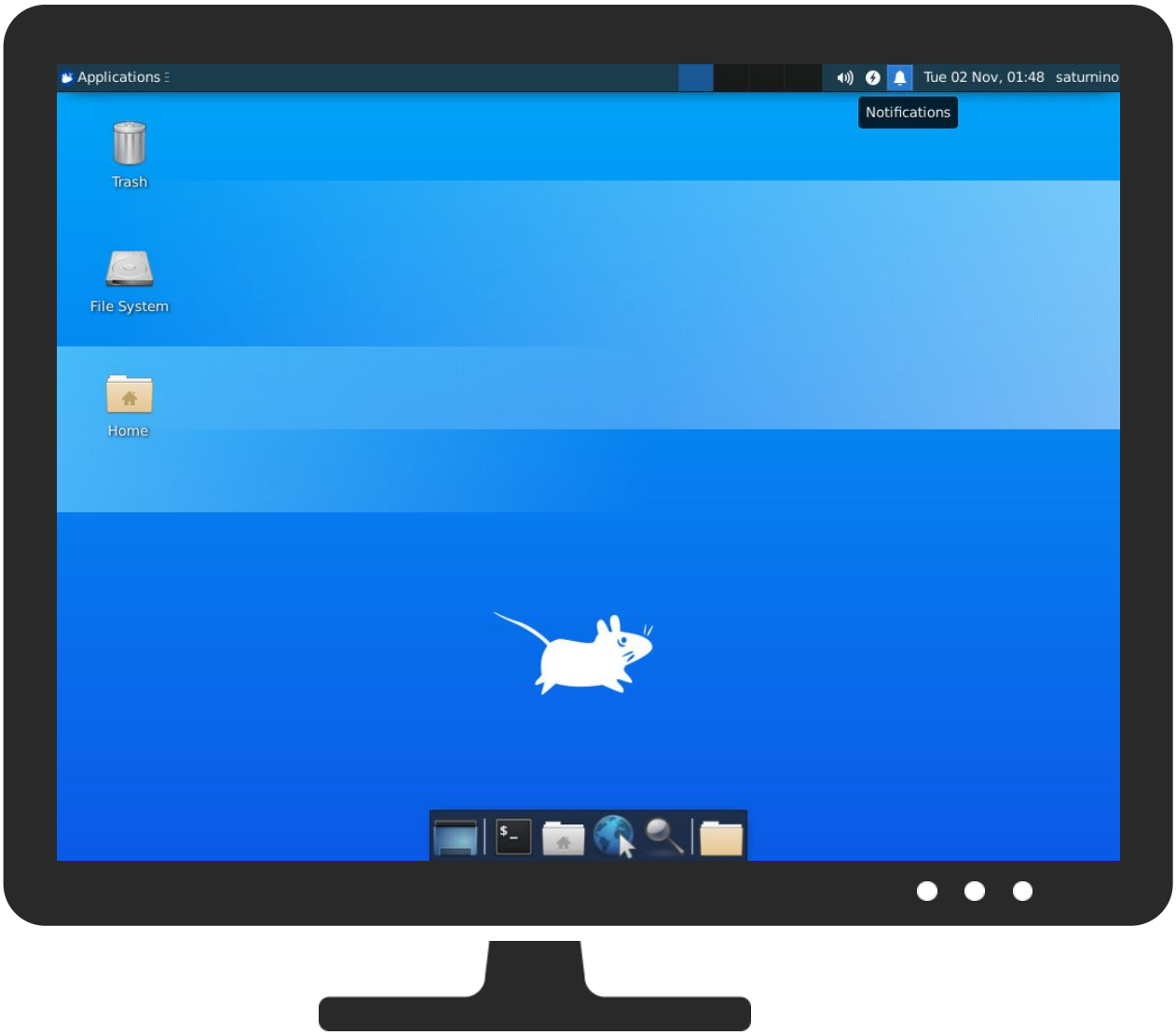


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Hilix.arm	53%	Virustotal		Browse
Hilix.arm	64%	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://37.0.9.202/bins/Hilix.mips	9%	Virustotal		Browse
http://37.0.9.202/bins/Hilix.mips	100%	Avira URL Cloud	malware	
http://127.0.0.1:52869/wanipcn.xml	0%	Virustotal		Browse
http://127.0.0.1:52869/wanipcn.xml	0%	Avira URL Cloud	safe	

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
45.104.67.34	unknown	Egypt		37069	MOBINILEG	false
185.119.218.5	unknown	Czech Republic		198167	APPTOCLOUDAppToCloudserversvpsCZ	false
91.52.65.178	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
45.128.22.52	unknown	Denmark		201290	BLACKGATENL	false
219.56.220.39	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
156.49.160.17	unknown	Sweden		29975	VODACOM-ZA	false
17.30.215.164	unknown	United States		714	APPLE-ENGINEERINGUS	false
156.254.70.171	unknown	Seychelles		135357	SKHT-ASShenzhenKatherineHengTechnologyInformationCo	false
38.206.46.24	unknown	United States		9009	M247GB	false
91.19.165.50	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
91.75.212.117	unknown	United Arab Emirates		15802	DU-AS1AE	false
91.120.152.33	unknown	Hungary		5588	GTSCEGTSCentralEuropeAntelGermanyCZ	false
90.70.5.162	unknown	France		3215	FranceTelecom-OrangeFR	false
141.150.163.18	unknown	United States		701	UUNETUS	false
95.156.176.206	unknown	Bosnia and Herzegowina		20875	HPTNET-ASBA	false
185.106.143.34	unknown	Serbia		7979	SERVERS-COMUS	false
38.181.75.64	unknown	United States		174	COGENT-174US	false
91.30.56.29	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
91.54.122.242	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
45.206.28.0	unknown	Seychelles		328608	Africa-on-Cloud-ASZA	false
59.1.188.143	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
77.110.64.247	unknown	Lebanon		34610	RIKSNETSE	false
45.9.143.74	unknown	Russian Federation		209038	ALEXGEINERMSKRU	false
45.18.215.62	unknown	United States		7018	ATT-INTERNET4US	false
185.75.12.212	unknown	Spain		201942	SOLTIAES	false
91.74.73.94	unknown	United Arab Emirates		15802	DU-AS1AE	false
185.38.220.169	unknown	Poland		56523	AMELEKTRONIKPL	false
185.23.188.242	unknown	France		60532	RENTACLOUDFR	false
45.63.53.230	unknown	United States		20473	AS-CHOOPAUS	false
45.237.157.87	unknown	Brazil		268286	TECHPIGNATONTELECOMBR	false
185.35.202.71	unknown	Norway		50304	BLIXNO	false
185.169.213.42	unknown	Germany		13012	GENIAS-ASDE	false
79.103.170.140	unknown	Greece		1241	FORTHNET-GRForthnetEU	false
176.196.62.156	unknown	Russian Federation		39927	ELIGHT-ASRU	false
194.28.179.238	unknown	Ukraine		197073	KUZNETSOVSK-ASUA	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.185.140.128	unknown	Brazil		269378	INFINITETELECOMBR	false
185.149.161.42	unknown	Russian Federation		61131	ZONATELECOM-ASRU	false
142.166.65.28	unknown	Canada		855	CANET-ASN-4CA	false
189.172.103.25	unknown	Mexico		8151	UninetSAdeCVMX	false
59.27.2.25	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
45.50.54.63	unknown	United States		20001	TWC-20001-PACWESTUS	false
185.19.109.133	unknown	United Kingdom		17804	LAODC-AS-APLaoDataCenterLA	false
190.94.7.150	unknown	Dominican Republic		12066	ALTICEDOMINICANASADO	false
41.239.218.36	unknown	Egypt		8452	TE-ASTE-ASEG	false
89.67.99.56	unknown	Poland		6830	LIBERTYGLOBALLibertyGlobalformerlyUPCBroadbandHolding	false
45.199.228.211	unknown	Seychelles		8100	ASN-QUADRANET-GLOBALUS	false
45.126.216.220	unknown	Hong Kong		23470	RELIABLESITEUS	false
99.56.5.185	unknown	United States		7018	ATT-INTERNET4US	false
197.164.175.168	unknown	Egypt		24863	LINKdotNET-ASEG	false
45.9.143.98	unknown	Russian Federation		209038	ALEXGEINERMSKRU	false
45.52.96.195	unknown	United States		5650	FRONTIER-FRTRUS	false
185.124.199.108	unknown	Germany		3337	KOMATSUDE	false
41.17.0.118	unknown	South Africa		29975	VODACOM-ZA	false
173.70.19.34	unknown	United States		701	UUNETUS	false
185.15.150.55	unknown	Spain		199930	WIFIBALEARES-ASCSabaters13ES	false
45.55.195.228	unknown	United States		14061	DIGITALOCEAN-ASNUS	false
185.187.222.120	unknown	Italy		31543	MYNET-ASmyNETgmbhAT	false
154.82.151.120	unknown	Seychelles		32708	ROOTNETWORKSUS	false
17.112.167.99	unknown	United States		714	APPLE-ENGINEERINGUS	false
2.41.35.61	unknown	Italy		30722	VODAFONE-IT-ASNIT	false
91.13.61.237	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
194.253.157.141	unknown	European Union		1759	TSF-IP-CORETeliaFinlandOyjEU	false
113.51.241.67	unknown	China		17506	UCOMARTERIANetworksCorporationJP	false
173.184.189.173	unknown	United States		7029	WINDSTREAMUS	false
185.192.230.56	unknown	United Kingdom		5503	RMIFLGB	false
156.158.248.174	unknown	Tanzania United Republic of		37133	airtel-tz-asTZ	false
41.45.223.165	unknown	Egypt		8452	TE-ASTE-ASEG	false
36.118.160.38	unknown	China		4847	CNIX-APChinaNetworksInter-ExchangeCN	false
41.17.127.1	unknown	South Africa		29975	VODACOM-ZA	false
5.218.125.60	unknown	Iran (ISLAMIC Republic Of)		197207	MCCI-ASIR	false
45.145.30.193	unknown	Turkey		197328	INETLTDTR	false
90.255.143.236	unknown	United Kingdom		5378	VodafoneGB	false
45.1.177.234	unknown	United States		7377	UCSDUS	false
53.82.186.160	unknown	Germany		31399	DAIMLER-ASITIGNGlobalNetworkDE	false
143.10.148.65	unknown	United States		11003	PANDGUS	false
59.218.207.68	unknown	China		2516	KDDIKDDICORPORATIONJP	false
222.202.165.36	unknown	China		4538	ERX-CERNET-BKBChinaEducationandResearchNetworkCenter	false
91.90.138.39	unknown	Israel		25046	CHECKPOINTIL	false
197.173.155.25	unknown	South Africa		37168	CELL-CZA	false
68.97.175.155	unknown	United States		22773	ASN-CXA-ALL-CCI-22773-RDCUS	false
37.155.189.38	unknown	Turkey		20978	TT_MOBILIstanbulTR	false
45.197.137.128	unknown	Seychelles		133201	COMING-ASABCDEGROUPCOMPANYLIMITEDHK	false
96.151.55.151	unknown	United States		7922	COMCAST-7922US	false
91.74.182.121	unknown	United Arab Emirates		15802	DU-AS1AE	false
91.60.221.230	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.235.70.182	unknown	Ukraine		33817	TELEGROUPUA-ASUA	false
91.5.97.3	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false
57.159.196.85	unknown	Belgium		2686	ATGS-MMD-ASUS	false
45.18.240.22	unknown	United States		7018	ATT-INTERNET4US	false
41.77.181.171	unknown	Algeria		36974	AFNET-ASCI	false
45.122.192.3	unknown	China		63535	FFANChengduWandaElectronicInformationTechnologyCoLtd	false
91.67.33.158	unknown	Germany		31334	KABELDEUTSCHLAND-ASDE	false
179.77.43.231	unknown	Brazil		26615	TIMSABR	false
173.12.201.233	unknown	United States		7922	COMCAST-7922US	false
45.130.62.123	unknown	Israel		60781	LEASEWEB-NL-AMS-01NetherlandsNL	false
185.21.99.54	unknown	Austria		49808	POWERSPEED-ASAT	false
185.70.118.221	unknown	Italy		204482	EPICLINK-ASIT	false
41.80.99.57	unknown	Kenya		33771	SAFARICOM-LIMITEDKE	false
45.242.108.39	unknown	Egypt		24863	LINKdotNET-ASEG	false
91.18.128.111	unknown	Germany		3320	DTAGInternetserviceprovideroperationsDE	false

Runtime Messages

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

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.63.53.230	NMlnVly7uv	Get hash	malicious	Browse	
45.128.22.52	leyw73RE9o	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DTAGInternetserviceprovideroperationsDE	L831wSjET5	Get hash	malicious	Browse	• 93.254.197.52
	JVHk2b1Yd5	Get hash	malicious	Browse	• 31.229.195.240
	Hilix.arm7	Get hash	malicious	Browse	• 91.21.45.255
	Hilix.x86	Get hash	malicious	Browse	• 91.29.31.23
	dUW6YG1Tdv	Get hash	malicious	Browse	• 31.237.215.12
	RPov9E0iot	Get hash	malicious	Browse	• 91.19.190.168
	uohdbohpYb	Get hash	malicious	Browse	• 91.27.218.9
	oiHTZaiKnI	Get hash	malicious	Browse	• 62.227.13.104
	7DoAjWX5uZ	Get hash	malicious	Browse	• 84.140.96.185
	1Y2rsDBP9s	Get hash	malicious	Browse	• 194.25.81.149
	t7WU0JjLAR	Get hash	malicious	Browse	• 80.156.66.212
	Yoshi.arm7	Get hash	malicious	Browse	• 193.159.83.138
	Yoshi.arm	Get hash	malicious	Browse	• 217.92.199.99
	arm	Get hash	malicious	Browse	• 31.240.167.60

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	arm7-20211101-1513	Get hash	malicious	Browse	• 84.176.76.151
	mips	Get hash	malicious	Browse	• 93.222.116.118
	JjHQ8Q1weT	Get hash	malicious	Browse	• 84.178.181.33
	anWxzNav9N	Get hash	malicious	Browse	• 87.152.224.174
	mxHkqAIYT0	Get hash	malicious	Browse	• 79.236.87.239
	Antisocial.x86	Get hash	malicious	Browse	• 84.136.240.4
MOBINILEG	Hilix.arm7	Get hash	malicious	Browse	• 45.104.67.35
	WhFNix8BoE	Get hash	malicious	Browse	• 102.15.76.212
	Hilix.x86	Get hash	malicious	Browse	• 105.45.177.25
	yVbcX1sEtS	Get hash	malicious	Browse	• 197.151.24 0.163
	SZAYTvvY9Y	Get hash	malicious	Browse	• 154.134.17 9.153
	BVBf45GBHP	Get hash	malicious	Browse	• 105.35.52.129
	u4M7XeqKtD	Get hash	malicious	Browse	• 154.130.49.5
	Yoshi.arm7	Get hash	malicious	Browse	• 105.37.57.179
	JjHQ8Q1weT	Get hash	malicious	Browse	• 105.182.20 4.221
	Antisocial.x86	Get hash	malicious	Browse	• 45.106.6.116
	Antisocial.arm	Get hash	malicious	Browse	• 45.104.92.31
	w66OTKGVFv	Get hash	malicious	Browse	• 45.104.148.77
	swOGb2sZYt	Get hash	malicious	Browse	• 45.104.148.98
	ydZLm6GD56	Get hash	malicious	Browse	• 45.111.37.156
	BitmCvTrdO	Get hash	malicious	Browse	• 45.104.148.75
	UQnO4DB8Z1	Get hash	malicious	Browse	• 45.99.107.249
	OhUy3woBmb	Get hash	malicious	Browse	• 45.103.171.147
	yxD7DmfG2j	Get hash	malicious	Browse	• 41.91.249.173
	x86	Get hash	malicious	Browse	• 105.180.23.14
	jGVlUAzDbQ	Get hash	malicious	Browse	• 154.128.84.191
BLACKGATENL	sora.x86	Get hash	malicious	Browse	• 45.128.22.98
	u9afRawaNV	Get hash	malicious	Browse	• 45.128.22.99
	x86-20211004-1530	Get hash	malicious	Browse	• 45.128.22.84
	65FRc9Gooh	Get hash	malicious	Browse	• 45.128.22.98
	leyw73RE9o	Get hash	malicious	Browse	• 45.128.22.52

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

/proc/5290/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:	high, very likely benign file
Preview:	-1000.

/proc/5405/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:	high, very likely benign file
Preview:	 -1000.

/proc/5409/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:	high, very likely benign file
Preview:	 -1000.

/run/sshd.pid	
Process:	/usr/sbin/sshd
File Type:	ASCII text
Category:	dropped
Size (bytes):	5
Entropy (8bit):	2.321928094887362
Encrypted:	false
SSDEEP:	3:E2v:EI
MD5:	B7E7F61E602E76B7E029FB1017EF47D8
SHA1:	6E59553854D7D99CB393905261B0B22600C3B713
SHA-256:	5A7BB77B731A3ECC715295E4F9ED20A306B64677B40260C2940B368339B7C50C
SHA-512:	65F0C1B62D7305AA7C644803CB310EAFD3195D941A2FBCAF03A9F835E00C795F1A6F111EBEEA44DAC9BCDF10BF11B24F938CA553B23702CB92316E05AFEC33 A9
Malicious:	false
Reputation:	low
Preview:	 5409.

Static File Info

General

File type:	ELF 32-bit LSB executable, ARM, version 1 (ARM), s tatically linked, stripped
Entropy (8bit):	6.095639721571195
TrID:	• ELF Executable and Linkable format (generic) (4004/1) 100.00%
File name:	Hilix.arm
File size:	62456
MD5:	9653f94dca32a23046c21ffeea172dd6

General	
SHA1:	a7037a2353ddf06c10144563b077c906b92ebbfa
SHA256:	dcd35159cd640f9b66aad91d5dc7d1e81fffd2478c1e44e0f3184db70285040f
SHA512:	eee662344819192c92fbc4fd428442c7702055a1f9eaa44edac679ba861d3062bd4297605038e87efa32897be286ce460daca7defcd911e5f225bef917ecdd6e
SSDEEP:	1536:UyW869O3GXz/z8a5OI2s/9M53e53mc0PKwl5p/a+53m:Uyx6EK3wRs/+5ORmhCwl5Ml
File Content Preview:	.ELF...a.....(.....4...h.....4. ...(.....(.....Q.td.....-...L."....6.....0@-.\P...0....S.0...P@...0... ....R.....0...0.....0.. .. ....R..... 0....S

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:	0x8190
Flags:	0x202
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	62056
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	0x8094	0x94	0x18	0x0	0x6	AX	0	0	4
.text	PROGBITS	0x80b0	0xb0	0xdb00	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x15bb0	0xdbb0	0x14	0x0	0x6	AX	0	0	4
.rodata	PROGBITS	0x15bc4	0xdbc4	0x1108	0x0	0x2	A	0	0	4
.ctors	PROGBITS	0x1f000	0xf000	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x1f008	0xf008	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x1f014	0xf014	0x214	0x0	0x3	WA	0	0	4
.bss	NOBITS	0x1f228	0xf228	0x2e8	0x0	0x3	WA	0	0	4
.shstrtab	STRTAB	0x0	0xf228	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	0x8000	0x8000	0xeccc	0xeccc	3.3634	0x5	R E	0x8000		.init .text .fini .rodata
LOAD	0xf000	0x1f000	0x1f000	0x228	0x510	1.5752	0x6	RW	0x8000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x7	RWE	0x4		

Network Behavior

TCP Packets

HTTP Request Dependency Graph

- 127.0.0.1:52869

System Behavior

Analysis Process: Hilix.arm PID: 5244 Parent PID: 5115

General

Start time:	01:46:13
Start date:	02/11/2021
Path:	/tmp/Hilix.arm
Arguments:	/tmp/Hilix.arm
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Analysis Process: Hilix.arm PID: 5246 Parent PID: 5244

General

Start time:	01:46:13
Start date:	02/11/2021
Path:	/tmp/Hilix.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: Hilix.arm PID: 5247 Parent PID: 5244

General

Start time:	01:46:13
Start date:	02/11/2021
Path:	/tmp/Hilix.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: Hilix.arm PID: 5248 Parent PID: 5244

General

Start time:	01:46:13
Start date:	02/11/2021
Path:	/tmp/Hilix.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: Hilix.arm PID: 5252 Parent PID: 5248

General

Start time:	01:46:13
Start date:	02/11/2021
Path:	/tmp/Hilix.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

File Activities

File Read

Directory Enumerated

Analysis Process: Hilix.arm PID: 5253 Parent PID: 5248

General

Start time:	01:46:13
Start date:	02/11/2021
Path:	/tmp/Hilix.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: Hilix.arm PID: 5255 Parent PID: 5248

General

Start time:	01:46:13
Start date:	02/11/2021
Path:	/tmp/Hilix.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: Hilix.arm PID: 5257 Parent PID: 5248

General

Start time:	01:46:13
Start date:	02/11/2021
Path:	/tmp/Hilix.arm

Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: Hilix.arm PID: 5260 Parent PID: 5248

General

Start time:	01:46:13
Start date:	02/11/2021
Path:	/tmp/Hilix.arm
Arguments:	n/a
File size:	4956856 bytes
MD5 hash:	5ebfcae4fe2471fcc5695c2394773ff1

Analysis Process: systemd PID: 5289 Parent PID: 1

General

Start time:	01:46:26
Start date:	02/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5289 Parent PID: 1

General

Start time:	01:46:26
Start date:	02/11/2021
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: 5290 Parent PID: 1

General

Start time:	01:46:27
Start date:	02/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5290 Parent PID: 1

General

Start time:	01:46:27
Start date:	02/11/2021
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: 5404 Parent PID: 1

General

Start time:	01:49:13
Start date:	02/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5404 Parent PID: 1

General

Start time:	01:49:13
Start date:	02/11/2021
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: 5405 Parent PID: 1

General

Start time:	01:49:13
Start date:	02/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a

File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5405 Parent PID: 1

General

Start time:	01:49:13
Start date:	02/11/2021
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: 5408 Parent PID: 1

General

Start time:	01:49:16
Start date:	02/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5408 Parent PID: 1

General

Start time:	01:49:16
Start date:	02/11/2021
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: 5409 Parent PID: 1

General

Start time:	01:49:16
Start date:	02/11/2021
Path:	/usr/lib/systemd/systemd
Arguments:	n/a
File size:	1620224 bytes
MD5 hash:	9b2bec7092a40488108543f9334aab75

Analysis Process: sshd PID: 5409 Parent PID: 1

General

Start time:	01:49:16
Start date:	02/11/2021
Path:	/usr/sbin/sshd
Arguments:	/usr/sbin/sshd -D
File size:	876328 bytes
MD5 hash:	dbca7a6bbf7bf57fedac243d4b2cb340

File Activities

File Read

File Written

Directory Enumerated