ABUSE REPORT

activity against www.asp-waf.com by

Wowrack.com

reported from Fri 25 Mar 22 till Sun 27 Mar 22

ABUSE REPORT
ISP Range WOW-IPV4-NET3

Incidents recorded between 25/03/2022 17:06:06 and 27/03/2022 07:23:18 UTC

To:
Wowrack.com12201 Tukwila
International Blvd
STE 100
Seattle
WA
98168
United States

Email abuse@Wowrack.com

From:
VESNX SA
29 Boulevard Grande Duchesse
Charlotte, 1331 Luxembourg,
Luxembourg
support@asp-waf.com
Domain : www.asp-waf.com

Date : 31 March 2022
Reference : WOW-IPV4-NET3-2022.84-2022.86 - 2
Regarding : Malicious activity detected against www.asp-waf.com dating 25/03/2022 17:06:06UTC - 27/03/2022 07:23:18UTC

Dear Sir/ Madam

This report is addressed to you based on activity that has been triggered by 1 IP addresses that are maintained by you.

We refer to the malicious activity that has been reported. In case you only host the hardware and not the hereafter mentioned IP addresses, we ask you kindly to contact us at support@asp-waf.com within 30 days.

In order to avoid further abuse through your hosted IP address(es) please address the issue internally within 5 working days.

To safeguard the domain www.asp-waf.com we will activate protective measures.

We expect an update regarding this matter and hereby inform you that we reserve the right to claim any damage made and communicate this report with cybercrime related law enforcement.

Thank you for your cooperation in this matter

Yours sincerely

TABLE OF CONTENTS

MANAGEMENT OVERVIEW

Activity against www.asp-waf.com by Wowrack.com

based on data captured from Mon 28 Feb 22 till Thu 31 Mar 22
for IP range 216.244.64.0 - 216.244.95.255 (8'191 IP in scope)

Every request against www.asp-waf.com is validated against the firewall's Guard-Modules and if any of the modules detects that then an incident is generated, this report contains detections with the following patterns:

2 attempts to URL exploit

Abuse score-card Wowrack.com

on the 19082 days between Thu 01 Jan 1970 and Thu 31 Mar 2022

IP addresses	:	1	IP addresses with incidents	:	1
HTTP requests served	:	42	HTTP incidents	:	6
IP address with port attacks	:	-	Last port attack	:	-
Ports attacked	:	-	Port based Incidents	:	-
Talking IP addresses	:	-	Last Talk	:	-
Talking Applications	:	-	Talks Detected	:	-

on the 31 days between Mon 28 Feb 2022 and Thu 31 Mar 2022

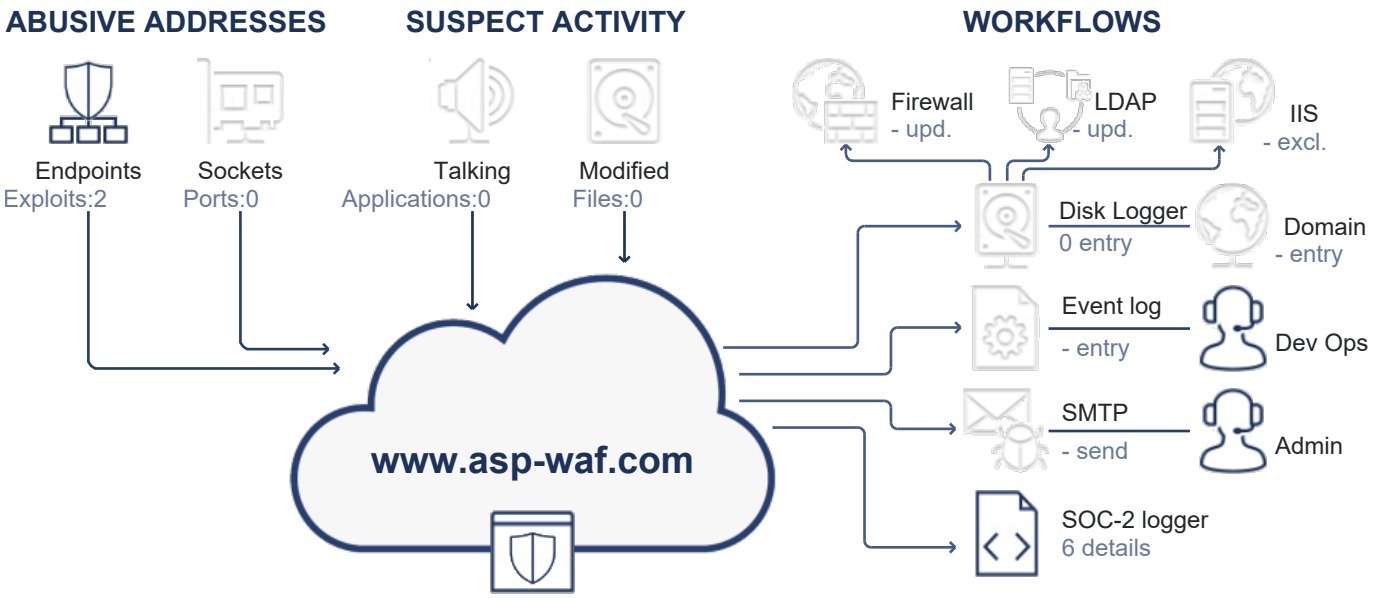
IP Addresses	:	1	IP addresses with incidents	:	-
HTTP requests served	:	39	HTTP incidents	:	-
IP address with port attacks	:	-	Last port attack	:	-
Ports attacked	:	-	Port based incidents	:	-

** The first priority of the ASP-WAF firewall is to protect the application, reporting, even though important comes second. Please consult the glossary for a detailed explanation of each metric.*

view activity diagram on the next page

ACTIVITY

Activity, response and impact visualization



REQUESTS BY ACTOR

Requests	39
Human	0
Bot	39
BlackHat	0
Abusive Search Engine	0
Search Engine	0

REQUEST CLASSIFICATION

OK	39
Suspect	0
Redirected	0
Blocked	0

DETECTED ATTACK VECTORS

2 an attempted access protected resources
2 continued attempted to probe exploits after being warned
2 repetitive visits while attempting to probe for exploits
2 repetitive attempts to probe for exploits
2 uses URL phishing to probe the system

ABUSE OVERVIEW

The malicious activity documented in the section is proof of activity that is considered outside regular activity that is expected in www.asp-waf.com. We define something outside of regular activity if it falls outside the terms of our services.

Some activity recorded here could is considered a cyber-crime, and next to us reporting the abuse to you, we reserve the right to file a formal complaint with relative authorities. We hope that, by you reviewing this document, you will cooperate with authorities if asked to do so and will take action and prevent any further abuse.

DO NOT CLICK ON HTTP EXPLOITS LINKS
YOUR PDF VIEWER MAY GENERATE THESE HEADERS AS LINKS.
CLICKING THESE LINKS WILL TRIGGER THE FIREWALL!

2 HTTP requests to abuse 2 endpoints

During the reporting period, from Fri 25 March 2022 17:06:06 till Sun 27 March 2022 07:23:18 UTC, we detected 5 unique exploits from 1 IP address under your management.

In 14 hours we detected:
- an attempted access protected resources
- continued attempted to probe exploits after being warned
- repetitive visits while attempting to probe for exploits
- repetitive attempts to probe for exploits
- uses URL phishing to probe the system

The below entry documents the activities in greater detail.

Malicious HTTP activity from 216.244.66.197

The user on IP address 216.244.66.197 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploits:

- an attempted access protected resources
- continued attempted to probe exploits after being warned
- repetitive visits while attempting to probe for exploits
- repetitive attempts to probe for exploits
- uses URL phishing to probe the system

During the reported time range user of IP address triggered and attempted to use 5 different exploits 2 times.

25.Mar.22 *2 penetration attempts period 25/03/2022 17:06:06 - 27/03/2022 07:23:18, all dates in UTC*

17:06:06 **https://www.asp-waf.com/NuGet**

The firewall flagged the HttpGet request as 3 actions that are of malicious intent where detected. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 3 exploits and triggered a incident expiring 25/03/2022 17:11:38

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : escalated thread-level after 3 incidents in 150 milliseconds
Action : Block, expires on 25 Mar 22 17:11:38 UTC

activity by 216.244.66.197 continues on the next page...

07:23:18 **https://www.asp-waf.com/abuse**

The firewall flagged the HttpGet request as 3 actions that are of malicious intent where detected. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 3 exploits and triggered a incident expiring 27/03/2022 07:32:14

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : escalated thread-level after 3 incidents in 146 milliseconds
Action : Block, expires on 27 Mar 22 07:32:14 UTC

27.Mar.22 *end or reported activity*

GLOSSARY

The following glossary explains some of the terms & states names used when communicating malicious activity in this abuse report.

MaliciousUser	A user is considered to be malicious having been previously rejected, after having been rejected the user still tries to access sensitive data and is therefore again rejected
PenetrationAttempt	The attacker attempted to gain access to the physical server by using cyber attack against the server to check for exploitable vulnerabilities.
PhishyRequest	The firewall detected access to a resource that was never presented to the user and that doesn't exist, The attacker has been detected to be phishing the system using an URL's in order to use exploitable vulnerabilities that he thinks may be present on the server.