ABUSE REPORT

activity against www.asp-waf.com by

Abuse-C Role

reported from Wed 16 Mar 22 till Wed 30 Mar 22

ABUSE REPORT
ISP Range NTS-1

Incidents recorded between 16/03/2022 20:35:17 and 30/03/2022 06:46:40 UTC

To:
Abuse-C RoleKerchenskaya st.
4
03151
Kiyv
UKRAINE

Email
vb@smartmedianetwork.com.u
a

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

Date : Thu 31 March 2022
Reference : NTS-1-2022.75-2022.89 - 7
Regarding : Malicious activity detected against www.asp-waf.com dating 16/03/2022 20:35:17UTC - 30/03/2022 06:46:40UTC

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 Abuse-C Role

based on data captured from Mon 28 Feb 22 till Thu 31 Mar 22
for IP range 194.38.20.0 - 194.38.20.255 (255 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:

7 attempts to access the system via PHP exploit

Abuse score-card Abuse-C Role

on the 19081 days between Thu 01 Jan 1970 and Wed 30 Mar 2022

IP addresses	:	1	IP addresses with incidents	:	1
HTTP requests served	:	7	HTTP incidents	:	29
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

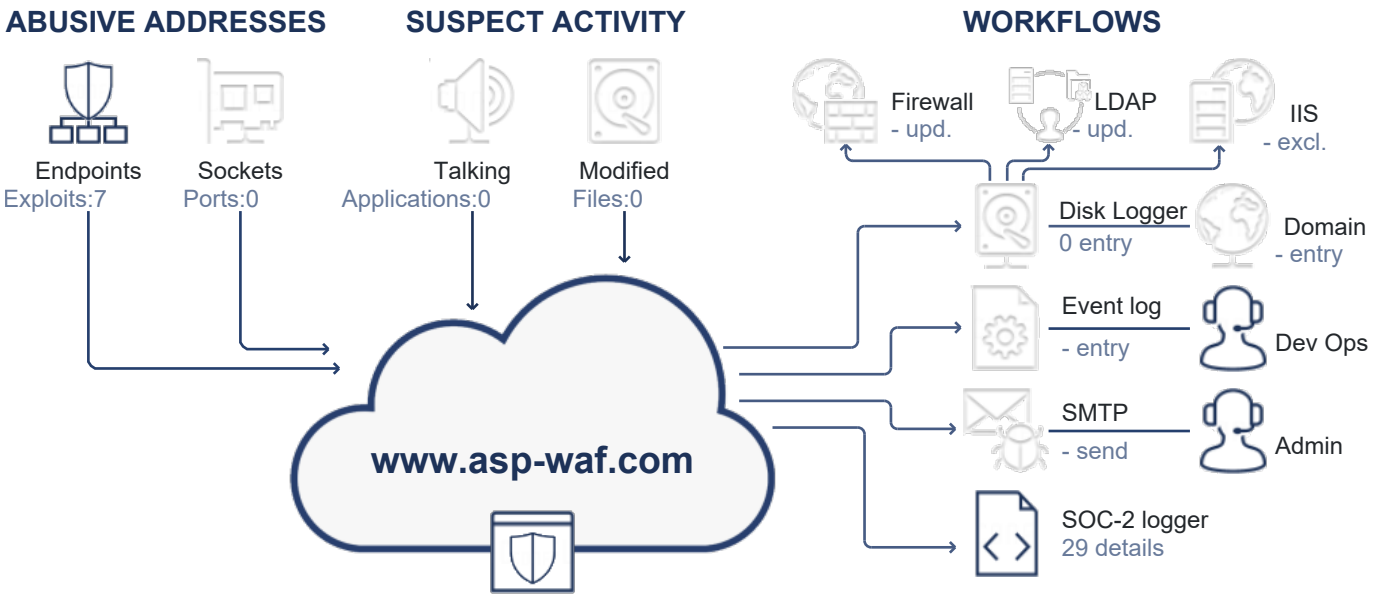
IP Addresses	:	1	IP addresses with incidents	:	-
HTTP requests served	:	7	HTTP incidents	:	-
IP address with port attacks	:	-	Last port attack	:	-
Ports attacked	:	-	Port based incidents	:	-

** 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	7
Human	0
Bot	7
BlackHat	0
Abusive Search Engine	0
Search Engine	0

REQUEST CLASSIFICATION

OK	7
Suspect	0
Redirected	0
Blocked	0

DETECTED ATTACK VECTORS

7 an attempted access protected resources
7 continued attempted to probe exploits after being warned
7 repetitive visits while attempting to probe for exploits
7 repetitive attempts to probe for exploits
7 uses URL phishing to probe the system
7 an attempt to access the site using the wrong technology stac
1 accessing a honey-pot trap

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!

7 HTTP requests to abuse 7 endpoints

During the reporting period, from Wed 16 March 2022 20:35:17 till Wed 30 March 2022 06:46:40 UTC, we detected 7 unique exploits from 1 IP address under your management.

In 13 days we detected:
- an attempted access protected resources
- continued attempted to probe exploits after being warned
- an attempted to access files while not authorized to do so
- repetitive visits while attempting to probe for exploits
- repetitive attempts to probe for exploits
- uses URL phishing to probe the system
- accessing a honey-pot trap

The below entry documents the activities in greater detail.

Malicious HTTP activity from 194.38.20.161

The user on IP address 194.38.20.161 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
- an attempted to access files while not authorized to do so
- repetitive visits while attempting to probe for exploits
- repetitive attempts to probe for exploits
- uses URL phishing to probe the system
- accessing a honey-pot trap

During the reported time range user of IP address triggered and attempted to use 7 different exploits 7 times.

time-line for 194.38.20.161 starts on the next page...

16.Mar.22 *7 penetration attempts period 16/03/2022 20:35:17 - 30/03/2022 06:46:40, all dates in UTC*

20:35:17 **https://www.asp-waf.com/assets/js/jquery-file-upload/server/php/index.php?f**

The firewall flagged the HttpGet request as 4 actions that are of malicious intent where detected.The fact that the user attempted to execute index.php clearly indicates that your user is attempting to guess his way to an exploit as we do not serve PHP requests. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 4 exploits and triggered a incident expiring 16/03/2022 20:41:25

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteUsingTheTechnologyStack
Decision : escalated thread-level after 4 incidents in 258 milliseconds
Action : Block, expires on 16 Mar 22 20:41:25 UTC

18.Mar.22 *13:24:45* **https://www.asp-waf.com/jquery-file-upload/server/php/index.php?file=tf2rgh**

The firewall flagged the HttpGet request as 4 actions that are of malicious intent where detected.The fact that the user attempted to execute index.php clearly indicates that your user is attempting to guess his way to an exploit as we do not serve PHP requests. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 4 exploits and triggered a incident expiring 18/03/2022 13:30:27

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteUsingTheTechnologyStack
Decision : escalated thread-level after 4 incidents in 178 milliseconds
Action : Block, expires on 18 Mar 22 13:30:27 UTC

19.Mar.22 *22:45:07* **https://www.asp-waf.com/assets/fileupload/server/php/index.php?file=tf2rghf**

The firewall flagged the HttpGet request as 4 actions that are of malicious intent where detected.The fact that the user attempted to execute index.php clearly indicates that your user is attempting to guess his way to an exploit as we do not serve PHP requests. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 4 exploits and triggered a incident expiring 19/03/2022 22:50:33

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteUsingTheTechnologyStack
Decision : escalated thread-level after 4 incidents in 448 milliseconds
Action : Block, expires on 19 Mar 22 22:50:33 UTC

21.Mar.22 *10:51:35* **https://www.asp-waf.com/assets/plugins/fileupload/server/php/index.php?file**

The firewall flagged the HttpGet request as 4 actions that are of malicious intent where detected.The fact that the user attempted to execute index.php clearly indicates that your user is attempting to guess his way to an exploit as we do not serve PHP requests. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 4 exploits and triggered a incident expiring 21/03/2022 10:59:09

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteUsingTheTechnologyStack

23:46:09 **https://www.asp-waf.com/admin/fileupload/server/php/index.php?file=tf2rghf**

The firewall flagged the HttpGet request as 5 actions that are of malicious intent where detected.The fact that the user attempted to execute index.php clearly indicates that your user is attempting to guess his way to an exploit as we do not serve PHP requests. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 5 exploits and triggered a incident expiring 23/03/2022 23:56:02

Triggered : HoneyPotTrap PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteUsingTheTechnologyStack
Decision : escalated thread-level after 5 incidents in 170 milliseconds
Action : Block, expires on 23 Mar 22 23:56:02 UTC

28.Mar.22 01:14:31 **https://www.asp-waf.com/assets/plugins/plupload/examples/upload.php**

The firewall flagged the HttpGet request as 4 actions that are of malicious intent where detected.The fact that the user attempted to execute upload.php clearly indicates that your user is attempting to guess his way to an exploit as we do not serve PHP requests. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 4 exploits and triggered a incident expiring 28/03/2022 01:19:57

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteUsingTheTechnologyStack
Decision : escalated thread-level after 4 incidents in 383 milliseconds
Action : Block, expires on 28 Mar 22 01:19:57 UTC

30.Mar.22 06:46:40 **https://www.asp-waf.com/assets/global/plugins/plupload/examples/upload.ph**

The firewall flagged the HttpGet request as 4 actions that are of malicious intent where detected.The fact that the user attempted to execute upload.php clearly indicates that your user is attempting to guess his way to an exploit as we do not serve PHP requests. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 4 exploits and triggered a incident expiring 30/03/2022 06:53:54

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteUsingTheTechnologyStack
Decision : escalated thread-level after 4 incidents in 347 milliseconds
Action : Block, expires on 30 Mar 22 06:53:54 UTC

30.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.

AttemptToAccessSiteUsingTheTechnologyStack	An attempt to obtain access the site using a framework not compatible with that what is used on the web application. This indicates that the BOT or script is guessing known exploits without knowing the software installed.
HoneyPotTrap	The firewall, or the site hosting the firewall, generated a trap for hackers hidden for normal users, the firewall detected that the system tried to access the trap.
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.