ABUSE REPORT

activity against www.asp-waf.com by

Sovintel Abuse Department

reported from Fri 18 Mar 22 till Wed 30 Mar 22

ABUSE REPORT
ISP Range RU-SOVINTEL-MSK-PoLaR-SoLuTioNS-NET

Incidents recorded between 18/03/2022 08:55:22 and 30/03/2022 08:49:50 UTC

To:
Sovintel Abuse
Department111250 Russia
Moscow Krasnokazarmennaya
12

Email abuse-b2b@beeline.ru

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 : RU-SOVINTEL-MSK-PoLaR-SoLuTioNS-NET-2022.77-2022.89 - 14
Regarding : Malicious activity detected against www.asp-waf.com dating 18/03/2022 08:55:22UTC - 30/03/2022 08:49:50UTC

Dear Sir/ Madam

This report is addressed to you based on activity that has been triggered by 2 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 Sovintel Abuse Department

based on data captured from Mon 28 Feb 22 till Thu 31 Mar 22
for IP range 212.44.136.168 - 212.44.136.175 (7 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:

14 attempts to URL exploit

Abuse score-card Sovintel Abuse Department

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

IP addresses	:	2	IP addresses with incidents	:	2
HTTP requests served	:	14	HTTP incidents	:	20
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

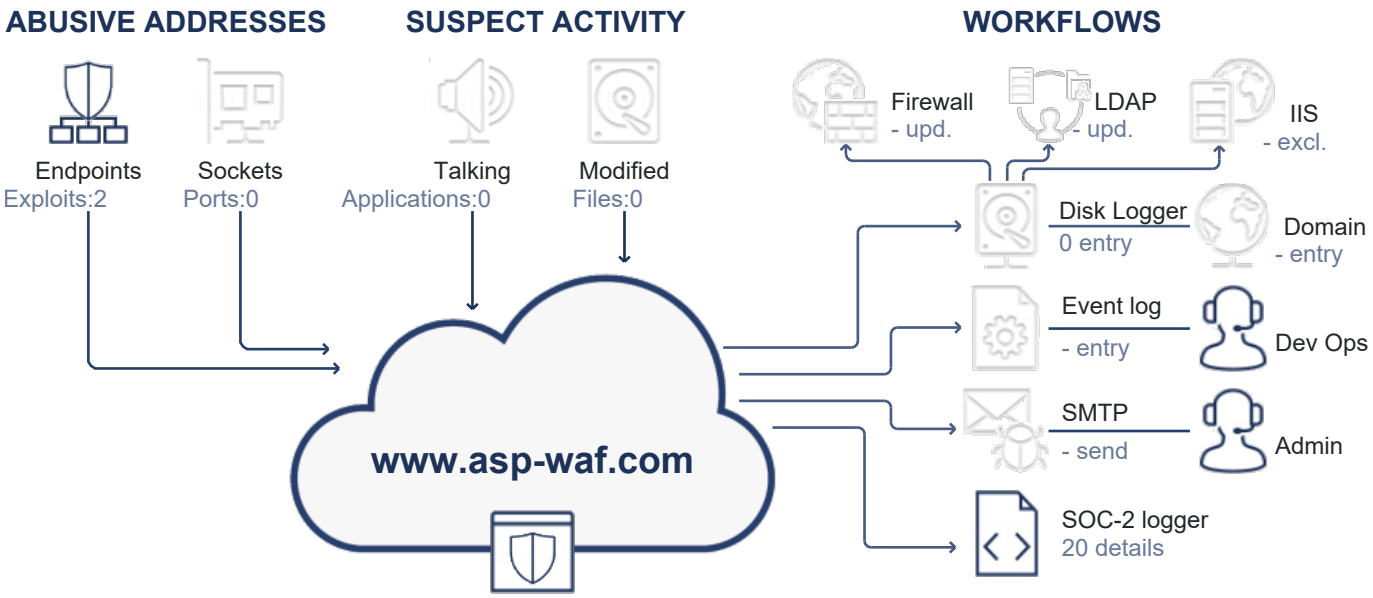
IP Addresses	:	2	IP addresses with incidents	:	-
HTTP requests served	:	14	HTTP incidents	:	-
IP address with port attacks	:	-	Last port attack	:	-
Ports attacked	:	-	Port based incidents	:	-

** 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	3
Human	0
Bot	3
BlackHat	0
Abusive Search Engine	0
Search Engine	0

REQUEST CLASSIFICATION

OK	14
Suspect	0
Redirected	0
Blocked	0

DETECTED ATTACK VECTORS

8 continued attempted to probe exploits after being warned

8 repetitive attempts to probe for exploits

6 an attempted to access the system from an unauthorized loca

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!

14 HTTP requests to abuse 2 endpoints

During the reporting period, from Fri 18 March 2022 08:55:22 till Wed 30 March 2022 08:49:50 UTC, we detected 2 unique exploits from 2 IP addresses under your management.

In 11 days we detected:
- an attempted to access the system from an unauthorized location
- continued attempted to probe exploits after being warned

The next 2 entries document the activities in greater detail.

Malicious HTTP activity from 212.44.136.170

The user on IP address 212.44.136.170 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploits:

- an attempted to access the system from an unauthorized location
- continued attempted to probe exploits after being warned

During the reported time range user of IP address triggered and attempted to use 2 different exploits 4 times.

18.Mar.22 *4 penetration attempts period 18/03/2022 08:55:22 - 18/03/2022 08:59:44, all dates in UTC*

08:55:22 **https://www.asp-waf.com/**

The firewall flagged the HttpGet request as 2 actions that are of malicious intent where detected.

The firewall detected 2 exploits and triggered a incident expiring 18/03/2022 09:05:35

Triggered : GeographyRejected
Decision : return Redirect
Action : GeoRedirect, expires on 18 Mar 22 09:05:35 UTC

activity by 212.44.136.170 continues on the next page...

08:55:28 **https://www.asp-waf.com/EuRegulation**

The firewall flagged the HttpGet request as a malicious intent was 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 exploit and triggered a incident expiring 18/03/2022 09:05:35

Triggered :
Decision : escalated thread-level
Action : Block, expires on 18 Mar 22 09:05:35 UTC

08:59:44 **https://www.asp-waf.com/**

The firewall flagged the HttpGet request as 2 actions that are of malicious intent where detected.

The firewall detected 2 exploits and triggered a incident expiring 18/03/2022 09:05:35

Triggered : GeographyRejected
Decision : return Redirect
Action : GeoRedirect, expires on 18 Mar 22 09:05:35 UTC

08:59:44 **https://www.asp-waf.com/EuRegulation**

The firewall flagged the HttpGet request as a malicious intent was 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 exploit and triggered a incident expiring 18/03/2022 09:05:35

Triggered :
Decision : escalated thread-level
Action : Block, expires on 18 Mar 22 09:05:35 UTC

18.Mar.22 *end or reported activity*

Malicious HTTP activity from 212.44.136.171

The user on IP address 212.44.136.171 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploits:

- an attempted to access the system from an unauthorized location
- continued attempted to probe exploits after being warned

During the reported time range user of IP address triggered and attempted to use 2 different exploits 10 times.

18.Mar.22 *10 penetration attempts period 18/03/2022 08:58:40 - 30/03/2022 08:49:50, all dates in UTC*

08:58:40 **https://www.asp-waf.com/**

The firewall flagged the HttpGet request as 2 actions that are of malicious intent where detected.

The firewall detected 2 exploits and triggered a incident expiring 18/03/2022 09:03:45

Triggered : GeographyRejected
Decision : return Redirect
Action : GeoRedirect, expires on 18 Mar 22 09:03:45 UTC

activity by 212.44.136.171 continues on the next page...

08:58:45 **https://www.asp-waf.com/EuRegulation**

The firewall flagged the HttpGet request as a malicious intent was 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 exploit and triggered a incident expiring 18/03/2022 09:05:35

Triggered :
Decision : escalated thread-level
Action : Block, expires on 18 Mar 22 09:05:35 UTC

22.Mar.22 08:07:46 **https://www.asp-waf.com/EuRegulation**

The firewall flagged the HttpGet request as 2 actions that are of malicious intent where detected.

The firewall detected 2 exploits and triggered a incident expiring 22/03/2022 08:12:49

Triggered : GeographyRejected
Decision : return Redirect
Action : GeoRedirect, expires on 22 Mar 22 08:12:49 UTC

08:07:47 **https://www.asp-waf.com/**

The firewall flagged the HttpGet request as 2 actions that are of malicious intent where detected.

The firewall detected 2 exploits and triggered a incident expiring 22/03/2022 08:12:49

Triggered : GeographyRejected
Decision : return Redirect
Action : GeoRedirect, expires on 22 Mar 22 08:12:49 UTC

08:07:50 **https://www.asp-waf.com/EuRegulation**

The firewall flagged the HttpGet request as a malicious intent was 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 exploit and triggered a incident expiring 22/03/2022 08:13:11

Triggered :
Decision : escalated thread-level
Action : Block, expires on 22 Mar 22 08:13:11 UTC

08:07:55 **https://www.asp-waf.com/**

The firewall flagged the HttpGet request as a malicious intent was 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 exploit and triggered a incident expiring 22/03/2022 08:13:11

Triggered :
Decision : escalated thread-level
Action : Block, expires on 22 Mar 22 08:13:11 UTC

activity by 212.44.136.171 continues on the next page...

08:49:39 **https://www.asp-waf.com/**

The firewall flagged the HttpGet request as 2 actions that are of malicious intent where detected.

The firewall detected 2 exploits and triggered a incident expiring 30/03/2022 08:54:39

Triggered : GeographyRejected
Decision : return Redirect
Action : GeoRedirect, expires on 30 Mar 22 08:54:39 UTC

08:49:39 **https://www.asp-waf.com/EuRegulation**

The firewall flagged the HttpGet request as a malicious intent was 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 exploit and triggered a incident expiring 30/03/2022 08:58:30

Triggered :
Decision : escalated thread-level
Action : Block, expires on 30 Mar 22 08:58:30 UTC

08:49:39 **https://www.asp-waf.com/**

The firewall flagged the HttpGet request as a malicious intent was 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 exploit and triggered a incident expiring 30/03/2022 08:58:30

Triggered :
Decision : escalated thread-level
Action : Block, expires on 30 Mar 22 08:58:30 UTC

08:49:50 **https://www.asp-waf.com/**

The firewall flagged the HttpGet request as a malicious intent was 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 exploit and triggered a incident expiring 30/03/2022 08:58:30

Triggered :
Decision : escalated thread-level
Action : Block, expires on 30 Mar 22 08:58:30 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.

GeographyRejected	Access to the resource has been blocked from a given country, normal access to the resource is not provided and the attacher was not presented with a link or documentation to access the resource