ABUSE REPORT

activity against www.asp-waf.com by

ALMOUROLTEC PTISP

reported from Fri 08 Oct 21 till Fri 08 Oct 21

ABUSE REPORT
ISP Range PT-ALMOUROLTEC

Incidents recorded between 08/10/2021 14:15:49 and 08/10/2021 14:23:25 UTC

To:
ALMOUROLTEC PTISPEstrada
Nacional 3
2250-028 Constancia

Email abuse@ptisp.pt

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

Date : Tue 26 October 2021
Reference : PT-ALMOUROLTEC-2021.281-2021.281 - 2
Regarding : Malicious activity detected against www.asp-waf.com dating 08/10/2021 14:15:49UTC - 08/10/2021 14:23:25UTC

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.

During 7 minutes we detected that 2 http requests to abuse 2 endpoints, we consider this activity to be malicious activity, we recorded the activity and present it to you in this PDF.

In order to avoid further abuse through your hosted IP addresses, please address the issue internally within 5 working days after which we will consider continued malicious activity to be condoned by you.

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 cyber-crime related law enforcement.

Feel free to contact me any time at support@asp-waf.com if you need more or other information.

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

Thank you for your cooperation in this matter

Yours sincerely

TABLE OF CONTENTS

MANAGEMENT OVERVIEW

Activity against www.asp-waf.com by ALMOUROLTEC PTISP

based on data captured from Thu 30 Sep 21 till Tue 26 Oct 21
for IP range 109.71.41.0 - 109.71.41.255 (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:

2 attempts to steal data by attempting to download confidential data

Abuse score-card ALMOUROLTEC PTISP

on the 18908 days between Thu 01 Jan 1970 and Fri 08 Oct 2021

IP addresses	:	2	IP addresses with incidents	:	2
HTTP requests served	:	11	HTTP incidents	:	30
IP address with port attacks	:	-	Last port attack	:	-
Ports attacked	:	-	Port based Incidents	:	-
Talking IP addresses	:	-	Last Talk	:	-
Talking Applications	:	-	Talks Detected	:	-

on the 25 days between Thu 30 Sep 2021 and Tue 26 Oct 2021

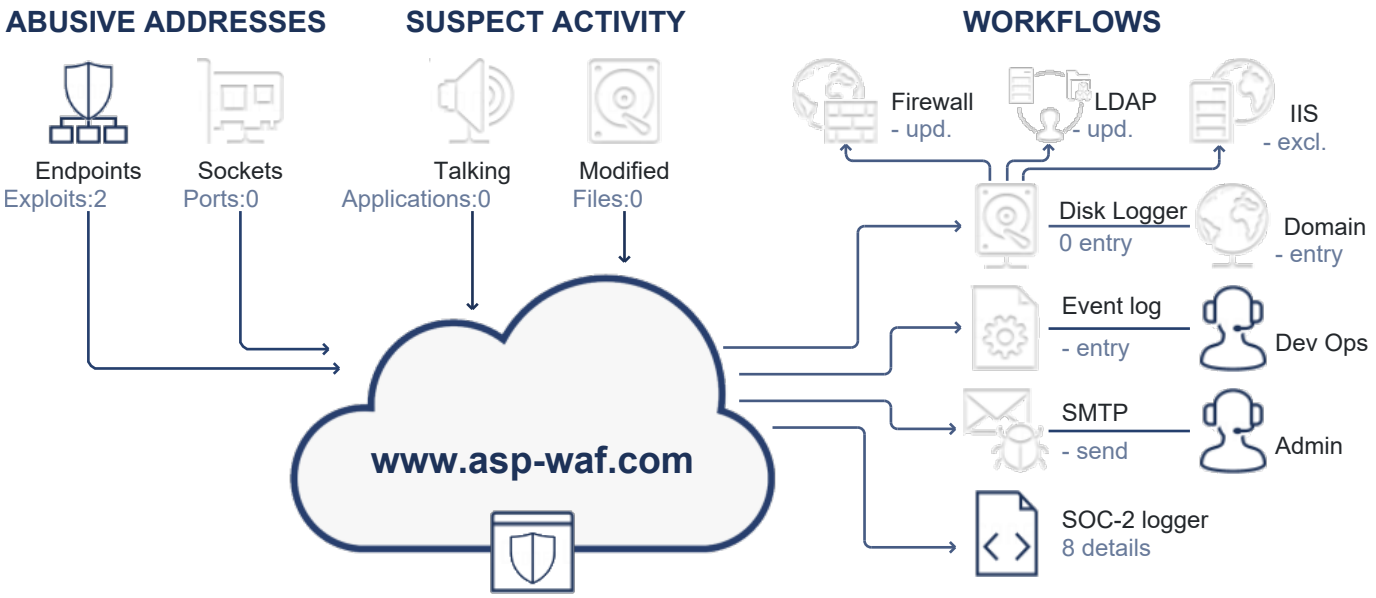
IP Addresses	:	1	IP addresses with incidents	:	-
HTTP requests served	:	2	HTTP incidents	:	-
IP address with port attacks	:	-	Last port attack	:	-
Ports attacked	:	-	Port based incidents	:	-

** 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	2
Human	0
Bot	2
BlackHat	0
Abusive Search Engine	0
Search Engine	0

REQUEST CLASSIFICATION

OK	2
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
2 an attempt to gain access to backups
2 a Common Vulnerabilities and Exposures (CVE) exploit detec

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 08 October 2021 14:15:49 till Fri 08 October 2021 14:23:25 UTC, we detected 7 unique exploits from 1 IP address under your management.

In 7 minutes 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
- an attempt to gain access to backups
- a Common Vulnerabilities and Exposures (CVE) exploit detected

The below entry documents the activities in greater detail.

Malicious HTTP activity from 109.71.41.219

The user on IP address 109.71.41.219 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
- an attempt to gain access to backups
- a Common Vulnerabilities and Exposures (CVE) exploit detected

During the reported time range user of IP address triggered and attempted to use 7 different exploits 2 times.

time-line for 109.71.41.219 starts on the next page...

08.Oct.21 *2 penetration attempts period 08/10/2021 14:15:49 - 08/10/2021 14:23:25, all dates in UTC*

14:15:49 **https://support.asp-waf.com/backups/backup.gz**

The firewall flagged the HttpHead request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download backup.gz as this clearly was an attempt to gain access to confidential data like possible stored credentials or proprietary data including that of our clients. 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 08/10/2021 14:25:32

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 134 milliseconds
Action : Block, expires on 08 Oct 21 14:25:32 UTC
Notes : Known abuser as a previous exploit was triggered

14:23:25 **https://support.asp-waf.com/old/website.gz**

The firewall flagged the HttpHead request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download website.gz as this clearly was an attempt to gain access to confidential data like possible stored credentials or proprietary data including that of our clients. 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 08/10/2021 14:25:32

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 107 milliseconds
Action : Block, expires on 08 Oct 21 14:25:32 UTC

08.Oct.21 *end or reported activity*

GLOSSARY

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

AttemptToAccessSiteBackup	An attempt to access backups or other confidential data was detected. Such request always indicate that data theft is being attempted
CommonVulnerabilitiesExposuresExploitDetected	An attempt to use a CVE registered exploit was detected. The user is trying to use what is likely dark-web malware to gain access using an attack vector that is a publicly disclosed vulnerability.
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.