

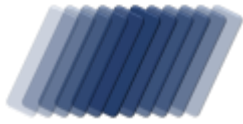
ABUSE REPORT

activity against www.asp-waf.com by

ALMOUROLTEC PTISP

reported from Mon 27 Sep 21 till Mon 27 Sep 21





ABUSE REPORT

ISP Range PT-ALMOUROLTEC

Incidents recorded between 27/09/2021 10:48:27 and 27/09/2021 10:48:27 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-2021.270-2021.270 - 1
Regarding : Malicious activity detected against www.asp-waf.com dating 27/09/2021 10:48:27UTC - 27/09/2021 10:48:27UTC

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 a single second we detected that 1 http requests to abuse 1 endpoint, 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

<i>topic</i>	<i>page</i>
Management Overview	4
Malicious HTTP activity from 109.71.41.220	6
Glossary	8

MANAGEMENT OVERVIEW

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

based on data captured from Tue 31 Aug 21 till Wed 29 Sep 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:

- 1 attempt 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 29 days between Tue 31 Aug 2021 and Wed 29 Sep 2021

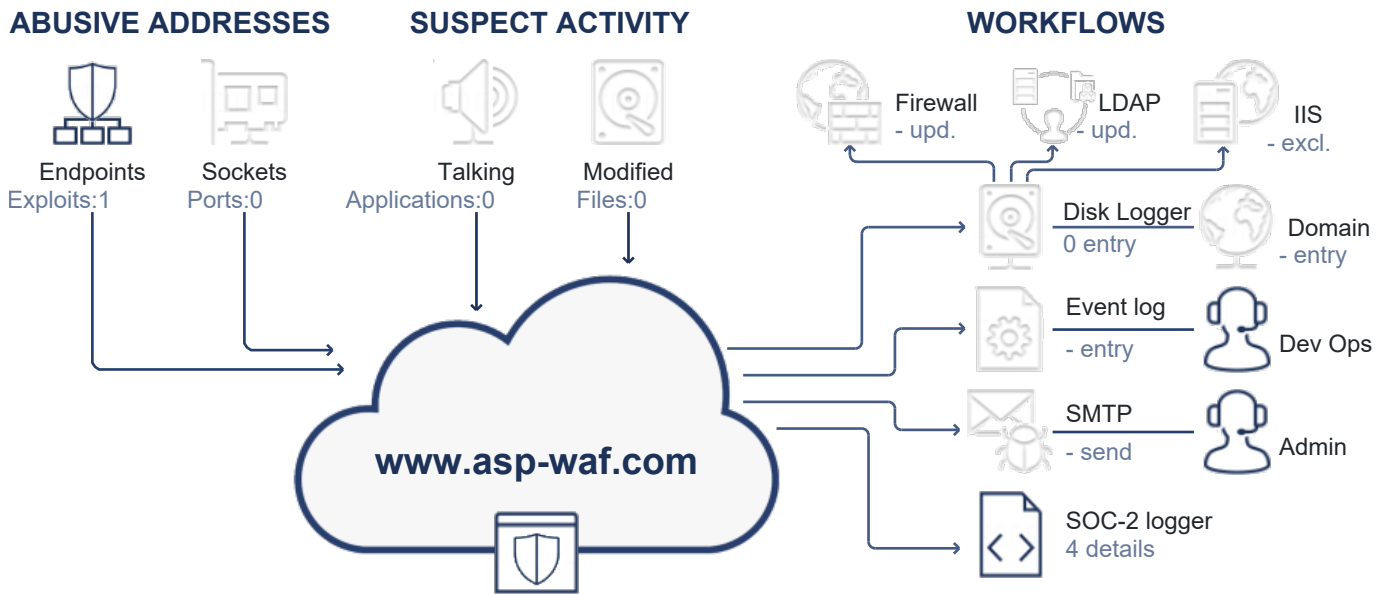
IP Addresses	: 1	IP addresses with incidents	: -
HTTP requests served	: 1	HTTP incidents	: -
IP address with port attacks	: -	Last port attack	: -
Ports attacked	: -	Port based incidents	: -

* 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		DETECTED ATTACK VECTORS	
Requests	1	1	an attempted access protected resources
Human	0	1	continued attempted to probe exploits after being warned
Bot	1	1	repetitive visits while attempting to probe for exploits
BlackHat	0	1	repetitive attempts to probe for exploits
Abusive Search Engine	0	1	uses URL phishing to probe the system
Search Engine	0	1	an attempt to gain access to backups
	0	1	a Common Vulnerabilities and Exposures (CVE) exploit detected
REQUEST CLASSIFICATION			
OK	1		
Suspect	0		
Redirected	0		
Blocked	0		

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 be 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!**

1 HTTP requests to abuse 1 endpoint

During the reporting period, from Mon 27 September 2021 10:48:27 till Mon 27 September 2021 10:48:27 UTC, we detected 7 unique exploits from 1 IP address under your management.

In a single second 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 109.71.41.220

The user on IP address 109.71.41.220 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 once.

time-line for 109.71.41.220 starts on the next page...

27.Sep.21 ○ 1 penetration attempt on 27/09/2021 10:48:27, all dates in UTC

● 10:48:27 **https://support.asp-waf.com/backups/directory.rar**

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 directory.rar 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 26/06/2022 14:27:48

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
AttemptToAccessSiteBackup
CommonVulnerabilitiesExposuresExploitDetected

Decision : return Forbidden after 4 incidents in 55 milliseconds

Action : Block, expires on 26 Jun 22 14:27:48 UTC

Notes : Known abuser as 18 exploits where triggered

27.Sep.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.