ABUSE REPORT

activity against www.asp-waf.com by

ALMOUROLTEC PTISP

reported from Sun 08 Aug 21 till Wed 25 Aug 21

ABUSE REPORT
ISP Range PT-ALMOUROLTEC

Incidents recorded between 08/08/2021 01:39:58 and 25/08/2021 13:44:16 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-2021.220-2021.237 - 8
Regarding : Malicious activity detected against www.asp-waf.com dating 08/08/2021 01:39:58UTC - 25/08/2021 13:44:16UTC

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 17 days we detected that 8 http requests to abuse 8 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

topic	*page*
Management Overview	4
Malicious HTTP activity from 109.71.41.220	6
Glossary	10

MANAGEMENT OVERVIEW

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

based on data captured from Sat 31 Jul 21 till Mon 30 Aug 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:

6 attempts to steal data by attempting to download confidential data
1 attempt to steal archived crypto currency wallets
1 attempt to URL exploit

Abuse score-card ALMOUROLTEC PTISP

on the 18875 days between Thu 01 Jan 1970 and Sun 05 Sep 2021

IP addresses	:	1	IP addresses with incidents	:	1
HTTP requests served	:	8	HTTP incidents	:	18
IP address with port attacks	:	-	Last port attack	:	-
Ports attacked	:	-	Port based Incidents	:	-
Talking IP addresses	:	-	Last Talk	:	-
Talking Applications	:	-	Talks Detected	:	-

on the 30 days between Sat 31 Jul 2021 and Mon 30 Aug 2021

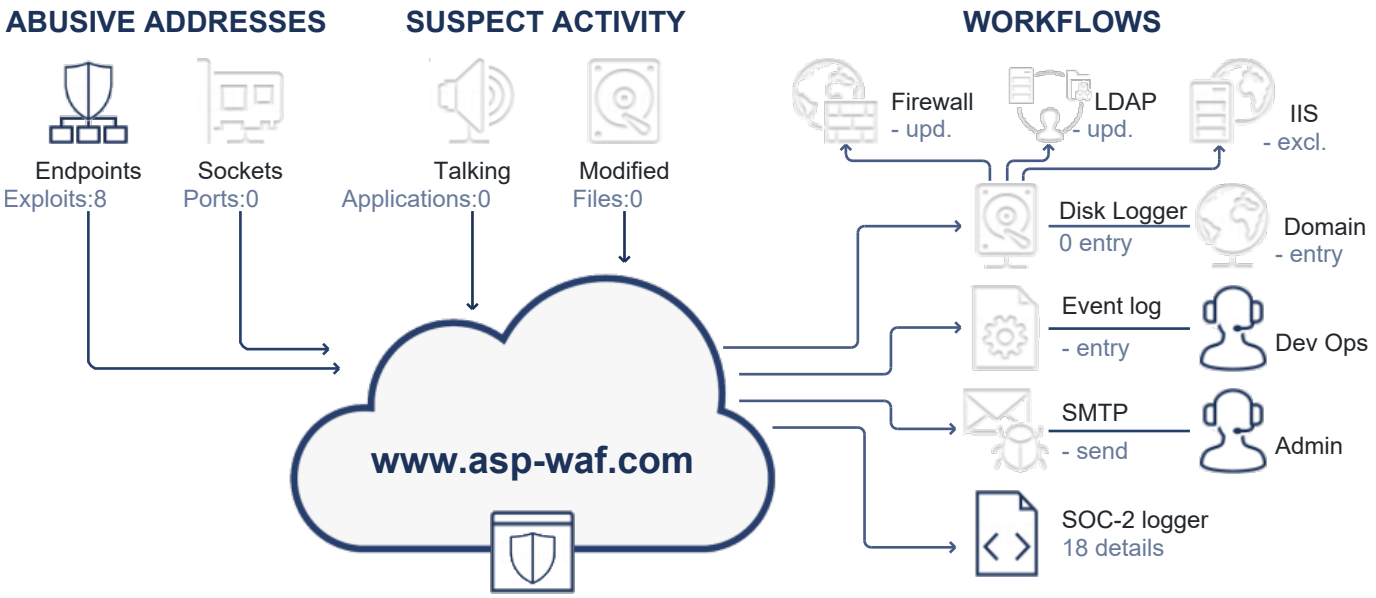
IP Addresses	:	1	IP addresses with incidents	:	1
HTTP requests served	:	4	HTTP incidents	:	4
IP address with port attacks	:	-	Last port attack	:	-
Ports attacked	:	-	Port based incidents	:	-

** 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	8
Human	0
Bot	8
BlackHat	0
Abusive Search Engine	0
Search Engine	0

REQUEST CLASSIFICATION

OK	4
Suspect	0
Redirected	0
Blocked	4

DETECTED ATTACK VECTORS

8 uses URL phishing to probe the system
4 continued attempted to probe exploits after being warned
4 repetitive attempts to probe for exploits
3 an attempted access protected resources
3 repetitive visits while attempting to probe for exploits
2 an attempt to gain access to backups
2 a Common Vulnerabilities and Exposures (CVE) exploit detec
1 repeat requests 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!

8 HTTP requests to abuse 8 endpoints

During the reporting period, from Sun 08 August 2021 01:39:58 till Wed 25 August 2021 13:44:16 UTC, we detected 7 unique exploits from 1 IP address under your management.

In 17 days we detected:
- uses URL phishing to probe the system
- an attempted access protected resources
- continued attempted to probe exploits after being warned
- repetitive attempts to probe for exploits
- repetitive visits while attempting to probe for exploits
- 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:

- uses URL phishing to probe the system
- an attempted access protected resources
- continued attempted to probe exploits after being warned
- repetitive attempts to probe for exploits
- repetitive visits while attempting to probe for exploits
- 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 8 times.In total we detected 4 exploits with 36 attempts from 08 Aug 21 and 25 Aug 21. We recorded:

- 18 attempts to access resources using malformed URL phishing technique
- 9 attempts to access confidential data
- 7 repeated engagements with the site while being blocked
- 2 TCP Reset-Attacks detected

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

08.Aug.21 *8 penetration attempts period 08/08/2021 01:39:58 - 25/08/2021 13:44:16, all dates in UTC*

01:39:58 **https://asp-waf.com/index.zip**

The firewall flagged the HttpHead request as a malicious intent was detected.We did not appreciate the attempt by your user to download index.zip 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 most significant reason to reject the request was "A non supported URL was called"

Triggered : PhishyRequest
Decision : return NotFound
Action : NoAction, expires on 08 Aug 21 01:46:06 UTC

01:40:37 **https://asp-waf.com/old/latest.zip**

The firewall flagged the HttpHead request as 3 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download latest.zip 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 most significant reasons to reject the request where "A non supported URL was called", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a UrlFishingSuspected pattern"

Triggered : PageRereshFishing PhishyRequest
Decision : return Forbidden after 3 incidents in 138 milliseconds
Action : Block, expires on 08 Aug 21 01:45:37 UTC

01:54:24 **https://asp-waf.com/restore/wallet.zip**

The firewall flagged the HttpHead request as a malicious intent was detected.We did not appreciate the attempt by your user to download crypto-currency walletwallet.zip this clearly was an attempt of theft.

The most significant reason to reject the request was "A non supported URL was called"

Triggered : PhishyRequest
Decision : return NotFound
Action : NoAction, expires on 08 Aug 21 03:54:43 UTC

01:58:05 **https://asp-waf.com/bak/.bash_history**

The firewall flagged the HttpHead request as a malicious intent was detected.

The most significant reason to reject the request was "A non supported URL was called"

Triggered : PhishyRequest
Decision : return NotFound
Action : NoAction, expires on 08 Aug 21 03:54:43 UTC

activity by 109.71.41.220 continues on the next page...

02:07:25 **https://asp-waf.com/back/.well-known.zip**

The firewall flagged the HttpHead request as a malicious intent was detected.We did not appreciate the attempt by your user to download .well-known.zip 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 most significant reason to reject the request was "A non supported URL was called"

Triggered : PhishyRequest
Decision : return NotFound
Action : NoAction, expires on 08 Aug 21 03:54:43 UTC

20.Aug.21 09:40:42 **https://asp-waf.com/restore/full_backup.zip**

The firewall flagged the HttpHead request as 3 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download full_backup.zip 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 most significant reasons to reject the request where "A non supported URL was called", "A non supported URL was called as the user has no access to https://asp-waf.com/restore/full_backup.zip", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application"

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 77 milliseconds
Action : Block, expires on 20 Aug 21 09:45:42 UTC

10:16:45 **https://asp-waf.com/backup/website.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 website.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 most significant reasons to reject the request where "A non supported URL was called", "A non supported URL was called as the user has no access to https://asp-waf.com/backup/website.rar", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToBackupsAllowed pattern"

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
AttemptToAccessSiteBackup
CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 240 milliseconds
Action : Block, expires on 20 Aug 21 10:21:45 UTC

25.Aug.21 13:44:16 **https://support.asp-waf.com/backup/public_html.tar.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 public_html.tar.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 most significant reasons to reject the request where "A non supported URL was called", "A non supported URL was called as the user has no access to

https://support.asp-waf.com/backup/public_html.tar.gz", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToBackupsAllowed pattern"

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 211 milliseconds
Action : Block, expires on 26 Jun 22 14:24:17 UTC

25.Aug.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
PageRereshFishing	Cyber-criminals use phishing URLs to try to obtain sensitive information for malicious use, this could be system files, configuration settings etc. They firewall detects such requests against the website.
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.