ABUSE REPORT

activity against www.asp-waf.com by

tnr technologies

reported from Mon 27 Sep 21 till Fri 08 Oct 21

VESNX AG | www.asp-waf.com | firewall release 2021.9.4.1124
application firewall for .Net

ABUSE REPORT

ISP Range VPN-Consumer-Network

Incidents recorded between 27/09/2021 07:42:20 and 08/10/2021 22:22:28 UTC

To:
tnr technologiesZweedsestraat
8a28
7418 BG
Deventer
NETHERLANDS

Email info@tnrtechnologies.nl

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 : VPN-Consumer-Network-2021.270-2021.281 - 22
Regarding : Malicious activity detected against www.asp-waf.com dating 27/09/2021 07:42:20UTC - 08/10/2021 22:22:28UTC

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.

During 11 days we detected that 22 http requests to abuse 21 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 tnr technologies

based on data captured from Sun 26 Sep 21 till Thu 30 Sep 21
for IP range 45.8.17.0 - 45.8.17.255 (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:

15 attempts to steal data by attempting to download confidential data
4 attempts to access archived SQL script
2 attempts to URL exploit
1 attempt to access SQL script

Abuse score-card tnr technologies

on the 18919 days between Thu 01 Jan 1970 and Tue 19 Oct 2021

IP addresses	:	10	IP addresses with incidents	:	10
HTTP requests served	:	63	HTTP incidents	:	211
IP address with port attacks	:	-	Last port attack	:	-
Ports attacked	:	-	Port based Incidents	:	-
Talking IP addresses	:	-	Last Talk	:	-
Talking Applications	:	-	Talks Detected	:	-

on the 4 days between Sun 26 Sep 2021 and Thu 30 Sep 2021

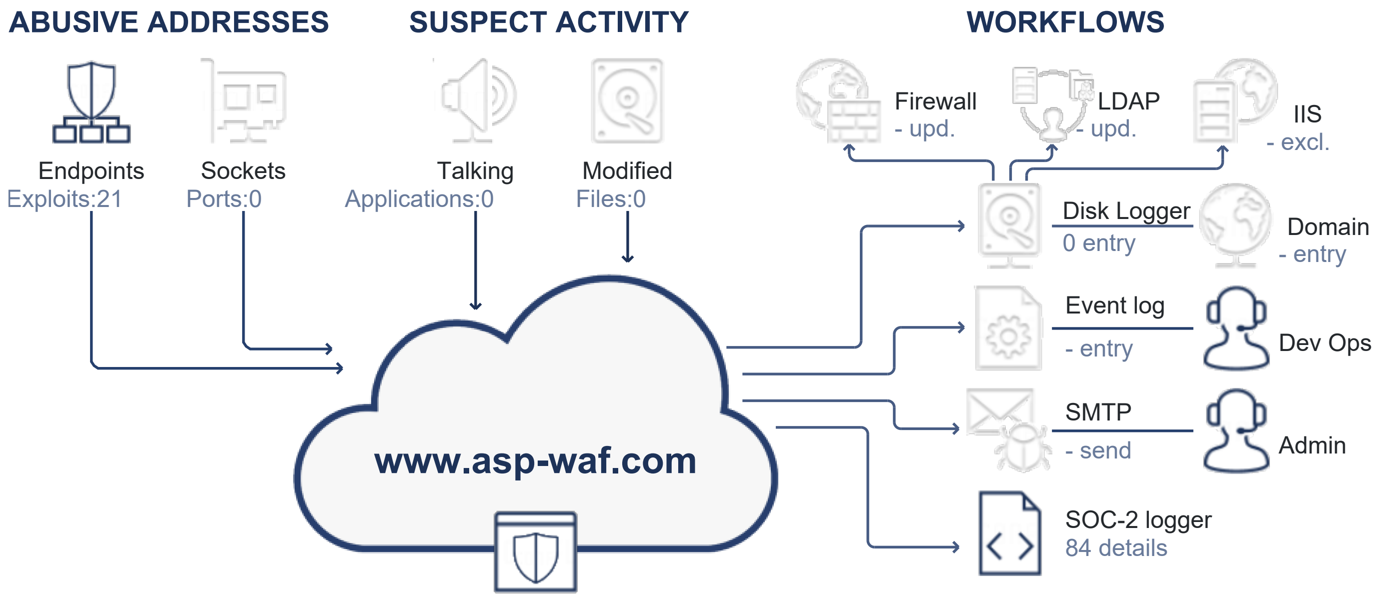
IP Addresses	:	2	IP addresses with incidents	:	-
HTTP requests served	:	22	HTTP incidents	:	-
IP address with port attacks	:	-	Last port attack	:	-
Ports attacked	:	-	Port based incidents	:	-

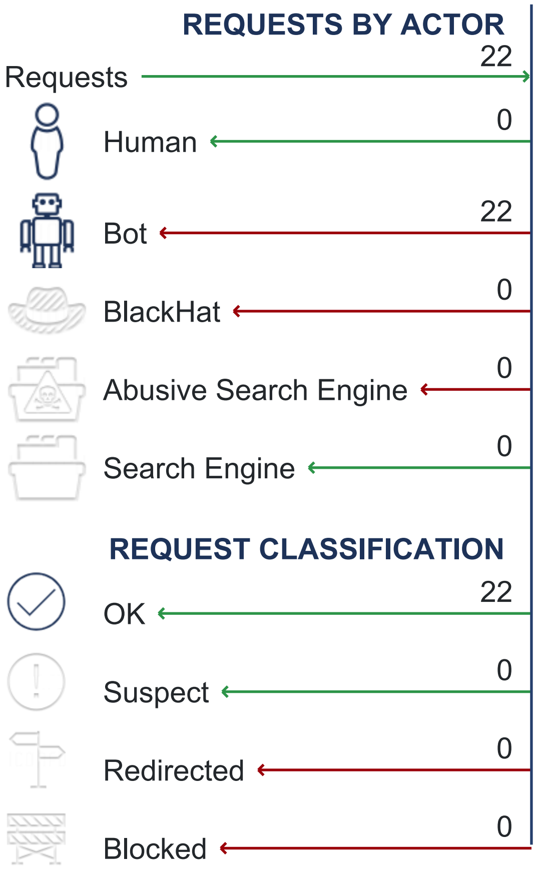
** The first priority of the ASP-WAF firewall is to protect the application, reporting, even though important comes second. Please consult the glossary for a detailed explanation of each metric.*

view activity diagram on the next page

ACTIVITY

Activity, response and impact visualization





DETECTED ATTACK VECTORS

22 uses URL phishing to probe the system

21 an attempted access protected resources

21 continued attempted to probe exploits after being warned

21 repetitive visits while attempting to probe for exploits

21 repetitive attempts to probe for exploits

20 a Common Vulnerabilities and Exposures (CVE) exploit dete

19 an attempt to gain access to backups

1 accessing a honey-pot trap

1 an attempts to gain access via a manipulated credential

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!

22 HTTP requests to abuse 21 endpoints

During the reporting period, from Mon 27 September 2021 07:42:20 till Fri 08 October 2021 22:22:28 UTC, we detected 9 unique exploits from 2 IP addresses under your management.

In 11 days 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
- accessing a honey-pot trap
- an attempts to gain access via a manipulated credential

The next 2 entries document the activities in greater detail.

Malicious HTTP activity from 45.8.17.100

The user on IP address 45.8.17.100 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 6 times.

time-line for 45.8.17.100 starts on the next page...

27.Sep.21 *6 penetration attempts period 27/09/2021 07:42:20 - 27/09/2021 08:31:29, all dates in UTC*

07:42:20 **https://support.asp-waf.com/back/backup.sql.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.sql.gz as this clearly was an attempt to gain access to archived SQL statements that we might have use to execute batch statements on our server. 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 27/09/2021 07:53:09

Triggered	:	PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision	:	return Forbidden after 4 incidents in 62 milliseconds
Action	:	Block, expires on 27 Sep 21 07:53:09 UTC
Notes	:	Known abuser as a previous exploit was triggered

07:42:56 **https://support.asp-waf.com/bak/backup.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 backup.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 firewall detected 4 exploits and triggered a incident expiring 27/09/2021 07:53:09

Triggered	:	PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision	:	return Forbidden after 4 incidents in 29 milliseconds
Action	:	Block, expires on 27 Sep 21 07:53:09 UTC

08:09:26 **https://support.asp-waf.com/old/backup.sql.tar**

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.sql.tar as this clearly was an attempt to gain access to archived SQL statements that we might have use to execute batch statements on our server. 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 27/09/2021 08:27:40

Triggered	:	PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision	:	return Forbidden after 4 incidents in 63 milliseconds
Action	:	Block, expires on 27 Sep 21 08:27:40 UTC

activity by 45.8.17.100 continues on the next page...

08:24:11 **https://support.asp-waf.com/backups/backup.sql.tar**

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.sql.tar as this clearly was an attempt to gain access to archived SQL statements that we might have use to execute batch statements on our server. 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 27/09/2021 08:27:40

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
AttemptToAccessSiteBackup
CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 64 milliseconds
Action : Block, expires on 27 Sep 21 08:27:40 UTC

08:25:35 **https://support.asp-waf.com/www.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 www.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 27/09/2021 08:27:40

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
AttemptToAccessSiteBackup
CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 137 milliseconds
Action : Block, expires on 27 Sep 21 08:27:40 UTC

08:31:29 **https://support.asp-waf.com/backups/www.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 www.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 27/09/2021 08:37:17

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
AttemptToAccessSiteBackup
CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 65 milliseconds
Action : Block, expires on 27 Sep 21 08:37:17 UTC

27.Sep.21 *end or reported activity*

Malicious HTTP activity from 45.8.17.172

The user on IP address 45.8.17.172 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
- accessing a honey-pot trap
- an attempts to gain access via a manipulated credential

During the reported time range user of IP address triggered and attempted to use 9 different exploits 16 times.

08.Oct.21 *16 penetration attempts period 08/10/2021 21:40:17 - 08/10/2021 22:22:28, all dates in UTC*

21:40:17 **https://support.asp-waf.com/old/bak.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 bak.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 firewall detected 4 exploits and triggered a incident expiring 09/10/2021 00:30:38

Triggered	:	PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision	:	return Forbidden after 4 incidents in 149 milliseconds
Action	:	Block, expires on 09 Oct 21 00:30:38 UTC
Notes	:	Known abuser as a previous exploit was triggered

21:41:11 **https://support.asp-waf.com/restore/backup.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 backup.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 09/10/2021 00:30:38

Triggered	:	PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision	:	return Forbidden after 4 incidents in 114 milliseconds
Action	:	Block, expires on 09 Oct 21 00:30:38 UTC

activity by 45.8.17.172 continues on the next page...

21:43:50 **https://support.asp-waf.com/back/backup.sql.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.sql.gz as this clearly was an attempt to gain access to archived SQL statements that we might have use to execute batch statements on our server. 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 09/10/2021 00:30:38

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 122 milliseconds
Action : Block, expires on 09 Oct 21 00:30:38 UTC

21:48:33 **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 09/10/2021 00:30:38

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 134 milliseconds
Action : Block, expires on 09 Oct 21 00:30:38 UTC

21:48:34 **https://support.asp-waf.com/old/asp-waf.com.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 asp-waf.com.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 09/10/2021 00:30:38

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 147 milliseconds
Action : Block, expires on 09 Oct 21 00:30:38 UTC

21:49:40 **https://support.asp-waf.com/backups/application.zip**

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 application.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 firewall detected 4 exploits and triggered a incident expiring 09/10/2021 00:30:38

Triggered : PenetrationAttempt MaliciousUser PhishyRequest

21:50:55 **https://support.asp-waf.com/restore/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 firewall detected 4 exploits and triggered a incident expiring 09/10/2021 00:30:38

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
AttemptToAccessSiteBackup
CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 412 milliseconds
Action : Block, expires on 09 Oct 21 00:30:38 UTC

21:50:57 **https://support.asp-waf.com/back/www.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 www.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 09/10/2021 00:30:38

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
AttemptToAccessSiteBackup
CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 251 milliseconds
Action : Block, expires on 09 Oct 21 00:30:38 UTC

22:01:01 **https://support.asp-waf.com/restore/.bash_history**

The firewall flagged the HttpHead request as 3 actions that are of malicious intent where 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 3 exploits and triggered a incident expiring 09/10/2021 00:30:38

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 141 milliseconds
Action : Block, expires on 09 Oct 21 00:30:38 UTC

22:01:10 **https://support.asp-waf.com/backups/public_html.zip**

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.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 firewall detected 4 exploits and triggered a incident expiring 09/10/2021 00:30:38

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
AttemptToAccessSiteBackup
CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 208 milliseconds

22:07:47 **https://support.asp-waf.com/backup/asp-waf.com.zip**

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 asp-waf.com.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 firewall detected 4 exploits and triggered a incident expiring 09/10/2021 00:30:38

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
AttemptToAccessSiteBackup
CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 207 milliseconds
Action : Block, expires on 09 Oct 21 00:30:38 UTC

22:08:27 **https://support.asp-waf.com/backup/sql.sql**

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 sql.sql as this clearly was an attempt to gain access to the SQL statements that we are used to execute batch statements on our server. 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 09/10/2021 00:30:38

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
AttemptToAccessSiteBackup
CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 252 milliseconds
Action : Block, expires on 09 Oct 21 00:30:38 UTC

22:12:06 **https://support.asp-waf.com/backup/index.zip**

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 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 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 09/10/2021 00:30:38

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
AttemptToAccessSiteBackup
CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 249 milliseconds
Action : Block, expires on 09 Oct 21 00:30:38 UTC

22:12:37 **https://support.asp-waf.com/back/backup.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 backup.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 firewall detected 4 exploits and triggered a incident expiring 09/10/2021 00:30:38

22:19:01 **https://support.asp-waf.com/bak/credentials.txt**

The firewall flagged the HttpHead request as 4 actions that are of malicious intent where 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 4 exploits and triggered a incident expiring 09/10/2021 00:30:38

Triggered	:	HoneyPotTrap ProxyUser PenetrationAttempt MaliciousUser PhishyRequest CommonVulnerabilitiesExposuresExploitDetected
Decision	:	return Forbidden after 4 incidents in 206 milliseconds
Action	:	Block, expires on 09 Oct 21 00:30:38 UTC

22:22:28 **https://support.asp-waf.com/backups/asp-waf.com.rar**

The firewall flagged the HttpHead request as a malicious intent was detected.We did not appreciate the attempt by your user to download asp-waf.com.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 detected exploit and triggered a incident expiring 09/10/2021 00:30:38

Triggered	:	PhishyRequest
Decision	:	escalated thread-level
Action	:	NoAction, expires on 09 Oct 21 00:30:38 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.
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.
ProxyUser	ProxyLogon is the formally generic name for a vulnerability on Server that allows an attacker bypassing the authentication and impersonating as the administrator.