ABUSE REPORT

activity against www.asp-waf.com by

Role object for Panq B.V.

reported from Thu 02 Sep 21 till Thu 16 Sep 21

ABUSE REPORT
ISP Range EXPRES-45-92-228-0

Incidents recorded between 02/09/2021 10:37:51 and 16/09/2021 13:40:28 UTC

To:
Luchthavenweg 81.221
5657EA
Eindhoven
NETHERLANDS
Email abuse@panq.nl

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

Date : Thu 23 September 2021
Reference : EXPRES-45-92-228-0-2021.245-2021.259 - 40
Regarding : Malicious activity detected against www.asp-waf.com dating 02/09/2021 10:37:51UTC - 16/09/2021 13:40:28UTC

Dear Sir/ Madam

This report is addressed to you based on activity that has been triggered by 4 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

Walter Verhoeven
R & D

TABLE OF CONTENTS

MANAGEMENT OVERVIEW

Activity against www.asp-waf.com by Role object for Panq B.V.

based on data captured from Tue 31 Aug 21 till Thu 23 Sep 21
for IP range 45.92.228.0 - 45.92.228.255 (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:

- 29 attempts to steal data by attempting to download confidential data
- 5 attempts to access SQL script
- 5 attempts to URL exploit
- 1 attempt to steal archived cryptocurrency wallets

Abuse score-card Role object for Panq B.V.

on the 18886 days between Thu 01 Jan 1970 and Thu 16 Sep 2021

IP addresses	:	7	IP addresses with incidents	:	7
HTTP requests served	:	61	HTTP incidents	:	176
IP address with port attacks	:	-	Last port attack	:	-
Ports attacked	:	-	Port based Incidents	:	-
Talking IP addresses	:	-	Last Talk	:	-
Talking Applications	:	-	Talks Detected	:	-

on the 22 days between Tue 31 Aug 2021 and Thu 23 Sep 2021

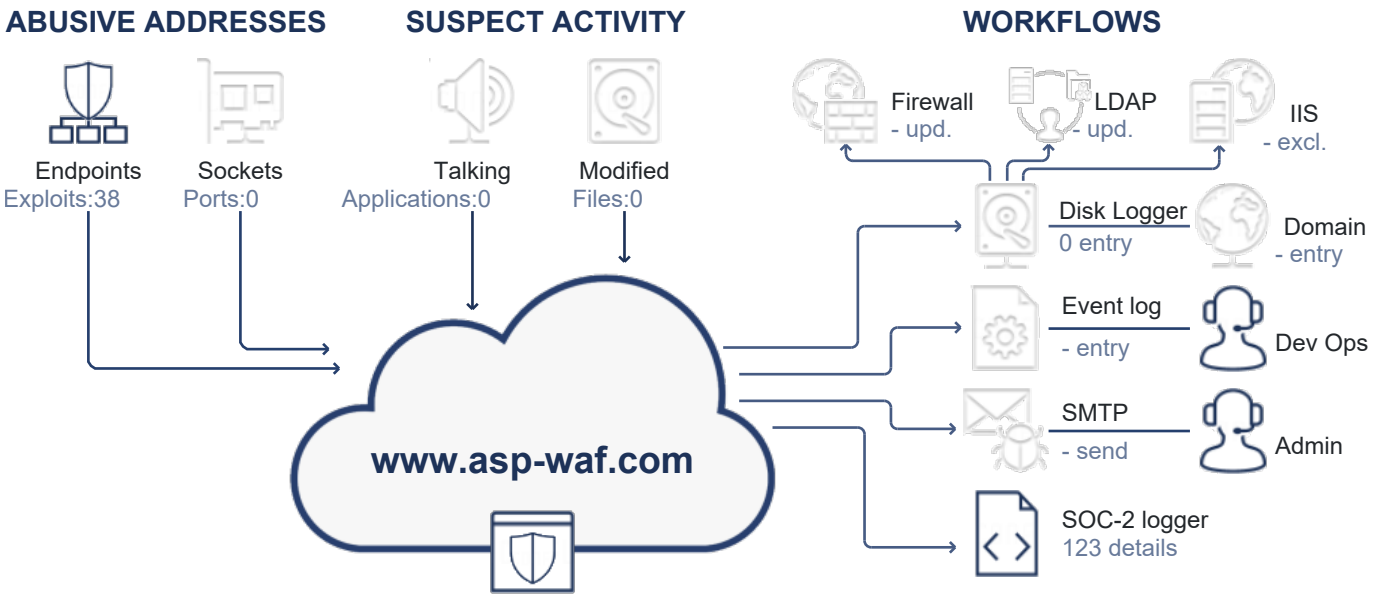
IP Addresses	:	4	IP addresses with incidents	:	-
HTTP requests served	:	40	HTTP incidents	:	-
IP address with port attacks	:	-	Last port attack	:	-
Ports attacked	:	-	Port based incidents	:	-

** 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	40
Human	0
Bot	40
BlackHat	0
Abusive Search Engine	0
Search Engine	0

REQUEST CLASSIFICATION

OK	40
Suspect	0
Redirected	0
Blocked	0

DETECTED ATTACK VECTORS

40	uses URL phishing to probe the system
30	an attempted access protected resources
30	continued attempted to probe exploits after being warned
30	repetitive visits while attempting to probe for exploits
30	repetitive attempts to probe for exploits
23	a Common Vulnerabilities and Exposures (CVE) exploit dete
19	an attempt to gain access to backups
3	accessing a honey-pot trap
3	an attempts to gain access via a manipulated credential
1	repeat requests to probe the system

USED FIREWALL MODULES

The domain www.asp-waf.com is protected using the modules listed in the below table. This abuse report is generated by evaluating the incidents triggered by module Walter.Web.FireWall. The firewall is configured to automatically detect malicious activity and process the incident based on the configuration set by the hosting application.

Modules	*Description*	*Version*
Walter.IO	Detect unauthorized file manipulation in the web application, undoing changes and or taking the site off-line if security is compromised.	2021.9.4.1124
Walter.Net.HoneyPot	Service responsible for detecting penetration attempts against the server. The service records the penetration attempt and issues a system-wide event alarming that there is an attack in progress.	2021.9.4.1124
Walter.Net.LookWhosTalking	Service responsible for recording communication by processes executing on the server with external endpoints.	2021.9.4.1124
Walter.Net.Networking	Resolves WHOIS requests resolving Internet Service Providers responsible for IP addresses as well as reverse DNS queries used for detecting search engines and country level geography discovery.	2021.9.4.1124
Walter.Web.FireWall	Web application firewall with detection service and configurable rule engine.	2021.9.4.1124
Walter.Web.FireWall.DiskLogger	Writes block and release configuration generated by the FireWall to disk and host PowerShell scripts used to configure the external firewall as well as IIS to block or release IP addresses.	2021.9.4.1124
Walter.Web.FireWall.EventLog	Writes incidents to the windows event log for enterprise monitoring and provides SOC-2 end ENISA compliant entries	2021.9.4.1124
Walter.Web.FireWall.Geo.MaxMind	Geo-Location plug-in from MaxMind user for ASN, city and country-level geography discovery using free or paid data from www.maxmind.com	2021.9.4.1124
Walter.Web.FireWall.SMTPLogger	Send incident detections using a mail client to configured mail addresses filtering to the delta of previously unreported activity based on membership profiles	2021.9.4.1124

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!

40 HTTP requests to abuse 38 endpoints

During the reporting period, from Thu 02 September 2021 10:37:51 till Thu 16 September 2021 13:40:28 UTC, we detected 10 unique exploits from 4 IP addresses under your management.

In 14 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
- repeat requests to probe the system
- accessing a honey-pot trap
- an attempts to gain access via a manipulated credential

The next 4 entries document the activities in greater detail.

Malicious HTTP activity from 45.92.228.61

The user on IP address 45.92.228.61 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
- repeat requests to probe the system
- 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 10 different exploits 23 times.

time-line for 45.92.228.61 starts on the next page...

02.Sep.21 *23 penetration attempts period 02/09/2021 10:37:51 - 02/09/2021 11:29:53, all dates in UTC*

10:37:51 **https://asp-waf.com/back/application.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 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 3 exploits and triggered a incident expiring 02/09/2021 14:13:17

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 86 milliseconds
Action : Block, expires on 02 Sep 21 14:13:17 UTC
Notes : Known abuser as a previous exploit was triggered

10:37:59 **https://asp-waf.com/backup/www.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 www.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 02/09/2021 14:13:17

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 96 milliseconds
Action : Block, expires on 02 Sep 21 14:13:17 UTC

10:39:57 **https://asp-waf.com/bak/backup.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 backup.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 02/09/2021 14:13:17

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 119 milliseconds
Action : Block, expires on 02 Sep 21 14:13:17 UTC

activity by 45.92.228.61 continues on the next page...

10:51:07 **https://asp-waf.com/restore/dump.sql**

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 dump.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 3 exploits and triggered a incident expiring 02/09/2021 14:13:17

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 84 milliseconds
Action : Block, expires on 02 Sep 21 14:13:17 UTC

10:55:06 **https://asp-waf.com/backups/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 02/09/2021 14:13:17

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
AttemptToAccessSiteBackup
CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 125 milliseconds
Action : Block, expires on 02 Sep 21 14:13:17 UTC

10:55:18 **https://asp-waf.com/website.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 website.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 3 exploits and triggered a incident expiring 02/09/2021 14:13:17

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 98 milliseconds
Action : Block, expires on 02 Sep 21 14:13:17 UTC

10:55:27 **https://asp-waf.com/public_html.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 public_html.tar 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 02/09/2021 14:13:17

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
AttemptToAccessSiteBackup
CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 142 milliseconds

10:57:52 **https://asp-waf.com/backup/asp-waf.com.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 asp-waf.com.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 02/09/2021 14:13:17

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 180 milliseconds
Action : Block, expires on 02 Sep 21 14:13:17 UTC

10:58:40 **https://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 02/09/2021 14:13:17

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 125 milliseconds
Action : Block, expires on 02 Sep 21 14:13:17 UTC

10:58:42 **https://asp-waf.com/bak/directory.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 directory.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 02/09/2021 14:13:17

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 197 milliseconds
Action : Block, expires on 02 Sep 21 14:13:17 UTC

10:59:22 **https://asp-waf.com/old/directory.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 directory.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 02/09/2021 14:13:17

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 209 milliseconds

11:00:40 **https://asp-waf.com/backup/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 02/09/2021 14:13:17

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 221 milliseconds
Action : Block, expires on 02 Sep 21 14:13:17 UTC

11:01:50 **https://asp-waf.com/back/wallet.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 crypto-currency walletwallet.zip this clearly was an attempt of theft. 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 02/09/2021 14:13:17

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 168 milliseconds
Action : Block, expires on 02 Sep 21 14:13:17 UTC

11:04:13 **https://asp-waf.com/back/www.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 www.tar 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 02/09/2021 14:13:17

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 243 milliseconds
Action : Block, expires on 02 Sep 21 14:13:17 UTC

11:05:02 **https://asp-waf.com/backups/public_html.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.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 02/09/2021 14:13:17

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected

11:06:52 **https://asp-waf.com/asp-waf.com.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 asp-waf.com.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 02/09/2021 14:13:17

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 269 milliseconds
Action : Block, expires on 02 Sep 21 14:13:17 UTC

11:08:58 **https://asp-waf.com/back/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 02/09/2021 14:13:17

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 258 milliseconds
Action : Block, expires on 02 Sep 21 14:13:17 UTC

11:10:58 **https://asp-waf.com/old/latest.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 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 firewall detected 4 exploits and triggered a incident expiring 02/09/2021 14:13:17

Triggered : PageRereshFishing PenetrationAttempt MaliciousUser PhishyRequest CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 238 milliseconds
Action : Block, expires on 02 Sep 21 14:13:17 UTC

11:11:09 **https://asp-waf.com/website.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 website.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 02/09/2021 14:13:17

Triggered : PenetrationAttempt MaliciousUser PhishyRequest

11:15:33 **https://asp-waf.com/bak/wallet.dat**

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 02/09/2021 14:13:17

Triggered : HoneyPotTrap ProxyUser PenetrationAttempt MaliciousUser PhishyRequest CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 224 milliseconds
Action : Block, expires on 02 Sep 21 14:13:17 UTC

11:18:39 **https://asp-waf.com/.bash_history**

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

The firewall detected exploit and triggered a incident expiring 02/09/2021 14:13:17

Triggered : PhishyRequest
Decision : escalated thread-level
Action : NoAction, expires on 02 Sep 21 14:13:17 UTC

11:27:24 **https://asp-waf.com/backups/website.gz**

The firewall flagged the HttpHead request as a malicious intent was 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 detected exploit and triggered a incident expiring 02/09/2021 14:13:17

Triggered : PhishyRequest
Decision : escalated thread-level
Action : NoAction, expires on 02 Sep 21 14:13:17 UTC

11:29:53 **https://asp-waf.com/restore/directory.rar**

The firewall flagged the HttpHead request as a malicious intent was 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 detected exploit and triggered a incident expiring 02/09/2021 14:13:17

Triggered : PhishyRequest
Decision : escalated thread-level
Action : NoAction, expires on 02 Sep 21 14:13:17 UTC

02.Sep.21 *end or reported activity*

Malicious HTTP activity from 45.92.228.52

The user on IP address 45.92.228.52 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.

05.Sep.21 *1 penetration attempt on 05/09/2021 15:38:12, all dates in UTC*

15:38:12 **https://support.asp-waf.com/restore/asp-waf.com.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 asp-waf.com.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 05/09/2021 15:47:40

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 149 milliseconds
Action : Block, expires on 05 Sep 21 15:47:40 UTC
Notes : Known abuser as 7 exploits where triggered

05.Sep.21 *end or reported activity*

Malicious HTTP activity from 45.92.228.63

The user on IP address 45.92.228.63 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploits:

- accessing a honey-pot trap
- an attempts to gain access via a manipulated credential
- 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
- a Common Vulnerabilities and Exposures (CVE) exploit detected
- an attempt to gain access to backups

During the reported time range user of IP address triggered and attempted to use 9 different exploits 7 times.

time-line for 45.92.228.63 starts on the next page...

05.Sep.21 *7 penetration attempts period 05/09/2021 19:06:22 - 05/09/2021 19:30:51, all dates in UTC*

19:06:22 **https://support.asp-waf.com/restore/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 05/09/2021 19:13:56

Triggered : HoneyPotTrap ProxyUser PenetrationAttempt MaliciousUser PhishyRequest CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 129 milliseconds
Action : Block, expires on 05 Sep 21 19:13:56 UTC
Notes : Known abuser as a previous exploit was triggered

19:16:16 **https://support.asp-waf.com/bak/www.rar**

The firewall flagged the HttpHead request as a malicious intent was 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 detected exploit and triggered a incident expiring 05/09/2021 20:06:22

Triggered : PhishyRequest
Decision : escalated thread-level
Action : NoAction, expires on 05 Sep 21 20:06:22 UTC

19:20:11 **https://support.asp-waf.com/backups/.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 firewall detected exploit and triggered a incident expiring 05/09/2021 20:09:07

Triggered : PhishyRequest
Decision : escalated thread-level
Action : NoAction, expires on 05 Sep 21 20:09:07 UTC

19:23:42 **https://support.asp-waf.com/old/latest.zip**

The firewall flagged the HttpHead request as a malicious intent was 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 detected exploit and triggered a incident expiring 05/09/2021 20:09:07

Triggered : PhishyRequest
Decision : escalated thread-level
Action : NoAction, expires on 05 Sep 21 20:09:07 UTC

19:24:02 **https://support.asp-waf.com/backup/directory.rar**

The firewall flagged the HttpHead request as a malicious intent was 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 detected exploit and triggered a incident expiring 05/09/2021 20:09:07

Triggered : PhishyRequest
Decision : return Forbidden
Action : Block, expires on 05 Sep 21 20:09:07 UTC

19:30:04 **https://support.asp-waf.com/restore/public_html.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.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 05/09/2021 20:09:07

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 120 milliseconds
Action : Block, expires on 05 Sep 21 20:09:07 UTC

19:30:51 **https://support.asp-waf.com/application.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 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 3 exploits and triggered a incident expiring 05/09/2021 20:09:07

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 81 milliseconds
Action : Block, expires on 05 Sep 21 20:09:07 UTC

05.Sep.21 *end or reported activity*

Malicious HTTP activity from 45.92.228.57

The user on IP address 45.92.228.57 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 visits while attempting to probe for exploits
- repetitive attempts to probe for exploits
- 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 9 times.

time-line for 45.92.228.57 starts on the next page...

16.Sep.21 *9 penetration attempts period 16/09/2021 10:40:10 - 16/09/2021 13:40:28, all dates in UTC*

10:40:10 **https://support.asp-waf.com/old/www.rar**

The firewall flagged the HttpHead request as a malicious intent was 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 detected exploit and triggered a incident expiring 16/09/2021 10:45:10

Triggered : PhishyRequest
Decision : return Forbidden
Action : Block, expires on 16 Sep 21 10:45:10 UTC

10:47:20 **https://support.asp-waf.com/bak/latest.zip**

The firewall flagged the HttpHead request as a malicious intent was 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 detected exploit and triggered a incident expiring 16/09/2021 10:52:20

Triggered : PhishyRequest
Decision : escalated thread-level
Action : NoAction, expires on 16 Sep 21 10:52:20 UTC

10:59:52 **https://support.asp-waf.com/restore/mysql.sql**

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 mysql.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 3 exploits and triggered a incident expiring 16/09/2021 11:08:58

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 289 milliseconds
Action : Block, expires on 16 Sep 21 11:08:58 UTC

11:05:06 **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 16/09/2021 11:55:06

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
AttemptToAccessSiteBackup
CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 104 milliseconds
Action : Block, expires on 16 Sep 21 11:55:06 UTC

activity by 45.92.228.57 continues on the next page...

11:05:35 **https://support.asp-waf.com/bak/asp-waf.com.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 asp-waf.com.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 16/09/2021 12:10:06

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 109 milliseconds
Action : Block, expires on 16 Sep 21 12:10:06 UTC

11:07:53 **https://support.asp-waf.com/backups/directory.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 directory.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 16/09/2021 12:25:06

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 126 milliseconds
Action : Block, expires on 16 Sep 21 12:25:06 UTC

11:09:45 **https://support.asp-waf.com/back/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 16/09/2021 13:10:06

Triggered : HoneyPotTrap ProxyUser PenetrationAttempt MaliciousUser PhishyRequest CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 140 milliseconds
Action : Block, expires on 16 Sep 21 13:10:06 UTC

11:14:26 **https://support.asp-waf.com/backups/asp-waf.com.zip**

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.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 detected exploit and triggered a incident expiring 16/09/2021 13:47:56

Triggered : PhishyRequest
Decision : escalated thread-level
Action : NoAction, expires on 16 Sep 21 13:47:56 UTC

activity by 45.92.228.57 continues on the next page...

13:40:28 **https://support.asp-waf.com/public_html.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 public_html.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 16/09/2021 13:47:56

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 152 milliseconds
Action : Block, expires on 16 Sep 21 13:47:56 UTC

16.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.
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
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.
ProxyUser	ProxyLogon is the formally generic name for a vulnerability on Server that allows an attacker bypassing the authentication and impersonating as the administrator.