ABUSE REPORT

activity against www.asp-waf.com by

Google LLC

reported from Sun 29 Aug 21 till Mon 27 Sep 21

ABUSE REPORT
ISP Range GOOGLE

Incidents recorded between 29/08/2021 17:38:27 and 27/09/2021 23:12:11 UTC

To:
Google LLC1600 Amphitheatre
Parkway
Mountain View
CA
94043
United States

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

Date : Wed 29 September 2021
Reference : GOOGLE-2021.241-2021.270 - 116
Regarding : Malicious activity detected against www.asp-waf.com dating 29/08/2021 17:38:27UTC - 27/09/2021 23:12:11UTC

Dear Sir/ Madam

This report is addressed to you based on activity that has been triggered by 49 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

TABLE OF CONTENTS

toc continues on the next page...

MANAGEMENT OVERVIEW

Activity against www.asp-waf.com by Google LLC

based on data captured from Sun 29 Aug 21 till Wed 29 Sep 21
for IP range 66.249.64.0 - 66.249.95.255 (8'191 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:

- 82 attempts to URL exploit
- 19 attempts to access the web applications configuration
- 7 attempts to access the system via PHP exploit
- 7 attempts to alter URL's to exploit the web server
- 1 attempt to exploit CVE (common vulnerability & exposure)

Abuse score-card Google LLC

on the 18899 days between Thu 01 Jan 1970 and Wed 29 Sep 2021

IP addresses	:	167	IP addresses with incidents	:	92
HTTP requests served	:	1,052	HTTP incidents	:	500
IP address with port attacks	:	-	Last port attack	:	-
Ports attacked	:	-	Port based Incidents	:	-
Talking IP addresses	:	-	Last Talk	:	-
Talking Applications	:	-	Talks Detected	:	-

on the 31 days between Sun 29 Aug 2021 and Wed 29 Sep 2021

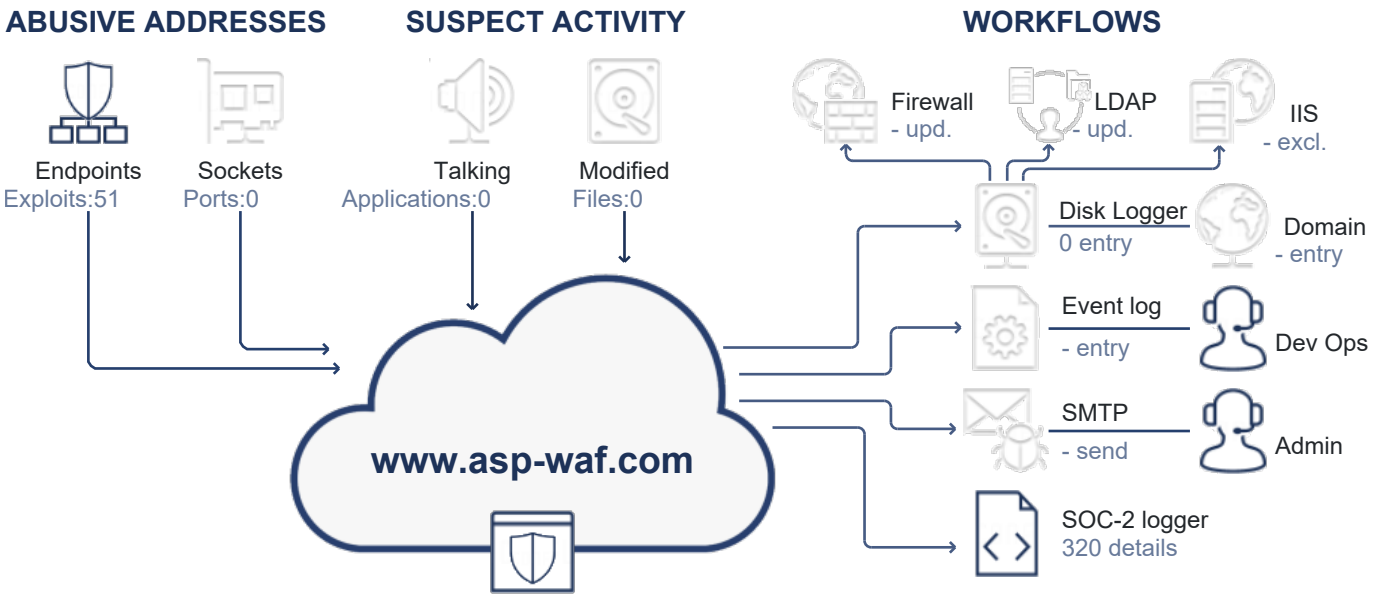
IP Addresses	:	97	IP addresses with incidents	:	1
HTTP requests served	:	401	HTTP incidents	:	1
IP address with port attacks	:	-	Last port attack	:	-
Ports attacked	:	-	Port based incidents	:	-

** 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	767
Human	0
Bot	366
BlackHat	0
Abusive Search Engine	1
Search Engine	400

REQUEST CLASSIFICATION

OK	401
Suspect	1
Redirected	0
Blocked	0

TOP 10 DETECTED ATTACK VECTORS

83	continued attempted to probe exploits after being warned
83	repetitive attempts to probe for exploits
83	uses URL phishing to probe the system
81	an attempted access protected resources
81	repetitive visits while attempting to probe for exploits
31	an attempted to use a CORS exploit
30	a Common Vulnerabilities and Exposures (CVE) exploit dete
20	an attempt to access application configuration
7	an attempt to access the site using the wrong technology sta
5	accessing a honey-pot trap

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!

115 HTTP requests to abuse 51 endpoints

During the reporting period, from Sun 29 August 2021 17:38:27 till Mon 27 September 2021 23:12:11 UTC, we detected 15 unique exploits from 49 IP addresses under your management.

In just 29 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 access application configuration
- a Common Vulnerabilities and Exposures (CVE) exploit detected
- an attempted to use a CORS exploit
- an attempt to access system files
- an attempted to access files while not authorized to do so
- an attempted to perform data scrubbing
- repeat requests to probe the system
- accessing a honey-pot trap
- an attempts to gain access via a manipulated credential
- an attempt to use developer tools to gain access

The next 49 entries document the activities in greater detail.

Malicious HTTP activity from 66.249.76.223

The user on IP address 66.249.76.223 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

During the reported time range user of IP address triggered and attempted to use 5 different exploits once.

02.Sep.21 *1 penetration attempt on 02/09/2021 14:42:28, all dates in UTC*

14:42:28 **https://www.asp-waf.com/images/Nxrs4tAtO/HCw4_2FQ7o69dmQEodXU/_2F**

The firewall flagged the HttpGet 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 14:47:46

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return NotFound after 3 incidents in 279 milliseconds
Action : Block, expires on 02 Sep 21 14:47:46 UTC
Notes : Known abuser as 19 exploits where triggered

02.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.76.44

The user on IP address 66.249.76.44 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 access application configuration
- 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 4 times.

05.Sep.21 *4 penetration attempts period 05/09/2021 14:55:21 - 26/09/2021 11:41:14, all dates in UTC*

14:55:21 **https://www.asp-waf.com/images/Nxrs4tAtO/HCw4_2FQ7o69dmQEodXU/_2F**

The firewall flagged the HttpGet 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 05/09/2021 15:02:31

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 140 milliseconds
Action : Block, expires on 05 Sep 21 15:02:31 UTC
Notes : Known abuser as a previous exploit was triggered

22:41:10 **https://www.asp-waf.com/api/swagger-ui.html**

The firewall flagged the HttpGet 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 09/09/2021 22:46:36

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return NotFound after 3 incidents in 380 milliseconds
Action : Block, expires on 09 Sep 21 22:46:36 UTC

13.Sep.21 16:43:24 **https://www.asp-waf.com/pods**

The firewall flagged the HttpGet 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 13/09/2021 16:48:43

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return NotFound after 3 incidents in 338 milliseconds
Action : Block, expires on 13 Sep 21 16:48:43 UTC

26.Sep.21 11:41:14 **https://www.asp-waf.com/test/wp-includes/wlwmanifest.xml**

The firewall flagged the HttpGet request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to access wlwmanifest.xml as this clearly was an attempt to access confidential configuration data. 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 26/09/2021 11:48:09

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
AttemptOnPluginConfiguration
CommonVulnerabilitiesExposuresExploitDetected
Decision : return NotFound after 4 incidents in 191 milliseconds
Action : Block, expires on 26 Sep 21 11:48:09 UTC

26.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.76.143

The user on IP address 66.249.76.143 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploit:

- an attempted to use a CORS exploit

During the reported time range user of IP address triggered an attempt to use and abuse a single exploit 6 times.

06.Sep.21 *2 penetration attempts on 06/09/2021 17:31:50, all dates in UTC*

17:31:50 **https://support.asp-waf.com/api/SiteMap**

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

The firewall detected exploit and triggered a incident expiring 06/09/2021 17:41:50

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 06 Sep 21 17:41:50 UTC

17:31:51 **https://support.asp-waf.com/api/UserDiscovery**

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

The firewall detected exploit and triggered a incident expiring 06/09/2021 17:43:44

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 06 Sep 21 17:43:44 UTC

06.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.64.170

The user on IP address 66.249.64.170 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

During the reported time range user of IP address triggered and attempted to use 5 different exploits once.

07.Sep.21 *1 penetration attempt on 07/09/2021 13:43:13, all dates in UTC*

13:43:13 **https://www.asp-waf.com/.well-known/security.txt**

The firewall flagged the HttpGet 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 07/09/2021 13:48:57

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 98 milliseconds
Action : Block, expires on 07 Sep 21 13:48:57 UTC
Notes : Known abuser as 11 exploits where triggered

07.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.64.172

The user on IP address 66.249.64.172 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 access system files
- a Common Vulnerabilities and Exposures (CVE) exploit detected

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

07.Sep.21 *2 penetration attempts period 07/09/2021 13:47:18 - 07/09/2021 20:24:55, all dates in UTC*

13:47:18 **https://www.asp-waf.com/console/**

The firewall flagged the HttpGet 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 07/09/2021 13:53:58

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSystemFiles CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 128 milliseconds
Action : Block, expires on 07 Sep 21 13:53:58 UTC
Notes : Known abuser as 10 exploits where triggered

20:24:55 **https://www.asp-waf.com/api/jsonws/invoke**

The firewall flagged the HttpGet 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 07/09/2021 20:33:15

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 110 milliseconds
Action : Block, expires on 07 Sep 21 20:33:15 UTC

07.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.64.174

The user on IP address 66.249.64.174 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
- an attempted to access files while not authorized to do so
- repetitive visits while attempting to probe for exploits
- repetitive attempts to probe for exploits
- uses URL phishing to probe the system
- an attempt to access application configuration
- a Common Vulnerabilities and Exposures (CVE) exploit detected

During the reported time range user of IP address triggered and attempted to use 8 different exploits 5 times.

07.Sep.21 *5 penetration attempts period 07/09/2021 14:17:38 - 10/09/2021 02:26:07, all dates in UTC*

14:17:38 **https://www.asp-waf.com/xmlrpc.php?rsd**

The firewall flagged the HttpGet request as 4 actions that are of malicious intent where detected.The fact that the user attempted to execute xmlrpc.php clearly indicates that your user is attempting to guess his way to an exploit as we do not serve PHP requests. 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 07/09/2021 14:26:05

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 4 incidents in 393 milliseconds
Action : Block, expires on 07 Sep 21 14:26:05 UTC
Notes : Known abuser as 4 exploits where triggered

21:40:02 **https://www.asp-waf.com/_ignition/execute-solution**

The firewall flagged the HttpGet 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 07/09/2021 21:48:31

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 111 milliseconds
Action : Block, expires on 07 Sep 21 21:48:31 UTC

23:49:14 **https://www.asp-waf.com/wp-includes/wlwmanifest.xml**

The firewall flagged the HttpGet request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to access wlwmanifest.xml as this clearly was an attempt to access confidential configuration data. 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 07/09/2021 23:54:29

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration CommonVulnerabilitiesExposuresExploitDetected

04:50:06 **https://www.asp-waf.com/images/Nxrs4tAtO/HCw4_2FQ7o69dmQEodXU/_2F**

The firewall flagged the HttpGet 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 08/09/2021 04:57:39

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 213 milliseconds
Action : Block, expires on 08 Sep 21 04:57:39 UTC

10.Sep.21 02:26:07 **https://www.asp-waf.com/actuator/env**

The firewall flagged the HttpGet 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 10/09/2021 02:35:00

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 164 milliseconds
Action : Block, expires on 10 Sep 21 02:35:00 UTC

10.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.64.74

The user on IP address 66.249.64.74 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploit:

- an attempted to use a CORS exploit

During the reported time range user of IP address triggered an attempt to use and abuse a single exploit 3 times.

08.Sep.21 *1 penetration attempt on 08/09/2021 08:40:12, all dates in UTC*

08:40:12 **https://support.asp-waf.com/api/UserDiscovery**

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

The firewall detected exploit and triggered a incident expiring 08/09/2021 08:45:13

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 08 Sep 21 08:45:13 UTC

08.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.64.76

The user on IP address 66.249.64.76 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploit:

- an attempted to use a CORS exploit

During the reported time range user of IP address triggered an attempt to use and abuse a single exploit 3 times.

08.Sep.21 *1 penetration attempt on 08/09/2021 08:40:11, all dates in UTC*

08:40:11 **https://support.asp-waf.com/api/SiteMap**
The firewall flagged the HttpPost request as a malicious intent was detected.

The firewall detected exploit and triggered a incident expiring 08/09/2021 08:45:12

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 08 Sep 21 08:45:12 UTC

08.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.76.79

The user on IP address 66.249.76.79 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploit:

- an attempted to use a CORS exploit

During the reported time range user of IP address triggered an attempt to use and abuse a single exploit 6 times.

08.Sep.21 *2 penetration attempts on 08/09/2021 19:05:21, all dates in UTC*

19:05:21 **https://asp-waf.com/api/SiteMap**
The firewall flagged the HttpPost request as a malicious intent was detected.

The firewall detected exploit and triggered a incident expiring 08/09/2021 19:15:21

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 08 Sep 21 19:15:21 UTC

19:05:22 **https://asp-waf.com/api/UserDiscovery**
The firewall flagged the HttpPost request as a malicious intent was detected.

The firewall detected exploit and triggered a incident expiring 08/09/2021 19:15:30

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 08 Sep 21 19:15:30 UTC

08.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.76.154

The user on IP address 66.249.76.154 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploits:

- an attempted to use a CORS exploit
- 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 access application configuration
- a Common Vulnerabilities and Exposures (CVE) exploit detected

During the reported time range user of IP address triggered and attempted to use 8 different exploits 12 times.

09.Sep.21 *12 penetration attempts period 09/09/2021 00:30:03 - 27/09/2021 23:12:11, all dates in UTC*

00:30:03 **https://support.asp-waf.com/api/SiteMap**
The firewall flagged the HttpPost request as a malicious intent was detected.

The firewall detected exploit and triggered a incident expiring 09/09/2021 00:40:03

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 09 Sep 21 00:40:03 UTC

00:30:03 **https://support.asp-waf.com/api/UserDiscovery**
The firewall flagged the HttpPost request as a malicious intent was detected.

The firewall detected exploit and triggered a incident expiring 09/09/2021 00:45:03

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 09 Sep 21 00:45:03 UTC

03:02:38 **https://support.asp-waf.com/api/SiteMap**
The firewall flagged the HttpPost request as a malicious intent was detected.

The firewall detected exploit and triggered a incident expiring 09/09/2021 03:07:39

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 09 Sep 21 03:07:39 UTC

03:02:39 **https://support.asp-waf.com/api/UserDiscovery**
The firewall flagged the HttpPost request as a malicious intent was detected.

The firewall detected exploit and triggered a incident expiring 09/09/2021 03:07:39

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 09 Sep 21 03:07:39 UTC

activity by 66.249.76.154 continues on the next page...

13:05:50 **https://support.asp-waf.com/api/SiteMap**
The firewall flagged the HttpPost request as a malicious intent was detected.

The firewall detected exploit and triggered a incident expiring 12/09/2021 13:10:50

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 12 Sep 21 13:10:50 UTC

14:32:07 **https://support.asp-waf.com/api/SiteMap**
The firewall flagged the HttpPost request as a malicious intent was detected.

The firewall detected exploit and triggered a incident expiring 12/09/2021 14:42:08

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 12 Sep 21 14:42:08 UTC

14:32:08 **https://support.asp-waf.com/api/UserDiscovery**
The firewall flagged the HttpPost request as a malicious intent was detected.

The firewall detected exploit and triggered a incident expiring 12/09/2021 14:47:08

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 12 Sep 21 14:47:08 UTC

14.Sep.21 02:49:00 **https://support.asp-waf.com/_all/_search**
The firewall flagged the HttpGet 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 14/09/2021 03:08:42

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 80 milliseconds
Action : Block, expires on 14 Sep 21 03:08:42 UTC

09:51:57 **https://support.asp-waf.com/pods**
The firewall flagged the HttpGet 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 14/09/2021 09:57:42

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 223 milliseconds
Action : Block, expires on 14 Sep 21 09:57:42 UTC

26.Sep.21 10:33:44 **https://support.asp-waf.com/pods**
The firewall flagged the HttpGet 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 26/09/2021 10:41:04

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 156 milliseconds
Action : Block, expires on 26 Sep 21 10:41:04 UTC

08:41:11 **https://support.asp-waf.com/wp1/wp-includes/wlwmanifest.xml**

The firewall flagged the HttpGet request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to access wlwmanifest.xml as this clearly was an attempt to access confidential configuration data. 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 08:51:33

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 196 milliseconds
Action : Block, expires on 27 Sep 21 08:51:33 UTC

23:12:11 **https://support.asp-waf.com/blog/wp-includes/wlwmanifest.xml**

The firewall flagged the HttpGet request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to access wlwmanifest.xml as this clearly was an attempt to access confidential configuration data. 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 23:26:37

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 193 milliseconds
Action : Block, expires on 27 Sep 21 23:26:37 UTC

27.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.76.42

The user on IP address 66.249.76.42 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
- an attempted to perform data scrubbing
- repetitive visits while attempting to probe for exploits
- repetitive attempts to probe for exploits
- uses URL phishing to probe the system
- an attempt to access application configuration
- a Common Vulnerabilities and Exposures (CVE) exploit detected
- repeat requests to probe the system

During the reported time range user of IP address triggered and attempted to use 9 different exploits 6 times.

time-line for 66.249.76.42 starts on the next page...

09.Sep.21 *6 penetration attempts period 09/09/2021 15:14:19 - 10/09/2021 06:50:51, all dates in UTC*

15:14:19 **https://www.asp-waf.com/shop/wp-includes/wlwmanifest.xml**

The firewall flagged the HttpGet request as 5 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to access wlwmanifest.xml as this clearly was an attempt to access confidential configuration data. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 5 exploits and triggered a incident expiring 09/09/2021 15:19:57

Triggered : PenetrationAttempt MaliciousUser PhishyRequest DenailOfService AttemptOnPluginConfiguration CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 5 incidents in 138 milliseconds
Action : Block, expires on 09 Sep 21 15:19:57 UTC
Notes : Known abuser as a previous exploit was triggered

21:07:01 **https://www.asp-waf.com/ftpsync.settings**

The firewall flagged the HttpGet 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 09/09/2021 21:14:44

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 222 milliseconds
Action : Block, expires on 09 Sep 21 21:14:44 UTC

23:26:10 **https://www.asp-waf.com/humans.txt**

The firewall flagged the HttpGet 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 09/09/2021 23:31:36

Triggered : PageRereshFishing PenetrationAttempt MaliciousUser PhishyRequest CommonVulnerabilitiesExposuresExploitDetected
Decision : return NotFound after 4 incidents in 513 milliseconds
Action : Block, expires on 09 Sep 21 23:31:36 UTC

10.Sep.21 *00:33:37* **https://www.asp-waf.com/api/v1/pods**

The firewall flagged the HttpGet 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 10/09/2021 00:39:37

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 261 milliseconds
Action : Block, expires on 10 Sep 21 00:39:37 UTC

activity by 66.249.76.42 continues on the next page...

03:33:37 **https://www.asp-waf.com/2020/wp-includes/wlwmanifest.xml**

The firewall flagged the HttpGet request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to access wlwmanifest.xml as this clearly was an attempt to access confidential configuration data. 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 10/09/2021 03:43:00

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration CommonVulnerabilitiesExposuresExploitDetected
Decision : return NotFound after 4 incidents in 498 milliseconds
Action : Block, expires on 10 Sep 21 03:43:00 UTC

06:50:51 **https://www.asp-waf.com/_all/_search**

The firewall flagged the HttpGet 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 10/09/2021 06:59:43

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 108 milliseconds
Action : Block, expires on 10 Sep 21 06:59:43 UTC

10.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.76.40

The user on IP address 66.249.76.40 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
- repeat requests to probe the system
- an attempted to access files while not authorized to do so
- a Common Vulnerabilities and Exposures (CVE) exploit detected

During the reported time range user of IP address triggered and attempted to use 8 different exploits 4 times.

09.Sep.21 *4 penetration attempts period 09/09/2021 20:20:19 - 13/09/2021 12:58:24, all dates in UTC*

20:20:19 **https://www.asp-waf.com/env**

The firewall flagged the HttpGet 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 09/09/2021 20:25:45

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return NotFound after 3 incidents in 390 milliseconds

23:03:37 **https://www.asp-waf.com/actuator/heapdump**

The firewall flagged the HttpGet 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 09/09/2021 23:11:42

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 233 milliseconds
Action : Block, expires on 09 Sep 21 23:11:42 UTC

10.Sep.21 08:27:03 **https://www.asp-waf.com/images/Nxrs4tAtO/HCw4_2FQ7o69dmQEodXU/_2F**

The firewall flagged the HttpGet 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 10/09/2021 08:35:02

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 242 milliseconds
Action : Block, expires on 10 Sep 21 08:35:02 UTC

13.Sep.21 12:58:24 **https://www.asp-waf.com/phpmyadmin/index.php**

The firewall flagged the HttpGet request as 5 actions that are of malicious intent where detected.The fact that the user attempted to execute index.php clearly indicates that your user is attempting to guess his way to an exploit as we do not serve PHP requests. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 5 exploits and triggered a incident expiring 13/09/2021 13:04:01

Triggered : PageRereshFishing PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteUsingTheTechnologyStack CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 5 incidents in 198 milliseconds
Action : Block, expires on 13 Sep 21 13:04:01 UTC

13.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.75.31

The user on IP address 66.249.75.31 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
- an attempted to access files while not authorized to do so
- repetitive visits while attempting to probe for exploits
- repetitive attempts to probe for exploits
- uses URL phishing to probe the system
- an attempt to access application configuration
- a Common Vulnerabilities and Exposures (CVE) exploit detected

During the reported time range user of IP address triggered and attempted to use 8 different exploits 2 times.

10.Sep.21 *2 penetration attempts period 10/09/2021 12:28:12 - 10/09/2021 22:13:21, all dates in UTC*

12:28:12 **https://www.asp-waf.com/wp-login.php**

The firewall flagged the HttpGet request as 5 actions that are of malicious intent where detected.The fact that the user attempted to execute wp-login.php clearly indicates that your user is attempting to guess his way to an exploit as we do not serve PHP requests. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 5 exploits and triggered a incident expiring 10/09/2021 12:36:42

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration AttemptToAccessSiteUsingTheTechnologyStack CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 5 incidents in 330 milliseconds
Action : Block, expires on 10 Sep 21 12:36:42 UTC
Notes : Known abuser as a previous exploit was triggered

22:13:21 **https://www.asp-waf.com/2019/wp-includes/wlwmanifest.xml**

The firewall flagged the HttpGet request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to access wlwmanifest.xml as this clearly was an attempt to access confidential configuration data. 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 10/09/2021 22:19:22

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 176 milliseconds
Action : Block, expires on 10 Sep 21 22:19:22 UTC

10.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.69.247

The user on IP address 66.249.69.247 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploits:

- an attempted to use a CORS exploit
- 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

During the reported time range user of IP address triggered and attempted to use 6 different exploits 4 times.

10.Sep.21 *4 penetration attempts period 10/09/2021 15:23:39 - 11/09/2021 08:19:25, all dates in UTC*

15:23:39 **https://support.asp-waf.com/api/UserDiscovery**

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

The firewall detected exploit and triggered a incident expiring 10/09/2021 15:33:39

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 10 Sep 21 15:33:39 UTC

15:23:40 **https://support.asp-waf.com/api/SiteMap**

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

The firewall detected exploit and triggered a incident expiring 10/09/2021 15:34:54

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 10 Sep 21 15:34:54 UTC

11.Sep.21 *01:09:17* **https://support.asp-waf.com/GponForm/diag_Form?style/**

The firewall flagged the HttpGet request as 3 actions that are of malicious intent where detected.The user tried to use URL Query string poisoning by injecting ?style/ to bypass detection or alter the system tricking it to do what it's not supposed to do. 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 11/09/2021 01:18:59

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 278 milliseconds
Action : Block, expires on 11 Sep 21 01:18:59 UTC

08:19:25 **https://support.asp-waf.com/api/UserDiscovery**

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

The firewall detected exploit and triggered a incident expiring 11/09/2021 08:24:26

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 11 Sep 21 08:24:26 UTC

11.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.75.1

The user on IP address 66.249.75.1 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
- 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 8 different exploits 2 times.

10.Sep.21 *2 penetration attempts period 10/09/2021 23:43:14 - 11/09/2021 07:09:02, all dates in UTC*

23:43:14 **https://www.asp-waf.com/sftp-config.json**

The firewall flagged the HttpGet request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to access sftp-config.json as this clearly was an attempt to access confidential configuration data. 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 10/09/2021 23:48:40

Triggered : PenetrationAttempt MaliciousUser PhishyRequest CommonVulnerabilitiesExposuresExploitDetected
Decision : return NotFound after 4 incidents in 512 milliseconds
Action : Block, expires on 10 Sep 21 23:48:40 UTC
Notes : Known abuser as a previous exploit was triggered

11.Sep.21 *07:09:02* **https://www.asp-waf.com/login**

The firewall flagged the HttpGet 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 11/09/2021 07:15:24

Triggered : HoneyPotTrap ProxyUser PenetrationAttempt MaliciousUser PhishyRequest CommonVulnerabilitiesExposuresExploitDetected
Decision : return NotFound after 4 incidents in 410 milliseconds
Action : Block, expires on 11 Sep 21 07:15:24 UTC

11.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.66.46

The user on IP address 66.249.66.46 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 access application configuration
- 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.

11.Sep.21 *1 penetration attempt on 11/09/2021 17:43:20, all dates in UTC*

17:43:20 **https://www.asp-waf.com/wp1/wp-includes/wlwmanifest.xml**

The firewall flagged the HttpGet request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to access wlwmanifest.xml as this clearly was an attempt to access confidential configuration data. 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 11/09/2021 17:48:55

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 207 milliseconds
Action : Block, expires on 11 Sep 21 17:48:55 UTC
Notes : Known abuser as a previous exploit was triggered

11.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.66.56

The user on IP address 66.249.66.56 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploit:

- an attempted to use a CORS exploit

During the reported time range user of IP address triggered an attempt to use and abuse a single exploit 3 times.

12.Sep.21 *1 penetration attempt on 12/09/2021 01:33:28, all dates in UTC*

01:33:28 **https://support.asp-waf.com/api/SiteMap**

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

The firewall detected exploit and triggered a incident expiring 12/09/2021 01:43:28

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 12 Sep 21 01:43:28 UTC

12.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.66.58

The user on IP address 66.249.66.58 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploit:

- an attempted to use a CORS exploit

During the reported time range user of IP address triggered an attempt to use and abuse a single exploit 3 times.

12.Sep.21 *1 penetration attempt on 12/09/2021 01:33:29, all dates in UTC*

01:33:29 **https://support.asp-waf.com/api/UserDiscovery**

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

The firewall detected exploit and triggered a incident expiring 12/09/2021 01:38:29

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 12 Sep 21 01:38:29 UTC

12.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.66.51

The user on IP address 66.249.66.51 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploit:

- an attempted to use a CORS exploit

During the reported time range user of IP address triggered an attempt to use and abuse a single exploit 3 times.

12.Sep.21 *1 penetration attempt on 12/09/2021 03:35:58, all dates in UTC*

03:35:58 **https://asp-waf.com/api/SiteMap**

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

The firewall detected exploit and triggered a incident expiring 12/09/2021 03:40:59

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 12 Sep 21 03:40:59 UTC

12.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.76.152

The user on IP address 66.249.76.152 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploits:

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

During the reported time range user of IP address triggered and attempted to use 9 different exploits 5 times.

12.Sep.21 *5 penetration attempts period 12/09/2021 13:05:49 - 27/09/2021 09:26:11, all dates in UTC*

13:05:49 **https://support.asp-waf.com/api/UserDiscovery**

The firewall flagged the HttpPost request as 2 actions that are of malicious intent where detected.

The firewall detected 2 exploits and triggered a incident expiring 12/09/2021 13:15:49

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 12 Sep 21 13:15:49 UTC

14.Sep.21 *08:44:27* **https://support.asp-waf.com/actuator/env**

The firewall flagged the HttpGet 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 14/09/2021 08:52:28

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 110 milliseconds
Action : Block, expires on 14 Sep 21 08:52:28 UTC

26.Sep.21 *06:26:17* **https://support.asp-waf.com/api/UserDiscovery**

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

The firewall detected exploit and triggered a incident expiring 26/09/2021 06:31:17

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 26 Sep 21 06:31:17 UTC

27.Sep.21 *00:48:43* **https://support.asp-waf.com/login**

The firewall flagged the HttpGet 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 27/09/2021 00:57:44

Triggered : HoneyPotTrap ProxyUser PenetrationAttempt MaliciousUser PhishyRequest CommonVulnerabilitiesExposuresExploitDetected

09:26:11 **https://support.asp-waf.com/api/swagger-ui.html**

The firewall flagged the HttpGet 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 27/09/2021 09:31:55

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 117 milliseconds
Action : Block, expires on 27 Sep 21 09:31:55 UTC

27.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.76.156

The user on IP address 66.249.76.156 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
- repeat requests to probe the system
- 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 3 times.

14.Sep.21 *3 penetration attempts period 14/09/2021 02:44:26 - 14/09/2021 09:06:57, all dates in UTC*

02:44:26 **https://support.asp-waf.com/heapdump**

The firewall flagged the HttpGet 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 14/09/2021 02:53:39

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 199 milliseconds
Action : Block, expires on 14 Sep 21 02:53:39 UTC
Notes : Known abuser as a previous exploit was triggered

07:36:57 **https://support.asp-waf.com/humans.txt**

The firewall flagged the HttpGet 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 14/09/2021 07:42:14

Triggered : PageRereshFishing PenetrationAttempt MaliciousUser PhishyRequest CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 331 milliseconds
Action : Block, expires on 14 Sep 21 07:42:14 UTC

activity by 66.249.76.156 continues on the next page...

09:06:57 **https://support.asp-waf.com/.git/config**

The firewall flagged the HttpGet 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 14/09/2021 09:12:32

Triggered : PenetrationAttempt MaliciousUser PhishyRequest CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 303 milliseconds
Action : Block, expires on 14 Sep 21 09:12:32 UTC

14.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.76.75

The user on IP address 66.249.76.75 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploit:

- an attempted to use a CORS exploit

During the reported time range user of IP address triggered an attempt to use and abuse a single exploit 6 times.

14.Sep.21 *1 penetration attempt on 14/09/2021 04:42:41, all dates in UTC*

04:42:41 **https://asp-waf.com/api/UserDiscovery**

The firewall flagged the HttpPost request as 2 actions that are of malicious intent where detected.

The firewall detected 2 exploits and triggered a incident expiring 14/09/2021 04:52:42

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 14 Sep 21 04:52:42 UTC

14.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.76.77

The user on IP address 66.249.76.77 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploit:

- an attempted to use a CORS exploit

During the reported time range user of IP address triggered an attempt to use and abuse a single exploit 3 times.

14.Sep.21 *1 penetration attempt on 14/09/2021 04:42:42, all dates in UTC*

04:42:42 **https://asp-waf.com/api/SiteMap**

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

The firewall detected exploit and triggered a incident expiring 14/09/2021 04:47:42

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 14 Sep 21 04:47:42 UTC

14.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.70.56

The user on IP address 66.249.70.56 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 access application configuration
- a Common Vulnerabilities and Exposures (CVE) exploit detected
- an attempted to access files while not authorized to do so

During the reported time range user of IP address triggered and attempted to use 8 different exploits 4 times.

14.Sep.21 *4 penetration attempts period 14/09/2021 15:29:27 - 19/09/2021 14:07:48, all dates in UTC*

15:29:27 **https://support.asp-waf.com/env**

The firewall flagged the HttpGet 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 14/09/2021 15:35:55

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 207 milliseconds
Action : Block, expires on 14 Sep 21 15:35:55 UTC
Notes : Known abuser as a previous exploit was triggered

15.Sep.21 *11:24:28* **https://support.asp-waf.com/2019/wp-includes/wlwmanifest.xml**

The firewall flagged the HttpGet request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to access wlwmanifest.xml as this clearly was an attempt to access confidential configuration data. 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 15/09/2021 11:30:09

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 176 milliseconds
Action : Block, expires on 15 Sep 21 11:30:09 UTC

11:31:41 **https://support.asp-waf.com/wp-content/plugins/wp-file-manager/readme.txt**

The firewall flagged the HttpGet 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 15/09/2021 11:33:11

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 130 milliseconds

14:07:48 **https://support.asp-waf.com/index.php?s=/Index/%5Cthink%5Capp/invokefu**

The firewall flagged the HttpGet request as 4 actions that are of malicious intent where detected.The fact that the user attempted to execute index.php clearly indicates that your user is attempting to guess his way to an exploit as we do not serve PHP requests. 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 19/09/2021 14:14:32

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 4 incidents in 62 milliseconds
Action : Block, expires on 19 Sep 21 14:14:32 UTC

19.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.70.58

The user on IP address 66.249.70.58 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

During the reported time range user of IP address triggered and attempted to use 5 different exploits 3 times.

14.Sep.21 *3 penetration attempts period 14/09/2021 17:44:27 - 15/09/2021 11:29:07, all dates in UTC*

17:44:27 **https://support.asp-waf.com/api/index.html**

The firewall flagged the HttpGet 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 14/09/2021 17:51:22

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 209 milliseconds
Action : Block, expires on 14 Sep 21 17:51:22 UTC
Notes : Known abuser as a previous exploit was triggered

18:41:07 **https://support.asp-waf.com/actuator/heapdump**

The firewall flagged the HttpGet 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 14/09/2021 18:46:33

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 351 milliseconds
Action : Block, expires on 14 Sep 21 18:46:33 UTC

activity by 66.249.70.58 continues on the next page...

11:29:07 **https://support.asp-waf.com/dns-query?dns=KhUBAAABAAAAAAAAA3d3dv**

The firewall flagged the HttpGet request as 3 actions that are of malicious intent where detected.The user tried to use URL Query string poisoning by injecting ?dns=KhUBAAABAAAAAAAAA3d3dwZnb29nbGUDY29tAAABAAE to bypass detection or alter the system tricking it to do what it's not supposed to do. 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 15/09/2021 12:33:10

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 105 milliseconds
Action : Block, expires on 15 Sep 21 12:33:10 UTC

15.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.70.54

The user on IP address 66.249.70.54 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

During the reported time range user of IP address triggered and attempted to use 5 different exploits 3 times.

15.Sep.21 *3 penetration attempts period 15/09/2021 11:12:30 - 19/09/2021 22:49:48, all dates in UTC*

11:12:30 **https://support.asp-waf.com/_all/_search**

The firewall flagged the HttpGet 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 15/09/2021 11:20:06

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 231 milliseconds
Action : Block, expires on 15 Sep 21 11:20:06 UTC
Notes : Known abuser as a previous exploit was triggered

11:27:45 **https://support.asp-waf.com/mifs/.;/services/LogService**

The firewall flagged the HttpGet 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 15/09/2021 11:33:11

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 351 milliseconds
Action : Block, expires on 15 Sep 21 11:33:11 UTC

activity by 66.249.70.54 continues on the next page...

22:49:48 **https://support.asp-waf.com/env**

The firewall flagged the HttpGet 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 19/09/2021 22:54:50

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 37 milliseconds
Action : Block, expires on 19 Sep 21 22:54:50 UTC

19.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.70.16

The user on IP address 66.249.70.16 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 access application configuration
- a Common Vulnerabilities and Exposures (CVE) exploit detected

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

15.Sep.21 *2 penetration attempts period 15/09/2021 11:33:33 - 19/09/2021 07:22:49, all dates in UTC*

11:33:33 **https://www.asp-waf.com/wp/wp-includes/wlwmanifest.xml**

The firewall flagged the HttpGet request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to access wlwmanifest.xml as this clearly was an attempt to access confidential configuration data. 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 15/09/2021 11:40:11

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 140 milliseconds
Action : Block, expires on 15 Sep 21 11:40:11 UTC
Notes : Known abuser as a previous exploit was triggered

19.Sep.21 07:22:49 **https://www.asp-waf.com/downloads/ASP-WAF-FireWall.chm**

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

The firewall detected exploit and triggered a incident expiring 19/09/2021 07:27:49

Triggered : PhishyRequest
Decision : escalated thread-level
Action : NoAction, expires on 19 Sep 21 07:27:49 UTC

19.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.65.26

The user on IP address 66.249.65.26 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 access application configuration
- a Common Vulnerabilities and Exposures (CVE) exploit detected
- an attempted to access files while not authorized to do so

During the reported time range user of IP address triggered and attempted to use 8 different exploits 4 times.

15.Sep.21 *4 penetration attempts period 15/09/2021 17:56:03 - 16/09/2021 02:42:32, all dates in UTC*

17:56:03 **https://support.asp-waf.com/env**

The firewall flagged the HttpGet 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 15/09/2021 18:01:09

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 136 milliseconds
Action : Block, expires on 15 Sep 21 18:01:09 UTC
Notes : Known abuser as a previous exploit was triggered

20:45:37 **https://support.asp-waf.com/wordpress/wp-includes/wlwmanifest.xml**

The firewall flagged the HttpGet request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to access wlwmanifest.xml as this clearly was an attempt to access confidential configuration data. 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 15/09/2021 20:53:15

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 151 milliseconds
Action : Block, expires on 15 Sep 21 20:53:15 UTC

21:41:05 **https://support.asp-waf.com/_cat/indices?v**

The firewall flagged the HttpGet request as 3 actions that are of malicious intent where detected.The user tried to use URL Query string poisoning by injecting ?v to bypass detection or alter the system tricking it to do what it's not supposed to do. 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 15/09/2021 21:46:32

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 362 milliseconds

02:42:32 **https://support.asp-waf.com/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.p**

The firewall flagged the HttpGet request as 4 actions that are of malicious intent where detected.The fact that the user attempted to execute eval-stdin.php clearly indicates that your user is attempting to guess his way to an exploit as we do not serve PHP requests. 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 02:50:33

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 4 incidents in 650 milliseconds
Action : Block, expires on 16 Sep 21 02:50:33 UTC

16.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.65.22

The user on IP address 66.249.65.22 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 access application configuration
- a Common Vulnerabilities and Exposures (CVE) exploit detected
- an attempted to use a CORS exploit

During the reported time range user of IP address triggered and attempted to use 8 different exploits 5 times.

15.Sep.21 *5 penetration attempts period 15/09/2021 19:48:32 - 16/09/2021 07:03:32, all dates in UTC*

19:48:32 **https://support.asp-waf.com/wp-includes/wlwmanifest.xml**

The firewall flagged the HttpGet request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to access wlwmanifest.xml as this clearly was an attempt to access confidential configuration data. 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 15/09/2021 19:53:48

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 135 milliseconds
Action : Block, expires on 15 Sep 21 19:53:48 UTC
Notes : Known abuser as 4 exploits where triggered

activity by 66.249.65.22 continues on the next page...

22:03:32 **https://support.asp-waf.com/cms/wp-includes/wlwmanifest.xml**

The firewall flagged the HttpGet request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to access wlwmanifest.xml as this clearly was an attempt to access confidential configuration data. 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 15/09/2021 22:11:38

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 325 milliseconds
Action : Block, expires on 15 Sep 21 22:11:38 UTC

16.Sep.21 01:19:22 **https://support.asp-waf.com/api/SiteMap**

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

The firewall detected exploit and triggered a incident expiring 16/09/2021 01:24:22

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 16 Sep 21 01:24:22 UTC

03:18:32 **https://support.asp-waf.com/sftp-config.json**

The firewall flagged the HttpGet request as a malicious intent was detected.We did not appreciate the attempt by your user to access sftp-config.json as this clearly was an attempt to access confidential configuration data.

The firewall detected exploit and triggered a incident expiring 16/09/2021 03:23:32

Triggered : PhishyRequest
Decision : escalated thread-level
Action : NoAction, expires on 16 Sep 21 03:23:32 UTC

07:03:32 **https://support.asp-waf.com/actuator/env**

The firewall flagged the HttpGet 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 16/09/2021 07:09:19

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 208 milliseconds
Action : Block, expires on 16 Sep 21 07:09:19 UTC

16.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.65.24

The user on IP address 66.249.65.24 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
- a Common Vulnerabilities and Exposures (CVE) exploit detected
- an attempt to access system files

During the reported time range user of IP address triggered and attempted to use 7 different exploits 5 times.

15.Sep.21 *5 penetration attempts period 15/09/2021 22:26:02 - 16/09/2021 05:33:32, all dates in UTC*

22:26:02 **https://support.asp-waf.com/Autodiscover/Autodiscover.xml**

The firewall flagged the HttpGet request as 3 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to access Autodiscover.xml as this clearly was an attempt to access confidential configuration data. 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 15/09/2021 22:31:42

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 208 milliseconds
Action : Block, expires on 15 Sep 21 22:31:42 UTC
Notes : Known abuser as 3 exploits where triggered

16.Sep.21 *01:03:32* **https://support.asp-waf.com/ftpsync.settings**

The firewall flagged the HttpGet 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 16/09/2021 01:12:33

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 256 milliseconds
Action : Block, expires on 16 Sep 21 01:12:33 UTC

02:08:07 **https://support.asp-waf.com/.git/config**

The firewall flagged the HttpGet 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 02:17:34

Triggered : PenetrationAttempt MaliciousUser PhishyRequest CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 376 milliseconds
Action : Block, expires on 16 Sep 21 02:17:34 UTC

activity by 66.249.65.24 continues on the next page...

04:48:32 **https://support.asp-waf.com/console/**

The firewall flagged the HttpGet 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 04:53:52

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSystemFiles CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 353 milliseconds
Action : Block, expires on 16 Sep 21 04:53:52 UTC

05:33:32 **https://support.asp-waf.com/_ignition/execute-solution**

The firewall flagged the HttpGet 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 16/09/2021 05:39:01

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 291 milliseconds
Action : Block, expires on 16 Sep 21 05:39:01 UTC

16.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.79.55

The user on IP address 66.249.79.55 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

During the reported time range user of IP address triggered and attempted to use 5 different exploits once.

16.Sep.21 *1 penetration attempt on 16/09/2021 18:41:11, all dates in UTC*

18:41:11 **https://support.asp-waf.com/ftpsync.settings**

The firewall flagged the HttpGet 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 16/09/2021 18:46:37

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 421 milliseconds
Action : Block, expires on 16 Sep 21 18:46:37 UTC
Notes : Known abuser as a previous exploit was triggered

16.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.79.156

The user on IP address 66.249.79.156 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
- an attempted to access files while not authorized to do so
- repetitive visits while attempting to probe for exploits
- repetitive attempts to probe for exploits
- uses URL phishing to probe the system

During the reported time range user of IP address triggered and attempted to use 6 different exploits once.

16.Sep.21 *1 penetration attempt on 16/09/2021 23:47:07, all dates in UTC*

23:47:07 **https://www.asp-waf.com/pmd/index.php**

The firewall flagged the HttpGet request as 4 actions that are of malicious intent where detected.The fact that the user attempted to execute index.php clearly indicates that your user is attempting to guess his way to an exploit as we do not serve PHP requests. 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 23:54:53

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 4 incidents in 314 milliseconds
Action : Block, expires on 16 Sep 21 23:54:53 UTC
Notes : Known abuser as a previous exploit was triggered

16.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.79.60

The user on IP address 66.249.79.60 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 access application configuration
- 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.

17.Sep.21 *1 penetration attempt on 17/09/2021 04:44:39, all dates in UTC*

activity by 66.249.79.60 continues on the next page...

04:44:39 **https://support.asp-waf.com/2020/wp-includes/wlwmanifest.xml**

The firewall flagged the HttpGet request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to access wlwmanifest.xml as this clearly was an attempt to access confidential configuration data. 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 17/09/2021 04:50:11

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 373 milliseconds
Action : Block, expires on 17 Sep 21 04:50:11 UTC
Notes : Known abuser as a previous exploit was triggered

17.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.79.32

The user on IP address 66.249.79.32 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

During the reported time range user of IP address triggered and attempted to use 5 different exploits once.

17.Sep.21 *1 penetration attempt on 17/09/2021 06:18:36, all dates in UTC*

06:18:36 **https://support.asp-waf.com/api/v1/pods**

The firewall flagged the HttpGet 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 17/09/2021 06:24:55

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 198 milliseconds
Action : Block, expires on 17 Sep 21 06:24:55 UTC
Notes : Known abuser as a previous exploit was triggered

17.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.70.18

The user on IP address 66.249.70.18 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

During the reported time range user of IP address triggered and attempted to use 5 different exploits 2 times.

18.Sep.21 *2 penetration attempts period 18/09/2021 00:15:14 - 19/09/2021 07:45:18, all dates in UTC*

00:15:14 **https://www.asp-waf.com/api/index.html**

The firewall flagged the HttpGet 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 18/09/2021 00:24:33

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 217 milliseconds
Action : Block, expires on 18 Sep 21 00:24:33 UTC
Notes : Known abuser as a previous exploit was triggered

19.Sep.21 *07:45:18* **https://www.asp-waf.com/NuGet**

The firewall flagged the HttpGet 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 19/09/2021 07:50:19

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 250 milliseconds
Action : Block, expires on 19 Sep 21 07:50:19 UTC

19.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.66.216

The user on IP address 66.249.66.216 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 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

During the reported time range user of IP address triggered and attempted to use 6 different exploits once.

21.Sep.21 *1 penetration attempt on 21/09/2021 02:49:41, all dates in UTC*

02:49:41 **https://support.asp-waf.com/solr/admin/info/system?wt=json**

The firewall flagged the HttpGet request as 4 actions that are of malicious intent where detected.The user tried to use URL Query string poisoning by injecting ?wt=json to bypass detection or alter the system tricking it to do what it's not supposed to do. 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 21/09/2021 03:00:29

Triggered : HoneyPotTrap PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 4 incidents in 173 milliseconds
Action : Block, expires on 21 Sep 21 03:00:29 UTC
Notes : Known abuser as a previous exploit was triggered

21.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.66.10

The user on IP address 66.249.66.10 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 access application configuration
- 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 3 times.

21.Sep.21 *3 penetration attempts period 21/09/2021 11:50:47 - 25/09/2021 10:33:35, all dates in UTC*

activity by 66.249.66.10 continues on the next page...

11:50:47 **https://www.asp-waf.com/wordpress/wp-includes/wlwmanifest.xml**

The firewall flagged the HttpGet request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to access wlwmanifest.xml as this clearly was an attempt to access confidential configuration data. 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 21/09/2021 11:55:50

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration CommonVulnerabilitiesExposuresExploitDetected
Decision : return NotFound after 4 incidents in 191 milliseconds
Action : Block, expires on 21 Sep 21 11:55:50 UTC
Notes : Known abuser as a previous exploit was triggered

22.Sep.21 09:12:30 **https://www.asp-waf.com/.env**

The firewall flagged the HttpGet request as 3 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to access the Laravel framework /.env as this clearly was an attempt to access Laravel to obtain sensitive information (such as externally usable passwords). 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 22/09/2021 09:20:54

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return NotFound after 3 incidents in 163 milliseconds
Action : Block, expires on 22 Sep 21 09:20:54 UTC

25.Sep.21 10:33:35 **https://www.asp-waf.com/abuse**

The firewall flagged the HttpGet 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 25/09/2021 10:48:36

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return NotFound after 3 incidents in 160 milliseconds
Action : Block, expires on 25 Sep 21 10:48:36 UTC

25.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.66.218

The user on IP address 66.249.66.218 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploit:

- an attempted to use a CORS exploit

During the reported time range user of IP address triggered an attempt to use and abuse a single exploit 3 times.

21.Sep.21 *1 penetration attempt on 21/09/2021 22:46:05, all dates in UTC*

22:46:05 **https://support.asp-waf.com/api/SiteMap**

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

The firewall detected exploit and triggered a incident expiring 21/09/2021 22:51:05

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 21 Sep 21 22:51:05 UTC

21.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.66.214

The user on IP address 66.249.66.214 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 access application configuration
- a Common Vulnerabilities and Exposures (CVE) exploit detected
- an attempted to use a CORS exploit

During the reported time range user of IP address triggered and attempted to use 8 different exploits 4 times.

21.Sep.21 *4 penetration attempts period 21/09/2021 23:49:38 - 26/09/2021 04:24:24, all dates in UTC*

23:49:38 **https://support.asp-waf.com/ads.txt**

The firewall flagged the HttpGet 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 22/09/2021 00:09:38

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 200 milliseconds
Action : Block, expires on 22 Sep 21 00:09:38 UTC
Notes : Known abuser as a previous exploit was triggered

activity by 66.249.66.214 continues on the next page...

14:39:08 **https://support.asp-waf.com/GponForm/diag_Form?style/**

The firewall flagged the HttpGet request as 3 actions that are of malicious intent where detected.The user tried to use URL Query string poisoning by injecting ?style/ to bypass detection or alter the system tricking it to do what it's not supposed to do. 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 23/09/2021 14:47:26

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 73 milliseconds
Action : Block, expires on 23 Sep 21 14:47:26 UTC

26.Sep.21 04:24:21 **https://support.asp-waf.com/api/UserDiscovery**

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

The firewall detected exploit and triggered a incident expiring 26/09/2021 04:34:21

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 26 Sep 21 04:34:21 UTC

04:24:24 **https://support.asp-waf.com/api/SiteMap**

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

The firewall detected exploit and triggered a incident expiring 26/09/2021 04:36:38

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 26 Sep 21 04:36:38 UTC

26.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.66.12

The user on IP address 66.249.66.12 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

During the reported time range user of IP address triggered and attempted to use 5 different exploits 2 times.

22.Sep.21 *2 penetration attempts period 22/09/2021 09:20:29 - 24/09/2021 05:00:26, all dates in UTC*

09:20:29 **https://www.asp-waf.com/dns-query?dns=KhUBAAABAAAAAAAAA3d3dwZr**

The firewall flagged the HttpGet request as 3 actions that are of malicious intent where detected.The user tried to use URL Query string poisoning by injecting ?dns=KhUBAAABAAAAAAAAA3d3dwZnb29nbGUDY29tAAABAAE to bypass detection or alter the system tricking it to do what it's not supposed to do. 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 22/09/2021 09:35:29

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return NotFound after 3 incidents in 168 milliseconds

05:00:26 **https://www.asp-waf.com/env**

The firewall flagged the HttpGet 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 24/09/2021 05:07:32

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return NotFound after 3 incidents in 175 milliseconds
Action : Block, expires on 24 Sep 21 05:07:32 UTC

24.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.69.144

The user on IP address 66.249.69.144 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 access application configuration
- 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.

22.Sep.21 *1 penetration attempt on 22/09/2021 23:41:22, all dates in UTC*

23:41:22 **https://www.asp-waf.com/cms/wp-includes/wlwmanifest.xml**

The firewall flagged the HttpGet request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to access wlwmanifest.xml as this clearly was an attempt to access confidential configuration data. 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 23/09/2021 00:01:23

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration CommonVulnerabilitiesExposuresExploitDetected
Decision : return NotFound after 4 incidents in 128 milliseconds
Action : Block, expires on 23 Sep 21 00:01:23 UTC
Notes : Known abuser as a previous exploit was triggered

22.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.72.86

The user on IP address 66.249.72.86 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploit:

- an attempted to use a CORS exploit

During the reported time range user of IP address triggered an attempt to use and abuse a single exploit 3 times.

23.Sep.21 *1 penetration attempt on 23/09/2021 10:24:32, all dates in UTC*

10:24:32 **https://support.asp-waf.com/api/SiteMap**

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

The firewall detected exploit and triggered a incident expiring 23/09/2021 10:29:32

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 23 Sep 21 10:29:32 UTC

23.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.66.199

The user on IP address 66.249.66.199 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
- continued attempted to probe exploits after being warned
- an attempt to use developer tools to gain access

During the reported time range user of IP address triggered and attempted to use 3 different exploits once.

24.Sep.21 *1 penetration attempt on 24/09/2021 08:45:24, all dates in UTC*

08:45:24 **https://84.195.151.207/**

The firewall flagged the HttpGet request as 2 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 2 exploits and triggered a incident expiring 24/09/2021 08:55:25

Triggered : HoneyPotTrap
Decision : return Forbidden
Action : Block, expires on 24 Sep 21 08:55:25 UTC

24.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.66.65

The user on IP address 66.249.66.65 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploit:

- an attempted to use a CORS exploit

During the reported time range user of IP address triggered an attempt to use and abuse a single exploit 3 times.

25.Sep.21 *1 penetration attempt on 25/09/2021 00:17:49, all dates in UTC*

00:17:49 **https://asp-waf.com/api/UserDiscovery**

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

The firewall detected exploit and triggered a incident expiring 25/09/2021 00:27:50

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 25 Sep 21 00:27:50 UTC

25.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.66.94

The user on IP address 66.249.66.94 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploit:

- an attempted to use a CORS exploit

During the reported time range user of IP address triggered an attempt to use and abuse a single exploit 3 times.

25.Sep.21 *1 penetration attempt on 25/09/2021 00:17:50, all dates in UTC*

00:17:50 **https://asp-waf.com/api/SiteMap**

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

The firewall detected exploit and triggered a incident expiring 25/09/2021 00:22:50

Triggered : CrossSiteRequestRejected
Decision : return Forbidden
Action : Block, expires on 25 Sep 21 00:22:50 UTC

25.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.66.75

The user on IP address 66.249.66.75 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

During the reported time range user of IP address triggered and attempted to use 5 different exploits once.

25.Sep.21 *1 penetration attempt on 25/09/2021 03:03:34, all dates in UTC*

03:03:34 **https://www.asp-waf.com/GponForm/diag_Form?style/**

The firewall flagged the HttpGet request as 3 actions that are of malicious intent where detected.The user tried to use URL Query string poisoning by injecting ?style/ to bypass detection or alter the system tricking it to do what it's not supposed to do. 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 25/09/2021 03:18:35

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return NotFound after 3 incidents in 173 milliseconds
Action : Block, expires on 25 Sep 21 03:18:35 UTC
Notes : Known abuser as a previous exploit was triggered

25.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.66.14

The user on IP address 66.249.66.14 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

During the reported time range user of IP address triggered and attempted to use 5 different exploits once.

26.Sep.21 *1 penetration attempt on 26/09/2021 03:03:33, all dates in UTC*

03:03:33 **https://www.asp-waf.com/security.txt**

The firewall flagged the HttpGet 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 26/09/2021 03:18:33

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return NotFound after 3 incidents in 159 milliseconds
Action : Block, expires on 26 Sep 21 03:18:33 UTC
Notes : Known abuser as a previous exploit was triggered

Malicious HTTP activity from 66.249.76.232

The user on IP address 66.249.76.232 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
- continued attempted to probe exploits after being warned
- an attempt to use developer tools to gain access

During the reported time range user of IP address triggered and attempted to use 3 different exploits once.

27.Sep.21 *1 penetration attempt on 27/09/2021 03:03:43, all dates in UTC*

03:03:43 **https://84.195.151.207/**

The firewall flagged the HttpGet request as 2 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 2 exploits and triggered a incident expiring 27/09/2021 03:09:53

Triggered : HoneyPotTrap
Decision : return Forbidden
Action : Block, expires on 27 Sep 21 03:09:53 UTC

27.Sep.21 *end or reported activity*

Malicious HTTP activity from 66.249.76.150

The user on IP address 66.249.76.150 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
- an attempted to access files while not authorized to do so
- repetitive visits while attempting to probe for exploits
- repetitive attempts to probe for exploits
- uses URL phishing to probe the system
- an attempt to access application configuration
- a Common Vulnerabilities and Exposures (CVE) exploit detected

During the reported time range user of IP address triggered and attempted to use 8 different exploits once.

27.Sep.21 *1 penetration attempt on 27/09/2021 09:03:41, all dates in UTC*

09:03:41 **https://support.asp-waf.com/wp-login.php**

The firewall flagged the HttpGet request as 5 actions that are of malicious intent where detected.The fact that the user attempted to execute wp-login.php clearly indicates that your user is attempting to guess his way to an exploit as we do not serve PHP requests. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 5 exploits and triggered a incident expiring 27/09/2021 09:09:00

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
AttemptOnPluginConfiguration
AttemptToAccessSiteUsingTheTechnologyStack
CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 5 incidents in 60 milliseconds

GLOSSARY

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

AttemptOnPluginConfiguration	An attempt to obtain access to plug-in configuration was detected and blocked. It is safe to say that accessing such resources is only needed when attempting to abuse them.
AttemptToAccessSiteUsingTheTechnologyStack	An attempt to obtain access the site using a framework not compatible with that what is used on the web application. This indicates that the BOT or script is guessing known exploits without knowing the software installed.
AttemptToAccessSystemFiles	An attempt to obtain access to internal files was detected and blocked
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.
CrossSiteRequestRejected	Cross-Site request was detected on a resource that is protected from such access, browser tend to not allow for this so the attacker is using a tool to gain access or manipulate the system
DenailOfService	An attempt was made to take the site down by flooding it with requests
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.