ABUSE REPORT

activity against www.asp-waf.com by

Google LLC

reported from Fri 18 Mar 22 till Sat 26 Mar 22

ABUSE REPORT
ISP Range GOOGLE

Incidents recorded between 18/03/2022 15:55:55 and 26/03/2022 15:35:10 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

Email abuse@google.com
Date : Thu 31 March 2022
Reference : GOOGLE-2022.77-2022.85 - 12
Regarding : Malicious activity detected against www.asp-waf.com dating 18/03/2022 15:55:55UTC - 26/03/2022 15:35:10UTC

Dear Sir/ Madam

This report is addressed to you based on activity that has been triggered by 5 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

MANAGEMENT OVERVIEW

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

based on data captured from Mon 28 Feb 22 till Thu 31 Mar 22
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:

- 10 attempts to URL exploit
- 1 attempt to access the system via PHP exploit
- 1 attempt to access the web applications configuration

Abuse score-card Google LLC

on the 19081 days between Thu 01 Jan 1970 and Wed 30 Mar 2022

IP addresses	:	18	IP addresses with incidents	:	5
HTTP requests served	:	118	HTTP incidents	:	41
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 Mon 28 Feb 2022 and Thu 31 Mar 2022

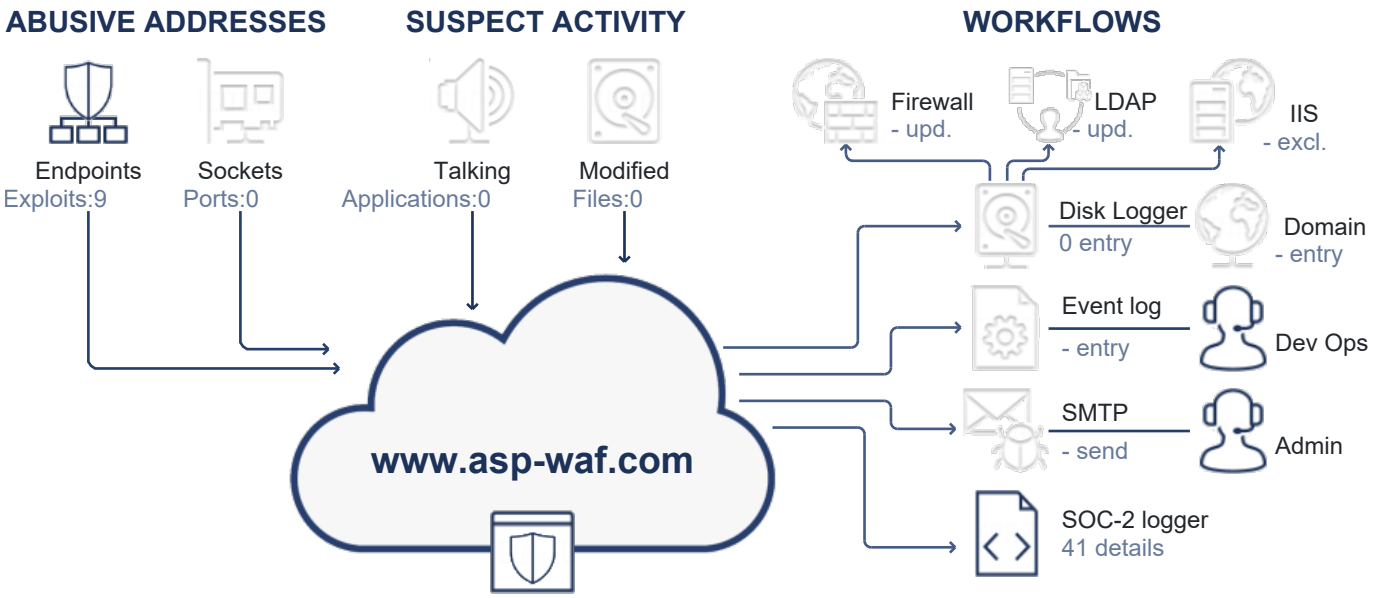
IP Addresses	:	17	IP addresses with incidents	:	-
HTTP requests served	:	118	HTTP incidents	:	-
IP address with port attacks	:	-	Last port attack	:	-
Ports attacked	:	-	Port based incidents	:	-

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

view activity diagram on the next page

ACTIVITY

Activity, response and impact visualization



REQUESTS BY ACTOR

Requests	236
Human	0
Bot	118
BlackHat	0
Abusive Search Engine	0
Search Engine	118

REQUEST CLASSIFICATION

OK	118
Suspect	0
Redirected	0
Blocked	0

DETECTED ATTACK VECTORS

12	an attempted access protected resources
12	continued attempted to probe exploits after being warned
12	repetitive visits while attempting to probe for exploits
12	repetitive attempts to probe for exploits
12	uses URL phishing to probe the system
4	an attempt to access application configuration
4	a Common Vulnerabilities and Exposures (CVE) exploit dete
1	an attempt to access the site using the wrong technology sta

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!

12 HTTP requests to abuse 9 endpoints

During the reporting period, from Fri 18 March 2022 15:55:55 till Sat 26 March 2022 15:35:10 UTC, we detected 8 unique exploits from 5 IP addresses under your management.

In 7 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 access files while not authorized to do so

The next 5 entries document the activities in greater detail.

Malicious HTTP activity from 66.249.76.50

The user on IP address 66.249.76.50 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 6 times.

time-line for 66.249.76.50 starts on the next page...

18.Mar.22 *6 penetration attempts period 18/03/2022 15:55:55 - 20/03/2022 22:15:14, all dates in UTC*

15:55:55 **https://www.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 18/03/2022 16:01:21

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration CommonVulnerabilitiesExposuresExploitDetected
Decision : return NotFound after 4 incidents in 366 milliseconds
Action : Block, expires on 18 Mar 22 16:01:21 UTC

20.Mar.22 *13:47:51* **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 20/03/2022 13:56:43

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return NotFound after 3 incidents in 336 milliseconds
Action : Block, expires on 20 Mar 22 13:56:43 UTC

15:54:35 **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 20/03/2022 16:00:01

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteUsingTheTechnologyStack
Decision : return NotFound after 4 incidents in 362 milliseconds
Action : Block, expires on 20 Mar 22 16:00:01 UTC

18:17:24 **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 20/03/2022 18:24:54

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return NotFound after 3 incidents in 235 milliseconds
Action : Block, expires on 20 Mar 22 18:24:54 UTC

activity by 66.249.76.50 continues on the next page...

19:28:52 **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 20/03/2022 19:34:18

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return NotFound after 3 incidents in 267 milliseconds
Action : Block, expires on 20 Mar 22 19:34:18 UTC

22:15:14 **https://www.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 20/03/2022 22:22:32

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration CommonVulnerabilitiesExposuresExploitDetected
Decision : return NotFound after 4 incidents in 198 milliseconds
Action : Block, expires on 20 Mar 22 22:22:32 UTC

20.Mar.22 *end or reported activity*

Malicious HTTP activity from 66.249.76.46

The user on IP address 66.249.76.46 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

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

20.Mar.22 *3 penetration attempts period 20/03/2022 01:05:09 - 21/03/2022 00:05:27, all dates in UTC*

01:05:09 **https://www.asp-waf.com/Desktop/2021/xaml**

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 20/03/2022 01:10:33

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return NotFound after 3 incidents in 340 milliseconds
Action : Block, expires on 20 Mar 22 01:10:33 UTC

activity by 66.249.76.46 continues on the next page...

10:36:51 **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 20/03/2022 10:42:17

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return NotFound after 3 incidents in 334 milliseconds
Action : Block, expires on 20 Mar 22 10:42:17 UTC

21.Mar.22 00:05:27 **https://www.asp-waf.com/Desktop/2021/xaml**

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 21/03/2022 00:10:59

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return NotFound after 3 incidents in 143 milliseconds
Action : Block, expires on 21 Mar 22 00:10:59 UTC

21.Mar.22 *end or reported activity*

Malicious HTTP activity from 66.249.76.48

The user on IP address 66.249.76.48 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.

20.Mar.22 *1 penetration attempt on 20/03/2022 15:22:55, all dates in UTC*

15:22:55 **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 20/03/2022 15:28:21

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
AttemptOnPluginConfiguration
CommonVulnerabilitiesExposuresExploitDetected
Decision : return NotFound after 4 incidents in 381 milliseconds
Action : Block, expires on 20 Mar 22 15:28:21 UTC

Malicious HTTP activity from 66.249.74.108

The user on IP address 66.249.74.108 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.

24.Mar.22 *1 penetration attempt on 24/03/2022 18:58:03, all dates in UTC*

18:58:03 **https://www.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 24/03/2022 19:03:28

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration CommonVulnerabilitiesExposuresExploitDetected
Decision : return NotFound after 4 incidents in 411 milliseconds
Action : Block, expires on 24 Mar 22 19:03:28 UTC

24.Mar.22 *end or reported activity*

Malicious HTTP activity from 66.249.69.76

The user on IP address 66.249.69.76 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.Mar.22 *1 penetration attempt on 26/03/2022 15:35:10, all dates in UTC*

15:35:10 **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 26/03/2022 15:40:36

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return NotFound after 3 incidents in 283 milliseconds
Action : Block, expires on 26 Mar 22 15:40:36 UTC

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.
CommonVulnerabilitiesExposuresExploitDetected	An attempt to use a CVE registered exploit was detected. The user is trying to use what is likely dark-web malware to gain access using an attack vector that is a publicly disclosed vulnerability.
MaliciousUser	A user is considered to be malicious having been previously rejected, after having been rejected the user still tries to access sensitive data and is therefore again rejected
PenetrationAttempt	The attacker attempted to gain access to the physical server by using cyber attack against the server to check for exploitable vulnerabilities.
PhishyRequest	The firewall detected access to a resource that was never presented to the user and that doesn't exist, The attacker has been detected to be phishing the system using an URL's in order to use exploitable vulnerabilities that he thinks may be present on the server.