ABUSE REPORT

activity against www.asp-waf.com by

IRT-HIPL-SG

reported from Sat 19 Mar 22 till Wed 30 Mar 22

ABUSE REPORT
ISP Range HIPL-SG

Incidents recorded between 19/03/2022 17:54:41 and 30/03/2022 04:50:12 UTC

To:
IRT-HIPL-SG15A Changi
Business Park Central 1
Eightrium # 03-03/04,
Singapore 486035
HUAWEI INTERNATIONAL
PTE. LTD.

Email
hws_security@huawei.com

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

Date : Thu 31 March 2022
Reference : HIPL-SG-2022.78-2022.89 - 10
Regarding : Malicious activity detected against www.asp-waf.com dating 19/03/2022 17:54:41UTC - 30/03/2022 04:50:12UTC

Dear Sir/ Madam

This report is addressed to you based on activity that has been triggered by 6 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 IRT-HIPL-SG

based on data captured from Mon 28 Feb 22 till Thu 31 Mar 22
for IP range 114.119.128.0 - 114.119.191.255 (16'383 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:

5 attempts to alter URL's to exploit the web server
5 attempts to URL exploit

Abuse score-card IRT-HIPL-SG

on the 19082 days between Thu 01 Jan 1970 and Thu 31 Mar 2022

IP addresses	:	10	IP addresses with incidents	:	6
HTTP requests served	:	49	HTTP incidents	:	26
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

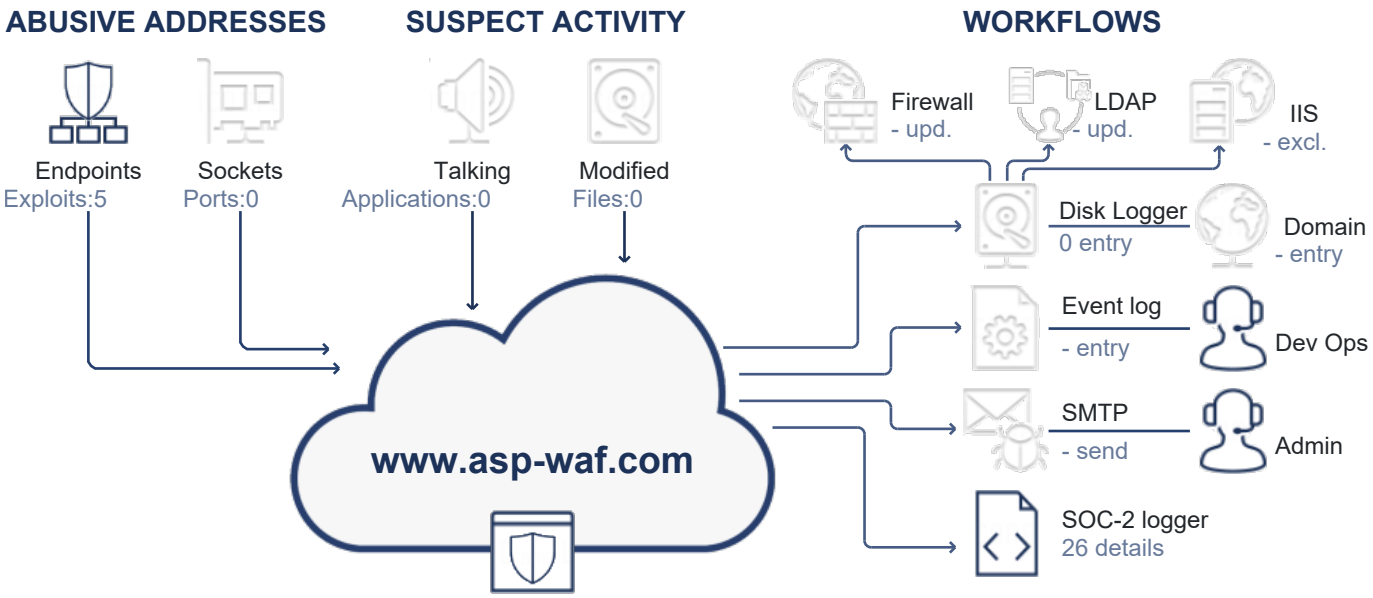
IP Addresses	:	9	IP addresses with incidents	:	-
HTTP requests served	:	47	HTTP incidents	:	-
IP address with port attacks	:	-	Last port attack	:	-
Ports attacked	:	-	Port based incidents	:	-

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

REQUEST CLASSIFICATION

OK	47
Suspect	0
Redirected	0
Blocked	0

DETECTED ATTACK VECTORS

8 an attempted access protected resources
8 continued attempted to probe exploits after being warned
8 repetitive visits while attempting to probe for exploits
8 repetitive attempts to probe for exploits
8 uses URL phishing to probe the system
2 accessing a honey-pot trap
2 an attempts to gain access via a manipulated credential
2 a Common Vulnerabilities and Exposures (CVE) exploit detec

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!

10 HTTP requests to abuse 5 endpoints

During the reporting period, from Sat 19 March 2022 17:54:41 till Wed 30 March 2022 04:50:12 UTC, we detected 8 unique exploits from 6 IP addresses under your management.

In 10 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
- accessing a honey-pot trap
- an attempts to gain access via a manipulated credential
- a Common Vulnerabilities and Exposures (CVE) exploit detected

We noted that there is an overlap between the 0 IP addresses that are attacking based on the same 5 ports. Is this a coincidence or a distributed attack? We would appreciate an update in regards to this matter.

The next 6 entries document the activities in greater detail.

Malicious HTTP activity from 114.119.143.135

The user on IP address 114.119.143.135 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.

19.Mar.22 *2 penetration attempts period 19/03/2022 17:54:41 - 30/03/2022 04:31:51, all dates in UTC*

17:54:41 **https://www.asp-waf.com/api/token?userName=guest&password=Guest**

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 ?userName=guest&password=Guest 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 19/03/2022 17:59:59

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : escalated thread-level after 3 incidents in 157 milliseconds
Action : Block, expires on 19 Mar 22 17:59:59 UTC

30.Mar.22 *04:31:51* **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 30/03/2022 04:41:12

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : escalated thread-level after 3 incidents in 147 milliseconds
Action : Block, expires on 30 Mar 22 04:41:12 UTC

30.Mar.22 *end or reported activity*

Malicious HTTP activity from 114.119.143.172

The user on IP address 114.119.143.172 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

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

21.Mar.22 *2 penetration attempts period 21/03/2022 17:59:20 - 24/03/2022 19:36:00, all dates in UTC*

17:59:20 **https://www.asp-waf.com/download/WAFGettingStarted.pdf**

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 18:04:46

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : escalated thread-level after 3 incidents in 368 milliseconds
Action : Block, expires on 21 Mar 22 18:04:46 UTC

24.Mar.22 *19:36:00* **https://www.asp-waf.com/api/token?userName=guest&password=Guest**

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 ?userName=guest&password=Guest 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 24/03/2022 19:43:36

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : escalated thread-level after 3 incidents in 83 milliseconds
Action : Block, expires on 24 Mar 22 19:43:36 UTC

24.Mar.22 *end or reported activity*

Malicious HTTP activity from 114.119.143.158

The user on IP address 114.119.143.158 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
- 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 8 different exploits 2 times.

23.Mar.22 *2 penetration attempts period 23/03/2022 06:41:10 - 28/03/2022 15:56:14, all dates in UTC*

06:41:10 **https://www.asp-waf.com/gdpr**

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 23/03/2022 06:46:36

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : escalated thread-level after 3 incidents in 249 milliseconds
Action : Block, expires on 23 Mar 22 06:46:36 UTC

28.Mar.22 *15:56:14* **https://www.asp-waf.com/Account/Login?ReturnUrl=/Membership**

The firewall flagged the HttpGet request as a malicious intent was detected.The user tried to use URL Query string poisoning by injecting ?ReturnUrl=/Membership to bypass detection or alter the system tricking it to do what it's not supposed to do.

The firewall detected exploit and triggered a incident expiring 28/03/2022 16:01:14

Triggered : HoneyPotTrap ProxyUser CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden
Action : Block, expires on 28 Mar 22 16:01:14 UTC

28.Mar.22 *end or reported activity*

Malicious HTTP activity from 114.119.143.145

The user on IP address 114.119.143.145 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploits:

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

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

23.Mar.22 *1 penetration attempt on 23/03/2022 13:36:46, all dates in UTC*

13:36:46 **https://www.asp-waf.com/Account/Login?ReturnUrl=/Membership**

The firewall flagged the HttpGet request as a malicious intent was detected.The user tried to use URL Query string poisoning by injecting ?ReturnUrl=/Membership to bypass detection or alter the system tricking it to do what it's not supposed to do.

The firewall detected exploit and triggered a incident expiring 23/03/2022 13:41:46

Triggered : HoneyPotTrap ProxyUser CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden
Action : Block, expires on 23 Mar 22 13:41:46 UTC

23.Mar.22 *end or reported activity*

Malicious HTTP activity from 114.119.143.14

The user on IP address 114.119.143.14 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 2 times.

24.Mar.22 *2 penetration attempts period 24/03/2022 22:14:54 - 28/03/2022 18:16:57, all dates in UTC*

22:14:54 **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 24/03/2022 22:20:14

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : escalated thread-level after 3 incidents in 250 milliseconds
Action : Block, expires on 24 Mar 22 22:20:14 UTC

activity by 114.119.143.14 continues on the next page...

18:16:57 **https://www.asp-waf.com/gdpr**

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 28/03/2022 18:24:38

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : escalated thread-level after 3 incidents in 83 milliseconds
Action : Block, expires on 28 Mar 22 18:24:38 UTC

28.Mar.22 *end or reported activity*

Malicious HTTP activity from 114.119.143.168

The user on IP address 114.119.143.168 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.

30.Mar.22 *1 penetration attempt on 30/03/2022 04:50:12, all dates in UTC*

04:50:12 **https://www.asp-waf.com/api/token?userName=guest&password=Guest**

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 ?userName=guest&password=Guest 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 30/03/2022 04:56:15

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : escalated thread-level after 3 incidents in 83 milliseconds
Action : Block, expires on 30 Mar 22 04:56:15 UTC

30.Mar.22 *end or reported activity*

GLOSSARY

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

CommonVulnerabilitiesExposuresExploitDetected	An attempt to use a CVE registered exploit was detected. The user is trying to use what is likely dark-web malware to gain access using an attack vector that is a publicly disclosed vulnerability.
HoneyPotTrap	The firewall, or the site hosting the firewall, generated a trap for hackers hidden for normal users, the firewall detected that the system tried to access the trap.
MaliciousUser	A user is considered to be malicious having been previously rejected, after having been rejected the user still tries to access sensitive data and is therefore again rejected
PenetrationAttempt	The attacker attempted to gain access to the physical server by using cyber attack against the server to check for exploitable vulnerabilities.
PhishyRequest	The firewall detected access to a resource that was never presented to the user and that doesn't exist, The attacker has been detected to be phishing the system using an URL's in order to use exploitable vulnerabilities that he thinks may be present on the server.
ProxyUser	ProxyLogon is the formally generic name for a vulnerability on Server that allows an attacker bypassing the authentication and impersonating as the administrator.