ABUSE REPORT

activity against localhost by

Kawmi Online administrator

reported from Mon 09 Aug 21 till Thu 09 Sep 21

ABUSE REPORT
ISP Range KAWMIONLINE-BD

Incidents recorded between 09/08/2021 23:00:05 and 09/09/2021 03:13:29 UTC

To:
B/6 Pallabi Extension Pallabi
Dhaka-1216 Dhaka
Email kawmionline@gmail.com

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

Date : Thu 09 September 2021
Reference : KAWMIONLINE-BD-221.252-31
Regarding : Malicious activity detected against localhost dating 09/08/2021 23:00:05UTC - 09/09/2021 03:13:29UTC

Dear Sir/ Madam

This report is addressed to you based on activity that has been triggered by 1 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 localhost 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 localhost by Kawmi Online administrator

based on data captured from Mon 09 Aug 21 till Thu 09 Sep 21
for IP range 144.48.116.0 - 144.48.119.255 (1'023 IP in scope)

Every request against localhost 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:

31 attempts to access the system via PHP exploit

Abuse score-card Kawmi Online administrator

on the 413 days between Wed 22 Jul 2020 and Thu 09 Sep 2021

IP addresses	:	1	IP addresses with incidents	:	1
HTTP requests served	:	41	HTTP incidents	:	218
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 09 Aug 2021 and Thu 09 Sep 2021

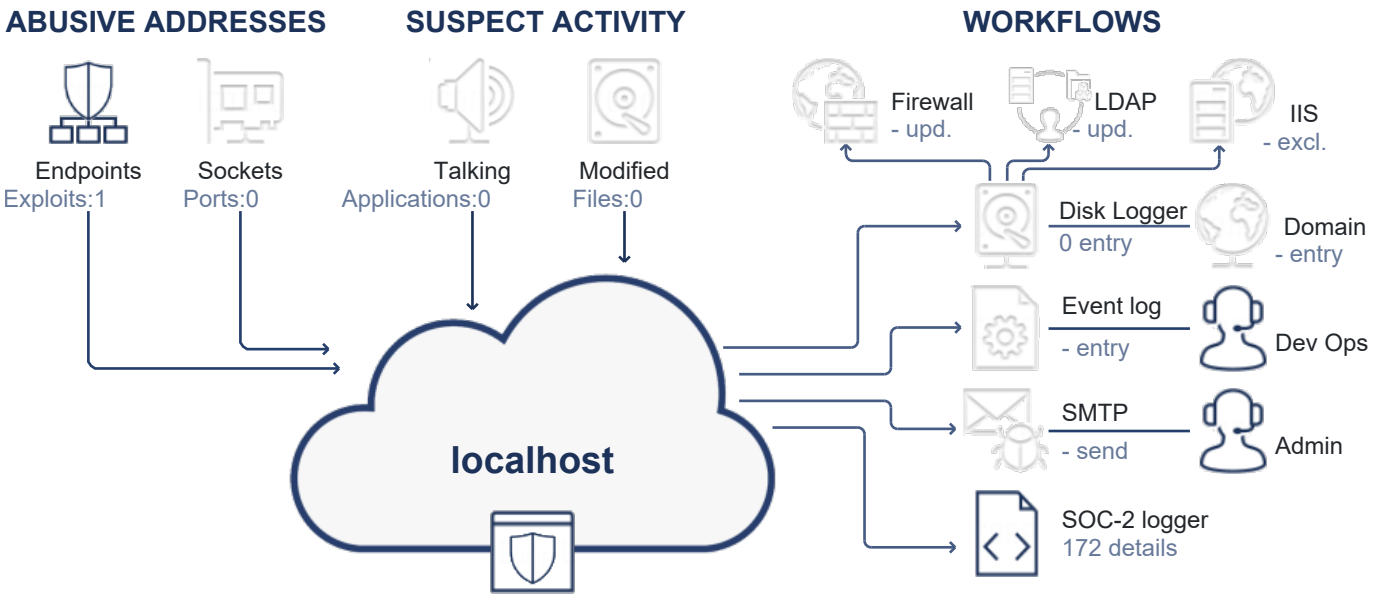
IP Addresses	:	1	IP addresses with incidents	:	1
HTTP requests served	:	5	HTTP incidents	:	26
IP address with port attacks	:	-	Last port attack	:	-
Ports attacked	:	-	Port based incidents	:	-

** 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	31
Human	0
Bot	31
BlackHat	0
Abusive Search Engine	0
Search Engine	0

REQUEST CLASSIFICATION

OK	5
Suspect	0
Redirected	0
Blocked	26

DETECTED ATTACK VECTORS

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

ABUSE OVERVIEW

The malicious activity documented in the section is proof of activity that is considered outside regular activity that is expected in localhost. 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!

31 HTTP requests to abuse 1 endpoint

During the reporting period, from Mon 09 August 2021 23:00:05 till Thu 09 September 2021 03:13:29 UTC, we detected 10 unique exploits from 1 IP address under your management.

In 30 days we detected:
- accessing a honey-pot trap
- an attempted access protected resources
- continued attempted to probe exploits after being warned
- an attempted to access files while not authorized to do so
- an attempt to use developer tools to gain access
- repetitive attempts to probe for exploits
- uses URL phishing to probe the system
- repetitive visits while attempting to probe for exploits
- an attempt to access application configuration
- a Common Vulnerabilities and Exposures (CVE) exploit detected

The below entry documents the activities in greater detail.

Malicious HTTP activity from 144.48.118.133

The user on IP address 144.48.118.133 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
- an attempted to access files while not authorized to do so
- an attempt to use developer tools to gain access
- repetitive attempts to probe for exploits
- uses URL phishing to probe the system
- repetitive visits while attempting to probe for exploits
- 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 10 different exploits 31 times.In total we detected 6 exploits with 493 attempts from 09 Aug 21 and 09 Sep 21. We recorded:

- 148 attempts to access resources using malformed URL phishing technique
- 121 port-based attempt to exploit the server
- 106 attempts to access confidential data
- 78 repeated engagements with the site while being blocked

09.Aug.21 *31 penetration attempts period 09/08/2021 23:00:05 - 09/09/2021 03:13:29, all dates in UTC*

23:00:05 **https://84.195.151.207/admin/config.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 config.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 most significant reasons to reject the request where "A non supported URL was called", "The user is using a port scanner", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToConfigurationAllowed pattern", "A non supported handler .php was called"

Triggered : HoneyPotTrap MaliciousUser PhishyRequest AttemptOnPluginConfiguration AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 5 incidents in 359 milliseconds
Action : Block, expires on 09 Aug 21 23:05:05 UTC
Notes : Known abuser as 44 exploits where triggered

10.Aug.21 *12:19:22* **https://84.195.151.207/admin/config.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 config.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 most significant reasons to reject the request where "A non supported URL was called", "The user is using a port scanner", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToConfigurationAllowed pattern", "A non supported handler .php was called"

Triggered : HoneyPotTrap MaliciousUser PhishyRequest AttemptOnPluginConfiguration AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 5 incidents in 146 milliseconds
Action : Block, expires on 10 Aug 21 12:24:22 UTC

11.Aug.21 *01:44:39* **https://84.195.151.207/admin/config.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 config.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 most significant reasons to reject the request where "A non supported URL was called", "The user is using a port scanner", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToConfigurationAllowed pattern", "A non supported handler .php was called"

Triggered : HoneyPotTrap MaliciousUser PhishyRequest AttemptOnPluginConfiguration

15:16:56 **https://84.195.151.207/admin/config.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 config.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 most significant reasons to reject the request where "A non supported URL was called", "The user is using a port scanner", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToConfigurationAllowed pattern", "A non supported handler .php was called"

Triggered : HoneyPotTrap MaliciousUser PhishyRequest AttemptOnPluginConfiguration AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 5 incidents in 151 milliseconds
Action : Block, expires on 11 Aug 21 15:21:56 UTC

12.Aug.21 04:24:07 **https://84.195.151.207/admin/config.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 config.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 most significant reasons to reject the request where "A non supported URL was called", "The user is using a port scanner", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToConfigurationAllowed pattern", "A non supported handler .php was called"

Triggered : HoneyPotTrap MaliciousUser PhishyRequest AttemptOnPluginConfiguration AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 5 incidents in 367 milliseconds
Action : Block, expires on 12 Aug 21 04:29:08 UTC

17:58:00 **https://84.195.151.207/admin/config.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 config.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 most significant reasons to reject the request where "A non supported URL was called", "The user is using a port scanner", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToConfigurationAllowed pattern", "A non supported handler .php was called"

Triggered : HoneyPotTrap MaliciousUser PhishyRequest AttemptOnPluginConfiguration AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 5 incidents in 314 milliseconds

07:01:41 **https://84.195.151.207/admin/config.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 config.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 most significant reasons to reject the request where "A non supported URL was called", "The user is using a port scanner", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToConfigurationAllowed pattern", "A non supported handler .php was called"

Triggered : HoneyPotTrap MaliciousUser PhishyRequest AttemptOnPluginConfiguration AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 5 incidents in 271 milliseconds
Action : Block, expires on 13 Aug 21 07:06:41 UTC

20:24:25 **https://84.195.151.207/admin/config.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 config.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 most significant reasons to reject the request where "A non supported URL was called", "The user is using a port scanner", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToConfigurationAllowed pattern", "A non supported handler .php was called"

Triggered : HoneyPotTrap MaliciousUser PhishyRequest AttemptOnPluginConfiguration AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 5 incidents in 173 milliseconds
Action : Block, expires on 13 Aug 21 20:29:26 UTC

14.Aug.21 09:40:28 **https://84.195.151.207/admin/config.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 config.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 most significant reasons to reject the request where "A non supported URL was called", "The user is using a port scanner", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToConfigurationAllowed pattern", "A non supported handler .php was called"

Triggered : HoneyPotTrap MaliciousUser PhishyRequest AttemptOnPluginConfiguration AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 5 incidents in 460 milliseconds

22:50:44 **https://84.195.151.207/admin/config.php**

The firewall flagged the HttpGet request as 6 actions that are of malicious intent where detected.The fact that the user attempted to execute config.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 most significant reasons to reject the request where "A non supported URL was called", "The user is using a port scanner", "A non supported URL was called as the user has no access to https://84.195.151.207/admin/config.php", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToConfigurationAllowed pattern", "A non supported handler .php was called"

Triggered : HoneyPotTrap PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 6 incidents in 354 milliseconds
Action : Block, expires on 14 Aug 21 22:55:45 UTC

15.Aug.21 12:14:17 **https://84.195.151.207/admin/config.php**

The firewall flagged the HttpGet request as 6 actions that are of malicious intent where detected.The fact that the user attempted to execute config.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 most significant reasons to reject the request where "A non supported URL was called", "The user is using a port scanner", "A non supported URL was called as the user has no access to https://84.195.151.207/admin/config.php", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToConfigurationAllowed pattern", "A non supported handler .php was called"

Triggered : HoneyPotTrap PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 6 incidents in 177 milliseconds
Action : Block, expires on 15 Aug 21 12:19:17 UTC

16.Aug.21 01:28:54 **https://84.195.151.207/admin/config.php**

The firewall flagged the HttpGet request as 6 actions that are of malicious intent where detected.The fact that the user attempted to execute config.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 most significant reasons to reject the request where "A non supported URL was called", "The user is using a port scanner", "A non supported URL was called as the user has no access to https://84.195.151.207/admin/config.php", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToConfigurationAllowed pattern", "A non supported handler .php was called"

Triggered : HoneyPotTrap PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration

15:00:57 **https://84.195.151.207/admin/config.php**

The firewall flagged the HttpGet request as 6 actions that are of malicious intent where detected.The fact that the user attempted to execute config.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 most significant reasons to reject the request where "A non supported URL was called", "The user is using a port scanner", "A non supported URL was called as the user has no access to https://84.195.151.207/admin/config.php", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToConfigurationAllowed pattern", "A non supported handler .php was called"

Triggered : HoneyPotTrap PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 6 incidents in 353 milliseconds
Action : Block, expires on 16 Aug 21 15:05:58 UTC

17.Aug.21 04:13:34 **https://84.195.151.207/admin/config.php**

The firewall flagged the HttpGet request as 6 actions that are of malicious intent where detected.The fact that the user attempted to execute config.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 most significant reasons to reject the request where "A non supported URL was called", "The user is using a port scanner", "A non supported URL was called as the user has no access to https://84.195.151.207/admin/config.php", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToConfigurationAllowed pattern", "A non supported handler .php was called"

Triggered : HoneyPotTrap PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 6 incidents in 349 milliseconds
Action : Block, expires on 17 Aug 21 04:18:35 UTC

17:37:57 **https://84.195.151.207/admin/config.php**

The firewall flagged the HttpGet request as 6 actions that are of malicious intent where detected.The fact that the user attempted to execute config.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 most significant reasons to reject the request where "A non supported URL was called", "The user is using a port scanner", "A non supported URL was called as the user has no access to https://84.195.151.207/admin/config.php", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToConfigurationAllowed pattern", "A non supported handler .php was called"

Triggered : HoneyPotTrap PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration

06:47:34 **https://84.195.151.207/admin/config.php**

The firewall flagged the HttpGet request as 6 actions that are of malicious intent where detected.The fact that the user attempted to execute config.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 most significant reasons to reject the request where "A non supported URL was called", "The user is using a port scanner", "A non supported URL was called as the user has no access to https://84.195.151.207/admin/config.php", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToConfigurationAllowed pattern", "A non supported handler .php was called"

Triggered : HoneyPotTrap PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 6 incidents in 391 milliseconds
Action : Block, expires on 18 Aug 21 06:52:35 UTC

19:49:59 **https://84.195.151.207/admin/config.php**

The firewall flagged the HttpGet request as 6 actions that are of malicious intent where detected.The fact that the user attempted to execute config.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 most significant reasons to reject the request where "A non supported URL was called", "The user is using a port scanner", "A non supported URL was called as the user has no access to https://84.195.151.207/admin/config.php", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToConfigurationAllowed pattern", "A non supported handler .php was called"

Triggered : HoneyPotTrap PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 6 incidents in 366 milliseconds
Action : Block, expires on 18 Aug 21 19:55:00 UTC

19.Aug.21 09:00:28 **https://84.195.151.207/admin/config.php**

The firewall flagged the HttpGet request as 6 actions that are of malicious intent where detected.The fact that the user attempted to execute config.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 most significant reasons to reject the request where "A non supported URL was called", "The user is using a port scanner", "A non supported URL was called as the user has no access to https://84.195.151.207/admin/config.php", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToConfigurationAllowed pattern", "A non supported handler .php was called"

Triggered : HoneyPotTrap PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration

22:06:05 **https://84.195.151.207/admin/config.php**

The firewall flagged the HttpGet request as 6 actions that are of malicious intent where detected.The fact that the user attempted to execute config.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 most significant reasons to reject the request where "A non supported URL was called", "The user is using a port scanner", "A non supported URL was called as the user has no access to https://84.195.151.207/admin/config.php", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToConfigurationAllowed pattern", "A non supported handler .php was called"

Triggered : HoneyPotTrap PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 6 incidents in 566 milliseconds
Action : Block, expires on 19 Aug 21 22:11:07 UTC

20.Aug.21 11:13:45 **https://84.195.151.207/admin/config.php**

The firewall flagged the HttpGet request as 6 actions that are of malicious intent where detected.The fact that the user attempted to execute config.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 most significant reasons to reject the request where "A non supported URL was called", "The user is using a port scanner", "A non supported URL was called as the user has no access to https://84.195.151.207/admin/config.php", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToConfigurationAllowed pattern", "A non supported handler .php was called"

Triggered : HoneyPotTrap PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration AttemptToAccessSiteUsingTheTechnologyStack CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 6 incidents in 317 milliseconds
Action : Block, expires on 20 Aug 21 11:18:45 UTC

21.Aug.21 00:50:33 **https://84.195.151.207/admin/config.php**

The firewall flagged the HttpGet request as 6 actions that are of malicious intent where detected.The fact that the user attempted to execute config.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 most significant reasons to reject the request where "A non supported URL was called", "The user is using a port scanner", "A non supported URL was called as the user has no access to https://84.195.151.207/admin/config.php", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToConfigurationAllowed pattern", "A non supported handler .php was called"

Triggered : HoneyPotTrap PenetrationAttempt MaliciousUser PhishyRequest

14:27:23 **https://84.195.151.207/admin/config.php**

The firewall flagged the HttpGet request as 6 actions that are of malicious intent where detected.The fact that the user attempted to execute config.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 most significant reasons to reject the request where "A non supported URL was called", "The user is using a port scanner", "A non supported URL was called as the user has no access to https://84.195.151.207/admin/config.php", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToConfigurationAllowed pattern", "A non supported handler .php was called"

Triggered : HoneyPotTrap PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration AttemptToAccessSiteUsingTheTechnologyStack CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 6 incidents in 183 milliseconds
Action : Block, expires on 21 Aug 21 14:34:35 UTC

22.Aug.21 03:57:54 **https://84.195.151.207/admin/config.php**

The firewall flagged the HttpGet request as 6 actions that are of malicious intent where detected.The fact that the user attempted to execute config.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 most significant reasons to reject the request where "A non supported URL was called", "The user is using a port scanner", "A non supported URL was called as the user has no access to https://84.195.151.207/admin/config.php", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToConfigurationAllowed pattern", "A non supported handler .php was called"

Triggered : HoneyPotTrap PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration AttemptToAccessSiteUsingTheTechnologyStack CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 6 incidents in 307 milliseconds
Action : Block, expires on 22 Aug 21 04:04:27 UTC

17:37:38 **https://84.195.151.207/admin/config.php**

The firewall flagged the HttpGet request as 6 actions that are of malicious intent where detected.The fact that the user attempted to execute config.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 most significant reasons to reject the request where "A non supported URL was called", "The user is using a port scanner", "A non supported URL was called as the user has no access to https://84.195.151.207/admin/config.php", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToConfigurationAllowed pattern", "A

non supported handler .php was called"

Triggered : HoneyPotTrap PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration AttemptToAccessSiteUsingTheTechnologyStack CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 6 incidents in 344 milliseconds
Action : Block, expires on 22 Aug 21 17:46:24 UTC

23.Aug.21 07:20:21 **https://84.195.151.207/admin/config.php**

The firewall flagged the HttpGet request as a malicious intent was detected.The fact that the user attempted to execute config.php clearly indicates that your user is attempting to guess his way to an exploit as we do not serve PHP requests.

The most significant reason to reject the request was "A non supported URL was called"

Triggered : PhishyRequest
Decision : escalated thread-level
Action : NoAction, expires on 23 Aug 21 07:25:22 UTC

24.Aug.21 23:42:21 **https://84.195.151.207/admin/config.php**

The firewall flagged the HttpGet request as 6 actions that are of malicious intent where detected.The fact that the user attempted to execute config.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 most significant reasons to reject the request where "A non supported URL was called", "The user is using a port scanner", "A non supported URL was called as the user has no access to https://84.195.151.207/admin/config.php", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToConfigurationAllowed pattern", "A non supported handler .php was called"

Triggered : HoneyPotTrap PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration AttemptToAccessSiteUsingTheTechnologyStack CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 6 incidents in 310 milliseconds
Action : Block, expires on 24 Aug 21 23:49:58 UTC

26.Aug.21 02:49:51 **https://84.195.151.207/admin/config.php**

The firewall flagged the HttpGet request as 6 actions that are of malicious intent where detected.The fact that the user attempted to execute config.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 most significant reasons to reject the request where "A non supported URL was called", "The user is using a port scanner", "A non supported URL was called as the user has no access to https://84.195.151.207/admin/config.php", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToConfigurationAllowed pattern", "A non supported handler .php was called"

Triggered : HoneyPotTrap PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration

11:09:02 **https://84.195.151.207/admin/config.php**

The firewall flagged the HttpGet request as 6 actions that are of malicious intent where detected.The fact that the user attempted to execute config.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 6 exploits and triggered a incident expiring 07/09/2021 11:16:02

Triggered : HoneyPotTrap PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration AttemptToAccessSiteUsingTheTechnologyStack CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 6 incidents in 217 milliseconds
Action : Block, expires on 07 Sep 21 11:16:02 UTC

08.Sep.21 00:27:30 **https://84.195.151.207/admin/config.php**

The firewall flagged the HttpGet request as 6 actions that are of malicious intent where detected.The fact that the user attempted to execute config.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 6 exploits and triggered a incident expiring 08/09/2021 00:34:37

Triggered : HoneyPotTrap PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration AttemptToAccessSiteUsingTheTechnologyStack CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 6 incidents in 223 milliseconds
Action : Block, expires on 08 Sep 21 00:34:37 UTC

13:50:30 **https://84.195.151.207/admin/config.php**

The firewall flagged the HttpGet request as 6 actions that are of malicious intent where detected.The fact that the user attempted to execute config.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 6 exploits and triggered a incident expiring 08/09/2021 13:59:27

Triggered : HoneyPotTrap PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration AttemptToAccessSiteUsingTheTechnologyStack CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 6 incidents in 176 milliseconds
Action : Block, expires on 08 Sep 21 13:59:27 UTC

activity by 144.48.118.133 continues on the next page...

03:13:29 **https://84.195.151.207/admin/config.php**

The firewall flagged the HttpGet request as 6 actions that are of malicious intent where detected.The fact that the user attempted to execute config.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 6 exploits and triggered a incident expiring 09/09/2021 03:20:58

Triggered : HoneyPotTrap PenetrationAttempt MaliciousUser PhishyRequest AttemptOnPluginConfiguration AttemptToAccessSiteUsingTheTechnologyStack CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 6 incidents in 145 milliseconds
Action : Block, expires on 09 Sep 21 03:20:58 UTC

09.Sep.21 *end or reported activity*

GLOSSARY

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

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.
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.