ABUSE REPORT

activity against localhost by

root S.A.

reported from Sat 14 Aug 21 till Thu 02 Sep 21

ABUSE REPORT
ISP Range LU-ROOT-20081021

Incidents recorded between 14/08/2021 12:43:35 and 02/09/2021 11:36:39 UTC

To:
3, op der Poukewiss
7795 Roost - Bissen
Luxembourg
Email abuse@as5577.net

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

Date : Thu 09 September 2021
Reference : LU-ROOT-20081021-226.245-30
Regarding : Malicious activity detected against localhost dating 14/08/2021 12:43:35UTC - 02/09/2021 11:36:39UTC

Dear Sir/ Madam

This report is addressed to you based on activity that has been triggered by 4 IP addresses that are maintained by you.

We refer to the malicious activity that has been reported. In case you only host the hardware and not the hereafter mentioned IP addresses, we ask you kindly to contact us at support@asp-waf.com within 30 days.

In order to avoid further abuse through your hosted IP address(es) please address the issue internally within 5 working days.

To safeguard the domain 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 root S.A.

based on data captured from Mon 09 Aug 21 till Thu 09 Sep 21
for IP range 94.242.192.0 - 94.242.255.255 (16'383 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:

- 23 attempts to steal data by attempting to download confidential data
- 3 attempts to access SQL script
- 2 attempts to URL exploit
- 1 attempt to steal archived cryptocurrency wallets
- 1 attempt to access archived SQL script

Abuse score-card root S.A.

on the 6919 days between Mon 23 Sep 2002 and Thu 02 Sep 2021

IP addresses	:	4	IP addresses with incidents	:	4
HTTP requests served	:	32	HTTP incidents	:	109
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

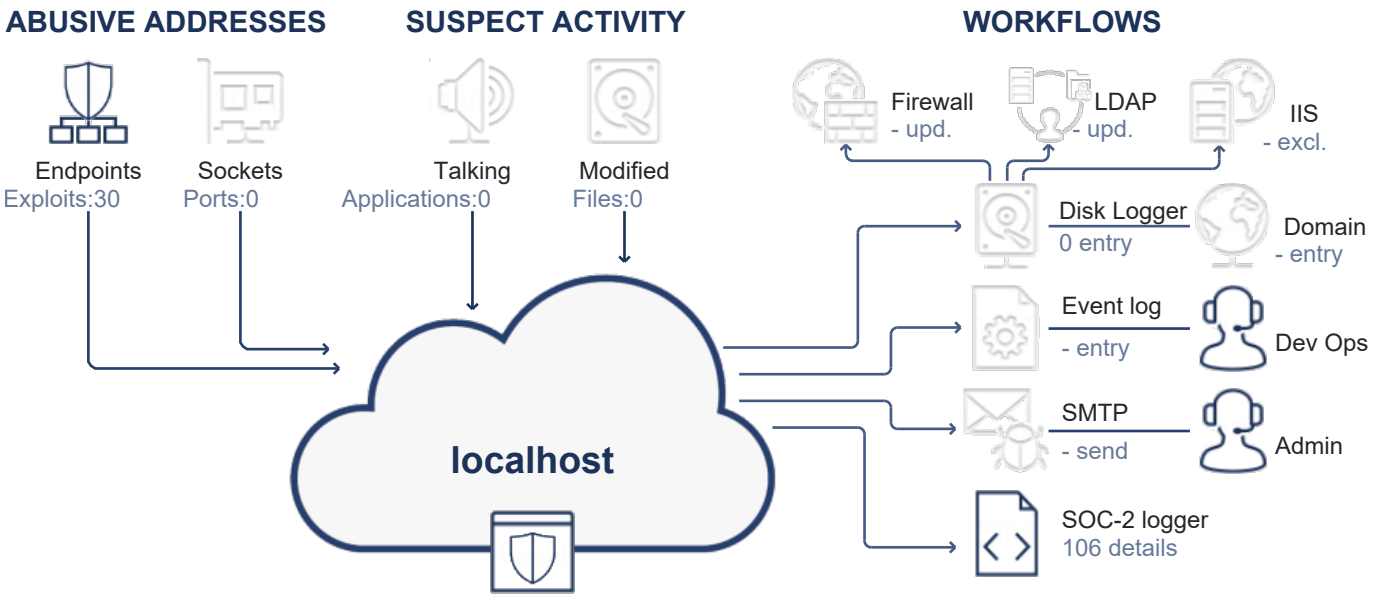
IP Addresses	:	4	IP addresses with incidents	:	2
HTTP requests served	:	20	HTTP incidents	:	10
IP address with port attacks	:	-	Last port attack	:	-
Ports attacked	:	-	Port based incidents	:	-

** 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	30
Human	0
Bot	30
BlackHat	0
Abusive Search Engine	0
Search Engine	0

REQUEST CLASSIFICATION

OK	20
Suspect	0
Redirected	0
Blocked	10

DETECTED ATTACK VECTORS

30 uses URL phishing to probe the system
28 an attempted access protected resources
28 repetitive visits while attempting to probe for exploits
27 continued attempted to probe exploits after being warned
27 repetitive attempts to probe for exploits
22 an attempt to gain access to backups
15 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!

30 HTTP requests to abuse 30 endpoints

During the reporting period, from Sat 14 August 2021 12:43:35 till Thu 02 September 2021 11:36:39 UTC, we detected 7 unique exploits from 4 IP addresses under your management.

In 18 days we detected:
- an attempted access protected resources
- uses URL phishing to probe the system
- continued attempted to probe exploits after being warned
- repetitive visits while attempting to probe for exploits
- repetitive attempts to probe for exploits
- an attempt to gain access to backups
- a Common Vulnerabilities and Exposures (CVE) exploit detected

The next 4 entries document the activities in greater detail.

Malicious HTTP activity from 94.242.204.61

The user on IP address 94.242.204.61 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploits:

- an attempted access protected resources
- uses URL phishing to probe the system
- continued attempted to probe exploits after being warned
- repetitive visits while attempting to probe for exploits
- repetitive attempts to probe for exploits

During the reported time range user of IP address triggered and attempted to use 5 different exploits 4 times.In total we detected 3 exploits with 22 attempts from 14 Aug 21 and 20 Aug 21. We recorded:

- 11 attempts to access resources using malformed URL phishing technique
- 8 attempts to access confidential data
- 3 repeated engagements with the site while being blocked

time-line for 94.242.204.61 starts on the next page...

14.Aug.21 *4 penetration attempts period 14/08/2021 12:43:35 - 20/08/2021 10:21:05, all dates in UTC*

12:43:35 **https://support.asp-waf.com/restore/backup.sql**

The firewall flagged the HttpHead request as 2 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download backup.sql as this clearly was an attempt to gain access to the SQL statements that we are used to execute batch statements on our server.

The most significant reasons to reject the request where "A non supported URL was called", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToBackupsAllowed pattern"

Triggered : PhishyRequest AttemptToAccessSiteBackup
Decision : return Forbidden
Action : Block, expires on 14 Aug 21 12:48:36 UTC

16:44:54 **https://support.asp-waf.com/bak/www.tar**

The firewall flagged the HttpHead request as 2 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download www.tar as this clearly was an attempt to gain access to confidential data like possible stored credentials or proprietary data including that of our clients.

The most significant reasons to reject the request where "A non supported URL was called", "The user provided a URL that looks like a penetration attempt was made using a NoPublicAccessToBackupsAllowed pattern"

Triggered : PhishyRequest AttemptToAccessSiteBackup
Decision : return Forbidden
Action : Block, expires on 14 Aug 21 16:49:55 UTC

20.Aug.21 *09:39:19* **https://asp-waf.com/old/public_html.tar.gz**

The firewall flagged the HttpHead request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download public_html.tar.gz as this clearly was an attempt to gain access to confidential data like possible stored credentials or proprietary data including that of our clients. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The most significant reasons to reject the request where "A non supported URL was called", "A non supported URL was called as the user has no access to https://asp-waf.com/old/public_html.tar.gz", "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 NoPublicAccessToBackupsAllowed pattern"

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup
Decision : return Forbidden after 4 incidents in 135 milliseconds
Action : Block, expires on 20 Aug 21 09:44:20 UTC

10:21:05 **https://asp-waf.com/application.zip**

The firewall flagged the HttpHead request as 3 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download application.zip as this clearly was an attempt to gain access to confidential data like possible stored credentials or proprietary data including that of our clients. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The most significant reasons to reject the request where "A non supported URL was called", "A non supported URL was called as the user has no access to https://asp-waf.com/application.zip", "The user has to many, and to serious

incidents, that have not expired to be allowed to access the application"

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 78 milliseconds
Action : Block, expires on 27 Feb 43 16:31:37 UTC

20.Aug.21 *end or reported activity*

Malicious HTTP activity from 94.242.249.197

The user on IP address 94.242.249.197 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploits:

- an attempted access protected resources
- continued attempted to probe exploits after being warned
- repetitive visits while attempting to probe for exploits
- repetitive attempts to probe for exploits
- uses URL phishing to probe the system
- an attempt to gain access to backups
- a Common Vulnerabilities and Exposures (CVE) exploit detected

During the reported time range user of IP address triggered and attempted to use 7 different exploits 7 times.In total we detected 4 exploits with 57 attempts on 20 Aug 21. We recorded:

- 24 attempts to access resources using malformed URL phishing technique
- 21 attempts to access confidential data
- 11 repeated engagements with the site while being blocked
- 1 TCP Reset-Attack detected

20.Aug.21 *7 penetration attempts period 20/08/2021 09:38:21 - 20/08/2021 10:20:47, all dates in UTC*

09:38:21 **https://asp-waf.com/backup/wallet.zip**

The firewall flagged the HttpHead request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download crypto-currency walletwallet.zip this clearly was an attempt of theft. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The most significant reasons to reject the request where "A non supported URL was called", "A non supported URL was called as the user has no access to https://asp-waf.com/backup/wallet.zip", "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 NoPublicAccessToBackupsAllowed pattern"

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup
Decision : return Forbidden after 4 incidents in 132 milliseconds
Action : Block, expires on 17 Nov 19 15:38:25 UTC
Notes : Known abuser as a previous exploit was triggered

09:39:22 **https://asp-waf.com/back/.bash_history**

The firewall flagged the HttpHead request as 3 actions that are of malicious intent where detected. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The most significant reasons to reject the request where "A non supported URL was called", "A non supported URL was called as the user has no access to https://asp-waf.com/back/.bash_history", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application"

09:40:18 **https://asp-waf.com/backup/backup.zip**

The firewall flagged the HttpHead request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download backup.zip as this clearly was an attempt to gain access to confidential data like possible stored credentials or proprietary data including that of our clients. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The most significant reasons to reject the request where "A non supported URL was called", "A non supported URL was called as the user has no access to https://asp-waf.com/backup/backup.zip", "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 NoPublicAccessToBackupsAllowed pattern"

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup
Decision : return Forbidden after 4 incidents in 135 milliseconds
Action : Block, expires on 17 Nov 19 15:38:25 UTC

09:43:48 **https://asp-waf.com/bak/website.tar.gz**

The firewall flagged the HttpHead request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download website.tar.gz as this clearly was an attempt to gain access to confidential data like possible stored credentials or proprietary data including that of our clients. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The most significant reasons to reject the request where "A non supported URL was called", "A non supported URL was called as the user has no access to https://asp-waf.com/bak/website.tar.gz", "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 NoPublicAccessToBackupsAllowed pattern"

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup
Decision : return Forbidden after 4 incidents in 139 milliseconds
Action : Block, expires on 17 Nov 19 15:38:25 UTC

09:44:13 **https://asp-waf.com/backups/www.sql**

The firewall flagged the HttpHead request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download www.sql as this clearly was an attempt to gain access to the SQL statements that we are used to execute batch statements on our server. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The most significant reasons to reject the request where "A non supported URL was called", "A non supported URL was called as the user has no access to https://asp-waf.com/backups/www.sql", "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 NoPublicAccessToBackupsAllowed pattern"

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup
Decision : return Forbidden after 4 incidents in 173 milliseconds
Action : Block, expires on 17 Nov 19 15:38:25 UTC

activity by 94.242.249.197 continues on the next page...

10:01:27 **https://asp-waf.com/backup/directory.rar**

The firewall flagged the HttpHead request as a malicious intent was detected.We did not appreciate the attempt by your user to download directory.rar as this clearly was an attempt to gain access to confidential data like possible stored credentials or proprietary data including that of our clients.

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

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return NotFound
Action : NoAction, expires on 17 Nov 19 15:38:25 UTC

10:20:47 **https://asp-waf.com/old/website.gz**

The firewall flagged the HttpHead request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download website.gz as this clearly was an attempt to gain access to confidential data like possible stored credentials or proprietary data including that of our clients. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The most significant reasons to reject the request where "A non supported URL was called", "A non supported URL was called as the user has no access to https://asp-waf.com/old/website.gz", "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 NoPublicAccessToBackupsAllowed pattern"

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
AttemptToAccessSiteBackup
CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 273 milliseconds
Action : Block, expires on 06 Jul 63 02:01:49 UTC

20.Aug.21 *end or reported activity*

Malicious HTTP activity from 94.242.231.195

The user on IP address 94.242.231.195 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploits:

- an attempted access protected resources
- continued attempted to probe exploits after being warned
- repetitive visits while attempting to probe for exploits
- repetitive attempts to probe for exploits
- uses URL phishing to probe the system
- an attempt to gain access to backups
- a Common Vulnerabilities and Exposures (CVE) exploit detected

During the reported time range user of IP address triggered and attempted to use 7 different exploits 18 times.

time-line for 94.242.231.195 starts on the next page...

02.Sep.21 *18 penetration attempts period 02/09/2021 09:47:30 - 02/09/2021 10:26:34, all dates in UTC*

09:47:30 **https://asp-waf.com/old/directory.rar**

The firewall flagged the HttpHead request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download directory.rar as this clearly was an attempt to gain access to confidential data like possible stored credentials or proprietary data including that of our clients. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 4 exploits and triggered a incident expiring 02/09/2021 11:37:32

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 124 milliseconds
Action : Block, expires on 02 Sep 21 11:37:32 UTC
Notes : Known abuser as a previous exploit was triggered

09:48:54 **https://asp-waf.com/back/bak.rar**

The firewall flagged the HttpHead request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download bak.rar as this clearly was an attempt to gain access to confidential data like possible stored credentials or proprietary data including that of our clients. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 4 exploits and triggered a incident expiring 02/09/2021 11:37:32

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 100 milliseconds
Action : Block, expires on 02 Sep 21 11:37:32 UTC

09:53:15 **https://asp-waf.com/backup/credentials.txt**

The firewall flagged the HttpHead request as 4 actions that are of malicious intent where detected. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 4 exploits and triggered a incident expiring 02/09/2021 11:37:32

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 110 milliseconds
Action : Block, expires on 02 Sep 21 11:37:32 UTC

activity by 94.242.231.195 continues on the next page...

09:53:21 **https://asp-waf.com/bak/www.zip**

The firewall flagged the HttpHead request as 3 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download www.zip as this clearly was an attempt to gain access to confidential data like possible stored credentials or proprietary data including that of our clients. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 3 exploits and triggered a incident expiring 02/09/2021 11:37:32

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 83 milliseconds
Action : Block, expires on 02 Sep 21 11:37:32 UTC

09:58:45 **https://asp-waf.com/back/asp-waf.com.zip**

The firewall flagged the HttpHead request as 3 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download asp-waf.com.zip as this clearly was an attempt to gain access to confidential data like possible stored credentials or proprietary data including that of our clients. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 3 exploits and triggered a incident expiring 02/09/2021 11:37:32

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 93 milliseconds
Action : Block, expires on 02 Sep 21 11:37:32 UTC

09:59:23 **https://asp-waf.com/restore/website.rar**

The firewall flagged the HttpHead request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download website.rar as this clearly was an attempt to gain access to confidential data like possible stored credentials or proprietary data including that of our clients. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 4 exploits and triggered a incident expiring 02/09/2021 11:37:32

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
AttemptToAccessSiteBackup
CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 146 milliseconds
Action : Block, expires on 02 Sep 21 11:37:32 UTC

10:02:10 **https://asp-waf.com/back/website.tar**

The firewall flagged the HttpHead request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download website.tar as this clearly was an attempt to gain access to confidential data like possible stored credentials or proprietary data including that of our clients. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 4 exploits and triggered a incident expiring 02/09/2021 11:37:32

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
AttemptToAccessSiteBackup
CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 165 milliseconds

10:06:19 **https://asp-waf.com/backups/backup.zip**

The firewall flagged the HttpHead request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download backup.zip as this clearly was an attempt to gain access to confidential data like possible stored credentials or proprietary data including that of our clients. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 4 exploits and triggered a incident expiring 02/09/2021 11:37:32

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 180 milliseconds
Action : Block, expires on 02 Sep 21 11:37:32 UTC

10:07:58 **https://asp-waf.com/backup/asp-waf.com.tar.gz**

The firewall flagged the HttpHead request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download asp-waf.com.tar.gz as this clearly was an attempt to gain access to confidential data like possible stored credentials or proprietary data including that of our clients. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 4 exploits and triggered a incident expiring 02/09/2021 11:37:32

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 183 milliseconds
Action : Block, expires on 02 Sep 21 11:37:32 UTC

10:08:39 **https://asp-waf.com/sql.sql**

The firewall flagged the HttpHead request as 3 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download sql.sql as this clearly was an attempt to gain access to the SQL statements that we are used to execute batch statements on our server. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 3 exploits and triggered a incident expiring 02/09/2021 11:37:32

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 138 milliseconds
Action : Block, expires on 02 Sep 21 11:37:32 UTC

10:09:34 **https://asp-waf.com/backups/website.zip**

The firewall flagged the HttpHead request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download website.zip as this clearly was an attempt to gain access to confidential data like possible stored credentials or proprietary data including that of our clients. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 4 exploits and triggered a incident expiring 02/09/2021 11:37:32

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup

10:12:48 **https://asp-waf.com/restore/public_html.tar**

The firewall flagged the HttpHead request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download public_html.tar as this clearly was an attempt to gain access to confidential data like possible stored credentials or proprietary data including that of our clients. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 4 exploits and triggered a incident expiring 02/09/2021 11:37:32

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 225 milliseconds
Action : Block, expires on 02 Sep 21 11:37:32 UTC

10:19:31 **https://asp-waf.com/restore/directory.tar**

The firewall flagged the HttpHead request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download directory.tar as this clearly was an attempt to gain access to confidential data like possible stored credentials or proprietary data including that of our clients. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 4 exploits and triggered a incident expiring 02/09/2021 11:37:32

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 198 milliseconds
Action : Block, expires on 02 Sep 21 11:37:32 UTC

10:22:10 **https://asp-waf.com/bak/web.zip**

The firewall flagged the HttpHead request as 3 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download web.zip as this clearly was an attempt to gain access to confidential data like possible stored credentials or proprietary data including that of our clients. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 3 exploits and triggered a incident expiring 02/09/2021 11:37:32

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 172 milliseconds
Action : Block, expires on 02 Sep 21 11:37:32 UTC

10:24:09 **https://asp-waf.com/back/directory.gz**

The firewall flagged the HttpHead request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download directory.gz as this clearly was an attempt to gain access to confidential data like possible stored credentials or proprietary data including that of our clients. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 4 exploits and triggered a incident expiring 02/09/2021 11:37:32

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup

10:24:57 **https://asp-waf.com/back/asp-waf.com.rar**

The firewall flagged the HttpHead request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download asp-waf.com.rar as this clearly was an attempt to gain access to confidential data like possible stored credentials or proprietary data including that of our clients. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 4 exploits and triggered a incident expiring 02/09/2021 11:37:32

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 307 milliseconds
Action : Block, expires on 02 Sep 21 11:37:32 UTC

10:25:37 **https://asp-waf.com/bak/website.zip**

The firewall flagged the HttpHead request as 3 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download website.zip as this clearly was an attempt to gain access to confidential data like possible stored credentials or proprietary data including that of our clients. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 3 exploits and triggered a incident expiring 02/09/2021 11:37:32

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 185 milliseconds
Action : Block, expires on 02 Sep 21 11:37:32 UTC

10:26:34 **https://asp-waf.com/old/backup.sql.zip**

The firewall flagged the HttpHead request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download backup.sql.zip as this clearly was an attempt to gain access to archived SQL statements that we might have use to execute batch statements on our server. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 4 exploits and triggered a incident expiring 02/09/2021 11:37:32

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 271 milliseconds
Action : Block, expires on 02 Sep 21 11:37:32 UTC

02.Sep.21 *end or reported activity*

Malicious HTTP activity from 94.242.231.198

The user on IP address 94.242.231.198 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploits:

- an attempted access protected resources
- continued attempted to probe exploits after being warned
- repetitive visits while attempting to probe for exploits
- repetitive attempts to probe for exploits
- uses URL phishing to probe the system
- an attempt to gain access to backups
- a Common Vulnerabilities and Exposures (CVE) exploit detected

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

02.Sep.21 *1 penetration attempt on 02/09/2021 11:36:39, all dates in UTC*

11:36:39 **https://asp-waf.com/backup/website.gz**

The firewall flagged the HttpHead request as 4 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to download website.gz as this clearly was an attempt to gain access to confidential data like possible stored credentials or proprietary data including that of our clients. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The firewall detected 4 exploits and triggered a incident expiring 02/09/2021 11:42:33

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 120 milliseconds
Action : Block, expires on 02 Sep 21 11:42:33 UTC
Notes : Known abuser as a previous exploit was triggered

02.Sep.21 *end or reported activity*

GLOSSARY

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

AttemptToAccessSiteBackup	An attempt to access backups or other confidential data was detected. Such request always indicate that data theft is being attempted
CommonVulnerabilitiesExposuresExploitDetected	An attempt to use a CVE registered exploit was detected. The user is trying to use what is likely dark-web malware to gain access using an attack vector that is a publicly disclosed vulnerability.
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.