ABUSE REPORT

activity against localhost by

Falco Abuse Contact

reported from Sat 14 Aug 21 till Sun 05 Sep 21

ABUSE REPORT
ISP Range Express-Telecity-Amsterdam

Incidents recorded between 14/08/2021 12:37:49 and 05/09/2021 18:27:34 UTC

To:
De schrijnwerker 10,1851PV
Heiloo,Netherlands
Email
jeroen@falco-networks.com

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

Date : Thu 09 September 2021
Reference : Express-Telecity-Amsterdam-226.248-23
Regarding : Malicious activity detected against localhost dating 14/08/2021 12:37:49UTC - 05/09/2021 18:27:34UTC

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 Falco Abuse Contact

based on data captured from Mon 09 Aug 21 till Thu 09 Sep 21
for IP range 85.203.44.0 - 85.203.44.255 (255 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:

- 18 attempts to steal data by attempting to download confidential data
- 2 attempts to exploit CVE (common vulnerability & exposure)
- 1 attempt to URL exploit
- 1 attempt to access SQL script
- 1 attempt to steal archived cryptocurrency wallets

Abuse score-card Falco Abuse Contact

on the 6906 days between Mon 16 Sep 2002 and Sat 14 Aug 2021

IP addresses	:	4	IP addresses with incidents	:	3
HTTP requests served	:	16	HTTP incidents	:	30
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

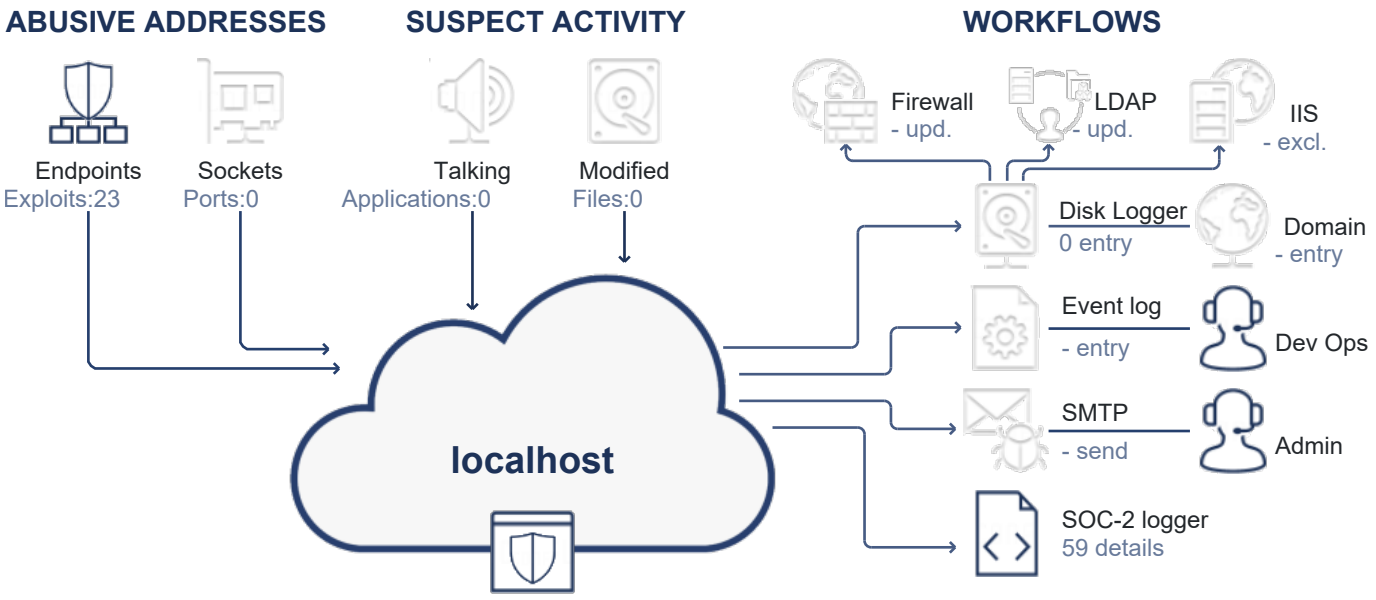
IP Addresses	:	4	IP addresses with incidents	:	2
HTTP requests served	:	14	HTTP incidents	:	9
IP address with port attacks	:	-	Last port attack	:	-
Ports attacked	:	-	Port based incidents	:	-

** 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	23
Human	0
Bot	23
BlackHat	0
Abusive Search Engine	0
Search Engine	0

REQUEST CLASSIFICATION

OK	14
Suspect	0
Redirected	0
Blocked	9

DETECTED ATTACK VECTORS

23	uses URL phishing to probe the system
12	continued attempted to probe exploits after being warned
12	repetitive attempts to probe for exploits
11	an attempt to gain access to backups
9	an attempted access protected resources
9	repetitive visits while attempting to probe for exploits
6	a Common Vulnerabilities and Exposures (CVE) exploit dete
4	repeat requests to probe the system

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!

23 HTTP requests to abuse 23 endpoints

During the reporting period, from Sat 14 August 2021 12:37:49 till Sun 05 September 2021 18:27:34 UTC, we detected 8 unique exploits from 4 IP addresses under your management.

In 22 days we detected:
- uses URL phishing to probe the system
- an attempted access protected resources
- continued attempted to probe exploits after being warned
- repetitive attempts to probe for exploits
- repetitive visits while attempting to probe for exploits
- an attempt to gain access to backups
- a Common Vulnerabilities and Exposures (CVE) exploit detected
- repeat requests to probe the system

The next 4 entries document the activities in greater detail.

Malicious HTTP activity from 85.203.44.7

The user on IP address 85.203.44.7 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploits:

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

During the reported time range user of IP address triggered and attempted to use 4 different exploits 11 times.In total we detected 3 exploits with 34 attempts on 14 Aug 21. We recorded:

- 21 attempts to access resources using malformed URL phishing technique
- 7 attempts to access confidential data
- 6 repeated engagements with the site while being blocked

time-line for 85.203.44.7 starts on the next page...

14.Aug.21 *11 penetration attempts period 14/08/2021 12:37:49 - 14/08/2021 13:41:18, all dates in UTC*

12:37:49 **https://support.asp-waf.com/restore/website.zip**

The firewall flagged the HttpHead request as a malicious intent was 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 most significant reason to reject the request was "A non supported URL was called"

Triggered : PhishyRequest
Decision : return NotFound
Action : NoAction, expires on 30 Jan 96 22:19:13 UTC

12:42:26 **https://support.asp-waf.com/restore/www.rar**

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.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 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 30 Jan 96 22:18:50 UTC

12:43:22 **https://support.asp-waf.com/old/backup.rar**

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 backup.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 most significant reasons to reject the request where "A non supported URL was called", "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 : PhishyRequest AttemptToAccessSiteBackup
Decision : return Forbidden after 3 incidents in 119 milliseconds
Action : Block, expires on 30 Jan 96 22:14:46 UTC

12:44:03 **https://support.asp-waf.com/directory.tar.gz**

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 directory.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", "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 : PhishyRequest AttemptToAccessSiteBackup
Decision : return Forbidden after 3 incidents in 128 milliseconds

12:53:57 **https://support.asp-waf.com/.env**

The firewall flagged the HttpHead request as a malicious intent was detected.We did not appreciate the attempt by your user to access the Laravel framework /.env as this clearly was an attempt to access Laravel to obtain sensitive information (such as externally usable passwords).

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

Triggered : PhishyRequest
Decision : return NotFound
Action : NoAction, expires on 31 Jan 96 02:28:08 UTC

13:01:04 **https://support.asp-waf.com/old/.bash_history**

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

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 UrlFishingSuspected pattern"

Triggered : PageRereshFishing PhishyRequest
Decision : return Forbidden
Action : Block, expires on 31 Jan 96 19:30:49 UTC

13:07:12 **https://support.asp-waf.com/old/bak.zip**

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 bak.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 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 UrlFishingSuspected pattern"

Triggered : PageRereshFishing PhishyRequest
Decision : return Forbidden
Action : Block, expires on 17 Feb 96 08:49:10 UTC

13:13:32 **https://support.asp-waf.com/old/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 20 Jun 97 19:10:17 UTC

13:14:12 **https://support.asp-waf.com/old/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 most significant reasons to reject the request where "A non supported URL was called", "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 UrlFishingSuspected pattern"

Triggered : PageRereshFishing PhishyRequest
Decision : return Forbidden after 3 incidents in 287 milliseconds
Action : Block, expires on 06 Dec 52 20:39:08 UTC

13:19:59 **https://support.asp-waf.com/restore/wallet.zip**

The firewall flagged the HttpHead request as a malicious intent was detected.We did not appreciate the attempt by your user to download crypto-currency walletwallet.zip this clearly was an attempt of theft.

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

Triggered : PhishyRequest
Decision : return NotFound
Action : NoAction, expires on 06 Dec 51 02:24:01 UTC

13:41:18 **https://support.asp-waf.com/restore/public_html.zip**

The firewall flagged the HttpHead request as a malicious intent was detected.We did not appreciate the attempt by your user to download public_html.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 most significant reason to reject the request was "A non supported URL was called"

Triggered : PhishyRequest
Decision : return NotFound
Action : NoAction, expires on 25 Aug 04 17:04:46 UTC

14.Aug.21 *end or reported activity*

Malicious HTTP activity from 85.203.44.45

The user on IP address 85.203.44.45 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploits:

- uses URL phishing to probe the system
- an attempted access protected resources

During the reported time range user of IP address triggered and attempted to use 2 different exploits 3 times.In total we detected 2 exploits with 7 attempts on 14 Aug 21. We recorded:

- 5 attempts to access resources using malformed URL phishing technique
- 2 attempts to access confidential data

14.Aug.21 *3 penetration attempts period 14/08/2021 12:49:17 - 14/08/2021 13:10:05, all dates in UTC*

12:49:17 **https://support.asp-waf.com/website.zip**

The firewall flagged the HttpHead request as a malicious intent was 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 most significant reason to reject the request was "A non supported URL was called"

Triggered : PhishyRequest
Decision : return NotFound
Action : NoAction, expires on 14 Aug 21 12:54:17 UTC

activity by 85.203.44.45 continues on the next page...

12:58:36 **https://support.asp-waf.com/backup/.env**

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 access the Laravel framework /backup/.env as this clearly was an attempt to access Laravel to obtain sensitive information (such as externally usable passwords).

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 13:03:37 UTC

13:10:05 **https://support.asp-waf.com/backups/public_html.gz**

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 public_html.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 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 13:15:06 UTC

14.Aug.21 *end or reported activity*

Malicious HTTP activity from 85.203.44.164

The user on IP address 85.203.44.164 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
- repeat requests to probe the system

During the reported time range user of IP address triggered and attempted to use 8 different exploits 7 times.

05.Sep.21 *7 penetration attempts period 05/09/2021 14:42:24 - 05/09/2021 15:31:23, all dates in UTC*

14:42:24 **https://support.asp-waf.com/backup/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 05/09/2021 15:22:24

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected

14:46:15 **https://support.asp-waf.com/.well-known.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 .well-known.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 05/09/2021 15:42:24

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 81 milliseconds
Action : Block, expires on 05 Sep 21 15:42:24 UTC

14:57:43 **https://support.asp-waf.com/back/index.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 index.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 05/09/2021 15:42:38

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 100 milliseconds
Action : Block, expires on 05 Sep 21 15:42:38 UTC

15:03:30 **https://support.asp-waf.com/public_html.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 public_html.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 05/09/2021 15:42:38

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 102 milliseconds
Action : Block, expires on 05 Sep 21 15:42:38 UTC

15:05:39 **https://support.asp-waf.com/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 05/09/2021 15:42:38

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
AttemptToAccessSiteBackup
CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 153 milliseconds
Action : Block, expires on 05 Sep 21 15:42:38 UTC

activity by 85.203.44.164 continues on the next page...

15:13:55 **https://support.asp-waf.com/bak/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 05/09/2021 15:42:38

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 338 milliseconds
Action : Block, expires on 05 Sep 21 15:42:38 UTC

15:31:23 **https://support.asp-waf.com/old/index.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 index.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 05/09/2021 15:42:38

Triggered : PageRereshFishing PenetrationAttempt MaliciousUser PhishyRequest CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 200 milliseconds
Action : Block, expires on 05 Sep 21 15:42:38 UTC

05.Sep.21 *end or reported activity*

Malicious HTTP activity from 85.203.44.144

The user on IP address 85.203.44.144 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploits:

- an attempted access protected resources
- continued attempted to probe exploits after being warned
- repetitive visits while attempting to probe for exploits
- repetitive attempts to probe for exploits
- uses URL phishing to probe the system
- an attempt to 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 2 times.

05.Sep.21 *2 penetration attempts period 05/09/2021 17:37:13 - 05/09/2021 18:27:34, all dates in UTC*

activity by 85.203.44.144 continues on the next page...

17:37:13 **https://support.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 05/09/2021 17:43:38

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 316 milliseconds
Action : Block, expires on 05 Sep 21 17:43:38 UTC
Notes : Known abuser as a previous exploit was triggered

18:27:34 **https://support.asp-waf.com/restore/www.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 www.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 05/09/2021 18:33:48

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 116 milliseconds
Action : Block, expires on 05 Sep 21 18:33:48 UTC

05.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
PageRereshFishing	Cyber-criminals use phishing URLs to try to obtain sensitive information for malicious use, this could be system files, configuration settings etc. They firewall detects such requests against the website.
PenetrationAttempt	The attacker attempted to gain access to the physical server by using cyber attack against the server to check for exploitable vulnerabilities.
PhishyRequest	The firewall detected access to a resource that was never presented to the user and that doesn't exist, The attacker has been detected to be phishing the system using an URL's in order to use exploitable vulnerabilities that he thinks may be present on the server.