ABUSE REPORT

activity against www.asp-waf.com by

Role object for Panq B.V.

reported from Tue 03 Aug 21 till Wed 25 Aug 21

ABUSE REPORT
ISP Range PANQ-45-86-202-0

Incidents recorded between 03/08/2021 16:42:34 and 25/08/2021 12:27:36 UTC

To:
Luchthavenweg 81.221
5657EA
Eindhoven
NETHERLANDS
Email abuse@panq.nl

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

Date : Thu 23 September 2021
Reference : PANQ-45-86-202-0-2021.215-2021.237 - 41
Regarding : Malicious activity detected against www.asp-waf.com dating 03/08/2021 16:42:34UTC - 25/08/2021 12:27:36UTC

Dear Sir/ Madam

This report is addressed to you based on activity that has been triggered by 6 IP addresses that are maintained by you.

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

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

To safeguard the domain www.asp-waf.com we will activate protective measures.

We expect an update regarding this matter and hereby inform you that we reserve the right to claim any damage made and communicate this report with cybercrime related law enforcement.

Thank you for your cooperation in this matter

Yours sincerely

Walter Verhoeven
R & D

TABLE OF CONTENTS

MANAGEMENT OVERVIEW

Activity against www.asp-waf.com by Role object for Panq B.V.

based on data captured from Sat 31 Jul 21 till Tue 31 Aug 21
for IP range 45.86.202.0 - 45.86.202.255 (255 IP in scope)

Every request against www.asp-waf.com is validated against the firewall's Guard-Modules and if any of the modules detects that then an incident is generated, this report contains detections with the following patterns:

- 28 attempts to steal data by attempting to download confidential data
- 4 attempts to access SQL script
- 3 attempts to URL exploit
- 2 attempts to access the web applications configuration
- 2 attempts to access archived SQL script
- 1 attempt to steal archived cryptocurrency wallets
- 1 attempt to exploit CVE (common vulnerability & exposure)

Abuse score-card Role object for Panq B.V.

on the 18886 days between Thu 01 Jan 1970 and Thu 16 Sep 2021

IP addresses	:	10	IP addresses with incidents	:	9
HTTP requests served	:	70	HTTP incidents	:	186
IP address with port attacks	:	1	Last port attack	:	31/07/2021
Ports attacked	:	1	Port based Incidents	:	1
Talking IP addresses	:	-	Last Talk	:	-
Talking Applications	:	-	Talks Detected	:	-

on the 31 days between Sat 31 Jul 2021 and Tue 31 Aug 2021

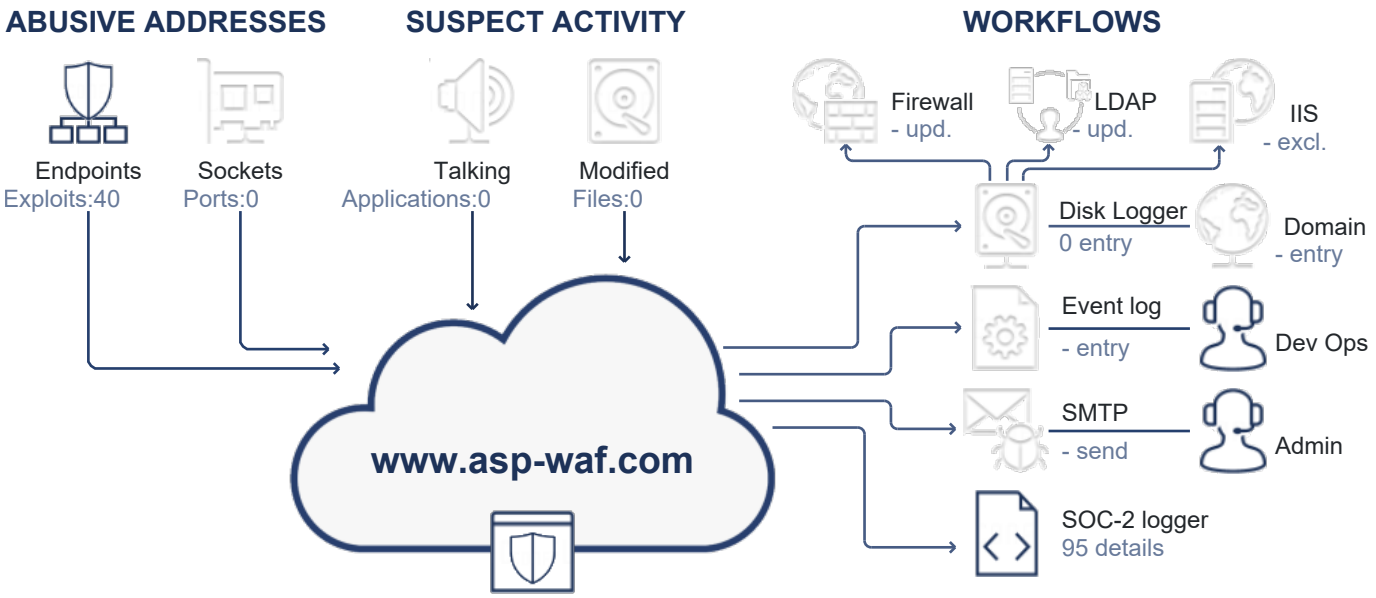
IP Addresses	:	6	IP addresses with incidents	:	6
HTTP requests served	:	10	HTTP incidents	:	31
IP address with port attacks	:	-	Last port attack	:	-
Ports attacked	:	-	Port based incidents	:	-

** 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	41
Human	0
Bot	41
BlackHat	0
Abusive Search Engine	0
Search Engine	0

REQUEST CLASSIFICATION

OK	10
Suspect	0
Redirected	0
Blocked	31

DETECTED ATTACK VECTORS

41	uses URL phishing to probe the system
20	an attempt to gain access to backups
16	an attempted access protected resources
14	continued attempted to probe exploits after being warned
14	repetitive attempts to probe for exploits
13	repetitive visits while attempting to probe for exploits
6	a Common Vulnerabilities and Exposures (CVE) exploit dete
2	accessing a honey-pot trap
2	an attempts to gain access via a manipulated credential
1	repeat requests to probe the system

USED FIREWALL MODULES

The domain www.asp-waf.com is protected using the modules listed in the below table. This abuse report is generated by evaluating the incidents triggered by module Walter.Web.FireWall. The firewall is configured to automatically detect malicious activity and process the incident based on the configuration set by the hosting application.

Modules	*Description*	*Version*
Walter.IO	Detect unauthorized file manipulation in the web application, undoing changes and or taking the site off-line if security is compromised.	2021.9.4.1124
Walter.Net.HoneyPot	Service responsible for detecting penetration attempts against the server. The service records the penetration attempt and issues a system-wide event alarming that there is an attack in progress.	2021.9.4.1124
Walter.Net.LookWhosTalking	Service responsible for recording communication by processes executing on the server with external endpoints.	2021.9.4.1124
Walter.Net.Networking	Resolves WHOIS requests resolving Internet Service Providers responsible for IP addresses as well as reverse DNS queries used for detecting search engines and country level geography discovery.	2021.9.4.1124
Walter.Web.FireWall	Web application firewall with detection service and configurable rule engine.	2021.9.4.1124
Walter.Web.FireWall.DiskLogger	Writes block and release configuration generated by the FireWall to disk and host PowerShell scripts used to configure the external firewall as well as IIS to block or release IP addresses.	2021.9.4.1124
Walter.Web.FireWall.EventLog	Writes incidents to the windows event log for enterprise monitoring and provides SOC-2 end ENISA compliant entries	2021.9.4.1124
Walter.Web.FireWall.Geo.MaxMind	Geo-Location plug-in from MaxMind user for ASN, city and country-level geography discovery using free or paid data from www.maxmind.com	2021.9.4.1124
Walter.Web.FireWall.SMTPLogger	Send incident detections using a mail client to configured mail addresses filtering to the delta of previously unreported activity based on membership profiles	2021.9.4.1124

ABUSE OVERVIEW

The malicious activity documented in the section is proof of activity that is considered outside regular activity that is expected in www.asp-waf.com. We define something outside of regular activity if it falls outside the terms of our services.

Some activity recorded here could is considered a cyber-crime, and next to us reporting the abuse to you, we reserve the right to file a formal complaint with relative authorities. We hope that, by you reviewing this document, you will cooperate with authorities if asked to do so and will take action and prevent any further abuse.

DO NOT CLICK ON HTTP EXPLOITS LINKS
YOUR PDF VIEWER MAY GENERATE THESE HEADERS AS LINKS.
CLICKING THESE LINKS WILL TRIGGER THE FIREWALL!

41 HTTP requests to abuse 40 endpoints

During the reporting period, from Tue 03 August 2021 16:42:34 till Wed 25 August 2021 12:27:36 UTC, we detected 7 unique exploits from 6 IP addresses under your management.

In 21 days we detected:
- an attempted access protected resources
- uses URL phishing to probe the system
- 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

The next 6 entries document the activities in greater detail.

Malicious HTTP activity from 45.86.202.145

The user on IP address 45.86.202.145 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

During the reported time range user of IP address triggered and attempted to use 2 different exploits 2 times.In total we detected 2 exploits with 6 attempts on 03 Aug 21. We recorded:

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

03.Aug.21 *2 penetration attempts period 03/08/2021 16:42:34 - 03/08/2021 16:43:54, all dates in UTC*

16:42:34 **https://support.asp-waf.com/backups/bak.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 bak.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 : PenetrationAttempt PhishyRequest

16:43:54 **https://support.asp-waf.com/bak/directory.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 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 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 : PenetrationAttempt PhishyRequest
Decision : return Forbidden
Action : Block, expires on 03 Aug 21 16:47:48 UTC

03.Aug.21 *end or reported activity*

Malicious HTTP activity from 45.86.202.108

The user on IP address 45.86.202.108 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 6 times.In total we detected 2 exploits with 10 attempts on 08 Aug 21. We recorded:

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

08.Aug.21 *6 penetration attempts period 08/08/2021 01:38:36 - 08/08/2021 02:10:08, all dates in UTC*

01:38:36 **https://asp-waf.com/backups/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 : escalated thread-level
Action : NoAction, expires on 30 Apr 23 23:09:24 UTC

01:39:10 **https://asp-waf.com/bak.gz**

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

Triggered : PhishyRequest
Decision : return Forbidden
Action : Block, expires on 30 Apr 23 23:04:58 UTC

activity by 45.86.202.108 continues on the next page...

01:43:43 **https://asp-waf.com/bak/sql.sql**

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

Triggered : PhishyRequest
Decision : return NotFound
Action : NoAction, expires on 30 Apr 23 23:04:31 UTC

01:46:15 **https://asp-waf.com/old/wallet.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 crypto-currency walletwallet.zip this clearly was an attempt of theft.

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 08 Feb 37 15:02:44 UTC

01:59:03 **https://asp-waf.com/back/www.zip**

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

Triggered : PhishyRequest
Decision : return NotFound
Action : NoAction, expires on 01 May 23 00:25:50 UTC

02:10:08 **https://asp-waf.com/bak/sftp-config.json**

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 sftp-config.json as this clearly was an attempt to access confidential configuration data.

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 NoPublicAccessToApplicationCodeAllowed pattern"

Triggered : PenetrationAttempt PhishyRequest
Decision : return InternalServerError
Action : Block, expires on 12 Dec 96 12:15:03 UTC

08.Aug.21 *end or reported activity*

Malicious HTTP activity from 45.86.202.16

The user on IP address 45.86.202.16 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 6 times.In total we detected 2 exploits with 10 attempts on 14 Aug 21. We recorded:

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

14.Aug.21 *6 penetration attempts period 14/08/2021 14:36:42 - 14/08/2021 15:05:23, all dates in UTC*

14:36:42 **https://support.asp-waf.com/latest.zip**

The firewall flagged the HttpHead request as a malicious intent was detected.We did not appreciate the attempt by your user to download latest.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 14:41:42 UTC

14:53:18 **https://support.asp-waf.com/bak/index.zip**

The firewall flagged the HttpHead request as a malicious intent was 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 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 15:05:27 UTC

14:56:23 **https://support.asp-waf.com/website.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 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 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 15:05:27 UTC

activity by 45.86.202.16 continues on the next page...

14:59:35 **https://support.asp-waf.com/bak/latest.zip**

The firewall flagged the HttpHead request as a malicious intent was detected.We did not appreciate the attempt by your user to download latest.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 15:05:27 UTC

15:00:36 **https://support.asp-waf.com/restore/application.zip**

The firewall flagged the HttpHead request as a malicious intent was 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 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 15:05:27 UTC

15:05:23 **https://support.asp-waf.com/back/www.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 www.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 15:05:27 UTC

14.Aug.21 *end or reported activity*

Malicious HTTP activity from 45.86.202.143

The user on IP address 45.86.202.143 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 attempts to probe for exploits

During the reported time range user of IP address triggered and attempted to use 4 different exploits 14 times.In total we detected 3 exploits with 36 attempts on 14 Aug 21. We recorded:

- 25 attempts to access resources using malformed URL phishing technique
- 10 attempts to access confidential data
- continues engaging with the site while being blocked

14.Aug.21 *14 penetration attempts period 14/08/2021 14:38:06 - 14/08/2021 17:08:16, all dates in UTC*

14:38:06 **https://support.asp-waf.com/backup/asp-waf.com.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 asp-waf.com.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 14:43:06 UTC

14:51:08 **https://support.asp-waf.com/bak/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 14:56:08 UTC

14:56:45 **https://support.asp-waf.com/backups/backup.sql.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 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 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 16:40:45 UTC

activity by 45.86.202.143 continues on the next page...

14:59:47 **https://support.asp-waf.com/backups/.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 NoPublicAccessToBackupsAllowed pattern"

Triggered : PhishyRequest AttemptToAccessSiteBackup
Decision : return Forbidden
Action : Block, expires on 14 Aug 21 16:40:45 UTC

15:06:18 **https://support.asp-waf.com/backups/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 NoPublicAccessToBackupsAllowed pattern"

Triggered : PhishyRequest AttemptToAccessSiteBackup
Decision : return Forbidden
Action : Block, expires on 14 Aug 21 16:40:45 UTC

15:08:00 **https://support.asp-waf.com/back/website.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 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 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 03 Sep 21 05:47:00 UTC

15:14:28 **https://support.asp-waf.com/backup/application.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 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 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 03 Sep 21 05:47:00 UTC

activity by 45.86.202.143 continues on the next page...

15:15:26 **https://support.asp-waf.com/www.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 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", "The user has to many, and to serious incidents, that have not expired to be allowed to access the application"

Triggered : PhishyRequest
Decision : return Forbidden
Action : Block, expires on 14 Aug 21 16:38:44 UTC

15:21:10 **https://support.asp-waf.com/backup/dump.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 dump.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 03 Sep 21 05:47:00 UTC

16:40:26 **https://support.asp-waf.com/bak/application.zip**

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

Triggered : PhishyRequest
Decision : return NotFound
Action : NoAction, expires on 03 Sep 21 05:42:18 UTC

16:43:30 **https://support.asp-waf.com/back/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 03 Sep 21 05:42:18 UTC

activity by 45.86.202.143 continues on the next page...

16:54:56 **https://support.asp-waf.com/backup/mysql.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 mysql.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 03 Sep 21 05:47:00 UTC

17:04:11 **https://support.asp-waf.com/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 03 Sep 21 05:47:00 UTC

17:08:16 **https://support.asp-waf.com/credentials.txt**

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 NoUserAuthenticationExists pattern"

Triggered : HoneyPotTrap ProxyUser PhishyRequest
Decision : return Forbidden
Action : Block, expires on 03 Sep 21 05:47:00 UTC

14.Aug.21 *end or reported activity*

Malicious HTTP activity from 45.86.202.88

The user on IP address 45.86.202.88 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 6 times.In total we detected 4 exploits with 60 attempts on 20 Aug 21. We recorded:

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

20.Aug.21 *6 penetration attempts period 20/08/2021 09:38:41 - 20/08/2021 10:28:37, all dates in UTC*

09:38:41 **https://asp-waf.com/back/sftp-config.json**

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 access sftp-config.json as this clearly was an attempt to access confidential configuration data. The firewall updated the block recommendation as previous penetration attempts were serious enough for the firewall to generate a block recommendation.

The 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/sftp-config.json", "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 NoPublicAccessToApplicationCodeAllowed pattern"

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 4 incidents in 121 milliseconds
Action : Block, expires on 01 Jan 78 00:00:00 UTC
Notes : Known abuser as a previous exploit was triggered

09:41:41 **https://asp-waf.com/bak/wallet.dat**

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 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/wallet.dat", "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 NoUserAuthenticationExists pattern"

Triggered : HoneyPotTrap ProxyUser PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 4 incidents in 118 milliseconds
Action : Block, expires on 01 Jan 78 00:00:00 UTC

activity by 45.86.202.88 continues on the next page...

09:45:23 **https://asp-waf.com/backups/asp-waf.com.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.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/backups/asp-waf.com.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 131 milliseconds
Action : Block, expires on 01 Jan 78 00:00:00 UTC

09:45:30 **https://asp-waf.com/backup/backup.sql.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 backup.sql.gz 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 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.sql.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 144 milliseconds
Action : Block, expires on 01 Jan 78 00:00:00 UTC

09:47:35 **https://asp-waf.com/bak/backup.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 backup.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 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/backup.tar", "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 167 milliseconds
Action : Block, expires on 01 Jan 78 00:00:00 UTC

activity by 45.86.202.88 continues on the next page...

10:28:37 **https://asp-waf.com/asp-waf.com.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.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/asp-waf.com.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 117 milliseconds
Action : Block, expires on 01 Jan 78 00:00:00 UTC

20.Aug.21 *end or reported activity*

Malicious HTTP activity from 45.86.202.140

The user on IP address 45.86.202.140 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 62 attempts on 25 Aug 21. We recorded:

- 26 attempts to access resources using malformed URL phishing technique
- 19 attempts to access confidential data
- 12 repeated engagements with the site while being blocked
- 5 TCP Reset-Attacks detected

25.Aug.21 *7 penetration attempts period 25/08/2021 11:46:50 - 25/08/2021 12:27:36, all dates in UTC*

11:46:50 **https://support.asp-waf.com/backups/.env**

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 access the Laravel framework /backups/.env as this clearly was an attempt to access Laravel to obtain sensitive information (such as externally usable passwords). 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://support.asp-waf.com/backups/.env", "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"

11:48:29 **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 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://support.asp-waf.com/back/index.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 108 milliseconds
Action : Block, expires on 25 Aug 21 13:16:50 UTC

12:02:36 **https://support.asp-waf.com/bak/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 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://support.asp-waf.com/bak/public_html.tar", "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 164 milliseconds
Action : Block, expires on 25 Aug 21 13:26:50 UTC

12:02:46 **https://support.asp-waf.com/bak/.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 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://support.asp-waf.com/bak/.well-known.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 136 milliseconds
Action : Block, expires on 25 Aug 21 13:41:50 UTC

activity by 45.86.202.140 continues on the next page...

12:15:56 **https://support.asp-waf.com/back/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 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://support.asp-waf.com/back/public_html.tar", "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 418 milliseconds
Action : Block, expires on 25 Aug 21 13:56:50 UTC

12:23:29 **https://support.asp-waf.com/restore/directory.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 directory.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://support.asp-waf.com/restore/directory.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 CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 138 milliseconds
Action : Block, expires on 25 Aug 21 12:26:22 UTC

12:27:36 **https://support.asp-waf.com/backups/public_html.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 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 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://support.asp-waf.com/backups/public_html.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 CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 413 milliseconds

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.
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
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.
ProxyUser	ProxyLogon is the formally generic name for a vulnerability on Server that allows an attacker bypassing the authentication and impersonating as the administrator.