ABUSE REPORT

activity against localhost by

i3D.net

reported from Sat 14 Aug 21 till Sun 05 Sep 21

ABUSE REPORT
ISP Range INTERACTIVE3D

Incidents recorded between 14/08/2021 11:44:06 and 05/09/2021 20:47:07 UTC

To:
i3D.net - Interactive 3D
Rivium 1e Straat 1
2909LE Capelle aan den IJssel
The Netherlands
Email abuse@i3d.net

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

Date : Thu 09 September 2021
Reference : INTERACTIVE3D-226.248-18
Regarding : Malicious activity detected against localhost dating 14/08/2021 11:44:06UTC - 05/09/2021 20:47:07UTC

Dear Sir/ Madam

This report is addressed to you based on activity that has been triggered by 7 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 i3D.net

based on data captured from Mon 09 Aug 21 till Thu 09 Sep 21
for IP range 31.204.150.0 - 31.204.151.255 (511 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:

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

Abuse score-card i3D.net

on the 4821 days between Tue 24 Jun 2008 and Sun 05 Sep 2021

IP addresses	:	7	IP addresses with incidents	:	7
HTTP requests served	:	21	HTTP incidents	:	68
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

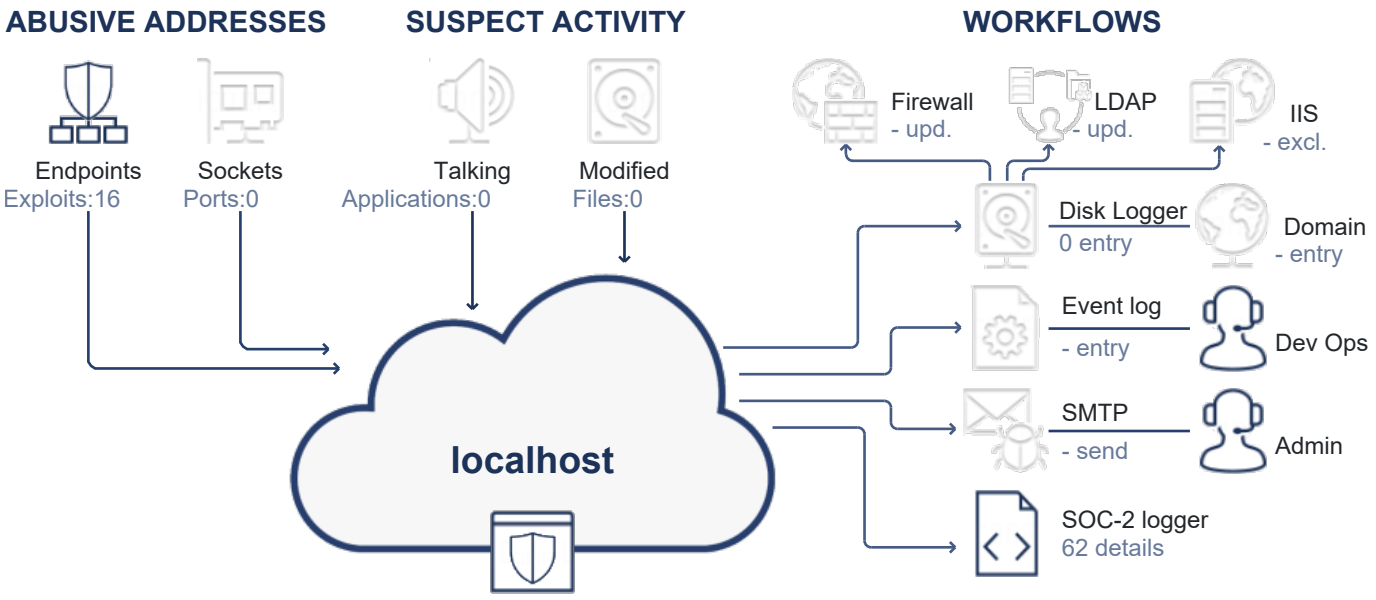
IP Addresses	:	7	IP addresses with incidents	:	5
HTTP requests served	:	5	HTTP incidents	:	13
IP address with port attacks	:	-	Last port attack	:	-
Ports attacked	:	-	Port based incidents	:	-

** 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	18
Human	0
Bot	18
BlackHat	0
Abusive Search Engine	0
Search Engine	0

REQUEST CLASSIFICATION

OK	5
Suspect	0
Redirected	0
Blocked	13

DETECTED ATTACK VECTORS

18	uses URL phishing to probe the system
14	an attempted access protected resources
14	continued attempted to probe exploits after being warned
14	repetitive visits while attempting to probe for exploits
14	repetitive attempts to probe for exploits
12	an attempt to gain access to backups
8	a Common Vulnerabilities and Exposures (CVE) exploit dete
3	accessing a honey-pot trap
3	an attempts to gain access via a manipulated credential
1	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!

18 HTTP requests to abuse 16 endpoints

During the reporting period, from Sat 14 August 2021 11:44:06 till Sun 05 September 2021 20:47:07 UTC, we detected 9 unique exploits from 7 IP addresses under your management.

In 22 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
- accessing a honey-pot trap
- an attempts to gain access via a manipulated credential

The next 7 entries document the activities in greater detail.

Malicious HTTP activity from 31.204.150.237

The user on IP address 31.204.150.237 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 once.In total we detected 2 exploits with 3 attempts on 14 Aug 21. We recorded:

- 2 attempts to access resources using malformed URL phishing technique
- 1 attempt to access confidential data was detected

14.Aug.21 *1 penetration attempt on 14/08/2021 11:44:06, all dates in UTC*

activity by 31.204.150.237 continues on the next page...

11:44:06 **https://support.asp-waf.com/backup/wallet.dat**

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 11:49:06 UTC

14.Aug.21 *end or reported activity*

Malicious HTTP activity from 31.204.150.250

The user on IP address 31.204.150.250 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 5 attempts on 14 Aug 21. We recorded:

- 4 attempts to access resources using malformed URL phishing technique
- 1 attempt to access confidential data was detected

14.Aug.21 *3 penetration attempts period 14/08/2021 17:49:55 - 14/08/2021 18:02:04, all dates in UTC*

17:49:55 **https://support.asp-waf.com/bak/.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 /bak/.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 14 Aug 21 17:54:55 UTC

17:55:30 **https://support.asp-waf.com/backup/.well-known.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 .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 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 17:56:00 UTC

activity by 31.204.150.250 continues on the next page...

18:02:04 **https://support.asp-waf.com/restore/asp-waf.com.sql**

The firewall flagged the HttpHead request as a malicious intent was detected.We did not appreciate the attempt by your user to download asp-waf.com.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 14 Aug 21 18:07:05 UTC

14.Aug.21 *end or reported activity*

Malicious HTTP activity from 31.204.151.8

The user on IP address 31.204.151.8 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 70 attempts on 20 Aug 21. We recorded:

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

20.Aug.21 *7 penetration attempts period 20/08/2021 09:36:55 - 20/08/2021 10:22:25, all dates in UTC*

09:36:55 **https://asp-waf.com/old/www.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 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 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/www.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 UrlFishingSuspected pattern"

Triggered : PageRereshFishing PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 4 incidents in 313 milliseconds
Action : Block, expires on 20 Aug 21 09:41:56 UTC
Notes : Known abuser as a previous exploit was triggered

activity by 31.204.151.8 continues on the next page...

09:43:39 **https://asp-waf.com/bak/www.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 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 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/www.rar", "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 111 milliseconds
Action : Block, expires on 14 Feb 58 11:55:08 UTC

09:46:39 **https://asp-waf.com/bak/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 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.sql.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 111 milliseconds
Action : Block, expires on 14 Feb 58 11:55:08 UTC

09:48:49 **https://asp-waf.com/backup/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 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/website.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 182 milliseconds
Action : Block, expires on 14 Feb 58 11:55:08 UTC

activity by 31.204.151.8 continues on the next page...

09:51:12 **https://asp-waf.com/restore/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/restore/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 165 milliseconds
Action : Block, expires on 14 Feb 58 11:55:08 UTC

09:52:19 **https://asp-waf.com/old/bak.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 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 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/bak.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 194 milliseconds
Action : Block, expires on 14 Feb 58 11:55:08 UTC

10:22:25 **https://asp-waf.com/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 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.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 CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 116 milliseconds
Action : Block, expires on 03 Oct 01 22:20:11 UTC

20.Aug.21 *end or reported activity*

Malicious HTTP activity from 31.204.151.56

The user on IP address 31.204.151.56 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.In total we detected 4 exploits with 20 attempts on 25 Aug 21. We recorded:

- 8 attempts to access resources using malformed URL phishing technique
- 6 attempts to access confidential data
- 4 repeated engagements with the site while being blocked
- 2 TCP Reset-Attacks detected

25.Aug.21 *2 penetration attempts period 25/08/2021 07:52:52 - 25/08/2021 10:57:58, all dates in UTC*

07:52:52 **https://support.asp-waf.com/restore/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 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/backup.sql.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 115 milliseconds
Action : Block, expires on 25 Aug 21 08:01:37 UTC
Notes : Known abuser as a previous exploit was triggered

10:57:58 **https://support.asp-waf.com/backup/www.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.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://support.asp-waf.com/backup/www.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

Malicious HTTP activity from 31.204.150.51

The user on IP address 31.204.150.51 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
- accessing a honey-pot trap
- an attempts to gain access via a manipulated credential

During the reported time range user of IP address triggered and attempted to use 9 different exploits 3 times.In total we detected 4 exploits with 20 attempts from 25 Aug 21 and 05 Sep 21. We recorded:

- 8 attempts to access resources using malformed URL phishing technique
- 6 attempts to access confidential data
- 4 repeated engagements with the site while being blocked
- 2 TCP Reset-Attacks detected

25.Aug.21 *3 penetration attempts period 25/08/2021 09:42:54 - 05/09/2021 15:58:53, all dates in UTC*

09:42:54 **https://support.asp-waf.com/backup/dump.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 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 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/backup/dump.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 CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 277 milliseconds
Action : Block, expires on 25 Aug 21 09:51:58 UTC
Notes : Known abuser as a previous exploit was triggered

10:31:02 **https://support.asp-waf.com/backups/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 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/website.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"

15:58:53 **https://support.asp-waf.com/old/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 05/09/2021 16:07:44

Triggered : HoneyPotTrap ProxyUser PenetrationAttempt MaliciousUser PhishyRequest CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 140 milliseconds
Action : Block, expires on 05 Sep 21 16:07:44 UTC

05.Sep.21 *end or reported activity*

Malicious HTTP activity from 31.204.150.64

The user on IP address 31.204.150.64 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.

05.Sep.21 *1 penetration attempt on 05/09/2021 14:59:33, all dates in UTC*

14:59:33 **https://support.asp-waf.com/backup/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 05/09/2021 15:07:31

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteBackup CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 300 milliseconds
Action : Block, expires on 05 Sep 21 15:07:31 UTC
Notes : Known abuser as a previous exploit was triggered

05.Sep.21 *end or reported activity*

Malicious HTTP activity from 31.204.151.0

The user on IP address 31.204.151.0 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploits:

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

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

05.Sep.21 *1 penetration attempt on 05/09/2021 20:47:07, all dates in UTC*

20:47:07 **https://support.asp-waf.com/restore/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 firewall detected 4 exploits and triggered a incident expiring 05/09/2021 20:54:16

Triggered : HoneyPotTrap ProxyUser PenetrationAttempt MaliciousUser PhishyRequest CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 127 milliseconds
Action : Block, expires on 05 Sep 21 20:54:16 UTC
Notes : Known abuser as 6 exploits where triggered

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.
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.