ABUSE REPORT

activity against www.asp-waf.com by

Hurricane Electric LLC

reported from Thu 02 Sep 21 till Mon 20 Sep 21

ABUSE REPORT
ISP Range HURRICANE-4

Incidents recorded between 02/09/2021 02:54:15 and 20/09/2021 01:03:36 UTC

To:
760 Mission Court
Fremont
CA
94539
United States
Email abuse@he.net

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

Date : Wed 22 September 2021
Reference : HURRICANE-4-2021.245-2021.263 - 16
Regarding : Malicious activity detected against www.asp-waf.com dating 02/09/2021 02:54:15UTC - 20/09/2021 01:03:36UTC

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 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

topic	*page*
Management Overview	4
Used firewall modules	6
Malicious socket and HTTP activity from 64.62.197.182	8
Malicious socket activity on port 3389 from 64.62.197.2	9
Malicious socket and HTTP activity from 64.62.197.62	9
Malicious socket activity on port 3389 from 64.62.197.32	11
Malicious HTTP activity from 64.62.197.152	11
Malicious HTTP activity from 64.62.197.92	12
Malicious HTTP activity from 64.62.197.212	13
Glossary	14

MANAGEMENT OVERVIEW

Activity against www.asp-waf.com by Hurricane Electric LLC

based on data captured from Tue 31 Aug 21 till Mon 20 Sep 21
for IP range 64.62.128.0 - 64.62.255.255 (32'767 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:

12 attempts to URL exploit

4 attempts to exploit port 3389 - remote desktop protocol (rdp)

Abuse score-card Hurricane Electric LLC

on the 18892 days between Thu 01 Jan 1970 and Wed 22 Sep 2021

IP addresses	:	7	IP addresses with incidents	:	7
HTTP requests served	:	29	HTTP incidents	:	68
IP address with port attacks	:	7	Last port attack	:	16/09/2021
Ports attacked	:	1	Port based Incidents	:	36
Talking IP addresses	:	-	Last Talk	:	-
Talking Applications	:	-	Talks Detected	:	-

on the 20 days between Tue 31 Aug 2021 and Mon 20 Sep 2021

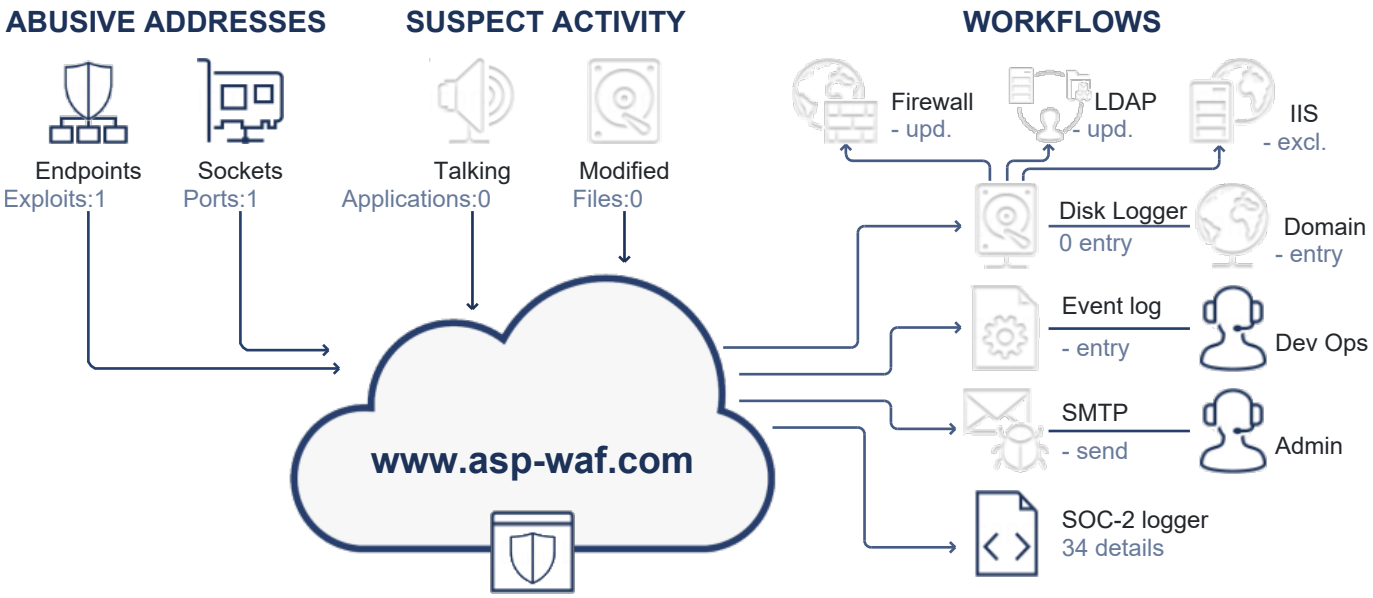
IP Addresses	:	7	IP addresses with incidents	:	4
HTTP requests served	:	13	HTTP incidents	:	-
IP address with port attacks	:	4	Last port attack	:	16/09/2021
Ports attacked	:	4	Port based incidents	:	4

** 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	17
Human	0
Bot	13
BlackHat	4
Abusive Search Engine	0
Search Engine	0

REQUEST CLASSIFICATION

OK	13
Suspect	0
Redirected	0
Blocked	0
Socket	4

DETECTED ATTACK VECTORS

12	accessing a honey-pot trap
12	continued attempted to probe exploits after being warned
12	an attempt to use developer tools to gain access
12	repetitive attempts to probe for exploits
6	repetitive visits while attempting to probe for exploits
4	Exploits against Port 3389 - Remote Desktop Protocol (RDI

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!

4 attempts against 1 socket and 12 HTTP requests to abuse 1 endpoint

During the reporting period, from Thu 02 September 2021 02:54:15 till Mon 20 September 2021 01:03:36 UTC, we detected 5 unique exploits from 7 IP addresses under your management.

In 17 days we detected:
- accessing a honey-pot trap
- continued attempted to probe exploits after being warned
- an attempted access systems while not authorized
- an attempt to use developer tools to gain access
- repetitive attempts to probe for exploits

We noted that all 4 IP addresses are attacking our system using the same port. Is this a coincidence or a distributed attack? We would appreciate an update concerning this matter.

We noted that there is an overlap between the 4 IP addresses that are attacking based on the same 1 ports. Is this a coincidence or a distributed attack? We would appreciate an update concerning this matter.

We also noted that all 5 IP addresses are attacking our system using the same URL. Is this a coincidence or a distributed attack? We would appreciate an update in regards to this matter.

We also noted that there is an overlap between the 4 IP addresses that are attacking based on the same 1 ports. Is this a coincidence or a distributed attack? We would appreciate an update in regards to this matter.

The next 7 entries document the activities in greater detail.

Malicious socket and HTTP activity from 64.62.197.182

The user on IP address 64.62.197.182 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
- continued attempted to probe exploits after being warned
- an attempted access systems while not authorized
- an attempt to use developer tools to gain access

During the reported time range user of IP address triggered and attempted to use 4 different exploits 3 times.

08.Sep.21 *3 penetration attempts period 08/09/2021 14:36:43 - 14/09/2021 03:40:48, all dates in UTC*

14:36:43

Port 3389 - Remote Desktop Protocol (RDP)

The firewall detected a attempt by an attacker to takes advantage of vulnerabilities in the

Remote Desktop Protocol to be able to use a graphical interface to connect to the server.

We rejected any data send by the attacker and stopped the attack before determining the exact exploit used.

Triggered : ProxyUser PenetrationAttempt
Decision :
Action : Continued recording activity

10.Sep.21 *00:45:09*

https://84.195.151.207/

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

The firewall detected 3 exploits and triggered a incident expiring 10/09/2021 00:54:40

Triggered : HoneyPotTrap MaliciousUser
Decision : return Forbidden after 3 incidents in 277 milliseconds
Action : Block, expires on 10 Sep 21 00:54:40 UTC

14.Sep.21 *03:40:48*

https://84.195.151.207/

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

The firewall detected 3 exploits and triggered a incident expiring 14/09/2021 03:45:49

Triggered : HoneyPotTrap MaliciousUser
Decision : return Forbidden after 3 incidents in 369 milliseconds
Action : Block, expires on 14 Sep 21 03:45:49 UTC

14.Sep.21 *end or reported activity*

Malicious socket activity on port 3389 from 64.62.197.2

The user on IP address 64.62.197.2 tried to exploit web based vulnerabilities.
During the reported time range user of IP address triggered an attempt to use and abuse a single exploit one time.

09.Sep.21 *1 penetration attempt on 09/09/2021 17:47:05, all dates in UTC*

17:47:05 **Port 3389 - Remote Desktop Protocol (RDP)**

The firewall detected a attempt by an attacker to takes advantage of vulnerabilities in the

Remote Desktop Protocol to be able to use a graphical interface to connect to the server.

We rejected any data send by the attacker and stopped the attack before determining the exact exploit used.

Triggered : ProxyUser PenetrationAttempt
Decision :
Action : Continued recording activity

09.Sep.21 *end or reported activity*

Malicious socket and HTTP activity from 64.62.197.62

The user on IP address 64.62.197.62 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
- continued attempted to probe exploits after being warned
- an attempt to use developer tools to gain access
- repetitive attempts to probe for exploits
- an attempted access systems while not authorized

During the reported time range user of IP address triggered and attempted to use 5 different exploits 5 times.

02.Sep.21 *5 penetration attempts period 02/09/2021 02:54:15 - 20/09/2021 01:03:36, all dates in UTC*

02:54:15 **https://84.195.151.207/**

The firewall flagged the HttpGet request as 2 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 2 exploits and triggered a incident expiring 02/09/2021 03:02:44

Triggered : HoneyPotTrap
Decision : return Forbidden
Action : Block, expires on 02 Sep 21 03:02:44 UTC

08.Sep.21 *02:43:16* **https://84.195.151.207/**

The firewall flagged the HttpGet request as 2 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 2 exploits and triggered a incident expiring 08/09/2021 02:52:46

Triggered : HoneyPotTrap
Decision : return Forbidden
Action : Block, expires on 08 Sep 21 02:52:46 UTC

11:02:02 **Port 3389 - Remote Desktop Protocol (RDP)**

The firewall detected a attempt by an attacker to takes advantage of vulnerabilities in the

Remote Desktop Protocol to be able to use a graphical interface to connect to the server.

We rejected any data send by the attacker and stopped the attack before determining the exact exploit used.

Triggered : ProxyUser PenetrationAttempt
Decision :
Action : Continued recording activity

20.Sep.21 00:57:08 **https://84.195.151.207/**

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

The firewall detected 3 exploits and triggered a incident expiring 20/09/2021 01:04:02

Triggered : HoneyPotTrap MaliciousUser
Decision : return Forbidden after 3 incidents in 178 milliseconds
Action : Block, expires on 20 Sep 21 01:04:02 UTC

01:03:36 **https://84.195.151.207/**

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

The firewall detected 3 exploits and triggered a incident expiring 20/09/2021 01:04:02

Triggered : HoneyPotTrap MaliciousUser
Decision : return Forbidden after 3 incidents in 185 milliseconds
Action : Block, expires on 20 Sep 21 01:04:02 UTC

20.Sep.21 *end or reported activity*

Malicious socket activity on port 3389 from 64.62.197.32

The user on IP address 64.62.197.32 tried to exploit web based vulnerabilities.
During the reported time range user of IP address triggered an attempt to use and abuse a single exploit one time.

16.Sep.21 *1 penetration attempt on 16/09/2021 09:00:48, all dates in UTC*

09:00:48 **Port 3389 - Remote Desktop Protocol (RDP)**

The firewall detected a attempt by an attacker to takes advantage of vulnerabilities in the

Remote Desktop Protocol to be able to use a graphical interface to connect to the server.

We rejected any data send by the attacker and stopped the attack before determining the exact exploit used.

Triggered : ProxyUser PenetrationAttempt
Decision :
Action : Continued recording activity

16.Sep.21 *end or reported activity*

Malicious HTTP activity from 64.62.197.152

The user on IP address 64.62.197.152 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
- continued attempted to probe exploits after being warned
- an attempt to use developer tools to gain access
- repetitive attempts to probe for exploits
- an attempted access systems while not authorized

During the reported time range user of IP address triggered and attempted to use 5 different exploits 4 times.

07.Sep.21 *4 penetration attempts period 07/09/2021 00:59:43 - 19/09/2021 04:28:43, all dates in UTC*

00:59:43 **https://84.195.151.207/**

The firewall flagged the HttpGet request as 2 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 2 exploits and triggered a incident expiring 07/09/2021 01:08:29

Triggered : HoneyPotTrap
Decision : return Forbidden
Action : Block, expires on 07 Sep 21 01:08:29 UTC

18.Sep.21 *04:33:56* **https://84.195.151.207/**

The firewall flagged the HttpGet request as 2 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 2 exploits and triggered a incident expiring 18/09/2021 04:42:36

Triggered : HoneyPotTrap
Decision : return Forbidden
Action : Block, expires on 18 Sep 21 04:42:36 UTC

04:21:25 **https://84.195.151.207/**

The firewall flagged the HttpGet request as 2 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 2 exploits and triggered a incident expiring 19/09/2021 04:29:21

Triggered : HoneyPotTrap
Decision : return Forbidden
Action : Block, expires on 19 Sep 21 04:29:21 UTC

04:28:43 **https://84.195.151.207/**

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

The firewall detected 3 exploits and triggered a incident expiring 19/09/2021 04:29:21

Triggered : HoneyPotTrap MaliciousUser
Decision : return Forbidden after 3 incidents in 395 milliseconds
Action : Block, expires on 19 Sep 21 04:29:21 UTC

19.Sep.21 *end or reported activity*

Malicious HTTP activity from 64.62.197.92

The user on IP address 64.62.197.92 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
- continued attempted to probe exploits after being warned
- an attempted access systems while not authorized
- an attempt to use developer tools to gain access

During the reported time range user of IP address triggered and attempted to use 4 different exploits once.

13.Sep.21 *1 penetration attempt on 13/09/2021 02:44:12, all dates in UTC*

02:44:12 **https://84.195.151.207/**

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

The firewall detected 3 exploits and triggered a incident expiring 13/09/2021 02:49:33

Triggered : HoneyPotTrap MaliciousUser
Decision : return Forbidden after 3 incidents in 245 milliseconds
Action : Block, expires on 13 Sep 21 02:49:33 UTC
Notes : Known abuser as 4 exploits where triggered

13.Sep.21 *end or reported activity*

Malicious HTTP activity from 64.62.197.212

The user on IP address 64.62.197.212 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
- continued attempted to probe exploits after being warned
- an attempt to use developer tools to gain access
- repetitive attempts to probe for exploits

During the reported time range user of IP address triggered and attempted to use 4 different exploits once.

17.Sep.21 *1 penetration attempt on 17/09/2021 04:18:12, all dates in UTC*

04:18:12 **https://84.195.151.207/**

The firewall flagged the HttpGet request as 2 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 2 exploits and triggered a incident expiring 17/09/2021 04:25:31

Triggered : HoneyPotTrap
Decision : return Forbidden
Action : Block, expires on 17 Sep 21 04:25:31 UTC

17.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.

HoneyPotTrap	The firewall, or the site hosting the firewall, generated a trap for hackers hidden for normal users, the firewall detected that the system tried to access the trap.
MaliciousUser	A user is considered to be malicious having been previously rejected, after having been rejected the user still tries to access sensitive data and is therefore again rejected
PenetrationAttempt	The attacker attempted to gain access to the physical server by using cyber attack against the server to check for exploitable vulnerabilities.
ProxyUser	ProxyLogon is the formally generic name for a vulnerability on Server that allows an attacker bypassing the authentication and impersonating as the administrator.