ABUSE REPORT

activity against www.asp-waf.com by

HOST1PLUS hosting services. Brazil.

reported from Sun 29 Aug 21 till Wed 22 Sep 21

ABUSE REPORT
ISP Range N/A

Incidents recorded between 29/08/2021 12:35:17 and 22/09/2021 20:31:04 UTC

To:

Email abuse@heficed.com

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 : N/A-2021.241-2021.265 - 22
Regarding : Malicious activity detected against www.asp-waf.com dating 29/08/2021 12:35:17UTC - 22/09/2021 20:31:04UTC

Dear Sir/ Madam

This report is addressed to you based on activity that has been triggered by 9 IP addresses that are maintained by you.
We would like to report activity related to:

- Malicious socket activity on port 3389 from 181.214.206.119
- Malicious socket activity on port 3389 from 181.214.206.150
- Malicious socket activity on port 3389 from 181.214.206.146
- Malicious socket activity on port 3389 from 181.214.206.66
- Malicious socket activity on port 3389 from 181.214.206.226
- Malicious socket activity on port 3389 from 181.214.206.124
- Malicious socket activity on port 3389 from 181.214.206.115
- Malicious Multi- socket activity from 181.214.206.228
- Malicious HTTP activity from 181.214.206.238

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
Walter Verhoeven
R & D

TABLE OF CONTENTS

MANAGEMENT OVERVIEW

Activity against www.asp-waf.com by HOST1PLUS hosting services. Brazil.

based on data captured from Mon 23 Aug 21 till Thu 23 Sep 21
for IP range 181.214.0.1 - 181.214.255.254 (65'533 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:

26 attempts to exploit port 3389 - remote desktop protocol (rdp)
1 attempt to URL exploit

Abuse score-card HOST1PLUS hosting services. Brazil.

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

IP addresses	:	38	IP addresses with incidents	:	10
HTTP requests served	:	3	HTTP incidents	:	28
IP address with port attacks	:	35	Last port attack	:	22/09/2021
Ports attacked	:	1	Port based Incidents	:	74
Talking IP addresses	:	-	Last Talk	:	-
Talking Applications	:	-	Talks Detected	:	-

on the 31 days between Mon 23 Aug 2021 and Thu 23 Sep 2021

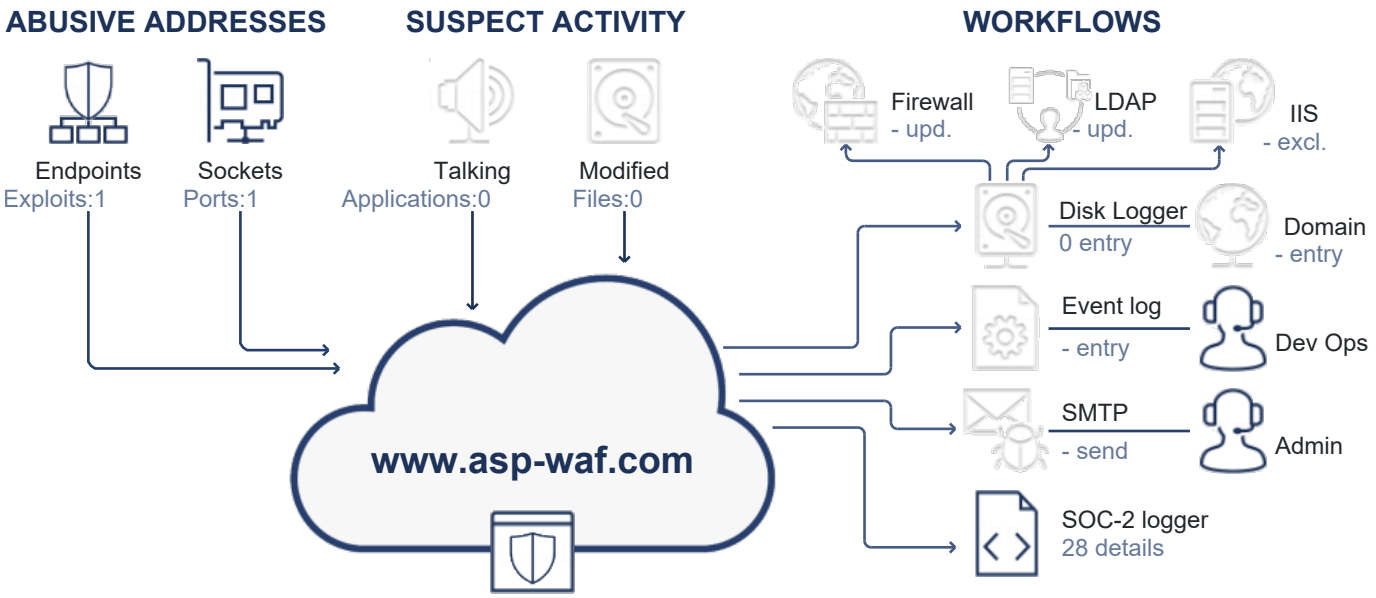
IP Addresses	:	9	IP addresses with incidents	:	8
HTTP requests served	:	1	HTTP incidents	:	-
IP address with port attacks	:	8	Last port attack	:	22/09/2021
Ports attacked	:	8	Port based incidents	:	21

** 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	22
Human	0
Bot	5
BlackHat	17
Abusive Search Engine	0
Search Engine	0

REQUEST CLASSIFICATION

OK	1
Suspect	0
Redirected	0
Blocked	0
Socket	21

DETECTED ATTACK VECTORS

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

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!

26 attempts against 1 socket and 1 HTTP requests to abuse 1 endpoint

During the reporting period, from Sun 29 August 2021 12:35:17 till Wed 22 September 2021 20:31:04 UTC, we detected 3 unique exploits from 9 IP addresses under your management.

In 24 days we detected:
- accessing a honey-pot trap
- continued attempted to probe exploits after being warned
- an attempt to use developer tools to gain access

We noted that all 8 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 8 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.

The next 9 entries document the activities in greater detail.

Malicious socket activity on port 3389 from 181.214.206.119

The user on IP address 181.214.206.119 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.

29.Aug.21 *1 penetration attempt period 29/08/2021 12:35:17 - 29/08/2021 12:41:09, all dates in UTC*

12:35:17 **Port 3389 - Remote Desktop Protocol (RDP)**

The firewall detected 2 attempts 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 stopped the attack before determining the exact exploit used. However, we have recorder 344 bytes of data send by the attacker using Stream, this data is available in the detailed report.

We responded to the attempt to exploit our server by answering legal note:This service is being monitored and we have detected your intentions attack {Name} via {IP}:{Port} to gain unlawful access to the system, please note that any unlawful activity will be reported to {ISP} as well as the relevant authorities in {Country}.

Malicious socket activity on port 3389 from 181.214.206.150

The user on IP address 181.214.206.150 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.

03.Sep.21 *1 penetration attempt period 03/09/2021 09:45:24 - 03/09/2021 09:56:55, all dates in UTC*

09:45:24 **Port 3389 - Remote Desktop Protocol (RDP)**

The firewall detected 3 attempts 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 stopped the attack before determining the exact exploit used. However, we have recorder 688 bytes of data send by the attacker using Stream, this data is available in the detailed report.

We responded to the attempt to exploit our server by answering legal note:This service is being monitored and we have detected your intentions attack {Name} via {IP}:{Port} to gain unlawful access to the system, please note that any unlawful activity will be reported to {ISP} as well as the relevant authorities in {Country}.

Triggered : ProxyUser PenetrationAttempt
Decision : legal note:This service is being monitored and we have detected your i
Action : legal note:This service is being monitored and we have detected your i

03.Sep.21 *end or reported activity*

Malicious socket activity on port 3389 from 181.214.206.146

The user on IP address 181.214.206.146 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.

04.Sep.21 *1 penetration attempt period 04/09/2021 18:24:51 - 04/09/2021 18:27:22, all dates in UTC*

18:24:51 **Port 3389 - Remote Desktop Protocol (RDP)**

The firewall detected 2 attempts 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 stopped the attack before determining the exact exploit used. However, we have recorder 344 bytes of data send by the attacker using Stream, this data is available in the detailed report.

We responded to the attempt to exploit our server by answering legal note:This service is being monitored and we have detected your intentions attack {Name} via {IP}:{Port} to gain unlawful access to the system, please note that any unlawful activity will be reported to {ISP} as well as the relevant authorities in {Country}.

Triggered : ProxyUser PenetrationAttempt
Decision : legal note:This service is being monitored and we have detected your i
Action : legal note:This service is being monitored and we have detected your i

04.Sep.21 *end or reported activity*

Malicious socket activity on port 3389 from 181.214.206.66

The user on IP address 181.214.206.66 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.

07.Sep.21 *1 penetration attempt period 07/09/2021 14:14:26 - 07/09/2021 14:16:58, all dates in UTC*

14:14:26 **Port 3389 - Remote Desktop Protocol (RDP)**

The firewall detected 2 attempts 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 stopped the attack before determining the exact exploit used. However, we have recorder 344 bytes of data send by the attacker using Stream, this data is available in the detailed report.

We responded to the attempt to exploit our server by answering legal note:This service is being monitored and we have detected your intentions attack {Name} via {IP}:{Port} to gain unlawful access to the system, please note that any unlawful activity will be reported to {ISP} as well as the relevant authorities in {Country}.

Triggered : ProxyUser PenetrationAttempt
Decision : legal note:This service is being monitored and we have detected your i
Action : legal note:This service is being monitored and we have detected your i

07.Sep.21 *end or reported activity*

Malicious socket activity on port 3389 from 181.214.206.226

The user on IP address 181.214.206.226 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.

15.Sep.21 *1 penetration attempt on 15/09/2021 11:18:09, all dates in UTC*

11:18:09 **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

15.Sep.21 *end or reported activity*

Malicious socket activity on port 3389 from 181.214.206.124

The user on IP address 181.214.206.124 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 06:59:47, all dates in UTC*

06:59:47 **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 socket activity on port 3389 from 181.214.206.115

The user on IP address 181.214.206.115 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.

18.Sep.21 *1 penetration attempt on 18/09/2021 06:51:48, all dates in UTC*

06:51:48 **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

18.Sep.21 *end or reported activity*

Malicious Multi- socket activity from 181.214.206.228

The user on IP address 181.214.206.228 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.

22.Sep.21 *14 penetration attempts period 22/09/2021 06:08:23 - 22/09/2021 20:31:04, all dates in UTC*

06:08:23 **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

08:32:54 **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

09:14:10 **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

10:16:17 **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

activity by 181.214.206.228 continues on the next page...

12:42:02 **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

14:05:54 **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

14:26:45 **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

16:12:04 **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

activity by 181.214.206.228 continues on the next page...

17:36:57 **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

17:58:20 **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

19:03:03 **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

19:24:52 **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

activity by 181.214.206.228 continues on the next page...

20:09:08 **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

20:31:04 **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

22.Sep.21 *end or reported activity*

Malicious HTTP activity from 181.214.206.238

The user on IP address 181.214.206.238 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

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

15.Sep.21 *1 penetration attempt on 15/09/2021 01:04:51, all dates in UTC*

01:04:51 **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 15/09/2021 01:10:17

Triggered : HoneyPotTrap
Decision : return Forbidden
Action : Block, expires on 15 Sep 21 01:10:17 UTC

15.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.
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.