ABUSE REPORT

activity against localhost by

Abuse Department

reported from Mon 16 Aug 21 till Thu 09 Sep 21

VESNX AG | www.asp-waf.com | firewall release 2021.9.2.708
application firewall for .Net

ABUSE REPORT
ISP Range EU-DIGITALOCEAN-NL1

Incidents recorded between 16/08/2021 14:45:27 and 09/09/2021 03:40:02 UTC

To:
DigitalOcean, LLC
101 Avenue of the Americas,
10th Floor
New York, NY, 10013
United States of America
Email abuse@digitalocean.com

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

Date : Thu 09 September 2021
Reference : EU-DIGITALOCEAN-NL1-228.252-105
Regarding : Malicious activity detected against localhost dating 16/08/2021 14:45:27UTC - 09/09/2021 03:40:02UTC

Dear Sir/ Madam

This report is addressed to you based on activity that has been triggered by 13 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 Abuse Department

based on data captured from Sun 01 Aug 21 till Thu 09 Sep 21
for IP range 188.166.0.0 - 188.166.127.255 (32'767 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:

- 72 attempts to URL exploit
- 26 attempts to exploit port 22 - secure shell (ssh)
- 6 attempts to access the web applications configuration
- 3 attempts to alter URL's to exploit the web server

Abuse score-card Abuse Department

on the 3183 days between Fri 21 Dec 2012 and Thu 09 Sep 2021

IP addresses	:	20	IP addresses with incidents	:	12
HTTP requests served	:	96	HTTP incidents	:	235
IP address with port attacks	:	13	Last port attack	:	09/09/2021
Ports attacked	:	3	Port based Incidents	:	31
Talking IP addresses	:	-	Last Talk	:	-
Talking Applications	:	-	Talks Detected	:	-

on the 39 days between Sun 01 Aug 2021 and Thu 09 Sep 2021

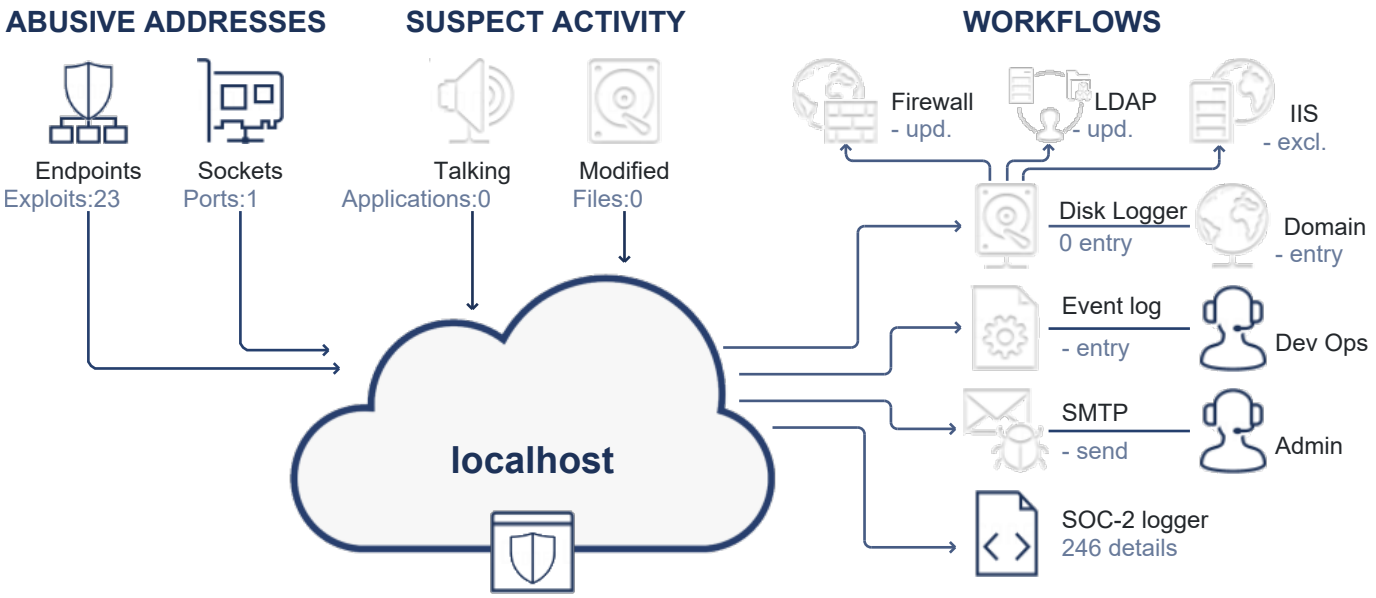
IP Addresses	:	14	IP addresses with incidents	:	7
HTTP requests served	:	96	HTTP incidents	:	-
IP address with port attacks	:	7	Last port attack	:	09/09/2021
Ports attacked	:	7	Port based incidents	:	24

** 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	8
Human	0
Bot	8
BlackHat	0
Abusive Search Engine	0
Search Engine	0

REQUEST CLASSIFICATION

OK	96
Suspect	0
Redirected	0
Blocked	0

DETECTED ATTACK VECTORS

78	uses URL phishing to probe the system
65	continued attempted to probe exploits after being warned
65	repetitive attempts to probe for exploits
64	an attempted access protected resources
63	repetitive visits while attempting to probe for exploits
8	a Common Vulnerabilities and Exposures (CVE) exploit dete
5	an attempt to access the site using the wrong technology sta
1	tries to crash 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!

26 attempts against 1 socket and 81 HTTP requests to abuse 23 endpoints

During the reporting period, from Mon 16 August 2021 14:45:27 till Thu 09 September 2021 03:40:02 UTC, we detected 8 unique exploits from 13 IP addresses under your management.

In 23 days we detected:
- 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
- an attempted to access files while not authorized to do so
- an attempted to perform data scrubbing

We noted that all 7 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 7 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 13 entries document the activities in greater detail.

Malicious Multi- socket activity from 188.166.99.59

The user on IP address 188.166.99.59 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.Aug.21 *10 penetration attempts period 16/08/2021 14:45:27 - 02/09/2021 01:49:13, all dates in UTC*

14:45:27 **Port 22 - Secure Shell (SSH)**

The firewall detected 2 attempts by an attacker to takes advantage of vulnerabilities in the

Secure Shell Protocol to gain physical access to our server.

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

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 DenySystemAccess
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

18.Aug.21 *10:00:55* **Port 22 - Secure Shell (SSH)**

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

Secure Shell Protocol to gain physical access to our server.

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

Triggered : ProxyUser DenySystemAccess
Decision :
Action : Continued recording activity

21:38:36 **Port 22 - Secure Shell (SSH)**

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

Secure Shell Protocol to gain physical access to our server.

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

Triggered : ProxyUser DenySystemAccess
Decision :
Action : Continued recording activity

21.Aug.21 *23:59:13* **Port 22 - Secure Shell (SSH)**

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

Secure Shell Protocol to gain physical access to our server.

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

Triggered : ProxyUser DenySystemAccess
Decision :
Action : Continued recording activity

activity by 188.166.99.59 continues on the next page...

12:22:51 **Port 22 - Secure Shell (SSH)**

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

Secure Shell Protocol to gain physical access to our server.

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

Triggered : ProxyUser DenySystemAccess
Decision :
Action : Continued recording activity

29.Aug.21 04:18:10 **Port 22 - Secure Shell (SSH)**

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

Secure Shell Protocol to gain physical access to our server.

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

Triggered : ProxyUser DenySystemAccess
Decision :
Action : Continued recording activity

23:41:13 **Port 22 - Secure Shell (SSH)**

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

Secure Shell Protocol to gain physical access to our server.

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

Triggered : ProxyUser DenySystemAccess
Decision :
Action : Continued recording activity

30.Aug.21 12:08:06 **Port 22 - Secure Shell (SSH)**

The firewall detected 2 attempts by an attacker to takes advantage of vulnerabilities in the

Secure Shell Protocol to gain physical access to our server.

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

Triggered : ProxyUser DenySystemAccess
Decision :
Action : Continued recording activity

31.Aug.21 17:49:16 **Port 22 - Secure Shell (SSH)**

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

Secure Shell Protocol to gain physical access to our server.

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

Triggered : ProxyUser DenySystemAccess
Decision :
Action : Continued recording activity

activity by 188.166.99.59 continues on the next page...

01:49:13 **Port 22 - Secure Shell (SSH)**

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

Secure Shell Protocol to gain physical access to our server.

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

Triggered : ProxyUser DenySystemAccess
Decision :
Action : Continued recording activity

02.Sep.21 *end or reported activity*

Malicious socket activity on port 22 from 188.166.17.31

The user on IP address 188.166.17.31 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.Aug.21 *1 penetration attempt on 18/08/2021 04:02:26, all dates in UTC*

04:02:26 **Port 22 - Secure Shell (SSH)**

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

Secure Shell Protocol to gain physical access to our server.

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

Triggered : ProxyUser DenySystemAccess
Decision :
Action : Continued recording activity

18.Aug.21 *end or reported activity*

Malicious Multi- socket activity from 188.166.100.150

The user on IP address 188.166.100.150 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.

01.Sep.21 *4 penetration attempts period 01/09/2021 11:57:55 - 03/09/2021 12:04:42, all dates in UTC*

11:57:55 **Port 22 - Secure Shell (SSH)**

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

Secure Shell Protocol to gain physical access to our server.

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

Triggered : ProxyUser DenySystemAccess
Decision :
Action : Continued recording activity

activity by 188.166.100.150 continues on the next page...

00:24:05 **Port 22 - Secure Shell (SSH)**

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

Secure Shell Protocol to gain physical access to our server.

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

Triggered : ProxyUser DenySystemAccess
Decision :
Action : Continued recording activity

03.Sep.21 01:35:34 **Port 22 - Secure Shell (SSH)**

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

Secure Shell Protocol to gain physical access to our server.

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

Triggered : ProxyUser DenySystemAccess
Decision :
Action : Continued recording activity

12:04:42 **Port 22 - Secure Shell (SSH)**

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

Secure Shell Protocol to gain physical access to our server.

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

Triggered : ProxyUser DenySystemAccess
Decision :
Action : Continued recording activity

03.Sep.21 *end or reported activity*

Malicious socket activity on port 22 from 188.166.99.240

The user on IP address 188.166.99.240 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.

05.Sep.21 *1 penetration attempt on 05/09/2021 00:55:59, all dates in UTC*

00:55:59 **Port 22 - Secure Shell (SSH)**

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

Secure Shell Protocol to gain physical access to our server.

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

Triggered : ProxyUser DenySystemAccess
Decision :
Action : Continued recording activity

05.Sep.21 *end or reported activity*

Malicious Multi- socket activity from 188.166.5.18

The user on IP address 188.166.5.18 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.

05.Sep.21 *3 penetration attempts period 05/09/2021 18:28:27 - 08/09/2021 14:55:18, all dates in UTC*

18:28:27 **Port 22 - Secure Shell (SSH)**

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

Secure Shell Protocol to gain physical access to our server.

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

Triggered : ProxyUser DenySystemAccess
Decision :
Action : Continued recording activity

06.Sep.21 *07:39:30* **Port 22 - Secure Shell (SSH)**

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

Secure Shell Protocol to gain physical access to our server.

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

Triggered : ProxyUser DenySystemAccess
Decision :
Action : Continued recording activity

08.Sep.21 *14:55:18* **Port 22 - Secure Shell (SSH)**

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

Secure Shell Protocol to gain physical access to our server.

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

Triggered : ProxyUser DenySystemAccess
Decision :
Action : Continued recording activity

08.Sep.21 *end or reported activity*

Malicious Multi- socket activity from 188.166.0.75

The user on IP address 188.166.0.75 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 *3 penetration attempts period 07/09/2021 14:08:06 - 08/09/2021 22:35:26, all dates in UTC*

14:08:06 **Port 22 - Secure Shell (SSH)**

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

Secure Shell Protocol to gain physical access to our server.

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

Triggered : ProxyUser DenySystemAccess
Decision :
Action : Continued recording activity

08.Sep.21 *07:33:03* **Port 22 - Secure Shell (SSH)**

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

Secure Shell Protocol to gain physical access to our server.

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

Triggered : ProxyUser DenySystemAccess
Decision :
Action : Continued recording activity

22:35:26 **Port 22 - Secure Shell (SSH)**

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

Secure Shell Protocol to gain physical access to our server.

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

Triggered : ProxyUser DenySystemAccess
Decision :
Action : Continued recording activity

08.Sep.21 *end or reported activity*

Malicious Multi- socket activity from 188.166.88.48

The user on IP address 188.166.88.48 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.

08.Sep.21 *2 penetration attempts period 08/09/2021 17:38:32 - 09/09/2021 03:40:02, all dates in UTC*

17:38:32 **Port 22 - Secure Shell (SSH)**
The firewall detected a attempt by an attacker to takes advantage of vulnerabilities in the

Secure Shell Protocol to gain physical access to our server.

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

Triggered : ProxyUser DenySystemAccess
Decision :
Action : Continued recording activity

09.Sep.21 *03:40:02* **Port 22 - Secure Shell (SSH)**
The firewall detected a attempt by an attacker to takes advantage of vulnerabilities in the

Secure Shell Protocol to gain physical access to our server.

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

Triggered : ProxyUser DenySystemAccess
Decision :
Action : Continued recording activity

09.Sep.21 *end or reported activity*

Malicious HTTP activity from 188.166.44.99

The user on IP address 188.166.44.99 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
- a Common Vulnerabilities and Exposures (CVE) exploit detected
- an attempted to access files while not authorized to do so
- an attempted to perform data scrubbing

During the reported time range user of IP address triggered and attempted to use 8 different exploits 15 times.

01.Sep.21 *15 penetration attempts period 01/09/2021 09:56:04 - 07/09/2021 21:43:38, all dates in UTC*

activity by 188.166.44.99 continues on the next page...

09:56:04 **https://d54c397cf.access.telenet.be/pods**

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 01/09/2021 12:55:53

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 234 milliseconds
Action : Block, expires on 01 Sep 21 12:55:53 UTC
Notes : Known abuser as a previous exploit was triggered

09:56:05 **https://d54c397cf.access.telenet.be/heapdump**

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 01/09/2021 12:55:53

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 79 milliseconds
Action : Block, expires on 01 Sep 21 12:55:53 UTC

09:56:06 **https://d54c397cf.access.telenet.be/actuator/heapdump**

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 01/09/2021 12:55:53

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 79 milliseconds
Action : Block, expires on 01 Sep 21 12:55:53 UTC

09:56:07 **https://d54c397cf.access.telenet.be/api/v1/pods**

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 01/09/2021 12:55:53

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 92 milliseconds
Action : Block, expires on 01 Sep 21 12:55:53 UTC

09:56:09 **https://d54c397cf.access.telenet.be/env**

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 01/09/2021 12:55:53

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 99 milliseconds

09:56:10 **https://d54c397cf.access.telenet.be/actuator/env**

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 01/09/2021 12:55:53

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 128 milliseconds
Action : Block, expires on 01 Sep 21 12:55:53 UTC

09:56:28 **https://d54c397cf.access.telenet.be/_cat/indices?v**

The firewall flagged the HttpGet request as 3 actions that are of malicious intent where detected.The user tried to use URL Query string poisoning by injecting ?v to bypass detection or alter the system tricking it to do what it's not supposed to do. 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 01/09/2021 12:55:53

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 115 milliseconds
Action : Block, expires on 01 Sep 21 12:55:53 UTC

09:56:28 **https://d54c397cf.access.telenet.be/_all/_search**

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 01/09/2021 12:55:53

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 130 milliseconds
Action : Block, expires on 01 Sep 21 12:55:53 UTC

02.Sep.21 07:58:30 **https://d54c397cf.access.telenet.be/druid/index.html**

The firewall flagged the HttpGet request as a malicious intent was detected.

The firewall detected exploit and triggered a incident expiring 02/09/2021 08:03:30

Triggered : PhishyRequest
Decision : return Forbidden
Action : Block, expires on 02 Sep 21 08:03:30 UTC

06.Sep.21 21:51:50 **https://d54c397cf.access.telenet.be/css../.git/config**

The firewall flagged the HttpGet 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 06/09/2021 21:57:22

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 157 milliseconds
Action : Block, expires on 06 Sep 21 21:57:22 UTC

activity by 188.166.44.99 continues on the next page

03:32:20 **https://d54c397cf.access.telenet.be/.git/config**

The firewall flagged the HttpGet 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 07/09/2021 03:38:59

Triggered : PenetrationAttempt MaliciousUser PhishyRequest CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 311 milliseconds
Action : Block, expires on 07 Sep 21 03:38:59 UTC

11:57:08 **https://d54c397cf.access.telenet.be/portal/main.jsp**

The firewall flagged the HttpGet 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 07/09/2021 12:06:12

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 4 incidents in 168 milliseconds
Action : Block, expires on 07 Sep 21 12:06:12 UTC

12:42:58 **https://d54c397cf.access.telenet.be/%3Cimg%20src=x%20data'a'onerror=ale**

The firewall flagged the HttpGet request as a malicious intent was detected.

The firewall detected exploit and triggered a incident expiring 07/09/2021 12:47:59

Triggered : PhishyRequest
Decision : return Forbidden
Action : Block, expires on 07 Sep 21 12:47:59 UTC

19:27:37 **https://d54c397cf.access.telenet.be/Autodiscover/XFrame/Scripts/XFrame.js**

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 07/09/2021 19:33:03

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 98 milliseconds
Action : Block, expires on 07 Sep 21 19:33:03 UTC

21:43:38 **https://d54c397cf.access.telenet.be/Autodiscover/XFrame/Scripts/XFrame.js**

The firewall flagged the HttpGet 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 07/09/2021 21:49:04

Triggered : PenetrationAttempt MaliciousUser PhishyRequest DenailOfService
Decision : return Forbidden after 4 incidents in 456 milliseconds
Action : Block, expires on 07 Sep 21 21:49:04 UTC

Malicious HTTP activity from 188.166.19.235

The user on IP address 188.166.19.235 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

During the reported time range user of IP address triggered and attempted to use 5 different exploits 12 times.

01.Sep.21 *12 penetration attempts period 01/09/2021 17:12:54 - 07/09/2021 16:47:37, all dates in UTC*

17:12:54 **https://d54c397cf.access.telenet.be/images/json**

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 01/09/2021 17:41:20

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 234 milliseconds
Action : Block, expires on 01 Sep 21 17:41:20 UTC
Notes : Known abuser as a previous exploit was triggered

17:12:59 **https://d54c397cf.access.telenet.be/images/json**

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 01/09/2021 17:41:20

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 78 milliseconds
Action : Block, expires on 01 Sep 21 17:41:20 UTC

17:13:24 **https://d54c397cf.access.telenet.be/server-status**

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 01/09/2021 17:41:20

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 92 milliseconds
Action : Block, expires on 01 Sep 21 17:41:20 UTC

activity by 188.166.19.235 continues on the next page...

18:07:38 **https://d54c397cf.access.telenet.be/env**

The firewall flagged the HttpGet request as a malicious intent was detected.

The firewall detected exploit and triggered a incident expiring 01/09/2021 18:37:55

Triggered : PhishyRequest
Decision : escalated thread-level
Action : NoAction, expires on 01 Sep 21 18:37:55 UTC

18:07:52 **https://d54c397cf.access.telenet.be/ftpsync.settings**

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 01/09/2021 18:41:59

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 199 milliseconds
Action : Block, expires on 01 Sep 21 18:41:59 UTC

18:07:53 **https://d54c397cf.access.telenet.be/_all/_search**

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 01/09/2021 18:41:59

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 96 milliseconds
Action : Block, expires on 01 Sep 21 18:41:59 UTC

06.Sep.21 23:58:58 **https://d54c397cf.access.telenet.be/Autodiscover/XFrame/Scripts/XFrame.js**

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 07/09/2021 00:08:17

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 113 milliseconds
Action : Block, expires on 07 Sep 21 00:08:17 UTC

07.Sep.21 11:02:08 **https://d54c397cf.access.telenet.be/%3Cimg%20src=x%20data'a'onerror=ale**

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 07/09/2021 12:06:12

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 229 milliseconds
Action : Block, expires on 07 Sep 21 12:06:12 UTC

activity by 188.166.19.235 continues on the next page...

12:39:14 **https://d54c397cf.access.telenet.be/portal/main.jsp**

The firewall flagged the HttpGet request as a malicious intent was detected.

The firewall detected exploit and triggered a incident expiring 07/09/2021 13:02:24

Triggered : PhishyRequest
Decision : escalated thread-level
Action : NoAction, expires on 07 Sep 21 13:02:24 UTC

14:18:56 **https://d54c397cf.access.telenet.be/heapdump**

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 07/09/2021 14:26:05

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 120 milliseconds
Action : Block, expires on 07 Sep 21 14:26:05 UTC

14:39:37 **https://d54c397cf.access.telenet.be/heapdump**

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 07/09/2021 14:56:11

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 220 milliseconds
Action : Block, expires on 07 Sep 21 14:56:11 UTC

16:47:37 **https://d54c397cf.access.telenet.be/swagger/index.html**

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 07/09/2021 16:57:32

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 111 milliseconds
Action : Block, expires on 07 Sep 21 16:57:32 UTC

07.Sep.21 *end or reported activity*

Malicious HTTP activity from 188.166.85.202

The user on IP address 188.166.85.202 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
- a Common Vulnerabilities and Exposures (CVE) exploit detected
- an attempted to access files while not authorized to do so

During the reported time range user of IP address triggered and attempted to use 7 different exploits 18 times.

01.Sep.21 *18 penetration attempts period 01/09/2021 19:26:49 - 07/09/2021 23:00:37, all dates in UTC*

19:26:49 **https://d54c397cf.access.telenet.be/Autodiscover/XFrame/Scripts/XFrame.js**

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 01/09/2021 19:32:39

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 203 milliseconds
Action : Block, expires on 01 Sep 21 19:32:39 UTC
Notes : Known abuser as a previous exploit was triggered

19:58:43 **https://d54c397cf.access.telenet.be/sftp-config.json**

The firewall flagged the HttpGet 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 firewall detected 4 exploits and triggered a incident expiring 01/09/2021 20:22:49

Triggered : PenetrationAttempt MaliciousUser PhishyRequest CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 260 milliseconds
Action : Block, expires on 01 Sep 21 20:22:49 UTC

19:58:44 **https://d54c397cf.access.telenet.be/ftpsync.settings**

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 01/09/2021 20:22:49

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 68 milliseconds
Action : Block, expires on 01 Sep 21 20:22:49 UTC

activity by 188.166.85.202 continues on the next page...

19:59:20 **https://d54c397cf.access.telenet.be/env**

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 01/09/2021 20:22:49

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 84 milliseconds
Action : Block, expires on 01 Sep 21 20:22:49 UTC

19:59:22 **https://d54c397cf.access.telenet.be/actuator/env**

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 01/09/2021 20:22:49

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 97 milliseconds
Action : Block, expires on 01 Sep 21 20:22:49 UTC

19:59:47 **https://d54c397cf.access.telenet.be/pods**

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 01/09/2021 20:22:49

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 112 milliseconds
Action : Block, expires on 01 Sep 21 20:22:49 UTC

19:59:48 **https://d54c397cf.access.telenet.be/api/v1/pods**

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 01/09/2021 20:22:49

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 102 milliseconds
Action : Block, expires on 01 Sep 21 20:22:49 UTC

20:00:03 **https://d54c397cf.access.telenet.be/heapdump**

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 01/09/2021 20:22:49

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 120 milliseconds
Action : Block, expires on 01 Sep 21 20:22:49 UTC

20:00:04 **https://d54c397cf.access.telenet.be/actuator/heapdump**

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 01/09/2021 20:22:49

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 210 milliseconds
Action : Block, expires on 01 Sep 21 20:22:49 UTC

20:00:05 **https://d54c397cf.access.telenet.be/_cat/indices?v**

The firewall flagged the HttpGet request as 3 actions that are of malicious intent where detected.The user tried to use URL Query string poisoning by injecting ?v to bypass detection or alter the system tricking it to do what it's not supposed to do. 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 01/09/2021 20:22:49

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 169 milliseconds
Action : Block, expires on 01 Sep 21 20:22:49 UTC

20:00:06 **https://d54c397cf.access.telenet.be/_all/_search**

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 01/09/2021 20:22:49

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 145 milliseconds
Action : Block, expires on 01 Sep 21 20:22:49 UTC

07.Sep.21 00:23:25 **https://d54c397cf.access.telenet.be/swagger/index.html**

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 07/09/2021 00:33:21

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 109 milliseconds
Action : Block, expires on 07 Sep 21 00:33:21 UTC

activity by 188.166.85.202 continues on the next page...

10:55:33 **https://d54c397cf.access.telenet.be/heapdump**

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 07/09/2021 11:00:59

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 226 milliseconds
Action : Block, expires on 07 Sep 21 11:00:59 UTC

13:18:59 **https://d54c397cf.access.telenet.be/heapdump**

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 07/09/2021 13:28:53

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 98 milliseconds
Action : Block, expires on 07 Sep 21 13:28:53 UTC

14:00:41 **https://d54c397cf.access.telenet.be/portal/main.jsp**

The firewall flagged the HttpGet request as a malicious intent was detected.

The firewall detected exploit and triggered a incident expiring 07/09/2021 14:05:41

Triggered : PhishyRequest
Decision : escalated thread-level
Action : NoAction, expires on 07 Sep 21 14:05:41 UTC

14:25:34 **https://d54c397cf.access.telenet.be/%3Cimg%20src=x%20data'a'onerror=ale**

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 07/09/2021 14:31:06

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 246 milliseconds
Action : Block, expires on 07 Sep 21 14:31:06 UTC

16:32:43 **https://d54c397cf.access.telenet.be/.git/config**

The firewall flagged the HttpGet request as a malicious intent was detected.

The firewall detected exploit and triggered a incident expiring 07/09/2021 17:33:45

Triggered : PhishyRequest
Decision : return Forbidden
Action : Block, expires on 07 Sep 21 17:33:45 UTC

activity by 188.166.85.202 continues on the next page...

23:00:37 **https://d54c397cf.access.telenet.be/portal/main.jsp**

The firewall flagged the HttpGet 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 07/09/2021 23:08:46

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 4 incidents in 336 milliseconds
Action : Block, expires on 07 Sep 21 23:08:46 UTC

07.Sep.21 *end or reported activity*

Malicious HTTP activity from 188.166.86.241

The user on IP address 188.166.86.241 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
- a Common Vulnerabilities and Exposures (CVE) exploit detected
- an attempted to access files while not authorized to do so

During the reported time range user of IP address triggered and attempted to use 7 different exploits 9 times.

02.Sep.21 *9 penetration attempts period 02/09/2021 00:21:57 - 07/09/2021 19:07:51, all dates in UTC*

00:21:57 **https://d54c397cf.access.telenet.be/api/v1/version**

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 02/09/2021 00:36:38

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 205 milliseconds
Action : Block, expires on 02 Sep 21 00:36:38 UTC
Notes : Known abuser as a previous exploit was triggered

00:21:59 **https://d54c397cf.access.telenet.be/Autodiscover/XFrame/Scripts/XFrame.js**

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 02/09/2021 00:36:38

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 72 milliseconds
Action : Block, expires on 02 Sep 21 00:36:38 UTC

activity by 188.166.86.241 continues on the next page...

00:22:19 **https://d54c397cf.access.telenet.be/**

The firewall flagged the HttpGet request as a malicious intent was 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 exploit and triggered a incident expiring 02/09/2021 00:36:38

Triggered :
Decision : return Forbidden
Action : Block, expires on 02 Sep 21 00:36:38 UTC

00:59:31 **https://d54c397cf.access.telenet.be/sftp-config.json**

The firewall flagged the HttpGet request as a malicious intent was 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 detected exploit and triggered a incident expiring 02/09/2021 01:11:57

Triggered : PenetrationAttempt
CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden
Action : Block, expires on 02 Sep 21 01:11:57 UTC

07.Sep.21 00:09:15 **https://d54c397cf.access.telenet.be/.git/config**

The firewall flagged the HttpGet 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 07/09/2021 00:18:18

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 138 milliseconds
Action : Block, expires on 07 Sep 21 00:18:18 UTC

11:32:07 **https://d54c397cf.access.telenet.be/Autodiscover/XFrame/Scripts/XFrame.js**

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 07/09/2021 11:41:07

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 180 milliseconds
Action : Block, expires on 07 Sep 21 11:41:07 UTC

12:55:53 **https://d54c397cf.access.telenet.be/sftp-config.json**

The firewall flagged the HttpGet 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 firewall detected 4 exploits and triggered a incident expiring 07/09/2021 13:03:48

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 206 milliseconds

15:45:51 **https://d54c397cf.access.telenet.be/portal/main.jsp**

The firewall flagged the HttpGet 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 07/09/2021 15:51:22

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 4 incidents in 150 milliseconds
Action : Block, expires on 07 Sep 21 15:51:22 UTC

19:07:51 **https://d54c397cf.access.telenet.be/heapdump**

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 07/09/2021 19:12:59

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 100 milliseconds
Action : Block, expires on 07 Sep 21 19:12:59 UTC

07.Sep.21 *end or reported activity*

Malicious HTTP activity from 188.166.42.142

The user on IP address 188.166.42.142 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

During the reported time range user of IP address triggered and attempted to use 5 different exploits 10 times.

03.Sep.21 *10 penetration attempts period 03/09/2021 08:59:32 - 07/09/2021 19:05:24, all dates in UTC*

08:59:32 **https://d54c397cf.access.telenet.be/v2/_catalog**

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 03/09/2021 09:04:58

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 387 milliseconds
Action : Block, expires on 03 Sep 21 09:04:58 UTC
Notes : Known abuser as a previous exploit was triggered

activity by 188.166.42.142 continues on the next page...

09:33:25 **https://d54c397cf.access.telenet.be/_cat/indices?v**
The firewall flagged the HttpGet request as a malicious intent was detected.The user tried to use URL Query string poisoning by injecting ?v to bypass detection or alter the system tricking it to do what it's not supposed to do.

The firewall detected exploit and triggered a incident expiring 03/09/2021 09:38:26

Triggered : PhishyRequest
Decision : escalated thread-level
Action : NoAction, expires on 03 Sep 21 09:38:26 UTC

09:33:25 **https://d54c397cf.access.telenet.be/ftpsync.settings**
The firewall flagged the HttpGet request as a malicious intent was detected.

The firewall detected exploit and triggered a incident expiring 03/09/2021 09:38:26

Triggered : PhishyRequest
Decision : escalated thread-level
Action : NoAction, expires on 03 Sep 21 09:38:26 UTC

19:01:43 **https://d54c397cf.access.telenet.be/te%3Cimg%20src=x%20onerror=alert(42)**
The firewall flagged the HttpGet request as a malicious intent was detected.

The firewall detected exploit and triggered a incident expiring 03/09/2021 19:06:43

Triggered : PhishyRequest
Decision : escalated thread-level
Action : NoAction, expires on 03 Sep 21 19:06:43 UTC

19:33:57 **https://d54c397cf.access.telenet.be/heapdump**
The firewall flagged the HttpGet request as a malicious intent was detected.

The firewall detected exploit and triggered a incident expiring 03/09/2021 19:38:58

Triggered : PhishyRequest
Decision : escalated thread-level
Action : NoAction, expires on 03 Sep 21 19:38:58 UTC

07.Sep.21 01:49:49 **https://d54c397cf.access.telenet.be/.git/config**
The firewall flagged the HttpGet request as a malicious intent was detected.

The firewall detected exploit and triggered a incident expiring 07/09/2021 01:54:50

Triggered : PhishyRequest
Decision : escalated thread-level
Action : NoAction, expires on 07 Sep 21 01:54:50 UTC

12:17:20 **https://d54c397cf.access.telenet.be/sftp-config.json**
The firewall flagged the HttpGet request as a malicious intent was 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 detected exploit and triggered a incident expiring 07/09/2021 12:22:21

Triggered : PhishyRequest
Decision : escalated thread-level
Action : NoAction, expires on 07 Sep 21 12:22:21 UTC

activity by 188.166.42.142 continues on the next page...

12:28:49 **https://d54c397cf.access.telenet.be/portal/main.jsp**
The firewall flagged the HttpGet request as a malicious intent was detected.

The firewall detected exploit and triggered a incident expiring 07/09/2021 12:33:50

Triggered : PhishyRequest
Decision : escalated thread-level
Action : NoAction, expires on 07 Sep 21 12:33:50 UTC

14:40:18 **https://d54c397cf.access.telenet.be/portal/main.jsp**
The firewall flagged the HttpGet request as a malicious intent was detected.

The firewall detected exploit and triggered a incident expiring 07/09/2021 14:45:18

Triggered : PhishyRequest
Decision : escalated thread-level
Action : NoAction, expires on 07 Sep 21 14:45:18 UTC

19:05:24 **https://d54c397cf.access.telenet.be/portal/main.jsp**
The firewall flagged the HttpGet request as a malicious intent was detected.

The firewall detected exploit and triggered a incident expiring 07/09/2021 19:10:24

Triggered : PhishyRequest
Decision : escalated thread-level
Action : NoAction, expires on 07 Sep 21 19:10:24 UTC

07.Sep.21 *end or reported activity*

Malicious HTTP activity from 188.166.42.183

The user on IP address 188.166.42.183 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
- a Common Vulnerabilities and Exposures (CVE) exploit detected
- an attempted to access files while not authorized to do so

During the reported time range user of IP address triggered and attempted to use 7 different exploits 17 times.

03.Sep.21 *17 penetration attempts period 03/09/2021 13:59:34 - 08/09/2021 01:16:17, all dates in UTC*

13:59:34 **https://d54c397cf.access.telenet.be/api/v1/version**
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 03/09/2021 14:07:45

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 211 milliseconds
Action : Block, expires on 03 Sep 21 14:07:45 UTC
Notes : Known abuser as a previous exploit was triggered

activity by 188.166.42.183 continues on the next page...

13:59:38 **https://d54c397cf.access.telenet.be/**

The firewall flagged the HttpGet request as a malicious intent was 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 exploit and triggered a incident expiring 03/09/2021 14:07:45

Triggered :
Decision : return Forbidden
Action : Block, expires on 03 Sep 21 14:07:45 UTC

14:32:20 **https://d54c397cf.access.telenet.be/sftp-config.json**

The firewall flagged the HttpGet 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 firewall detected 4 exploits and triggered a incident expiring 03/09/2021 14:52:54

Triggered : PenetrationAttempt MaliciousUser PhishyRequest CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 284 milliseconds
Action : Block, expires on 03 Sep 21 14:52:54 UTC

14:32:21 **https://d54c397cf.access.telenet.be/ftpsync.settings**

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 03/09/2021 14:52:54

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 75 milliseconds
Action : Block, expires on 03 Sep 21 14:52:54 UTC

14:32:34 **https://d54c397cf.access.telenet.be/heapdump**

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 03/09/2021 14:52:54

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 74 milliseconds
Action : Block, expires on 03 Sep 21 14:52:54 UTC

14:32:34 **https://d54c397cf.access.telenet.be/actuator/heapdump**

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 03/09/2021 14:52:54

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 83 milliseconds

14:33:00 **https://d54c397cf.access.telenet.be/env**

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 03/09/2021 14:52:54

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 120 milliseconds
Action : Block, expires on 03 Sep 21 14:52:54 UTC

14:33:13 **https://d54c397cf.access.telenet.be/_all/_search**

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 03/09/2021 14:52:54

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 130 milliseconds
Action : Block, expires on 03 Sep 21 14:52:54 UTC

14:33:22 **https://d54c397cf.access.telenet.be/api/v1/pods**

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 03/09/2021 14:52:54

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 126 milliseconds
Action : Block, expires on 03 Sep 21 14:52:54 UTC

04.Sep.21 12:22:15 **https://d54c397cf.access.telenet.be/Autodiscover/XFrame/Scripts/XFrame.js**

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 04/09/2021 12:30:44

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 246 milliseconds
Action : Block, expires on 04 Sep 21 12:30:44 UTC

06.Sep.21 23:44:38 **https://d54c397cf.access.telenet.be/%3Cimg%20src=x%20data'a'onerror=ale**

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 06/09/2021 23:53:14

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 125 milliseconds
Action : Block, expires on 06 Sep 21 23:53:14 UTC

12:00:39 **https://d54c397cf.access.telenet.be/%3Cimg%20src=x%20data'a'onerror=ale**

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 09/09/2021 09:33:34

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 129 milliseconds
Action : Block, expires on 09 Sep 21 09:33:34 UTC

12:48:09 **https://d54c397cf.access.telenet.be/portal/main.jsp**

The firewall flagged the HttpGet 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 09/09/2021 09:34:47

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 4 incidents in 171 milliseconds
Action : Block, expires on 09 Sep 21 09:34:47 UTC

14:03:41 **https://d54c397cf.access.telenet.be/%3Cimg%20src=x%20data'a'onerror=ale**

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 09/09/2021 09:33:34

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 239 milliseconds
Action : Block, expires on 09 Sep 21 09:33:34 UTC

14:33:15 **https://d54c397cf.access.telenet.be/portal/main.jsp**

The firewall flagged the HttpGet 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 09/09/2021 09:34:47

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 4 incidents in 348 milliseconds
Action : Block, expires on 09 Sep 21 09:34:47 UTC

activity by 188.166.42.183 continues on the next page...

18:08:40 **https://d54c397cf.access.telenet.be/Autodiscover/XFrame/Scripts/XFrame.js**

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 09/09/2021 09:34:47

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 106 milliseconds
Action : Block, expires on 09 Sep 21 09:34:47 UTC

08.Sep.21 01:16:17 **https://d54c397cf.access.telenet.be/sftp-config.json**

The firewall flagged the HttpGet 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 firewall detected 4 exploits and triggered a incident expiring 09/09/2021 09:34:47

Triggered : PenetrationAttempt MaliciousUser PhishyRequest CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 346 milliseconds
Action : Block, expires on 09 Sep 21 09:34:47 UTC

08.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.

AttemptToAccessSiteUsingTheTechnologyStack	An attempt to obtain access the site using a framework not compatible with that what is used on the web application. This indicates that the BOT or script is guessing known exploits without knowing the software installed.
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.
DenailOfService	An attempt was made to take the site down by flooding it with requests
DenySystemAccess	An attempt to obtain system access was detected and blocked
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.
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.