ABUSE REPORT

activity against localhost by

LLC

reported from Thu 12 Aug 21 till Thu 09 Sep 21

ABUSE REPORT
ISP Range DIGITALOCEAN-167-99-0-0

Incidents recorded between 12/08/2021 08:21:30 and 09/09/2021 06:11:08 UTC

To:
101 Ave of the Americas\r
10th Floor
New York
NY
10013
United States

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

Date : Thu 09 September 2021
Reference : DIGITALOCEAN-167-99-0-0-224.252-35
Regarding : Malicious activity detected against localhost dating 12/08/2021 08:21:30UTC - 09/09/2021 06:11:08UTC

Dear Sir/ Madam

This report is addressed to you based on activity that has been triggered by 10 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 LLC

based on data captured from Mon 09 Aug 21 till Thu 09 Sep 21
for IP range 167.99.0.0 - 167.99.255.255 (65'535 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:

- 20 attempts to URL exploit
- 10 attempts to exploit port 22 - secure shell (ssh)
- 5 attempts to access the web applications configuration
- 1 attempt to exploit port 3389 - remote desktop protocol (rdp)

Abuse score-card LLC

on the 1398 days between Fri 10 Nov 2017 and Thu 09 Sep 2021

IP addresses	:	26	IP addresses with incidents	:	2
HTTP requests served	:	36	HTTP incidents	:	84
IP address with port attacks	:	14	Last port attack	:	31/08/2021
Ports attacked	:	3	Port based Incidents	:	31
Talking IP addresses	:	-	Last Talk	:	-
Talking Applications	:	-	Talks Detected	:	-

on the 31 days between Mon 09 Aug 2021 and Thu 09 Sep 2021

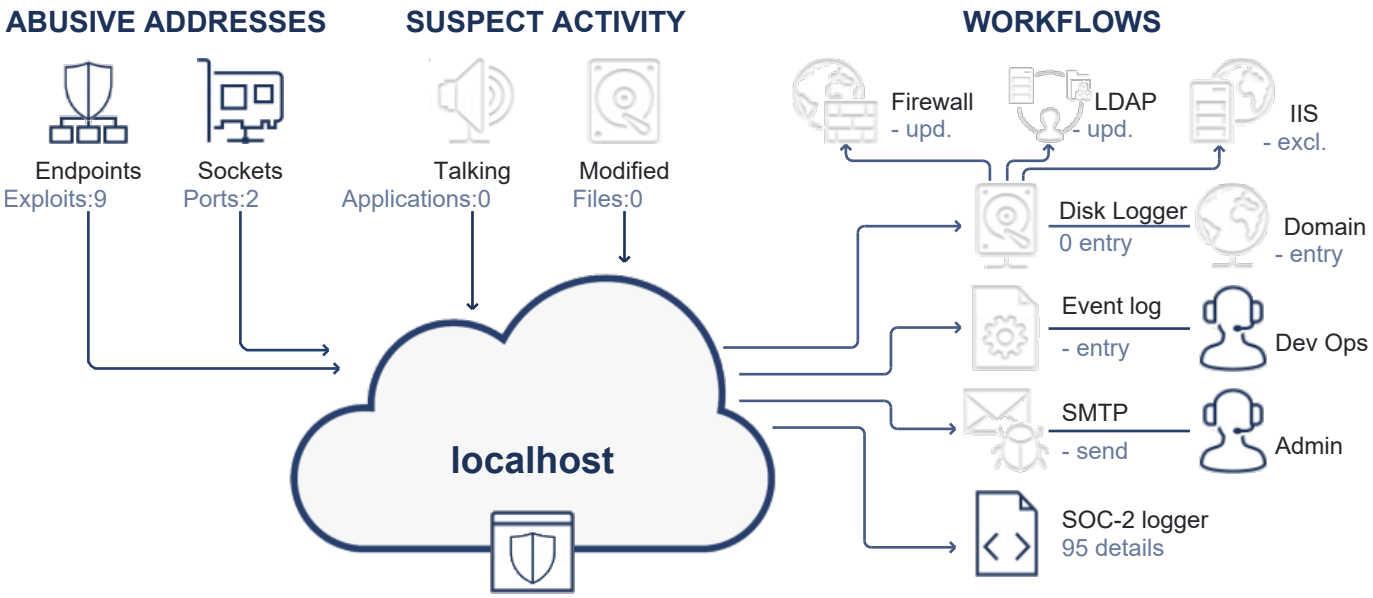
IP Addresses	:	16	IP addresses with incidents	:	8
HTTP requests served	:	32	HTTP incidents	:	-
IP address with port attacks	:	8	Last port attack	:	31/08/2021
Ports attacked	:	8	Port based incidents	:	10

** 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	3
Human	0
Bot	3
BlackHat	0
Abusive Search Engine	0
Search Engine	0

REQUEST CLASSIFICATION

OK	32
Suspect	0
Redirected	0
Blocked	0

DETECTED ATTACK VECTORS

25	uses URL phishing to probe the system
23	an attempted access protected resources
23	continued attempted to probe exploits after being warned
23	repetitive visits while attempting to probe for exploits
23	repetitive attempts to probe for exploits
7	an attempt to access the site using the wrong technology sta
6	a Common Vulnerabilities and Exposures (CVE) exploit dete

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!

11 attempts against 2 sockets and 25 HTTP requests to abuse 9 endpoints

During the reporting period, from Thu 12 August 2021 08:21:30 till Thu 09 September 2021 06:11:08 UTC, we detected 7 unique exploits from 10 IP addresses under your management.

In 27 days we detected:
- uses URL phishing to probe the system
- 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
- an attempted to access files while not authorized to do so
- a Common Vulnerabilities and Exposures (CVE) exploit detected

We noted that there is an overlap between the 8 IP addresses that are attacking based on the same 2 ports. Is this a coincidence or a distributed attack? We would appreciate an update concerning this matter.

The next 10 entries document the activities in greater detail.

Malicious socket activity on port 22 from 167.99.107.57

The user on IP address 167.99.107.57 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.

12.Aug.21 *1 penetration attempt on 12/08/2021 08:21:30, all dates in UTC*

08:21:30 **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

12.Aug.21 *end or reported activity*

Malicious Multi- socket activity from 167.99.34.181

The user on IP address 167.99.34.181 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.

13.Aug.21 *3 penetration attempts period 13/08/2021 13:22:12 - 17/08/2021 14:59:29, all dates in UTC*

13:22:12 **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

14.Aug.21 *12:20:39* **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 167.99.34.181 continues on the next page...

14:59:29 **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

17.Aug.21 *end or reported activity*

Malicious socket activity on port 22 from 167.99.133.28

The user on IP address 167.99.133.28 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 *1 penetration attempt period 16/08/2021 01:12:03 - 16/08/2021 01:12:05, all dates in UTC*

01:12:03 **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

16.Aug.21 *end or reported activity*

Malicious socket activity on port 22 from 167.99.216.191

The user on IP address 167.99.216.191 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.

17.Aug.21 *1 penetration attempt on 17/08/2021 20:27:39, all dates in UTC*

20:27:39 **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

17.Aug.21 *end or reported activity*

Malicious socket activity on port 3389 from 167.99.169.240

The user on IP address 167.99.169.240 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.

18.Aug.21 *1 penetration attempt on 18/08/2021 21:40:03, all dates in UTC*

21:40:03 **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

18.Aug.21 *end or reported activity*

Malicious socket activity on port 22 from 167.99.241.55

The user on IP address 167.99.241.55 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.

23.Aug.21 *1 penetration attempt on 23/08/2021 08:48:47, all dates in UTC*

08:48:47 **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.Aug.21 *end or reported activity*

Malicious socket activity on port 22 from 167.99.119.168

The user on IP address 167.99.119.168 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.

25.Aug.21 *1 penetration attempt on 25/08/2021 23:41:19, all dates in UTC*

23:41:19 **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

25.Aug.21 *end or reported activity*

Malicious socket activity on port 22 from 167.99.1.98

The user on IP address 167.99.1.98 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.

31.Aug.21 *1 penetration attempt on 31/08/2021 08:23:14, all dates in UTC*

08:23:14 **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

31.Aug.21 *end or reported activity*

Malicious HTTP activity from 167.99.211.249

The user on IP address 167.99.211.249 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploits:

- uses URL phishing to probe the system
- an attempted access protected resources
- continued attempted to probe exploits after being warned
- repetitive visits while attempting to probe for exploits
- repetitive attempts to probe for exploits
- an attempted to access files while not authorized to do so
- a Common Vulnerabilities and Exposures (CVE) exploit detected

During the reported time range user of IP address triggered and attempted to use 7 different exploits 13 times.

01.Sep.21 *13 penetration attempts period 01/09/2021 04:50:39 - 09/09/2021 06:11:08, all dates in UTC*

04:50:39 **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 01/09/2021 04:55:39

Triggered : PhishyRequest
Decision : escalated thread-level
Action : NoAction, expires on 01 Sep 21 04:55:39 UTC

03.Sep.21 *11:56:41* **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 12:05:13

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 111 milliseconds
Action : Block, expires on 03 Sep 21 12:05:13 UTC

activity by 167.99.211.249 continues on the next page...

12:33:39 **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 15:07:57

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 344 milliseconds
Action : Block, expires on 03 Sep 21 15:07:57 UTC

06.Sep.21 23:41:54 **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 06/09/2021 23:48:12

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 107 milliseconds
Action : Block, expires on 06 Sep 21 23:48:12 UTC

07.Sep.21 11:21:04 **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 11:31:05

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 119 milliseconds
Action : Block, expires on 07 Sep 21 11:31:05 UTC

13:00:16 **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 13:08:49

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 4 incidents in 154 milliseconds
Action : Block, expires on 07 Sep 21 13:08:49 UTC

14:10:23 **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 15:06:13

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
AttemptToAccessSiteUsingTheTechnologyStack

15:22:25 **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 15:31:18

Triggered : PenetrationAttempt MaliciousUser PhishyRequest CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 370 milliseconds
Action : Block, expires on 07 Sep 21 15:31:18 UTC

16:48:58 **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 16:57:32

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 94 milliseconds
Action : Block, expires on 07 Sep 21 16:57:32 UTC

23:20:45 **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 23:38:52

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 4 incidents in 207 milliseconds
Action : Block, expires on 07 Sep 21 23:38:52 UTC

08.Sep.21 07:01:24 **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 08/09/2021 07:08:05

Triggered : PenetrationAttempt MaliciousUser PhishyRequest CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 151 milliseconds
Action : Block, expires on 08 Sep 21 07:08:05 UTC

activity by 167.99.211.249 continues on the next page...

20:55:38 **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 08/09/2021 21:04:42

Triggered : PenetrationAttempt MaliciousUser PhishyRequest CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 334 milliseconds
Action : Block, expires on 08 Sep 21 21:04:42 UTC

09.Sep.21 06:11:08 **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 09/09/2021 06:17:33

Triggered : PenetrationAttempt MaliciousUser PhishyRequest CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 375 milliseconds
Action : Block, expires on 09 Sep 21 06:17:33 UTC

09.Sep.21 *end or reported activity*

Malicious HTTP activity from 167.99.221.146

The user on IP address 167.99.221.146 tried to exploit web based vulnerabilities.In its totality the user of IP address tried to use a HTTP request to exploits:

- an attempted access protected resources
- continued attempted to probe exploits after being warned
- repetitive visits while attempting to probe for exploits
- repetitive attempts to probe for exploits
- uses URL phishing to probe the system
- an attempted to access files while not authorized to do so
- a Common Vulnerabilities and Exposures (CVE) exploit detected

During the reported time range user of IP address triggered and attempted to use 7 different exploits 12 times.

03.Sep.21 *12 penetration attempts period 03/09/2021 18:36:28 - 09/09/2021 06:06:49, all dates in UTC*

18:36:28 **https://d54c397cf.access.telenet.be/s/xxx/_/;/WEB-INF/web.xml**

The firewall flagged the HttpGet request as 3 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to access web.xml 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 3 exploits and triggered a incident expiring 03/09/2021 18:47:25

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 362 milliseconds
Action : Block, expires on 03 Sep 21 18:47:25 UTC
Notes : Known abuser as a previous exploit was triggered

18:36:30 **https://d54c397cf.access.telenet.be/s/xxx/_/;/WEB-INF/web.xml**

The firewall flagged the HttpGet request as 3 actions that are of malicious intent where detected.We did not appreciate the attempt by your user to access web.xml 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 3 exploits and triggered a incident expiring 03/09/2021 18:47:25

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 82 milliseconds
Action : Block, expires on 03 Sep 21 18:47:25 UTC

06.Sep.21 23:27:30 **https://d54c397cf.access.telenet.be/Autodiscover/XFrame/Scripts/XFrame.js**

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

The firewall detected exploit and triggered a incident expiring 06/09/2021 23:32:30

Triggered : PhishyRequest
Decision : escalated thread-level
Action : NoAction, expires on 06 Sep 21 23:32:30 UTC

07.Sep.21 12:06:53 **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 12:16:14

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 4 incidents in 171 milliseconds
Action : Block, expires on 07 Sep 21 12:16:14 UTC

13:09:28 **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 13:18:52

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 4 incidents in 155 milliseconds
Action : Block, expires on 07 Sep 21 13:18:52 UTC

15:41:11 **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 15:46:21

Triggered : PenetrationAttempt MaliciousUser PhishyRequest CommonVulnerabilitiesExposuresExploitDetected

20:11:44 **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 20:18:12

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 4 incidents in 143 milliseconds
Action : Block, expires on 07 Sep 21 20:18:12 UTC

23:54:30 **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 23:59:30

Triggered : PenetrationAttempt MaliciousUser PhishyRequest CommonVulnerabilitiesExposuresExploitDetected
Decision : return Forbidden after 4 incidents in 145 milliseconds
Action : Block, expires on 07 Sep 21 23:59:30 UTC

08.Sep.21 02:42:11 **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 08/09/2021 02:47:45

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 132 milliseconds
Action : Block, expires on 08 Sep 21 02:47:45 UTC

03:57:02 **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 08/09/2021 06:43:00

Triggered : PenetrationAttempt MaliciousUser PhishyRequest AttemptToAccessSiteUsingTheTechnologyStack
Decision : return Forbidden after 4 incidents in 573 milliseconds
Action : Block, expires on 08 Sep 21 06:43:00 UTC

activity by 167.99.221.146 continues on the next page...

02:34:53 **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 09/09/2021 02:40:49

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 96 milliseconds
Action : Block, expires on 09 Sep 21 02:40:49 UTC

06:06:49 **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 09/09/2021 08:18:27

Triggered : PenetrationAttempt MaliciousUser PhishyRequest
Decision : return Forbidden after 3 incidents in 245 milliseconds
Action : Block, expires on 09 Sep 21 08:18:27 UTC

09.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.
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.