SECNAP Security Incident Report f[..] printed by Lloyd Lucas (Lloyd.Lucas@secnap.com) 10/06/201[..]

Article Print

State:	closed(by CESIT)	Age:	4 days 16 [illegible]
Priority:	3 normal	Created:	06/19/2014 06:12:45
Queue:	IT-Sec	Accounted time:	0
Lock:	unlock	Pending till:	-
Customer id:	security@secnap.com		
Owner:	administrator (Admin OTRS)		

Articles

 # 1

From: NY-CESC IPS Alert <security@secnap.net>

To: <abuse-ht@secnap.com>

Subject: SECNAP Security Incident Report for NY-CESC IPS Alert - NY-CESC IPS Alert

Created: 06/19/2014 06:12:47 by customer

Type: email-external

```
211.115.199.210 in Korea was found running an attack against your network . Abuse has been reported to their ISP.  Your
intrusion prevention system has automatically blocked this traffic
Notes: snort:1:2003466:ET WEB_SERVER PHP Attack Tool Morfeus F Scanner :
      http://www.webmasterworld.com/search_engine_spiders/3227720.htm
      http://doc.emergingthreats.net/2003466

Events listed in GMT timezone



GET /user/soapCaller.bs HTTP/1.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Morfeus Fucking Scanner
Host: 64.94.172.148
Connection: Close


length = 182

000 : 47 45 54 20 2F 75 73 65 72 2F 73 6F 61 70 43 61   GET /user/soapCa
010 : 6C 6C 65 72 2E 62 73 20 48 54 54 50 2F 31 2E 31   ller.bs HTTP/1.1
020 : 0D 0A 41 63 63 65 70 74 3A 20 2A 2F 2A 0D 0A 41   ..Accept: */*..A
030 : 63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65 3A 20   ccept-Language:
040 : 65 6E 2D 75 73 0D 0A 41 63 63 65 70 74 2D 45 6E   en-us..Accept-En
050 : 63 6F 64 69 6E 67 3A 20 67 7A 69 70 2C 20 64 65   coding: gzip, de
060 : 66 6C 61 74 65 0D 0A 55 73 65 72 2D 41 67 65 6E   flate..User-Agen
070 : 74 3A 20 4D 6F 72 66 65 75 73 20 46 75 63 6B 69   t: Morfeus Fucki
080 : 6E 67 20 53 63 61 6E 6E 65 72 0D 0A 48 6F 73 74   ng Scanner..Host
090 : 3A 20 36 34 2E 39 34 2E 31 37 32 2E 31 34 38 0D   : 64.94.172.148.
0a0 : 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 43 6C 6F   .Connection: Clo
0b0 : 73 65 0D 0A 0D 0A                                 se....

[2014-06-19 10:09:08] | 1 | 211.115.199.210:47065 -> 192.168.42.2:80 | TCP | ACK[1]    | snort:1:2003466

--
>|SECNAP Network Security
US:+1.561.948.2255
EU:+31(0)85 8880490, Option 4
AU:+61 (07) 3 1235961, Option 4
IL:+972 (3) 7219011, Option 4
```


CONFIDENTIAL HS 001644

SECNAP Security Incident Report f[..] printed by Lloyd Lucas (Lloyd.Lucas@secnap.com) 10/06/201[..]

Article Print

State:	closed successful	Age:	414 d 18 h
Priority:	3 normal	Created:	06/19/2014 06:13:11
Queue:	Firewall	Accounted time:	0
Lock:	unlock	Pending till:	-
Customer ID:	security@secnap.com		
Owner:	administrator (Admin OTRS)		

Articles

 # 1

From:	NY-CESC IPS Alert <security@secnap.net>
To:	<abuse-ht@secnap.com>
Subject:	SECNAP Security Incident Report for NY-CESC IPS Alert - NY-CESC IPS Alert
Created:	06/19/2014 06:13:13 by customer
Type:	email-external

```
211.115.199.210 in Korea was found running an attack against your network . Abuse has been reported to their ISP.  Your
intrusion prevention system has automatically blocked this traffic
Notes: snort:1:2003466:ET WEB_SERVER PHP Attack Tool Morfeus F Scanner :
     http://www.webmasterworld.com/search_engine_spiders/3227720.htm
     http://doc.emergingthreats.net/2003466

Events listed in GMT timezone



GET /user/soapCaller.bs HTTP/1.1
Accept: */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Morfeus Fucking Scanner
Host: 64.94.172.148
Connection: Close


length = 182

000 : 47 45 54 20 2F 75 73 65 72 2F 73 6F 61 70 43 61   GET /user/soapCa
010 : 6C 6C 65 72 2E 62 73 20 48 54 54 50 2F 31 2E 31   ller.bs HTTP/1.1
020 : 0D 0A 41 63 63 65 70 74 3A 20 2A 2F 2A 0D 0A 41   ..Accept: */*..A
030 : 63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65 3A 20   ccept-Language:
040 : 65 6E 2D 75 73 0D 0A 41 63 63 65 70 74 2D 45 6E   en-us..Accept-En
050 : 63 6F 64 69 6E 67 3A 20 67 7A 69 70 2C 20 64 65   coding: gzip, de
060 : 66 6C 61 74 65 0D 0A 55 73 65 72 2D 41 67 65 6E   flate..User-Agen
070 : 74 3A 20 4D 6F 72 66 65 75 73 20 46 75 63 6B 69   t: Morfeus Fucki
080 : 6E 67 20 53 63 61 6E 6E 65 72 0D 0A 48 6F 73 74   ng Scanner..Host
090 : 3A 20 36 34 2E 39 34 2E 31 37 32 2E 31 34 38 0D   : 64.94.172.148.
0a0 : 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 43 6C 6F   .Connection: Clo
0b0 : 73 65 0D 0A 0D 0A                                 se....

[2014-06-19 10:09:08] | 1 | 211.115.199.210:47065 -> 192.168.42.2:80 | TCP | ACK[1]     | snort:1:2003466

--
>|SECNAP Network Security
US:+1.561.948.2255
EU:+31(0)85 8880490, Option 4
AU:+61 (07) 3 1235961, Option 4
IL:+972 (3) 7219011, Option 4
```


CONFIDENTIAL HS 001645

SECNAP Security Incident Report f[..] printed by Lloyd Lucas (Lloyd.Lucas@secnap.com) 10/06/201[..]

Article Print

State:	closed successful	Age:	44 days 10 h
Priority:	3 normal	Created:	07/14/2014 02:38:56
Queue:	HT (1)	Accounted time:	0
Lock:	unlock	Pending till:	-
Customer id:	security@secnap.com		
Owner:	administrator (Admin OTRS)		

Articles

 # 1

From:	NY-CESC IPS Alert <security@secnap.net>
To:	<abuse-ht@secnap.com>
Subject:	SECNAP Security Incident Report for NY-CESC IPS Alert - NY-CESC IPS Alert
Created:	07/14/2014 02:38:58 by customer
Type:	email-external

```
118.186.67.13 in China attempted to connect to a machine on your network via HTTP.  Abuse has been reported to their
ISP.  This traffic is being blocked by your intrusion prevention system

Notes: snort:1:2012936:ET SCAN ZmEu Scanner User-Agent Inbound:

Events listed in GMT timezone

[2014-07-14 06:34:30] | 1 | 118.186.67.13:49153 -> 192.168.42.22:80 | TCP | ACK[1]    | snort:1:2012936

--
>|SECNAP Network Security
US:+1 561 948 2255
EU:+31(0)85 8880490, Option 4
AU:+61 (07) 3 1235961, Option 4
IL:+972 (3) 7219011, Option 4
```


CONFIDENTIAL HS 001646

SECNAP Security Incident Report f[..] printed by Lloyd Lucas (Lloyd.Lucas@secnap.com) 10/06/201[..]

Article Print

State:	closed successful	Age:	250 days 1 h
Priority:	3 normal	Created:	01/28/2015 14:19:01
Queue:	IT-SOC	Accounted time:	0
Lock:	unlock	Pending till:	-
Customer:	security@secnap.com		
Owner:	llucas (Lloyd Lucas)		

Articles

 # 1

From:	NY-CESC IPS Alert <security@secnap.net>
To:	<abuse-ht@secnap.com>
Subject:	SECNAP Security Incident Report for NY-CESC IPS Alert - NY-CESC IPS Alert
Created:	01/28/2015 14:19:03 by customer
Type:	email-external

```
This host in France was found attacking a web server on your network.  CloudJacket has blocked this traffic.


Notes: snort:1:25975:POLICY-OTHER Adobe ColdFusion admin interface access attempt :
     http://www.adobe.com/support/security/advisories/apsa13-01.html
     http://cve.mitre.org/cgi-bin/cvename.cgi?name=2013-0632
     http://www.securityfocus.com/bid/57330

Events listed in GMT timezone

[2015-01-28 19:11:05] | 1 | 37.187.252.180:53907 -> 192.168.42.22:80 |  |     | snort:1:25975

--
>|SECNAP Network Security
US:+1.561.948.2255
EU:+31(0)85 8880490, Option 4
AU:+61 (07) 3 1235961, Option 4
IL:+972 (3) 7219011, Option 4
```


CONFIDENTIAL HS 001661

SECNAP Security Incident Report f[..] printed by Lloyd Lucas (Lloyd.Lucas@secnap.com) 10/06/201[..]

Article Print

Priority:	3 normal	Created:	12/08/2013 18:40:20
Queue:	[redacted]	[redacted]	
Lock:	unlock	Pending till:	-
Customer ID:	[redacted]	[redacted]	
Owner:	administrator (admin OTRS)		

Articles

 # 1

From:	NY-CESC IPS Alert <security@secnap.net>
To:	<abuse-ht@secnap.com>
Subject:	SECNAP Security Incident Report for NY-CESC IPS Alert - NY-CESC IPS Alert
Created:	12/08/2013 18:40:22 by customer
Type:	email-external

```
The host at 69.163.138.235 in the U.S. is attempting to run an attack against a machine on your network, this traffic
should be blocked.


Notes: snort:1:2014704:ET WEB_SPECIFIC_APPS PHP-CGI query string parameter vulnerability :
     http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/
     http://varandid.com/research-alerts/us-cert/vu520827-php-cgi-query-string-parameter-vulnerability/
     http://cve.mitre.org/cgi-bin/cvename.cgi?name=2012-1823

Events listed in GMT timezone

[2013-12-08 23:29:51] | 1 | 69.163.138.235:47397 -> 192.168.42.22:80 | TCP | ACK[1]    | snort:1:2014704


>|SECNAP Network Security
US:+1 561.948.2255
EU:+31(0)85 8880490, Option 4
AU:+61 (07) 3 1235961, Option 4
IL:+972 (3) 7219011, Option 4
```


CONFIDENTIAL HS 001618

SECNAP Security Incident Report f[..] printed by Lloyd Lucas (Lloyd.Lucas@secnap.com) 10/06/201[..]

Article Print

State:	closed successful	Age:	4 d 1 h
Priority:	3 normal	Created:	06/18/2014 23:46:31
Queue:	RT-OUT	Accounted time:	0
Lock:	unlock	Pending till:	-
Customer ID:	security@secnap.com		
Owner:	administrator (Admin OTRS)		

Articles

 # 1

From:	NY-CESC IPS Alert <security@secnap.net>
To:	<abuse-ht@secnap.com>
Subject:	SECNAP Security Incident Report for NY-CESC IPS Alert - NY-CESC IPS Alert
Created:	06/18/2014 23:46:33 by customer
Type:	email-external

```
ns.km20603-05.keymachine.de[84.19.188.40] in Germany was found running an attack against your network . Abuse has been
reported to their ISP.  Your intrusion prevention system has automatically blocked this traffic
Notes: snort:1:2006402:ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted :
     http://doc.emergingthreats.net/bin/view/Main/2006402

Events listed in GMT timezone



POST /admin/assets/themes/case.php?act=tools&d=%2Ftmp HTTP/1.1
host: 64.94.172.146
content-type: application/x-www-form-urlencoded
charset=utf-8
authorization: Basic dmFtcGlyZTpldmlsQGFjY2Vzcw==
content-length: 322
Connection: keep-alive


length = 247

000 : 50 4F 53 54 20 2F 61 64 6D 69 6E 2F 61 73 73 65   POST /admin/asse
010 : 74 73 2F 74 68 65 6D 65 73 2F 63 61 73 65 2E 70   ts/themes/case.p
020 : 68 70 3F 61 63 74 3D 74 6F 6F 6C 73 26 64 3D 25   hp?act=tools&amp;d=%
030 : 32 46 74 6D 70 20 48 54 54 50 2F 31 2E 31 0D 0A   2Ftmp HTTP/1.1..
040 : 68 6F 73 74 3A 20 36 34 2E 39 34 2E 31 37 32 2E   host: 64.94.172.
050 : 31 34 36 0D 0A 63 6F 6E 74 65 6E 74 2D 74 79 70   146..content-typ
060 : 65 3A 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 78   e: application/x
070 : 2D 77 77 77 2D 66 6F 72 6D 2D 75 72 6C 65 6E 63   -www-form-urlenc
080 : 6F 64 65 64 3B 20 63 68 61 72 73 65 74 3D 75 74   oded; charset=ut
090 : 66 2D 38 0D 0A 61 75 74 68 6F 72 69 7A 61 74 69   f-8..authorizati
0a0 : 6F 6E 3A 20 42 61 73 69 63 20 64 6D 46 74 63 47   on: Basic dmFtcG
0b0 : 6C 79 5A 54 70 6C 64 6D 6C 73 51 47 46 6A 59 32   lyZTpldmlsQGFjY2
0c0 : 56 7A 63 77 3D 3D 0D 0A 63 6F 6E 74 65 6E 74 2D   Vzcw==..content-
0d0 : 6C 65 6E 67 74 68 3A 20 33 32 32 0D 0A 43 6F 6E   length: 322..Con
0e0 : 6E 65 63 74 69 6F 6E 3A 20 6B 65 65 70 2D 61 6C   nection: keep-al
0f0 : 69 76 65 0D 0A 0D 0A                              ive....

[2014-06-19 03:40:35] | 1 | 84.19.188.40:38463 -> 192.168.42.22:80 | TCP | ACK[1]     | snort:1:2006402

--
>|SECNAP Network Security
US:+1.561.948.2255
EU:+31(0)85 8880490, Option 4
AU:+61 (07) 3 1235961, Option 4
IL:+972 (3) 7219011, Option 4
```


CONFIDENTIAL HS 001643

SECNAP Security Incident Report f[..] printed by Lloyd Lucas (Lloyd.Lucas@secnap.com) 10/06/201[..]

Article Print

State:	closed successful	Age:	244 days
Priority:	3 normal	Created:	02/04/2015 00:31:54
Queue:	IT::Ops	Accounted time:	0
Lock:	unlock	Pending till:	-
Customer ID:	security@secnap.com		
Owner:	llucas (Lloyd Lucas)		

Articles

 # 1

From:	NY-CESC IPS Alert <security@secnap.net>
To:	<abuse-ht@secnap.com>
Subject:	SECNAP Security Incident Report for NY-CESC IPS Alert - NY-CESC IPS Alert
Created:	02/04/2015 00:31:57 by customer
Type:	email-external

```
198.154.63.131 in United States attempted to connect to a machine on your network via HTTP.  Abuse has been reported to
their ISP.  This traffic is being blocked by your intrusion prevention system.

Notes: snort:1:2013115:ET WEB_SERVER Muieblackcat scanner;

Notes: snort;1:80003:SECNAP Known Malicious Hosts -;

Events listed in GMT timezone

[2015-02-04 05:33:52] | 1 | 198.154.63.131:58176 -> 192.168.42.22:80 |   |     | snort:1:80003
[2015-02-04 05:33:52] | 1 | 198.154.63.131:58176 -> 192.168.42.22:80 |   |     | snort:1:2013115

--
>|SECNAP Network Security
US:+1.561.948.2255
EU:+31(0)85 8880490, Option 4
AU:+61 (07) 3 1235961, Option 4
IL:+972 (3) 7219011, Option 4
```


CONFIDENTIAL HS 001662