# Incident Report



Incident : Suspicious event
Date Reported : 03/08/2010

Status : Closed - Resolved

Document ID : DSTS-87Y6MV

## Reporter Details

Reported By : [redacted] Staff/ABS
Created By : [redacted] Staff/ABS
Office : VIC
Section : No Section
Branch : Technology Services (Vic)
Division : Technology Services Division
Phone : (03) 9615[redacted]
Location : VIC L5 WS 119

## Incident Occurred

Incident Start date : Tue 03/08/2010
Incident End Date (if over a period) : Tue 03/08/2010

Start Time : 12:15 PM
End Time : 01:00 PM

State/Office Where Incident Occurred : CO
Where did the Incident Occur? ● Office ○ Outside Office

Describe the Location : Gateway environment - Main website servers

Other, was selected as part of Incident:
Please explain Security Description : Noticed multiple security threats detected by our IPS devices and agents in the gateway [redacted]

Description

Tell us what happened :
Please provide short explanation of the incident including any information that could assist in its resolution such as the names of witnesses or contributing circumstances.

➲ See

| Tag Name | Status | Severity | Event Count |
|---|---|---|---|
| Shell_Command_Injection | Detected attack (block response not enabled) | Medium | 42 |
| XML_RPC_PHP_CmdExec | Attack failure (blocked by [redacted] appliance) | High | 24 |
| HTTP_Oracle_WebCache_Overflow | Successful attack (confirmed by agent) | High | 1 |


Out of scope - automated report

Don't believe there was any detrimental effect of these events. Noteworthy none the less.

Details :
Has property been Stolen/Lost/Damaged/Destroyed? ○ Yes ● No

Details of people responsible for the incident
If known, please enter the names and addresses of people responsible for the incident.

Name : Address :

Was any body injured? : ○ Yes ● No ○ Not Applicable

Signature - Signed by [redacted] Staff/ABS on 10/08/2010 09:06:59 AM, according to /ABS

First Created By : [redacted] On : 03/08/2010 01:56:35 PM

## Police Involvement

Police involvement information is not required for this Incident.
Were police called? : ○ Yes ● No

## Administration

Investigator/s:

Investigation Started:

Investigation Ended: Tue 10/08/2010

### General

Security Description : Other
Security Incident : other
Incident Rating :

Summary of the Security Action taken :
Please provide summary of the action taken including any doclinks to relevant documents.This is part is to be filled when the investigation is completed.
Spoke to [redacted] all OK to close;
Total Hours :

### Fraud

Fraud Method :
Type of Loss (if any) :
Specify Other Method :

Person Responsible: Relation with ABS :
Security Level :

Person Responsible:
Security Level :
Person Responsible:
Security Level :

Relation with ABS :

Relation with ABS :

## Document Access

Authors : [Security Staff], [Security Admin]
Readers : [Security Staff], [Security Admin]

## Related Documents

| Date Created | Doc Type |
|---|---|

## Reminder Information

Reminder Sent Date: 10/08/2010
Reminder No.: 0

Next Reminder: 17/08/2010
Last Edited Date: 10/08/2010

## Edit History

Report Closed by [redacted] on 10/08/2010 09:06:58 AM
Incident Submitted by [redacted] on 03/08/2010 02:02:48 PM
Incident Created by [redacted] on 03/08/2010 01:57:39 PM

SIRs -Prod v2.0

# Incident Report

v 1.0

Incident : Theft - Other
Date Reported : 03/10/2008

Status : Closed - Resolved

Document ID : AWAN-7K35PN

## Reporter Details

Reported By : [redacted]
Created By : [redacted]
Office : CO
Section : IT Communications
Branch :
Division :
Phone : (02) 6252[redacted]
Location : CO 1S 131

## Incident Occurred

Incident Start date : Sat 27/09/2008
Incident End Date (if over a period) : Mon 29/09/2008

Start Time : 02:00 AM
End Time : 07:00 PM

State/Office Where Incident Occurred : CO
Where did the Incident Occur? ● Office ○ Outside Office

Describe the Location : telephone toll fraud from Sierra Leone origin

Other, was selected as part of Incident:
Please explain Security Description :

**Tell us what happened :**
Please provide short explanation of the incident including any information that could assist in its resolution such as the names of witnesses or contributing circumstances.

➲ Incoming telephone calls apparently from Sierra Leone on upper portion of in-dial range were configured to reflect themselves back to numbers in Sierra Leone.

It is suspected that the called numbers are a premium service and thus some of the charges would eventually return to the perpetrators.

The sum involved is $128k

**Details :**
**Has property been Stolen/Lost/Damaged/Destroyed?** ○ Yes ● No

**Details of people responsible for the incident**
If known, please enter the names and addresses of people responsible for the incident.

**Name :** **Address :**

**Was any body injured? :** ○ Yes ● No ○ Not Applicable

Signature - Signed by [redacted] /Staff/ABS on 14/10/2008 02:19:55 PM, according to /Staff/ABS

First Created By : [redacted] On : 03/10/2008 01:08:13 PM

**Police Involvement**

**Police involvement information is not required for this Incident.**
**Were police called? :** ○ Yes ● No

## Administration

**Investigator/s:**

**Investigation Started:**

**Investigation Ended:** 05/02/2009

## General

**Security Description :** Theft
**Security Incident :** Other
**Incident Rating :**

**Summary of the Security Action taken :**
Please provide summary of the action taken including any doclinks to relevant documents.This is part is to be filled when the investigation is completed.
Awaiting response from [redacted] incident report to DSD; flaw fixed in CISCO parameters

**Total Hours :**

## Fraud

**Fraud Method :**
**Type of Loss (if any) :**
**Specify Other Method :**

**Person Responsible:** **Relation with ABS :**
**Security Level :**
**Person Responsible:** **Relation with ABS :**
**Security Level :**
**Person Responsible:** **Relation with ABS :**
**Security Level :**

## Document Access

Authors : [Security Admin], [Servers]
Readers : [Security Admin], [Security Staff], [redacted]

## Related Documents

| Date Created | Doc Type |
|---|---|

## Reminder Information

Reminder Sent Date:
Reminder No.: 0
Next Reminder:
Last Edited Date:

## Edit History

Incident Report has been modified for correct readers and authors fields 23/02/2009 06:31:28 PM
Incident Report has been upgraded to new format on 05/02/2009 07:38:57 PM
Incident Submitted by [redacted] on 03/10/2008 01:13:44 PM
Incident Submitted by [redacted] on 03/10/2008 01:12:54 PM

SIRs-Prod v2.0

# Incident Report

v 1.0

Incident : Suspicious event
Date Reported : 04/10/2012

Status : Closed - Resolved

Document ID : JGRN-8YR28H

## Reporter Details

| | |
|---|---|
| Reported By : | [redacted] Staff/ABS |
| Created By : | [redacted] Staff/ABS |
| Office : | CO |
| Section : | Network Services |
| Branch : | Technology Infrastructure Delivery |
| Division : | Technology Services Division |
| Phone : | (02) 6252[redacted] |
| Location : | CO 1S 329 |

## Incident Occurred

| | | | |
|---|---|---|---|
| Incident Start date : | Wed 03/10/2012 | Start Time : | 01:26 PM |
| Incident End Date (if over a period) : | Wed 03/10/2012 | End Time : | 01:26 PM |

State/Office Where Incident Occurred: CO

Where did the Incident Occur? ● Office ○ Outside Office

Describe the Location :

Other, was selected as part of Incident:
Please explain Security Description :

**Tell us what happened :**
Please provide short explanation of the incident including any information that could assist in its resolution such as the names of witnesses or contributing circumstances.

35 attempts to access server Monkfish (webprod1021 - austats website) using default admin/user accounts between 13:26:05 and 13:26:22. The accounts attempted to be accessed were admin, tomcat, manager and user. See:


Out of scope - automated report

All attempts were from [redacted]

**Details :**
**Has property been Stolen/Lost/Damaged/Destroyed?** ○ Yes ● No

**Details of people responsible for the incident**
If known, please enter the names and addresses of people responsible for the incident.

**Name :** **Address :**

**Was any body injured? :** ○ Yes ○ No ● Not Applicable

[redacted] Signature - Signed by [redacted] Staff/ABS on 18/10/2012 02:36:49 PM, according to /ABS

First Created By : [redacted], On : 04/10/2012 10:10:21 AM

## Police Involvement

Police involvement information is not required for this Incident.
Were police called? : ○ Yes ● No

## Administration

Investigator/s:

Investigation Started:

Investigation Ended: Thu 18/10/2012

## General

Security Description : Other
Security Incident : other
Incident Rating :

Summary of the Security Action taken :
Please provide summary of the action taken including any doclinks to relevant documents.This is part is to be filled when the investigation is completed.

Total Hours :

## Fraud

Fraud Method :
Type of Loss (if any) :
Specify Other Method :

Person Responsible:
Security Level :
Relation with ABS :

Person Responsible:
Security Level :
Relation with ABS :

Person Responsible:
Relation with ABS :

Security Level :

Document Access

Authors : [Security Staff], [Security Admin]
Readers : [Security Staff], [Security Admin]

Related Documents

| Date Created | Doc Type | |
|---|---|---|
| 04/10/2012 | Response By | CN=Chris Soczynski/OU=Staff/O=ABS |

Reminder Information

Reminder Sent Date: 18/10/2012
Reminder No.: 0
Next Reminder: 25/10/2012
Last Edited Date: 18/10/2012

Edit History

Report Closed by [redacted] on 18/10/2012 02:36:48 PM
Response Document Created/Updated by NotesACT07 on 04/10/2012 10:25:14 AM
Document Updated by Chris Soczynski on 04/10/2012 10:24:06 AM

Incident Submitted by [redacted] on 04/10/2012 10:21:21 AM
Incident Created by [redacted] on 04/10/2012 10:11:59 AM

SIRs -Prod v2.0

# Incident Report

v 1.0

**Incident :** Suspicious event
**Date Reported :** 26/10/2012

**Status :** Closed - Resolved

**Document ID :** JGRN-8ZET83

## Reporter Details

| | |
|---|---|
| **Reported By :** | [redacted] Staff/ABS |
| **Created By :** | [redacted] Staff/ABS |
| **Office :** | CO |
| **Section :** | Network Services |
| **Branch :** | Technology Infrastructure Delivery |
| **Division :** | Technology Services Division |
| **Phone :** | (02) 6252[redacted] |
| **Location :** | CO 1S 329 |

## Incident Occurred

| | | | |
|---|---|---|---|
| **Incident Start date :** | Thu 25/10/2012 | **Start Time :** | 01:52 AM |
| **Incident End Date (if over a period) :** | Thu 25/10/2012 | **End Time :** | 01:52 AM |

**State/Office Where Incident Occurred** CO
**Where did the Incident Occur?** ● Office ○ Outside Office

**Describe the Location :**

**Other, was selected as part of Incident:**
**Please explain Security Description :**

Describe the Location : Toll Fraud on ISDN line coming into Polycom RMX, which is located in the Data Centre

## Description

Tell us what happened :
Please provide short explanation of the incident including any information that could assist in its resolution such as the names of witnesses or contributing circumstances.

➲ Starting at 12/6/2012 at 9:51 there were 437 suspect calls to Somalia Hot Number 2524058[redacted], Kuwait Number 9659901[redacted] and many other countries. The calls entered the ABS on [redacted] and [redacted] and left the ABS on [redacted] This is an Telstra ISDN circuit connected to out Polycom RMX Video Confrencing Bridge.

We have physically disconnected this circuit while investigations continue

Details :
Has property been Stolen/Lost/Damaged/Destroyed? ○ Yes ● No

Details of people responsible for the incident
If known, please enter the names and addresses of people responsible for the incident.

Name : Address :

Was any body injured? : ○ Yes ○ No ● Not Applicable

Signature - Signed by [redacted] Staff/ABS on 27/06/2012 09:00:26 AM, according to /ABS

First Created By : [redacted] On : 13/06/2012 10:20:31 AM

## Police Involvement

Police involvement information is not required for this Incident.

| | | | |
|---|---|---|---|
| Were police called? : | ● Yes ○ No | State Police or AFP : | Federal Police |
| Date Called : | Fri 15/06/2012 | Time Called : | |
| Station Called : | | Police Attended : | ○ Yes ● No |
| Date Attended : | | Time Attended : | |
| Name of Officer : | [redacted]@afp.gov.au | Police Reference Number (if known) : | 5042610 |
| Action Police Taken (if applicable) : | | | |

## Administration

Investigator/s: [redacted]Staff/ABS,

Investigation Started:

Investigation Ended: Wed 27/06/2012

### General

Security Description : Unauthorised Access
Security Incident : to ABS IT Network
Incident Rating : High

Summary of the Security Action taken :
Please provide summary of the action taken including any doclinks to relevant documents.This is part is to be filled when the investigation is completed.

Telstra Info

[redacted]

Could you please attach this detail to the security incident. You may wish to pass it on to AFP or DSD, or at least let them know we have it.

We disconnected the service at around 10am, so there may have been more calls - not sure if they had stopped or or more likely it is to do with the billing cycle.

**Lyn Little**

*Director*

Network Services | Technical Services Division | **Australian Bureau of Statistics**

**(P) (02) 6252** [redacted] **(M)** [redacted]

**(E) Lyn.Little@abs.gov.au (W) www.abs.gov.au**

---- Forwarded by Lyn Little/Staff/ABS on 18/06/2012 03:23 PM ----

From: [redacted]@team.telstra.com>
To: [redacted]@team.telstra.com>, [redacted]@abs.gov.au>
Cc: Lyn Little <lyn.little@abs.gov.au>, [redacted]@team.telstra.com>
Date: 18/06/2012 02:38 PM
Subject: RE: SUSPECT FRAUD ALERT: AUSTRALIAN BUREAU OF STATISTICS [SEC=UNCLASSIFIED]

All

Please find attached the pre-bill information for this service extracted today.

Regards

[redacted]
Service Management Lead
Federal Government | Telstra Enterprise & Government
GPO Box 1827, Canberra ACT, 2601
Lvl 3, 490 Northbourne Ave, Dickson, ACT 2602 Australia
Email: [redacted]@team.telstra.com | Web: www.telstra.com/enterprise
Phone: 02 6129[redacted] | Mobile: [redacted]

WELCOME TO LIFE IN FULL COLOUR

**From:** [redacted]
**Sent:** Wednesday, 13 June 2012 10:34 AM
**To:** [redacted]
**Cc:** Lyn Little; [redacted]
**Subject:** RE: SUSPECT FRAUD ALERT: AUSTRALIAN BUREAU OF STATISTICS [SEC=UNCLASSIFIED]

Dear Lyn and [redacted]

Thank you for such prompt action – I'm glad ABS were able to take such decisive action to minimise future risks.

As discussed briefly with Lyn, below are the links to the AFP contact you may require as part of your process:

**Report fraud incident to the Police**
All CPE Fraud should be **reported to the Australian Federal Police** (AFP):

- AFP Operations Monitoring Centre in their state via the **AFP website**.
- Fraud incident reports must be done in writing either via email, mail or fax, as per the **instructions on the AFP** site.

The AFP will provide a reference number for insurance purposes.

Lyn, regarding the other part of your question, the charges for the calls will not have arrived in our billing systems yet (last night is too soon). We don't expect this to happen until about next week – [redacted] or [redacted] will provide you the billing information as soon as they obtain it.

Kind regards,
[redacted]

[redacted]
Account Executive | Telstra Enterprise & Government
P (02) 6129[redacted] | M [redacted]

**From:** [redacted]@abs.gov.au]

**Sent:** Wednesday, 13 June 2012 9:57 AM
**To:** [redacted]
**Cc:** Lyn Little; [redacted]
**Subject:** Re: SUSPECT FRAUD ALERT: AUSTRALIAN BUREAU OF STATISTICS [SEC=UNCLASSIFIED]

Hello [redacted] and colleagues,

Lyn is not in the office yet.

It turns out to be one of our ISDN services for video conferencing. We have temporarily disconnected the line and will investigate the incident further.

Cheers,
--
[redacted]
Network Services
Australian Bureau of Statistics
p: +61 (0)2 6252 [redacted] | m: [redacted] | e: [redacted]@abs.gov.au

"[redacted]"---13/06/2012 09:41:42 AM---Dear Lyn and [redacted] We have detected unusual calling patterns on your Customer Premise Equipment (

From: [redacted]@team.telstra.com>
To: Lyn Little <lyn.little@abs.gov.au>, [redacted]@abs.gov.au>
Cc: [redacted]@team.telstra.com>, [redacted]@team.telstra.com>
Date: 13/06/2012 09:41 AM
Subject: SUSPECT FRAUD ALERT: AUSTRALIAN BUREAU OF STATISTICS

Dear Lyn and [redacted]

We have detected unusual calling patterns on your Customer Premise Equipment (CPE) system.

INCIDENT REPORT:

- **CSI Reference #** CSI-0000063905
- **Customer Name:** AUSTRALIAN BUREAU OF STATISTICS
- **CIDN:** 5111116030
- **Accounts #** [redacted]
- **Service #** [redacted]

Starting **12/6/2012 at 9:51pm** there were **437 suspect calls (199 answered)** to Somalia Hot Number 2524058[redacted], Kuwait Number 965990[redacted] calls to Ethiopia, Senegal, Cuba, Afghanistan, Taiwan, Eritrea, France, Greece, Lebanon, USA, Oman, South Africa, Pakistan, calls to blocked Revenue Share Fraud Codes in Senegal, Zimbabwe, Belarus, Chile and unanswered calls to nine other countries.

The calls entered the CPE on [redacted] and [redacted] and left the CPE on [redacted]

Please ask your maintainer to **check, verify and correct all the service connected to the CPE,** as there could be other numbers or internet access with a security weakness.

WHAT YOU NEED TO KNOW:

- There is no fault with the Telstra Network, rather this message is to alert to you that your Customer Premise Equipment (CPE) may be compromised, and in which case your maintainer will be required to resolve this issue.
- Your maintainer can verify the the extent of the compromise, as other numbers might have a security weakness and the maintainer should check all numbers on the customer's equipment.
- Calls can be viewed on Flexcab pre-bill, unless carried over from another carrier's network by use of an override code. We will indicate if this is the case in the "Incident Report" details.
- Due to Privacy Legislation, Telstra is unable to provide further information other than what is visible on your pre and post bill account.

I will give Lyn a call to discuss.

Kind regards,

[redacted]

[redacted]
Account Executive | Telstra Enterprise & Government
P (02) 6129[redacted] | M [redacted]



---

Free publications and statistics available on www.abs.gov.au

ABS Prebill for service [redacted] as at 20120618-1413 .xlsx

International dialling has also been disabled on the line
Total Hours :

Fraud

| | |
|---|---|
| Fraud Method : | Dishonestly acquiring benefits |
| Type of Loss (if any) : | Financial |
| Specify Other Method : | Toll Fraud |

| | | | |
|---|---|---|---|
| Person Responsible: | | Relation with ABS : | External to the ABS |
| Security Level : | | | |
| Person Responsible: | | Relation with ABS : | |
| Security Level : | | | |
| Person Responsible: | | Relation with ABS : | |
| Security Level : | | | |

Document Access

| | |
|---|---|
| Authors : | [Security Staff], [Security Admin], [redacted]/Staff/ABS |
| Readers : | [Security Staff], [Security Admin], [redacted]/Staff/ABS |

## Related Documents

| Date Created | Doc Type |
|---|---|

## Reminder Information

| | | | |
|---|---|---|---|
| Reminder Sent Date: | 27/06/2012 | Next Reminder: | 04/07/2012 |
| Reminder No.: | 0 | Last Edited Date: | 27/06/2012 |

## Edit History

Report Closed by [redacted] on 27/06/2012 09:00:25 AM
Document Updated by [redacted] on 13/06/2012 03:27:19 PM
Document Updated by [redacted] on 13/06/2012 03:16:00 PM
Document Updated by [redacted] on 13/06/2012 03:11:36 PM
Incident Submitted by [redacted] on 13/06/2012 10:42:47 AM
Incident Created by [redacted] on 13/06/2012 10:22:05 AM

**FLEXCAB SYSTEM ** 18/06/2012
Pre-bill Usage List
Australian Bureau of Statistics
Account: [redacted]
Ser Number [redacted]

| Type | Date | Time | Country Called | Number Called | Duration | Cost |
|---|---|---|---|---|---|---|
| _ ISDN | 12-Jun | 09:52pm | France | 33141104[redacted] | 00:00:05 | 0.27 |
| _ ISDN | 12-Jun | 09:57pm | Kuwait | 96599037[redacted] | 00:00:06 | 0.37 |
| _ ISDN | 12-Jun | 09:58pm | Ethiopia | 25191136[redacted] | 00:00:07 | 0.51 |
| _ ISDN | 12-Jun | 09:58pm | Afghanistan | 93799474[redacted] | 00:06:10 | 14.92 |
| _ ISDN | 12-Jun | 10:08pm | Ethiopia | 25191192[redacted] | 00:35:04 | 83.75 |
| _ ISDN | 12-Jun | 10:12pm | Ethiopia | 25191374[redacted] | 00:00:38 | 1.74 |
| _ ISDN | 12-Jun | 10:16pm | Ethiopia | 25191300[redacted] | 00:05:27 | 13.21 |
| _ ISDN | 12-Jun | 10:16pm | Taiwan | 88695116[redacted] | 00:00:42 | 1.01 |
| _ ISDN | 12-Jun | 10:20pm | Cuba | 53582239[redacted] | 00:03:51 | 4.46 |
| _ ISDN | 12-Jun | 10:30pm | Ethiopia | 25191072[redacted] | 00:13:35 | 32.58 |
| _ ISDN | 12-Jun | 10:32pm | Ethiopia | 25191877[redacted] | 00:02:15 | 5.59 |
| _ ISDN | 12-Jun | 10:32pm | USA Ohio | 19377342[redacted] | 00:00:12 | 0.28 |
| _ ISDN | 12-Jun | 10:42pm | Afghanistan | 93773425[redacted] | 00:10:49 | 25.99 |
| _ ISDN | 12-Jun | 10:50pm | Ethiopia | 25192022[redacted] | 00:00:17 | 0.9 |
| _ ISDN | 12-Jun | 10:52pm | Ethiopia | 25192022[redacted] | 00:00:19 | 0.98 |
| _ ISDN | 12-Jun | 10:53pm | Ethiopia | 25192022[redacted] | 00:00:24 | 1.18 |
| _ ISDN | 12-Jun | 10:55pm | Ethiopia | 25192022[redacted] | 00:01:26 | 3.64 |
| _ ISDN | 12-Jun | 10:57pm | Ethiopia | 25192022[redacted] | 00:02:54 | 7.13 |
| _ ISDN | 12-Jun | 11:00pm | Ethiopia | 25191803[redacted] | 00:00:51 | 2.25 |
| _ ISDN | 12-Jun | 11:02pm | Ethiopia | 25191803[redacted] | 00:03:42 | 9.04 |
| _ ISDN | 12-Jun | 11:06pm | Ethiopia | 25192285[redacted] | 00:01:57 | 4.87 |
| _ ISDN | 12-Jun | 11:09pm | Ethiopia | 25133115[redacted] | 00:32:16 | 77.08 |
| _ ISDN | 12-Jun | 11:09pm | Ethiopia | 25191860[redacted] | 00:03:51 | 9.4 |
| _ ISDN | 12-Jun | 11:15pm | Ethiopia | 25191376[redacted] | 00:02:05 | 5.19 |
| _ ISDN | 12-Jun | 11:16pm | Cuba | 53532743[redacted] | 00:04:18 | 4.96 |
| _ ISDN | 12-Jun | 11:22pm | Cuba | 53422220[redacted] | 00:10:56 | 12.25 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| _ | ISDN | 12-Jun | 11:25pm | Cuba | 53786230 | 00:21:25 | 23.79 |
| _ | ISDN | 12-Jun | 11:26pm | Ethiopia | 25111466 | 00:06:49 | 16.46 |
| _ | ISDN | 12-Jun | 11:26pm | Ethiopia | 25191367 | 00:00:13 | 0.74 |
| _ | ISDN | 12-Jun | 11:27pm | Ethiopia | 25191870 | 00:00:02 | 0.31 |
| _ | ISDN | 12-Jun | 11:29pm | Ethiopia | 25191374 | 00:10:58 | 26.35 |
| _ | ISDN | 12-Jun | 11:30pm | Ethiopia | 25191361 | 00:09:13 | 22.18 |
| _ | ISDN | 12-Jun | 11:40pm | Kuwait | 96597894 | 00:00:05 | 0.35 |
| _ | ISDN | 12-Jun | 11:49pm | Ethiopia | 25191417 | 00:01:18 | 3.32 |
| _ | ISDN | 12-Jun | 11:54pm | Ethiopia | 25191437 | 00:09:38 | 23.17 |
| _ | SEN | 12-Jun | 11:24pm | Sensis 1234 | 1234 | 00:00:11 | 1.59 |
| _ | ISDN | 13-Jun | 12:03am | Cuba | 53413269 | 00:05:49 | 6.63 |
| _ | ISDN | 13-Jun | 12:17am | Ethiopia | 25191197 | 00:22:22 | 53.5 |
| _ | ISDN | 13-Jun | 12:23am | Ethiopia | 25191171 | 00:06:10 | 14.92 |
| _ | ISDN | 13-Jun | 12:31am | Ethiopia | 25191171 | 00:00:07 | 0.51 |
| _ | ISDN | 13-Jun | 12:35am | Ethiopia | 25192832 | 00:01:37 | 4.08 |
| _ | ISDN | 13-Jun | 12:37am | Ethiopia | 25111465 | 00:08:45 | 21.07 |
| _ | ISDN | 13-Jun | 12:37am | Ethiopia | 25191171 | 00:04:15 | 10.35 |
| _ | ISDN | 13-Jun | 12:39am | Ethiopia | 25191167 | 00:09:16 | 22.3 |
| _ | ISDN | 13-Jun | 12:44am | Ethiopia | 25191374 | 00:24:16 | 58.03 |
| _ | ISDN | 13-Jun | 12:47am | Ethiopia | 25191031 | 00:04:41 | 11.38 |
| _ | ISDN | 13-Jun | 12:49am | Ethiopia | 25191237 | 00:00:17 | 0.9 |
| _ | ISDN | 13-Jun | 01:01am | Ethiopia | 25191735 | 00:02:45 | 6.78 |
| _ | ISDN | 13-Jun | 01:01am | Lebanon | 96171675 | 00:01:15 | 1.6 |
| _ | ISDN | 13-Jun | 01:03am | Ethiopia | 25191318 | 00:03:21 | 8.21 |
| _ | ISDN | 13-Jun | 01:08am | Lebanon | 96171675 | 00:14:21 | 16.01 |
| _ | ISDN | 13-Jun | 01:11am | Ethiopia | 25192374 | 00:11:29 | 27.58 |
| _ | ISDN | 13-Jun | 01:11am | Ethiopia | 25191146 | 00:00:44 | 1.97 |
| _ | ISDN | 13-Jun | 01:16am | Ethiopia | 25192365 | 00:02:02 | 5.07 |
| _ | ISDN | 13-Jun | 01:21am | Ethiopia | 25192622 | 00:08:56 | 21.5 |
| _ | ISDN | 13-Jun | 01:21am | Eritrea | 29171266 | 00:08:45 | 21.07 |
| _ | ISDN | 13-Jun | 01:24am | Sri Lanka | 94774311 | 00:14:30 | 12.62 |
| _ | ISDN | 13-Jun | 01:24am | Ethiopia | 25191211 | 00:13:27 | 32.26 |
| _ | ISDN | 13-Jun | 01:26am | Cuba | 53535083 | 00:02:51 | 3.36 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| _ | ISDN | 13-Jun | 01:28am | Cuba | 5353298 | 00:02:16 | 2.72 |
| _ | ISDN | 13-Jun | 01:30am | Cuba | 5353219 | 00:01:44 | 2.13 |
| _ | ISDN | 13-Jun | 01:31am | Cuba | 5352461 | 00:18:14 | 20.28 |
| _ | ISDN | 13-Jun | 01:33am | Cuba | 5372093 | 00:03:00 | 3.53 |
| _ | ISDN | 13-Jun | 01:34am | Cuba | 5353110 | 00:04:09 | 4.79 |
| _ | ISDN | 13-Jun | 01:40am | Cuba | 5347524 | 00:02:18 | 2.76 |
| _ | ISDN | 13-Jun | 01:42am | Cuba | 5353274 | 00:26:44 | 29.63 |
| _ | ISDN | 13-Jun | 01:44am | Ethiopia | 2519130 | 00:00:44 | 1.97 |
| _ | ISDN | 13-Jun | 01:46am | Cuba | 5322633 | 00:16:23 | 18.25 |
| _ | ISDN | 13-Jun | 01:52am | Ethiopia | 2519111 | 00:00:20 | 1.02 |
| _ | ISDN | 13-Jun | 01:54am | Cuba | 5353508 | 00:14:23 | 16.05 |
| _ | ISDN | 13-Jun | 01:57am | Cuba | 5352371 | 00:04:17 | 4.94 |
| _ | ISDN | 13-Jun | 01:58am | Ethiopia | 2519111 | 00:00:42 | 1.89 |
| _ | ISDN | 13-Jun | 01:59am | Cuba | 5352371 | 00:02:24 | 2.87 |
| _ | ISDN | 13-Jun | 02:01am | Greece | 3069439 | 00:04:04 | 3.26 |
| _ | ISDN | 13-Jun | 02:06am | Ethiopia | 2519179 | 00:05:47 | 14 |
| _ | ISDN | 13-Jun | 02:06am | Greece | 3069439 | 00:14:31 | 11.05 |
| _ | ISDN | 13-Jun | 02:08am | Cuba | 5331564 | 00:01:41 | 2.08 |
| _ | ISDN | 13-Jun | 02:09am | Ethiopia | 2519210 | 00:10:13 | 24.56 |
| _ | ISDN | 13-Jun | 02:11am | Ethiopia | 2519114 | 00:09:38 | 23.17 |
| _ | ISDN | 13-Jun | 02:12am | Ethiopia | 2519111 | 00:03:46 | 9.2 |
| _ | ISDN | 13-Jun | 02:17am | Ethiopia | 2519219 | 00:46:48 | 111.7 |
| _ | ISDN | 13-Jun | 02:22am | Cuba | 5378301 | 00:05:21 | 6.11 |
| _ | ISDN | 13-Jun | 02:24am | Cuba | 5353219 | 00:06:20 | 7.19 |
| _ | ISDN | 13-Jun | 02:24am | Ethiopia | 2519231 | 00:01:54 | 4.75 |
| _ | ISDN | 13-Jun | 02:26am | Ethiopia | 2519201 | 00:22:10 | 53.02 |
| _ | ISDN | 13-Jun | 02:27am | Cuba | 5331564 | 00:11:30 | 12.88 |
| _ | ISDN | 13-Jun | 02:40am | Cuba | 5353219 | 00:09:50 | 11.04 |
| _ | ISDN | 13-Jun | 02:42am | Oman | 968989 | 00:00:01 | 0.25 |
| _ | ISDN | 13-Jun | 02:43am | Ethiopia | 2519147 | 00:00:22 | 1.1 |
| _ | ISDN | 13-Jun | 02:44am | Ethiopia | 2519147 | 00:08:49 | 21.23 |
| _ | ISDN | 13-Jun | 02:45am | Ethiopia | 2519204 | 00:27:52 | 66.6 |
| _ | ISDN | 13-Jun | 02:49am | Ethiopia | 2519171 | 00:16:04 | 38.5 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| _ | ISDN | 13-Jun | 02:52am | Cuba | 5358069 | 00:18:55 | 21.04 |
| _ | ISDN | 13-Jun | 02:58am | Cuba | 5353321 | 00:08:26 | 9.5 |
| _ | ISDN | 13-Jun | 02:58am | Ethiopia | 2519173 | 00:15:38 | 37.46 |
| _ | ISDN | 13-Jun | 03:01am | Cuba | 5331513 | 00:00:34 | 0.85 |
| _ | ISDN | 13-Jun | 03:05am | Cuba | 5372658 | 00:08:01 | 9.05 |
| _ | ISDN | 13-Jun | 03:07am | Ethiopia | 2519173 | 00:02:24 | 5.94 |
| _ | ISDN | 13-Jun | 03:11am | Ethiopia | 2519173 | 00:00:41 | 1.85 |
| _ | ISDN | 13-Jun | 03:13am | Cuba | 5358069 | 00:20:19 | 22.58 |
| _ | ISDN | 13-Jun | 03:14am | Ethiopia | 2519205 | 00:01:36 | 4.04 |
| _ | ISDN | 13-Jun | 03:15am | Cuba | 5348772 | 00:10:49 | 12.13 |
| _ | ISDN | 13-Jun | 03:20am | Ethiopia | 2519205 | 00:09:08 | 21.98 |
| _ | ISDN | 13-Jun | 03:21am | Ethiopia | 2519101 | 00:00:55 | 2.41 |
| _ | ISDN | 13-Jun | 03:22am | Pakistan | 9230761 | 00:03:00 | 5.08 |
| _ | ISDN | 13-Jun | 03:22am | Cuba | 5352940 | 00:28:42 | 31.8 |
| _ | ISDN | 13-Jun | 03:23am | Cuba | 5341675 | 00:18:42 | 20.8 |
| _ | ISDN | 13-Jun | 03:24am | Ethiopia | 2519101 | 00:09:15 | 22.26 |
| _ | ISDN | 13-Jun | 03:26am | Cuba | 5343569 | 00:45:23 | 50.15 |
| _ | ISDN | 13-Jun | 03:32am | Somalia | 2524058 | 00:00:01 | 0.27 |
| _ | ISDN | 13-Jun | 03:36am | Ethiopia | 2519242 | 00:08:50 | 21.27 |
| _ | ISDN | 13-Jun | 03:40am | Cuba | 5352890 | 00:03:53 | 4.5 |
| _ | ISDN | 13-Jun | 03:41am | Ethiopia | 2519116 | 00:17:50 | 42.7 |
| _ | ISDN | 13-Jun | 03:42am | Cuba | 5358069 | 00:16:52 | 18.78 |
| _ | ISDN | 13-Jun | 03:44am | Cuba | 5353779 | 00:08:42 | 9.8 |
| _ | ISDN | 13-Jun | 03:46am | Ethiopia | 2519242 | 00:07:07 | 17.18 |
| _ | ISDN | 13-Jun | 03:49am | Ethiopia | 2519130 | 00:03:15 | 7.97 |
| _ | ISDN | 13-Jun | 03:55am | Cuba | 5378631 | 00:03:04 | 3.6 |
| _ | ISDN | 13-Jun | 03:57am | Cuba | 5333636 | 00:16:58 | 18.89 |
| _ | ISDN | 13-Jun | 03:58am | Cuba | 5353224 | 00:12:54 | 14.42 |
| _ | ISDN | 13-Jun | 03:58am | Ethiopia | 2519271 | 00:01:14 | 3.16 |
| _ | ISDN | 13-Jun | 03:59am | Ethiopia | 2511112 | 00:07:53 | 19 |
| _ | ISDN | 13-Jun | 04:03am | Ethiopia | 2519271 | 00:09:29 | 22.81 |
| _ | ISDN | 13-Jun | 04:07am | Cuba | 5353533 | 00:03:28 | 4.04 |
| _ | ISDN | 13-Jun | 04:11am | Cuba | 5372900 | 00:00:06 | 0.34 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| _ | ISDN | 13-Jun | 04:13am | Cuba | 5352520[redacted] | 00:20:51 | 23.16 |
| _ | ISDN | 13-Jun | 04:21am | Cuba | 5352400[redacted] | 00:00:07 | 0.36 |
| _ | ISDN | 13-Jun | 04:24am | Cuba | 5358067[redacted] | 00:00:11 | 0.43 |
| _ | ISDN | 13-Jun | 04:25am | Cuba | 5358067[redacted] | 00:02:42 | 3.2 |
| _ | ISDN | 13-Jun | 04:27am | Cuba | 5352400[redacted] | 00:01:32 | 1.91 |
| _ | ISDN | 13-Jun | 04:29am | Ethiopia | 2519268[redacted] | 00:04:31 | 10.99 |
| _ | ISDN | 13-Jun | 04:30am | Cuba | 5376443[redacted] | 00:03:33 | 4.13 |
| _ | ISDN | 13-Jun | 04:30am | Eritrea | 2911400[redacted] | 00:07:42 | 18.57 |
| _ | ISDN | 13-Jun | 04:30am | Cuba | 5321382[redacted] | 00:00:22 | 0.63 |
| _ | ISDN | 13-Jun | 04:32am | Cuba | 5342499[redacted] | 00:33:45 | 37.35 |
| _ | ISDN | 13-Jun | 04:32am | South Afric | a 277825[redacted] | 00:00:48 | 1.01 |
| _ | ISDN | 13-Jun | 04:32am | Ethiopia | 2519134[redacted] | 00:08:37 | 20.75 |
| _ | ISDN | 13-Jun | 04:36am | Ethiopia | 2519103[redacted] | 00:07:57 | 19.16 |
| _ | ISDN | 13-Jun | 04:38am | Ethiopia | 2511141[redacted] | 00:30:11 | 72.12 |
| _ | ISDN | 13-Jun | 04:41am | Cuba | 5352825[redacted] | 00:06:56 | 7.85 |
| _ | ISDN | 13-Jun | 04:47am | Ethiopia | 2519101[redacted] | 00:01:18 | 3.32 |
| _ | ISDN | 13-Jun | 04:48am | Cuba | 5342883[redacted] | 00:00:21 | 0.61 |
| _ | ISDN | 13-Jun | 04:49am | Cuba | 5352825[redacted] | 00:14:32 | 16.21 |
| _ | ISDN | 13-Jun | 04:54am | Cuba | 5352368[redacted] | 00:19:38 | 21.82 |
| _ | ISDN | 13-Jun | 04:55am | Ethiopia | 2519118[redacted] | 00:27:36 | 65.97 |
| _ | ISDN | 13-Jun | 04:55am | Ethiopia | 2519137[redacted] | 00:00:22 | 1.1 |
| _ | ISDN | 13-Jun | 04:57am | Ethiopia | 2519137[redacted] | 00:09:13 | 22.18 |
| _ | ISDN | 13-Jun | 05:05am | Cuba | 5347854[redacted] | 00:05:13 | 5.97 |
| _ | ISDN | 13-Jun | 05:05am | Cuba | 5342883[redacted] | 00:16:15 | 18.1 |
| _ | ISDN | 13-Jun | 05:12am | Cuba | 5347854[redacted] | 00:06:55 | 7.84 |
| _ | ISDN | 13-Jun | 05:13am | Cuba | 5372602[redacted] | 00:07:59 | 9.01 |
| _ | ISDN | 13-Jun | 05:17am | Ethiopia | 2519217[redacted] | 00:01:10 | 3.01 |
| _ | ISDN | 13-Jun | 05:21am | Senegal | 2217753[redacted] | 00:06:41 | 16.15 |
| _ | ISDN | 13-Jun | 05:23am | Cuba | 5372602[redacted] | 00:12:06 | 13.54 |
| _ | ISDN | 13-Jun | 05:24am | Cuba | 5353759[redacted] | 00:06:36 | 7.49 |
| _ | ISDN | 13-Jun | 05:25am | Cuba | 5342883[redacted] | 00:17:51 | 19.86 |
| _ | ISDN | 13-Jun | 05:27am | Ethiopia | 2519103[redacted] | 00:02:34 | 6.34 |
| _ | ISDN | 13-Jun | 05:29am | Ethiopia | 2519120[redacted] | 00:00:32 | 1.5 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| _ | ISDN | 13-Jun | 05:30am | Senegal | 221775364 | 00:08:40 | 20.87 |
| _ | ISDN | 13-Jun | 05:31am | Cuba | 535293919 | 00:25:56 | 28.75 |
| _ | ISDN | 13-Jun | 05:32am | Ethiopia | 251913721 | 00:02:58 | 7.29 |
| _ | ISDN | 13-Jun | 05:34am | Ethiopia | 251910041 | 00:14:23 | 34.49 |
| _ | ISDN | 13-Jun | 05:36am | Cuba | 535350415 | 00:18:35 | 20.67 |
| _ | ISDN | 13-Jun | 05:38am | Cuba | 535330358 | 00:03:46 | 4.37 |
| _ | ISDN | 13-Jun | 05:40am | Ethiopia | 251912702 | 00:08:13 | 19.8 |
| _ | ISDN | 13-Jun | 05:42am | Ethiopia | 251912044 | 00:48:40 | 116.14 |
| _ | ISDN | 13-Jun | 05:44am | Cuba | 535343736 | 00:00:45 | 1.05 |
| _ | ISDN | 13-Jun | 05:47am | Cuba | 537209451 | 00:00:01 | 0.25 |
| _ | ISDN | 13-Jun | 05:48am | Cuba | 537861091 | 00:07:44 | 8.73 |
| _ | ISDN | 13-Jun | 05:53am | Ethiopia | 251911371 | 00:12:17 | 29.48 |
| _ | ISDN | 13-Jun | 05:57am | Cuba | 534166354 | 00:15:57 | 17.77 |
| _ | ISDN | 13-Jun | 06:00am | Cuba | 535347481 | 00:13:01 | 14.55 |
| _ | ISDN | 13-Jun | 06:05am | Ethiopia | 251912604 | 00:21:56 | 52.47 |
| _ | ISDN | 13-Jun | 06:07am | Cuba | 537763568 | 00:00:21 | 0.61 |
| _ | ISDN | 13-Jun | 06:09am | Cuba | 537763568 | 00:09:21 | 10.51 |
| _ | ISDN | 13-Jun | 06:11am | Cuba | 535275849 | 00:13:08 | 14.67 |
| _ | ISDN | 13-Jun | 06:15am | Ethiopia | 251917324 | 00:07:01 | 16.94 |
| _ | ISDN | 13-Jun | 06:18am | Cuba | 535312940 | 00:13:01 | 14.55 |
| _ | ISDN | 13-Jun | 06:18am | Eritrea | 291820615 | 00:05:35 | 13.53 |
| _ | ISDN | 13-Jun | 06:22am | Cuba | 535354268 | 00:09:46 | 10.97 |
| _ | ISDN | 13-Jun | 06:25am | Cuba | 537794729 | 00:12:33 | 14.03 |
| _ | ISDN | 13-Jun | 06:27am | Cuba | 534561075 | 00:03:05 | 3.62 |
| _ | ISDN | 13-Jun | 06:28am | Cuba | 535377384 | 00:11:57 | 13.37 |
| _ | ISDN | 13-Jun | 06:32am | Cuba | 534561075 | 00:06:20 | 7.19 |
| _ | ISDN | 13-Jun | 06:35am | Ethiopia | 251912604 | 00:09:57 | 23.93 |
| _ | ISDN | 13-Jun | 06:48am | Cuba | 537694342 | 00:05:10 | 5.91 |
| _ | ISDN | 13-Jun | 06:55am | Oman | 968961530 | 00:09:15 | 12.84 |
| _ | ISDN | 13-Jun | 06:55am | Cuba | 537265835 | 00:26:07 | 28.96 |
| _ | ISDN | 13-Jun | 06:58am | Cuba | 532263473 | 00:09:32 | 10.71 |
| _ | ISDN | 13-Jun | 06:59am | Cuba | 537762678 | 00:15:48 | 17.61 |
| _ | ISDN | 13-Jun | 07:03am | Cuba | 535380989 | 00:05:05 | 5.82 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| _ | ISDN | 13-Jun | 07:14am | Cuba | 53533091[redacted] | 00:05:27 | 6.22 |
| _ | ISDN | 13-Jun | 07:24am | Cuba | 53422142[redacted] | 00:44:48 | 49.51 |
| _ | ISDN | 13-Jun | 07:27am | Cuba | 53533737[redacted] | 00:22:50 | 25.34 |
| _ | ISDN | 13-Jun | 07:40am | Cuba | 53580718[redacted] | 00:05:42 | 6.5 |
| _ | ISDN | 13-Jun | 07:44am | Cuba | 53315133[redacted] | 00:02:32 | 3.01 |
| _ | ISDN | 13-Jun | 07:48am | Cuba | 53315133[redacted] | 00:05:30 | 6.28 |
| _ | ISDN | 13-Jun | 07:48am | Cuba | 53531893[redacted] | 00:07:58 | 8.99 |
| _ | ISDN | 13-Jun | 07:55am | Cuba | 53528942[redacted] | 00:03:21 | 3.91 |

Report a crime to the AFP - AFP website form submission
do-not-reply
to:
[redacted]
15/06/2012 10:38 AM
EPM:
DOCUMENT NOT YET CLASSIFIED more info..,
Hide Details
From: do-not-reply@afp.gov.au
To: [redacted]@abs.gov.au,

The following details were submitted via the AFP website:
Reason for email: Request AFP action
Details: On Tuesday night 12/06 we (the Australian Bureau of Statistics) have had a Toll Fraud incident on the ISDN line coming into our Polycom RMX.Starting at 12/6/2012 at 9:51 there were 437 suspect calls to Somalia Hot Number 2524058[redacted], Kuwait Number 965990[redacted] and many other countries. The calls entered the ABS on [redacted] and [redacted] and left the ABS on [redacted] This is an Telstra ISDN circuit connected to out Polycom RMX Video Confrencing Bridge.We have disconneeted the outside ISDN line while we investigate the incident.We require an AFP police reference number for insurance purposes. I have also logged this with DSD.Cheers,[redacted]IT SecurityAustralian Bureau of Statistics

When submitting forms to the AFP, please use either Microsoft Internet Explorer or Mozilla FirePox browsers

## Email AFP - Report a Commonwealth crime

**Before completing this form, please** read information on reporting a Commonwealth crime.

**Are you reporting online child sex exploitation? Please go to the** online child sex exploitation form.

* indicates mandatory fields - complete these to submit the email form.

**Please note: An error has been identified that prevents some forms from being submitted. Please remove single quotes or apostrophes (For example O'connell, police officer's, etc.) and ampersands (&).**

Are you reporting a Commonwealth crime?
What are Commonwealth crimes?

Yes, I am reporting a Commonwealth crime

Details*
(limit of 5000 characters)

On Tuesday night 12/6 we (the Australian Bureau of Statistics) have had a Toll fraud incident on the ISDN line coming into our Polycom RMX.
Starting at 12/6/2012 at 9:51 there were 137 suspect calls to Somalia Hot Number 252705[redacted], Kuwait Number 965990[redacted] and many other countries. The calls entered the ABS on 03[redacted] and 02[redacted] and left the ABS on 02[redacted]. This is an Telstra ISDN circuit connected to our Polycom RMX Video Conferecing Bridge.

We have disconnected the outside ISDN line while we investigate the incident.

We require an AFP police reference number for insurance purposes. I have also logged this with DSD.

Cheers,

Reason for email*

- Provide information
- Request AFP action

### Your contact details

Contact name: [redacted]
Date of birth: 05/10/1977
Email address*: [redacted]@abs.gov.au
Confirm email address*: [redacted]@abs.gov.au
Phone number: 026252[redacted]
Postal address: Australian Bureau of Statistics, Locked Bag 10, Belconnen, ACT
State/Territory*: ACT

### Acceptance of the AFP's Privacy Statement

Privacy Statement Acceptance*
I have read and understood the AFP's Privacy Statement. I understand that the information and other private data which the AFP obtains may be used for the purposes of identifying me, sharing with other law enforcement and government agencies or for criminal investigations and/or legal proceedings

Yes, I understand and accept the AFP's Privacy Statement

Submit | Clear Form

**Police report details**
Lyn Little to: [redacted] [redacted] 15/06/2012 02:01 PM
EPM: UNCLASSIFIED more info...
This message is digitally signed.

The AFP job number is: 5042610

The investigating officer is [redacted]@afp.gov.au

Please use this on Insurance and update SIRS.

**Lyn Little**
*Director*
Network Services | Technical Services Division | **Australian Bureau of Statistics**
**(P) (02) 6252[redacted] (M)** [redacted]
**(E) Lyn.Little@abs.gov.au (W) www.abs.gov.au**

**From:** [redacted]
**Sent:** Wednesday, 13 June 2012 10:34 AM
**To:** [redacted]
**Cc:** Lyn Little; [redacted]
**Subject:** RE: SUSPECT FRAUD ALERT: AUSTRALIAN BUREAU OF STATISTICS [SEC=UNCLASSIFIED]

Dear Lyn and [redacted]

Thank you for such prompt action – I'm glad ABS were able to take such decisive action to minimise future risks.

As discussed briefly with Lyn, below are the links to the AFP contact you may require as part of your process:

**Report fraud incident to the Police**
All CPE Fraud should be **reported to the Australian Federal Police** (AFP):

- AFP Operations Monitoring Centre in their state via the **AFP website**.
- Fraud incident reports must be done in writing either via email, mail or fax, as per the **instructions on the AFP** site.

The AFP will provide a reference number for insurance purposes.

Lyn, regarding the other part of your question, the charges for the calls will not have arrived in our billing systems yet (last night is too soon). We don't expect this to happen until about next week – [redacted] or [redacted] will provide you the billing information as soon as they obtain it.

Kind regards,
[redacted]

[redacted]
Account Executive | Telstra Enterprise & Government
P (02) 6129[redacted] | M [redacted]

**From:** [redacted]@abs.gov.au]
**Sent:** Wednesday, 13 June 2012 9:57 AM
**To:** [redacted]
**Cc:** Lyn Little; [redacted]
**Subject:** Re: SUSPECT FRAUD ALERT: AUSTRALIAN BUREAU OF STATISTICS [SEC=UNCLASSIFIED]

Hello [redacted] and colleagues,

Lyn is not in the office yet.

It turns out to be one of our ISDN services for video conferencing. We have temporarily disconnected the line and will investigate the incident further.

Cheers,
--
[redacted]
Network Services
Australian Bureau of Statistics
p: +61 (0)2 6252[redacted] | m: [redacted] | e: [redacted]@abs.gov.au

[redacted]---13/06/2012 09:41:42 AM---Dear Lyn and [redacted] We have detected unusual calling patterns on your Customer Premise Equipment (

RE: SUSPECT FRAUD ALERT: AUSTRALIAN BUREAU OF STATISTICS [SEC=UNCLASSIFIED]

[redacted]
to:
[redacted]
19/06/2012 11:44 AM
EPM:
UNCLASSIFIED more info...
Hide Details
From: [redacted]@afp.gov.au>
To: [redacted]@abs.gov.au>,
Security:
To ensure privacy, images from remote sites were prevented from downloading. Show Images

6 Attachments

afpcorporatesignature.gif 0F959534.jpg 0F426430.jpg 0F513960.gif 0F340605.gif 0F174602.jpg

[redacted]

Information added to the job.

Regards

**SENIOR CONSTABLE** [redacted]
OPERATIONS MONITORING CENTRE
ACT POLICING
Tel +61(0) 2 6256[redacted] Fax +61(0) 2 6256[redacted]
www.afp.gov.au

---

**From:** [redacted]@abs.gov.au]
**Sent:** Monday, 18 June 2012 3:47 PM
**To:** [redacted]
**Cc:** Lyn Little
**Subject:** Fw: SUSPECT FRAUD ALERT: AUSTRALIAN BUREAU OF STATISTICS [SEC=IN-CONFIDENCE:SECURITY]

[redacted]

See below for updated information from Telstra.

Cheers,

[redacted]

*Ag IT Security Advisor / TSD Change Manager*

IT Security | Technology Services Division | **Australian Bureau of Statistics**

**(P) (02) 6252[redacted] (M)[redacted]**

**(E)** [redacted]**@abs.gov.au (W) www.abs.gov.au**
----- Forwarded by [redacted] Staff/ABS on 18/06/2012 03:41 PM -----

sender of its incorrect delivery, and then delete both it and your reply.

---

Free publications and statistics available on www.abs.gov.au

*(See attached file: ABS Prebill for service 02625 as at 20120618-1413 .xlsx)*

---

Free publications and statistics available on www.abs.gov.au

SIRs -Prod v2.0

# Incident Report

v 1.0

Incident : Illegal access to IT Network - external (hacking)
Date Reported : 02/01/2013

Status : Closed - Resolved

Document ID : NFIK-93K5HF

## Reporter Details

Reported By : [redacted]/Staff/ABS
Created By : [redacted]/Staff/ABS
Office : CO
Section : Network Services
Branch : Technology Infrastructure Delivery
Division : Technology Services Division
Phone : (02) 6252[redacted]
Location : CO 1S 333

## Incident Occurred

Incident Start date : Wed 26/12/2012
Incident End Date (if over a period) : Wed 26/12/2012

Start Time : 04:46 PM
End Time : 04:47 PM

State/Office Where Incident Occurred : CO
Where did the Incident Occur? ● Office ○ Outside Office

Describe the Location :

## Description

Tell us what happened :
Please provide short explanation of the incident including any information that could assist in its resolution such as the names of witnesses or contributing circumstances.

➲ Attempt to access server WebProd1021 from IP address [redacted] using userid's (root, user, manager, tomcat, and admin)

Details :
Has property been Stolen/Lost/Damaged/Destroyed? ○ Yes ● No

Details of people responsible for the incident
If known, please enter the names and addresses of people responsible for the incident.

Name : Address :

Was any body injured? : ○ Yes ○ No ● Not Applicable

Signature - Signed by Chris Soczynski/Staff/ABS on 02/01/2013 02:27:10 PM, according to /ABS

First Created By : [redacted] On : 02/01/2013 02:02:45 PM

Police Involvement

Police involvement information is not required for this Incident.
Were police called? : ○ Yes ● No

Administration

Investigator/s: Chris Soczynski/Staff/ABS,
Investigation Started:

Wed 02/01/2013

Investigation Ended: Wed 02/01/2013

## General

Security Description : Unauthorised Access
Security Incident : to ABS IT Network
Incident Rating : Low

Summary of the Security Action taken :
Please provide summary of the action taken including any doclinks to relevant documents.This is part is to be filled when the investigation is completed.
Refer to response document created. Chris S
Total Hours : 0.25

## Fraud

Fraud Method :
Type of Loss (if any) :
Specify Other Method :

Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :

## Document Access

Authors : [Security Staff], [Security Admin]
Readers : [Security Staff], [Security Admin]

## Related Documents

| Date Created | Doc Type | |
|---|---|---|
| 02/01/2013 | Response By | CN=Chris Soczynski/OU=Staff/O=ABS |

## Reminder Information

Reminder Sent Date:
Reminder No.: 0

Next Reminder: 09/01/2013
Last Edited Date: 02/01/2013

## Edit History

Report Closed by Chris Soczynski on 02/01/2013 02:27:11 PM
Document Updated by Chris Soczynski on 02/01/2013 02:25:56 PM
Report Registered by [redacted] on 02/01/2013 02:05:32 PM
Incident Submitted by [redacted] on 02/01/2013 02:05:21 PM
Incident Created by [redacted] on 02/01/2013 02:02:54 PM

SIRs-Prod v2.0

# Response

v 1.0

Document ID : NFIK-93K5L9
Response from : Chris Soczynski/Staff/ABS

Doclink :
Date Response Created : 02/01/2013

Comments :

ip address belongs to a network managed in China

route: [redacted]
descr: China Mobile communications corporation
origin: AS9808
mnt-by: MAINT-CN-CMCC
changed: [redacted]@chinamobile.com 20120215
source: APNIC

person: [redacted]
nic-hdl: MC285-AP
e-mail: [redacted]@cq.chinamobile.com
address: [redacted] keyuan, high-tech, industrial zone, Chongqing,400041
phone: +86-[redacted]
fax-no: +86-[redacted]
country: cn
changed: [redacted]@chinamobile.com 20040625
mnt-by: MAINT-NEW
source: APNIC

No further action is required at this time. If this activity becomes persistent, then I will recommend blocking the address range at the perimeter router.

Tell us what happened :
Please provide short explanation of the incident including any information that could assist in its resolution such as the names of witnesses or contributing circumstances.

➲ Attempt to access server WebProd1020 from IP address [redacted] using userid's "manager, tomcat and admin).

Details :
Has property been Stolen/Lost/Damaged/Destroyed? ○ Yes ● No

Details of people responsible for the incident
If known, please enter the names and addresses of people responsible for the incident.

Name : Address :

Was any body injured? : ○ Yes ○ No ● Not Applicable

Signature - Signed by Chris Soczynski/Staff/ABS on 02/01/2013 02:23:50 PM, according to /ABS

First Created By : [redacted] On : 02/01/2013 01:58:15 PM

Police Involvement

Police involvement information is not required for this Incident.
Were police called? : ○ Yes ● No

Administration

Investigator/s: Chris Soczynski/Staff/ABS,
Investigation Started:

Wed 02/01/2013

Investigation Ended: Wed 02/01/2013

## General

Security Description : Unauthorised Access
Security Incident : to ABS IT Network
Incident Rating : Low

Summary of the Security Action taken :
Please provide summary of the action taken including any doclinks to relevant documents.This is part is to be filled when the investigation is completed.
Refer to response document created. Chris S.
Total Hours : 0.25

## Fraud

Fraud Method :
Type of Loss (if any) :
Specify Other Method :

Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :

## Document Access

Authors : [Security Staff], [Security Admin]
Readers : [Security Staff], [Security Admin]

## Related Documents

| Date Created | Doc Type | |
|---|---|---|
| 02/01/2013 | Response By | CN=Chris Soczynski/OU=Staff/O=ABS |

## Reminder Information

Reminder Sent Date:
Reminder No.: 0

Next Reminder: 09/01/2013
Last Edited Date: 02/01/2013

## Edit History

Report Closed by Chris Soczynski on 02/01/2013 02:23:50 PM
Report Registered by [redacted] on 02/01/2013 02:01:32 PM
Incident Submitted by [redacted] on 02/01/2013 02:01:18 PM
Incident Created by [redacted] on 02/01/2013 01:59:01 PM

Document ID : NFIK-93K5HF
Response from : Chris Soczynski/Staff/ABS

Doclink :
Date Response Created : 02/01/2013

Comments :

ip address belongs to a network managed in China

route: [redacted]
descr: China Mobile communications corporation
origin: AS9808
mnt-by: MAINT-CN-CMCC
changed: [redacted]@chinamobile.com 20120215
source: APNIC

person: [redacted]
nic-hdl: MC285-AP
e-mail: [redacted]@cq.chinamobile.com
address: [redacted] keyuan, high-tech, industrial zone, Chongqing,400041
phone: +86-[redacted]
fax-no: +86-[redacted]
country: cn
changed: [redacted]@chinamobile.com 20040625
mnt-by: MAINT-NEW
source: APNIC

No further action is required at this time. If this activity becomes persistent, then I will recommend blocking the address range at the perimeter router.

SIRs -Prod v2.0

# Incident Report

v 1.0

Incident : Other
Date Reported : 07/12/2012

Status : Closed - Resolved

Document ID : PMAZ-92R677

## Reporter Details

Reported By : [redacted] Staff/ABS
Created By : [redacted] Staff/ABS
Office : VIC
Section : Technology Infrastructure Delivery (Vic)
Branch : Technology Services (Vic)
Division : Technology Services Division
Phone : (03) 9615 [redacted]
Location : VIC 5 256

## Incident Occurred

Incident Start date : Thu 06/12/2012
Incident End Date (if over a period) : Thu 06/12/2012

Start Time : 12:45 AM
End Time : 01:00 AM

State/Office Where Incident Occurred : VIC
Where did the Incident Occur? ● Office ○ Outside Office

Describe the Location : buffer overflow attempt ?

Other, was selected as part of Incident:
Please explain Security Description :

## Description

**Tell us what happened :**
Please provide short explanation of the incident including any information that could assist in its resolution such as the names of witnesses or contributing circumstances.

---

➲ Access using illegal characters... Buffer overflow attempt ? Just registering this in case there is more occurrences.

| Agent Id | Agent DateTime | Full Message |
|---|---|---|
| SHORTFIN | 2012-12-06 18:04:43 EST | (SERVER: WebProd1050/SVR/ABSWebProd) Warning(low): nHTTP: aball [redacted] authentication failure using internet password^^ |
| GREATWHITE | 2012-12-06 18:13:58 EST | (SERVER: WebProd1070/SVR/ABSWebProd) Warning(low): nHTTP: RUSSLA_DETAIL [redacted] authentication failure using internet |
| ELEPHANTNOSE | 2012-12-06 00:58:51 EST | (SERVER: WebProd1020/SVR/ABSWebProd) Warning(low): nHTTP: @^Y@.@o&,2,**2]pq{]vk@-1{'@]vo-/&1(,1.,(1&&@.(& [redacted] authentication failure using internet password^^ |
| ELEPHANTNOSE | 2012-12-06 01:04:56 EST | (SERVER: WebProd1020/SVR/ABSWebProd) Warning(low): nHTTP: @^Y@.@~q]wpmymzz2,&,2]pq{]vk@-1('@]vo-/&1(,1.,-1.*'@./&[redacted] authentication failure using |
| ELEPHANTNOSE | 2012-12-06 03:01:10 EST | (SERVER: WebProd1020/SVR/ABSWebProd) Warning(low): nHTTP: @^Y@.@~q]wpmymzz2,&,2]pq{]vk@-1('@]vo-,}1.(-1.,*1-.+@./* [redacted] authentication failure |
| SHORTFIN | 2012-12-06 12:21:07 EST | (SERVER: WebProd1050/SVR/ABSWebProd) Warning(low): nHTTP: mab[redacted] [redacted] authentication failure using internet password^^ |
| SHORTFIN | 2012-12-06 12:04:06 EST | (SERVER: WebProd1050/SVR/ABSWebProd) Warning(low): nHTTP: danny.[redacted] [redacted] authentication failure using internet password^^ |
| SHORTFIN | 2012-12-06 12:06:32 EST | (SERVER: WebProd1050/SVR/ABSWebProd) Warning(low): nHTTP: danny.[redacted]@[redacted] [redacted] authentication failure using internet password^^ |
| SHORTFIN | 2012-12-06 12:03:57 EST | (SERVER: WebProd1050/SVR/ABSWebProd) Warning(low): nHTTP: danny[redacted] [redacted] authentication failure using internet password^^ |
| SHORTFIN | 2012-12-06 12:04:23 EST | (SERVER: WebProd1050/SVR/ABSWebProd) Warning |

Details :
Has property been Stolen/Lost/Damaged/Destroyed? ○ Yes ● No

Details of people responsible for the incident
If known, please enter the names and addresses of people responsible for the incident.

Name : Address :

Was any body injured? : ○ Yes ○ No ● Not Applicable

Signature - Signed by [redacted] Staff/ABS on 14/12/2012 07:59:37 AM, according to /Staff/ABS

First Created By : [redacted] On : 07/12/2012 02:33:03 PM

## Police Involvement

Police involvement information is not required for this incident.
Were police called? : ○ Yes ● No

## Administration

Investigator/s:

Investigation Started:

Investigation Ended: Fri 14/12/2012

General

Security Description : Other
Security Incident : other
Incident Rating :

Summary of the Security Action taken :
Please provide summary of the action taken including any doclinks to relevant documents.This is part is to be filled when the investigation is completed.
nothing further noted; closing
Total Hours :

Fraud

Fraud Method :
Type of Loss (if any) :
Specify Other Method :

Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :

Document Access

Authors : [Security Staff], [Security Admin]
Readers : [Security Staff], [Security Admin]

Related Documents

| Date Created | Doc Type |
| --- | --- |

Reminder Information

| | | | |
| --- | --- | --- | --- |
| Reminder Sent Date: | 14/12/2012 | Next Reminder: | 21/12/2012 |
| Reminder No.: | 0 | Last Edited Date: | 14/12/2012 |

Edit History

Report Closed by [redacted] on 14/12/2012 07:59:36 AM
Incident Submitted by [redacted] on 07/12/2012 02:40:34 PM
Incident Created by [redacted] on 07/12/2012 02:35:21 PM

SIRs -Prod v2.0

# Incident Report

v 1.0

Incident : Illegal access to IT Network - external (hacking)
Date Reported : 12/11/2012

Status : Closed - Resolved

Document ID : TMMS-8ZXVFP

## Reporter Details

Reported By : [redacted] Staff/ABS
Created By : [redacted] Staff/ABS
Office : CO
Section : Enterprise Systems and Software Management
Branch : Technology Infrastructure Delivery
Division : Technology Services Division
Phone : (02) 6252[redacted]
Location : CO 1S 432

## Incident Occurred

Incident Start date : Fri 09/11/2012
Incident End Date (if over a period) : Fri 09/11/2012

Start Time : 11:01 PM
End Time : 11:01 PM

State/Office Where Incident Occurred : CO
Where did the Incident Occur? ○ Office ● Outside Office
Describe the Location : ABS House internet gateway

## Description

Tell us what happened :
Please provide short explanation of the incident including any information that could assist in its resolution such as the names of witnesses or contributing circumstances.

This is a similar attack to (Subject: Incident Report; Database: SIRS Database; Author: [redacted] Created: 29/10/2012) being an unauthorised attempt to access services provided by ABSWebprod (server Monkfish).

For mor information: (Subject: SOC-20121112-01 - Notes Attack [SEC=IN-CONFIDENCE:SECURITY]; Database: Security Operations Centre WDB; Author: [redacted] Created: 12/11/2012; Doc Ref: TMMS-8ZXUAV)

Details :
Has property been Stolen/Lost/Damaged/Destroyed? ○ Yes ● No

Details of people responsible for the incident
If known, please enter the names and addresses of people responsible for the incident.

Name : Address :

Was any body injured? : ○ Yes ○ No ● Not Applicable

Signature - Signed by [redacted] Staff/ABS on 14/11/2012 09:34:56 AM, according to /ABS

First Created By : [redacted] On : 12/11/2012 10:24:17 AM

Police Involvement

Police involvement information is not required for this incident.

SOC-20121112-01 - Notes Attack [SEC=IN-CONFIDENCE:SECURITY]
Security Operations Centre WDB [redacted] 12/11/2012 09:25 AM

# SECURITY-IN-CONFIDENCE

Basics

| Protective Mark | SECURITY-IN-CONFIDENCE |
|---|---|

Attack Information

## 1. Summary of attack

| Executive Summary |
|---|
| This is an unauthorised attempt to access ABSWebProd |

| Start Time | End Time | Total Attempts | Successful Attemp |
|---|---|---|---|
| 2012-11-09 11:01:35 pm | 2012-11-09 11:01:35 pm | 53 | 0 |

## 2. Target of attack

| Target IP | Ports |
|---|---|
| Monkfish | |

## 3. About the attacker

| Source IP | Ports |
|---|---|

```
% APNIC found the following authoritative answer from:
whois.apnic.net
% [whois.apnic.net node-1]
% Whois data copyright terms
http://www.apnic.net/db/dbcopyright.html

inetnum:        [redacted]
netname:        ZiBoLinZiinfocenter
country:        CN
descr:          ZiBo LinZi Information Center
descr:          Information services enterprise
descr:          Construct information network □provide
common information services
descr:          Linzi County, Zibo,2563000
admin-c:        JS686-AP
```

```
tech-c:         CT74-AP
status:         ASSIGNED NON-PORTABLE
changed:        [redacted]@chinamobile.com 20030701
mnt-by:         MAINT-CN-CMCC
source:         APNIC

route:          [redacted]
descr:          China Mobile communications corporation
origin:         AS9808
mnt-by:         MAINT-CN-CMCC
changed:        [redacted]@chinamobile.com 20120215
source:         APNIC
```

4. Attack profile

5. Attack description

| Attack description |
| --- |
| |

6 [redacted] Report

Out of scope
- automated reports


SOC-20121112-01 - Notes Attack.xlsx SOC-20121112-01 - Monkfish traffic.csv

| Security Incident Report Information |
| --- |
| |

| Gateway Incident Report Information |
| --- |
| |

| ABS Results |
| --- |
| No further action is required. |

Were police called? : ○ Yes ● No

## Administration

Investigator/s: [redacted] Staff/ABS,
Investigation Started: Wed 14/11/2012
Investigation Ended: Wed 14/11/2012

### General

Security Description : Unauthorised Access
Security Incident : to ABS IT Network
Incident Rating :

Summary of the Security Action taken :
Please provide summary of the action taken including any doclinks to relevant documents.This is part is to be filled when the investigation is completed.

Total Hours :

### Fraud

Fraud Method :
Type of Loss (if any) :
Specify Other Method :

Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :

Document Access

Authors : [Security Staff], [Security Admin]
Readers : [Security Staff], [Security Admin]

Related Documents

| Date Created | Doc Type | |
|---|---|---|
| 14/11/2012 | Response By | CN=[redacted] OU=Staff/O=ABS |

Reminder Information

Reminder Sent Date:
Reminder No.: 0
Next Reminder: 21/11/2012
Last Edited Date: 14/11/2012

Edit History

Report Closed by [redacted] on 14/11/2012 09:34:54 AM
Response Document Created/Updated by NotesACT07 on 14/11/2012 09:34:36 AM
Report Under Investigation by [redacted] on 14/11/2012 09:33:36 AM
Report Registered by [redacted] on 14/11/2012 09:33:23 AM
Incident Submitted by [redacted] on 12/11/2012 10:32:09 AM

Incident Created by [redacted] on 12/11/2012 10:24:44 AM

# Response



Document ID : TMMS-8ZXVFP
Response from : [redacted] Staff/ABS
Comments :
Adhoc attack, and all of their request failed. Nothing further to add.

Doclink :
Date Response Created : 14/11/2012

eSIRs -Prod v2.0

# Incident Report

v 1.0

Incident : Illegal access to IT Network - external (hacking)
Date Reported : 29/10/2012

Status : Closed - Resolved

Document ID : TMMS-8ZJ4ZH

## Reporter Details

Reported By : [redacted] Staff/ABS
Created By : [redacted] Staff/ABS
Office : CO
Section : Enterprise Systems and Software Management
Branch : Technology Infrastructure Delivery
Division : Technology Services Division
Phone : (02) 6252[redacted]
Location : CO 1S 432

## Incident Occurred

Incident Start date : Sat 20/10/2012
Incident End Date (if over a period) : Sat 27/10/2012

Start Time : 01:10 AM
End Time : 12:09 AM

State/Office Where Incident Occurred : CO
Where did the Incident Occur? ● Office ○ Outside Office
Describe the Location : Internet Gateway

## Description

Tell us what happened :
Please provide short explanation of the incident including any information that could assist in its resolution such as the names of witnesses or contributing circumstances.

This is a low volume attack by a couple of external address and so is unlikely to be automated in nature. A number of entries in the included spreadsheet are by ABS staff and may have legitimate password issues.

(Subject: SOC-20121029-01 - Notes Attacks [SEC=IN-CONFIDENCE:SECURITY]; Database: Security Operations Centre WDB; Author: [redacted] Created: 29/10/2012; Doc Ref: TMMS-8ZJ2BH)

Details :
Has property been Stolen/Lost/Damaged/Destroyed? ○ Yes ● No

Details of people responsible for the incident
If known, please enter the names and addresses of people responsible for the incident.

Name : Address :

Was any body injured? : ○ Yes ○ No ● Not Applicable

Signature - Signed by [redacted] Staff/ABS on 05/11/2012 07:55:10 AM, according to /ABS

First Created By : [redacted], On : 29/10/2012 01:32:46 PM

Police Involvement

Police involvement information is not required for this incident.
Were police called? : ○ Yes ● No

## Administration

Investigator/s:

Investigation Started:

Investigation Ended: Mon 05/11/2012

## General

Security Description : Unauthorised Access
Security Incident : to ABS IT Network
Incident Rating :

Summary of the Security Action taken :
Please provide summary of the action taken including any doclinks to relevant documents.This is part is to be filled when the investigation is completed.
nothing further to add
Total Hours :

## Fraud

Fraud Method :
Type of Loss (if any) :
Specify Other Method :

Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :

## Document Access

Authors : [Security Staff], [Security Admin]

Readers : [Security Staff], [Security Admin]

## Related Documents

| Date Created | Doc Type |
|---|---|

## Reminder Information

| | | | |
|---|---|---|---|
| Reminder Sent Date: | 05/11/2012 | Next Reminder: | 12/11/2012 |
| Reminder No.: | 0 | Last Edited Date: | 05/11/2012 |

## Edit History

Report Closed by [redacted] on 05/11/2012 07:55:08 AM
Incident Submitted by [redacted] on 29/10/2012 02:04:21 PM
Incident Created by [redacted] on 29/10/2012 01:33:32 PM

# SECURITY-IN-CONFIDENCE

Basics

| Protective Mark | SECURITY-IN-CONFIDENCE |
|---|---|

Attack Information

## 1. Summary of attack

| Executive Summary |
|---|
| This attack was targeted over a week |

| Start Time | End Time | Total Attempts | Successful Attemp |
|---|---|---|---|
| 2012-10-22 09:01:10 EST | 2012-10-27 00:09:18 EST | 131 | 0 |

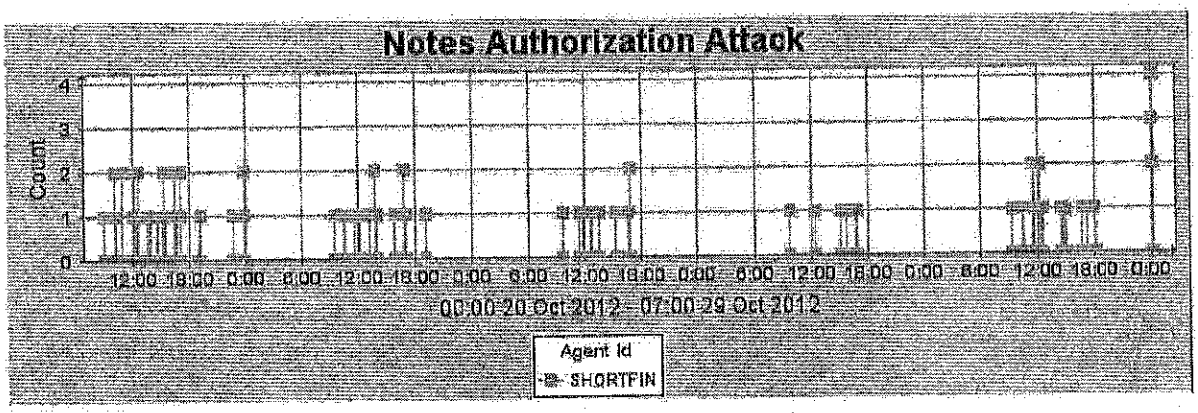
## 2. Target of attack

| Target IP | Ports |
|---|---|
| SHORTEN | |

## 3. About the attacker

| Source IP | Ports |
|---|---|
| Various | |

## 4. Attack profile




5. Attack description

Attack description

This is a low volume attack by a couple of external address and so is unlikely to be automated in nature. A number have legitimate password issues.

6 [redacted] Report

SOC-20121029-01 - Notes Attacks.xlsx

out of scope - automated report

Security Incident Report Information

(Database: SIRS Database; Author: ; Created: 29/10/2012)

Gateway Incident Report Information

ABS Results

SIR

SIRs -Prod v2.0

# Incident Report

v 1.0

Incident : Illegal access to IT Network - external (hacking)
Date Reported : 11/10/2012

Status : Closed - Resolved

Document ID : NFIK-8YXUU8

## Reporter Details

Reported By : [redacted] Staff/ABS
Created By : [redacted] Staff/ABS
Office : CO
Section : Network Services
Branch : Technology Infrastructure Delivery
Division : Technology Services Division
Phone : (02) 6252 [redacted]
Location : CO 1S 333

## Incident Occurred

Incident Start date : Wed 10/10/2012
Incident End Date (if over a period) : Wed 10/10/2012

Start Time : 01:50 AM
End Time : 01:50 AM

State/Office Where Incident Occurred : CO
Where did the Incident Occur? ● Office ○ Outside Office

Describe the Location :

## Description

Tell us what happened :
Please provide short explanation of the incident including any information that could assist in its resolution such as the names of witnesses or contributing circumstances.

➲ Attempt to access WebPRod1021 from IP address [redacted] using Admin userid

| | | |
|---|---|---|
| MONKFISH | 2012-10-10 01:50:19 EST | (SERVER: WebProd1021/SVR/ABSWebProd) Warning(low): nHTTP: user [redacted] authentication failure using internet password^^ |

[redacted]13doc_30933.pdf

Out of scope - automated report

Details :
Has property been Stolen/Lost/Damaged/Destroyed? ○ Yes ● No

Details of people responsible for the incident
If known, please enter the names and addresses of people responsible for the incident.

Name : Address :

Was any body injured? : ○ Yes ○ No ● Not Applicable

Signature - Signed by [redacted] Staff/ABS on 18/10/2012 08:17:07 AM according to /ABS

First Created By : [redacted] On : 11/10/2012 09:53:08 AM

Police Involvement

Police involvement information is not required for this incident.

Were police called? : ○ Yes ● No

## Administration

Investigator/s:

Investigation Started:

Investigation Ended: Thu 18/10/2012

## General

Security Description : Unauthorised Access
Security Incident : to ABS IT Network
Incident Rating :

Summary of the Security Action taken :
Please provide summary of the action taken including any doclinks to relevant documents.This is part is to be filled when the investigation is completed.

Total Hours :

## Fraud

Fraud Method :
Type of Loss (if any) :
Specify Other Method :

Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :

Document Access

Authors : [Security Staff], [Security Admin]
Readers : [Security Staff], [Security Admin]

Related Documents

| Date Created | Doc Type |
|---|---|

Reminder Information

Reminder Sent Date: 18/10/2012
Reminder No.: 0
Next Reminder: 25/10/2012
Last Edited Date: 18/10/2012

Edit History

Report Closed by [redacted] on 18/10/2012 08:17:12 AM
Incident Submitted by [redacted] on 11/10/2012 09:55:33 AM
Incident Created by [redacted] on 11/10/2012 09:53:23 AM

SIRs-Prod v2.0

# Incident Report

v 1.0

Incident : Illegal access to IT Network - external (hacking)
Date Reported : 09/10/2012

Status : Closed - Resolved

Document ID : NFIK-8YW362

## Reporter Details

Reported By : [redacted] Staff/ABS
Created By : [redacted] Staff/ABS
Office : CO
Section : Network Services
Branch : Technology Infrastructure Delivery
Division : Technology Services Division
Phone : (02) 6252 [redacted]
Location : CO 1S 333

## Incident Occurred

Incident Start date : Fri 05/10/2012
Incident End Date (if over a period) : Fri 05/10/2012

Start Time : 01:46 PM
End Time : 01:46 PM

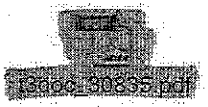
State/Office Where Incident Occurred : CO
Where did the Incident Occur? ● Office ○ Outside Office
Describe the Location :

## Description

Tell us what happened :
Please provide short explanation of the incident including any information that could assist in its resolution such as the names of witnesses or contributing circumstances.

➲ Attempt to access WebProd1021 using userid's admin, tomcat, manager, user. All from ip address [redacted]

| | | |
|---|---|---|
| MONKFISH | 2012-10-05 13:46:46 EST | (SERVER: WebProd1021/SVR/ABS/WebProd) Warning(low): nHTTP: user [redacted] authentication failure using internet password*** |



Out of scope : automated report

Details :
Has property been Stolen/Lost/Damaged/Destroyed? ○ Yes ● No

Details of people responsible for the incident
If known, please enter the names and addresses of people responsible for the incident.

Name : Address :

Was any body injured? : ○ Yes ○ No ● Not Applicable

Signature - Signed by [redacted] Staff/ABS on 16/10/2012 09:12:57 AM, according to /ABS

First Created By : [redacted] On : 09/10/2012 11:57:38 AM

Police Involvement

Police involvement information is not required for this incident.
Were police called? : ○ Yes ● No

## Administration

Investigator/s:

Investigation Started:

Investigation Ended: Tue 16/10/2012

## General

Security Description : Unauthorised Access
Security Incident : to ABS IT Network
Incident Rating :

Summary of the Security Action taken :
Please provide summary of the action taken including any doclinks to relevant documents.This is part is to be filled when the investigation is completed.

Total Hours :

## Fraud

Fraud Method :
Type of Loss (if any) :
Specify Other Method :

Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :

## Document Access

Authors : [Security Staff], [Security Admin]
Readers : [Security Staff], [Security Admin]

## Related Documents

| Date Created | Doc Type |
|---|---|

## Reminder Information

Reminder Sent Date: 16/10/2012
Reminder No.: 0
Next Reminder: 23/10/2012
Last Edited Date: 16/10/2012

## Edit History

Report Closed by [redacted] on 16/10/2012 09:12:57 AM
Incident Submitted by [redacted] on 09/10/2012 12:02:41 PM
Incident Created by [redacted] on 09/10/2012 11:58:52 AM

# Incident Report



Incident : Illegal access to IT Network - external (hacking)
Date Reported : 11/07/2012

Status : Closed - Resolved

Document ID : TMMS-8W495R

## Reporter Details

| | |
|---|---|
| Reported By : | [redacted] Staff/ABS |
| Created By : | [redacted] Staff/ABS |
| Office : | CO |
| Section : | Enterprise Systems and Software Management |
| Branch : | Technology Infrastructure |
| Division : | Technology Services Division |
| Phone : | (02) 6252[redacted] |
| Location : | CO 1S 432 |

## Incident Occurred

| | | | |
|---|---|---|---|
| Incident Start date : | Tue 10/07/2012 | Start Time : | 10:30 AM |
| Incident End Date (if over a period) : | Wed 11/07/2012 | End Time : | 01:23 AM |

State/Office Where Incident Occurred : CO
Where did the Incident Occur? ● Office ○ Outside Office
Describe the Location : Internet gateway

## Description

Tell us what happened :
Please provide short explanation of the incident including any information that could assist in its resolution such as the names of witnesses or contributing circumstances.

On 2 occasions the ABS gateway IP address range was scanned, each time the number of attempts exceeded 5000.

(Subject: SOC-20120711-02 - Attack by [redacted] [SEC=IN-CONFIDENCE:SECURITY]; Database: Security Operations Centre WDB; Author: [redacted] Created: 11/07/2012; Doc Ref: TMMS-8W4737)

Details :
Has property been Stolen/Lost/Damaged/Destroyed? ○ Yes ● No

Details of people responsible for the incident
If known, please enter the names and addresses of people responsible for the incident.

Name : Address :

Was any body injured? : ○ Yes ○ No ● Not Applicable

[redacted] Signature - Signed by [redacted] Staff/ABS on 18/07/2012 02:30:57 PM, according to /Staff/ABS

First Created By : [redacted], On : 11/07/2012 04:04:20 PM

Police Involvement

Police involvement information is not required for this incident.
Were police called? : ○ Yes ● No

## Administration

Investigator/s:

Investigation Started:

Investigation Ended: Wed 18/07/2012

## General

Security Description : Unauthorised Access
Security Incident : to ABS IT Network
Incident Rating :

Summary of the Security Action taken :
Please provide summary of the action taken including any doclinks to relevant documents.This is part is to be filled when the investigation is completed.

Total Hours :

## Fraud

Fraud Method :
Type of Loss (if any) :
Specify Other Method :

Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :

## Document Access

Authors : [Security Staff], [Security Admin]

Readers : [Security Staff], [Security Admin]

## Related Documents

| Date Created | Doc Type |
|---|---|

## Reminder Information

Reminder Sent Date: 18/07/2012
Reminder No.: 0
Next Reminder: 25/07/2012
Last Edited Date: 18/07/2012

## Edit History

Report Closed by [redacted] on 18/07/2012 02:30:57 PM
Incident Submitted by [redacted] on 11/07/2012 04:13:40 PM
Incident Created by [redacted] on 11/07/2012 04:06:08 PM

SOC-20120711-02 - Attack by [redacted] [SEC=IN-CONFIDENCE:SECURITY]
Security Operations Centre WDE [redacted] 11/07/2012 02:17 PM

# SECURITY-IN-CONFIDENCE

## Basics

| Protective Mark | SECURITY-IN-CONFIDENCE |
|---|---|

## Attack information

1. Summary of attack

| Executive Summary |
|---|
| This is an individual fishing for an unauthorised access point of which none have been found. |

| Start Time | End Time | Total Attempts | Successful Connect Attempts |
|---|---|---|---|
| 2012-07-10 10:31 am | 2012-07-10 10:31 am | 5124 | 201 |
| 2012-07-11 01:23 am | 2012-07-11 01:23 am | 5392 | 28 |

2. Target of attack

| Target IP | Ports |
|---|---|
| [redacted] | 80, 3128, 8080, 8888 |

3. About the attacker

| Source IP | Ports |
|---|---|
| [redacted] | 2929 - 6000 |

4. Attack profile

Event types

5. Attack description

| Attack description |
|---|
| This source is fishing for an unauthorised access point to gain entry into the ABS network. The attack was divided i around which the attacked focused are well known for various Trojans. |

6[redacted] Report

Out of scope - automated reports

SOC-20120711-02 - Attack by [redacted].pdfSOC-20120711-02 - Attack by [redacted] - Access granted.pc

## Security Incident Report Information

(Database: SIRS Database; Author: ; Created: 11/07/2012)

## Gateway Incident Report Information

## ABS Results

Open ports to connected servers appear to be correct, traffic was denied due to malformed TCP headers.

# Incident Report



Incident : Illegal access to IT Network - external (hacking)
Date Reported : 22/06/2012
Status : Closed - Resolved
Document ID : TMMS-8VGUCX

## Reporter Details

Reported By : [redacted] Staff/ABS
Created By : [redacted] Staff/ABS
Office : CO
Section : Enterprise Systems and Software Management
Branch : Technology Infrastructure
Division : Technology Services Division
Phone : (02) 6252[redacted]
Location : CO 1S 432

## Incident Occurred

Incident Start date : Thu 21/06/2012
Start Time : 10:29 AM
Incident End Date (if over a period) : Thu 21/06/2012
End Time : 10:29 AM

State/Office Where Incident Occurred : CO
Where did the Incident Occur? ● Office ○ Outside Office
Describe the Location : Internet gateway

## Description

Tell us what happened :
Please provide short explanation of the incident including any information that could assist in its resolution such as the names of witnesses or contributing circumstances.

During a 31 second period on the 21-June-2012 from 10:29:13 am to 10:29:43 am, the ABS experienced a scanning attack encompassing 3088 attempts with 2 being successful SOC-20120621-02 - Connections By [redacted].pdf. A detailed breakdown can be found here SOC-20120621-02 - Attack By [redacted].pdf and investigation by SOC is identified as SOC-20120621-02 - Attack By 96.127.162.178.

Out of scope automated reports

Details :
Has property been Stolen/Lost/Damaged/Destroyed? ○ Yes ● No

Details of people responsible for the incident
If known, please enter the names and addresses of people responsible for the incident.

Name : Address :

Was any body injured? : ○ Yes ○ No ● Not Applicable

Signature - Signed By [redacted] Staff/ABS on 25/06/2012 03:27:21 PM, according to /ABS

First Created By : [redacted] On : 22/06/2012 08:28:32 AM

Police Involvement

Police involvement information is not required for this Incident.
Were police called? : ○ Yes ● No

## Administration

Investigator/s: [redacted] Staff/ABS,
Investigation Started: Thu 21/06/2012
Investigation Ended: Mon 25/06/2012

### General

Security Description : Unauthorised Access
Security Incident : to ABS IT Network
Incident Rating :

Summary of the Security Action taken :
Please provide summary of the action taken including any doclinks to relevant documents.This is part is to be filled when the investigation is completed.
(Subject: SOC-20120621-02 - Attack by [redacted] [SEC=IN-CONFIDENCE:SECURITY]; Database: Security Operations Centre WDB; Author: [redacted] Created: 22/06/2012; Doc Ref: TMMS-8VH6UN)
Total Hours :

### Fraud

Fraud Method :
Type of Loss (if any) :
Specify Other Method :

Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :

Authors : [Security Staff], [Security Admin]
Readers : [Security Staff], [Security Admin]

## Related Documents

| Date Created | Doc Type |
|---|---|

## Reminder Information

Reminder Sent Date:
Reminder No.: 0

Next Reminder: 02/07/2012
Last Edited Date: 25/06/2012

## Edit History

Report Closed by [redacted] on 25/06/2012 03:27:20 PM
Document Updated by [redacted] on 22/06/2012 09:05:47 AM
Document Updated by [redacted] on 22/06/2012 09:01:01 AM
Incident Submitted by [redacted] on 22/06/2012 08:35:48 AM
Incident Created by [redacted] on 22/06/2012 08:28:53 AM

DECLASSIFIED

SOC-20120621-02 - Attack by [redacted] [SEC=IN-CONFIDENCE:SECURITY]
Security Operations Centre WEB [redacted] 22/06/2012 02:07 PM

# SECURITY-IN-CONFIDENCE

Basics

| Protective Mark | SECURITY-IN-CONFIDENCE |
|---|---|

Attack Information

1. Nature of attack

Attack Description

This attack comes in the form of a scan across a number of servers on a particular port.

| Start Time | End Time | Total Attempts | Successful Attemp |
|---|---|---|---|
| 2012-06-21 10:29:13 | 2012-06-21 10:29:34 | 3088 | 2 |

2. [redacted] Report

Out of scope
Automated reports

SOC-20120621-02 - Attack By [redacted].pdf SOC-20120621-02 - Connections By [redacted].pdf

Security Incident Report Information

(Database: SIRS Database; Author: ; Created: 22/06/2012)

ABS Results

| Target IP | Port | Service | External Connec |
|---|---|---|---|
| [redacted] | 25 | mail.abs.gov.au | Yes |
| [redacted] | 25 | mail.test.abs.gov.au | Yes |

All of the traffic in the table above appears to be correct, scan found no vulnerabilities.

SIRs -Prod v2.0

# Incident Report

v 1.0

**Incident :** Illegal access to IT Network - external (hacking)
**Date Reported :** 22/06/2012

**Status :** Closed - Resolved

**Document ID :** TMMS-8VGU2Q

## Reporter Details

**Reported By :** [redacted] Staff/ABS
**Created By :** [redacted] Staff/ABS
**Office :** CO
**Section :** Enterprise Systems and Software Management
**Branch :** Technology Infrastructure
**Division :** Technology Services Division
**Phone :** (02) 6252[redacted]
**Location :** CO 1S 432

## Incident Occurred

**Incident Start date :** Thu 21/06/2012
**Incident End Date (if over a period) :** Thu 21/06/2012
**Start Time :** 10:29 AM
**End Time :** 10:29 AM

**State/Office Where Incident Occurred** CO
**Where did the Incident Occur?** ● Office ○ Outside Office
**Describe the Location :** Internet gateway

## Description

**Tell us what happened :**
Please provide short explanation of the incident including any information that could assist in its resolution such as the names of witnesses or contributing circumstances.

During a 5 second period on the 21-June-2012 from 11:14:22 am to 11:14:27 am, the ABS experienced a scanning attack encompassing 3089 attempts of which 20 were successful SOC-20120621-01 - Connections By [redacted].pdf. A detailed breakdown can be found here SOC-20120621-01 - Attack By [redacted].pdf and investigation by SOC is identified as SOC-20120621-01 - Attack By [redacted]

Out of scope - automated reports

**Details :**
**Has property been Stolen/Lost/Damaged/Destroyed?** ○ Yes ● No

**Details of people responsible for the incident**
If known, please enter the names and addresses of people responsible for the incident.

**Name :** **Address :**

**Was any body injured? :** ○ Yes ○ No ● Not Applicable

Signature - Signed by [redacted] Staff/ABS on 25/06/2012 03:28:29 PM, according to /ABS

First Created By : [redacted], On : 22/06/2012 08:12:06 AM

**Police Involvement**

**Police involvement information is not required for this Incident.**
○ Yes ● No

Were police called? :

Administration

Investigator/s: [redacted] Staff/ABS,
Investigation Started: Thu 21/06/2012
Investigation Ended: Mon 25/06/2012

General

Security Description : Unauthorised Access
Security Incident : to ABS IT Network
Incident Rating :

Summary of the Security Action taken :
Please provide summary of the action taken including any doclinks to relevant documents.This is part is to be filled when the investigation is completed.
(Subject: SOC-20120612-01 - Attack by [redacted] [SEC=IN-CONFIDENCE:SECURITY]; Database: Security Operations Centre WDB; Author: [redacted] Created: 22/06/2012; Doc Ref: TMMS-8VH425)
Total Hours :

Fraud

Fraud Method :
Type of Loss (if any) :
Specify Other Method :

Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :

## Document Access

Authors : [Security Staff], [Security Admin]
Readers : [Security Staff], [Security Admin]

## Related Documents

| Date Created | Doc Type |
|---|---|

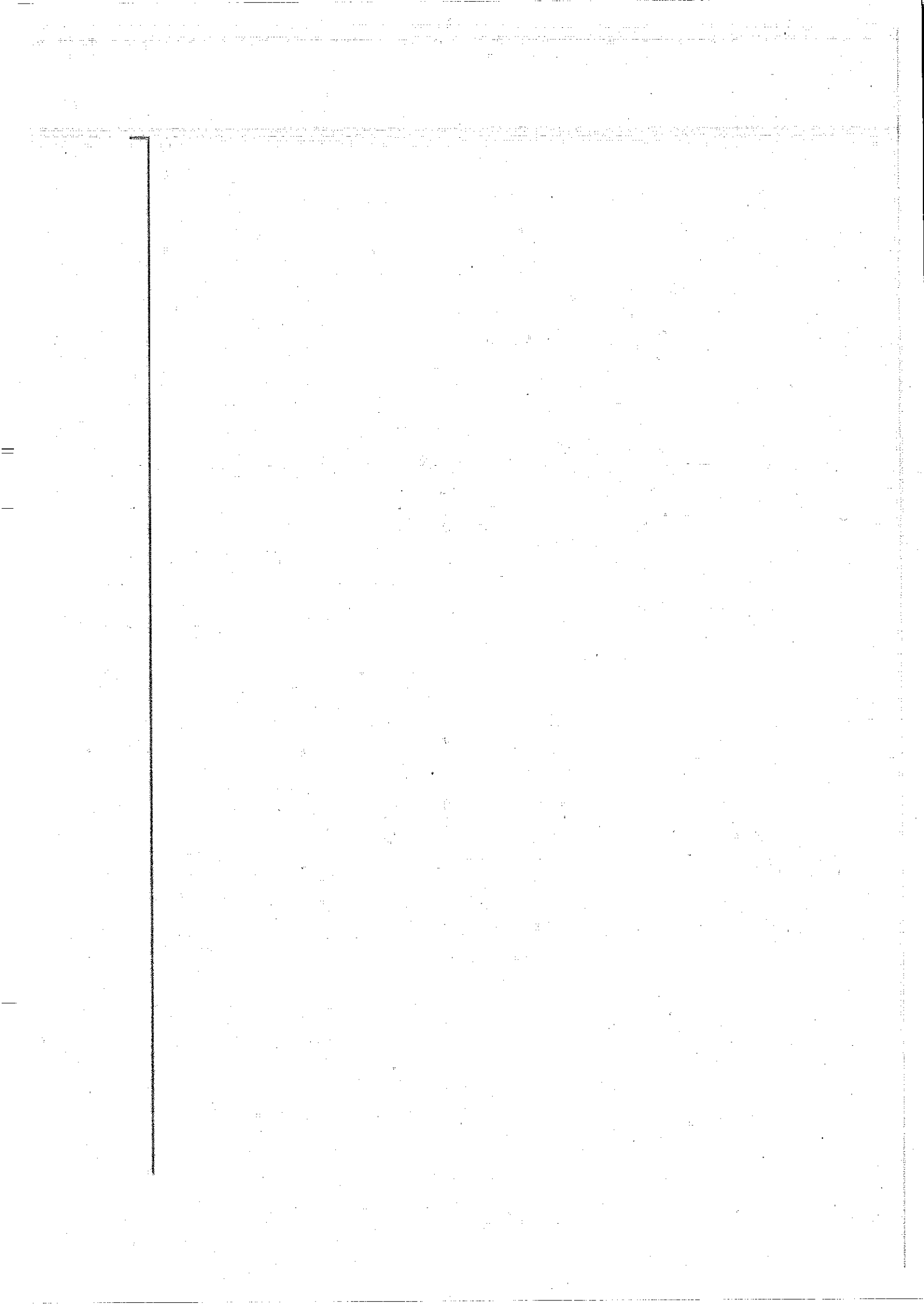
## Reminder Information

Reminder Sent Date:
Reminder No.: 0

Next Reminder: 02/07/2012
Last Edited Date: 25/06/2012

## Edit History

Report Closed by [redacted] on 25/06/2012 03:28:28 PM
Document Updated by [redacted] on 22/06/2012 09:03:17 AM
Incident Submitted by [redacted] on 22/06/2012 08:28:17 AM
Incident Created by [redacted] on 22/06/2012 08:13:14 AM



DECLASSIFIED

SOC-20120612-01 - Attack by [redacted] [SEC=IN-CONFIDENCE:SECURITY]
Security Operations Centre WDB [redacted] 22/06/2012 11:42 AM

# SECURITY-IN-CONFIDENCE

Basics

| Protective Mark | SECURITY-IN-CONFIDENCE |
|---|---|

Attack Information

1. Nature of attack

Attack Description

This attack comes in the form of a scan across a number of servers on a particular port.

| Total Attempts | Successful Attempts |
|---|---|
| 3089 | 20 |

Out of scope: automated reports

2[redacted] Report

SOC-20120621-01 - Attack By [redacted] pdf SOC-20120621-01 - Connections By [redacted] pdf

Security Incident Report Information

(Database: SIRS Database; Author: ; Created: 22/06/2012)

ABS Results

| Target IP | Port | Service | External Connec |
|---|---|---|---|
| [redacted] | 443 | stream1.collection.abs.gov.au | Yes |
| | 443 | www6.iprod.abs.gov.au | Yes |
| | 443 | www.nss.gov.au | Yes |

| | | | |
|---|---|---|---|
| [redacted] | 443 | taxonomy-collaboration.sbr.abs.gov.au | Yes |
| | 443 | taxonomy-testing.sbr.abs.gov.au | Yes |
| | 443 | www7.abs.gov.au | Yes |
| | 443 | www4.abs.gov.au | Yes |
| | 443 | www.growingup.gov.au | Yes |
| | 443 | airwatchds.abs.gov.au | Yes |
| | 443 | NDN Central | Yes |
| | 443 | NDN Node | Yes |
| | 443 | NDN Forums | Yes |
| | 443 | Census Output Application | Yes |
| | 443 | ace.abs.gov.au | Yes |
| | 443 | secure.abs.gov.au | Yes |
| | 443 | sbr-trax.test.abs.gov.au | Yes |
| | 443 | reverseproxy.test.abs.gov.au | Yes |
| | 443 | airwatchds.test.abs.gov.au | Yes |
| | 443 | nss, and, sch | Yes |
| | 443 | secure.test.abs.gov.au | Yes |

All of the traffic in the table above appears to be correct, scan found no vulnerabilities.

SIRs -Prod v2.0

# Incident Report

v 1.0

Incident : Illegal access to IT Network - external (hacking)
Date Reported : 13/06/2012

Status : Closed - Resolved

Document ID : CHET-8V82EV

## Reporter Details

| | |
|---|---|
| Reported By : | [redacted] Staff/ABS |
| Office : | CO |
| Section : | Network Services |
| Branch : | Technology Infrastructure |
| Division : | EXEC1 |
| Phone : | (02) 6252[redacted] |
| Address: | CO 1S 313 |
| Created By : | [redacted] /Staff/ABS |
| Office : | CO |
| Section : | Network Services |
| Branch : | Technology Infrastructure |
| Division : | Technology Services Division |
| Phone : | (02) 6252[redacted] |
| Location : | CO 1S 309 |

## Incident Occurred

| | | | |
|---|---|---|---|
| Incident Start date : | Tue 12/06/2012 | Start Time : | 09:51 PM |
| Incident End Date (if over a period) : | Wed 13/06/2012 | End Time : | 10:00 AM |

State/Office Where Incident Occurred: CO
Where did the Incident Occur? ● Office ○ Outside Office

Tell us what happened :
Please provide short explanation of the incident including any information that could assist in its resolution such as the names of witnesses or contributing circumstances.

➲ 37 attempts to access server Monkfish (webprod1021 ~ austats website) using default admin/user accounts between 01:25:19 and 01:52:34. The accounts attempted to be accessed were admin, tomcat, manager and user. See:


Out of scope: automated reports

Details :
Has property been Stolen/Lost/Damaged/Destroyed? ○ Yes ● No

Details of people responsible for the incident
If known, please enter the names and addresses of people responsible for the incident.

Name : Address :

Was any body injured? : ○ Yes ○ No ● Not Applicable

Signature Signed by [redacted] Staff/ABS on 02/11/2012 08:40:15 AM, according to /ABS

First Created By : [redacted] On : 26/10/2012 08:29:36 AM

Police Involvement

Police involvement information is not required for this incident.
Were police called? : ○ Yes ● No

## Administration

Investigator/s:

Investigation Started:

Investigation Ended: Fri 02/11/2012

## General

Security Description : Other
Security Incident : other
Incident Rating :

Summary of the Security Action taken :
Please provide summary of the action taken including any doclinks to relevant documents.This is part is to be filled when the investigation is completed.

Total Hours :

## Fraud

Fraud Method :
Type of Loss (if any) :
Specify Other Method :

Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :

## Document Access

| | |
|---|---|
| Authors : | [Security Staff], [Security Admin] |
| Readers : | [Security Staff], [Security Admin] |

## Related Documents

| Date Created | Doc Type |
|---|---|

## Reminder Information

| | | | |
|---|---|---|---|
| Reminder Sent Date: | 02/11/2012 | Next Reminder: | 09/11/2012 |
| Reminder No.: | 0 | Last Edited Date: | 02/11/2012 |

## Edit History

Report Closed by [redacted] on 02/11/2012 08:40:17 AM
Incident Submitted by [redacted] on 26/10/2012 08:33:49 AM
Incident Created by [redacted] on 26/10/2012 08:29:44 AM

SIRs-Prod v2.0

# Incident Report

v 1.0

Incident : Illegal access to IT Network - external (hacking)
Date Reported : 27/03/2009

Status : Closed - Resolved

Document ID : TMMS-7QJ3HZ

## Reporter Details

Reported By : [redacted] Staff/ABS
Created By : [redacted] Staff/ABS
Office : CO
Section : IT Communications
Branch :
Division :
Phone : (02) 6252[redacted]
Location : CO 1S 341

## Incident Occurred

Incident Start date : Mon 23/03/2009
Incident End Date (if over a period) : Mon 23/03/2009

Start Time : 10:15 PM
End Time : 11:34 PM

State/Office Where Incident Occurred : CO
Where did the Incident Occur? ● Office ○ Outside Office
Describe the Location :

## Description

**Tell us what happened :**
Please provide short explanation of the incident including any information that could assist in its resolution such as the names of witnesses or contributing circumstances.

The following activity on our VoIP gateways is considered to be of a suspicious nature as it targets our test number range [redacted]
Calls from [redacted] were attempted at 10:15:43 pm, 10:16:20 pm, 11:34:27pm.

Detailed CDR records available on request.

**Details :**
Has property been Stolen/Lost/Damaged/Destroyed? ○ Yes ● No

**Details of people responsible for the incident**
If known, please enter the names and addresses of people responsible for the incident.

**Name :** **Address :**

**Was any body injured? :** ○ Yes ○ No ● Not Applicable

Signature : Signed by Chris Soczynski/Staff/ABS on 31/03/2009 07:52:32 AM according to /Staff/ABS

First Created By : [redacted] On : 27/03/2009 12:16:45 PM

**Police Involvement**

Police involvement information is not required for this Incident.
**Were police called? :** ○ Yes ● No

Investigator/s: Chris Soczynski/Staff/ABS,
Investigation Started: Tue 31/03/2009
Investigation Ended: Tue 31/03/2009

General

Security Description : Unauthorised Access
Security Incident : to ABS IT Network
Incident Rating :

Summary of the Security Action taken :
Please provide summary of the action taken including any doclinks to relevant documents.This is part is to be filled when the investigation is completed.
Spoke to [redacted] this morning. It is unclear whether there was malicious intent behind this dialling. Tom said he will keep an eye on the CDR records in case there are further such incidents.
Total Hours :

Fraud

Fraud Method :
Type of Loss (If any) :
Specify Other Method :

Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :

Document Access

Authors : [Security Staff], [Security Admin]
Readers : [Security Staff], [Security Admin]

## Related Documents

| Date Created | Doc Type |
|---|---|

## Reminder Information

Reminder Sent Date:
Reminder No.: 0

Next Reminder: 07/04/2009
Last Edited Date: 31/03/2009

## Edit History

Report Closed by Chris Soczynski on 31/03/2009 07:52:32 AM
Incident Submitted by [redacted] on 27/03/2009 12:21:24 PM
Incident Created by [redacted] on 27/03/2009 12:16:53 PM

SIRs -Prod v2.0

# Incident Report

v 1.0

Incident : Illegal access to IT Network - external (hacking)
Date Reported : 27/03/2009

Status : Closed - Resolved

Document ID : TMMS-7QHVPA

## Reporter Details

Reported By : [redacted] Staff/ABS
Created By : [redacted] Staff/ABS
Office : CO
Section : IT Communications
Branch :
Division :
Phone : (02) 6252[redacted]
Location : CO 1S 341

## Incident Occurred

Incident Start date : Mon 23/03/2009
Incident End Date (if over a period) : Mon 23/03/2009

Start Time : 08:16 PM
End Time : 08:35 PM

State/Office Where Incident Occurred : CO
Where did the Incident Occur? ● Office ○ Outside Office
Describe the Location :

## Description

Tell us what happened :
Please provide short explanation of the incident including any information that could assist in its resolution such as the names of witnesses or contributing circumstances.

The following activity on our VoIP gateways is considered to be of a suspicious nature as it targets our test number range [redacted]
Calls from [redacted] were attempted at 08:16:32 pm, 08:16:33 pm, 08:16:34 pm, 08:16:35 pm.

Detailed CDR records available on request.

Details :
Has property been Stolen/Lost/Damaged/Destroyed? ○ Yes ● No

Details of people responsible for the incident
If known, please enter the names and addresses of people responsible for the incident.

Name : Address :

Was any body injured? : ○ Yes ○ No ● Not Applicable

Signature: Signed by Chris Soczynski/Staff/ABS on 31/03/2009 07:51:58 AM, according to /Staff/ABS

First Created By : [redacted] On : 27/03/2009 10:36:25 AM

Police Involvement

Police involvement information is not required for this incident.
Were police called? : ○ Yes ● No

Investigator/s: Chris Soczynski/Staff/ABS,

Investigation Started: Tue 31/03/2009

Investigation Ended: Tue 31/03/2009

General

Security Description : Unauthorised Access
Security Incident : to ABS IT Network
Incident Rating :

Summary of the Security Action taken :
Please provide summary of the action taken including any doclinks to relevant documents.This is part is to be filled when the investigation is completed.
Spoke to [redacted] this morning. It is unclear whether there was malicious intent behind this dialling. [redacted] said he will keep an eye on the CDR records in case there are further such incidents.
Total Hours :

Fraud

Fraud Method :
Type of Loss (if any) :
Specify Other Method :

Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :

Document Access

Authors : [Security Staff], [Security Admin]
Readers : [Security Staff], [Security Admin]

## Related Documents

| Date Created | Doc Type |
|---|---|

## Reminder Information

Reminder Sent Date:
Reminder No.: 0

Next Reminder: 07/04/2009
Last Edited Date: 31/03/2009

## Edit History

Report Closed by Chris Soczynski on 31/03/2009 07:51:57 AM
Incident Submitted by [redacted] on 27/03/2009 10:44:27 AM
Incident Created by [redacted] on 27/03/2009 10:36:35 AM

SIRs-Prod v2.0

# Incident Report

v1.0

Incident : Illegal access to IT Network - external (hacking)
Date Reported : 27/03/2009
Status : Closed - Resolved
Document ID : TMMS-7QHVD4

## Reporter Details

Reported By : [redacted] Staff/ABS
Created By : [redacted] Staff/ABS
Office : CO
Section : IT Communications
Branch :
Division :
Phone : (02) 6252[redacted]
Location : CO 1S 341

## Incident Occurred

Incident Start date : Fri 20/03/2009
Start Time : 06:35 PM
Incident End Date (if over a period) : Fri 20/03/2009
End Time : 06:35 PM

State/Office Where Incident Occurred : CO
Where did the Incident Occur? ● Office ○ Outside Office
Describe the Location :

## Description

Tell us what happened :
Please provide short explanation of the incident including any information that could assist in its resolution such as the names of witnesses or contributing circumstances.

The following activity on our VoIP gateways is considered to be of a suspicious nature as it targets our test number range [redacted]
Calls from [redacted] were attempted at 06:35:35 pm, 06:35:36 pm, 06:35:38 pm, 06:35:39 pm, 06:35:41 pm

Detailed CDR records available on request.

Details :
Has property been Stolen/Lost/Damaged/Destroyed? ○ Yes ● No

Details of people responsible for the incident
If known, please enter the names and addresses of people responsible for the incident.

Name : Address :

Was any body injured? : ○ Yes ○ No ● Not Applicable

Signature : Signed by Chris Soczynski/Staff/ABS on 31/03/2009 07:51:33 AM, according to /Staff/ABS

First Created By : [redacted] On : 27/03/2009 10:20:06 AM

Police Involvement

Police involvement information is not required for this Incident.
Were police called? : ○ Yes ● No

## Administration

| | |
|---|---|
| Investigator/s: | Chris Soczynski/Staff/ABS, |
| Investigation Started: | Tue 31/03/2009 |
| Investigation Ended: | Tue 31/03/2009 |

## General

Security Description : Unauthorised Access
Security Incident : to ABS IT Network
Incident Rating :

Summary of the Security Action taken :
Please provide summary of the action taken including any doclinks to relevant documents.This is part is to be filled when the investigation is completed.
Spoke to Tom this morning. It is unclear whether there was malicious intent behind this dialling. [redacted] said he will keep an eye on the CDR records in case there are further such incidents.
Total Hours :

## Fraud

Fraud Method :
Type of Loss (if any) :
Specify Other Method :

Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :

## Document Access

Authors : [Security Staff], [Security Admin]

Readers : [Security Staff], [Security Admin]

## Related Documents

| Date Created | Doc Type |
|---|---|

## Reminder Information

Reminder Sent Date:
Reminder No.: 0

Next Reminder: 07/04/2009
Last Edited Date: 31/03/2009

## Edit History

Report Closed by Chris Soczynski on 31/03/2009 07:51:32 AM
Document Updated by [redacted] on 27/03/2009 10:39:46 AM
Incident Submitted by [redacted] on 27/03/2009 10:36:14 AM
Incident Created by [redacted] on 27/03/2009 10:20:17 AM

SIRs-Prod v2.0

# Incident Report

v 1.0

Incident : Illegal access to IT Network - external (hacking)
Date Reported : 27/03/2009

Status : Closed - Resolved

Document ID : TMMS-7QHUJD

## Reporter Details

Reported By : [redacted] Staff/ABS
Created By : [redacted] /Staff/ABS
Office : CO
Section : IT Communications
Branch :
Division :
Phone : (02) 6252 [redacted]
Location : CO 1S 341

## Incident Occurred

Incident Start date : Sat 14/03/2009
Incident End Date (if over a period) : Sat 14/03/2009

Start Time : 01:31 PM
End Time : 01:52 PM

State/Office Where Incident Occurred : CO
Where did the Incident Occur? ● Office ○ Outside Office
Describe the Location :

## Description

Tell us what happened :
Please provide short explanation of the incident including any information that could assist in its resolution such as the names of witnesses or contributing circumstances.

The following activity on our VoIP gateways is considered to be of a suspicious nature as it targets our test number range [redacted]
Calls from [redacted] were attempted at 1:31:18 pm, 1:31:40 pm, 1:31:56 pm, 1:52:17 pm.

Detailed CDR records available on request.

Details :
Has property been Stolen/Lost/Damaged/Destroyed? ○ Yes ● No

Details of people responsible for the incident
If known, please enter the names and addresses of people responsible for the incident.

Name : Address :

Was any body injured? : ○ Yes ○ No ● Not Applicable

Signature - Signed by Chris Soczynski/Staff/ABS on 31/03/2009 07:50:46 AM, according to /Staff/ABS

First Created By : [redacted] On : 27/03/2009 09:37:18 AM

Police Involvement

Police involvement information is not required for this Incident.
Were police called? : ○ Yes ● No

## Administration

Investigator/s: Chris Soczynski/Staff/ABS,
Investigation Started: Tue 31/03/2009
Investigation Ended: Tue 31/03/2009

## General

Security Description : Unauthorised Access
Security Incident : to ABS IT Network
Incident Rating :

Summary of the Security Action taken :
Please provide summary of the action taken including any doclinks to relevant documents.This is part is to be filled when the investigation is completed.
Spoke to Tom this morning. It is unclear whether there was malicious intent behind this dialling. [redacted] said he will keep an eye on the CDR records in case there are further such incidents.
Total Hours :

## Fraud

Fraud Method :
Type of Loss (if any) :
Specify Other Method :

Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :

## Document Access

Authors : [Security Staff], [Security Admin]

Readers : [Security Staff], [Security Admin]

## Related Documents

| Date Created | Doc Type |
|---|---|

## Reminder Information

Reminder Sent Date:
Reminder No.: 0
Next Reminder: 07/04/2009
Last Edited Date: 31/03/2009

## Edit History

Report Closed by Chris Soczynski on 31/03/2009 07:50:45 AM
Document Updated by [redacted] on 27/03/2009 10:39:17 AM
Incident Submitted by [redacted] on 27/03/2009 10:18:15 AM
Incident Created by [redacted] on 27/03/2009 09:39:03 AM

SIRs -Prod v2.0

# Incident Report

v 1.0

Incident : Illegal access to IT Network - external (hacking)
Date Reported : 21/07/2009

Status : Closed - Resolved

Document ID : DWIR-7U62X4

## Reporter Details

Reported By : [redacted] Staff/ABS
Created By : [redacted] Staff/ABS
Office : CO
Section : Internet Services
Branch :
Division :
Phone : (02) 6252[redacted]
Location : CO 1S 350

## Incident Occurred

Incident Start date : Sun 19/07/2009
Incident End Date (if over a period) : Sun 19/07/2009

Start Time : 03:21 AM
End Time : 03:21 AM

State/Office Where Incident Occurred : CO
Where did the Incident Occur? ● Office ○ Outside Office
Describe the Location :

## Description

Tell us what happened :
Please provide short explanation of the incident including any information that could assist in its resolution such as the names of witnesses or contributing circumstances.

---

➲ Noticed the following access attempts accross a few domino servers:

SILVERTIP
2009-07-19 03:21:08.0
(SERVER: WebProd1051/SVR/ABSWebProd) Warning(low): nHTTP: fakeuser [redacted] authentication failure using internet password
SILVERTIP
2009-07-19 03:21:09.0
(SERVER: WebProd1051/SVR/ABSWebProd) Warning(low): nHTTP: fakeuser [redacted] authentication failure using internet password
ELEPHANTNOSE
2009-07-19 03:21:09.0
(SERVER: WebProd1020/SVR/ABSWebProd) Warning(low): nhttp: fakeuser [redacted] authentication failure using internet password
SILVERTIP
2009-07-19 03:21:09.0
(SERVER: WebProd1051/SVR/ABSWebProd) Warning(low): nHTTP: fakeuser [redacted] authentication failure using internet password
ELEPHANTNOSE
2009-07-19 03:21:10.0
(SERVER: WebProd1020/SVR/ABSWebProd) Warning(low): nhttp: fakeuser [redacted] authentication failure using internet password
SILVERTIP
2009-07-19 03:21:10.0
(SERVER: WebProd1051/SVR/ABSWebProd) Warning(low): nHTTP: fakeuser [redacted] authentication failure using internet password
SILVERTIP
2009-07-19 03:21:11.0
(SERVER: WebProd1051/SVR/ABSWebProd) Warning(low): nHTTP: fakeuser [redacted] authentication failure using internet password
SILVERTIP
2009-07-19 03:21:11.0
(SERVER: WebProd1051/SVR/ABSWebProd) Warning(low): nHTTP: fakeuser [redacted] authentication failure using internet password
SILVERTIP
2009-07-19 03:21:12.0
(SERVER: WebProd1051/SVR/ABSWebProd) Warning(low): nHTTP: fakeuser [redacted] authentication failure using internet password
ELEPHANTNOSE
2009-07-19 03:21:12.0
(SERVER: WebProd1020/SVR/ABSWebProd) Warning(low): nhttp: fakeuser [redacted] authentication failure using internet password
ELEPHANTNOSE
2009-07-19 03:21:13.0

(SERVER: WebProd1020/SVR/ABSWebProd) Warning(low): nhttp: fakeuser [redacted] authentication failure using internet password SILVERTIP
2009-07-19 03:21:13.0
(SERVER: WebProd1051/SVR/ABSWebProd) Warning(low): nHTTP: fakeuser [redacted] authentication failure using internet password ELEPHANTNOSE
2009-07-19 03:21:14.0
(SERVER: WebProd1020/SVR/ABSWebProd) Warning(low): nhttp: fakeuser [redacted] authentication failure using internet password SILVERTIP
2009-07-19 03:21:14.0
(SERVER: WebProd1051/SVR/ABSWebProd) Warning(low): nHTTP: fakeuser [redacted] authentication failure using internet password

[redacted]
ORLANDONET OOD

[redacted]
ORLANDONET OOD
[redacted]
BG-1225 Sofia
Bulgaria
+359 2 [redacted]

[redacted]
Sport BG OOD
[redacted]
BG-1000 Sofia
Bulgaria
+359 2 [redacted]
[redacted]@bonev.com

Details :
Has property been Stolen/Lost/Damaged/Destroyed? ○ Yes ● No

Details of people responsible for the incident
If known, please enter the names and addresses of people responsible for the incident.

Name : Address :

Was any body injured? : ○ Yes ○ No ● Not Applicable

Signature - Signed by [redacted] Staff/ABS on 05/08/2009 09:30:55 AM, according to /ABS

First Created By [redacted] On : 21/07/2009 10:46:31 AM

## Police Involvement

Police involvement information is not required for this Incident.
Were police called? : ○ Yes ● No

## Administration

Investigator/s: [redacted] Staff/ABS,
Investigation Started: Sun 19/07/2009
Investigation Ended: Thu 30/07/2009

### General

Security Description : Unauthorised Access
Security Incident : to ABS IT Network
Incident Rating : Low

Summary of the Security Action taken :
Please provide summary of the action taken including any doclinks to relevant documents.This is part is to be filled when the investigation is completed.
No access was gained to the network.
22/7/09 Leaving the investigation open for a while longer, as a logging issue has delayed some of these events being available.

30/7/09 Confirmed that no more attacks were taking place. Closing incident.
Total Hours : 1

## Fraud

Fraud Method :
Type of Loss (if any) :
Specify Other Method :

Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :

## Document Access

Authors : [Security Staff], [Security Admin]
Readers : [Security Staff], [Security Admin]

## Related Documents

| Date Created | Doc Type |
| --- | --- |

## Reminder Information

| | | | |
| --- | --- | --- | --- |
| Reminder Sent Date: | 05/08/2009 | Next Reminder: | 12/08/2009 |
| Reminder No.: | 0 | Last Edited Date: | 05/08/2009 |

## Edit History

Report Closed by [redacted] on 05/08/2009 09:30:54 AM
Document Updated by [redacted] on 05/08/2009 09:30:35 AM
Document Updated by [redacted] on 22/07/2009 03:14:43 PM
Incident Submitted by [redacted] on 21/07/2009 10:50:03 AM
Incident Created by [redacted] on 21/07/2009 10:47:46 AM

SIRs -Prod v2.0

# Incident Report

v 1.0

Incident : Other Unauthorised Access (not classified in choices)
Date Reported : 22/09/2011

Status : Closed - Resolved

Document ID : KMUN-8LWUKZ

## Reporter Details

Reported By : [redacted]/Staff/ABS
Created By : [redacted]/Staff/ABS
Office : CO
Section : Network Services
Branch : Technology Infrastructure
Division : Technology Services Division
Phone : (02) 6252[redacted]
Location : CO 1S 332

## Incident Occurred

Incident Start date : Wed 21/09/2011
Incident End Date (if over a period) :

Start Time : 09:00 AM
End Time :

State/Office Where Incident Occurred : CO
Where did the Incident Occur? ○ Office ● Outside Office

Describe the Location :

Other, was selected as part of Incident;
Please explain Security Description :

**Tell us what happened :**
Please provide short explanation of the incident including any information that could assist in its resolution such as the names of witnesses or contributing circumstances.

➲ Same as previous incidents about this..

| Agent Id | Agent Date/Time | Full Message |
|---|---|---|
| MONKFISH | 2011-09-21 08:59:53 EST | (SERVER: WebProd1021/SVR/ABSWebProd) Warning(low): nHTTP: admin [redacted] authentication failure using internet password^^ |
| MONKFISH | 2011-09-21 08:59:54 EST | (SERVER: WebProd1021/SVR/ABSWebProd) Warning(low): nHTTP: admin [redacted] authentication failure using internet password^^ |
| MONKFISH | 2011-09-21 08:59:56 EST | (SERVER: WebProd1021/SVR/ABSWebProd) Warning(low): nHTTP: admin [redacted] authentication failure using internet password^^ |
| MONKFISH | 2011-09-21 08:59:57 EST | (SERVER: WebProd1021/SVR/ABSWebProd) Warning(low): nHTTP: admin [redacted] authentication failure using internet password^^ |
| MONKFISH | 2011-09-21 08:59:59 EST | (SERVER: WebProd1021/SVR/ABSWebProd) Warning(low): nHTTP: admin [redacted] authentication failure using internet password^^ |
| MONKFISH | 2011-09-21 09:00:00 EST | (SERVER: WebProd1021/SVR/ABSWebProd) Warning(low): nHTTP: tomcat [redacted] authentication failure using internet password^^ |
| MONKFISH | 2011-09-21 09:00:02 EST | (SERVER: WebProd1021/SVR/ABSWebProd) Warning(low): nHTTP: tomcat [redacted] authentication failure using internet password^^ |
| MONKFISH | 2011-09-21 09:00:03 EST | (SERVER: WebProd1021/SVR/ABSWebProd) Warning(low): nHTTP: tomcat [redacted] authentication failure using internet password^^ |
| MONKFISH | 2011-09-21 09:00:05 EST | (SERVER: WebProd1021/SVR/ABSWebProd) Warning(low): nHTTP: tomcat [redacted] authentication failure using internet password^^ |
| | | (SERVER: WebProd1021/SVR/ABSWebProd) |

| | | |
|---|---|---|
| MONKFISH | 2011-09-21 09:00:06 EST | Warning(low): nHTTP: tomcat [redacted] authentication failure using internet password^^ |
| MONKFISH | 2011-09-21 09:00:07 EST | (SERVER: WebProd1021/SVR/ABSWebProd) Warning(low): nHTTP: tomcat [redacted] |





Signature - Signed by [redacted] Staff/ABS on 27/09/2011 08:38:49 AM according to /Staff/ABS

First Created By : [redacted] On : 22/09/2011 08:39:58 AM

## Police Involvement

Police involvement information is not required for this incident.

## Administration

Investigator/s:

Investigation Started:

Investigation Ended: Tue 27/09/2011

### General

Security Description : Unauthorised Access
Security Incident : Other
Incident Rating :

Summary of the Security Action taken :
Please provide summary of the action taken including any doclinks to relevant documents.This is part is to be filled when the investigation is

completed.
Spoken to Chris Soczynski and he is happy we just close off. These reports are useful for data in case DSD ever get involved.
Total Hours :

## Fraud

Fraud Method :
Type of Loss (if any) :
Specify Other Method :

Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :

## Document Access

Authors : [Security Staff], [Security Admin]
Readers : [Security Staff], [Security Admin]

## Related Documents

| Date Created | Doc Type |
| --- | --- |

Reminder Information

Reminder Sent Date:
Reminder No.: 0

Next Reminder: 04/10/2011
Last Edited Date: 27/09/2011

Edit History

Report Closed by [redacted] on 27/09/2011 08:38:49 AM
Incident Submitted by [redacted] on 22/09/2011 08:40:46 AM
Incident Created by [redacted] on 22/09/2011 08:40:05 AM

SIRs-Prod V2.0

# Incident Report

v 1.0

Incident : Other Unauthorised Access (not classified in choices)
Date Reported : 16/09/2011

Status : Closed - Resolved

Document ID : KMUN-8LQV2W

## Reporter Details

Reported By : [redacted] Staff/ABS
Created By : [redacted] Staff/ABS
Office : CO
Section : Network Services
Branch : Technology Infrastructure
Division : Technology Services Division
Phone : (02) 6252[redacted]
Location : CO 1S 332

## Incident Occurred

Incident Start date : Thu 15/09/2011
Start Time : 06:37 PM
Incident End Date (if over a period) :
End Time :

State/Office Where Incident Occurred : CO
Where did the Incident Occur? ○ Office ● Outside Office

Describe the Location :

Other, was selected as part of Incident:
Please explain Security Description :

Tell us what happened :
Please provide short explanation of the incident including any information that could assist in its resolution such as the names of witnesses or contributing circumstances.

➲ Much the same as [redacted] incident last week..

several attacks on the ausstats webservers using tomcat/manager/admin usernames

| Agent Id | Agent Date/Time | Full Message |
|---|---|---|
| MONKFISH | 2011-09-15 18:37:49 EST | (SERVER: WebProd1021/SVR/ABSWebProd) Warning(low): nHTTP: admin [redacted] authentication failure using internet password^ |
| MONKFISH | 2011-09-15 18:37:47 EST | (SERVER: WebProd1021/SVR/ABSWebProd) Warning(low): nHTTP: admin [redacted] authentication failure using internet password^ |
| MONKFISH | 2011-09-15 18:37:43 EST | (SERVER: WebProd1021/SVR/ABSWebProd) Warning(low): nHTTP: admin [redacted] authentication failure using internet password^ |
| MONKFISH | 2011-09-15 18:37:41 EST | (SERVER: WebProd1021/SVR/ABSWebProd) Warning(low): nHTTP: admin [redacted] authentication failure using internet password^ |
| | | |
| ELEPHANTNOSE | 2011-09-15 18:38:18 EST | (SERVER: WebProd1020/SVR/ABSWebProd) Warning(low): nHTTP: manager [redacted] authentication failure using internet password^ |
| ELEPHANTNOSE | 2011-09-15 18:38:20 EST | (SERVER: WebProd1020/SVR/ABSWebProd) Warning(low): nHTTP: manager [redacted] authentication failure using internet password^ |
| ELEPHANTNOSE | 2011-09-15 18:38:18 EST | (SERVER: WebProd1020/SVR/ABSWebProd) Warning(low): nHTTP: manager [redacted] authentication failure using internet password^ |

Signature - Signed by [redacted] Staff/ABS on 27/09/2011 08:38:17 AM, according to /Staff/ABS

First Created By : [redacted] On : 16/09/2011 09:03:49 AM

## Police Involvement

Police involvement information is not required for this incident.

## Administration

Investigator/s:

Investigation Started:

Investigation Ended: Tue 27/09/2011

### General

Security Description : Unauthorised Access
Security Incident : Other
Incident Rating :

Summary of the Security Action taken :
Please provide summary of the action taken including any doclinks to relevant documents.This is part is to be filled when the investigation is completed.
Spoken to Chris Soczynski and he is happy we just close off. These reports are useful for data in case DSD ever get involved.
Total Hours :

### Fraud

Fraud Method :
Type of Loss (if any) :
Specify Other Method :

| | |
|---|---|
| Person Responsible: | Relation with ABS : |
| Security Level : | |
| Person Responsible: | Relation with ABS : |
| Security Level : | |
| Person Responsible: | Relation with ABS : |
| Security Level : | |

## Document Access

| | |
|---|---|
| Authors : | [Security Staff], [Security Admin] |
| Readers : | [Security Staff], [Security Admin] |

## Related Documents

| Date Created | Doc Type |
|---|---|

## Reminder Information

| | | | |
|---|---|---|---|
| Reminder Sent Date: | 23/09/2011 | Next Reminder: | 04/10/2011 |
| Reminder No.: | 0 | Last Edited Date: | 27/09/2011 |

Edit History

Report Closed by [redacted] on 27/09/2011 08:38:16 AM
Incident Submitted by [redacted] on 16/09/2011 09:07:14 AM
Incident Created by [redacted] on 16/09/2011 09:03:55 AM

SIRs-Prod v2.0

# Incident Report

v 1.0

Incident : Other Unauthorised Access (not classified in choices)
Date Reported : 14/09/2011
Status : Closed - Resolved
Document ID : JGRN-8LNVZ9

## Reporter Details

Reported By : [redacted]/Staff/ABS
Created By : [redacted]/Staff/ABS
Office : CO
Section : Network Services
Branch : Technology Infrastructure
Division : Technology Services Division
Phone : (02) 6252[redacted]
Location : CO 1S 329

## Incident Occurred

Incident Start date : Thu 08/09/2011
Start Time : 05:17 AM
Incident End Date (if over a period) : Thu 08/09/2011
End Time : 05:18 AM

State/Office Where Incident Occurred : CO
Where did the Incident Occur? ● Office ○ Outside Office
Describe the Location : Ausstats website

Other, was selected as part of Incident:
Please explain Security Description : Someone attempted multiple times to login to both Elephantnose and Monkfish using the accounts Admin, Tomcat and Manager (I assume these are default accounts). All attempts failed.

Description

Tell us what happened :
Please provide short explanation of the incident including any information that could assist in its resolution such as the names of witnesses or contributing circumstances.

---

➲ Someone attempted multiple times to login to both Elephantnose and Monkfish using the accounts Admin, Tomcat and Manager (I assume these are default accounts). All attempts failed.

Agent Id Agent Date/Time Full Message
ELEPHANTNOSE 2011-09-08 05:17:06 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: admin [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:07 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: admin [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:09 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: admin [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:10 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: admin [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:13 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: admin [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:14 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: admin [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:16 EST
(SERVER: WebProd1020/SVR/ABSWebProd)

Warning(low): nHTTP: admin [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:16 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: admin [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:18 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: admin [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:19 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: admin [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:20 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: admin [redacted]
ELEPHANTNOSE 2011-09-08 05:17:22 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: tomcat [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:23 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: tomcat [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:25 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: tomcat [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:26 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: tomcat [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:28 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: tomcat [redacted]
authentication failure using internet password^^

ELEPHANTNOSE 2011-09-08 05:17:29 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: tomcat [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:31 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: tomcat [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:32 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: tomcat [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:34 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: tomcat [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:35 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: tomcat [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:37 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: tomcat [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:38 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: manager [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:40 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: manager [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:41 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: manager [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:43 EST

(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: manager [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:44 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: manager [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:46 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: manager [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:48 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: manager [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:49 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: manager [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:51 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: manager [redacted]
authentication failure using internet password^^
ELEPHANTNOSE 2011-09-08 05:17:52 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: manager [redacted]
ELEPHANTNOSE 2011-09-08 05:17:53 EST
(SERVER: WebProd1020/SVR/ABSWebProd)
Warning(low): nHTTP: manager [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:07 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: admin [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:08 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: admin [redacted]

authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:09 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: admin [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:11 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: admin [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:12 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: admin [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:13 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: admin [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:15 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: admin [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:17 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: admin [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:18 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: admin [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:21 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: admin [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:22 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: tomcat [redacted]
authentication failure using internet password^^

MONKFISH 2011-09-08 05:17:24 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: tomcat [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:25 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: tomcat [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:27 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: tomcat [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:28 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: tomcat [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:30 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: tomcat [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:31 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: tomcat [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:33 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: tomcat [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:34 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: tomcat [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:36 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: tomcat [redacted]
MONKFISH 2011-09-08 05:17:37 EST
(SERVER: WebProd1021/SVR/ABSWebProd)

Warning(low): nHTTP: tomcat [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:39 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: manager [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:40 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: manager [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:42 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: manager [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:44 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: manager [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:45 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: manager [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:46 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: manager [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:47 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: manager [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:49 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: manager [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:50 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: manager [redacted]

authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:52 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: manager [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:54 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: manager [redacted]
authentication failure using internet password^^
MONKFISH 2011-09-08 05:17:05 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: admin [redacted]
authentication failure using internet password^^

## Results for [redacted]:

```
% [whois.apnic.net node-4]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

inetnum:        [redacted]
netname:        HUARUI
descr:          Langfang Development Area Huarui Xintong Network Technology
                Co., Ltd.
descr:          Langfang university Langfang Development Area
country:        CN
admin-c:        WH271-AP
tech-c:         WH271-AP
changed:        [redacted]@cnnic.cn 20080520
status:         ASSIGNED NON-PORTABLE
mnt-by:         MAINT-CNNIC-AP
mnt-lower:      MAINT-CNNIC-AP
mnt-routes:     MAINT-CNCGROUP-RR
source:         APNIC

route:          [redacted]
```

```
descr:          CNC Group CHINA169 Hebei Province network
descr:          Addresses from CNNIC(HUARUI)
country:        CN
origin:         AS4837
mnt-by:         MAINT-CNCGROUP-RR
changed:        [redacted]@cnc-noc.net 20080521
source:         APNIC

person:         [redacted]
nic-hdl:        WH271-AP
e-mail:         [redacted]@sinnet.com.cn
address:        Langfang university Langfang Development Area
phone:          +86-[redacted]
fax-no:         +86-[redacted]
country:        CN
changed:        [redacted]@cnnic.cn 20080227
mnt-by:         MAINT-CNNIC-AP
source:         APNIC
```

Signature - Signed by [redacted] Staff/ABS on 27/09/2011 08:38:31 AM, according to /Staff/ABS

First Created By : [redacted], On : 14/09/2011 09:52:21 AM

**Police Involvement**

Police involvement information is not required for this incident.

**Administration**

Investigator/s:

Investigation Started:

Investigation Ended: Tue 27/09/2011

## General

Security Description : Unauthorised Access
Security Incident : Other
Incident Rating :

Summary of the Security Action taken :
Please provide summary of the action taken including any doclinks to relevant documents.This is part is to be filled when the investigation is completed.
Spoken to Chris Soczynski and he is happy we just close off. These reports are useful for data in case DSD ever get involved.
Total Hours :

## Fraud

Fraud Method :
Type of Loss (if any) :
Specify Other Method :

Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :

## Document Access

Authors : [Security Staff], [Security Admin]
Readers : [Security Staff], [Security Admin]

## Related Documents

| Date Created | Doc Type |
|---|---|

## Reminder Information

| | | | |
|---|---|---|---|
| Reminder Sent Date: | 21/09/2011 | Next Reminder: | 04/10/2011 |
| Reminder No.: | 0 | Last Edited Date: | 27/09/2011 |

## Edit History

Report Closed by [redacted] on 27/09/2011 08:38:31 AM
Incident Submitted by [redacted] on 14/09/2011 10:00:24 AM
Incident Created by [redacted] on 14/09/2011 09:53:31 AM

SIRs -Prod v2.0

# Incident Report

v 1.0

Incident : Other
Date Reported : 12/08/2011

Status : Closed - Resolved

Document ID : JGRN-8KN4Q7

## Reporter Details

Reported By : [redacted] Staff/ABS
Created By : [redacted] Staff/ABS
Office : CO
Section : Network Services
Branch : Technology Infrastructure
Division : Technology Services Division
Phone : (02) 6252[redacted]
Location : CO 1S 329

## Incident Occurred

Incident Start date : Fri 12/08/2011
Incident End Date (if over a period) :

Start Time : 11:33 AM
End Time :

State/Office Where Incident Occurred : CO
Where did the Incident Occur? ● Office ○ Outside Office

Describe the Location : ABS Internet Gateway

Other, was selected as part of Incident:
Please explain Security Description : [redacted] detected a successful attack (confirmed by agent) on the Census Field Portal [redacted]

Date/Time 2011-08-12 11:33:24 EST

Tag Name HTTP_Oracle_WebCache_Overflow
Alert Name HTTP_Oracle_WebCache_Overflow
Severity High
Observance Type Intrusion Detection
Combined Event Count 1
Cleared Flag false
Target IP Address [redacted]
Target Object Name 80
Target Object Type Target Port
Target Service 80
Source IP Address [redacted]
SourcePort Name 60408
Sensor DNS Name [redacted]abs.gov.au
Sensor IP Address [redacted]
Sensor Name Server Protection for Windows
DestinationDNSName www.censusfieldportal.abs.gov.au
DestinationNetBiosName [redacted]
IANAProtocolId 6
IssueId 2110062
len 448
PacketFlags 5248
ResponseLevel 5
SensorGUID 1E1F43AA-E60B-42F3-9C21-7F875BF710F5

See http://www.iss.net/security_center/reference/vuln/HTTP_Oracle_WebCache_Overflow.htm for some further information.

IBM PMR opened. Number is 27036.102.616. 15/08/2011 11:05AM

---

Description

Tell us what happened :
Please provide short explanation of the incident including any information that could assist in its resolution such as the names of witnesses or contributing circumstances.

---

➲ [redacted] detected a successful attack (confirmed by agent) on the Census Field Portal ([redacted])

Date/Time 2011-08-12 11:33:24 EST
Tag Name HTTP_Oracle_WebCache_Overflow
Alert Name HTTP_Oracle_WebCache_Overflow
Severity High
Observance Type Intrusion Detection
Combined Event Count 1
Cleared Flag false
Target IP Address [redacted]
Target Object Name 80
Target Object Type Target Port
Target Service 80
Source IP Address [redacted]
SourcePort Name 60408
Sensor DNS Name [redacted]abs.gov.au
Sensor IP Address [redacted]
Sensor Name Server Protection for Windows
DestinationDNSName www.censusfieldportal.abs.gov.au
DestinationNetBiosName [redacted]
IANAProtocolId 6
IssueId 2110062
len 448
PacketFlags 5248
ResponseLevel 5
SensorGUID 1E1F43AA-E60B-42F3-9C21-7F875BF710F5

See http://www.iss.net/security_center/reference/vuln/HTTP_Oracle_WebCache_Overflow.htm for some further information.

Chatted with [redacted] and everything looked ok as far as he could tell. It does not appear to have affected the Census Field Portal.

There was only one mention of that source ip address in [redacted] As we are unsure what "successful attack (confirmed by agent)" really means, a PMR will be raised with IBM to get clarification.

IBM PMR opened. Number is 27036.102.616. 15/08/2011 11:05AM

It was a pleasure assisting you with PMR #27036,102,616, concerning <GX5008 What does "Successful attack" mean. >. As discussed on the phone, successful attack just means that one of the vulnerability scanners found that IP address to have a specific vulnerability, and then an IPS saw traffic going to that IP that exploits that vulnerability.

---

Second PMR 27046,102,616

Hello [redacted],

Thank you for contacting IBM Security Solutions! My name is [redacted] amd I will be assisting you with PMR #27046,102,616. This PMR has been marked as having a Low (SEV4) severity, is that correct?

It is from my understanding that your are experiencing the signature HTTP_Oracle_WebCache_overflow firing from a non-Oracle running system. Please see below regarding the information regarding this signature:

---

This signature detects an HTTP request for which the method name in the header contains 432 or more characters (not including null, tabs, or spaces). This may indicate an attacker's attempt to overflow a buffer in an Oracle WebCache server.

---

A Successful attack means that the machine had a detected vulnerability by a scanner, and then an HIPS saw traffic that attempts to exploit that vulnerability. When the box is not an Oracle box it may be a false positive, however we would need to know what [redacted] product that this signature is firing on to provide the proper steps on how to bypass this false positive.

Details :
Has property been Stolen/Lost/Damaged/Destroyed? ○ Yes ● No

Details of people responsible for the incident
If known, please enter the names and addresses of people responsible for the incident.

Name : [redacted] Address : Telstra ip address

Was any body injured? : ○ Yes ○ No ● Not Applicable

Signature - Signed by [redacted] Staff/ABS on 12/09/2011 10:12:24 AM, according to /ABS

First Created By : [redacted] On : 12/08/2011 12:17:50 PM

## Police Involvement

Police involvement information is not required for this Incident.
Were police called? : ○ Yes ● No

## Administration

Investigator/s:

Investigation Started:

Investigation Ended: Fri 09/09/2011

### General

Security Description : Other
Security Incident : other
Incident Rating :

Summary of the Security Action taken :
Please provide summary of the action taken including any doclinks to relevant documents.This is part is to be filled when the investigation is completed.

Total Hours :

## Fraud

Fraud Method :
Type of Loss (if any) :
Specify Other Method :

Person Responsible: [redacted] Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :

Person Responsible:
Security Level :

Relation with ABS :

Document Access

Authors : [Security Staff], [Security Admin]
Readers : [Security Staff], [Security Admin]

Related Documents

| Date Created | Doc Type |
|---|---|

Reminder Information

Reminder Sent Date: 25/08/2011
Reminder No.: 0

Next Reminder: 19/09/2011
Last Edited Date: 12/09/2011

Edit History

Report Closed by [redacted] on 12/09/2011 10:12:24 AM

Document Updated by [redacted] on 18/08/2011 01:38:21 PM
Document Updated by [redacted] on 18/08/2011 01:38:18 PM
Document Updated by [redacted] on 15/08/2011 12:35:54 PM
Document Updated by [redacted] on 15/08/2011 11:09:34 AM
Document Updated by [redacted] on 15/08/2011 11:09:09 AM
Incident Submitted by [redacted] on 12/08/2011 12:31:15 PM
Incident Created by [redacted] on 12/08/2011 12:20:53 PM

SIRs -Prod v2.0

# Incident Report

v.1.0

Incident : Gateway Issue - Hacking
Date Reported : 23/03/2011
Status : Closed - Resolved
Document ID : JGRN-8F7V4Q

## Reporter Details

Reported By : [redacted]/Staff/ABS
Created By : [redacted]/Staff/ABS
Office : CO
Section : Network Services
Branch : Technology Infrastructure
Division : Technology Services Division
Phone : (02) 6252[redacted]
Location : CO 1S 328

## Incident Occurred

Incident Start date : Tue 22/03/2011
Start Time : 12:36 AM
Incident End Date (if over a period) : Tue 22/03/2011
End Time : 12:40 AM

State/Office Where Incident Occurred : CO
Where did the Incident Occur? ● Office ○ Outside Office
Describe the Location : Somebody was trying multiple times to login into WebProd1070 with false username/password.

## Description

Tell us what happened :
Please provide short explanation of the incident including any information that could assist in its resolution such as the names of witnesses or contributing circumstances.

---

➲ It appears as though someone was trying to login to WebProd1070 using a brute force username/password attack.

See Domino Lockouts section in pdf in (Subject: [redacted] Automated Report Delivery - Gateway Services Daily Report [SEC=IN-CONFIDENCE:SECURITY]; Database: Firewall Reports WDB; Author: [redacted] Created: 22/03/2011; Doc Ref: NACT-8F7D8X)

```
#
# Query terms are ambiguous.  The query is assumed to be:
#     "n[redacted]"
#
# Use "?" to get help.
#

#
# The following results may also be obtained via:
# http://whois.arin.net/rest/nets;q=[redacted]?showDetails=true&showARIN=false
#

Cox Communications Inc. NETBLK-OK-CBS-68-15-96-0 (NET-[redacted]) [redacted]-
[redacted]
Cox Communications Inc. COX-ATLANTA (NET-[redacted]) [redacted]


#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois_tou.html
#
```

Server Name : ➲ WebProd1070

Incident Rating :
Please select one from the following that best describes impact. ➲ Low

Business Impact: Minimal.

Low level singular attempts to breach system controls or obtain data. These attempts are unsuccessful and were stopped by standard preventative measures and have little to no impact on the ABS.

[redacted] Signature - Signed by [redacted] Staff/ABS on 30/03/2011 09:41:18 AM, according to /ABS

First Created By : [redacted] On : 23/03/2011 10:06:44 AM

## Police Involvement

Police involvement information is not required for this Incident.
Were police called? : ○ Yes ● No

## Administration

Investigator/s:

Investigation Started:

Investigation Ended: Thu 24/03/2011

### General

Security Description : Gateway
Security Incident : Gateway availability or Security
Incident Rating : Low

Summary of the Security Action taken :

Please provide summary of the action taken including any doclinks to relevant documents.This is part is to be filled when the investigation is completed.

Total Hours :

## Fraud

Fraud Method :
Type of Loss (if any) :
Specify Other Method :

Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :
Person Responsible: Relation with ABS :
Security Level :

## Document Access

Authors : [Security Staff], [Security Admin]
Readers : [Security Staff], [Security Admin]

## Related Documents

| Date Created | Doc Type |
| --- | --- |

## Reminder Information

Reminder Sent Date:
Reminder No.: 0

Next Reminder: 06/04/2011
Last Edited Date: 30/03/2011

## Edit History

Report Closed by [redacted] on 30/03/2011 09:41:06 AM
Incident Submitted by [redacted] on 23/03/2011 10:17:00 AM
Incident Created by [redacted] on 23/03/2011 10:08:35 AM

SIRs -Prod v2.0

# Incident Report

v 1.0

Incident : Gateway Issue - Hacking
Date Reported : 28/09/2010
Status : Closed - Resolved
Document ID : DWIR-89Q6KM

## Reporter Details

Reported By : [redacted] Staff/ABS
Created By : [redacted] Staff/ABS
Office : CO
Section : Network Services
Branch : Technology Infrastructure
Division : Technology Services Division
Phone : (02) 6252[redacted]
Location : CO 1S 329

## Incident Occurred

Incident Start date : Thu 23/09/2010
Start Time : 08:40 PM
Incident End Date (if over a period) : Thu 23/09/2010
End Time : 08:40 PM

State/Office Where Incident Occurred : CO
Where did the Incident Occur? ● Office ○ Outside Office
Describe the Location :

## Description

Tell us what happened :
Please provide short explanation of the incident including any information that could assist in its resolution such as the names of witnesses or contributing circumstances.

---

➲ Noted a number of access attempts in the Domino lockout section of the [redacted] report.

This is against Ausstats and SDB servers.

**SILVERTIP 2010-09-23 20:40:31 GMT+10:00**

**(SERVER: WebProd1051/SVR/ABSWebProd)**

**Warning(low): nHTTP: fakeuser[redacted]**
**authentication failure using internet password**

**MONKFISH 2010-09-23 20:40:34 GMT+10:00**
**(SERVER: WebProd1021/SVR/ABSWebProd)**
**Warning(low): nHTTP: fakeuser[redacted]**
**authentication failure using internet password**

**Whois info:**

**% This is the RIPE Database query service.**
**% The objects are in RPSL format.**
**%**
**% The RIPE Database is subject to Terms and Conditions.**
**% See http://www.ripe.net/db/support/db-terms-conditions.pdf**

**% Note: This output has been filtered.**
**% To receive output for a database update, use the "-B" flag.**

**% Information related to [redacted]**

inetnum: [redacted]
netname: CARNET-IRBZG
descr: Institut Rudjer Boskovic
descr: Bijenicka 54
descr: 10000 Zagreb
country: HR
admin-c: Cla22-RIPE
tech-c: Cla22-RIPE
status: ASSIGNED PA
mnt-by: AS2108-MNT
source: RIPE # Filtered

role: CARNet IP administrator
address: CARNet
address: J.Marohnica 5
address: 10000 Zagreb
address: Croatia
abuse-mailbox: abuse at carnet.hr
admin-c: IV762-RIPE
admin-c: DK2798-RIPE
tech-c: IV762-RIPE
tech-c: DK2798-RIPE
nic-hdl: Cla22-RIPE
mnt-by: AS2108-MNT
source: RIPE # Filtered

% Information related to '[redacted]16AS2108'

route: [redacted]
descr: CARNET
origin: AS2108
mnt-by: AS2108-MNT
source: RIPE # Filtered

Server Name : ➲ Elephantnose, Silvertip, monkfish

Incident Rating : ➲ Low

Please select one from the following that best Business Impact: Minimal.

describes impact.

Low level singular attempts to breach system controls or obtain data. These attempts are unsuccessful and were stopped by standard preventative measures and have little to no impact on the ABS.

Signature - Signed by [redacted] Staff/ABS on 15/10/2010 11:08:35 AM, according to /ABS

First Created By [redacted] On : 28/09/2010 01:51:22 PM

Police Involvement

Police involvement information is not required for this incident.
Were police called? : ○ Yes ● No

Administration

Investigator/s:

Investigation Started:

Investigation Ended: Fri 15/10/2010

General

Security Description : Gateway
Security Incident : Gateway availability or Security
Incident Rating : Low

Summary of the Security Action taken :
Please provide summary of the action taken including any doclinks to relevant documents.This is part is to be filled when the investigation is completed.

Total Hours :

Fraud

Fraud Method :
Type of Loss (if any) :
Specify Other Method :

Person Responsible:
Security Level :
Relation with ABS :

Person Responsible:
Security Level :
Relation with ABS :

Person Responsible:
Security Level :
Relation with ABS :

Document Access

Authors : [Security Staff], [Security Admin]
Readers : [Security Staff], [Security Admin]

Related Documents

| Date Created | Doc Type |
| --- | --- |

## Reminder Information

| | | | |
| --- | --- | --- | --- |
| Reminder Sent Date: | | Next Reminder: | 22/10/2010 |
| Reminder No.: | 0 | Last Edited Date: | 15/10/2010 |

## Edit History

Report Closed by [redacted] on 15/10/2010 11:08:34 AM
Incident Submitted by [redacted] on 28/09/2010 01:56:24 PM
Incident Created by [redacted] on 28/09/2010 01:51:38 PM