<table>
<thead>
<tr>
<th>Incident</th>
<th>Suspicious event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date Reported</td>
<td>03/08/2010</td>
</tr>
<tr>
<td>Document ID</td>
<td>DSTS-87Y6MV</td>
</tr>
<tr>
<td>Reporter Details</td>
<td></td>
</tr>
<tr>
<td>Reported By</td>
<td>Staff/ABS</td>
</tr>
<tr>
<td>Created By</td>
<td>Staff/ABS</td>
</tr>
<tr>
<td>Office</td>
<td>VIC</td>
</tr>
<tr>
<td>Section</td>
<td>No Section</td>
</tr>
<tr>
<td>Branch</td>
<td>Technology Services (Vic)</td>
</tr>
<tr>
<td>Division</td>
<td>Technology Services Division</td>
</tr>
<tr>
<td>Phone</td>
<td>(03) 9615</td>
</tr>
<tr>
<td>Location</td>
<td>VIC L5 WS 119</td>
</tr>
<tr>
<td>Incident Occurred</td>
<td></td>
</tr>
<tr>
<td>Incident Start date</td>
<td>Tue 03/08/2010</td>
</tr>
<tr>
<td>Incident End Date</td>
<td>Tue 03/08/2010</td>
</tr>
<tr>
<td>Start Time</td>
<td>12:15 PM</td>
</tr>
<tr>
<td>End Time</td>
<td>01:00 PM</td>
</tr>
<tr>
<td>State/Office Where Incident Occurred</td>
<td>CO</td>
</tr>
<tr>
<td>Where did the Incident Occur?</td>
<td>Office</td>
</tr>
<tr>
<td>Describe the Location :</td>
<td>Gateway environment - Main website servers</td>
</tr>
<tr>
<td>Other, was selected as part of Incident:</td>
<td>Noticed multiple security threats detected by our IPS devices and agents in the gateway</td>
</tr>
</tbody>
</table>
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.

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?  

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?:  

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 all OK to close;
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:  

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

Related Documents:  

<table>
<thead>
<tr>
<th>Date Created</th>
<th>Doc Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Reminder Information:  
Reminder Sent Date:  10/08/2010  
Reminder No.:  0  
Next Reminder:  17/08/2010  
Last Edited Date:  10/08/2010  

Edit History:  

## Incident Report

### Incident Details
- **Incident**: Theft - Other
- **Date Reported**: 03/10/2008
- **Document ID**: AWAN-7K35PN
- **Status**: Closed - Resolved

### Reporter Details
- **Reported By**: [Redacted]
- **Created By**: [Redacted]
- **Office**: CO
- **Section**: IT Communications
- **Branch**: [Redacted]
- **Division**: [Redacted]
- **Phone**: (02) 6252 [Redacted]
- **Location**: CO 1S 131

### Incident Occurred
- **Incident Start date**: Sat 27/09/2008
- **Start Time**: 02:00 AM
- **Incident End Date**: Mon 29/09/2008
- **End Time**: 07:00 PM

**State/Office Where Incident Occurred**
- CO

**Where did the Incident Occur?**
- 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 anybody injured? ○ Yes ● No ○ Not Applicable

Signature: Signed by [Signature] /Staff/ABS on 14/10/2008 02:19:56 PM, according to /Staff/ABS

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

Police Involvement:

Police involvement information is not required for this Incident.
Were police called? ○ Yes ● No
Investigator(s):
Investigation Started: 05/02/2009
Investigation Ended:

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 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: Relationship with ABS:
Security Level:
Person Responsible: Relationship with ABS:
Security Level:
Person Responsible: Relationship with ABS:
Security Level:

Document Access:
Incident Report

Incident: Suspicious event
Date Reported: 04/10/2012
Document ID: JGRN-SYR28H

Status: Closed - Resolved

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) 6292 [Redacted]
Location: CO 1S 329

Incident Occurred:
Incident Start Date: Wed 03/10/2012
Incident End Date: Wed 03/10/2012
Start Time: 01:26 PM
End Time: 01:26 PM

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

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 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:
Security Incident:
Incident Rating:
Summary of the Security Action taken:
Please provide summary of the action taken including any doctinks 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:
Relation with ABS:
Relation with ABS:
Incident Report

Incident: Suspicious event.
Date Reported: 26/10/2012
Document ID: JGRN-8ZET83

Status: Closed - Resolved

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
Incident End Date: Thu 25/10/2012
Start Time: 01:52 AM
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, Kuwait Number 9659903, and many other countries. The calls entered the ABS on [numbers redacted] and [numbers redacted] and left the ABS on [numbers redacted]. This is a Telstra ISDN circuit connected to out Polycom RMX Video Conferencing 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] on 27/06/2012 09:00:26 AM, according to [redacted]

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
Date Called:
Station Called:
Date Attended:
Name of Officer:
Action Police Taken
(if applicable):

State Police or AFP:
○ Yes ○ No
Time Called:
Police Attended:
Time Attended:
Police Reference Number
(if known):

Administration:

Investigator(s):
Staff/ABS
Investigation Started:
Wed 27/06/2012
Investigation Ended:

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 declines to relevant documents. This is part is to be filled when the investigation is completed.

Telstra Info

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 more likely it is to do with the billing cycle.
All,

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

Regards

---

Service Management Lead
Telstra Enterprise & Government
GPC Box 1827, Canberra ACT, 2601
1/L 3, 450 Northbourne Ave, Dickson, ACT 2602 Australia
Email: [Redacted]@team.telstra.com, Web: [Redacted]@team.telstra.com
Phone: 02 6121 0126, Mobile: [Redacted]

This communication may contain confidential or copyright information of Telstra Corporation Limited (ABN 33 051 775 556). If you are not an intended recipient, you must not keep, forward, copy, use, save or rely on this communication, and any such action is unauthorised and prohibited. If you have received this communication in error, please reply to this email to notify the sender of its incorrect delivery, and then delete both it and your reply.
WELCOME TO LIFE IN FULL COLOUR

From: 
Sent: Wednesday, 13 June 2012 10:34 AM
To: 
Cc: Lyn Little;
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](http://www.afp.gov.au).
- Fraud incident reports must be done in writing either via email, mail or fax, as per the [instructions on the AFP site](http://www.afp.gov.au). 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]

Account Executive | Telestra Enterprise & Government
P: (02) 6125 [redacted] M: [redacted]

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

---

13/08/2012 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>
Cc: [redacted]@team.telstra.com>
Date: 13/08/2012 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 252405; [redacted], Kuwait Number [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 Flexcap 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,
Account Executive | Telstra Enterprise & Government
P: (02) 6126 M: [redacted]

This communication may contain confidential or copyright information of Telstra Corporation Limited (ABN 32 051 775 556). If you are not an intended recipient, you must not keep, forward, copy, use, store or rely on this communication and any such action is unauthorised and prohibited. If you have received this communication in error, please reply to this email to notify the sender of its incorrect delivery, and then delete both it and your reply.

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

Person Responsible: [redacted]
Security Level: [redacted]
Relation with ABS: External to the ABS

Person Responsible: [redacted]
Security Level: [redacted]

Document Access:
<table>
<thead>
<tr>
<th>Type</th>
<th>Date</th>
<th>Time</th>
<th>Country Called</th>
<th>Number Called</th>
<th>Duration</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISDN</td>
<td>12-Jun</td>
<td>09:52pm</td>
<td>France</td>
<td>33141104</td>
<td>00:00:05</td>
<td>0.27</td>
</tr>
<tr>
<td>ISDN</td>
<td>12-Jun</td>
<td>09:57pm</td>
<td>Kuwait</td>
<td>96599037</td>
<td>00:00:06</td>
<td>0.37</td>
</tr>
<tr>
<td>ISDN</td>
<td>12-Jun</td>
<td>09:58pm</td>
<td>Ethiopia</td>
<td>25191138</td>
<td>00:00:07</td>
<td>0.51</td>
</tr>
<tr>
<td>ISDN</td>
<td>12-Jun</td>
<td>09:58pm</td>
<td>Afghanistan</td>
<td>93799474</td>
<td>00:06:10</td>
<td>14.92</td>
</tr>
<tr>
<td>ISDN</td>
<td>12-Jun</td>
<td>10:08pm</td>
<td>Ethiopia</td>
<td>251911192</td>
<td>00:35:04</td>
<td>83.75</td>
</tr>
<tr>
<td>ISDN</td>
<td>12-Jun</td>
<td>10:12pm</td>
<td>Ethiopia</td>
<td>25191374</td>
<td>00:00:38</td>
<td>1.74</td>
</tr>
<tr>
<td>ISDN</td>
<td>12-Jun</td>
<td>10:16pm</td>
<td>Ethiopia</td>
<td>25191300</td>
<td>00:05:27</td>
<td>13.21</td>
</tr>
<tr>
<td>ISDN</td>
<td>12-Jun</td>
<td>10:16pm</td>
<td>Taiwan</td>
<td>88695116</td>
<td>00:00:42</td>
<td>1.01</td>
</tr>
<tr>
<td>ISDN</td>
<td>12-Jun</td>
<td>10:20pm</td>
<td>Cuba</td>
<td>53582239</td>
<td>00:03:51</td>
<td>4.46</td>
</tr>
<tr>
<td>ISDN</td>
<td>12-Jun</td>
<td>10:30pm</td>
<td>Ethiopia</td>
<td>25191072</td>
<td>00:13:35</td>
<td>32.58</td>
</tr>
<tr>
<td>ISDN</td>
<td>12-Jun</td>
<td>10:32pm</td>
<td>Ethiopia</td>
<td>25191877</td>
<td>00:02:15</td>
<td>5.59</td>
</tr>
<tr>
<td>ISDN</td>
<td>12-Jun</td>
<td>10:32pm</td>
<td>USA Ohio</td>
<td>19377342</td>
<td>00:00:12</td>
<td>0.28</td>
</tr>
<tr>
<td>ISDN</td>
<td>12-Jun</td>
<td>10:42pm</td>
<td>Afghanistan</td>
<td>93773425</td>
<td>00:10:49</td>
<td>25.99</td>
</tr>
<tr>
<td>ISDN</td>
<td>12-Jun</td>
<td>10:50pm</td>
<td>Ethiopia</td>
<td>25192022</td>
<td>00:00:17</td>
<td>0.9</td>
</tr>
<tr>
<td>ISDN</td>
<td>12-Jun</td>
<td>10:52pm</td>
<td>Ethiopia</td>
<td>25192022</td>
<td>00:00:19</td>
<td>0.98</td>
</tr>
<tr>
<td>ISDN</td>
<td>12-Jun</td>
<td>10:53pm</td>
<td>Ethiopia</td>
<td>25192027</td>
<td>00:00:24</td>
<td>1.18</td>
</tr>
<tr>
<td>ISDN</td>
<td>12-Jun</td>
<td>10:55pm</td>
<td>Ethiopia</td>
<td>25192027</td>
<td>00:01:26</td>
<td>3.64</td>
</tr>
<tr>
<td>ISDN</td>
<td>12-Jun</td>
<td>10:57pm</td>
<td>Ethiopia</td>
<td>25192022</td>
<td>00:02:54</td>
<td>7.13</td>
</tr>
<tr>
<td>ISDN</td>
<td>12-Jun</td>
<td>11:00pm</td>
<td>Ethiopia</td>
<td>25191805</td>
<td>00:00:51</td>
<td>2.25</td>
</tr>
<tr>
<td>ISDN</td>
<td>12-Jun</td>
<td>11:02pm</td>
<td>Ethiopia</td>
<td>25191805</td>
<td>00:03:42</td>
<td>9.04</td>
</tr>
<tr>
<td>ISDN</td>
<td>12-Jun</td>
<td>11:06pm</td>
<td>Ethiopia</td>
<td>25192285</td>
<td>00:01:57</td>
<td>4.87</td>
</tr>
<tr>
<td>ISDN</td>
<td>12-Jun</td>
<td>11:09pm</td>
<td>Ethiopia</td>
<td>25133115</td>
<td>00:32:16</td>
<td>77.08</td>
</tr>
<tr>
<td>ISDN</td>
<td>12-Jun</td>
<td>11:09pm</td>
<td>Ethiopia</td>
<td>25191860</td>
<td>00:03:51</td>
<td>9.4</td>
</tr>
<tr>
<td>ISDN</td>
<td>12-Jun</td>
<td>11:15pm</td>
<td>Ethiopia</td>
<td>25191376</td>
<td>00:02:05</td>
<td>5.19</td>
</tr>
<tr>
<td>ISDN</td>
<td>12-Jun</td>
<td>11:16pm</td>
<td>Cuba</td>
<td>53532743</td>
<td>00:04:18</td>
<td>4.96</td>
</tr>
<tr>
<td>ISDN</td>
<td>12-Jun</td>
<td>11:22pm</td>
<td>Cuba</td>
<td>53422220</td>
<td>00:10:56</td>
<td>12.25</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>01:28am</td>
<td>Cuba</td>
<td>5353298</td>
<td>00:02:16</td>
<td>2.72</td>
</tr>
<tr>
<td>-------</td>
<td>--------</td>
<td>---------</td>
<td>------------</td>
<td>---------</td>
<td>----------</td>
<td>--------</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>01:30am</td>
<td>Cuba</td>
<td>5353219</td>
<td>00:01:44</td>
<td>2.13</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>01:31am</td>
<td>Cuba</td>
<td>5352461</td>
<td>00:18:14</td>
<td>20.28</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>01:33am</td>
<td>Cuba</td>
<td>5372093</td>
<td>00:03:00</td>
<td>3.53</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>01:34am</td>
<td>Cuba</td>
<td>5353110</td>
<td>00:04:09</td>
<td>4.79</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>01:40am</td>
<td>Cuba</td>
<td>5347524</td>
<td>00:02:18</td>
<td>2.76</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>01:42am</td>
<td>Cuba</td>
<td>5353274</td>
<td>00:26:44</td>
<td>29.63</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>01:44am</td>
<td>Ethiopia</td>
<td>2519130</td>
<td>00:00:44</td>
<td>1.97</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>01:46am</td>
<td>Cuba</td>
<td>5322635</td>
<td>00:16:23</td>
<td>18.25</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>01:52am</td>
<td>Ethiopia</td>
<td>2519113</td>
<td>00:00:20</td>
<td>1.02</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>01:54am</td>
<td>Cuba</td>
<td>5353508</td>
<td>00:14:23</td>
<td>16.05</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>01:57am</td>
<td>Cuba</td>
<td>5352371</td>
<td>00:04:17</td>
<td>4.94</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>01:58am</td>
<td>Ethiopia</td>
<td>2519111</td>
<td>00:00:42</td>
<td>1.89</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>01:59am</td>
<td>Cuba</td>
<td>5352372</td>
<td>00:02:24</td>
<td>2.87</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>02:00am</td>
<td>Greece</td>
<td>3069432</td>
<td>00:04:04</td>
<td>3.26</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>02:06am</td>
<td>Ethiopia</td>
<td>2519179</td>
<td>00:05:47</td>
<td>14</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>02:06am</td>
<td>Greece</td>
<td>3069439</td>
<td>00:14:31</td>
<td>11.05</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>02:08am</td>
<td>Cuba</td>
<td>5331560</td>
<td>00:01:41</td>
<td>2.08</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>02:09am</td>
<td>Ethiopia</td>
<td>2519219</td>
<td>00:10:13</td>
<td>24.56</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>02:11am</td>
<td>Ethiopia</td>
<td>2519114</td>
<td>00:09:38</td>
<td>23.17</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>02:12am</td>
<td>Ethiopia</td>
<td>2519114</td>
<td>00:03:46</td>
<td>9.2</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>02:17am</td>
<td>Ethiopia</td>
<td>2519217</td>
<td>00:46:48</td>
<td>111.7</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>02:22am</td>
<td>Cuba</td>
<td>5378308</td>
<td>00:05:21</td>
<td>6.11</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>02:24am</td>
<td>Cuba</td>
<td>5353219</td>
<td>00:06:20</td>
<td>7.19</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>02:24am</td>
<td>Ethiopia</td>
<td>2519234</td>
<td>00:01:54</td>
<td>4.75</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>02:26am</td>
<td>Ethiopia</td>
<td>2519209</td>
<td>00:22:10</td>
<td>53.02</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>02:27am</td>
<td>Cuba</td>
<td>5331560</td>
<td>00:11:30</td>
<td>12.88</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>02:40am</td>
<td>Cuba</td>
<td>5353219</td>
<td>00:09:50</td>
<td>11.04</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>02:42am</td>
<td>Oman</td>
<td>968989</td>
<td>00:00:01</td>
<td>0.25</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>02:43am</td>
<td>Ethiopia</td>
<td>2519144</td>
<td>00:00:22</td>
<td>1.1</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>02:44am</td>
<td>Ethiopia</td>
<td>2519144</td>
<td>00:08:49</td>
<td>21.23</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>02:45am</td>
<td>Ethiopia</td>
<td>2519209</td>
<td>00:27:52</td>
<td>66.6</td>
</tr>
<tr>
<td>ISDN</td>
<td>13-Jun</td>
<td>02:49am</td>
<td>Ethiopia</td>
<td>2519179</td>
<td>00:16:04</td>
<td>38.5</td>
</tr>
<tr>
<td>Date</td>
<td>Time</td>
<td>Region</td>
<td>Code</td>
<td>Duration</td>
<td>Rate</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>--------</td>
<td>-------------</td>
<td>-------------</td>
<td>------------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>05:30am</td>
<td>Senegal</td>
<td>221775363</td>
<td>00:08:40</td>
<td>20.87</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>05:31am</td>
<td>Cuba</td>
<td>535293915</td>
<td>00:25:56</td>
<td>28.75</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>05:32am</td>
<td>Ethiopia</td>
<td>251913721</td>
<td>00:02:58</td>
<td>7.29</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>05:34am</td>
<td>Ethiopia</td>
<td>251910042</td>
<td>00:14:23</td>
<td>34.49</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>05:36am</td>
<td>Cuba</td>
<td>535350415</td>
<td>00:18:35</td>
<td>20.67</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>05:38am</td>
<td>Cuba</td>
<td>535330353</td>
<td>00:03:46</td>
<td>4.37</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>05:40am</td>
<td>Ethiopia</td>
<td>251912703</td>
<td>00:08:13</td>
<td>19.8</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>05:42am</td>
<td>Ethiopia</td>
<td>251912064</td>
<td>00:48:40</td>
<td>116.14</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>05:44am</td>
<td>Cuba</td>
<td>535343730</td>
<td>00:00:45</td>
<td>1.05</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>05:47am</td>
<td>Cuba</td>
<td>537209452</td>
<td>00:00:01</td>
<td>0.25</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>05:48am</td>
<td>Cuba</td>
<td>537861093</td>
<td>00:07:44</td>
<td>8.73</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>05:53am</td>
<td>Ethiopia</td>
<td>251911371</td>
<td>00:12:17</td>
<td>29.48</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>05:57am</td>
<td>Cuba</td>
<td>534166364</td>
<td>00:15:57</td>
<td>17.77</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>06:00am</td>
<td>Cuba</td>
<td>535347489</td>
<td>00:13:01</td>
<td>14.55</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>06:05am</td>
<td>Ethiopia</td>
<td>251912604</td>
<td>00:21:56</td>
<td>52.47</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>06:07am</td>
<td>Cuba</td>
<td>537763565</td>
<td>00:00:21</td>
<td>0.61</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>06:09am</td>
<td>Cuba</td>
<td>537763569</td>
<td>00:09:21</td>
<td>10.51</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>06:11am</td>
<td>Cuba</td>
<td>535273849</td>
<td>00:13:08</td>
<td>14.67</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>06:15am</td>
<td>Ethiopia</td>
<td>251917324</td>
<td>00:07:01</td>
<td>16.94</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>06:18am</td>
<td>Cuba</td>
<td>535312946</td>
<td>00:13:01</td>
<td>14.55</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>06:18am</td>
<td>Eritrea</td>
<td>291820615</td>
<td>00:05:35</td>
<td>13.53</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>06:22am</td>
<td>Cuba</td>
<td>535354260</td>
<td>00:09:46</td>
<td>10.97</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>06:25am</td>
<td>Cuba</td>
<td>537794729</td>
<td>00:12:33</td>
<td>14.03</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>06:27am</td>
<td>Cuba</td>
<td>534561075</td>
<td>00:03:05</td>
<td>3.62</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>06:28am</td>
<td>Cuba</td>
<td>535373735</td>
<td>00:11:57</td>
<td>13.37</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>06:32am</td>
<td>Cuba</td>
<td>534561075</td>
<td>00:06:20</td>
<td>7.19</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>06:35am</td>
<td>Ethiopia</td>
<td>251912604</td>
<td>00:09:57</td>
<td>23.93</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>06:48am</td>
<td>Cuba</td>
<td>537694342</td>
<td>00:05:10</td>
<td>5.91</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>06:55am</td>
<td>Oman</td>
<td>968961530</td>
<td>00:09:15</td>
<td>12.84</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>06:55am</td>
<td>Cuba</td>
<td>537265835</td>
<td>00:26:07</td>
<td>28.96</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>06:58am</td>
<td>Cuba</td>
<td>532263473</td>
<td>00:09:32</td>
<td>10.71</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>06:59am</td>
<td>Cuba</td>
<td>537762673</td>
<td>00:15:48</td>
<td>17.61</td>
<td></td>
</tr>
<tr>
<td>13-Jun</td>
<td>07:03am</td>
<td>Cuba</td>
<td>535380589</td>
<td>00:05:05</td>
<td>5.82</td>
<td></td>
</tr>
</tbody>
</table>
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 our Polycom RMX Video Conferencing 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, [Redacted] IT Security Australian Bureau of Statistics
Police report details
Lyn Little to: [redacted] [redacted]
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
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 website](http://www.afp.gov.au)
- Fraud incident reports must be done in writing either via email, mail or fax, as per the [instructions on the AFP site](http://www.afp.gov.au)

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]

Account Executive | Telstra Enterprise & Government
P (02) 6128 [redacted] | M [redacted]

---

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,

Network Services
Australian Bureau of Statistics
p: +61 (0)2 6295 [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]

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

6 Attachments

afpcorporatesignature.gif 0F959934.jpg 0F426430.jpg 0F513960.gif 0F346605.gif 0F174602.jpg

Information added to the job.

Regards

[Signature]

SENIOR CONSTABLE
OPERATIONS MONITORING CENTRE
ACT POLICING
Tel +61(0) 2 6256, Fax +61(0) 2 6256
www.abs.gov.au

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

See below for updated information from Telstra.

Cheers,

[Signature]

Ag IT Security Advisor / TSD Change Manager
IT Security | Technology Services Division | Australian Bureau of Statistics

(P) (02) 6262 (M) ______________
(E) ______________________@abs.gov.au (W) www.abs.gov.au

------ Forwarded by ______________________ABS on 18/06/2012 03:41 PM ------

file:///C:/Users/ruttsi/AppData/Local/Temp/notes82945F/~web1221.htm 04/04/2013
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 02628 as at 20120618-1413.xlsx)

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

*********************************************************************************************

WARNING

This email message and any attached files may contain information that is confidential and subject of legal privilege intended only for use by the individual or entity to whom they are addressed. If you are not the intended recipient or the person responsible for delivering the message to the intended recipient be advised that you have received this message in error and that any use, copying, circulation, forwarding, printing or publication of this message or attached files is strictly forbidden, as is the disclosure of the information contained therein. If you have received this message in error, please notify the sender immediately and delete it from your inbox.

AFP Web site: http://www.afp.gov.au

*********************************************************************************************
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 userids (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:
<table>
<thead>
<tr>
<th>Security Description :</th>
<th>Unauthorised Access to ABS IT Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Rating :</td>
<td>Low</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Person Responsible:</th>
<th>Relation with ABS :</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Level :</td>
<td></td>
</tr>
<tr>
<td>Person Responsible:</td>
<td>Relation with ABS :</td>
</tr>
<tr>
<td>Security Level :</td>
<td></td>
</tr>
<tr>
<td>Person Responsible:</td>
<td>Relation with ABS :</td>
</tr>
<tr>
<td>Security Level :</td>
<td></td>
</tr>
</tbody>
</table>

---

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

**Readers :** [Security Staff], [Security Admin]
### Related Documents

<table>
<thead>
<tr>
<th>Date Created</th>
<th>Doc Type</th>
<th>CN=Chris Soczynski/OU=Staff/O=ABS</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/01/2013</td>
<td>Response By</td>
<td></td>
</tr>
</tbody>
</table>

### 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**
Document ID: NFIK-93K5L9
Response from: Chris Soczynski/Staff/ABS
Comments:
ip address belongs to a network managed in China

route: 
descr: China Mobile communications corporation
origin: AS3808
mnt-by: MAINT-CN-CMCC
changed: @chinamobile.com.26120245.
source: APNIC

person: 
nic-hid: MC285-AP
email: @cq.chinamobile.com
address: Room 1002, No. 5, Xingqiao International Building, Qianjiang New Area, Hangzhou, Zhejiang, 310012
phone: +86-
fax: +86-
country: cn
changed: @chinamobile.com.cn.26120245
mnt-by: MAINT-NEW
source: APNIC

Doclink: 
Date Response Created: 02/01/2013

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
 ○ Yes ○ No
Stolen/Lost/Damaged/Destroyed?

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 02:23:59 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 02/1/2013

Investigation Ended: Wed 02/1/2013

General

Security Description: Unauthorized 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: 
Security Level: 
Person Responsible: 
Security Level: 
Person Responsible: 
Security Level: 

Relation with ABS:

Relation with ABS:

Relation with ABS:

Document Access

Authors: [Security Staff], [Security Admin]
Readers: [Security Staff], [Security Admin]
<table>
<thead>
<tr>
<th>Date Created</th>
<th>Doc Type</th>
<th>CN=Chris Soczyński/OU=Staff/O=ABS</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/01/2013</td>
<td>Response By</td>
<td></td>
</tr>
</tbody>
</table>

**Reminder Information**

<table>
<thead>
<tr>
<th>Reminder Sent Date:</th>
<th>Next Reminder:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>09/01/2013</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reminder No.:</th>
<th>Last Edited Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>02/01/2013</td>
</tr>
</tbody>
</table>

**Edit History**

- Report Closed by Chris Soczyński 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
Comments:
ip address belongs to a network managed in China

route: 
descr: China Mobile communications corporation
origin: AS9808
mnt-by: MAINT-CN-CMCC
changed: person@chinamobile.com 26/2/2015
source: APNIC

person: 
role-hub: MC285-AP
e-mail: person@cq.chinamobile.com
address: 
phone: +86-
fax-no: +85-
country: cn
changed: person@chinamobile.com 26/2/2015
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.

Access using illegal characters... Buffer overflow attempt? Just registering this in case there is more occurrences.
<table>
<thead>
<tr>
<th>Agent Id</th>
<th>Agent Role/Tier</th>
<th>Full Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>ELEPHANTNOSE</td>
<td>2012-12-06 00:58:51 EST</td>
<td>(SERVER: WebProd1029/SVR/AWSWebProd) Warning(low): nHTTP: @&quot;Y%@8o,2,~2pqq@vk@-1]@vo-/81,1,1,.1,4&amp;@,8 &amp; ******** authentication failure using Internet password**</td>
</tr>
<tr>
<td>ELEPHANTNOSE</td>
<td>2012-12-06 01:04:58 EST</td>
<td>(SERVER: WebProd1820/SVR/AWSWebProd) Warning(low): nHTTP: @&quot;Y%@8o,2,~2pqq@vk@-1]@vo-/81,1,1,.1,4&amp;@,8 &amp; ******** authentication failure using Internet password**</td>
</tr>
<tr>
<td>ELEPHANTNOSE</td>
<td>2012-12-06 03:01:19 EST</td>
<td>(SERVER: WebProd1620/SVR/AWSWebProd) Warning(low): nHTTP: @&quot;Y%@8o,2,~2pqq@vk@-1]@vo-/81,1,1,.1,4&amp;@,8 &amp; ******** authentication failure using Internet password**</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Signature</th>
<th>Signed by: Staff/ABS on 14/12/2012 07:59:37 AM, according to: /Staff/ABS</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Created By: [Redacted] On: 07/12/2012 02:33:03 PM</td>
<td></td>
</tr>
</tbody>
</table>

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

Administration:
Investigator(s):
Investigation Started: Fri 14/12/2012
Investigation Ended:
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
<table>
<thead>
<tr>
<th>Date Created</th>
<th>Doc Type</th>
</tr>
</thead>
</table>

**Reminder Information**

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

**Edit History**

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

Incident: Illegal access to IT Network - external (hacking)
Date Reported: 12/11/2012
Document ID: TMMS-8ZXVFP

Status: Closed - Resolved

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: (92) 6282[Redacted]
Location: CO 1S 432

Incident Occurred

Incident Start Date: Fri 09/11/2012
Incident End Date: Fri 09/11/2012
Start Time: 11:01 PM
End Time: 11:01 PM

State/Office Where Incident Occurred
Where did the Incident Occur?

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.

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

For more information: [SOC-2012112-01 - Notes Attack [SEC=IN-CONFIDENCE:SECURITY]; Database: Security Operations Centre WDB; Author: [REDACTED]; Created: 12/11/2012; Doc Ref: TMMS-SZXUAV]

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 anybody 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.
1. Summary of attack

This is an unauthorised attempt to access ABSWebProd

<table>
<thead>
<tr>
<th>Start Time</th>
<th>End Time</th>
<th>Total Attempts</th>
<th>Successful Attempts</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012-11-09 11:01:35 pm</td>
<td>2012-11-09 11:01:35 pm</td>
<td>53</td>
<td>0</td>
</tr>
</tbody>
</table>

2. Target of attack

<table>
<thead>
<tr>
<th>Object</th>
<th>IPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monkfish</td>
<td></td>
</tr>
</tbody>
</table>

3. About the attacker

% 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 [Ip]provide common information services
descr: Linzi County, Zibo, 2563000
admin-c: JS686-AP
4. Attack profile

5. Attack description

Out of scope - automated reports

No further action is required.
Were police called?:  ○ Yes  ● No

Administration

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

General

Security Description:  Unauthorized Access to ABS IT Network
Security Incident:  
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:
Person Responsible:
Security Level:
Person Responsible:
Security Level:
Ad hoc attack, and all of their request failed. Nothing further to add.
Incident Report

Incident: Illegal access to IT Network - external (hacking)
Date Reported: 29/10/2012
Document ID: TMMS-8ZJ4ZH

Status: Closed - Resolved

Reporter Details:
Reported By: Staff/ABS
Created By: 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: Sat 27/10/2012
Start Time: 01:10 AM
End Time: 12:09 AM

State/Office Where Incident Occurred
Where did the Incident Occur?
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.

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.

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

First Created By: [Signature] Signed by: Staff/ABS on 05/11/2012 07:56:10 AM, according to ABS.

Police Involvement

Police Involvement Information is not required for this Incident.
Were police called?: ○ Yes ● No
Readers: [Security Staff], [Security Admin]

Related Documents:

<table>
<thead>
<tr>
<th>Date Created</th>
<th>Doc Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Reminder Information:

<table>
<thead>
<tr>
<th>Reminder Sent Date:</th>
<th>Next Reminder:</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/11/2012</td>
<td>12/11/2012</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reminder No.:</th>
<th>Last Edited Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>05/11/2012</td>
</tr>
</tbody>
</table>

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
### Attack Information

#### 1. Summary of attack

**Executive Summary:**
This attack was targeted over a week.

<table>
<thead>
<tr>
<th>Suburb</th>
<th>Start Time</th>
<th>End Time</th>
<th>Total Attempts</th>
<th>Successful Attempts</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012-10-22</td>
<td>09:01:10 EST</td>
<td>2012-10-27 00:00:18 EST</td>
<td>131</td>
<td>0</td>
</tr>
</tbody>
</table>

#### 2. Target of attack

<table>
<thead>
<tr>
<th>Target</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHORTEN</td>
<td></td>
</tr>
</tbody>
</table>

#### 3. About the attacker

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Various</td>
<td></td>
</tr>
</tbody>
</table>

#### 4. Attack profile
6. 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.

5. Report

out of scope - automated report

Security incident Report

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

**Incident:** Illegal access to IT Network - external (hacking)

**Date Reported:** 11/10/2012

**Document ID:** NFIK-8YXUU8

**Status:** Closed - Resolved

### Reporter Details

**Reported By:** [Redacted]

**Created By:** [Redacted]

**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:** 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*

**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


Out of scope - automated report

Details:
Has property been ☐ Yes ☐ No
Stolen/Lost/Damaged/Destroyed?
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: Unauthorized Access to ABS IT Network
Security Incident:
Incident Rating:

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

<table>
<thead>
<tr>
<th>Date Created</th>
<th>Doc Type</th>
</tr>
</thead>
</table>

**Reminder Information**

- Reminder Sent Date: 18/10/2012
- Next Reminder: 25/10/2012
- Reminder No.: 0
- 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
Incident Report

Incident: Illegal access to IT Network - external (hacking)
Date Reported: 09/10/2012
Document ID: NFIK-8YW362

Status: Closed - Resolved

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

Incident Occurred:
Incident Start date: Fri 05/10/2012
Incident End Date: 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 user/id's admin, tomcat, manager, user. All from ip address

<table>
<thead>
<tr>
<th>MONKFISH</th>
<th>2012-10-05 13:48:46 EST</th>
</tr>
</thead>
</table>
| WARNING! | r6HTTP: user [REDacted] authentication failure using internal password

Out of scope: automated report

Details:
Has property been O Yes O No
Stolen/Lost/Damaged/Destroyed?
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?: O Yes O No O Not Applicable

Signature: Signed by [REDACTED] Staff/ABS on 16/10/2012 09:12:57 AM, according to I/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 to ABS IT Network
Security Incident:    
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:
Security Level:
Relation with ABS:
Incident Report

Incident: Illegal access to IT Network - external (hacking)
Date Reported: 11/07/2012
Document ID: TMMS-8W495R

Status: Closed - Resolved

Reporter Details

Reported By: Staff/ABS
Created By: Staff/ABS
Office: CO
Section: Enterprise Systems and Software Management
Branch: Technology Infrastructure
Division: Technology Services Division
Phone: (02) 5252
Location: CO 15 452

Incident Occurred

Incident Start date: Tue 10/07/2012
Incident End Date: Wed 11/07/2012
Start Time: 10:30 AM
End Time: 01:23 AM

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

Description
Tell us what happened:
Please provide a 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.

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

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: Unauthorized 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]
1. Summary of attack

**Executive Summary**

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

<table>
<thead>
<tr>
<th>Start Time</th>
<th>End Time</th>
<th>Source Port</th>
<th>Session ID</th>
<th>Attempts</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012-07-10 10:31 am</td>
<td>2012-07-10 10:31 am</td>
<td>5124</td>
<td></td>
<td>201</td>
</tr>
<tr>
<td>2012-07-11 01:23 am</td>
<td>2012-07-11 01:23 am</td>
<td>5392</td>
<td></td>
<td>28</td>
</tr>
</tbody>
</table>

2. Target of attack

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>[REDACTED]</td>
<td>80, 3128, 8080, 8888</td>
</tr>
<tr>
<td></td>
<td>2929 - 6000</td>
</tr>
</tbody>
</table>

3. About the attacker

4. Attack profile

**Event types**

5. Attack description

This source is fishing for an unauthorised access point to gain entry into the ABS network. The attack was divided into a number of sessions which the attacker focused on are well known for various Trojans.
Open ports to connected servers appear to be correct, traffic was denied due to malformed TCP headers.
Incident Report

Description:

Incident Occurred: 

Internet Gateway: 

Office

Outside Office

Start Time: 10:29 AM 

End Time: 10:29 AM

Incident Date

Thu 21/06/2012

Incident Status:

Closed

Report Details:

Document ID: 

Date Reported: 21/06/2012

Incident:

Illegal access to IT Network - Exchange (accounting)
Tell us what happened:
Please provide a 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. A detailed breakdown can be found here.

Details:
Has property been Stolen/Lost/Damaged/Destroyed?

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

Was anybody injured?:

Signature: Signed by Staff/ABS on 29/06/2012 03:27:21 PM, according to ABS.

Police involvement:

Police involvement information is not required for this incident.
Were police called?:

Out of scope automated reports
Investigator/s: Staff/ABS
Investigation Started: Thu 21/06/2012
Investigation Ended: Mon 25/06/2012

Security Description: Unauthorised Access to ABS IT Network

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.

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:
1. Nature of attack

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

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Duration</th>
<th>Status</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012-06-21 10:29:13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2012-06-21 10:29:34</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30X8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. [Redacted] report

Out of scope

Automated reports

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

ABS Results

| Trafic | IP Address | App Name | EAV [Access]
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>mail.abs.gov.au</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>25</td>
<td>mail.test.abs.gov.au</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

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

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

Reporter Details:
Reported By: [Redacted]
Created By: [Redacted]
Office: CO
Section: Enterprise Systems and Software Management
Branch: Technology Infrastructure
Division: Technology Services Division
Phone: (02) 6252 [Redacted]
Location: CO 1S 452

Status: Closed - Resolved

Incident Occurred:
Incident Start Date: Thu 21/06/2012
Incident End Date: 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. A detailed breakdown can be found here and investigation by SOC is identified as SOC-20120621-01 - Attack.

Details:
Has property been stolen/lost/damaged/destroyed?

- 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?

- Police Involvement
Police involvement information is not required for this incident.

Out of scope: automated reports

Signature: Signed by: [Redacted] Staff/ARS on 25/06/2012 03:28:29 PM, according to IABS.

First Created By: [Redacted], On: 22/06/2012 08:12:06 AM
Were police called?:

Administration

Investigator/s: [Redacted]
Investigation Started: Thu 21/06/2012
Investigation Ended: Mon 25/06/2012

General:

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

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

(Security Incident: SOQ-20120612-01 - Attack by [Redacted] [SEC-CONFIDENTIALITY/SECURITY]; Database: Security Operations Centre WOB; Author: [Redacted]; Created: 22/06/2012; Doc Ref: TMMS-8V1425)

Total Hours:

Fraud:

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

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

Relation with ABS:
Relation with ABS:
Relation with ABS:
1. Nature of attack

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

<table>
<thead>
<tr>
<th>Target</th>
<th>Port</th>
<th>Service</th>
<th>Autonomic Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td></td>
<td>stream1.collection.abs.gov.au</td>
<td>Yes</td>
</tr>
<tr>
<td>443</td>
<td></td>
<td>www6.iprod.abs.gov.au</td>
<td>Yes</td>
</tr>
<tr>
<td>443</td>
<td></td>
<td><a href="http://www.nss.gov.au">www.nss.gov.au</a></td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>taxonomy-collaboration.sbr.abs.gov.au</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>----</td>
<td>-------------------------------------</td>
<td>-----</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>taxonomy-testing.sbr.abs.gov.au</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>www7.abs.gov.au</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>www4.abs.gov.au</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td><a href="http://www.growingup.gov.au">www.growingup.gov.au</a></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>alnwatchds.abs.gov.au</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>NDN Central</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>NDN Node</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>NDN Forums</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>Census Output Application</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>ace.abs.gov.au</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>secure.abs.gov.au</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>sbr-trax.test.abs.gov.au</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>reverseproxy.test.abs.gov.au</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>alnwatchds.test.abs.gov.au</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>nsx, and, sch</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>secure.test.abs.gov.au</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

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

Incident: Illegal access to IT Network - external (hacking)
Date Reported: 13/06/2012
Document ID: CHET-8V82EV

Status: Closed - Resolved

Reported By: [Redacted] Staff/ABS
Office: CO
Section: Network Services
Branch: Technology Infrastructure
Division: EXEC1

Created By: [Redacted] Staff/ABS
Office: CO
Section: Network Services
Branch: Technology Infrastructure
Division: Technology Services Division
Phone: (02) 6252 [Redacted]
Address: CO 1S 313
Location: CO 1S 509

Incident Occurred:

Incident Start date: Tue 12/06/2012
Incident End Date: Wed 13/06/2012
Start Time: 09:51 PM
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 a 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 - ausstats 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?

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?:

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

First Created By:
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**

<table>
<thead>
<tr>
<th>Security Description :</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Incident :</td>
<td>other</td>
</tr>
<tr>
<td>Incident Rating :</td>
<td></td>
</tr>
</tbody>
</table>

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

**Total Hours :**

**Fraud**

**Fraud Method :**

**Type of Loss (if any) :**

**Specify Other Method :**

<table>
<thead>
<tr>
<th>Person Responsible:</th>
<th>Relation with ABS :</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Level :</td>
<td></td>
</tr>
<tr>
<td>Person Responsible:</td>
<td>Relation with ABS :</td>
</tr>
<tr>
<td>Security Level :</td>
<td></td>
</tr>
<tr>
<td>Person Responsible:</td>
<td>Relation with ABS :</td>
</tr>
<tr>
<td>Security Level :</td>
<td></td>
</tr>
</tbody>
</table>

**Document Access**
Incident Report

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

Document ID: TMMS-7QJ3HZ

Reporter Details:

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

Incident Occurred

Incident Start date: Mon 23/03/2009
Incident End Date: Mon 23/03/2009
Start Time: 10:15 PM
End Time: 11:34 PM

State/Office Where Incident Occurred
Where did the Incident Occur?

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, 11:34:27 pm.

Detailed CDR records available on request.

Details:
Has property been Stolen/Lost/Damaged/Destroyed?

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?:

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 Socznak/Staff/ABS.
Investigation Started: Tue 31/03/2009
Investigation Ended: Tue 31/03/2009

General

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

Summary of the Security Action taken:
Please provide summary of the action taken including any doclinks to relevant documents. This is part 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:
Security Level:
Person Responsible:
Security Level:
Person Responsible:
Security Level:

Relation with ABS:

Relation with ABS:

Relation with ABS:

Document Access

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

Incident: Illegal access to IT Network - external (hacking)
Date Reported: 27/03/2009
Document ID: TMMS-7QHVP Across

Reported By: Staff/ABS
Created By: 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: 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: [Blank]
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. 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 ○ Yes ○ No
Stolen/Lost/Damaged/Destroyed?

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 Sochynski Staff/ABS on 31/03/2009 07:51:59 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
<table>
<thead>
<tr>
<th>Investigator/s:</th>
<th>Chris Soczynski/Staff/ABS,</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investigation Started:</td>
<td>Tue 31/03/2009</td>
</tr>
<tr>
<td>Investigation Ended:</td>
<td>Tue 31/03/2009</td>
</tr>
</tbody>
</table>

**General**

<table>
<thead>
<tr>
<th>Security Description:</th>
<th>Unauthorised Access to ABS IT Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Incident:</td>
<td></td>
</tr>
<tr>
<td>Incident Rating:</td>
<td></td>
</tr>
</tbody>
</table>

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

**Fraud**

<table>
<thead>
<tr>
<th>Fraud Method:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of Loss (if any):</td>
</tr>
<tr>
<td>Specify Other Method:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Person Responsible:</th>
<th>Relation with ABS:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Level:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Person Responsible:</th>
<th>Relation with ABS:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Level:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Person Responsible:</th>
<th>Relation with ABS:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Level:</td>
<td></td>
</tr>
</tbody>
</table>

**Document Access**

<table>
<thead>
<tr>
<th>Authors:</th>
<th>[Security Staff], [Security Admin]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Readers:</td>
<td>[Security Staff], [Security Admin]</td>
</tr>
</tbody>
</table>
**Incident Report**

**Incident:** Illegal access to IT Network - external (hacking)

**Date Reported:** 27/03/2009

**Document ID:** TMMS-7QHVD4

**Reporter Details**

- **Reported By:** [Redacted]
- **Created By:** [Redacted]
- **Office:** CO
- **Section:** IT Communications
- **Branch:**
- **Division:**
- **Phone:** (02) 6259 [Redacted]
- **Location:** CO 1S 341

**Incident Occurred**

<table>
<thead>
<tr>
<th>Incident Start date</th>
<th>Fri 20/03/2009</th>
<th>Start Time</th>
<th>06:35 PM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident End Date</td>
<td>Fri 20/03/2009</td>
<td>End Time</td>
<td>06:35 PM</td>
</tr>
</tbody>
</table>

**State/Office Where Incident Occurred**

- **CO**

**Where did the Incident Occur?**

- Office
- Outside Office

**Describe the Location:**

**Description:**

- [Redacted]
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. 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 anybody injured? ○ Yes ○ No ● Not Applicable

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

Security Description: Unauthorised Access 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: [Security Staff], [Security Admin]
Security Level:
Person Responsible: [Security Staff], [Security Admin]
Security Level:
Person Responsible: [Security Staff], [Security Admin]
Security Level:

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

Related Documents:

<table>
<thead>
<tr>
<th>Date Created</th>
<th>Doc Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Reminder Information:

<table>
<thead>
<tr>
<th>Reminder Sent Date:</th>
<th>Reminder No.:</th>
<th>Next Reminder:</th>
<th>Last Edited Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>07/04/2009</td>
<td>31/03/2009</td>
</tr>
</tbody>
</table>

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
**Incident Report**

**Incident:** Illegal access to IT Network - external (hacking)

**Date Reported:** 27/03/2009

**Document ID:** TMMS-7QHUJD

**Status:** Closed - Resolved

**Incident Occurred:**

- **Incident Start date:** Sat 14/03/2009
- **Incident End Date:** 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. Provide a description 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.

Calls from 200XX-0X00 were attempted at 1:31:17 pm, 1:31:40 pm, 1:31:55 pm, 1:52:17 pm.

Details:
- Has property been Stolen/Lost/Damaged/Destroyed?  
  - Yes
- Was any body injured?  
  - No

Details of people responsible for the incident:
- Name:
- Address:
- Phone:
- Email:
- Occupation:
- Relationship:
- Description:

Did you or someone else get hurt?  
- Yes
- No

Did you report to your manager?  
- Yes
- No

Did you alert the system administrator?  
- Yes
- No

Detailed CDR records available on request.

On: 27/03/2009 09:37:18 AM

First Created By: [Redacted]

Signature: [Redacted]
Security Description: Unauthorised Access to ABS IT Network

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.

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]
**Incident Report**

**Incident:** Illegal access to IT Network - external (hacking)

**Date Reported:** 21/07/2009

**Document ID:** DWIR-7U62X4

**Status:** Closed - Resolved

**Reporter Details**

<table>
<thead>
<tr>
<th>Reported By:</th>
<th>Staff/ABS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Created By:</td>
<td>Staff/ABS</td>
</tr>
<tr>
<td>Office:</td>
<td>CO</td>
</tr>
<tr>
<td>Section:</td>
<td>Internet Services</td>
</tr>
<tr>
<td>Branch:</td>
<td></td>
</tr>
<tr>
<td>Division:</td>
<td></td>
</tr>
<tr>
<td>Phone:</td>
<td>(02) 6252</td>
</tr>
<tr>
<td>Location:</td>
<td>CO IS 350</td>
</tr>
</tbody>
</table>

**Incident Occurred:**

| Incident Start date:   | Sun 19/07/2009 |
| Incident End Date:     | Sun 19/07/2009 |

| (If over a period):    |                  |

| 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.

Forum Noticed the following access attempt across a few domino servers:

<table>
<thead>
<tr>
<th>Server</th>
<th>Date</th>
<th>Time</th>
<th>Event Details</th>
</tr>
</thead>
</table>
SILVERTIP
2009-07-19 03:21:13.0
ELEPHANTNOSE
2009-07-19 03:21:14.0
SILVERTIP
2009-07-19 03:21:14.0

ORLANDONET OOD
BG-1226 Sofia
Bulgaria
+359 2

Spire BG OOD
BG-1000 Sofia
Bulgaria
+359 2

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

Police Involvement:
- Police involvement information is not required for this Incident.
- Was police called? :
  - Yes
  - No

Administration:
- Investigator/s: Staff/ABS,
- Investigation Started: Sun 19/07/2009
- Investigation Ended: Thu 30/07/2009

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

Summary of the Security Action taken: Please provide summary of the action taken including any links 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:
Incident Report

Incident: Other Unauthorised Access (not classified in choices)
Date Reported: 22/09/2011
Document ID: KMUN-8LWUJKZ

Reporter Details:
- Reported By: [redacted]
- Created By: [redacted]
- 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
- Office
- Outside Office

Where did the Incident Occur?
- 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.
<table>
<thead>
<tr>
<th>Agent Id</th>
<th>Agent Date/Time</th>
<th>Full Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>MONKFISH</td>
<td>2011-09-21 09:00:00 EST</td>
<td>(SERVER: WebProd1021/SVR/ABSWebProd) Warning(low): nHTTP: tomcat [redacted] authentication failure using internet password^a</td>
</tr>
<tr>
<td>MONKFISH</td>
<td>2011-09-21 09:00:02 EST</td>
<td>(SERVER: WebProd1021/SVR/ABSWebProd) Warning(low): nHTTP: tomcat [redacted] authentication failure using internet password^a</td>
</tr>
</tbody>
</table>
Police Involvement

Police Involvement Information is not required for this Incident.

Administration

Investigator/s:
Investigation Started:
Investigation Ended: Tue 27/09/2011

Security Incident: Unauthorised Access
Incident Rating: Other

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:

<table>
<thead>
<tr>
<th>Fraud Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of Loss (if any):</td>
</tr>
<tr>
<td>Specify Other Method:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Person Responsible</th>
<th>Security Level</th>
<th>Relation with ABS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Person Responsible</td>
<td>Security Level</td>
<td>Relation with ABS</td>
</tr>
<tr>
<td>Person Responsible</td>
<td>Security Level</td>
<td>Relation with ABS</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Document Access</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Authors:</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Security Staff], [Security Admin]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Readers:</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Security Staff], [Security Admin]</td>
</tr>
</tbody>
</table>

Related Documents:
Incident Report

Incident: Other Unauthorised Access (not classified in choices)
Date Reported: 16/09/2011
Document ID: KMUN-8LQV2W

Reporter Details:

- Reported By: [Redacted]
- Created By: [Redacted]
- Office: CO
- Section: Network Services
- Branch: Technology Infrastructure
- Division: Technology Services Division
- Phone: (02) 8252
- Location: CO 1S 332

Incident Occurred:

- Incident Start Date: Thu 15/09/2011
- Incident End Date (if over a period):
- Start Time: 06:37 PM
- 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 incident last week.

several attacks on the ausstats web servers using tomcat/manager/admin usernames
<table>
<thead>
<tr>
<th>Agent Id</th>
<th>Agent Date/Time</th>
<th>Full Message</th>
</tr>
</thead>
</table>
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:  Person Responsible:  Person Responsible:  Person Responsible:  
Security Level:  Security Level:  Security Level:  Security Level:  
Relation with ABS:  Relation with ABS:  Relation with ABS:  Relation with ABS:  

Document Access

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

Related Documents

<table>
<thead>
<tr>
<th>Date Created</th>
<th>Doc Type</th>
</tr>
</thead>
</table>

Reminder Information

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

Incident: Other Unauthorised Access (not classified in choices)
Date Reported: 14/09/2011
Document ID: JGRN-9LNVZ9

Status: Closed - Resolved

Report Details:
Reported By: [Redacted]
Created By: [Redacted]
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
Incident End Date: Thu 08/09/2011
Start Time: 05:17 AM
End Time: 05:18 AM

State/Office Where Incident Occurred
CO

Where did the Incident Occur?
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.
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
authentication failure using internet password

ELEPHANTNOSE 2011-09-08 05:17:16 EST
(SERVER: WebProd1020/SVR/ABSWebProd)

Warning(low): nHTTP: admin
authentication failure using internet password

ELEPHANTNOSE 2011-09-08 05:17:18 EST
(SERVER: WebProd1020/SVR/ABSWebProd)

Warning(low): nHTTP: admin
authentication failure using internet password

ELEPHANTNOSE 2011-09-08 05:17:19 EST
(SERVER: WebProd1020/SVR/ABSWebProd)

Warning(low): nHTTP: admin
authentication failure using internet password

ELEPHANTNOSE 2011-09-08 05:17:22 EST
(SERVER: WebProd1020/SVR/ABSWebProd)

Warning(low): nHTTP: admin
authentication failure using internet password

ELEPHANTNOSE 2011-09-08 05:17:23 EST
(SERVER: WebProd1020/SVR/ABSWebProd)

Warning(low): nHTTP: admin
authentication failure using internet password

ELEPHANTNOSE 2011-09-08 05:17:25 EST
(SERVER: WebProd1020/SVR/ABSWebProd)

Warning(low): nHTTP: admin
authentication failure using internet password

ELEPHANTNOSE 2011-09-08 05:17:26 EST
(SERVER: WebProd1020/SVR/ABSWebProd)

Warning(low): nHTTP: admin
authentication failure using internet password

ELEPHANTNOSE 2011-09-08 05:17:28 EST
(SERVER: WebProd1020/SVR/ABSWebProd)

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

ELEPHANTNOSE 2011-09-08 05:17:44 EST

Warning(low): nHTTP: manager authentication failure using internet password

ELEPHANTNOSE 2011-09-08 05:17:46 EST

Warning(low): nHTTP: manager authentication failure using internet password

ELEPHANTNOSE 2011-09-08 05:17:48 EST

Warning(low): nHTTP: manager authentication failure using internet password

ELEPHANTNOSE 2011-09-08 05:17:49 EST

Warning(low): nHTTP: manager authentication failure using internet password

ELEPHANTNOSE 2011-09-08 05:17:51 EST

Warning(low): nHTTP: manager authentication failure using internet password

ELEPHANTNOSE 2011-09-08 05:17:52 EST

Warning(low): nHTTP: manager authentication failure using internet password

ELEPHANTNOSE 2011-09-08 05:17:53 EST

Warning(low): nHTTP: manager authentication failure using internet password

MONKFISH 2011-09-08 05:17:07 EST

Warning(low): nHTTP: admin authentication failure using internet password

MONKFISH 2011-09-08 05:17:08 EST
authentication failure using internet password^A^A
MONKFISH 2011-09-08 05:17:09 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: admin^********^ authentication failure using internet password^A^A
MONKFISH 2011-09-08 05:17:11 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: admin^********^ authentication failure using internet password^A^A
MONKFISH 2011-09-08 05:17:12 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: admin^********^ authentication failure using internet password^A^A
MONKFISH 2011-09-08 05:17:13 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: admin^********^ authentication failure using internet password^A^A
MONKFISH 2011-09-08 05:17:15 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: admin^********^ authentication failure using internet password^A^A
MONKFISH 2011-09-08 05:17:17 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: admin^********^ authentication failure using internet password^A^A
MONKFISH 2011-09-08 05:17:18 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: admin^********^ authentication failure using internet password^A^A
MONKFISH 2011-09-08 05:17:21 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: admin^********^ authentication failure using internet password^A^A
MONKFISH 2011-09-08 05:17:22 EST
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: tomcat^********^ authentication failure using internet password^A^A
Warning(low): nHTTP: tomcat authentication failure using internet password
MONKFISH 2011-09-08 05:17:39 EST
(SERVER: WebProd1021/SVR/ABSWepProd)
Warning(low): nHTTP: manager authentication failure using internet password
MONKFISH 2011-09-08 05:17:40 EST
(SERVER: WebProd1021/SVR/ABSWepProd)
Warning(low): nHTTP: manager authentication failure using internet password
MONKFISH 2011-09-08 05:17:42 EST
(SERVER: WebProd1021/SVR/ABSWepProd)
Warning(low): nHTTP: manager authentication failure using internet password
MONKFISH 2011-09-08 05:17:44 EST
(SERVER: WebProd1021/SVR/ABSWepProd)
Warning(low): nHTTP: manager authentication failure using internet password
MONKFISH 2011-09-08 05:17:45 EST
(SERVER: WebProd1021/SVR/ABSWepProd)
Warning(low): nHTTP: manager authentication failure using internet password
MONKFISH 2011-09-08 05:17:46 EST
(SERVER: WebProd1021/SVR/ABSWepProd)
Warning(low): nHTTP: manager authentication failure using internet password
MONKFISH 2011-09-08 05:17:47 EST
(SERVER: WebProd1021/SVR/ABSWepProd)
Warning(low): nHTTP: manager authentication failure using internet password
MONKFISH 2011-09-08 05:17:49 EST
(SERVER: WebProd1021/SVR/ABSWepProd)
Warning(low): nHTTP: manager authentication failure using internet password
MONKFISH 2011-09-08 05:17:50 EST
(SERVER: WebProd1021/SVR/ABSWepProd)
Warning(low): nHTTP: manager authentication failure using internet password
<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>inetnum</strong></td>
<td>[REDACTED]</td>
</tr>
<tr>
<td><strong>netname</strong></td>
<td>HUARUI</td>
</tr>
<tr>
<td><strong>descr</strong></td>
<td>Langfang Development Area Huarui Xintong Network Technology Co., Ltd.</td>
</tr>
<tr>
<td><strong>descr</strong></td>
<td>Langfang university Langfang Development Area</td>
</tr>
<tr>
<td><strong>country</strong></td>
<td>CN</td>
</tr>
<tr>
<td><strong>admin-c</strong></td>
<td>WH271-AP</td>
</tr>
<tr>
<td><strong>tech-c</strong></td>
<td>WH271-AP</td>
</tr>
<tr>
<td><strong>changed</strong></td>
<td>[REDACTED] 20080520</td>
</tr>
<tr>
<td><strong>status</strong></td>
<td>ASSIGNED NON-PORABLE</td>
</tr>
<tr>
<td><strong>mnt-by</strong></td>
<td>MAINT-CNNIC-AP</td>
</tr>
<tr>
<td><strong>mnt-lower</strong></td>
<td>MAINT-CNNIC-AP</td>
</tr>
<tr>
<td><strong>mnt-routes</strong></td>
<td>MAINT-CNCGROUP-RR</td>
</tr>
<tr>
<td><strong>source</strong></td>
<td>APNIC</td>
</tr>
<tr>
<td><strong>route</strong></td>
<td>[REDACTED]</td>
</tr>
</tbody>
</table>
CNC Group CHINA169 Hebei Province network

descr: Addresses from CNNIC(HUARUI)
country: CN
origin: AS4837
mnt-by: MAINT-CNGROUP-RR
changed: 00238@cnc-noc.net 20080521
source: APNIC

person: 00238@cnc-noc.net
nic-hdl: WH271-AP
e-mail: 00238@cnc-noc.net
address: Langfang University Langfang Development Area
phone: +86-0316
fax-no: +86-0316

country: CN
changed: 00238@cnnic.cn 20080227
mnt-by: MAINT-CNINC-AP
source: APNIC

Police involvement

Police involvement information is not required for this incident.

Administration
Investigator/s:  
Investigation Started:  
Investigation Ended:  Tue 27/09/2011

<table>
<thead>
<tr>
<th>General</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Description :</td>
</tr>
<tr>
<td>Security Incident :</td>
</tr>
<tr>
<td>Incident Rating :</td>
</tr>
<tr>
<td>Summary of the Security Action taken :</td>
</tr>
<tr>
<td>Please provide summary of the action taken including any doctinks to relevant documents. This is part to be filled when the investigation is completed.</td>
</tr>
<tr>
<td>Spoken to Chris Soczynski and he is happy we just close off. These reports are useful for data in case DSD ever get involved.</td>
</tr>
<tr>
<td>Total Hours :</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud Method :</td>
</tr>
<tr>
<td>Type of Loss (if any) :</td>
</tr>
<tr>
<td>Specify Other Method :</td>
</tr>
<tr>
<td>Person Responsible:</td>
</tr>
<tr>
<td>Security Level :</td>
</tr>
<tr>
<td>Person Responsible:</td>
</tr>
<tr>
<td>Security Level :</td>
</tr>
<tr>
<td>Person Responsible:</td>
</tr>
<tr>
<td>Security Level :</td>
</tr>
<tr>
<td>Relation with ABS :</td>
</tr>
<tr>
<td>Relation with ABS :</td>
</tr>
<tr>
<td>Relation with ABS :</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Document Access:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authors : [Security Staff], [Security Admin]</td>
</tr>
<tr>
<td>Readers : [Security Staff], [Security Admin]</td>
</tr>
</tbody>
</table>
Incident Report

Incident: Other
Date Reported: 12/08/2011
Document ID: JGRN-8KN4Q7

Status: Closed - Resolved

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: Fri 12/08/2011
Start Time: 11:33 AM
End Time:

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

Describe the Location:

Other, was selected as part of Incident:

Please explain Security Description:

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

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]
Source Port Name: 60408
Sensor DNS Name: [redacted]
sensor.abs.gov.au
Sensor IP Address: [redacted]
Sensor Name: Server Protection for Windows
Destination DNS Name: www.censusfieldportal.abs.gov.au
Destination NetBIOS Name: [redacted]
IANAProtocolId: 6
IssueId: 2116062
Len: 448
PacketFlags: 5248
ResponseLevel: 5
SensorGUID: 1E1F43AA-E60B-42F3-9C21-7F8758F710F5


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])

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 [redacted] 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,

Thank you for contacting IBM Security Solutions! My name is [Redacted] and 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 you are experiencing the signature STTF_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 product that this signature is firing on to provide the proper steps on how to bypass this false positive.

Details:
Has property been [Redacted] Yes [Redacted] No
Stolen/Lost/Damaged/Destroyed?

Details of people responsible for the incident:
If known, please enter the names and addresses of people responsible for the incident.
Name: [Redacted] Address: [Redacted]

Was any body injured?: [Redacted] Yes [Redacted] No [Redacted] Not Applicable

[Signature - Signed by: [Redacted] Staff/ABS on 12/03/2011 10:12:24 AM; according to JABS] (Redacted)
First Created By: [Redacted] On: 12/08/2011 12:17:59 PM
Police Involvement

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

Administration

Investigator/s:

Investigation Started:  Fri 09/09/2011

Investigation Ended:  

General

Security Description:  Other
Security Incident:  other
Incident Rating:  

Summary of the Security Action taken:
Please provide summary of the action taken including any doctlinks 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:
Security Level:  
Relation with ABS:
**Incident Report**

**Incident:** Gateway Issue - Hacking  
**Date Reported:** 23/03/2011  
**Document ID:** JGRN-3F7V4Q  
**Status:** Closed - Resolved

**Reporter Details**

- **Reported By:**  
- **Created By:**  
- **Office:** CO  
- **Section:** Network Services  
- **Branch:** Technology Infrastructure  
- **Division:** Technology Services Division  
- **Phone:** (02) 8252*  
- **Location:** CO 1S 328

**Incident Occurred**

- **Incident Start Date:** Tue 22/03/2011  
- **Incident End Date:** Tue 22/03/2011  
- **Start Time:** 12:36 AM  
- **End Time:** 12:40 AM

**State/Office Where Incident Occurred**  
**Where did the Incident Occur?**  
- CO Office  
- □ Outside Office

**Describe the Location:**  
Somebody was trying multiple times to login into WebProd1070 with false username/password.
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: Automated Report Delivery - Gateway Services Daily Report [SEC=IN-CONFIDENCE:SECURITY]; Database: Firewall Reports WDB; Author Created: 22/03/2011; Doc Ref: NACT-8F7D8X)

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

# The following results may also be obtained via:
# http://whois.arin.net/rest/nets?q=\[\]
# showDetails=true&showARIN=false
#
Cox Communications Inc. NETBLK-OK-CBS-68-15-96-0 (NET-\[\])
Cox Communications Inc. COX-ATLANTA (NET-\[\])

# 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: 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.

First Created By: 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 part is to be filed when the investigation is completed.

Total Hours:

<table>
<thead>
<tr>
<th>Fraud</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud Method:</td>
<td></td>
</tr>
<tr>
<td>Type of Loss (if any):</td>
<td></td>
</tr>
<tr>
<td>Specify Other Method:</td>
<td></td>
</tr>
<tr>
<td>Person Responsible:</td>
<td>Relation with ABS:</td>
</tr>
<tr>
<td>Security Level:</td>
<td></td>
</tr>
<tr>
<td>Person Responsible:</td>
<td>Relation with ABS:</td>
</tr>
<tr>
<td>Security Level:</td>
<td></td>
</tr>
<tr>
<td>Person Responsible:</td>
<td>Relation with ABS:</td>
</tr>
<tr>
<td>Security Level:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Document Access</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Authors: [Security Staff], [Security Admin]</td>
<td></td>
</tr>
<tr>
<td>Readers: [Security Staff], [Security Admin]</td>
<td></td>
</tr>
</tbody>
</table>

Related Documents:
Incident Report

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

Status: Closed - Resolved

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 323

Incident Occurred:
Incident Start date: Thu 23/09/2010
Incident End Date: Thu 23/09/2010
Start Time: 08:40 PM
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 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: authentication failure using internet password

MONKFISH 2010-09-23 20:40:34 GMT+10:00
(SERVER: WebProd1021/SVR/ABSWebProd)
Warning(low): nHTTP: fakeuser: 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
inetnum: CARNET-IRBZG
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

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

route: CARNET
origin: AS2108
mnt-by: AS2108-MNT
source: RIPE # Filtered

Server Name:
Incident Rating:
Please select one from the following that best

- Elephantnose, Silvertip, monkfish
- Low
- 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.

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 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: