

1. ABUSIVE CONTENT
 - Spam
 - Harrasment
 - Child/Sexual/Violent
2. MALICIOUS CODE
 - Virus
 - Worm
 - Trojan
 - Spyware
 - Dialer
3. INFORMATION GATHERING
 - Scanning
 - Sniffing
 - Social Engineering
4. INTRUSION ATTEMPTS
 - Exploiting of known Vulnerabilities
 - Login Attempts
 - New Attack Signature
5. INTRUSIONS
 - Priviliged Account Compromise
 - Unpriviliged Account Compromise
 - Application Compromise
6. AVAILABILITY
 - DoS
 - DDoS
 - Sabotage
7. INFORMATION SECURITY
 - Unauthorized Access to Information
 - Unauthorized Modification of Information
8. FRAUD
 - Unauthorized Use of Resources
 - Copyright
 - Masquerade
9. OTHER

Report examples included in these exercises are taken from actual reports submitted to the CERT Polska team. Data in most of the reports were sanitized or otherwise altered in the following manner:

- * All personal data was erased or changed to fictitious characters
- * 10.187/16 is used for networks owned by NASK
- * Rest of 10/8 is used for other networks in Poland
- * Content of the reports written in Polish was translated into English when needed

Try to explain what really happened and classify the reports using list of categories used in CERT Polska as a reference. Explain, what can a CSIRT do to help the reporters or a site that was affected during the incident.

Exercise 1:

To: cert@cert.pl
From: info@cert.pl
Subject: [ARAKIS] Scanning from IP 10.17.131.34

IP address: 10.17.131.34
Date start: 2005-06-22 09:04:40
Date end: 2005-06-22 11:43:09
Packets: 20

Date	Time	IP src	IP dst	Port
2005-06-22	11:43:09	10.17.131.34	10.187.245.184	TCP/8080
2005-06-22	11:43:09	10.17.131.34	10.187.245.184	TCP/6588
2005-06-22	11:43:09	10.17.131.34	10.187.245.184	TCP/3128
2005-06-22	11:43:09	10.17.131.34	10.187.245.184	TCP/1080
2005-06-22	11:43:09	10.17.131.34	10.187.245.184	TCP/1080
2005-06-22	11:43:09	10.17.131.34	10.187.245.184	TCP/80
2005-06-22	11:43:09	10.17.131.34	10.187.245.184	TCP/80
2005-06-22	11:43:09	10.17.131.34	10.187.245.184	TCP/23
2005-06-22	11:43:09	10.17.131.34	10.187.245.184	TCP/23
2005-06-22	11:42:59	10.17.131.34	10.187.245.184	TCP/113
2005-06-22	09:04:51	10.17.131.34	10.187.245.184	TCP/8080
2005-06-22	09:04:51	10.17.131.34	10.187.245.184	TCP/6588
2005-06-22	09:04:51	10.17.131.34	10.187.245.184	TCP/3128
2005-06-22	09:04:51	10.17.131.34	10.187.245.184	TCP/1080
2005-06-22	09:04:51	10.17.131.34	10.187.245.184	TCP/1080
2005-06-22	09:04:51	10.17.131.34	10.187.245.184	TCP/80
2005-06-22	09:04:51	10.17.131.34	10.187.245.184	TCP/80
2005-06-22	09:04:51	10.17.131.34	10.187.245.184	TCP/23
2005-06-22	09:04:51	10.17.131.34	10.187.245.184	TCP/23
2005-06-22	09:04:40	10.17.131.34	10.187.245.184	TCP/113

Exercise 2:

To: cert@cert.pl
From: info@cert.pl
Subject: [ARAKIS] Scanning from IP 10.136.40.185

IP address: 10.136.40.185
Date start: 2005-06-22 20:34:53
Date end: 2005-06-22 20:46:10
Packets: 40

Date	Time	IP src	IP dst	Port
2005-06-22	20:46:10	10.136.40.185	10.187.103.159	TCP/445
2005-06-22	20:45:53	10.136.40.185	10.187.103.153	TCP/445
2005-06-22	20:45:36	10.136.40.185	10.187.103.228	TCP/445
2005-06-22	20:45:33	10.136.40.185	10.187.103.178	TCP/445
2005-06-22	20:45:31	10.136.40.185	10.187.103.254	TCP/445
2005-06-22	20:45:30	10.136.40.185	10.187.103.220	TCP/445
2005-06-22	20:45:16	10.136.40.185	10.187.103.150	TCP/445
2005-06-22	20:45:14	10.136.40.185	10.187.103.144	TCP/445
2005-06-22	20:44:49	10.136.40.185	10.187.103.182	TCP/445
2005-06-22	20:44:44	10.136.40.185	10.187.103.241	TCP/445
2005-06-22	20:44:39	10.136.40.185	10.187.103.247	TCP/445
2005-06-22	20:44:24	10.136.40.185	10.187.103.194	TCP/445
2005-06-22	20:44:23	10.136.40.185	10.187.103.139	TCP/445
2005-06-22	20:43:48	10.136.40.185	10.187.103.151	TCP/445
2005-06-22	20:42:57	10.136.40.185	10.187.103.156	TCP/445
2005-06-22	20:42:51	10.136.40.185	10.187.103.154	TCP/445
2005-06-22	20:42:49	10.136.40.185	10.187.103.238	TCP/445
2005-06-22	20:42:48	10.136.40.185	10.187.103.180	TCP/445
2005-06-22	20:42:26	10.136.40.185	10.187.103.202	TCP/445
2005-06-22	20:41:27	10.136.40.185	10.187.103.226	TCP/445
2005-06-22	20:41:15	10.136.40.185	10.187.103.153	TCP/445
2005-06-22	20:41:04	10.136.40.185	10.187.103.196	TCP/445
2005-06-22	20:40:39	10.136.40.185	10.187.103.242	TCP/445
2005-06-22	20:40:36	10.136.40.185	10.187.103.178	TCP/445
2005-06-22	20:40:12	10.136.40.185	10.187.103.209	TCP/445
2005-06-22	20:39:54	10.136.40.185	10.187.103.199	TCP/445
2005-06-22	20:39:44	10.136.40.185	10.187.103.151	TCP/445
2005-06-22	20:39:27	10.136.40.185	10.187.103.215	TCP/445
2005-06-22	20:39:21	10.136.40.185	10.187.103.210	TCP/445
2005-06-22	20:39:01	10.136.40.185	10.187.103.209	TCP/445
2005-06-22	20:38:34	10.136.40.185	10.187.103.155	TCP/445
2005-06-22	20:38:13	10.136.40.185	10.187.103.228	TCP/445
2005-06-22	20:38:09	10.136.40.185	10.187.103.171	TCP/445
2005-06-22	20:37:44	10.136.40.185	10.187.103.205	TCP/445
2005-06-22	20:37:40	10.136.40.185	10.187.103.204	TCP/445

Exercise 3:

From: Kokos <XXXX@XXX.pl>
To: spam@cert.pl
Subject: [Fwd: NASA to buy!]

[-- Attachment #1 --]
[-- Type: text/plain, Encoding: 7bit, Size: 0.2K --]

--

sender's signature here

[-- Attachment #2: NASA to buy! --]
[-- Type: message/rfc822, Encoding: 7bit, Size: 1.3K --]

X-Account-Key: account3
X-mf: first3.pl v0.6
From: Andy <delonia@free.fr>
Subject: NASA to buy!
To: xxxxx@xx.pl
Reply-To: offi@hotmail.nl

[-- Attachment #3: Casino with free deposit --]
[-- Type: message/rfc822, Encoding: 7bit, Size: 1.1K --]

X-Account-Key: account2
From: kogzaal@dfg.com
Subject: Casino with free deposit

Online gaming has reached a <acj></acj>new <acy></acy>level
with <aco></aco>huge developments <acy></acy>in the internet.

I along with a select group of internet professional
<ack></ack>tried a number of online gaming sites, the results
were extraordinary.
We found the Highest pay out
percentages <aca></aca>in <acq></acq>the industry, Most secure
and profitable places on the net, with the best online support
working 24/7.
These Sites provide what every
<acq></acq>player needs, a guaranteed positive online gaming
experience. <acv></acv>If you have any interest in this new
world of <acj></acj>entertainment you have <ack></ack>no
choice but try it yourself.

www.casinosfree.com

Sincerely, kogzaal@dfg.com

Exercise 4:

From: bilbo <xxxxxxx@xx.pl>
To: cert@cert.pl
Subject: intrusion

Name of reporter: John Doe
Phone: 1-555-573-031
Fax:
Company Name:
E-mail: xxxxxxx@xx.pl
Alternative E-mail:
Incident happened: recently on June 20, 2005
Incident spotted: June 20, 2005
Attacked host/IP: 10.31.242.178
OS: Windows.98

Description:

Weird things happen to my PC (eg. it reboots at the end of installation. Occasionally my Panda Antivirus Software blocks an attack from IP 10.22.128.1¹)

Remarks:

¹ Note: This IP address was not sanitized. It is put here in the form as it appeared in the original report

Exercise 5:

```
From: _Michele_ <x.xxxxxxx@xxxxxxx.it>
To: postmaster@katowice.pl, postmaster@nask.net.pl
Subject: [spam] [email]: help
Resent-To: Abuse NASK <abuse@nask.pl>,
          Postmaster NASK <postmaster@nask.pl>
ReSent-Subject: [spam] [email]: help
```

Dear postmaster,
please deal with following unsolicited e-mail I've recently
received: it's a commercial advertisement not requested by me
and I don't want any more of it.

The 'Received:' headers show it comes from
(HELO xxxxxx.polsl.katowice.pl) (10.158.128.xxx)

see:
<http://dsbl.org/listing?10.158.128.xxx>

```
#####
whois katowice.pl
katowice.pl = [ ]
  Domain object:
    domain:      katowice.pl
    registrant's handle: nsk001 (CORPORATE)
    nservers:    kirdan.nask.net.pl
                a.nask.pl a10: 1: 1: 0: 0: 0:
44][195.187.245.44]
  created:      2003.03.25
  last modified: 2005.02.03
  registrar: nask
  option: the domain name has not option
  Holder's Contact object:
    company: NAUKOWA I AKADEMICKA SIEC KOMPUTEROWA
    street:  UL. WAWOZOWA 18
    city:    02-796 WARSZAWA
    location: PL
    handle: nsk001
    last modified: 2003.03.29
    registrar: nask
    Whois database last updated: 2005.06.21
#####
```

Thank you
Best regards

```
##### Email with full headers: #####
Return-Path: <qvteqkz@hotmail.com>
Delivered-To: x.xxxxxxx@xxxxxxx.it
```

Received: (gmail 16428 invoked from network); 21 Jun 2005
12:39:34 -0000
Received: from unknown (HELO xxxxxx.polsl.katowice.pl)
(10.158.128.xxx)
by mail.lombardiacom.it with SMTP; 21 Jun 2005 12:39:34 -
0000
FCC: mailbox://qvteqkz@hotmail.com/Sent
X-Identity-Key: id1
Date: Tue, 21 Jun 2005 17:38:03 +0400
From: Ronny Kirkpatrick <qvteqkz@hotmail.com>
X-Accept-Language: en-us, en
MIME-Version: 1.0
To: x.xxxxxxxxx@xxxxxxxxxxxxx.it
Subject: help
Content-Type: multipart/related;
boundary="-----090602010907080700060001"
Status: RO
X-Status: RT
X-KMail-EncryptionState: N
X-KMail-SignatureState: N
X-KMail-MDN-Sent:

This is a multi-part message in MIME format.

-----090602010907080700060001
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: 7bit

```
<html><head><meta http-equiv="Content-Type"
content="text/html;
charset=iso-8859-1"></head><body bgcolor="#FFFFFF4"
text="#11168B"><p><IMG
SRC="cid:part1.00030601.07090102@ecitzlol@yahoo.com"
border="0"
ALT=""></p><p><font color="#FFFFFF2">Gnutella in 1842 Marijuana
Nostradamus</font></p><p><font color="#FFFFFF0">in 1996 Pull
yourself
together!</font></p></body></html>
```

Exercise 6:

From: xxxx@xxxxx.edu.pl
To: cert@cert.pl
Subject: Logs from a curious attacker

[-- Attachment #1: Mail message body --]
[-- Type: text/plain, Encoding: 7bit, Size: 0.1K --]

Reporter's signature here

[-- Attachment #2: Text from file 'login_failed.csv' --]
[-- Type: text/plain, Encoding: 7bit, Size: 1.9M --]

TextData	HostName	StartTime	LoginName
Login failed for user 'sa'.	DEKKO	16.06.2005 13:50:42	sa
Login failed for user 'sa'.	DEKKO	16.06.2005 13:50:43	sa
Login failed for user 'sa'.	DEKKO	16.06.2005 13:50:43	sa
Login failed for user 'sa'.	DEKKO	16.06.2005 13:50:43	sa
Login failed for user 'sa'.	DEKKO	16.06.2005 13:50:43	sa
Login failed for user 'sa'.	DEKKO	16.06.2005 13:50:43	sa
Login failed for user 'sa'.	DEKKO	16.06.2005 13:50:44	sa
Login failed for user 'sa'.	DEKKO	16.06.2005 13:51:29	sa
Login failed for user 'sa'.	DEKKO	16.06.2005 13:51:43	sa
Login failed for user 'sa'.	DEKKO	16.06.2005 13:52:15	sa
Login failed for user 'sa'.	DEKKO	16.06.2005 13:52:18	sa
Login failed for user 'sa'.	DEKKO	16.06.2005 13:52:20	sa
Login failed for user 'sa'.	DEKKO	16.06.2005 13:52:21	sa
Login failed for user 'sa'.	DEKKO	16.06.2005 13:52:21	sa
Login failed for user 'sa'.	DEKKO	16.06.2005 13:52:22	sa
Login failed for user 'sa'.	DEKKO	16.06.2005 13:52:22	sa

Exercise 7:

From: reiner@vp.pl
To: info@cert.pl
Subject: advice

I'd be very grateful for any information regarding removal of a website from the resources of the internet search engine gogle.pl. thank you.

Exercise 8:

X-Original-To: cert@fingon2.nask.waw.pl
From: XXXXXXXX XXXXXXXXXXXX <XXXXXX@XXXX.EDU.PL>
To: spam@cert.pl
Subject: Spam o jakichś tam akcjach

[-- Attachment #1 --]
[-- Type: text/plain, Encoding: 7bit, Size: 0.1K --]

-kl

[-- Attachment #2 --]
[-- Type: message/rfc822, Encoding: 7bit, Size: 5.2K --]

X-Original-To: XXXXX@XXXX.EDU.PL
Mail-From: andrzej.sielecki@o2.pl Wed Jun 15 08:45:30 2005
X-Orig-From: Andrzej Sielecki <andrzej.sielecki@o2.pl>
Subject: [PLUG-Z] Prasa finansowa i emisje akcji | Jaka wiarygodność?
From: Andrzej SXXXXXXX via PLUG-Z <plug-z@linux.org.pl>
To: plug-z <plug-z@linux.org.pl>
X-Cc: Andrzej SXXXXXXX <andrzejXXXXXXX@o2.pl>
X-List: plug-z@linux.org.pl
Reply-To: plug-z@linux.org.pl
X-Spam-Checker-Version: SpamAssassin 3.0.3 (2005-04-27) on
lsd.camk.edu.pl
X-Spam-Level: *
X-Spam-Status: No, score=1.8 required=4.0
tests=BAYES_05,DCC_CHECK,HTML_50_60,
HTML_MESSAGE autolearn=no version=3.0.3

Na przykładzie spółki Ambra inwestorzy instytucjonalni jasno dali wyraz temu, co sądzą o spółce. W rezultacie wprowadzający akcje odstąpił od przeprowadzenia Oferty Sprzedaży Akcji Serii A w Transzy Inwestorów Instytucjonalnych oraz Ambra ustaliła cenę emisyjną na 9,50 - blisko dolnej granicy przedziału 9-13 zł.

Rzeczpospolita natomiast wydrukowała artykuł 8 czerwca 2005, w dniu rozpoczęcia zapisów, pod zachęcającym tytułem (i treścią): "Walory nie tylko dla smakoszy". W załączonych linkach jest artykuł z Rzeczpospolitej i niezależny raport o spółce Ambra, który został upowszechniony w kręgu inwestorów instytucjonalnych.

Co sądzą inwestorzy instytucjonalni o spółce, a co serwuje się publiczności?

Warto przeczytać i porównać.

[some links follow]

Exercise 9:

To: cert@cert.pl
From: Internet Identity <service@internetidentity.com>
Subject: ASSISTANCE REQUESTED -- FRAUD PHISHING WEBSITE -
HACKED IP 10.210.98.130

2005-06-14

Dear Poland Cert:

We are contacting you on behalf of VISA International regarding an urgent abuse matter. The following site:

<<http://10.210.98.130/~ivanhoe/visa.com/webscr-id/secure-SSL/cmd-run=/index.html>><http://10.210.98.130/~ivanhoe/visa.com/webscr-id/secure-SSL/cmd-run=/index.html>

is illegally attempting to collect the credit card information of innocent users. Due to the duration of this attack, our client has become extremely concerned. We have contacted the provider several times requesting assistance, and each time our requests are apparently disregarded. The provider is Xxxxx.pl. I have personally spoken with Mario at 1 555 302233 and he has informed me that the matter will be investigated.

Please assist us in getting this site shut down.

Thanks,

Client Services
Internet Identity -- on behalf of VISA International

service@internetidentity.com
+1 253 590 4100

Full-Service Phishing Prevention
<http://www.internetidentity.com>

Exercise 10:

From: support@xxxxxxxxxxxxx.com
To: abuse@nask.pl
Cc: hostmaster@nask.pl
Subject: abuse!

Hello abuse,

A hour ago we receive too many internet connections from your network.

It seems someone ddos our site.

Please check you net!

```
#netstat -an | grep "SYN" | grep "10.187."  
tcp      0      0 172.50.187.195:80    10.187.56.223:1749    SYN_RECV  
tcp      0      0 172.50.187.195:80    10.187.56.234:1142    SYN_RECV  
tcp      0      0 172.50.187.195:80    10.187.55.82:1848     SYN_RECV  
tcp      0      0 172.50.187.195:80    10.187.50.235:1304    SYN_RECV  
tcp      0      0 172.50.187.195:80    10.187.56.194:1765    SYN_RECV  
tcp      0      0 172.50.187.195:80    10.187.55.92:1824     SYN_RECV  
tcp      0      0 172.50.187.195:80    10.187.56.236:1498    SYN_RECV  
tcp      0      0 172.50.187.195:80    10.187.54.203:1255    SYN_RECV  
tcp      0      0 172.50.187.195:80    10.187.55.202:1662    SYN_RECV  
tcp      0      0 172.50.187.195:80    10.187.56.2:1762      SYN_RECV  
tcp      0      0 172.50.187.195:80    10.187.55.91:1458     SYN_RECV  
tcp      0      0 172.50.187.195:80    10.187.55.81:1766     SYN_RECV  
tcp      0      0 172.50.187.195:80    10.187.55.243:1651    SYN_RECV  
tcp      0      0 172.50.187.195:80    10.187.56.215:1399    SYN_RECV  
tcp      0      0 172.50.187.195:80    10.187.50.234:1732    SYN_RECV  
tcp      0      0 172.50.187.195:80    10.187.56.227:1971    SYN_RECV  
tcp      0      0 172.50.187.195:80    10.187.55.101:1960    SYN_RECV  
tcp      0      0 172.50.187.195:80    10.187.56.228:1348    SYN_RECV  
tcp      0      0 172.50.187.195:80    10.187.55.232:1114    SYN_RECV  
tcp      0      0 172.50.187.195:80    10.187.55.118:1458    SYN_RECV  
tcp      0      0 172.50.187.195:80    10.187.55.88:1532     SYN_RECV  
tcp      0      0 172.50.187.195:80    10.187.50.224:1698    SYN_RECV  
tcp      0      0 172.50.187.195:80    10.187.54.181:1399    SYN_RECV  
tcp      0      0 172.50.187.195:80    10.187.56.214:1672    SYN_RECV  
tcp      0      0 172.50.187.195:80    10.187.55.192:1038    SYN_RECV  
tcp      0      0 172.50.187.195:80    10.187.55.85:1373     SYN_RECV  
tcp      0      0 172.50.187.195:80    10.187.55.224:1936    SYN_RECV  
[...]
```

Exercise 11:

From: ttc <144752xxxx@reports.spamcop.net>
To: cert@cert.pl
Subject: [SpamCop (10.181.191.130) id:144752xxxx]IDC Mobility
Roadshow CEE 2005- 23 czerwca

[SpamCop V1.460]
This message is brief for your comfort. Please use links
below for details.

Email from 10.181.191.130 / Tue, 14 Jun 2005 12:47:36 +0200
<http://www.spamcop.net/w3m?i=z14475xxxx0z32814a006420a550da5f469ca742dea7z>

[Offending message]
Return-Path: <x>
Received: from idcserver.idc.local (unknown [10.181.191.130])
by x (Neo MailServer) with ESMTP id 92C2A38F6A
for <x>; Tue, 14 Jun 2005 12:47:36 +0200 (CEST)
Subject: IDC Mobility Roadshow CEE 2005- 23 czerwca
Date: Tue, 14 Jun 2005 12:49:38 +0200
Message-ID: <A19C_____8FBA@idcserver.idc.local>
MIME-Version: 1.0
X-Content-Type: multipart/alternative;
boundary="----_=_NextPart_001_01C570CE.C2F60D6A"
X-MS-Has-Attach:
X-MS-TNEF-Correlator:
content-class: urn:content-classes:message
X-MimeOLE: Produced By Microsoft Exchange V6.0.6603.0
Thread-Topic: IDC Mobility Roadshow CEE 2005- 23 czerwca
Thread-Index:
AcVsKV/SPVJdebPaRm6wf31iHcHmsgAABgAQADANptAAAP+msAArxLwAAAyCE
AAIU+UAAANBFAAAAkblAAABkcUAAB5RbgAABWfQAAAHTRoAAANCngAMEL0iA=
From: "Magda Brandt" <mbrandt@idcpoland.pl>
To: "Magda Brandt" <x>
Content-Type: text/plain
X-SpamCop-note: Converted to text/plain by SpamCop
(outlook/eudora hack)

IDC Mobility Roadshow CEE 2005

23 czerwca, Warszawa, hotel Westin

W stronę mobilnego przedsiębiorstwa

[...]

Exercise 12:

From: Zenobius Xavierus <xxxxxxxxxx@xx.pl>
To: cert@cert.pl
Subject: Someone fooling people out of ID cards

Hello,

Name of reporter: Peter B.
Phone: 1-555-223-017
Fax:
Company Name:
E-mail: xxxxxxxx@xx.pl
Alternative E-mail:
Incident happened: 11.06.2005
Incident spotted: 11.06.2005 12:00
Attacked host/IP: N/A
OS: N/A

Description:

Someone is trying to trick people into giving away ID over Instant Messenger software, "as a hobby". I attach the message I received:

879xxxx (12:05)

Hi, My name is Judy and I'm 19. I collect ID cards. If you own a scanner or a digital camera and want to help me to extend my collection, I'll be very thankful. I know my hobby is unusual, but at least it's not common ☺

I'm pretty sure the scans collected this way are later used for taking loans, setting up fictional bank account etc.

--

regards
Peter

Exercise 13:

From: xxxxx xxxx <xxxxxxxxxxxxxxxx@xxxxxx.xx>
Subject: abuse report
To: abuse@nask.pl

Hello;

here i come to you to report an abuse, i received : Wed, 08 Jun 2005 05:47:57 +0000i : 3 mails wich every one of them contain lot of insults towards my self the mails i received are listen below and those mails contain a links to a webpage wich contain all my private information and lot of insults and linked to a porn websites. all the research i made about the IP sender senders drive us to this IP : 10.17.41.72 after trace this IP it sends us to your internet privider so all ask for is to stop this person or provide us information about this user to let the justice and lawyer finish them work.

i must say that there is not only me wich is touched by this user, we are 9 person in all .please note that all the private information given in the mail a real

waiting for your response please agree Mister all my greetings.

Thank you

(Xxxx xxxxx)

-----here is the mail received : in intact format and the all the mail information. (copie les mails et l'entete de chaque mail)

original version :
Xxxxx XXXXX el kahba el maz3ouka

galek xxxx xxxxxx el maz3ouka a une tete ta3 rass zeb zebi bent biskra el kavia !!!!!!!!! hicham gali il l a encul\351 fel berraqa dialha pour 50 dinar!!!!
la mere ta3 el kalba amel sassi kahba kalba fi biskra xxxx xxxxx kahba salope maz3ouka hatchounha fi a3mrou34 ans kalba fi barbes ya zeb zebi !!!!
ila 7abitou atnikou el kahba xxxxx xxxxx batel hawlik
l'adresse dialha

Sassi Amel
8 rue XXXXXXX 7xxxxx PARIS
xx xx xxx xxx xx

[translation of insults into english follows]

Exercise 14:

From: fox-no-reply@copyright-compliance.com
Subject: Copyright Infringement Notice ID: 27-39403
To: abuse@nask.pl

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Re: Unauthorized Use of Twentieth Century FOX Film Corporation Property

Notice ID:27-39403
Notice Date:7 Jun 2005 17:25:14 GMT

Dear Sir or Madam:

TWENTIETH CENTURY FOX FILM CORPORATION and its affiliated companies (collectively, "FOX") are the exclusive owners of copyrights in motion pictures.

It has come to our attention that NASK is the service provider for the IP address listed below, from which unauthorized copying and distribution (downloading, uploading, file serving, file "swapping" or other similar activities) of FOX'S property is taking place. The documentation included at the end of this notice specifies the location of the infringement. We believe that the Internet access of the user engaging in this infringement is provided by NASK or a downstream service provider who purchases this connectivity from NASK.

This unauthorized copying and distribution constitutes copyright infringement under applicable national laws and international treaties. Although various legal and equitable remedies may be available to FOX as a result of such infringement, FOX believes that the entire Internet community benefits when these matters are resolved cooperatively. We urge you to take immediate action to effect removal of the detected infringement listed in the attached report, including:

- (1) Notify the account holder of this infringement
- (2) Request the account holder remove the infringing material
- (3) Disable access to the infringing material
- (4) Take appropriate action against the account holder under your Abuse Policy/Terms of Service

We appreciate your efforts toward this common goal. Please send us a prompt response indicating the actions you have taken to resolve this matter. Please reference the above noted Notice ID in the subject line of all email correspondence.

The undersigned has a good faith belief that use of FOX's property in the manner described herein is not authorized by FOX, its agents or the law. Also, we hereby state, under penalty of perjury, under the laws of the State of California and under the laws of the United States, that the information in this notification is accurate and that the undersigned is authorized to act on behalf of FOX with respect to this matter.

Please be advised that this letter is not and is not intended to be a complete statement of the facts or law as they may pertain to this matter or of FOX's positions, rights or remedies, legal or equitable, all of which are specifically reserved.

Please contact us at the above listed address or by replying to this email should you have any questions. Also note that this infringement notice contains an XML tag that can be used to automate the processing of this data. If you would like more information on how to use this tag, please do not hesitate to contact BayTSP.

Very truly yours,
Sarah Bergman
Compliance Manager
BayTSP, Inc.
PO Box 1314
Los Gatos, CA 95031

v: 408-341-2300
f: 408-341-2399

[A pgp public key is available on the key server at ldap://keyserver.pgp.com if you would like to verify the authenticity of this notice.]

Evidentiary Information:

Notice ID: 39403
Asset: Star Wars - Episode III: Revenge of the Sith
Protocol: eDonkey
IP Address: 10.81.133.40
DNS: xxxxx.xxxx.waw.pl
File Name: Revenge Of The Sith Starwars Iii.avi
File Size: 734734336
Timestamp: 7 Jun 2005 13:54:39 GMT
Last Seen Date: 7 Jun 2005 13:54:39 GMT
URL: ed2k://|file|Revenge Of The Sith Starwars Iii.avi|734734336|3E60A0690C85DE29E0E5C61FA037E331|/
Username (if available):

[above information in XML format]

-----BEGIN PGP SIGNATURE-----
Version: 8.0

iD8DBQFCpdzrUONhpY5vJJIRAuEMAKC0p0xkJenQu7YRSCGMx2tM3ibsdgCfeOIC
9ktex+m3Mj7Ux3Ydxh+81H0=
=78o5

-----END PGP SIGNATURE-----

Exercise 15:

From: XXXXXXXX XXXXXXXX <xxx@xxxxxxxxxxxxxxxxxxxx.pl>
To: "'cert@cert.pl'" <cert@cert.pl>
Subject: attacks

Hi,

Today I got rid of a dos on 1 company. From what I know, the attck came from the follwing addresses:

207.xxx.xxx.211/32;
130.xxx.xxx.131/32;
66.xxx.xxx.105/32;
209.xxx.xxx.146/32;
216.xxx.xxx.143/32;

doing eg telnet 216.xxx.xxx.143 31337

:Welcome!psyBNC@lam3rz.de NOTICE * :psyBNC2.3.2-5

All they have irc-bots on them. Can you do something about it?
The attacks are lame, so it's probably a script-kiddie we're dealing with.

Regards,

XXXXXXXXXX XXXXXXXXXX.