Trend Micro™
Data Loss Prevention

Trend Micro™ Data Loss Prevention 5.2
(formerly LeakProof)
Data Leakage through certain HTTP/HTTPS channels

Alejandro Hernández H. a.k.a nitrØus
nitrousenador@gmail.com

http://www.brainoverflow.org
http://nitr0us.blogspot.com
June 1st, 2010
Mexico

DISCLAIMER:
The author is not responsible for the misuse of the information presented in this document.
This security advisory should be used for educational purposes only.

1.- VULNERABILITY INFORMATION

Vendor: Trend Micro™
Product Name: Data Loss Prevention (formerly LeakProof).
Vulnerable versions: DLP 5.2 and LeakProof <= 5.0
Product URL:
http://us.trendmicro.com/us/products/enterprise/data-loss-prevention/index.html
Author: nitrØus [Alejandro Hernandez H.]
Discovery Date: 09/Sept/2009
Disclosure Date: 01/Jun/2010
Attack Vector: Local
Attack Channels: Some HTTP/HTTPS non-analyzed channels
Impact: Data Theft / Data Leakage / Data Loss
Risk: Medium

2.- PRODUCT INFORMATION

Trend Micro™ Data Loss Prevention (DLP) is a family of solutions that secure your private data and intellectual property, while reducing complexity and costs. You'll gain broad coverage, high performance, and deployment flexibility needed to comply with regulatory mandates that protect employee and customer data. Trend Micro DLP solutions also offer advanced DataDNA™ fingerprinting to secure unstructured data and intellectual property and protect all data modalities: data at rest, data in use and data in motion.

Trend Micro™ DLP for Endpoint – non-intrusive monitoring and enforcement client software detects and prevents data loss at each endpoint, across the broadest variety of threat vectors, whether online or off.

Trend Micro™ DLP Management Server – provides a central point of visibility and control for discovery, fingerprint extraction, policy enforcement, and reporting violations. The server is available as a hardware appliance or software virtual appliance—for greater flexibility and lower costs.

File Types Supported

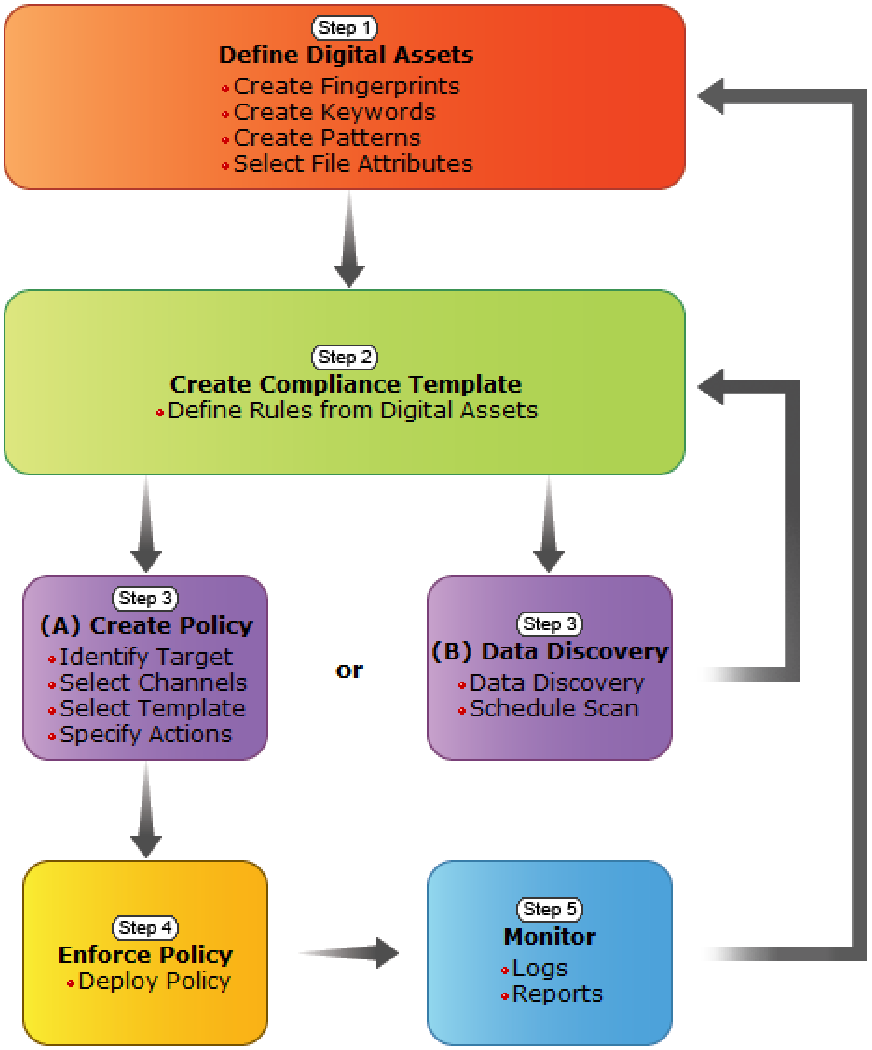
- Recognizes and processes 300+ file types
- Microsoft™ Office files including Office 2007: Microsoft Word, Excel, PowerPoint, Outlook™ email; Lotus™ 1-2-3, OpenOffice, RTF, Wordpad, Text, etc.
- Graphics files: Visio, Postscript, PDF, TIFF, etc.
- Software/engineering files: C/C++, JAVA, Verilog, AutoCAD, etc.
- Archived/compressed files: Win ZIP, RAR, TAR, JAR, ARJ, 7Z, RPM, CPIO, GZIP, BZIP2, Unix/Linux ZIP, LZH, etc.

Network/Applications Controlled

- Email: Microsoft Outlook, Lotus Notes and SMTP Email

- Web mail: MSN/Hotmail, Yahoo, GMail, AOL Mail, and more
- Instant Messaging: MSN, AIM, Yahoo, and more
- Network Protocols: FTP, HTTP/HTTPS and SMTP Endpoint Devices Controlled
- USB, CD/DVD, COM & LPT ports, removable disks, floppy, infrared and imaging devices, print screen, modems, PCMCIA

Workflow



3.- DISCLOSURE TIMELINE

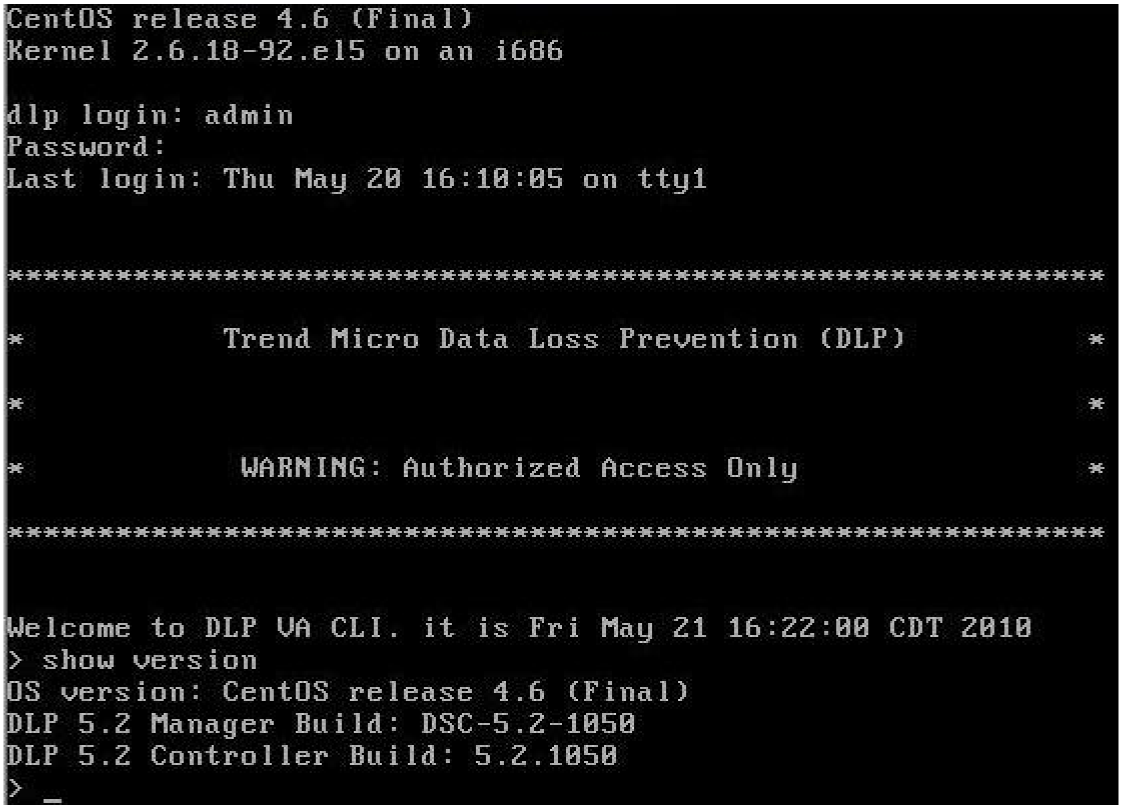
DD/MM/YYYY

09/09/2009 The vulnerability was discovered.
20/02/2010 Trend Micro was informed about the vulnerability.
21/02/2010 Trend Micro assigned a Service Request Number #1
23/02/2010 Trend Micro asked to reproduce the vulnerability with certain policies and Web browsers as well as the details of the testing environment.
23/02/2010 Details sent, including screenshots.
25/02/2010 Trend Micro, asked again to retest LeakProof in certain circumstances.
03/03/2010 Service Request #1 automatically closed due to inactivity
16/03/2010 Trend Micro assigned a Service Request Number #2
16/03/2010 Thread retaken and I explained to Trend Micro about the technical nature of the flaw
18/03/2010 I got no response, so, I warned them about the soon public disclosure
24/03/2010 Service Request #2 automatically closed due to inactivity
23/03/2010 Trend Micro assigned a Service Request Number #3
23/03/2010 Thread retaken and Trend Micro asked me to debug and log all the endpoint activity
31/03/2010 Explained about the results and no answer received from Trend Micro
06/04/2010 Service Request #3 automatically closed due to inactivity
21/05/2010 Retested the vulnerability against the latest version of Data Loss Prevention (5.2)
01/06/2010 Public Disclosure

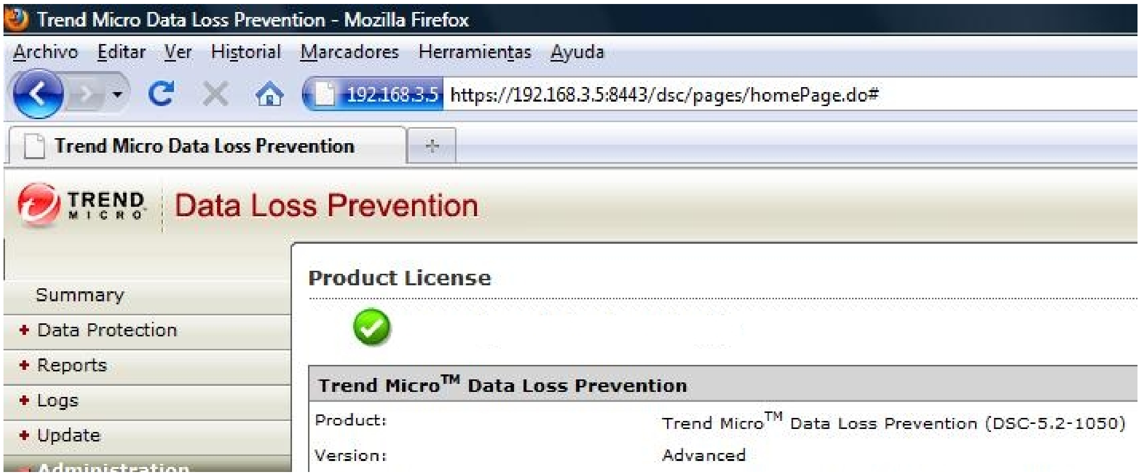
4.- TESTING ENVIRONMENT

4.1.- Management Server

Operating System: CentOS 4.6 (Kernel 2.6.18-92.el5)
Management Server: DLP 5.2.1050



```
CentOS release 4.6 (Final)
Kernel 2.6.18-92.el5 on an i686

dlp login: admin
Password:
Last login: Thu May 20 16:10:05 on tty1


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

*           Trend Micro Data Loss Prevention (DLP)           *

*                                                            *

*            WARNING: Authorized Access Only                 *

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


Welcome to DLP VA CLI. it is Fri May 21 16:22:00 CDT 2010
> show version
OS version: CentOS release 4.6 (Final)
DLP 5.2 Manager Build: DSC-5.2-1050
DLP 5.2 Controller Build: 5.2.1050
> _
```



https://192.168.3.5:8443/dsc/pages/homePage.do#

Product License

✓

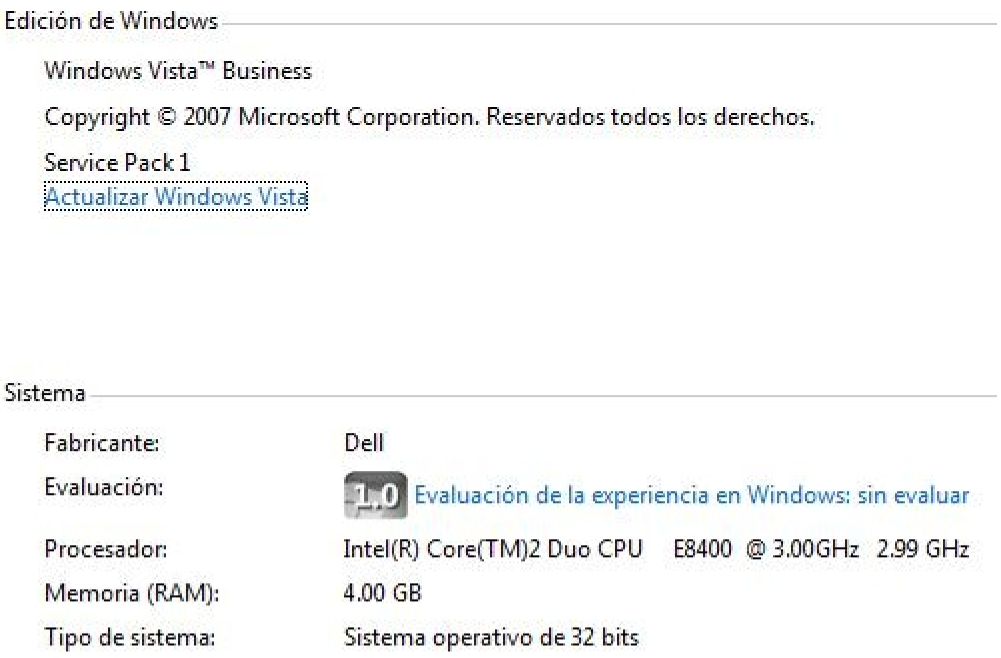
Trend Micro™ Data Loss Prevention

Product: Trend Micro™ Data Loss Prevention (DSC-5.2-1050)

Version: Advanced

4.2.- Endpoints

Operating System: Windows Vista^{TM} Business SP1
DLP Agent: 5.2.1053 (Patch applied)



Edición de Windows

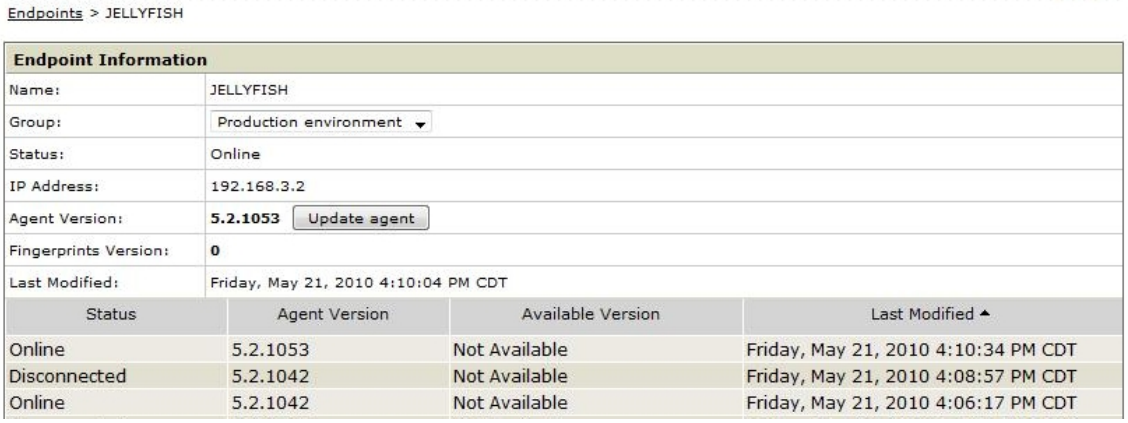
Windows Vista™ Business

Copyright © 2007 Microsoft Corporation. Reservados todos los derechos.

Service Pack 1
Actualizar Windows Vista

Sistema

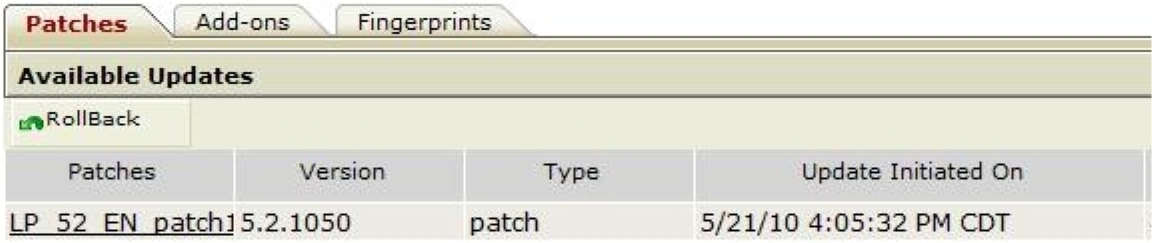
Fabricante:	Dell
Evaluación:	1,0 Evaluación de la experiencia en Windows: sin evaluar
Procesador:	Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GHz 2.99 GHz
Memoria (RAM):	4.00 GB
Tipo de sistema:	Sistema operativo de 32 bits



Endpoints > JELLYFISH

Endpoint Information	
Name:	JELLYFISH
Group:	Production environment
Status:	Online
IP Address:	192.168.3.2
Agent Version:	**5.2.1053** Update agent
Fingerprints Version:	**0**
Last Modified:	Friday, May 21, 2010 4:10:04 PM CDT

Status	Agent Version	Available Version	Last Modified ▲
Online	5.2.1053	Not Available	Friday, May 21, 2010 4:10:34 PM CDT
Disconnected	5.2.1042	Not Available	Friday, May 21, 2010 4:08:57 PM CDT
Online	5.2.1042	Not Available	Friday, May 21, 2010 4:06:17 PM CDT



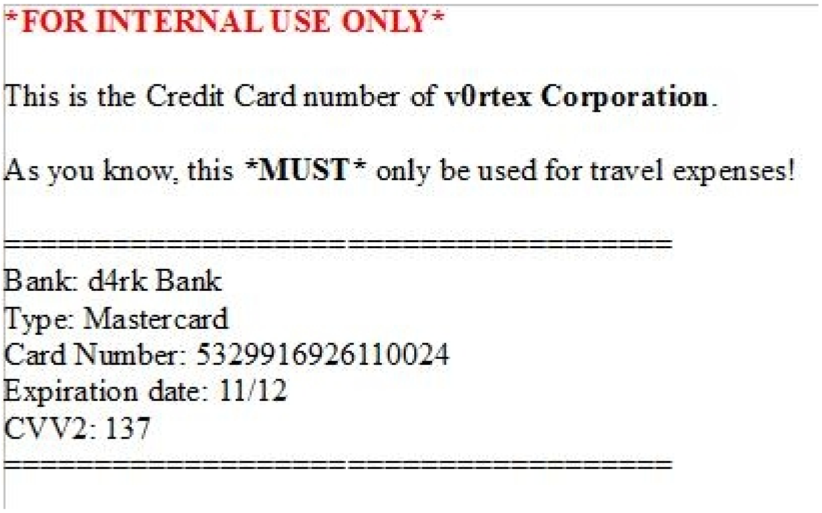
Available Updates

Patches	Version	Type	Update Initiated On
LP_52_EN_patch1	5.2.1050	patch	5/21/10 4:05:32 PM CDT

5.- VULNERABILITY EXPLAINATION / EXPLOIT

5.1.- Files to protect

The information contained in these files are for demonstration purposes only, hence, the shown data is not real.



FOR INTERNAL USE ONLY

This is the Credit Card number of **v0rtex Corporation**.

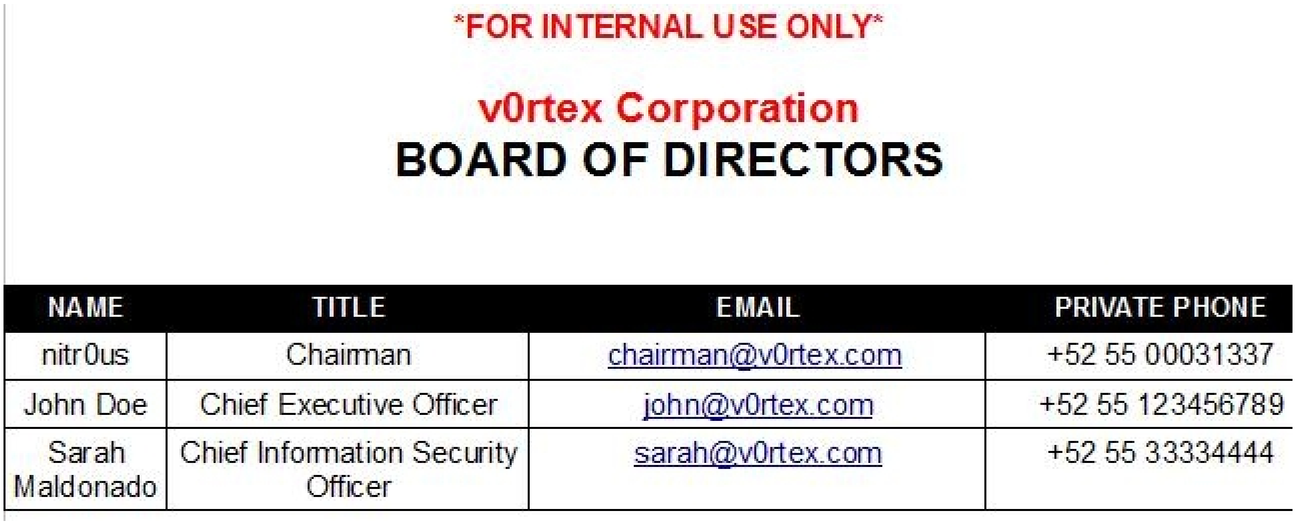
As you know, this ***MUST*** only be used for travel expenses!

==

Bank: d4rk Bank
Type: Mastercard
Card Number: 5329916926110024
Expiration date: 11/12
CVV2: 137

==

MS Word document (.doc) containing a valid ***Credit Card Number***



FOR INTERNAL USE ONLY

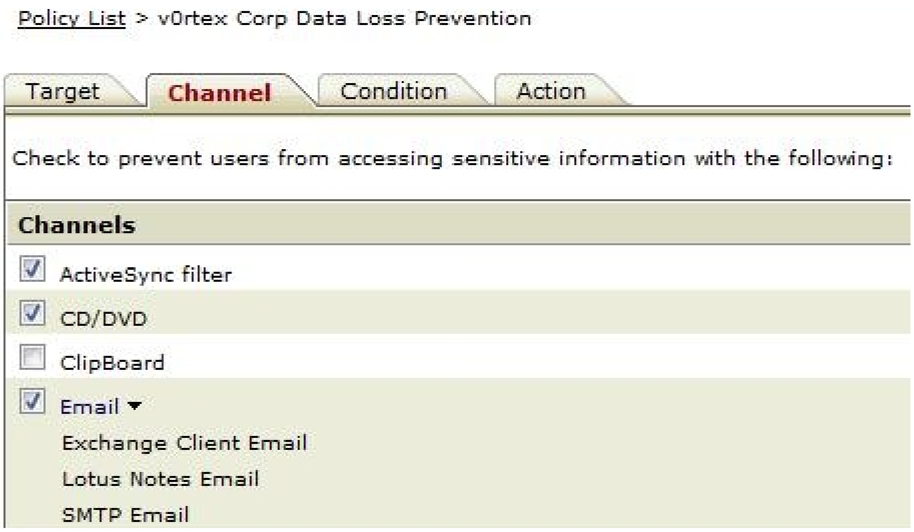
v0rtex Corporation
BOARD OF DIRECTORS

NAME	TITLE	EMAIL	PRIVATE PHONE
nitr0us	Chairman	chairman@v0rtex.com	+52 55 00031337
John Doe	Chief Executive Officer	john@v0rtex.com	+52 55 123456789
Sarah Maldonado	Chief Information Security Officer	sarah@v0rtex.com	+52 55 33334444

MS Word document (.doc) containing the ***keywords*** (Boards of Directors)

5.2.- Constraint

For a successfully exploitation, the “**Clipboard**” channel must not be selected in order to allow the copy from the original file to the attack vector of your preference. (Gmail chat, facebook chat, etc.).



Policy List > v0rtex Corp Data Loss Prevention

Check to prevent users from accessing sensitive information with the following:

Channels

☑ ActiveSync filter

☑ CD/DVD

☐ ClipBoard

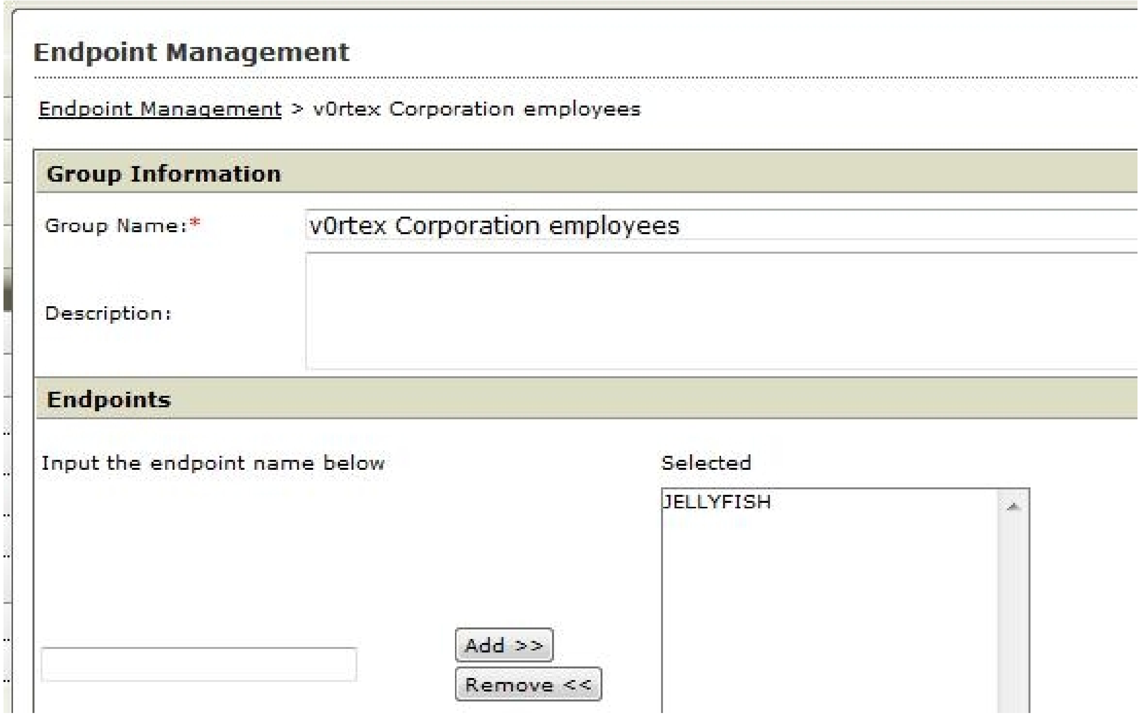
☑ Email ▾

Exchange Client Email

Lotus Notes Email

SMTP Email

5.3.- Configuration of the environment to be tested



Endpoint Management

Endpoint Management > v0rtex Corporation employees

Group Information

Group Name:* v0rtex Corporation employees

Description:

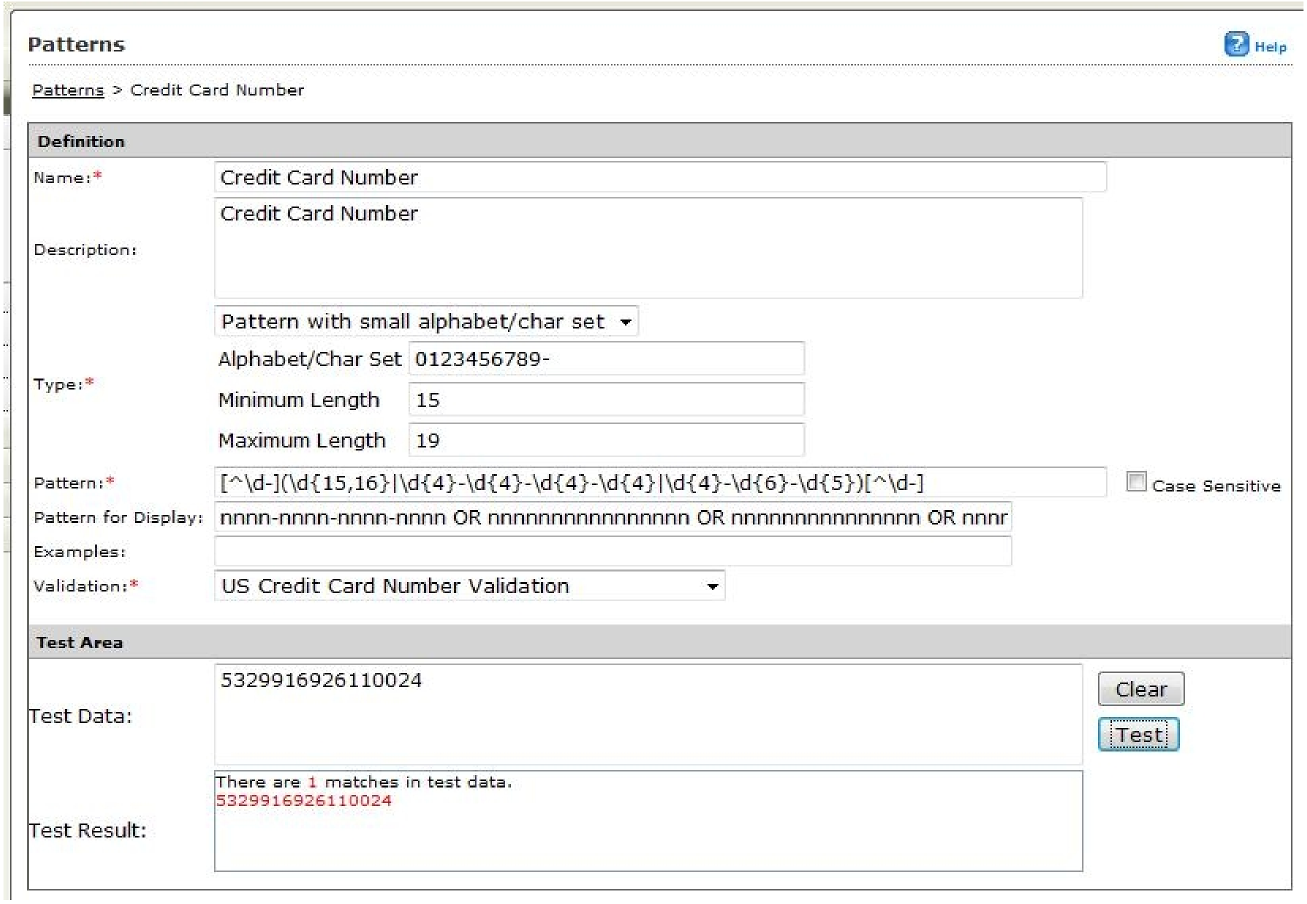
Endpoints

Input the endpoint name below

Selected

JELLYFISH

Endpoint group creation.



Patterns

Patterns > Credit Card Number

Definition

Name:* Credit Card Number

Description: Credit Card Number

Type:* Pattern with small alphabet/char set

Alphabet/Char Set 0123456789-

Minimum Length 15

Maximum Length 19

Pattern:* [^\d-](\d{15,16}|\d{4}-\d{4}-\d{4}-\d{4}|\d{4}-\d{6}-\d{5})[^\d-] □ Case Sensitive

Pattern for Display: nnnn-nnnn-nnnn-nnnn OR nnnnnnnnnnnnnnnn OR nnnnnnnnnnnnnnn OR nnnr

Examples:

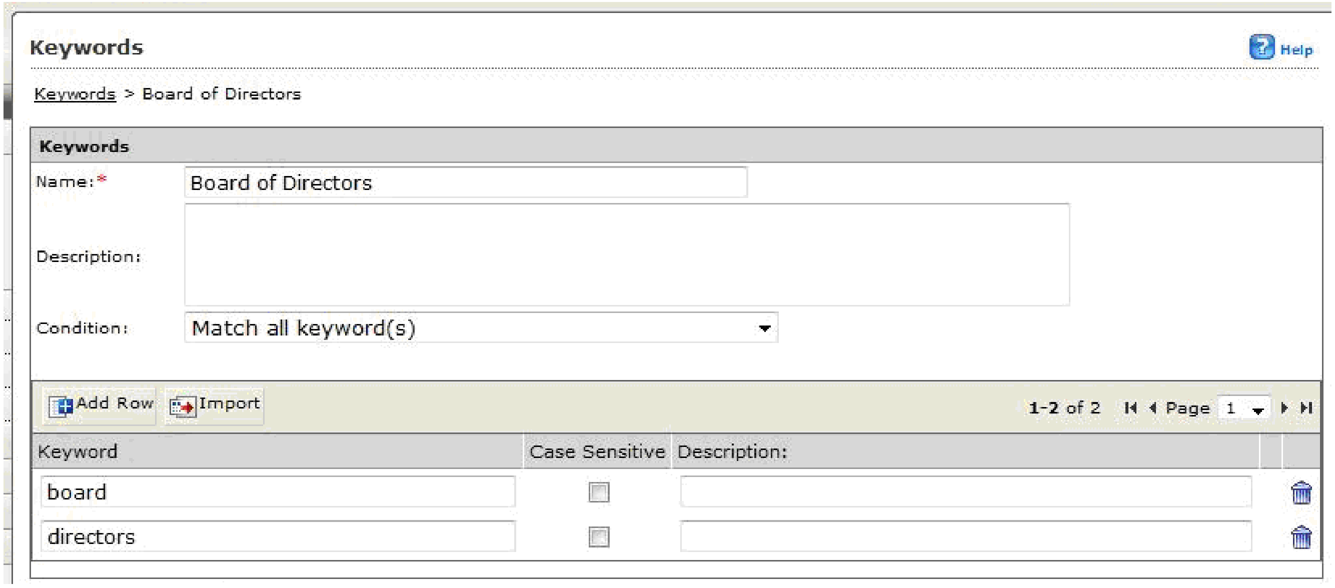
Validation:* US Credit Card Number Validation

Test Area

Test Data: 5329916926110024

Test Result: There are 1 matches in test data.
5329916926110024

Test of the pattern to ensure that the ***Credit Card Number*** (included in the .doc file) supplied matches.



Keywords

Keywords > Board of Directors

Keywords

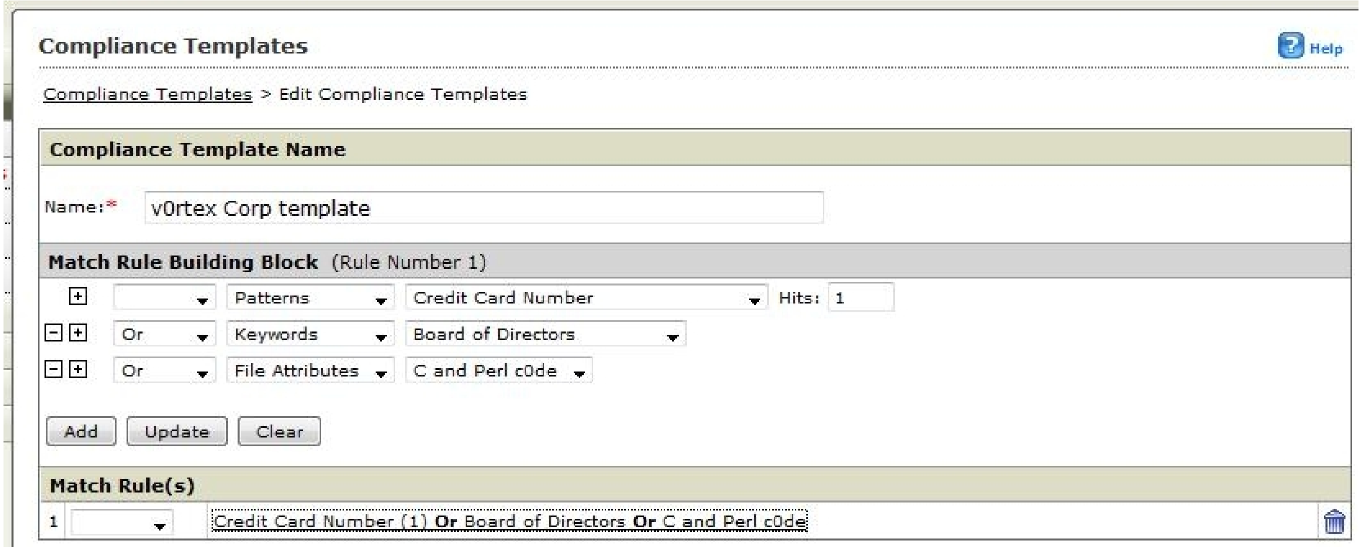
Name:* Board of Directors

Description:

Condition: Match all keyword(s)

Keyword	Case Sensitive	Description:
board	□	
directors	□	

Creation of the pattern named "***Board of Directors***" that includes two keywords, ***board*** and ***directors***.



Compliance Template Name

Name:* v0rtex Corp template

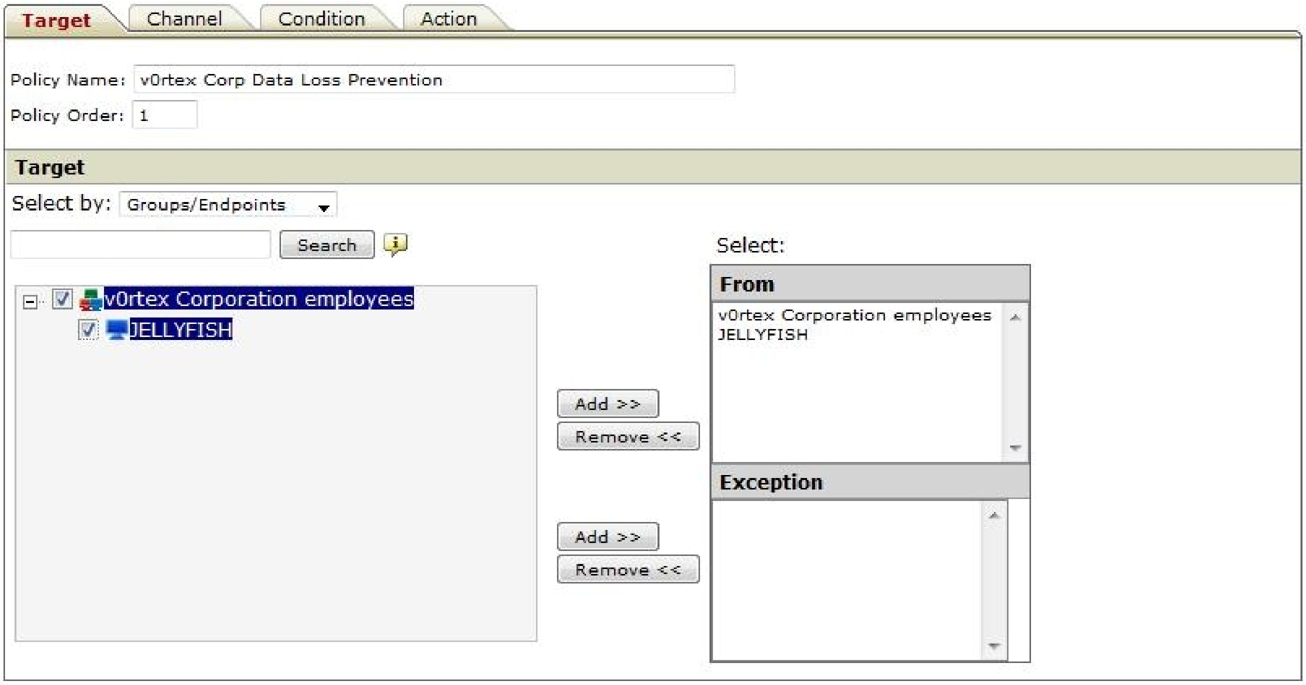
Match Rule Building Block (Rule Number 1)

	Patterns	Credit Card Number	Hits: 1
Or	Keywords	Board of Directors	
Or	File Attributes	C and Perl c0de	

Match Rule(s)

1 Credit Card Number (1) **Or** Board of Directors **Or** C and Perl c0de

Creation of the compliance template which includes the ***Credit Card Number*** pattern and the "***Board of Directors***" keyword. The match rule is based on the ***OR*** operand.



Policy Name: v0rtex Corp Data Loss Prevention

Policy Order: 1

Target

Select by: Groups/Endpoints

☑ v0rtex Corporation employees

☑ JELLYFISH

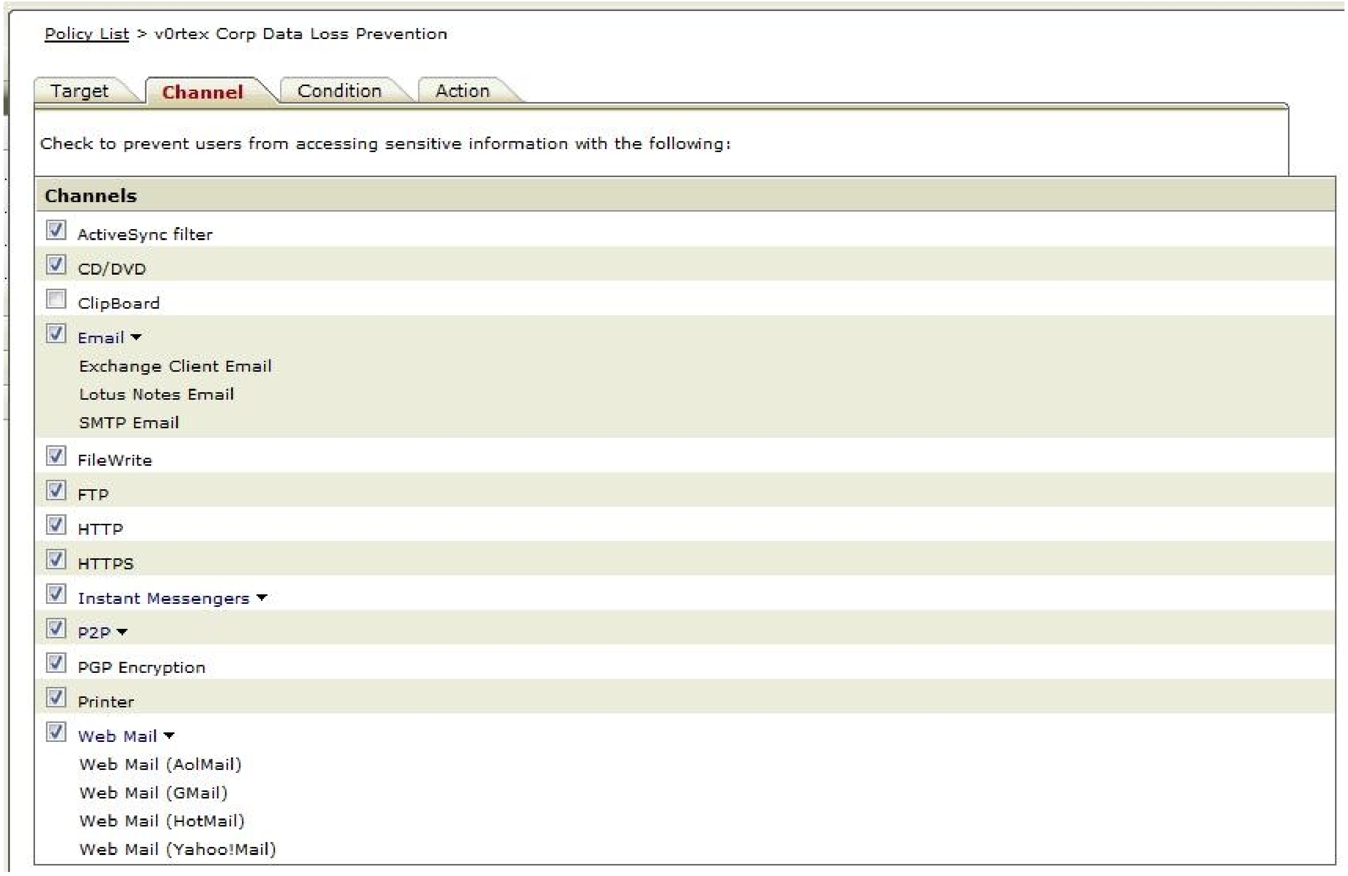
Select:

From

v0rtex Corporation employees
JELLYFISH

Exception

Creation of the Company Policy.
Selection of the ***endpoints*** to which the policy will apply.



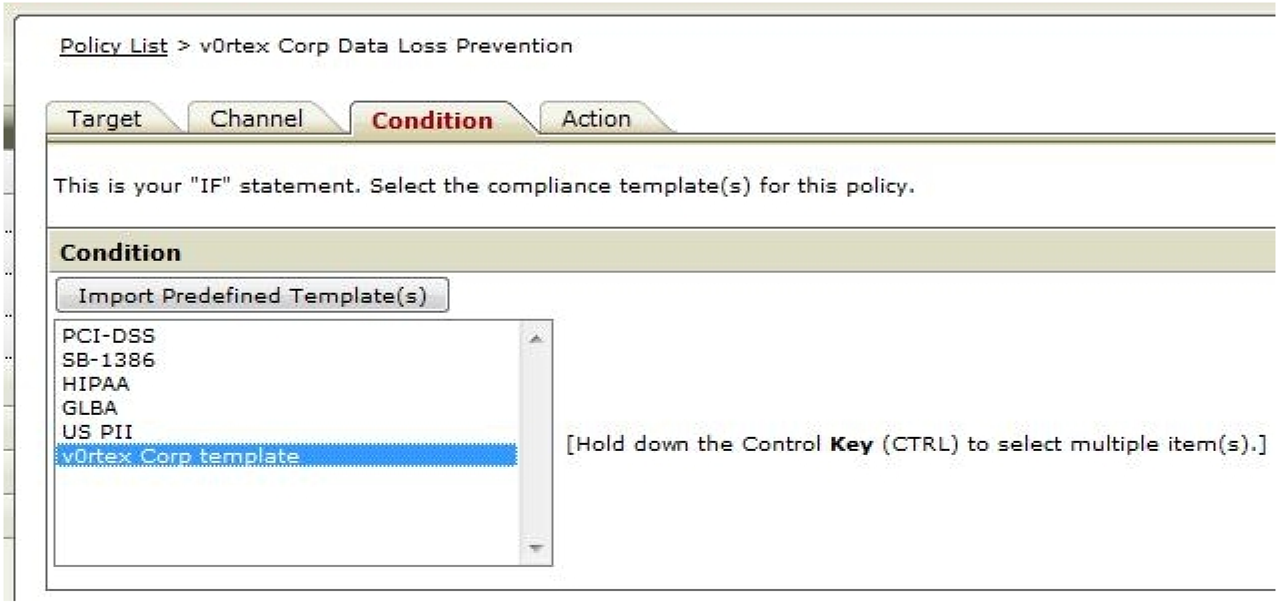
Policy List > v0rtex Corp Data Loss Prevention

Check to prevent users from accessing sensitive information with the following:

Channels

- ☑ ActiveSync filter
- ☑ CD/DVD
- ☐ ClipBoard
- ☑ Email ▾
  - Exchange Client Email
  - Lotus Notes Email
  - SMTP Email
- ☑ FileWrite
- ☑ FTP
- ☑ HTTP
- ☑ HTTPS
- ☑ Instant Messengers ▾
- ☑ P2P ▾
- ☑ PGP Encryption
- ☑ Printer
- ☑ Web Mail ▾
  - Web Mail (AolMail)
  - Web Mail (GMail)
  - Web Mail (HotMail)
  - Web Mail (Yahoo!Mail)

Creation of the Company Policy.
Selection of the ***channels*** to which the policy will apply.
Note that HTTP, HTTPS and all the Webmail channels are selected.
On the other hand, the ***Clipboard*** channel is disabled (see 4.2.- Constraint for details).



Policy List > v0rtex Corp Data Loss Prevention

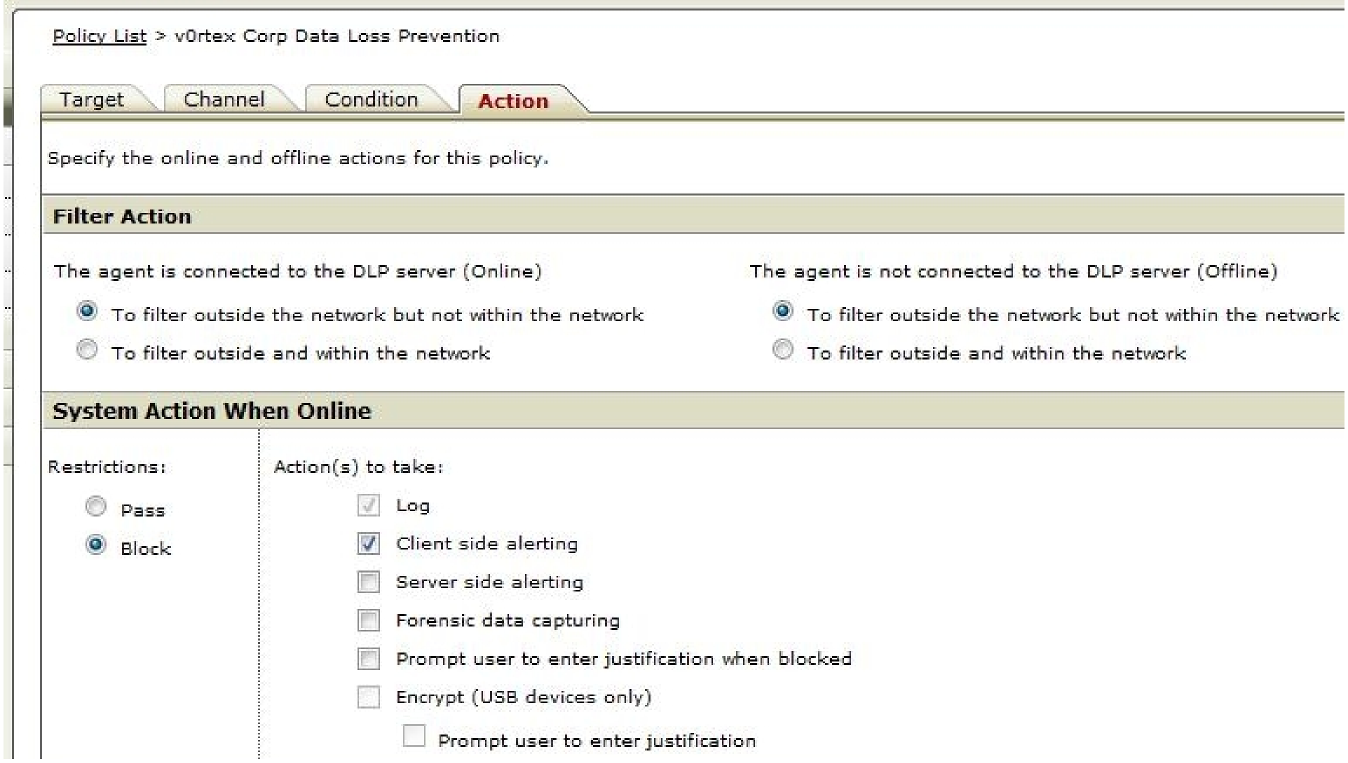
This is your "IF" statement. Select the compliance template(s) for this policy.

Condition

PCI-DSS
SB-1386
HIPAA
GLBA
US PII
v0rtex Corp template

[Hold down the Control **Key** (CTRL) to select multiple item(s).]

Creation of the Company Policy.
Selection of the previously defined template.



Policy List > v0rtex Corp Data Loss Prevention

Specify the online and offline actions for this policy.

Filter Action

The agent is connected to the DLP server (Online)

- ● To filter outside the network but not within the network
- ○ To filter outside and within the network

The agent is not connected to the DLP server (Offline)

- ● To filter outside the network but not within the network
- ○ To filter outside and within the network

System Action When Online

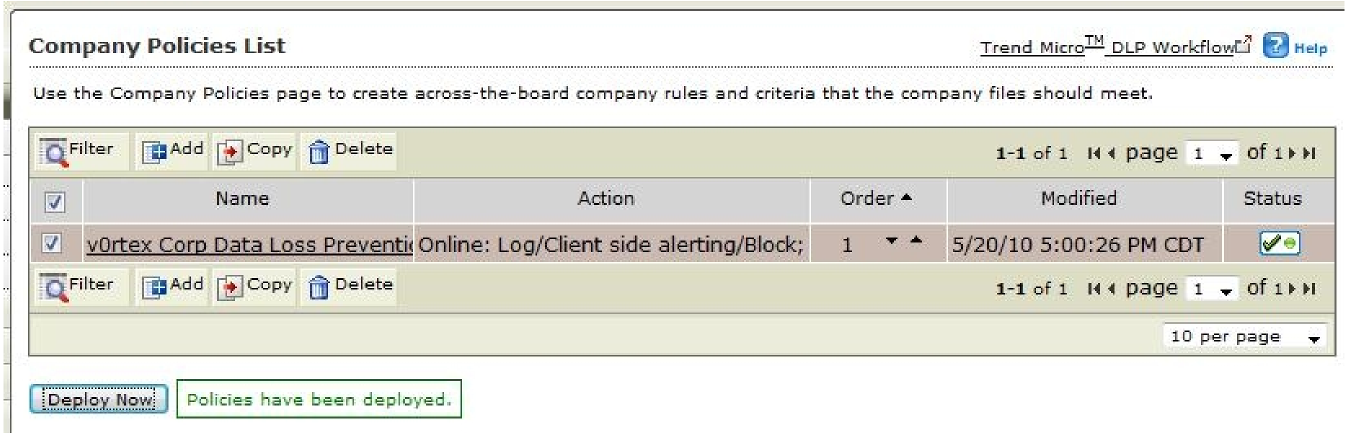
Restrictions:

- ○ Pass
- ● Block

Action(s) to take:

- ☑ Log
- ☑ Client side alerting
- □ Server side alerting
- □ Forensic data capturing
- □ Prompt user to enter justification when blocked
- □ Encrypt (USB devices only)
  - □ Prompt user to enter justification

Creation of the Company Policy.
Selection of the action to be taken on the endpoints once they try to violate the defined policy.



Company Policies List

Use the Company Policies page to create across-the-board company rules and criteria that the company files should meet.

1-1 of 1 page 1 of 1

☑	Name	Action	Order ▲	Modified	Status
☑	v0rtex Corp Data Loss Preventi	Online: Log/Client side alerting/Block;	1	5/20/10 5:00:26 PM CDT	✓

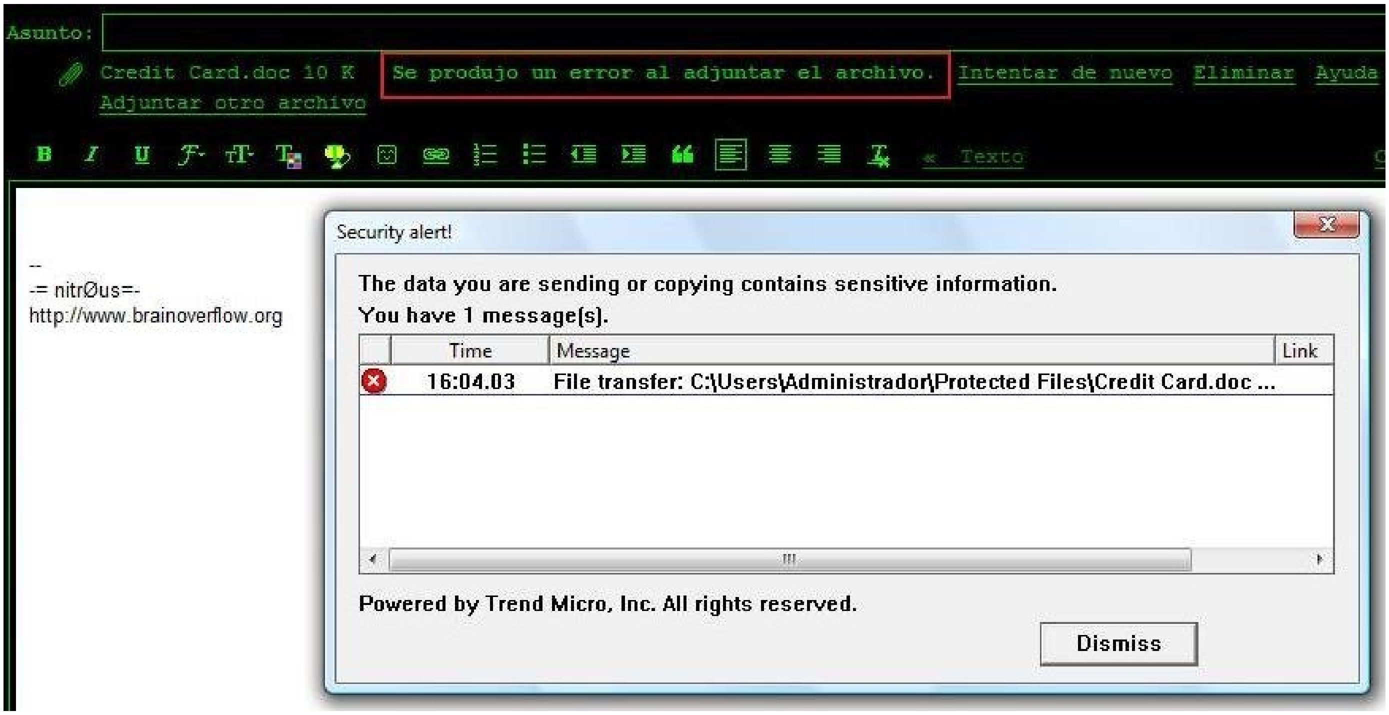
1-1 of 1 page 1 of 1

10 per page

Policies have been deployed.

Policy deployment to the endpoints.

5.4.- Test to validate if the DLP works properly



Credit Card.doc 10 K

Se produjo un error al adjuntar el archivo.

--
-= nitrØus=-
http://www.brainoverflow.org

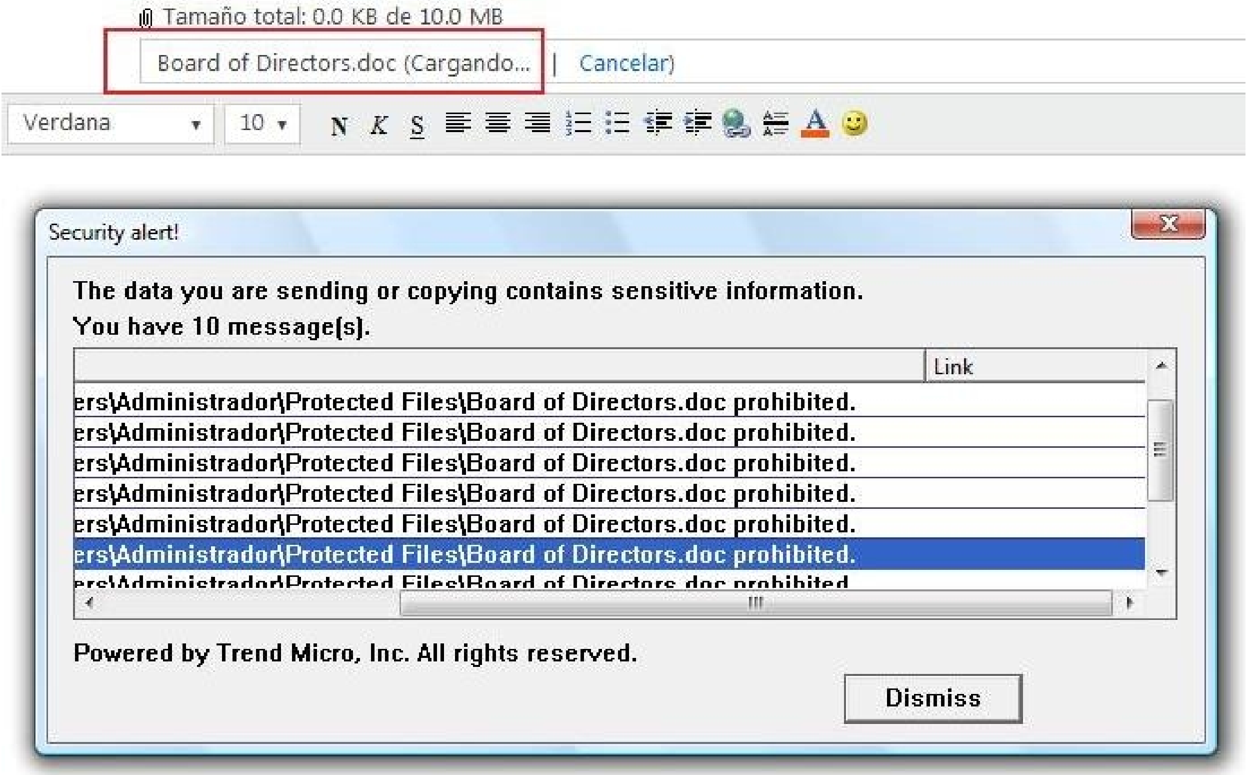
Security alert!

The data you are sending or copying contains sensitive information.
You have 1 message(s).

Time	Message	Link
16:04.03	File transfer: C:\Users\Administrador\Protected Files\Credit Card.doc ...	

Powered by Trend Micro, Inc. All rights reserved.

Error received when trying to attach the “***Credit Card.doc***” file on Gmail Webmail.



Tamaño total: 0.0 KB de 10.0 MB

Board of Directors.doc (Cargando...

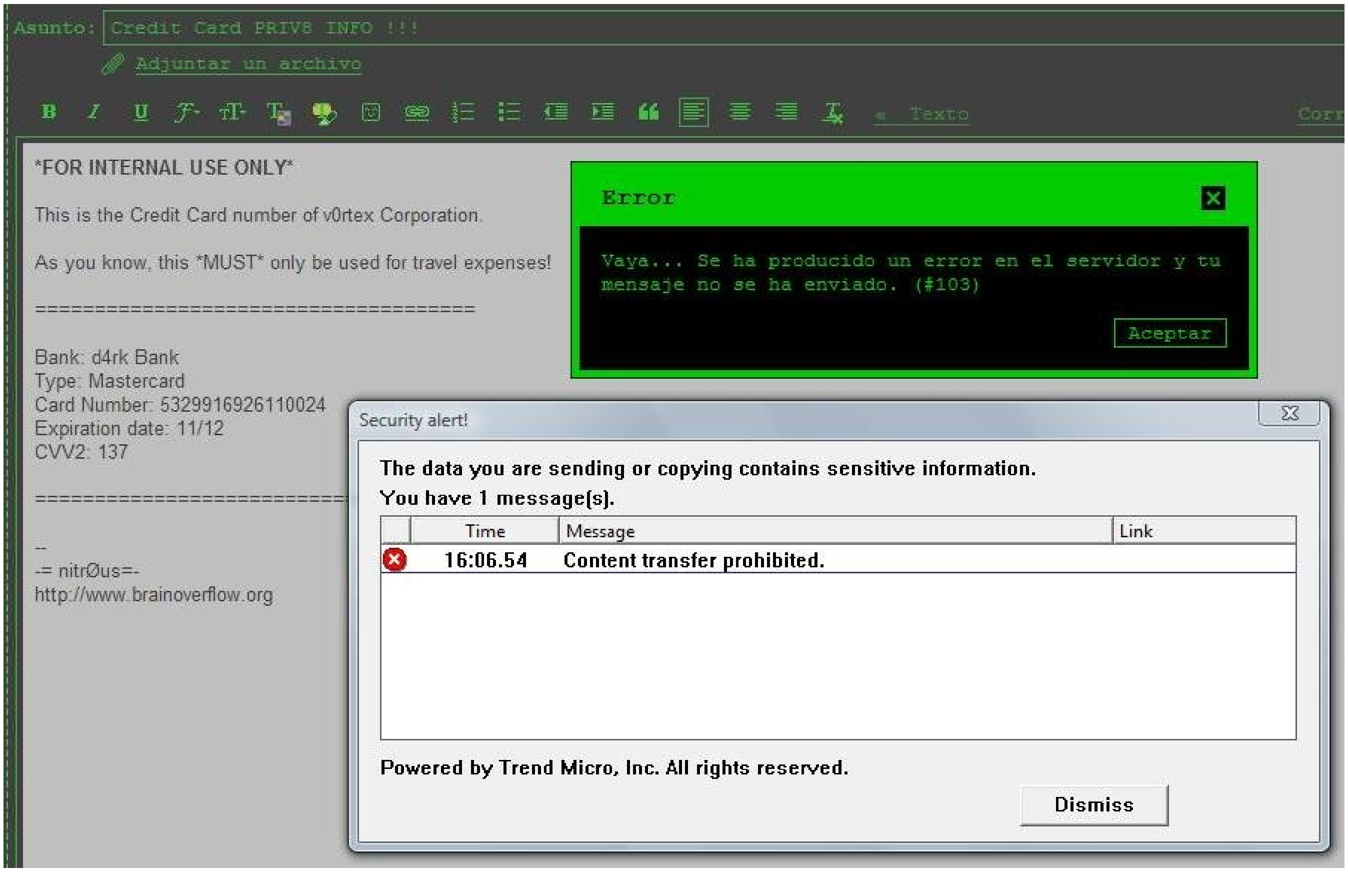
Security alert!

The data you are sending or copying contains sensitive information.
You have 10 message(s).

	Link
ers\Administrador\Protected Files\Board of Directors.doc prohibited.	
ers\Administrador\Protected Files\Board of Directors.doc prohibited.	
ers\Administrador\Protected Files\Board of Directors.doc prohibited.	
ers\Administrador\Protected Files\Board of Directors.doc prohibited.	
ers\Administrador\Protected Files\Board of Directors.doc prohibited.	
ers\Administrador\Protected Files\Board of Directors.doc prohibited.	
ers\Administrador\Protected Files\Board of Directors.doc prohibited.	

Powered by Trend Micro, Inc. All rights reserved.

Error received when trying to attach the “***Board of Directors.doc***” file on Hotmail Webmail.



Asunto: Credit Card PRIV8 INFO !!!

FOR INTERNAL USE ONLY

This is the Credit Card number of v0rtex Corporation.

As you know, this *MUST* only be used for travel expenses!

=====================================

Bank: d4rk Bank
Type: Mastercard
Card Number: 5329916926110024
Expiration date: 11/12
CVV2: 137

=============================

--
-= nitrØus=-
http://www.brainoverflow.org

Vaya... Se ha producido un error en el servidor y tu mensaje no se ha enviado. (#103)

The data you are sending or copying contains sensitive information.
You have 1 message(s).

	Time	Message	Link
⊗	16:06.54	Content transfer prohibited.	

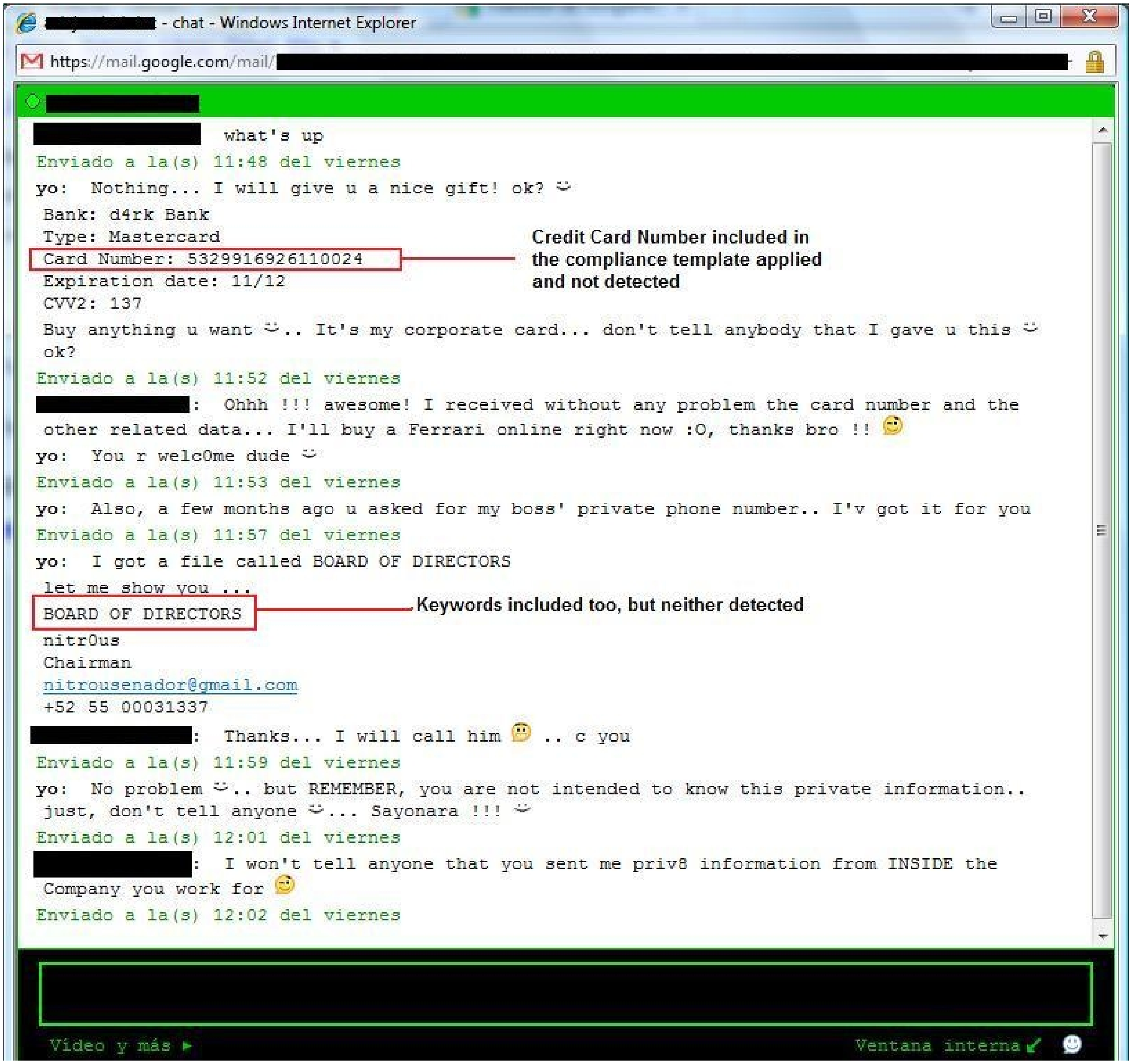
Powered by Trend Micro, Inc. All rights reserved.

Error received when trying to send the ***Credit Card info in plain text*** through Gmail Webmail.

5.5.- Exploitation (Data Leakage Proof-of-Concept)

The flaw as such is in the lack of analysis of certain HTTP/HTTPS channels such as Web chats. Two attack vectors were used, Gmail Chat and Facebook Chat, and the successful exploitation was achieved in both of them.

It's important to mention that there could be others attack vectors than those listed above, but for demonstration purposes, I'll only include in this advisory the popular ones, Gmail and Facebook webchats.

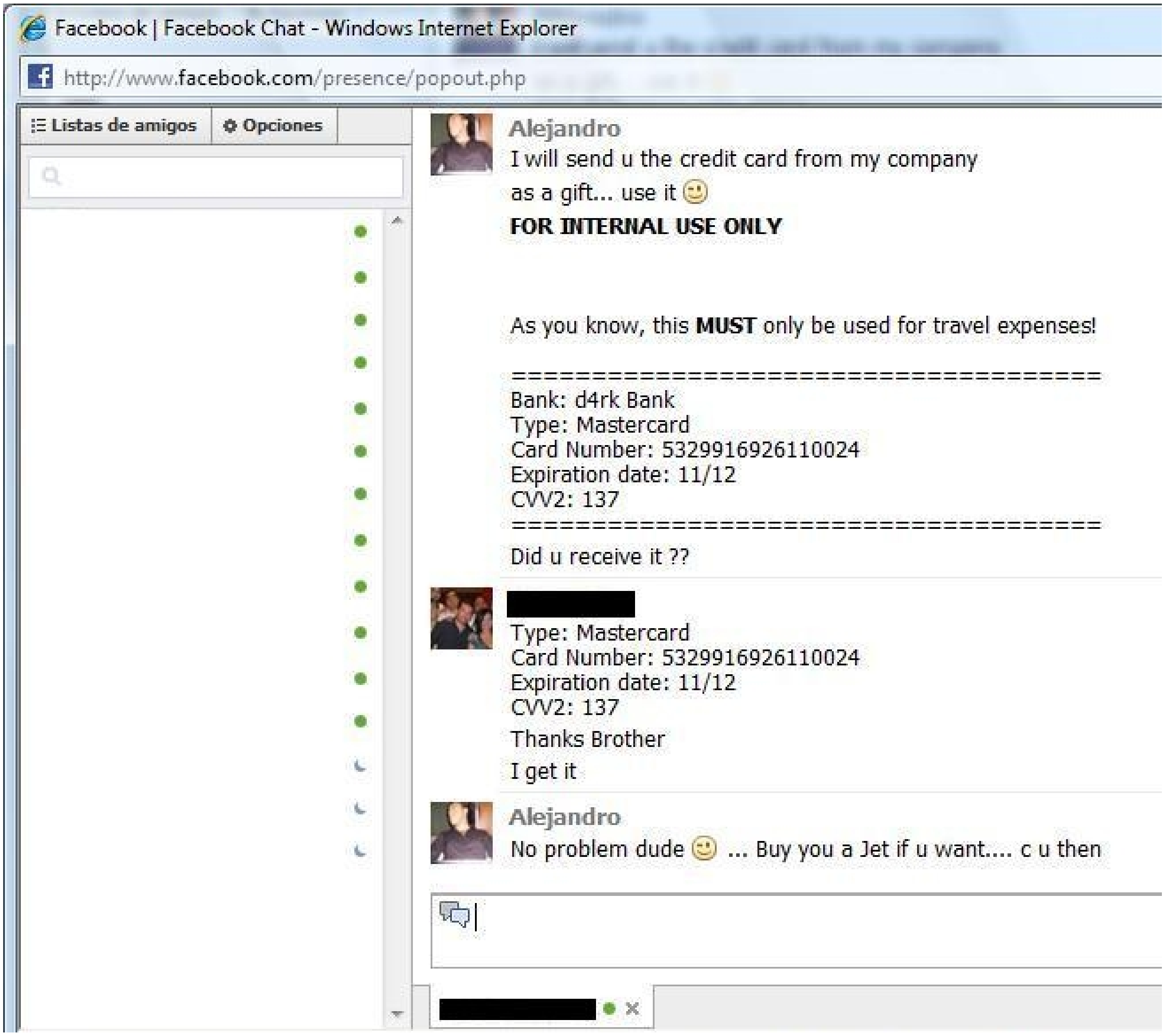

[redacted] - chat - Windows Internet Explorer
https://mail.google.com/mail/[redacted]
[redacted]

```
[redacted]   what's up
Enviado a la(s) 11:48 del viernes
yo:  Nothing... I will give u a nice gift! ok? ☺
 Bank: d4rk Bank
 Type: Mastercard
 Card Number: 5329916926110024
 Expiration date: 11/12
 CVV2: 137
 Buy anything u want ☺.. It's my corporate card... don't tell anybody that I gave u this ☺
 ok?
Enviado a la(s) 11:52 del viernes
[redacted]:  Ohhh !!! awesome! I received without any problem the card number and the
 other related data... I'll buy a Ferrari online right now :O, thanks bro !! ☺
yo:  You r welc0me dude ☺
Enviado a la(s) 11:53 del viernes
yo:  Also, a few months ago u asked for my boss' private phone number.. I'v got it for you
Enviado a la(s) 11:57 del viernes
yo:  I got a file called BOARD OF DIRECTORS
 let me show you ...
 BOARD OF DIRECTORS
 nitr0us
 Chairman
 nitrousenador@gmail.com
 +52 55 00031337
[redacted]:  Thanks... I will call him ☺ .. c you
Enviado a la(s) 11:59 del viernes
yo:  No problem ☺.. but REMEMBER, you are not intended to know this private information..
 just, don't tell anyone ☺... Sayonara !!! ☺
Enviado a la(s) 12:01 del viernes
[redacted]:  I won't tell anyone that you sent me priv8 information from INSIDE the
 Company you work for ☺
Enviado a la(s) 12:02 del viernes
```

Credit Card Number included in the compliance template applied and not detected

Keywords included too, but neither detected

Data Leakage through ***Gmail*** Chat.


Facebook | Facebook Chat - Windows Internet Explorer
http://www.facebook.com/presence/popout.php
Listas de amigos
Opciones

Alejandro

I will send u the credit card from my company

as a gift... use it 🙂

FOR INTERNAL USE ONLY

As you know, this **MUST** only be used for travel expenses!

```
=======================================
Bank: d4rk Bank
Type: Mastercard
Card Number: 5329916926110024
Expiration date: 11/12
CVV2: 137
=======================================
```

Did u receive it ??

[redacted]

```
Type: Mastercard
Card Number: 5329916926110024
Expiration date: 11/12
CVV2: 137
```

Thanks Brother

I get it

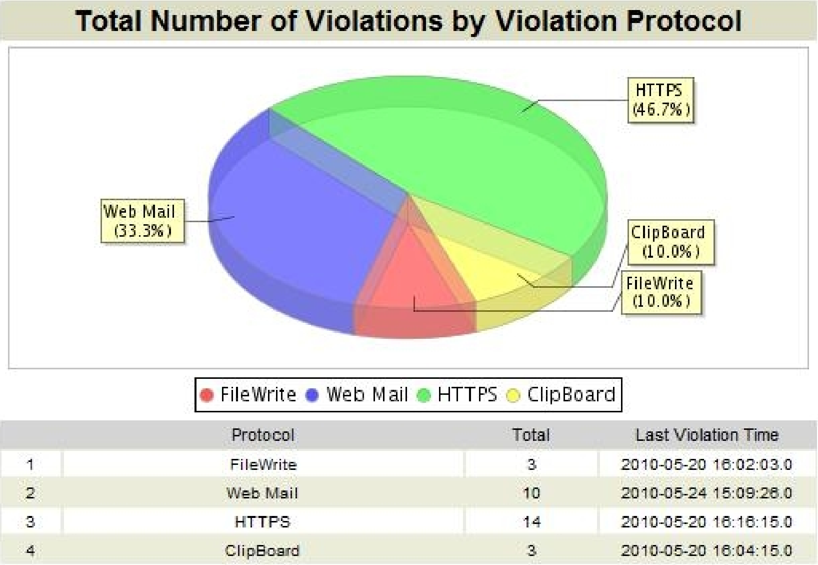
Alejandro

No problem dude 🙂 ... Buy you a Jet if u want.... c u then

[redacted] ● ×

Data Leakage through ***Facebook*** Chat.

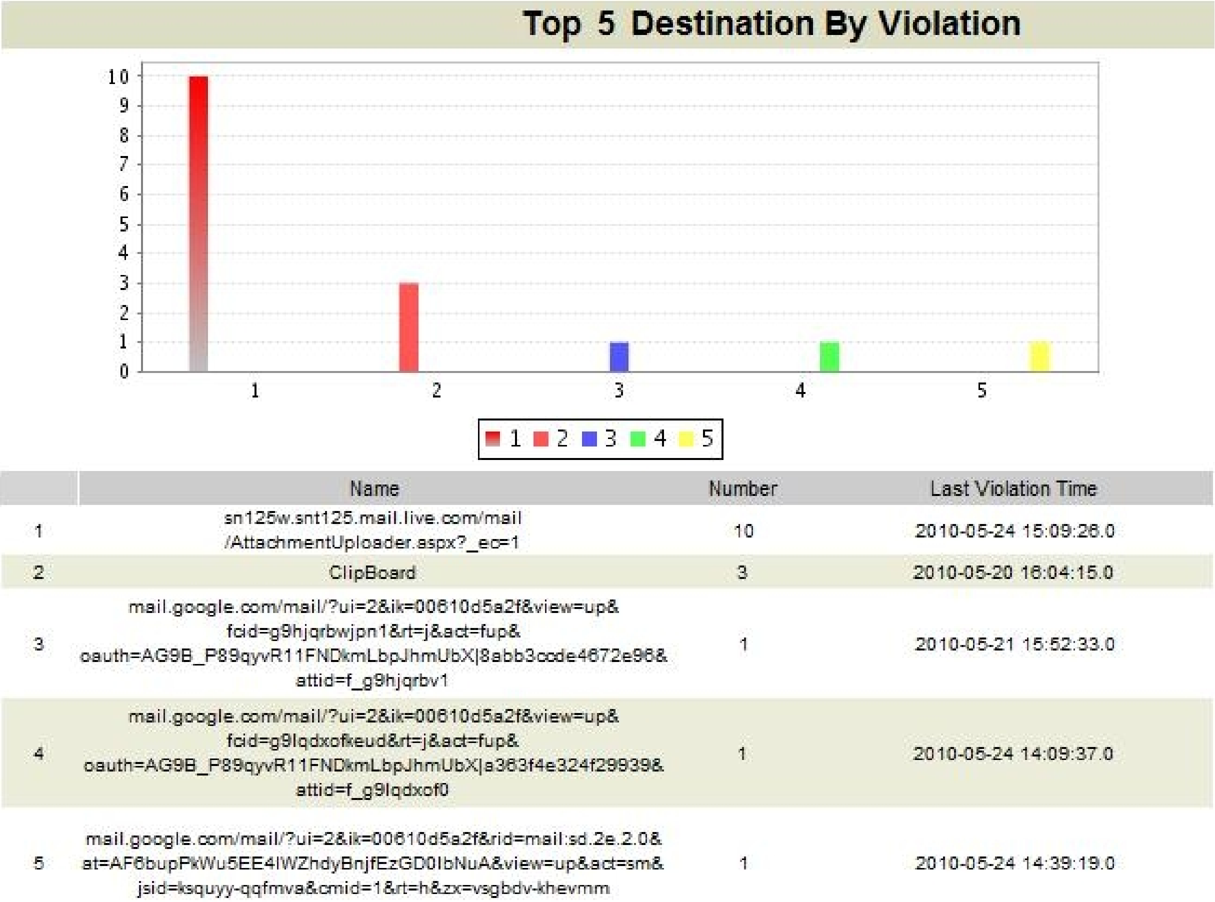
5.6.- Reports after the tests



Total Number of Violations by Violation Protocol

	Protocol	Total	Last Violation Time
1	FileWrite	3	2010-05-20 16:02:03.0
2	Web Mail	10	2010-05-24 15:09:26.0
3	HTTPS	14	2010-05-20 16:16:15.0
4	ClipBoard	3	2010-05-20 16:04:15.0

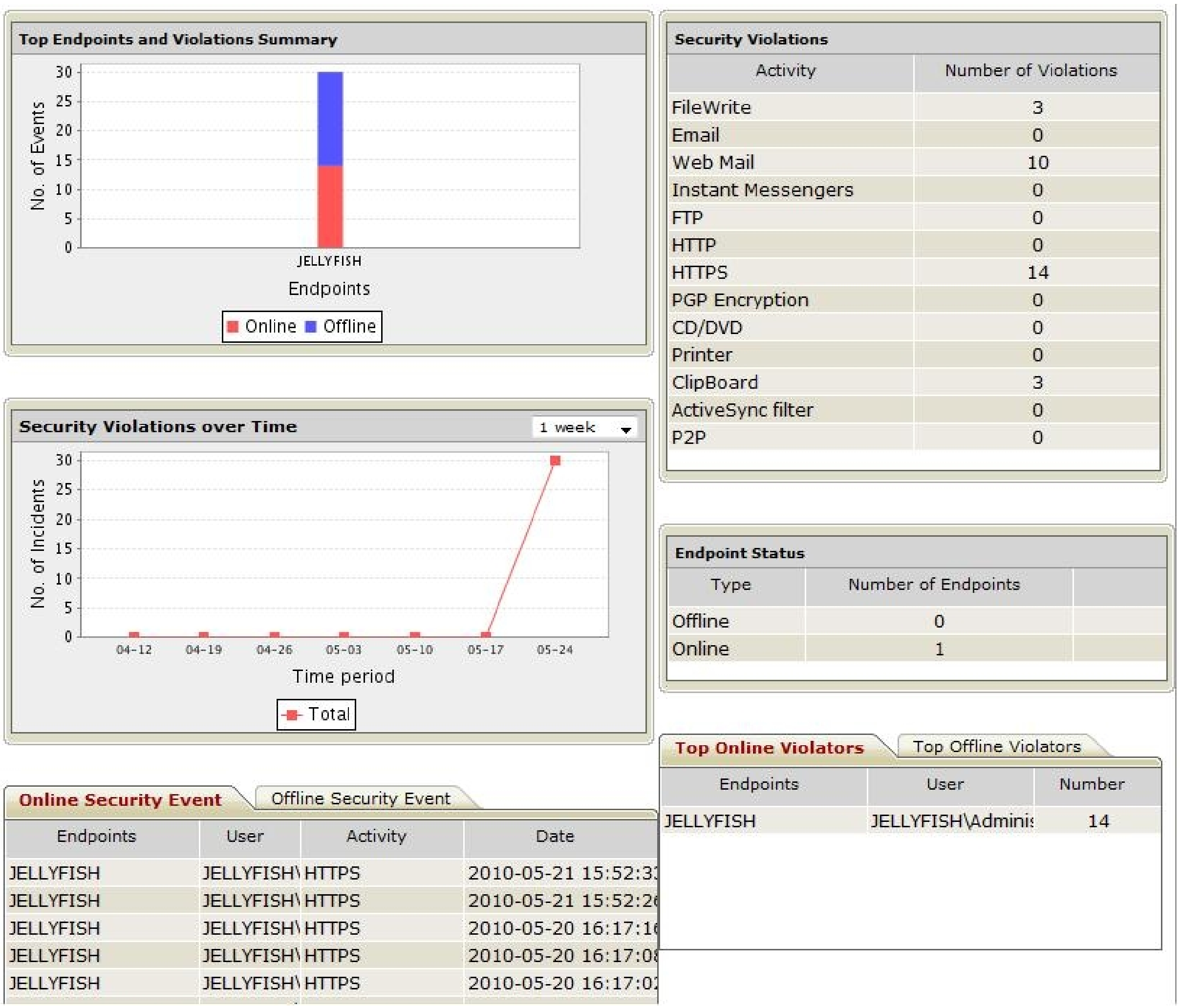
This graph clearly shows that the Webmail and HTTPS had violations during the file attachment process in Hotmail and Gmail.



Top 5 Destination By Violation

	Name	Number	Last Violation Time
1	sn125w.snt125.mail.live.com/mail /AttachmentUploader.aspx?_ec=1	10	2010-05-24 15:09:26.0
2	ClipBoard	3	2010-05-20 16:04:15.0
3	mail.google.com/mail/?ui=2&ik=00610d5a2f&view=up& fcid=g9hjqrbwjpn1&rt=j&act=fup& oauth=AG9B_P89qyvR11FNDkmLbpJhmUbX|8abb3code4672e96& attid=f_g9hjqrbv1	1	2010-05-21 15:52:33.0
4	mail.google.com/mail/?ui=2&ik=00610d5a2f&view=up& fcid=g9lqdxofkeud&rt=j&act=fup& oauth=AG9B_P89qyvR11FNDkmLbpJhmUbX|a363f4e324f29939& attid=f_g9lqdxof0	1	2010-05-24 14:09:37.0
5	mail.google.com/mail/?ui=2&ik=00610d5a2f&rid=mail:sd.2e.2.0& at=AF6bupPkWu5EE4lWZhdyBnjfEzGD0IbNuA&view=up&act=sm& jsid=ksquyy-qqfmva&cmid=1&rt=h&zx=vsgbdv-khevmm	1	2010-05-24 14:39:19.0

The URLs of the violations raised on the file attachment process in Hotmail and Gmail.



Security Violations

Activity	Number of Violations
FileWrite	3
Email	0
Web Mail	10
Instant Messengers	0
FTP	0
HTTP	0
HTTPS	14
PGP Encryption	0
CD/DVD	0
Printer	0
ClipBoard	3
ActiveSync filter	0
P2P	0

Endpoint Status

Type	Number of Endpoints
Offline	0
Online	1

Endpoints	User	Number
JELLYFISH	JELLYFISH\Adminis	14

Endpoints	User	Activity	Date
JELLYFISH	JELLYFISH\	HTTPS	2010-05-21 15:52:3
JELLYFISH	JELLYFISH\	HTTPS	2010-05-21 15:52:2
JELLYFISH	JELLYFISH\	HTTPS	2010-05-20 16:17:1
JELLYFISH	JELLYFISH\	HTTPS	2010-05-20 16:17:0
JELLYFISH	JELLYFISH\	HTTPS	2010-05-20 16:17:0

The main dashboard showing the endpoints and their respective violations.

6.- GREETS

I'd like to thank Yess G., F. Vilchis and Raaka_elgaupo for testing... And, as usual, all the dogs in the scene, CRAc, nahual, ran, chr1x, hkm, nediam, Federico L. Bossi Bonin, dex, Cj, crypkey, Bucio, beck, Optix, sunLevy, sdc, tr3w, zeus, Héctor López, alt3kx, underground.org.mx, beavis, vendetta, Armin, #mendozaaaa.

EOF