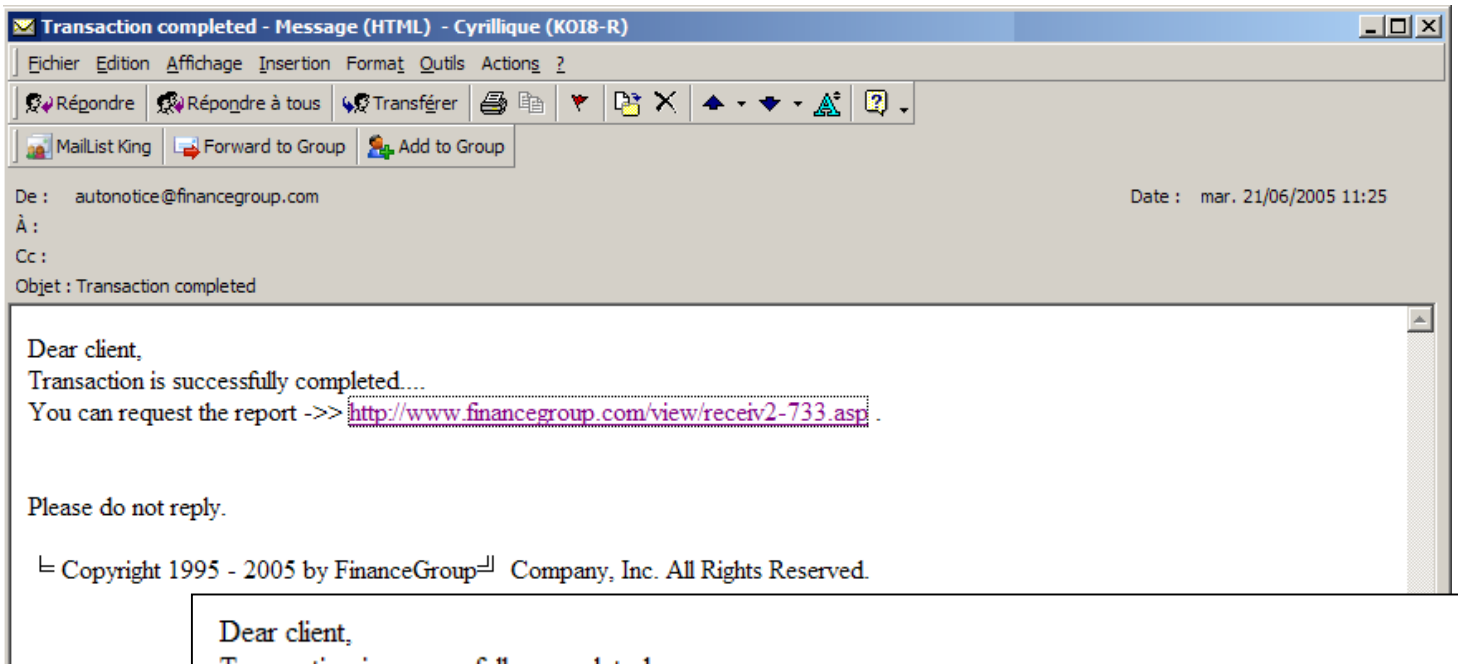


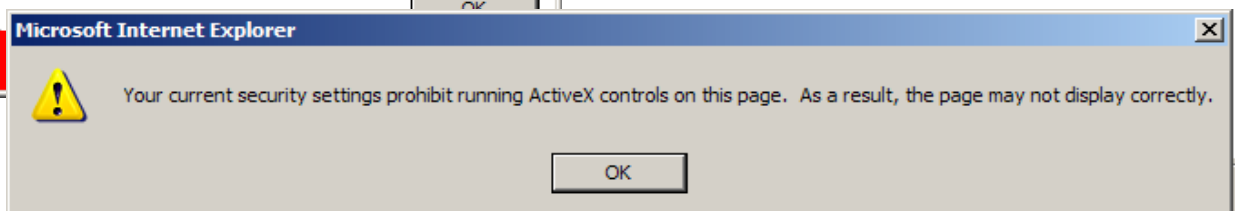
## 1. Le message, son aspect général :

Plusieurs versions ont été reportées :



## 2. La technique utilisée :

Cette tentative n'est pas, à priori, un essai de phishing mais elle dissimule le téléchargement du virus connu sous le nom de « BackDoor.Haxdoor.D » chez Symantec **ceci via un ActiveX.**



Le virus « BackDoor.Haxdoor.D » est bien documenté chez Symantec:

[http://securityresponse.symantec.com/avcenter/venc/data/backdoor\\_haxdoor.d.html#technicaldetails](http://securityresponse.symantec.com/avcenter/venc/data/backdoor_haxdoor.d.html#technicaldetails)

## "Backdoor.Haxdoor-D" Trojan Opens Door : January 25, 2005

*Backdoor.Haxdoor.D is a Trojan horse program that opens a back door on the compromised system and **allows unauthorized access to a remote attacker. It also attempts to log key strokes and steal passwords.***

*Also Known As: Backdoor.Win32.Haxdoor.bg [Kaspersky Lab], BackDoor-BAC [McAfee]*

*Systems Affected: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP*

*Type: Trojan Horse*

*Infection Length: 46,708 bytes*

Quant au serveur SMTP à l'origine de l'essai, il suffit d'analyser les logs :

```
SMTPD (dcb5005102f866fb) [IP-LOCAL] connect 72.29.71.223 port 52430
SMTPD (dcb5005102f866fb) [72.29.71.223] HELO meric.sameservers.com
SMTPD (dcb5005102f866fb) [72.29.71.223] MAIL FROM: <autonotice@financegroup.com>
SMTPD (dcb5005102f866fb) [72.29.71.223] RCPT TO: <essai3@associatedwinners.com>
SMTPD (dcb5005102f866fb) [72.29.71.223] C:\Local\spool\Ddcb5005102f866fb.SMD 1756
SMTP (dcb5005102f866fb) processing C:\Local\spool\Qdcb5005102f866fb.SMD
SMTP (dcb5005102f866fb) ldeliver associatedwinners.com pop3(1)
autonotice@financegroup.com 2278
SMTP (dcb5005102f866fb) finished C:\Local\spool\Qdcb5005102f866fb.SMD status=1
```

Un administrateur système écrira donc facilement un filtre efficace.

### 3. Actions engagées :

- La publication de ce document,
- Ce cas n'a pas été reporté au niveau « .org » car il ne relève pas du phishing.

Cet exemple reste intéressant au moins à deux titres :

- Il utilise une astuce de plus en plus répandue dans les essais de phishing : « une transaction vient d'être validée ... » ou « une transaction importante attend votre confirmation... » etc pour inciter l'internaute à se connecter.
- Le mélange « des genres » : la fraude financière et le téléchargement de codes dits « Key Logger » qui transmettent en différé des informations confidentielles.