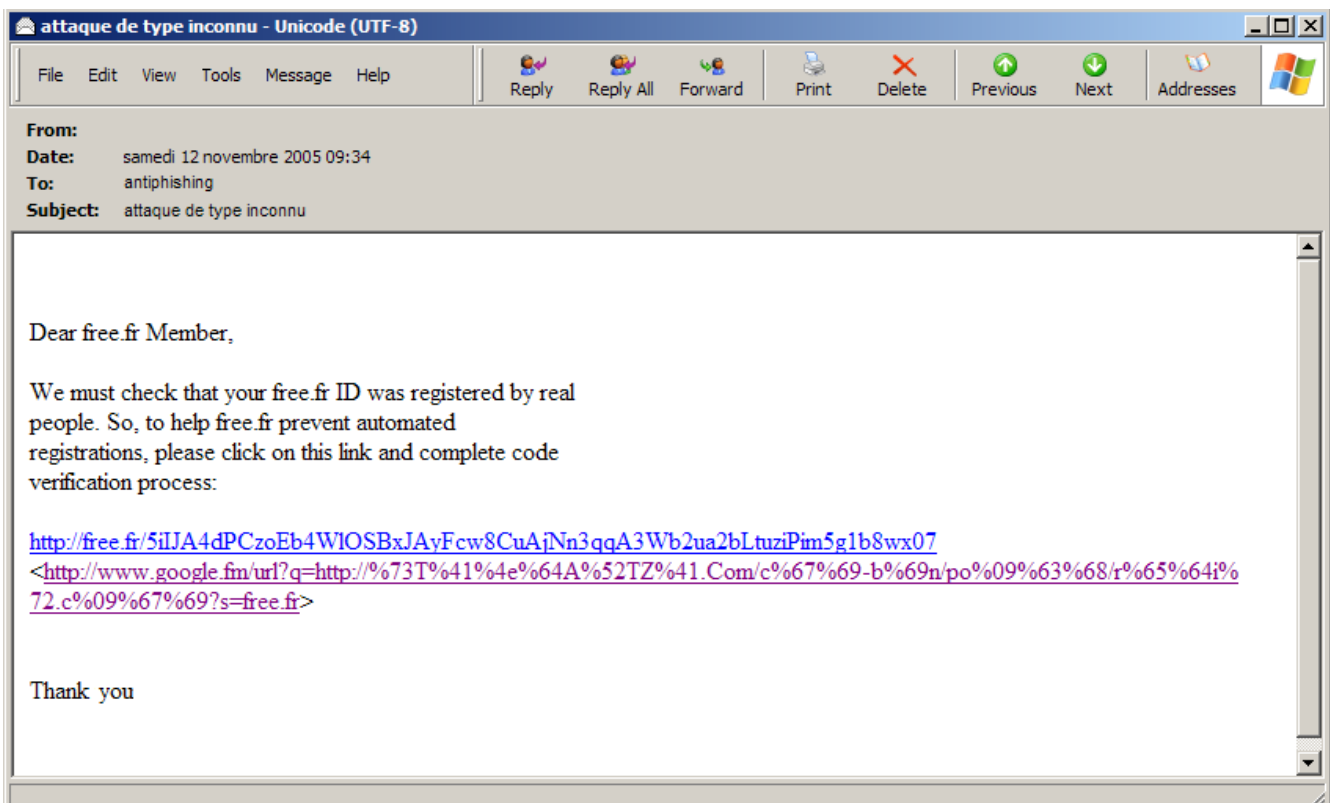
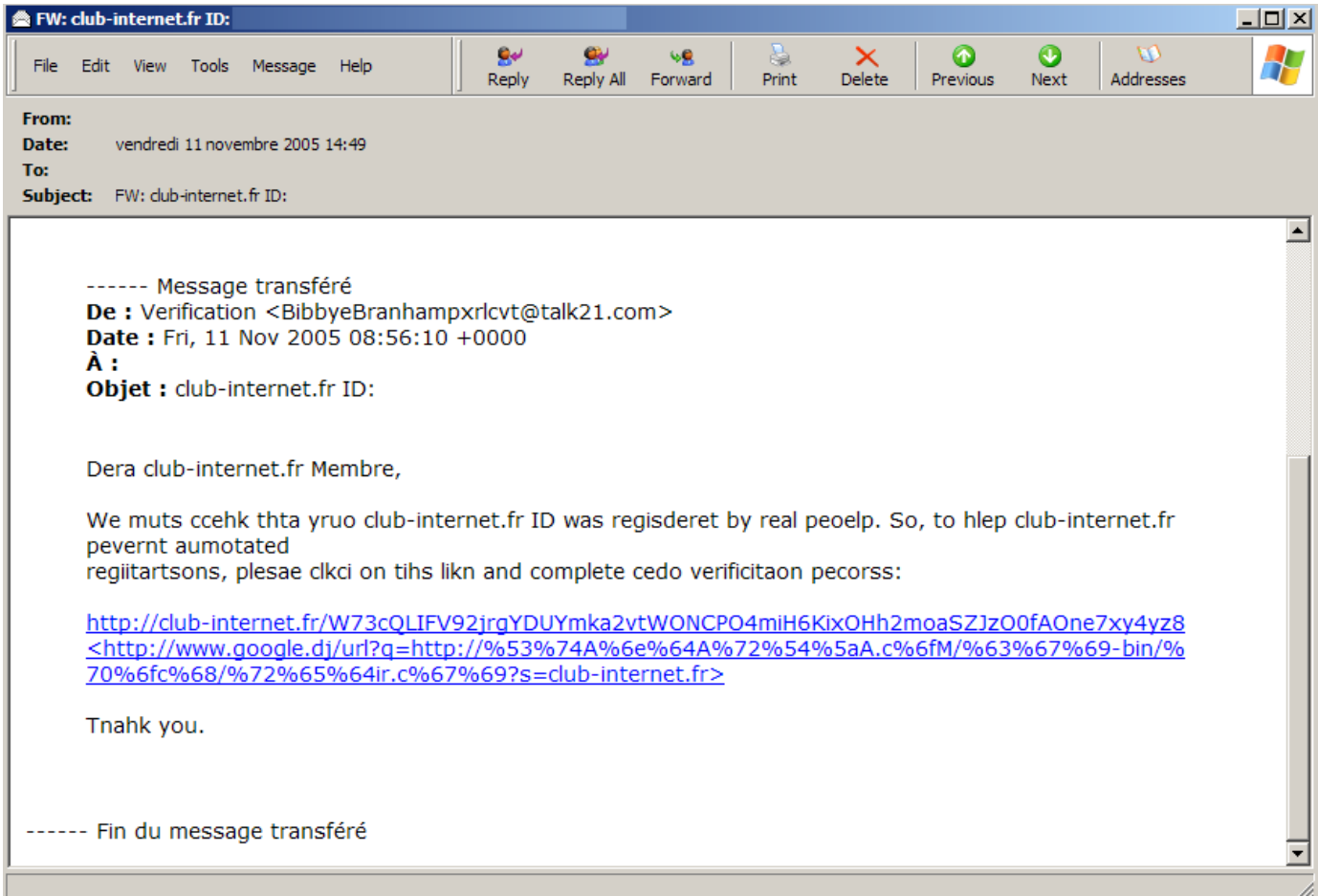
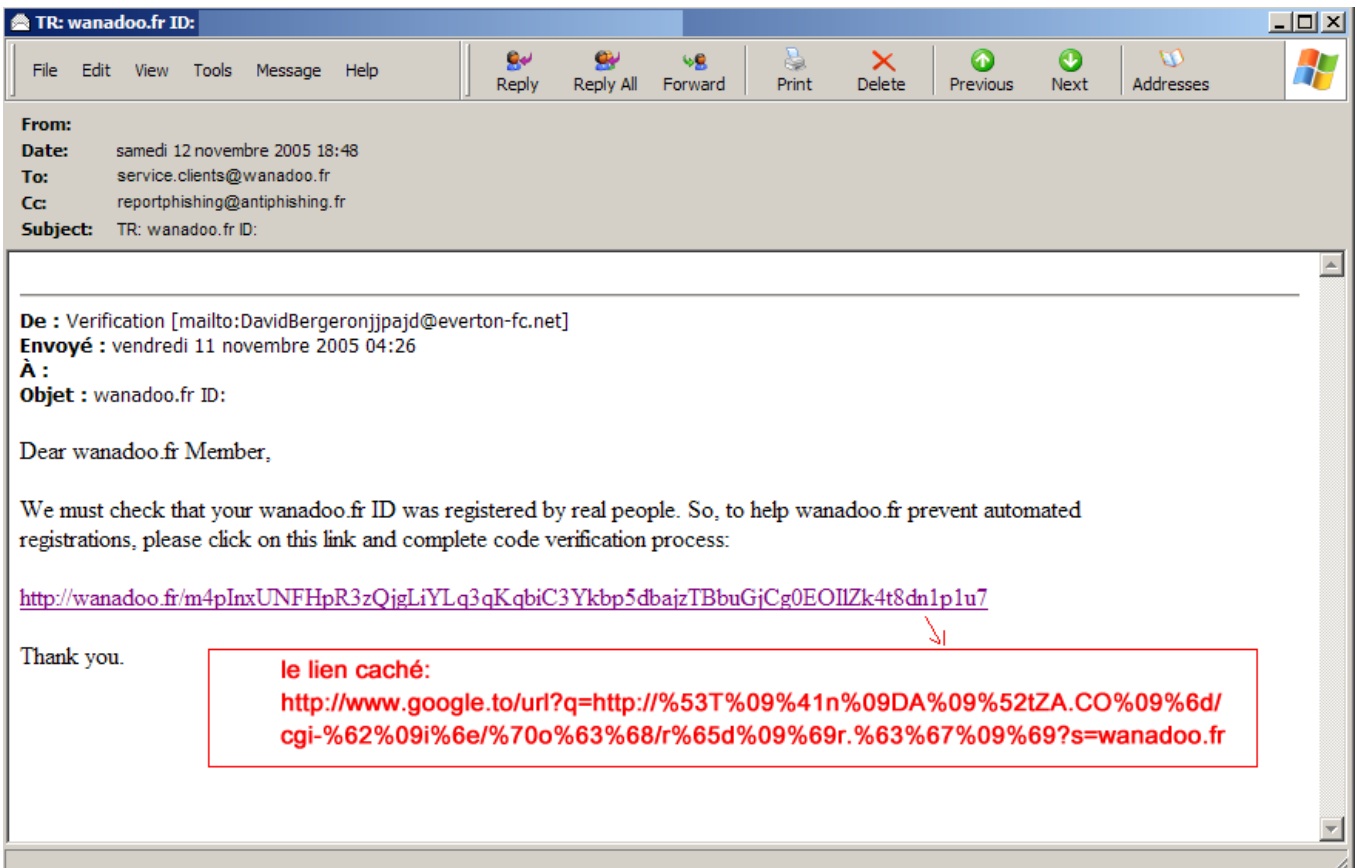
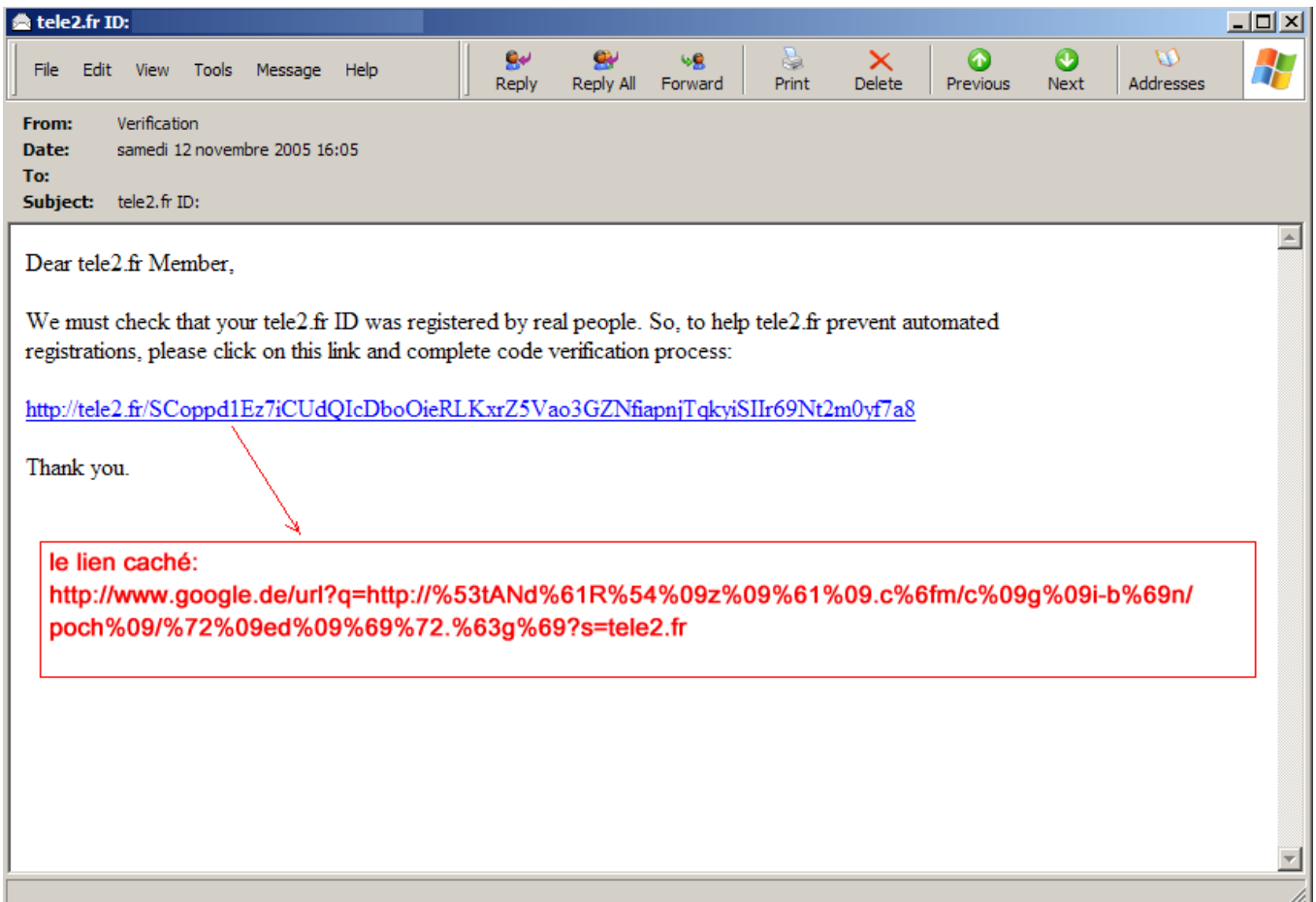


1. Le message, son aspect général :

Une tentative de phishing vise les fournisseurs d'accès français depuis le 9 novembre 2005. Cette arnaque se présente sous la forme d'un message en anglais dont l'expéditeur est nommé "Verification" (associé à des emails divers). Quelques exemples :





2. La technique utilisée :

Cet exemple nous permet d'illustrer un des classiques du phishing qui est l'emploi de l'UNICODE pour dissimuler les liens HTML cachés.

En effet, ce qui est affiché dans l'email ne sera pas le lien activé. Il suffit de lire le code HTML pour voir le lien réel :

<http://wanadoo.fr/m4pInxUNFHpR3zQjgLiYLq3qKqbiC3Ykbp5dbajzTBbuGjCg0EOIIZk4t8dn1p1u7>

le lien caché:

<http://www.google.to/url?q=http://%53T%09%41n%09DA%09%52tZA.CO%09%6d/cgi-%62%09i%6e/%70o%63%68/r%65d%09%69r.%63%67%09%69?s=wanadoo.fr>

Cette technique a déjà été employée lors d'un essai de phishing sur les banques françaises :

<http://www.associatedwinners.com/phishing/phishingfr.pdf>

Elle consiste à exploiter les capacités de recherche des moteurs et à masquer l'URL avec l'UNICODE. Pour télécharger un descriptif complet de l'UNICODE :

<http://www.unicode.org/charts/PDF/U2000.pdf>

1	SOH 0001	DC1 0011	! 0021	1 0031	A 0041	Q 0051	a 0061	q 0071
2	STX 0002	DC2 0012	" 0022	2 0032	B 0042	R 0052	b 0062	r 0072
3	ETX 0003	DC3 0013	# 0023	3 0033	C 0043	S 0053	c 0063	s 0073
4	EOT 0004	DC4 0014	\$ 0024	4 0034	D 0044	T 0054	d 0064	t 0074
5	ENQ 0005	NAK 0015	% 0025	5 0035	E 0045	U 0055	e 0065	u 0075
6	ACK 0006	SYN 0016	& 0026	6 0036	F 0046	V 0056	f 0066	v 0076
7	BEL 0007	ETB 0017	' 0027	7 0037	G 0047	W 0057	g 0067	w 0077

Ainsi :

<http://www.google.to/url?q=http://%53T%09%41n%09DA%09%52tZA.CO%09%6d/cgi-%62%09i%6e/%70o%63%68/r%65d%09%69r.%63%67%09%69?s=wanadoo.fr>

contient :

%53 T %09 %41 n %09 D A %09 %52 tZA.CO...

soit :

%53 définit le caractère S

T

%09 définit une tabulation non interprétée par le navigateur (en général)

%41 définit le caractère A

n

%09 définit une tabulation non interprétée par le navigateur (en général)

D

A

%09 définit une tabulation non interprétée par le navigateur (en général)

%52 définit le caractère R

etc...

ou : STAnDAR...etc. Pour les emails pris en exemple, les liens cachés sont ainsi :

<http://www.google.de/url?q=http://StANdaRTza.com/cgi-bin/poch/redirect.cgi?s=tele2.fr>

<http://www.google.fm/url?q=http://sTANdARTZA.Com/cgi-bin/poch/redirect.cgi?s=free.fr>

<http://www.google.dj/url?q=http://StAndArTZa.coM/cgi-bin/poch/redirect.cgi?s=club-internet.fr>

<http://www.google.to/url?q=http://STAnDARtZA.COm/cgibin/poch/redirect.cgi?s=wanadoo.fr>

autrement dit la nuisance se cache derrière le domaine : **standartza.com !!!**

Le reste de l'attaque est maintenant bien connu mais lors de nos recherches le serveur Web associé a été désactivé et peu d'informations sont exploitables via le WHOIS :

```
DOMAIN
Domain Name      : standartza.com (STANDA3-BMN-DOM)
Registrar       : BookMyName
Whois Server     : whois.bookmyname.com
Referral URL    : https://www.bookmyname.com
```

```
Registrant / Admin Contact :
PERSON
Stephan ZEVESKA (ZEVESK2-BMN-PE)
```

3. Actions engagées

- La publication de ce document,
- Ce cas a été reporté au niveau « .org »,