

Le Phishing vu par le Cert-IST

Philippe.Bourgeois (à) cert-ist.com



Industrie Services Tertiaire

Septembre 2005



Plan de la présentation

- Le Phishing reçu par le Cert-IST
- Analyse technique de deux cas de phishing
 - Cas 1 : Tracer un phishing
 - Quels sont les techniques des phishers ?
 - Cas 2 : Analyse des logs d'un site web de phishing
 - Qui sont les victimes ?
- Evolution observée pour les techniques de phishing

Industrie Service Tertiaire

- En moyenne 1 phishing reçu par jour
 - 80 % adressés directement au Cert-IST, mais stoppés par l'anti-spam et/ou l'antivirus
 - Phishing **Ebay** et **PayPal**
 - 20 % nous parviennent réellement et sont traités
 - Phishing reçus en **direct**, ou signalés par des **internautes**, ou plaintes transmises par d'**autres CERTs**
 - Ex : "Barclays", "Union Planter" (USA), "BBVA" (ES), banques françaises, etc...
- 5 articles du Bulletin Mensuel Cert-IST consacrés au phishing
 - Mai 2004 : Les attaques de type "Phishing"
 - Sept 2004 : Guide NGS pour la lutte contre le phishing
 - Janv 2005 : Comment traiter un incident de type "phishing" bancaire ?
 - Fév 2005 : Etude sur l'impact du "phishing" sur Internet de CipherTrust
 - Mars 2005: Evolution des techniques de "phishing" : le "pharming", les "keyloggers", ...

Industrie Service Tertiaire

- Phishing www.barclays.com (Illustration)
 - Traité le 18 mai 2005
 - Le même mode opératoire sera réutilisé 15 jours plus tard pour le phishing "4 banques françaises"
 - Point de départ
 - <http://www.google.gg/url?q=http://www.google.lv/url?q=http://8%75u%79f%09%680.%64a%2E%09%52%09%55%09/>
 - Aka : <http://8uuyfh0.da.RU/>
 - Techniques utilisées
 - Obfuscation d'URL
 - Redirections multiples (Google, MSN, ...)
 - Dyn-DNS
 - Tags "<META refresh"
 - Web-bug

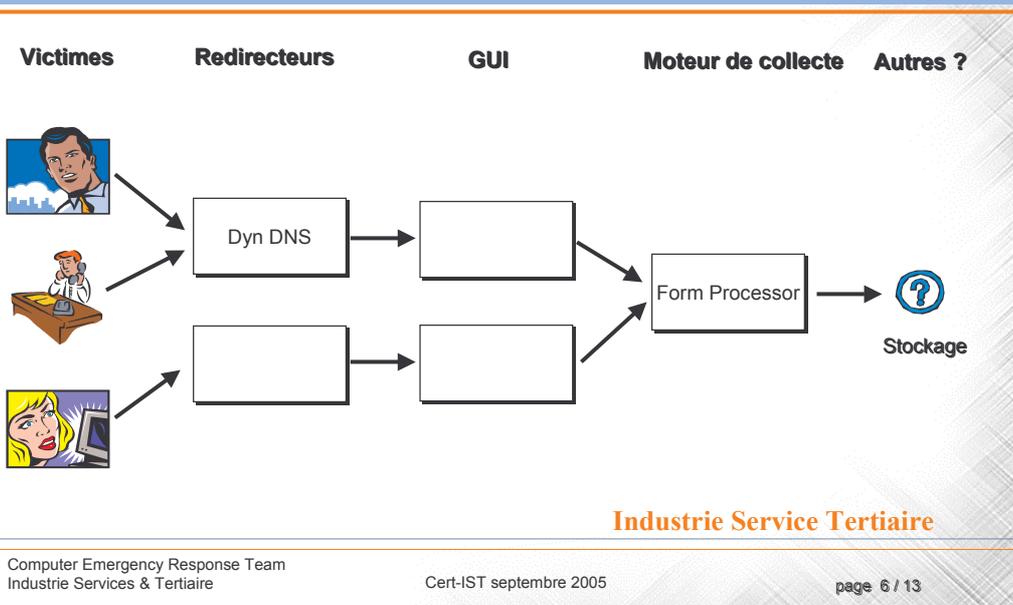
(Analyse)

(www.da.ru)

Industrie Service Tertiaire

- Les rebonds sous toutes ses formes
 - Dyn-DNS
 - Scripts répartis sur plusieurs sites (de plus en plus)
- Les portails "scripts PHP"
 - <http://www.cutandpastescrpts.com/cgi-bin/formprocessing/forms.pl>
 - <http://formprocessors.com/process/?id=xxxx>
- L'hébergement gratuit
 - Serveurs piratés
 - Ou services gratuits offerts par les FAI

Industrie Service Tertiaire



Industrie Service Tertiaire

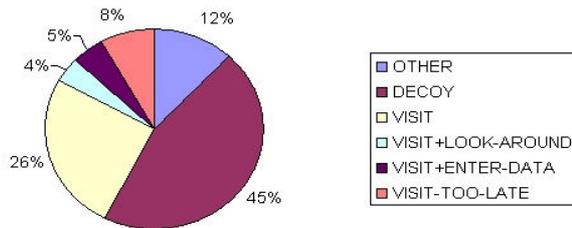
- Phishing touchant une banque espagnole
www.bbva.com
- Un site web en France héberge le phishing
- Cert-IST obtient une copie des journaux HTTP après une collaboration fructueuse avec la banque espagnole
([Logs](#))

Industrie Service Tertiaire

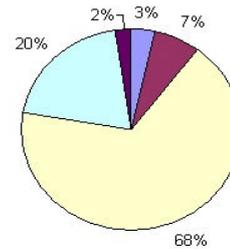
- L'analyse de log montre que 2 phishings ont été hébergés
 - [14/Apr/2005:14:22:54] => **Premier phishing** : 'GET /usr/tmp/index.html '
 - [14/Apr/2005:15:35:07] => Phishing détecté (= T0 + 44 minutes 23 secondes)
 - [15/Apr/2005:16:19:30] => Désactivé
 - => Durée de vie : **1 jour** - visiteurs : **148 IP distinctes**, dont :
 - 51 IP visiteurs "normaux"
 - 12 IP sont arrivés ensuite (une fois le phishing terminé)
 - [25/Apr/2005:04:07:58] => **Second phishing** 'GET /usr/bbva/bbva/index.htm '
 - [25/Apr/2005:09:11:14] => Détecté (= T0 + 5 heures 4 minutes)
 - [27/Apr/2005:10:38:07] => Dernière trace
 - => Durée de vie : **2 jours** – visiteurs **416 IP distinctes**, dont :
 - 385 visiteurs "normaux"

Industrie Service Tertiaire

EBay : 148 IP sources



BBVA : 416 IP sources



- 2 observations très dissemblables : difficile d'extrapoler !
2 à 5% des IP ont rempli les formulaires.

Industrie Service Tertiaire

- Les Phishings sont détectés très tôt :
Il faudrait pouvoir les arrêter vite !
 - Faciliter les remontés d'alertes vers les banques
 - Abuse@ma_banque.com
 - Faciliter la collaboration entre les victimes et les hébergeurs
 - Etablissement de points de contacts avec les CERTs
 - PS : Aux USA : <http://www.digitalphisnet.com>
"Phishing is about to become a very dangerous sport."
- Moyens techniques de lutte
 - L'analyse du "referer" HTTP semble un outil intéressant pour la détection, ou le "blocage" des sites de phishing

Industrie Service Tertiaire

- Evolution modélisée par CNCERT/CC (Chine)
 - Première génération => Ce que l'on vient de voir
 - Seconde génération => Tentative de dépôt de spyware/malware sur le poste
 - Seuls 5% des visiteurs saisissent des informations ?
 - Mais combien peuvent être infectés par un "spyware ?" **(Exemple)**
 - Troisième génération => DNS "hacking"
 - Pharming
 - Corruption de cache DNS pour détourner le "poisson" vers le site de phishing
 - Et la corruption des caches Web ?
"HTTP response splitting", "HTTP request smuggling", etc...
 - Enregistrement "abusif" de noms de domaines
 - creditmutuei.com et credillyonnais.com (13/08/2005)
 - ciscoessage.com ☺
 - Etc...

Industrie Service Tertiaire

- Progression constante des techniques d'attaques
 - Techniques "bas niveau" (rebond, portail PHP, DynDNS)
 - Techniques pour "augmenter le rendement" (Pharming, Spywares)
- Il est nécessaire de réagir rapidement face à une attaque
 - Se préparer
 - Etablir des structures d'échange et de collaboration

Industrie Service Tertiaire

Computer Emergency Response Team - Industrie Services et Tertiaire - Mozilla

http://www.cert-ist.com/

CertIST | Le CERT dédié à la communauté Industrie, Services et Tertiaire française

Accès membres [English version]

ACCUEIL | PRESENTATION | RESSOURCES | CONTACTS | FAQ | RECHERCHER

Contacter le Cert-IST au sujet d'un incident, d'une vulnérabilité ou pour adhérer.

Menaces en cours [RSS]

Date	AV	DG	AL	Maj.	Info
12.09.2005	FirefoX IDN	AV	DG	AL	Maj.
	Vul PnP MS05-029	AV	DG	AL	Maj.
	Vuln. Modems 01	AV	DG	AL	Maj.
	Backup softwares	AV	DG	AL	Maj.
	Cisco & Black-Hat	AV	DG	AL	Maj.

Risque normal

Derniers avis au 12 septembre 2005 [RSS]

- Vulnérabilité dans le démon IMAP sous Linux
- Vulnérabilité IDN dans les navigateurs Firefox, Mozilla et Netscape
- Vulnérabilité dans le serveur web Apache 2.0.x
- Multiplés vulnérabilités dans "Sun Java Web Proxy Server"
- Vulnérabilité dans "Cisco Content Services Switches 11500 Series"

Seuls les membres du Cert-IST peuvent accéder au contenu des avis.

Dernières Nouvelles [RSS]

2005-08-14 ▶ **Alerte sur le ver "Zotob"**
Le Cert-IST a émis une alerte sur le ver "Zotob" qui exploite la vulnérabilité MS05-039 (Plug & Play)

2005-08-24 ▶ **Ouverture du nouveau site web du Cert-IST**

2005-09-09 ▶ **Articles Bulletin**
Le Cert-IST met à la disposition du public certains articles de ses "Bulletins Sécurité" mensuels, cette semaine ont été rajouté(s) :

- Vulnérabilité dans les commutateurs Cisco supportant les mécanismes de sécurité 902.1x
- Faiblesse dans les concentrateurs VPN Cisco Série 3000

Copyright © 1999-2005 Cert-IST | Mentions légales | Plan du site

W3C HTML 4.01 W3C CEE