

## 第2回 救援募金する人を標的にしたフィッシング詐欺

フィッシングで情報を詐取しようとする人は、オンラインバンキングやインターネットショッピングの利用者からだけではなく、自然災害の被災者に募金しようとする善意の人たちも標的にします。今回のケースは、ハリケーンの名前が発表されると、偽サイトの開設を始め、偽サイトとは知らずに募金をしようとアクセスした人に対して、トロイの木馬を送り込んで情報を詐取しました。

- - - - 「APWG Phishing Activity Trends Report 2005年9月 日本語版」より抜粋 - - - -

### 9月期の特殊事例と新しい標的 救援募金とフォト・フィッシング攻撃

9月期 APWG は、絶望のふちにある人々を救済するという人間の善意に付け込んだフィッシング攻撃のいくつかの新事例を観測しました。今回の攻撃は、自然災害の被災者への救援募金に寄付を行う人々の善意を利用して個人情報を詐取するものでした。様々な攻撃目標と案件を対象にした攻撃があり、それらの中には、赤十字社、救世軍、ハリケーン「カトリーナ」募金およびハリケーン「リタ」募金が含まれていました。中でも攻撃件数が最も多かったのが、ハリケーン「カトリーナ」に関連した事例で、大抵の場合は赤十字社の名を騙った詐欺行為でした。ハリケーンの呼び名が発表されるや否や、詐欺工作者達は先ず救援と募金を募るサイトを反映するドメイン名を登録し、ハリケーンが上陸した直後からフィッシングメールを爆発的勢いでばら撒き始めました。

#### ハリケーン「カトリーナ」での詐欺行為事例

Websense Security Labs では、ユーザーを詐欺用サイトに誘い出す行為を行う新しいeメール詐欺について複数の報告を受けました。eメールでは先ずハリケーン「カトリーナ」についての最新情報を手短かに述べ、詳細な情報を提供するサイトへのリンクを提供します。このウェブサイトが暗号化されたJavaScript を包含しており、それが HTML Help の二つの脆弱性に付け込んでいきます。Microsoft ではこれらの脆弱性について、<http://www.microsoft.com/japan/technet/security/bulletin/MS05-001.msp> で公表しています。二つの内どちらかの脆弱性に付け込むことに成功した場合、トロイの木馬系ダウンロードがワークステーションに設置されることになります。トロイの木馬は第2の不正ファイル(これもトロイの木馬)を取り込み始めます。第2のトロイは「裏口機能」を持ち、フィッシング工作者がそのワークステーションを完全に制御することを可能にしてしまいます。ここで利用されたテクニックおよびトロイの木馬は、8月初めより出回り始めたイラクのニュースeメール詐欺事件 (Iraqi News Email Scam) と酷似しています。最初のウェブサイトのホスト国はメキシコ、第2のウェブサイトのホスト国はアメリカでした。

Websense Security Labs ではまた、数百件に上る新しいウェブサイトがハリケーン「カトリーナ」被害者救援のための募金を呼びかけていることを観測しています。これらのサイトの多くは詐欺であると思われる。

## ～ フィッシング詐欺トピックス ～

### 詐欺サイトに誘導するeメールのサンプルとメールにリンクされている詐欺サイト

Sample email text:

Just before daybreak Tuesday, Katrina, now a tropical storm, was 35 miles northeast of Tupelo, Miss., moving north-northeast with winds of 50 mph.

Forecasters at the National Hurricane Center said the amount of rainfall has been adjusted downward Monday. Mississippi Gov. Haley Barbour said Tuesday that Hurricane Katrina killed as many as 80 people in his state and burst levees in Louisiana flooded New Orleans.



**Katrina killed as many as 80 people.**

NEW ORLEANS, United States (UPI) -- Mississippi Gov. Haley Barbour said Tuesday that Hurricane Katrina killed as many as 80 people in his state and burst levees in Louisiana flooded New Orleans.

Just before daybreak Tuesday, Katrina, now a tropical storm, was 35 miles northeast of Tupelo, Miss., moving north-northeast with winds of 50 mph. Forecasters at the National Hurricane Center said the amount of rainfall has been adjusted downward Monday.

Thirty storm-related deaths in Mississippi's Harrison County were at an apartment complex, near the beach in Biloxi, Kelly Jakubic with the county's Emergency Operations Center told CNN.

Louisiana Gov. Kathleen Babineaux Blanco said there was no official death tally in Louisiana, but said she expected that to change.

Meanwhile, New Orleans Mayor Ray Nagin said a levee holding back the waters of Lake Pontchartrain breached, forcing the air evacuation of 90 patients from a hospital.

"The city of New Orleans is in a state of devastation," Nagin told WWL-TV. "We probably have 80 percent of our city underwater. With some sections of our city, the water is as deep as 20 feet."

next article  
Zotob worm exploits Windows  
**VIRUS ALERT**  
Exploit code for recently patched Windows flaws has swiftly evolved into a new series of worms...  
[Read more...](#)

### 事例その2

Websense Security Labs では、ハリケーン「カトリーナ」の被災者救援努力を支えるために募金をする人々を標的とする新しいフィッシング攻撃についての報告を受けました。詐欺メールは HTML で書かれ、あたかも赤十字社からのメールであるかのように装っていました。このメールはまた、ベリサイン社 (Verisign) の安全サイト (Secure Site) の認証ロゴを付けており、エンド・ユーザーを騙して合法的なメールであるかのように信じ込ませる試みでした。そのメールに書かれたリンクに接続すると、ユーザーは (本警告の発表時点では) ブラジルにあった詐欺用のウェブサイトへ誘導されました。このサイトは他のコンテンツのホストにもなっており、互換性があるようでした。ユーザーのクレジットカード番号、有効期限、PIN コードをオンライン・フォームで入力するよう求められ、その後、本物の赤十字社のウェブサイトへ転送される仕組みでした。

### 赤十字社を装った詐欺メール

Phishing email body:

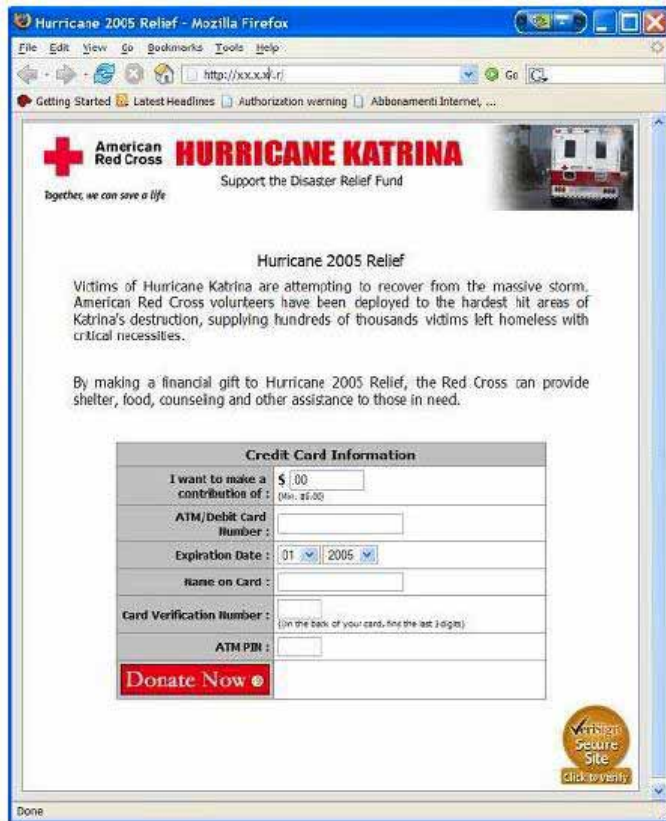
Victims of Hurricane Katrina are attempting to recover from the massive storm. American Red Cross volunteers have been deployed to the hardest hit areas of Katrina's destruction, supplying hundreds of thousands victims left homeless with critical necessities.

By making a financial gift to Hurricane 2005 Relief, the Red Cross can provide shelter, food, counseling and other assistance to those in need.

Phishing website screenshot

## ～ フィッシング詐欺トピックス ～

### メールにリンクされている詐欺サイト



APWG では、これらの事例に加え、一般に普及しているオンライン・サービスやオンライン・ゲームをターゲットとしたフィッシング攻撃の出現を察知し始めました。ほとんどの場合、エンド・ユーザーの信用情報を取得し、そのアカウントで接続できる他のサービスに接続したり、ログオン信用情報を得るためのキーロガーをインストールしたり、または、オンライン・ゲームのトークンを得るためにログオン信用情報を獲得するというのが目的でした。