सत्यमेव जयते

Dr. Gulshan Rai

Director General
CERT-In

भारत सरकार
संचार एवं सूचना प्रौद्योगिकी मंत्रालय
सूचना प्रौद्योगिकी विभाग
भारतीय कम्प्यूटर आपात प्रतिक्रिया दल (सर्ट-इन)
इलेक्ट्रॉनिक्स निकेतन, 6, सी.जी.ओ. कॉम्प्लेक्स, नई दिल्ली-110003

Government of India
Ministry of Communications and Information Technology
Department of Information Technology
Indian Computer Emergency Responce Team (CERT-In)
Electronics Niketan, 6, C.G.O. Complex, New Delhi-110003
Tel : 24368544 Fax : 24366806 E-mail: grai@mit.gov.in

D.O.No.2 (44)/2009-CERT-In

24.12.2009

Dy. No. 4-4925
Date 31/12

Dear Madam,

Sub: Targeted attacks on Government organizations through malicious emails

We have received reports that targeted attacks are being launched on Government organizations through malicious emails. In these attacks malicious PDF documents with malware embedded inside are being crafted and sent as attachment with convincing emails pretending to be from trusted sources. The emails could be from spoofed or compromised email accounts.

An advisory indicating the precautionary measures to be taken against these attacks is enclosed herewith.

We would request that all email users in your Ministry and other organizations under purview of the Ministry may kindly be alerted accordingly.

With regards,

Yours sincerely,

Encl: As above

53/US(AI)
6.1.10

(Gulshan Rai)

Ms. K. Sujata Rao
Secretary,
Deparment of Health and Family,Welfare,
M/o Health and Family Welfare,
Nirman Bhavan, New Delhi.

52

CERT-In Advisory CIAD-2009-S-2

Targeted attacks on Government Networks exploiting Adobe Flash player, Reader and Acrobat vulnerabilities

Original Issue Date: December 18, 2009
Severity Rating: High

It has been observed that targeted attacks are being launched on government networks through maliciously crafted emails and PDF attachments. These PDF file attachments are embedded with malicious code specially designed for exploiting Adobe flash player, Acrobat and Reader vulnerabilities.

Typically the emails sent by attacker are spoofed with "From" addresses of trusted agencies and colleagues. Since this embedded malicious code is not publicly known, the Antivirus and Anti spyware programs popular in India may not detect the same.

Users are advised to take following precautions to protect their systems against these targeted attacks.

- Do not open PDF files received from untrusted and unknown sources
- Apply patches and security updates for Adobe flash player, Acrobat and Reader
- Exercise caution while opening email attachments
    - Do not open emails and attachments received from untrusted sources and unexpectedly received from trusted sources
- Access web mails through trusted systems
- Do not visit untrusted websites or click URLs provided in emails
- Disable automatic opening of PDF documents in web browser
- Set the Security settings in the browser to prompt before executing active scripting such as Java applets/scripts, ActiveX controls etc. Execute scripts from trusted sources only.
- Deploy different antivirus/anti spyware products at multiple defense levels
- Use Antivirus/Antispyware programs for Gateway, servers, desktops and email clients and update them regularly
- Apply patches and updates at the Operating System and Application level
- Use personal/desktop firewalls apart from perimeter firewalls
- Preferably use Host IPS/Host IDS in addition to Network IPS
- Monitor systems for any suspicious activities such as unusual traffic, unknown processes, reduced system performance, abnormal memory usage etc.
- Mail server administrators should enforce policies for setting up strong passwords for mail accounts and change of passwords periodically
- Report any suspicious activities to System/Network administrator and CERT-In Incident Response Help Desk

For further information refer to following resources:

http://www.cert-in.org.in/vulnerability/civn-2009-154.htm
http://www.cert-in.org.in/advisory/ciad-2009-58.htm
http://www.cert-in.org.in/virus/PDF_Malware.htm
http://www.cert-in.org.in/vulnerability/civn-2009-119.htm
http://www.cert-in.org.in/vulnerability/civn-2009-91.htm
http://www.cert-in.org.in/advisory/ciad-2009-28.htm
http://www.cert-in.org.in/advisory/ciad-2009-09.htm