



सत्यमेव जयते
Director
CERT-In

Dr. Gulshan Rai

Handwritten signature and date:
17/3/09

D.O. No. 2(6)/2009-CERT-In

भारत सरकार
संचार एवं सूचना प्रौद्योगिकी मंत्रालय
सूचना प्रौद्योगिकी विभाग
भारतीय कंप्यूटर 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 Response Team (CERT-In)
Electronics Niketan, 6, C.G.O. Complex, New Delhi-110003
Tel : 24368544 Fax : 24366806 E-mail: grai@cert-in.org.in

04.03.2009

396

17/3/09

Sub: Large scale propagation of Conficker/Downadup worm

Dear Shri Jain,

It has been observed that a self-updating worm Win32 Conficker alias Downadup, Kido is spreading widely and its infections in India has risen exponentially.

It was first discovered in November 2008 and very successful in propagating across the Internet in short span of time. Following observations have been made so far:

- The initial variant of the worm used a vulnerability in Microsoft's Windows operating system to spread to vulnerable computers. This vulnerability has been addressed by Microsoft in security bulletin MS08-067 and respective patches for different affected Microsoft operating systems have been released.
- The second iteration of the worm also spreads through open network shares and attempts to access weakly-protected systems by trying common passwords.
- The later variant, known as Conficker.B, also propagates by copying itself through USB memory sticks by infecting the autorun.inf file. This worm prevents the infected computers from updating security and systems software by blocking access to domains of Microsoft and many security firms.

In view of the wide spread exploitation, organizations are advised to follow the following countermeasures:

- Apply appropriate patches as described in CERT-In vulnerability Note CIVN-2008-170
- Disable autoplay/autorun features on all removable drives.
- Block ports 139 and 445 at the perimeter
- Install and maintain updated anti-virus software at gateway and desktop level
- Install and maintain Desktop Firewall and block the ports which are not required
- Exercise caution when opening email attachments and accepting file transfers
- Exercise caution when clicking on links to web pages


For further details regarding this threat and related countermeasures refer to:

- CERT-In vulnerability note (CIVN-2008-170)
<http://www.cert-in.org.in/vulnerability/civn-2008-170.htm>
- CERT-In Virus alert
http://www.cert-in.org.in/virus/win32_conficker.htm
- CERT-In Current activity
<http://www.cert-in.org.in/currentacts/currentact07.htm#WCDK>

For any further technical advice please contact our Incident Response Help Desk.

With regards,

Yours sincerely,



(Gulshan Rai)

Shri Anurag Jain, IAS
Secretary IT
Government of Madhaya Pradesh,
Dept. of IT, Room No.533,
Mantralaya,
Bhopal 462 004.