

RB Balch – VIRUS ALERT – PEACOMM Trojan Virus

=====

This is being sent to you as a subscriber of the RB Balch IT Consultants PC Tips monthly newsletter.

VIRUS ALERT: Trojan.Peacomm

SYSTEMS AFFECTED: Windows 2000, Windows 95, Windows 98, Windows ME, Windows NT, Windows XP

Major antivirus teams are reporting the increase in infections from the Trojan.Peacomm. The threat arrived in an email with an empty body and a variety of subjects such as:

- A killer at 11, he's free at 21 and kill again!
- U.S. Secretary of State Condoleezza Rice has kicked German Chancellor Angela Merkel
- British Muslims Genocide
- Naked teens attack home director.
- 230 dead as storm batters Europe.
- Re: Your text
- Radical Muslim drinking enemies's blood.
- Chinese missile shot down Russian satellite
- Chinese missile shot down Russian aircraft
- Chinese missile shot down USA aircraft
- Chinese missile shot down USA satellite
- Russian missile shot down USA aircraft
- Russian missile shot down USA satellite
- Russian missile shot down Chinese aircraft
- Russian missile shot down Chinese satellite
- Saddam Hussein safe and sound!
- Saddam Hussein alive!
- Venezuelan leader: "Let's the War beginning".
- Fidel Castro dead.

ATTACHMENT: (NOTE: Do NOT open)

There may be one of the following attachments:

- FullVideo.exe
- Full Story.exe
- Video.exe
- Read More.exe
- FullClip.exe
- GreetingPostcard.exe
- MoreHere.exe
- FlashPostcard.exe
- GreetingCard.exe
- ClickHere.exe
- ReadMore.exe
- FlashPostcard.exe
- FullNews.exe

The attachment is actually a Trojan Horse program that, when installed, causes the computer to connect to a network and download additional malware for installation. This creates a network of infected computers that the attackers can use in a variety of ways. Symantec has recently upgraded this threat to a Category 3 due to the increased message traffic as a direct result of the infection.

RECOMMENDATIONS:

All users are advised to adhere to the following basic security "best practices":

- Always keep your patch levels up-to-date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, mail, and DNS services (for example, all Windows-based computers should have the current Service Pack and Critical Updates installed.)
- Ensure all Antivirus software is updated regularly
- Enforce a password policy. Complex passwords make it difficult to crack password files on compromised computers. This helps to prevent or limit damage when a computer is compromised.
- Isolate infected computers quickly to prevent further compromising your organization. Perform a forensic analysis and restore the computers using trusted media. UNPLUG infected computer from the network and contact RB Balch to service the infected machine.
- Do not open attachments unless you are expecting them. Also, do not execute software that is downloaded from the Internet unless it has been scanned for viruses. Simply visiting a compromised Web site can cause infection if certain browser vulnerabilities are not patched.
- Turn off HTML email – a specially crafted HTML email may install this or other malicious software on your system without your approval.

From time to time, in the event of computer related information we believe is of an urgent nature, you may receive an ALERT, in addition to our regular newsletter.

MAINTENANCE

To be added or removed from our newsletter, go to: <http://www.rbbalch.com> and click on the Newsletter box on the right. OR call us OR simply reply to this email and write remove in the message or subject. Your email address is absolutely only used by us at RB Balch.

=====

RB Balch Computer Consultants
PO BOX 10007
Glendale, AZ 85318
<mailto:help@rbbalch.com>
1-800-922-5249 (1-800-9-BALCH-9)

Copyright (c) 2004, 2005, 2006, 2007 RB Balch & Associates, Inc. ALL RIGHTS RESERVED
newsletter sent to: %%EMAIL%%