NEW YORK STATE OFFICE OF CYBER SECURITY AND CRITICAL INFRASTRUCTURE COORDINATION
CYBER ADVISORY

CSCIC ADVISORY NUMBER:
2007-003

DATE ISSUED:
January 23, 2007

SUBJECT:
Wide-Spread Trojan Horse Infection

OVERVIEW:
A wide-spread Trojan horse infection called Peacomm is being distributed via email attachments. When the attachment is opened, the Trojan infects the computer and allows a hacker to control the infected system. It also attempts to download other malicious software for further exploitation of the affected computer.

The highest risk is to home users since most organizations already block executable email attachments. However, an organization's risk may be higher if it allows staff to use their personal computers (e.g. remote access via dial in or broadband connections) to access the organization's internal network or allows employees to connect their laptops to unprotected, external networks.

SYSTEMS AFFECTED:

- Microsoft Windows 2000/95/98/ME/NT/XP

RISK:
Government:

- Large and medium government entities: **Medium**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **Medium**
- Small business entities: **Medium**

Home users: **High**

DESCRIPTION:

Trojan.Peacomm arrives via an unsolicited email as an attachment, typically an executable file (e.g. .exe). Once this attachment has been executed the Trojan creates the file wincom.sys in the %System% folder, which varies depending on the Operating System. The wincom.sys file opens UDP ports 4000 and 7871 for listening and scans on those same ports for other infected hosts which are then deposited into a list stored on the infected host. The host will attempt to contact, or be contacted by, a controlling server. If a connection is made, the Trojan will download a worm, or other malware, depending on the configuration of the controlling server.

RECOMMENDATIONS:
We recommend that all of the following actions be taken:

- Ensure email gateways are configured to filter executable attachments, such as .exe. .scr, .pif, .vbs and .bat.
- Update your anti-virus software signatures on all desktops, laptops and servers as soon as possible. Virus definitions to detect this Trojan are available from multiple vendors.
- Remind staff of the dangers of opening suspicious and unsolicited emails.

- Ensure that VPN connections are configured to only allow business services, and remind users to disconnect from the VPN when there is no longer a need to access the business internal services.
- Ensure that your organization requires home computers that access your organization's internal network to have the following protection mechanisms:
    - Antivirus software with current signature files
    - Firewall
    - Current operating system and software patches installed
    - Ensure that unauthorized hosts cannot connect to the organization's internal network.

REFERENCES:

Common Malware Enumeration
http://cme.mitre.org/data/list.html#711

Symantec
http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2007-011917-1403-99

McAfee
http://vil.nai.com/vil/content/v_141316.htm

Trend Micro
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ%5FSMALL%2EEDW&VSect=P

F-Secure
http://www.f-secure.com/v-descs/small_dam.shtml