OCC ALERT

Comptroller of the Currency
Administrator of National Banks

Subject: Threat Posed by New Internet Virus (Bugbear.B)

TO: Chief Executive Officers and Chief Information Technology Officers of National Banks, Federal Branches, Service Providers and Software Vendors, Department and Division Heads, and Examining Personnel

PURPOSE

This alert is intended to raise awareness of an Internet virus, Bugbear.B, that recently surfaced as a potentially serious threat to financial institutions and to prompt banks and bank technology service providers to take immediate steps to mitigate the threat to their organizations and customers.

BACKGROUND

Viruses are an increasing threat to Internet-connected systems. The Bugbear.B virus is the latest and most capable variant that threatens financial institutions. Institutions with the capability to access the Internet, including dial-up connections, may be vulnerable to the Bugbear.B virus and other viruses, and should institute appropriate measures to mitigate the risks posed to their servers, desktops, laptops, and other computing devices.

Information about Bugbear.B is available from many sources, such as FedCIRC, CERT/CC, and commercial anti-virus vendors. Although the available information varies, and may be subject to change, Bugbear.B seems to possess the following general characteristics:

- Disables security software such as anti-virus software;
- Installs spyware such as a keystroke logger and a remote control program;
- Captures keystrokes to obtain authentication information, gathers other potentially sensitive information, and e-mails it outside the bank;
- Collects and uses e-mail addresses to further distribute the virus from the infected machines; and
- Targets more than 1,300 specific financial institutions with additional features by including their Internet addresses in the virus's code.

The disabling of security software is a concern because the victim loses the protection and audit trail provided by the software. The insertion of spyware combined with the e-mail distribution of the resulting information could also provide an attacker with confidential information such as including usernames and passwords to bank systems. With such information, the attacker could

access bank systems to insert new malicious software or to steal confidential information and funds. Additionally, the remote control features appear to be available to anyone who wishes to use them. Access to these features increases the risk from internal and external attackers.

The disabling of security software, insertion of spyware, and e-mailing of information outside an infected bank could occur whether or not the bank is included in the 1,300 specifically mentioned bank Internet addresses.

RESPONSE TO THE ELEVATED VIRUS THREAT

Institutions should review their capabilities to prevent, detect, and respond to Bugbear.B consistent with the guidance provided in *Federal Financial Institution Examination Council's Information Technology Handbook.*[1] Specific steps include:

- Increasing awareness among system users so they can help identify and stop the spread of computer viruses;
- Ensuring anti-virus software is installed on all servers and clients with updated anti-virus signatures;
- Contacting service providers and other vendors to ensure appropriate awareness and response;
- Installing specific intrusion detection system signatures;
- Following-up closely on abnormal system and printer behavior;
- Changing passwords on potentially compromised systems;
- Following-up rigorously any suspected infection;
- Verifying configurations and patch levels; and
- Updating the information security program to address any new threats or controls.

In the event your institution is a victim of Bugbear.B, you should notify your OCC portfolio manager. You should also report to law enforcement and file a Suspicious Activity Report as appropriate based on the impact of the virus infection on your institution.

Questions regarding this alert should be directed to Clifford A. Wilke, Director, Bank Technology Division at (202) 874-5920 or clifford.wilke@occ.treas.gov.

_____

Ralph Sharpe
Deputy Comptroller for Bank Technology

[1] The FFIEC Information Security Booklet is available at http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html.