Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

January 20, 2012

## JOINT FBI AND DHS PUBLIC SERVICE ANNOUNCEMENT: BEST PRACTICES FOR RECOVERY FROM THE MALICIOUS ERASURE OF FILES

Cyber criminals can damage their victim's computer systems and data by changing or deleting files, wiping hard drives, or erasing backups to hide some or all of their malicious activity and tradecraft. By wiping, or "zeroing out," the hard disk drives, which overwrites good data with zeros or other characters, the criminals effectively erase or alter all existing data, greatly impeding restoration. This sort of criminal activity makes it difficult to determine whether criminals merely accessed the network, stole information, or altered network access and configuration files. Completing network restoration efforts and business damage assessments may also be hampered.

The FBI and DHS encourage businesses and individuals to employ mitigation strategies and best practices such as:

- Implement a data back-up and recovery plan to maintain copies of sensitive or proprietary data in a separate and secure location. Backup copies of sensitive data should not be readily accessible from local networks.
- Regularly mirror and maintain an image of critical system files.
- Encrypt and secure sensitive information.
- Use strong passwords, implement a schedule for changing passwords frequently, and do not reuse passwords for multiple accounts.
- Enable network monitoring and logging where feasible.
- Be aware of social engineering tactics aimed at obtaining sensitive information.
- Securely eliminate sensitive files and data from hard drives when no longer needed or required.

The US-CERT Web page at www.us-cert.gov hosts a wide range of tips, best practices, and threat information for business and home users.

To receive the latest information about cyber schemes, please visit the FBI Web site and sign up for e-mail alerts by clicking on one of the red envelopes.

If you have been a victim of cyber crime, please file a report with the Internet Crime Complaint Center at www.IC3.gov.