Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 11:33:33 UTC

(US-CERT) This file is a malicious 32-bit Windows executable. Analysis indicates the primary purpose of this application is to destroy a compromised Windows system by overwriting and deleting the Master Boot Record (MBR) on the victim's system and deleting files on network mapped shares as well as physically attached storage devices.

The malware must be executed from a command line using any alphanumeric character or string as an argument. Once executed, themalware first attempts to disable the 'System Event Notification' and 'Alerter' services.

Note: The Alerter service is present in Windows XP and Windows 2003, which are no longer supported by Microsoft. Current operating systems supported by Microsoft do not run the Alerter service.

Next, the malware overwrites the MBR, displaying a status in the command (CMD) window. If the malware is able to overwrite the MBR, an 'OK' status is displayed in the CMD window. If the malware is unable to overwrite the MBR, a 'Fail' status is displayed.

After the MBR is overwritten, the malware attempts to gain access to physical and network drives attached to the victim's system and recursively enumerate through the drive’s contents. When the malware identifies a file, it overwrites the file's contents with NULL bytes, renames the file with a randomly generated file name, then deletes the file, making forensic recovery impossible.

If the malware is able to overwrite, rename and delete the file, the CMD window will display a 'Break>' status. If the malware is only able to delete the file, the CMD window will display a 'Del>' status.

Once the malware has completed deleting files, the system is rebooted. If the malware has executed successfully, the system is rendered inoperative.
