



Best of ThreatChaos

## Ten Most Important Security Incidents Involving Removable Devices

I thought it would be valuable to put the top ten most important incidents regarding removable devices, including hardware keystroke loggers, USB thumb drives, and MP3 players, together into a list. It helps highlight the risks inherent in removable devices to have all of these incidents in one place.

### 10. UK Policeman loses memory stick containing terrorist cell information

“The black 4GB stick was lost after being taken out of Castle Vale police station by an officer on patrol. It was reported that the memory stick contains details of terror cells being tracked by police but the force refused to comment.” [Article.](#)

9. **UK Prison inmate information loss.** “a consultant for PA Consulting copied files containing records on all 84,000 prisoners in England and Wales onto a USB drive, which then got lost.” [Article.](#)

8. **Sumitomo Bank Heist.** This incident is still the largest attempted bank robbery in history. A PS2 hardware keystroke logger was used to capture information used to attempt SWIFT wire transfers from the London Branch of Sumitomo Mitsui. More details are trickling out from the trial of the some members of the gang this month. [Questions on Sumitomo.](#)

7. **Apple [ships](#) iPods infected with a windows virus.** It turns out that manufacturers of removable media have to ensure antiseptic environments when they pre-load software and data on their devices. Also worth mentioning is [Sony's inclusion of hidden files](#) on USB devices that could prove useful to virus and worm writers.

6. **US Military spy incident.** A former U.S. military contractor has [pleaded guilty](#) to exceeding authorized access to a computer and aggravated identity theft after he was accused of selling names and Social Security numbers of 17,000 military employees, the U.S. Department of Justice said. Price \$500.

5. **USB Candy Drop.** A Security investigator dropped 20 Trojan carrying USB thumb drives in a Credit Union Parking Lot. According to [his report](#) “Of the 20 USB drives we planted, 15 were found by employees, and all had been plugged into company computers” within three days.

4. **New Zealand man buys MP3 player with US military data.** ONE News has [gained access](#) to the personal files of American soldiers, uncovering military secrets from the most powerful nation in the world.

3. **Indian Spy Incident.** A CIA operative “Rosanne Minchew, third secretary in the US embassy in Delhi” [reportedly](#) paid \$50,000 for a USB device loaded with Indian secret information. Note that the CIA pays considerably more for information than other agencies (see above).

2. **Countrywide theft of 2 million records.** “For more than two years, the employee was able to steal up to 20,000 records a time by copying files from the corporate network to a USB flash drive.” [Article.](#)

1. **Russian attack on US Military Central Command.** The agent for this attack is apparently the USB born worm w32.agent.btz According to F-Secure the worm is installed from an infected thumb drive and places itself on every drive on a computer including any USB drive that is attached to it. [Article.](#)

This entry was posted on Monday, February 23rd, 2009 at 11:26 am and is filed under [Australia](#), [Bank security](#), [Security](#), [data protection](#). You can follow any responses to this entry through the [RSS 2.0](#) feed. You can [leave a response](#), or [trackback](#) from your own site.