

DoD Hit By Massive Cyber Attack

Facts & Intelligence

INTEL: The hybrid worm/virus is said to be called "Agent.btz." That's a variation of the "SillyFDC" worm, which spreads by copying itself to thumb drives and the like.

INTEL: The US-CERT (Computer Emergency Response Team) issued a warning on Thursday that malicious code is increasingly propagating via USB flash drive devices.

INTEL: Oddly enough, all Internet users are being warned to stay vigilant by security experts who believe that next Monday (11/24/2008) is poised to be the worst day the year for computer attacks.

FACT: In any given month there are over 225 new computer viruses identified.

The Pentagon has suffered a direct hit from a cyber attack. The weapon used is said to be a hybrid computer worm/virus. Insiders say the hybrid rapidly spread through the thousands of interconnected computer networks. A computer worm is different from a computer virus. A worm is thought to be more dangerous because it can run itself where a virus needs a host program to run. The DoD responded quickly and have taken steps to slow the advancement of the worm/virus by quarantining networks and systems until the worm/virus can be removed.

Cyber investigators have not pinpointed the entry point for the worm/virus, but insider sources point to removable storage devices as the most likely point of infection. This seems to be supported by the fact that U.S. Strategic Command (STRATCOM) has banned the use of removable media (thumb drives, CDRs/DVDRs, floppy disks) on all DoD networks and computers effective immediately. This incident has been deemed "So Severe" that unprecedented defensive measures have been instituted to protect the military systems.

Security experts at Spy-Ops I spoke with said, "If this can happen to the Department of Defense it can happen to any organization." They went on to say that the cost of this attack could easily reach into the billions of dollars if the worm/virus destroys data. If that is not bad enough, one expert went on to say that the nightmare scenario is if the malicious code alters data rather than deleting it – a much more difficult problem to resolve.

News of the cyber attack came on the heels of today's release of the "Global Trends 2025: A Transformed World" document by the Office of the Director of National Intelligence (ODNI). In that document it stated that **Non-military means of warfare, such as cyber, economic, resource, psychological, and information-based forms of conflict will become more prevalent in conflicts over the next two decades.** While the source of the attack remains classified, the usual cast of characters comes to mind. At the head of the list are of course China and the RBN – Russian Business Network. If the attack is found to be sponsored by another country, could this be considered an act of cyber war?



The Technolytics Institute

4017 Washington Road
Mail Stop # 348
McMurray, PA 15317
P 888-650-0800
F 412-291-1193
I www.technolytics.com
E info@technolytics.com
© Technolytics 2001-2008
All Right Reserved.

When was the last time you updated your antivirus software and scanned your computer?