NOAH SHACHTMAN SECURITY 11.19.08 03:12 PM

UNDER WORM ASSAULT, MILITARY BANS DISKS, USB DRIVES

The Defense Department's geeks are spooked by a rapidly spreading worm crawling across their networks. So they've suspended the use of so-called thumb drives, CDs, flash media cards, and all other removable data storage devices from their nets, to try to keep the worm from multiplying any further.

The ban comes from the commander of U.S. Strategic Command, according to an internal Army e-mail. It applies to both the secret SIPR and unclassified NIPR nets. The suspension, which includes everything from external hard drives to "floppy disks," is supposed to take effect "immediately." Similar notices went out to the other military services.

In some organizations, the ban would be only a minor inconvenience. But the military relies heavily on such drives to store information. Bandwidth is often scarce out in the field. Networks are often considered unreliable. Takeaway storage is used constantly as a substitute.

The problem, according to a second Army e-mail, was prompted by a "virus called Agent.btz." That's a variation of the "SillyFDC" worm, which spreads by copying itself to thumb drives and the like. When that drive or disk is plugged into a second computer, the worm replicates itself again — this time on the PC. "From there, it automatically downloads code from another location. And that code could be pretty much anything," says Ryan Olson, director of rapid response for the iDefense computer security firm. SillyFDC has been around, in various forms,

since July 2005. Worms that use a similar method of infection go back even further — to the early '90s. "But at that time they relied on infecting floppy disks rather than USB drives," Olson adds.

Servicemembers are supposed to "cease usage of all USB storage media until the USB devices are properly scanned and determined to be free of malware," one e-mail notes.
Eventually, some government-approved drives will be allowed back under certain "mission-critical," but unclassified, circumstances. "Personally owned or non-authorized devices" are "prohibited" from here on out.

To make sure troops and military civilians are observing the suspension, government security teams "will be conducting daily scans and running custom scripts on NIPRNET and SIPRNET to ensure the commercial malware has not been introduced," an e-mail says. "Any discovery of malware will result in the opening of a security incident report and will be referred to the appropriate security officer for action."

"The USB ban should be effective in stopping the worm," Olson says. Asked if such a wide-spread measure was a bit of over-kill, Olson responded, "I don't know."

"I know this [is an] inconvenience," e-mails one Michigan Army National Guardsman. "This has been briefed to the CoS [Chief of Staff] of the ARMY. This is not just a problem for Michigan, and is effecting operations around the world. This is a very serious threat and should be treated as such. Please understand that this is a form of attack, and we need to have patience in dealing with this issue."

[Photo: Department of Defense]

#INFO WAR

VULNERABILITIES

Police Bodycams Can Be Hacked to Doctor Footage

LILY HAY NEWMAN

SECURITY ROUNDUP

Surprise, the FCC Lied About That DDoS Attack

EMILY DREYFUSS

VOTING MACHINES

At DefCon, the Biggest Election Threat Is Lack of Funding

LILY HAY NEWMAN

#NEVERTWEET

A Tweet About Hacking Gets a Google Engineer in Trouble

LOUISE MATSAKIS

BUGS

Millions of Android Devices Are Vulnerable Out of the Box

BRIAN BARRETT

IOT

HACKABLE TOUCHSCREENS COUL ON HOTEL ROOMS AND MEETINGS

LOUISE MATSAKIS

WE RECOMMEND

POWERED BY OUTBRAIN

LOUISE MATSAKIS

Even Anonymous Coders Leave Fingerprints

LILY HAY NEWMAN

Bugs in Mobile Credit Card Readers C Expose Buyers

LILY HAY NEWMAN

Hacking a Brand New Mac Remotely, Out of the Box

EMILY DREYFUSS

Smartphone Voting Is Happening, bu One Knows if It's Safe

LILY HAY NEWMAN

A New Pacemaker Hack Puts Malwar Directly on the Device

GET OUR NEWSLETTER

WIRED's biggest stories delivered to your inbox.

Enter your email

SUBMIT

WIRED