YET ANOTHER "LADY GAGA" EXPOSURE FORCES DOD TO WIPE DRONE CONTROL COMPUTERS

On Friday, Wired broke the news that the DOD suffered yet another breach because they continue to leave computers exposed to outside storage systems. (h/t WO) In this case, the Ground Control Stations they use to control drones got infected with a keylogger virus.

> But time and time again, the so-called "air gaps" between classified and public networks have been bridged, largely through the use of discs and removable drives. In late 2008, for example, the drives helped introduce the agent.btz worm to hundreds of thousands of Defense Department computers. The Pentagon is still disinfecting machines, three years later.
>
> Use of the drives is now severely restricted throughout the military. But the base at Creech was one of the exceptions, until the virus hit. Predator and Reaper crews use removable hard drives to load map updates and transport mission videos from one computer to another. The virus is believed to have spread through these removable drives. Drone units at other Air Force bases worldwide have now been ordered to stop their use.

After a virus was introduced into computers in Iraq three years ago via thumb drive, DOD claimed it had prohibited the use of any removable media with their computers. But then Bradley Manning allegedly removed hundreds of thousands of classified cables from SIPRNet

using a Lady Gaga CD. Rather than making all computers inaccessible to removable media at that point, DOD left 12% of their computers vulnerable, deploying a buddy-system to prevent people from taking files inappropriately; but human buddy systems don't necessarily prevent the transmission of viruses.

The good news is that the Host-Based Security System implemented in response to Wikileaks discovered the virus—two weeks ago.

But here's the other interesting wrinkle. To get rid of these viruses, techs have resorted to wiping the hard drives of the targeting computers.

> In the meantime, technicians at Creech are trying to get the virus off the GCS machines. It has not been easy. At first, they followed removal instructions posted on the website of the Kaspersky security firm. "But the virus kept coming back," a source familiar with the infection says. Eventually, the technicians had to use a software tool called BCWipe to completely erase the GCS' internal hard drives. "That meant rebuilding them from scratch" — a time-consuming effort.

Given what little we know about the Anwar al-Awlaki assassination (which, as Wired points out, happened after the virus had knowingly infected these computers), this should not affect the computers that ten days ago killed two US citizens with no due process. The Newsweek story describing the CIA's targeting process says **that** targeting is done in VA, not NV, where the virus hit.

But particularly given the questions about Samir Khan's death, consider if that weren't the case. That would mean a key piece of evidence about whether or not the US knowingly executed an American engaging in speech might be completely eliminated, wiped clean to fix a predictable

virus.

That’s not the only risk, of course. We’ve talked before about how long it’ll take for Iran or Mexican drug cartels to hack our armed drones. If this virus were passed via deliberate hack, rather than sloppiness, then we might be one step closer to that eventuality.

All because DOD continues to refuse to take simple steps to secure their computers.