Computer Virus Hits U.S. Drone Fleet

by Noah Shachtman via Kismo - Wired *Monday, Oct 10 2011, 7:53am*
international / peace/war / other press

This Story is DoD 'Phishing' -- no way DoD would advertise its weakness if it were Real

> A computer virus has infected the cockpits of America's Predator and Reaper drones, logging pilots' every keystroke as they remotely fly missions over Afghanistan and other warzones. *[Really! Editorial advice is the story is not to be taken at face value; "Wired" is a suss source, as verified with the Lamo, Assange and Bradley Manning affair. Technically speaking, it is well known that all remote control computer systems are subject to hacker intervention, though in this instance we doubt authenticity. Most sustained attacks are directed at high yield/reward military satellite systems. Nevertheless, if such a breach has occurred it would be more the result of USAF ineptitudes rather than external hacker skills. The USA continues to trail most nations in the field of Cyber warfare -- closing wide IT gaps in expertise is almost impossible.]*

The virus, first detected nearly two weeks ago by the military's Host-Based Security System, has not prevented pilots at Creech Air Force Base in Nevada from flying their missions overseas. Nor have there been any confirmed incidents of classified information being lost or sent to an outside source. But the virus has resisted multiple efforts to remove it from Creech's computers, network security specialists say. And the infection underscores the ongoing security risks in what has become the U.S. military's most important weapons system.

"We keep wiping it off, and it keeps coming back," says a source familiar with the network infection, one of three that told Danger Room about the virus. "We think it's benign. But we just don't know."

Military network security specialists aren't sure whether the virus and its so-called "keylogger" payload were introduced intentionally or by accident; it may be a common piece of malware that just happened to make its way into these sensitive networks. The specialists don't know exactly how far the virus has spread. But they're sure that the infection has hit both classified and unclassified machines at Creech. That raises the possibility, at least, that secret data may have been captured by the keylogger, and then transmitted over the public internet to someone outside the military chain of command.

Drones have become America's tool of choice in both its conventional and shadow wars, allowing U.S. forces to attack targets and spy on its foes without risking American lives. Since President Obama assumed office, a fleet of approximately 30 CIA-directed drones have hit targets in Pakistan more than 230 times; all told, these drones have killed more than 2,000 suspected militants and civilians, according to the Washington Post. More than 150 additional Predator and Reaper drones, under U.S. Air Force control, watch over the fighting in Afghanistan and Iraq. American military drones struck 92 times in Libya between mid-April and late August. And late last month, an American drone killed top terrorist Anwar al-Awlaki — part of an escalating unmanned air assault in the Horn of Africa and southern Arabian peninsula.

But despite their widespread use, the drone systems are known to have security flaws. Many Reapers and Predators don't encrypt the video they transmit to American troops on the ground. In

the summer of 2009, U.S. forces discovered “days and days and hours and hours” of the drone footage on the laptops of Iraqi insurgents. A $26 piece of software allowed the militants to capture the video.

The lion’s share of U.S. drone missions are flown by Air Force pilots stationed at Creech, a tiny outpost in the barren Nevada desert, 20 miles north of a state prison and adjacent to a one-story casino. In a nondescript building, down a largely unmarked hallway, is a series of rooms, each with a rack of servers and a “ground control station,” or GCS. There, a drone pilot and a sensor operator sit in their flight suits in front of a series of screens. In the pilot’s hand is the joystick, guiding the drone as it soars above Afghanistan, Iraq, or some other battlefield.

Some of the GCSs are classified secret, and used for conventional warzone surveillance duty. The GCSs handling more exotic operations are top secret. None of the remote cockpits are supposed to be connected to the public internet. Which means they are supposed to be largely immune to viruses and other network security threats.

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.

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.

The Air Force declined to comment directly on the virus. “We generally do not discuss specific vulnerabilities, threats, or responses to our computer networks, since that helps people looking to exploit or attack our systems to refine their approach,” says Lt. Col. Tadd Sholtis, a spokesman for Air Combat Command, which oversees the drones and all other Air Force tactical aircraft. “We invest a lot in protecting and monitoring our systems to counter threats and ensure security, which includes a comprehensive response to viruses, worms, and other malware we discover.”

However, insiders say that senior officers at Creech are being briefed daily on the virus.

“It’s getting a lot of attention,” the source says. “But no one’s panicking. Yet.”

http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/
