|  |  |  |
| --- | --- | --- |
|    |  | MEDIA ADVISORY AIR FORCE SPACE COMMANDDirectorate of Public Affairs, 150 Vandenberg St, Suite 1105, Peterson AFB, CO 80914-4500 Phone (719) 554-3731 |

 **FOR IMMEDIATE RELEASE
Release No: 11-10-01**

**Oct. 12, 2011**

**Flying operations of remotely piloted aircraft unaffected by malware**

**PETERSON AIR FORCE BASE, Colo.** – To correct recent reporting, the malware detected on stand-alone systems on Creech Air Force Base, Nev., in September, has not affected Remotely Piloted Aircraft operations.

On 15 September, 24th AF first detected and subsequently notified Creech AFB regarding the malware on their portable hard drives approved for transferring information between systems. It was detected and isolated by the 24th Air Force using standard tools and processes for monitoring and protecting Air Force computer systems and networks. The Air Force then began a forensic process to track the origin of the malware and clean the infected systems.

The malware was detected on a stand-alone mission support network using a Windows-based operating system. The malware in question is a credential stealer, not a keylogger, found routinely on computer networks and is considered more of a nuisance than an operational threat. It is not designed to transmit data or video, nor is it designed to corrupt data, files or programs on the infected computer. Our tools and processes detect this type of malware as soon as it appears on the system, preventing further reach.

The infected computers were part of the ground control system that supports RPA operations. The ground system is separate from the flight control system Air Force pilots use to fly the aircraft remotely; the ability of the RPA pilots to safely fly these aircraft remained secure throughout the incident.

“It’s standard policy not to discuss the operational status of our forces,” said Colonel Kathleen Cook, spokesperson for Air Force Space Command. “However, we felt it important to declassify portions of the information associated with this event to ensure the public understands that the detected and quarantined virus posed no threat to our operational mission and that control of our remotely piloted aircraft was never in question.”

“We continue to strengthen our cyber defenses, using the latest anti-virus software and other methods to protect Air Force resources and assure our ability to execute Air Force missions. Continued education and training of all users will also help reduce the threat of malware to Department of Defense systems.”

For more information contact Air Force Space Command Public Affairs at (719) 554-3731.

-30-