# Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

**September 18, 2013**

## BETA BOT MALWARE BLOCKS USERS ANTI-VIRUS PROGRAMS

The FBI is aware of a new type of malware known as Beta Bot. Cyber criminals use Beta Bot to target financial institutions, e-commerce sites, online payment platforms, and social networking sites to steal sensitive data such as log-in credentials and financial information. Beta Bot blocks computer users' access to security websites and disables anti-virus programs, leaving computers vulnerable to compromise.

Beta Bot infection vectors include an illegitimate but official looking Microsoft Windows message box named "User Account Control" that requests a user's permission to allow the "Windows Command Processor" to modify the user's computer settings. If the user complies with the request, the hackers are able to exfiltrate data from the computer. Beta Bot is also spread via USB thumb drives or online via Skype, where it redirects the user to compromised websites.

*

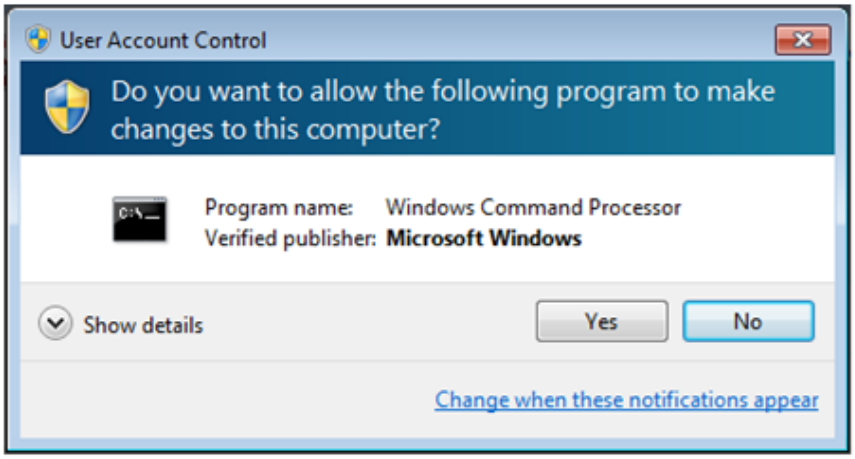


**Figure 1, Beta Bot "Windows Command Process" message box**

Although Beta Box masquerades as the "User Account Control" message box, it is also able to perform modifications to a user's computer. If the above pop-up message or a similar prompt appears on your computer and you did not request it or are not making modifications to your system's configuration, do not authorize "Windows Command Processor" to make any changes.

Remediation strategies for Beta Bot infection include running a full system scan with up-to-date anti-virus software on the infected computer. If Beta Bot blocks access to security sites, download the latest anti-virus updates or a whole new anti-virus program onto an uninfected computer, save it to a USB drive and load and run it on the infected computer. It is advisable to subsequently re-format the USB drive to remove any traces of the malware.

---

*blogs.rsa.com; nbcnews.com

If you have been a victim of an internet scam or have received an e-mail that you believe was an attempted scam, please file a complaint at www.IC3.gov.