Microsoft's Malware Protection Center is reporting that Bohu, a trojan largely confined to China, is able to bypass anti-virus solutions which assess the risk posed by files by querying a server in the cloud. Bohu uses a number of techniques to avoid detection.

According to the report, Bohu appends random data to its own files in order to thwart hash-based detection. Cloud scanners send a file's hash to the cloud server to determine whether information is available for a given file. The random data results in a new hash being generated which the server does not recognise.

Bohu also attempts to block data traffic between anti-virus software and the cloud. It does so by installing a filter via the Windows Sockets Service Provider Interface (Winsock SPI) and an NDIS driver which, according to Microsoft, blocks network traffic and HTTP requests containing specific keywords and server addresses from being uploaded to the server.

Currently, Bohu apparently only tries to block connections to cloud solutions from popular Chinese vendors Kingsoft, Rising and Qihoo. Bohu infects computers by disguising itself as a video codec and once there installs additional files. It's not clear from Microsoft's report and its description of the malware
what, apart from blocking cloud access, Bohu actually does, whether, for example, it steals data or performs some other nefarious function.