Chinese hackers use Dropbox, WordPress attacks Southeast Asia

The Chinese cybercrime gang DNSCalc has added Dropbox and WordPress to the list of malware distribution tools. Their goals are government-related individuals and organizations.

The Chinese cybercrime gang DNSCalc has added Dropbox and WordPress to the list of malware distribution tools. Their goals are government-related individuals and organizations.

In fact, these services have been exploited by them over the past 12 months according to intelligence director *Rich Barger* from *Cyber ??Squared* . This tactic is not new, but it still surpasses most security companies because " *people don't really care about it* ."

According to *PC World* , **DNSCalc** is one of 20 Chinese hacker groups that have been exposed by security firm *Mandiant* to participate in cyber attacks aimed at specific targets to steal information. This time, DNSCalc targets intelligence documents of ASEAN-related government and individual organizations.

They do not take advantage of any security holes of **Dropbox** or **WordPress** . Instead, this group opens accounts for these services and uses them as an infrastructure for attack. A **.zip** file will be uploaded to Dropbox, with fake information belonging to the " *US-ASEAN Business Council* ". Messages will be sent to individuals and

organizations interested in this association's policy.

When the victim **opens the zip file** , there will be another file named " ***2013 US-ASEAN Business Council Statement of Priorities in the US-ASEAN Commercial Relationship Policy Paper.scr"*** . Clicking to open this file will launch another **.pdf** file, while the malware will implicitly open the **backdoor** to the criminal server.

Just that, malicious software will connect to **WordPress blogs** created by hackers. This blog contains the IP address and port number of the server to which the malware will continue to connect to download additional programs.

Dropbox is an ideal platform for attacks by employees of many companies using this cloud storage service. " ***People trust Dropbox,*** " Barger said.

For companies that have put Dropbox on the white list of the security system, malware that moves from Dropbox will not be detected. Also, connecting to WordPress will not be monitored because this is not the usual behavior of employees equipped with an Internet connection.

According to *Cnet* , in general no technology can alone prevent such attacks. The only way to stop it is that security experts share information when their company is in the hacker's sights, thereby strengthening their defense system.