

New malware uses search terms like 'Lost' as bait

May 19 2010, By Wailin Wong

"Lost" fans searching for secrets of the ABC show's final episode may be in store for a nasty surprise: An infected computer.

PandaLabs, a unit of computer company Panda Security, said it has detected a new distribution method for a kind of malware called the MySecurityEngine fake antivirus. This malware and the way it infects a computer are not new, but the bait it uses does change according to current events and popular search terms.

Most recently, the malware has affected searches related to "Lost," which will have its final episode this Sunday. Searches for tidbits about the upcoming series finale or ways to watch the show on streaming video turn up fake websites that appear high up on results pages, PandaLabs said. Anyone who clicks the links will get a prompt to accept a file download, which then installs the malware on the computer.

"What continues to surprise us is the speed with which the numerous websites are created, and then indexed and positioned on the Internet," said Luis Corrons, PandaLabs' technical director. "As the screening of the final episode of 'Lost' approaches, we expect the number of malicious links to double or triple."

PandaLabs said it has also come across other search terms for TV shows and films being exploited for malware, including "Glee," "Family Guy" and "Iron Man 2."

(c) 2010, Chicago Tribune.

Distributed by McClatchy-Tribune Information Services.

Citation: New malware uses search terms like 'Lost' as bait (2010, May 19) retrieved 19 April 2024 from <https://phys.org/news/2010-05-malware-terms-lost-bait.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.