

Trojan worms' hybrid

In the past few months, security circles have witnessed an increase in the number of mutants of worms that can steal data like trojans. According to security firm Panda Security, cybercriminals increasingly favor the 'hybrid' worm when fish

In the past few months, security circles have witnessed an increase in the number of mutants of worms that can steal data like trojans. According to security firm Panda Security, cybercriminals increasingly favor the "hybrid" worm when traditional worms seem to be down.

These "hybrid" worms are designed to steal top-secret information from inferior users.

According to its statistics, hybrid worms accounted for 17.6% of the total malware (malware) in February, slightly up from 15% in January. Meanwhile, the Trojan still stood still. place with 23.7%.



Source: SecurityLabs " The new worm generation is becoming more sophisticated and they behave more and more like the Trojan, " said technical director Luis Carrons of PandaLabs. " Their capabilities are constantly expanding, so deep exploding can be considered an inevitable consequence ."

" In the past, most computer worms were designed to spread from one computer to another. But over the past few months, they have been able to steal data, making it difficult for antivirus tools. distinguish and classify "

According to PandaLabs, the Trojan Downloader.MDW program is the most "active and effective" malware in

February. The Trojan is designed to open the computer door to other malware.

Standing in the second position is the Bagle.RC, while the third place belongs to Lineage.GXD, a worm that only attacks users of Lineage online game.

The 7 "faces" left in the Top 10 include: Bagle.RP worms, Lineage.HJT worms, Perlovga.A worms, Bagle.HX worms, Lineage.HIC worms, Puce.E worms and deep Lineage.HJB.

You finished reading the article "**Trojan worms' hybrid**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.