

Symantec Study: Online Crooks Make Good Money

1,704 Views

[1 Comment](#) [Share](#) [Flag as inappropriate](#)



Featured Author:

DailyTech



DailyTech is a leading online magazine for a well-educated, tech audience. Its readers enjoy hard-hitting and up to the minute CE, PC, IT and information technology news. DailyTech's fast-moving content also reaches out via news syndications, public portals, and forums.

More articles from this author:

- [Vista Fails to Improve on Windows XP's Opening Act](#)
- [HBO and Time Warner Make Viewers an Offer They Can't Refuse](#)
- [In-Flight Wi-Fi Coming to Southwest, American](#)

Jason Mick / DailyTech

November 26, 2008

'One of security's leading firms say that crooks are striking it rich in an underground market and becoming increasing cohesive.' -

You hear about it on the news every day—criminals and profiteers have made the internet into a war zone. From [bank intrusions](#), to assaults by massive botnets, to [coordinated attacks by foreign nationalists](#), there seems to be no end in sight to cybercrime.

Indeed, the internet, according to Symantec, is becoming the high-crime district of the next century as hackers find themselves part of a [thriving market](#) with little fear of serious repercussions if they play it by the book.

The Symantec Report on the Internet Underground Economy, to be released today, details the hale and hearty internet black market. A keystroke logger might run you \$23, a host for your phishing scheme \$10. If you [want a botnet](#), it will cost you \$225. Want a tool to crack bank security using a known vulnerability? It will cost an average of \$740, and could cost you as much as \$3,000 for a good one. However, for both the buyer and the seller, the reward for online crime is proving to be equally lucrative, according to Symantec's report.

For over a year, from July 1, 2007 to June 30, 2008, Symantec monitored cybercriminals on IRC channels and internet forums. Through the extensive research, they generated one of the most cohesive pictures of the modern state of internet crime, including the tools used, the average prices, and even the flow of stolen financial information.

Credit card information was the most commonly requested good or service, accounting for approximately 30 percent of sales. Bank account credentials were a hot seller, priced anywhere from \$10 to \$1,000 depending on the amount of money in the account and where it was located.

Apparently cybercrime does pay; Symantec found that sellers' total goods had a combined sales price of around \$275M USD. Adding in the extra income from emptying victims' accounts and maxing their credit cards, this total could soar to a \$7B USD business.

Aside from tracking hackers and cyberthieves, the study also tracked another form of illicit internet activity – [software piracy](#). The study tracked sales of pirated software between July and December. The most commonly pirated type of software was desktop games, followed by utility applications and then multimedia software, such as photo editors, 3D animation, and HTML editors.

It appears that people within the U.S. are making most of the money off the sale of pirated software. Of the underground sales, 41 percent were uploaded by people within the U.S., with [Romania a distant second](#) with 13 percent. North America had by far the largest underground economy of servers.

One intriguing trend that Symantec noted was the rise of cybergangs in Russia and Eastern Europe. These gangs typically consist of acquaintances met online and in IRC chats and were much more coherent and aggressive than their western counterparts. For this reason Russia has often been cited as a haven for illegal internet activity.