

The Underground Digital Economy

By Dean Turner

Driven by the promise of big profits, cybercriminals have built the foundation of an underground digital economy.

Driven by the promise of big profits, cybercriminals have built the foundation of an underground digital economy that can turn anything from stolen credit card data to email cookies into cash with little more than a few mouse clicks. Selling this kind of personal information has been facilitated by enterprising criminals who have developed an entire underground network.

According to Symantec's latest *Internet Security Threat Report*,¹ a credit card from a United States-based bank goes for between US\$1 and US\$6, while a full identity – including U.S. bank account information, credit card data, date of birth, mother's maiden name, and social security number – can be purchased for US\$14 to US\$18. This thriving underground market enables criminals to buy, sell, and trade bundles of contraband in a community of highly organized and efficient crime rings. It may take a lot of stolen identities to make a person wealthy which is why today's cybercriminals cast such big nets.

But not all stolen data pays the same. For example, credit cards in the United States are generally advertised for about half as much as those from the United Kingdom. This may simply be the result of supply-and-demand since more cards from the United States are available for sale. Or, it could be because the UK pound is currently stronger than the dollar. Then again, a list of 29,000 emails will net a cybercriminal just US\$5; but a verified PayPal account with a balance can bring in as much as US\$500.

This illegal activity is also extremely sophisticated and competitive. Cybercriminals outfit their servers with encryption to make them less visible, and so-called "bot herders" take down competitors' servers in an effort to consolidate their networks and ease management while expanding their reach. This digital underground marketplace is teeming with activ-

ity as cybercriminals leverage increasingly elaborate tools and techniques to steal information for financial gain. Similar to malicious Web sites, these rings are in a constant state of flux, making it difficult for law enforcement to find them and prevent this activity from taking place.

Serving up crime

It is the "land of opportunity" for cybercriminals who continue to target the United States – both as a place for launching their criminal activities as well as for reaching a larger pool of potential victims. For example, many of the underground economy servers in these rings are located in the U.S. and are used by criminals and criminal organizations to sell stolen information, typically for subsequent use in identity theft. 51 percent of the underground economy servers monitored throughout the world during the last half of 2006 were in the United States. This comes as no surprise to Internet watchers, since the United States has a larger Internet infrastructure and more broadband use than any other country in the world – the two primary elements that create a wealth of opportunities for criminals to carry out their malicious activities. In fact, the report also found that the United States accounts for 19 percent of the world's Internet users and, as of June 2006, had more than 57 million broadband Internet users.

The United States is also home to 40 percent of the world's bot command-and-control servers, the highest percentage of any country. These are computers that botnet owners use to relay commands and instructions to the bot-infected computers that make up their botnets. This high proportion of command-and-control servers in the United States likely indicates that servers in this country control not only botnets within the country but offshore as well.

However, while the number of bot-infected computers increased by 29 percent, the number of command-and-con-



¹ Figures throughout are cited from Symantec's Internet Security Threat Report – <http://www.symantec.com/enterprise/theme.jsp?themeid=threatreport>

trol servers worldwide decreased by 25 percent due to botnet owners consolidating their networks and increasing the size of their existing networks. To that end they launch denial of service attacks and push their rivals' networks out of business. Or they steal their competitors' bots and, in turn, expand their own botnet franchises.

Exploits and malware

So, how do these cybercriminals get such information in the first place? You name it. They use phishing attacks, keystroke loggers, Trojan horses, worms, spam, spyware, and more as well as new and noxious combinations of all such malware – anything that will help them compromise systems and get at valuable information.

Staged downloaders are just one example. Sometimes referred to as modular malicious code, a staged downloader is a specialized Trojan horse that downloads and installs other malicious programs such as a backdoor or worm. A worrisome 75 percent of the volume of the top 50 malicious codes reported to Symantec contained a modular component such as this.

Cybercriminals are also exploiting more zero-day vulnerabilities – software flaws for which a patch has not yet been released. Twelve zero-day vulnerabilities were documented in the last half of 2006 compared to just one found in the previous two reporting periods. And, five of the 12 zero-day

vulnerabilities released in the second half of last year targeted Microsoft Office. Why? Because PowerPoint presentations, Word documents, Excel spreadsheets and the like are rarely blocked by security software and nearly always opened by their recipients.

Bottom line

Clearly, cybercrime has become a legitimate concern for anyone who uses the Internet. With cybercriminals using increasingly sophisticated methods for gaining access to private information, supported by a thriving underground economy, the need for applying aggressive countermeasures has never been more important. In the face of this malicious new ecosystem, consumers, businesses, academic institutions, and even government agencies will have to collectively raise the bar in protecting our digital assets, make security a higher priority, and take back some cyberturf.

About the Author

As Security Manager for Symantec Security Response, Dean Turner's primary role is as the Executive Editor of the Internet Security Threat Report. Turner coordinates the research and analysis of attack data gathered from Symantec's Deep-Sight Threat Management System, Managed Security Services, Business Intelligence Services and Symantec Antivirus Research Automation for use in the publication of the ISTR. He can be reached at dean_turner@symantec.com.