Security Spotlight
July 12, 2010

Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

EMERGING MALWARE BUSINESS PLATFORMS

Leveraging the ever-growing number of Web 2.0 and computing platforms to facilitate their operations, today's generation of cybercriminals have been selling do-it-yourself (DIY) malware tool kits to reel in more victims and, hence, more profit. In the past few months, TrendLabs engineers have seen and documented their findings on this development and featured some of them in this article.

Malware for Sale

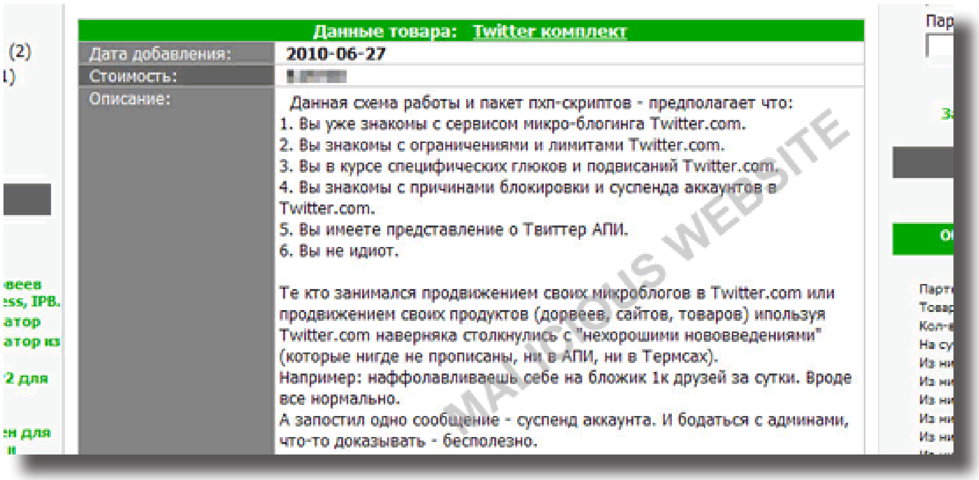
Today, malware development has become so profitable that it can be likened to legitimate commercial software development.

Today, malware development has become so profitable that it can be likened to legitimate commercial software development. Malware developers are now serious businesses complete with marketing, advertising, software development, and even after-sales support groups.

Cybercriminals are always on the lookout for ways to exploit vulnerabilities in the global payment system. But now more than ever, they are formulating more direct tactics to be able to sneak their malicious activities into our normal day-to-day transactions and to obtain quicker access to cash.

Competition for a large amount of profit in the cybercrime market also paved the way for cybercriminals to develop more sophisticated malware applications that provide a wide range of functionality and that require little or no expertise to use. DIY malware construction kits, for instance, allow even new cybercriminals to produce their own malicious programs according to what they want their programs to do.

The recently discovered *Twitter Kit*, for example, is a new tool that cybercriminals can use to send *Twitter* spam to thousands of affected users' followers. It is especially useful in search engine optimization (SEO) projects, among the other features that it offers to its buyers. It is being promoted in underground forums for only US$20, making it easily available to virtually anyone who is interested, other cybercriminals included.



Данные товара: Twitter комплект

Дата добавления:	2010-06-27
Стоимость:	[redacted]
Описание:	Данная схема работы и пакет пхп-скриптов - предполагает что: 1. Вы уже знакомы с сервисом микро-блогинга Twitter.com. 2. Вы знакомы с ограничениями и лимитами Twitter.com. 3. Вы в курсе специфических глюков и подвисаний Twitter.com. 4. Вы знакомы с причинами блокировки и суспенда аккаунтов в Twitter.com. 5. Вы имеете представление о Твиттер АПИ. 6. Вы не идиот. Те кто занимался продвижением своих микроблогов в Twitter.com или продвижением своих продуктов (дорвеев, сайтов, товаров) ипользуя Twitter.com наверняка столкнулись с "нехорошими нововведениями" (которые нигде не прописаны, ни в АПИ, ни в Термсах). Например: наффолавливаешь себе на бложик 1к друзей за сутки. Вроде все нормально. А запостил одно сообщение - суспенд аккаунта. И бодаться с админами, что-то доказывать - бесполезно.

Figure 1. *Sample post advertising the* Twitter Kit

Social Networking as an Advertising Platform

Just as social media have proven to be an effective marketing tool for businesses, social networking has also become a common avenue for cybercriminals to proliferate their malicious creations due to its popularity. Its continuous growth in terms of population and usage has made it a good means for cybercriminals to post fake ads, to launch malware attacks, and to gather useful information from users.

One recent example is an ad for a distributed denial-of-service (DDoS) tool in the popular media-sharing site, *YouTube*. In this attack, the seller posted a video showing the features of and details on how to purchase the said DDoS tool.

Just as social media have proven to be an effective marketing tool for businesses, social networking has also become a common avenue for cybercriminals to proliferate their malicious creations due to its popularity.

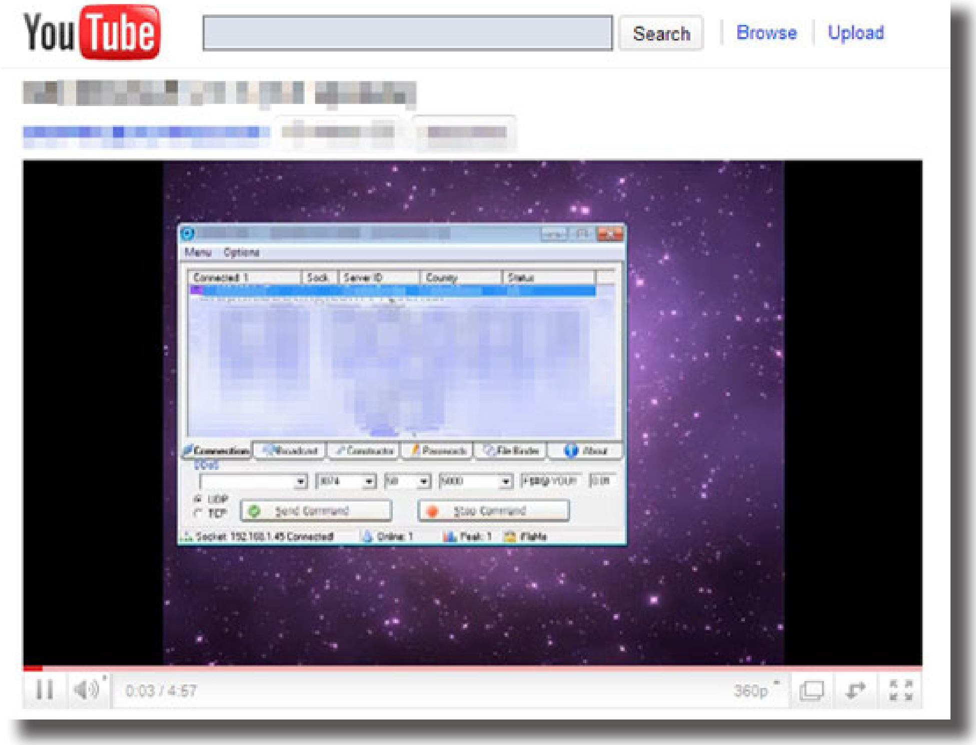


Figure 2. YouTube *video advertising a DDoS tool*

While most ads can be found in underground forums, this *YouTube* post is just one of the many malware ads that cybercriminals put up on social media sites. This goes to show that cybercriminals are using social networks the same way legitimate businesses do in order to gain "customers," to sell products, and to profit from selling malicious software.

From Software to Hardware

Not only do cybercriminals create and sell malicious programs to facilitate threat attacks. Because hardware have become so cheap, they are now also delving into reproducing machines that will help them more easily and directly steal information from their victims.

Last June, security researchers discovered a post in an underground forum about a rigged point-of-sale (POS) device with flash memory up for sale. Though it seems like any normal POS terminal, this fake device can be used to steal data from credit and debit cards. During transactions, it falsely claims that it encountered an error while it collects and saves data held in the card's magnetic strip, including the victim's personal identification number (PIN).

Because hardware have become so cheap, they are now also delving into reproducing machines that will help them more easily and directly steal information from their victims.

In most cases, users will dismiss this as a normal failed transaction. But what they don't know is that their information has already been stolen in the background. This device sells for EUR 1,000 in the underground market with an additional EUR 200 for setup and delivery charges.

The Free Enterprise

Not all malicious programs are, however, sold for profit. Some cybercriminals instead dedicate their efforts to rapidly creating malware tool kits that can be distributed for free.

One example of this is the *Twitter Bot Builder,* which has the ability to attack users' systems by launching DDoS attacks and by downloading other malicious files onto victims' systems. The program can be used to build an executable file that connects to *Twitter.com* and to execute commands based on a user's Tweets.

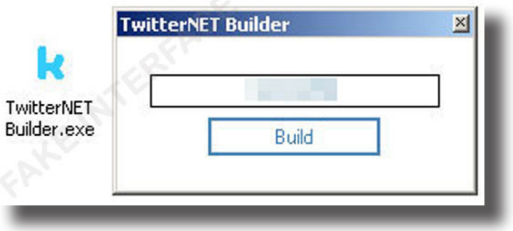


Figure 3. Twitter Bot Builder *icon and executable file*

The said bot builder is being freely distributed on the Internet and can be manually installed by an attacker onto a system. A cybercriminal can also trick a user into executing the malicious file.

The Booming Underground Economy

There is no doubt that today's underground economy is booming due to an increase in malware sales and the availability of malicious services. With attacks coming in various channels, it seems that the malware business will continue to gain momentum through the growth and increasing sophistication of cybercriminal activities.

There is no doubt that today's underground economy is booming due to an increase in malware sales and the availability of malicious services.

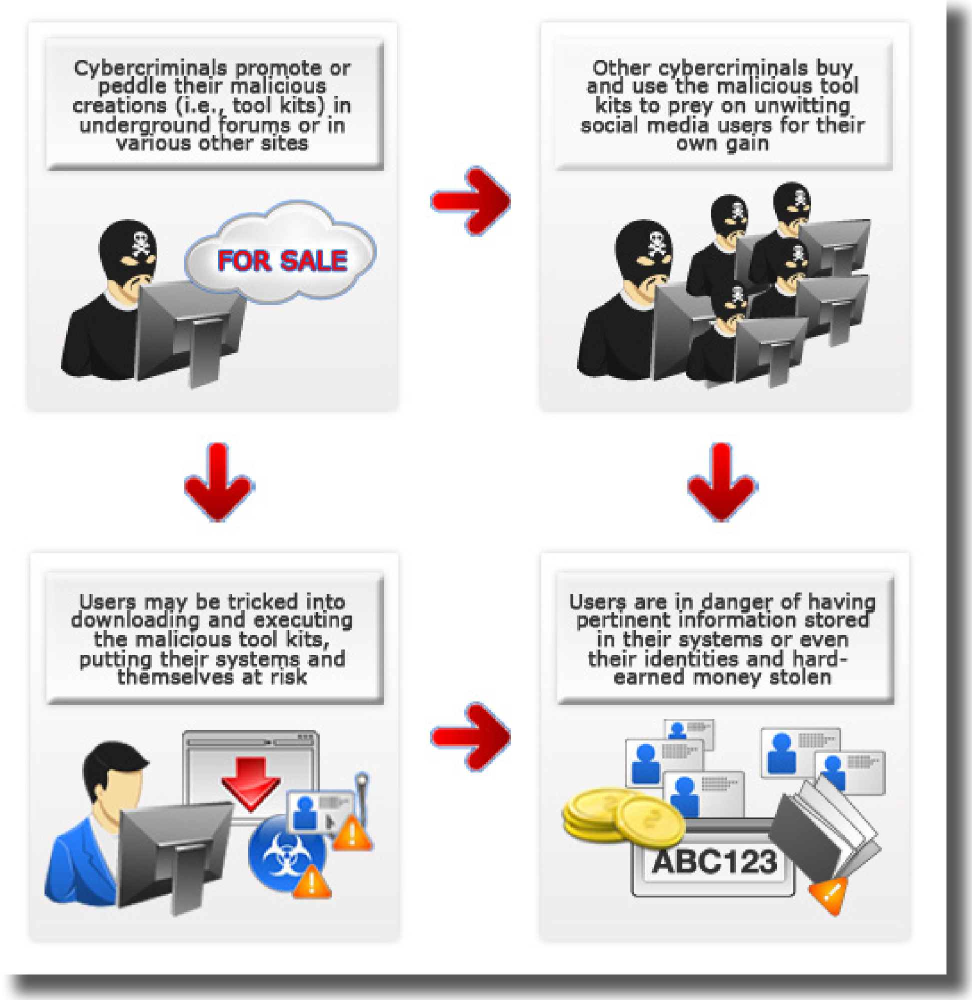

Cybercriminals promote or peddle their malicious creations (i.e., tool kits) in underground forums or in various other sites
FOR SALE
Other cybercriminals buy and use the malicious tool kits to prey on unwitting social media users for their own gain
Users may be tricked into downloading and executing the malicious tool kits, putting their systems and themselves at risk
Users are in danger of having pertinent information stored in their systems or even their identities and hard-earned money stolen
ABC123

Figure 4. *How the sale and use of malicious tool kits can affect users*

Today, anyone can find whatever he/she is looking for in the underground market. Through the use of tool kits, there is no longer even a need for technical background to get into information theft and cybercrime, thus creating more opportunities for malicious users to spread their malware badness.

With attacks coming in different forms and from many different channels, we can say that the malware industry has truly found its way into integrating their activities into people's daily lives. Users should, therefore, be aware and gain a better understanding of how organized cybercrime works. This way, they have a better chance of mitigating risks and of recognizing and preventing attacks before they even happen and do some serious damage.

References:

- JM Hipolito. (June 28, 2010). *TrendLabs Malware Blog.* "Malware Sales Through Social Networks." http://blog.trendmicro.com/malware-advertising-through-social-media/ (Retrieved July 2010).

- Karl Dominguez. (May 13, 2010). *TrendLabs Malware Blog.* "Your Tweet Is My Command." http://blog.trendmicro.com/your-tweet-is-my-command/ (Retrieved July 2010).

- Maxim Goncharov. (July 4, 2010). *TrendLabs Malware Blog. "Twitter Kit* Out to Make *Twitter* a Spammer's Dream." http://blog.trendmicro.com/twitter-kit-out-to-make-twitter-a-spammers%E2%80%99-dream/ (Retrieved July 2010).

- Maxim Goncharov. (June 23, 2010). *TrendLabs Malware Blog.* "For Sale: Fake POS Devices." http://blog.trendmicro.com/for-sale-fake-pos-devices/ (Retrieved July 2010).

- Rik Van Luvender. (April 2010). "Fraud Trends in 2010: Top Threats from a Growing Underground Economy." http://www.firstdata.com/downloads/thought-leadership/fraudtrends2010_wp.pdf (Retrieved July 2010).

- Steven Bucci. (June 24, 2010). *Adfero Group.* "Cybercrime Continues to Grow Out of Control." http://securitydebrief.adfero.com/2010/06/24/cyber-crime-continues-to-grow-out-of-control/ (Retrieved July 2010).

- The Nielsen Company. (June 15, 2010). *NielsenWire.* "Social Networks/Blogs Now Account for One in Every Four-and-a-Half Minutes Online." http://blog.nielsen.com/nielsenwire/online_mobile/social-media-accounts-for-22-percent-of-time-online/ (Retrieved July 2010).

- Trend Micro Incorporated. (December 2009). *TrendWatch.* "The Future of Threats and Threat Technologies: How the Landscape Is Changing." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/trend_micro_2010_future_threat_report_final.pdf (Retrieved July 2010).