

Welcome to 2007: the year of professional organized malware development

Increasingly, we are drifting away from the chaotic distribution of new malware (malicious software). The distribution of new malware has become highly organized and will continue to be so. The “Detect and Forget” times of Antivirus programs belong to the past. This is relevant, at least, for most of recent new malware.

Malware writers have noticed that they can gain large amounts of money from distributing malware. This is a completely different situation from a few years ago, when malware authors wrote malware to gain acceptance and “fame” within a small group of other virus writers, says Michael St. Neitzel, Technical Spokesman and Senior Antivirus Architect for F-PROT Antivirus.

Malware writers try to keep the malware up and running, since the longer the malware is running, the more money they are likely to receive. This causes the first problem for the antivirus industry: the new generation of malware writers, test their creations constantly and make changes enabling them to bypass existing antivirus detections. Some individuals gain more than \$25,000 a month, which is equivalent to the salary that a senior manager in a large corporation receives. Most of these people, when releasing their malware, have nothing to lose. Also, they are aware that it is difficult to track their activities down in certain regions, for example Asia.

Malware writers have also learned that it is much safer for them not to use stolen credit card numbers themselves, but to sell the numbers to others instead, for a small amount of money. Such activities take place most of the time in irc channels, or closed private forums. Michael registered himself, undercover, in an account, in such a forum, where announcements take place for such trading activities of selling stolen credit card numbers. The date and time for the trading is announced, together with access data to join the trading channel.

The forum itself, of course, is concerned about it’s “good” name; people who question the activities of the forum, face the following answer from the site administrator:

“Iceman is gone. I am now the Administrator of Cardersmarket.com If anyone has any questions contact me or one of the Mods. I don’t want to read any more drama on this site or there will be a massive DDOS against it. No more kiddie games.”

There is the possibility for a reasonable income if a malware writer has, for example, obtained the numbers for 1000 credit cards. If it is assumed that not every credit card is working or maybe close to the credit limit, it can be estimated that it is possible to obtain on average, \$190 US per card. This amounts to US\$ 190,000, which is an excellent return on investment, considering that the data costs up to a few hundred dollars. All that is needed, is a temporary bank account and a credit card machine attached to it. You do not even need to have the cards in your hand, the data is entered via the keyboard of the credit card machine.

Modern malware allows several different ways to obtain money from an infected machine, so if one method does not work, writers simply try another. If it is not possible to steal passwords or credit card data, then the machine is at least used for sending spam or as a proxy gateway. In this way, the malware writers are anonymous,

when using other people's machines for fraudulent transactions, since they can remove all trace of themselves from the machine. Also, the physical location of the machine is in no way associated with where they live.

Another trend which is rapidly increasing, is the selling of virtual money, so called in-game currency, for real money. Players in the computer game, World of Warcraft, need gold to buy equipment for their character. 1000 World of Warcraft Gold sells for about \$39 US. There is always a market for the gold, since some people do not have the time to spend hours for collecting gold during gameplay. The password stealers for such online games significantly outnumber the game serial stealers from other games. The reason for this, is that there are so called Goldseller Companies which not only sell gold, but also buy gold for real money from other players so that they can resell it later, in a professional way, for profit. This motivates hobby hackers to create their own keylogging software to gain some extra money. Once a person has access to the playing character, the Gold can be sent via the in-game e-mail to themselves. In most cases, the hackers create a temporary account. Later, they simply delete the account once successful transactions have been made.

Recently, we have seen many so called "plugins" for World of Warcraft. The plugins contain a backdoor, particularly for the latest game patches from Blizzard, the producer of World of Warcraft, after almost all other regular plugins stopped working. This was the chance for criminals to advertise "working" plugins for this new version which contained malicious code.

The current situation is almost the same in every antivirus company. Significant manpower resources are required in the virus laboratories (viruslab) to keep up with current threats. "Our Viruslab is on 24/7 alert and presently the department staff barely sleep, due to the constant attacks" said Michael St. Neitzel. "Our improved state-of-the art heuristics helps significantly to stop nightly outbreaks, but following this we have to add such threats anyway as a virus signature file with a correct name and description. The times have changed when working in a viruslab was considered to be something special. It has turned into employees becoming irritated and employee-zombie-behavior, due to the need for continuously adding samples at midnight. An emergency team at night is almost not enough anymore. It is necessary to have a fully manned Viruslab around the clock, in order to ensure that you provide as fast as possible, the necessary protection. There is no end in sight as long as criminals are gaining money out of threats. You can add millions of signatures, but you will never manage to solve the real problem: To stop the virus-writer from what he's doing."

"We have to find another way of solving this, than only detecting malware. We, the antivirus industry need go into the offensive, if needed with our own headhunter team for tracing and tracking professional malware writers. If we have only official government and police working on this, it takes too long for them to research this. The best solution would be a cooperation, between various teams of different antivirus companies providing all the required information, working closely with the law enforcement agencies." says Michael St. Neitzel.

Michael St. Neitzel is the Technical Spokesman for FRISK Software, a globally focused computer security company and a leader in antivirus product development and research. FRISK Software produces the popular F-PROT Antivirus product range. More information on www.f-prot.com

