

## Exploring the boundaries of IT security

Whenever we enter a new decade, many of us like to take stock and think about the things that have changed over the last ten years and what may happen during the next twelve months. But as Niels Bohr once said, prediction is difficult, especially about the future. Nevertheless, almost all network security companies try to assess risk and the potential impact of criminal behaviour, fraud and Internet malware for their clients.

This is necessary to stay ahead in the development of efficient countermeasures to match the creativity of cyber-criminals and fraudsters. The problem is that each time the number of variables change, and by that I am referring to the new emerging communication platforms, the number of attack vectors and the exposure to computer malware increase dramatically.

### So what should we expect from the next year anyway?

Our research has shown that BotNets have been acquiring new computers continuously during 2009 and the criminal activities of renting these services is flourishing. But as in any economy, either legal or underground, once the market becomes saturated the competition becomes even more intense.

So we can expect BotNet owners will have to provide demonstrations of power in order to prove that their services are exactly as advertised. This can be done with DDOS attacks to different targets chosen by their prospective client. Also the competition might take the form of malware that would first strip the computer of any competitors' malware before infecting the computer and joining it in the BotNet.

Another area of concern is social media. Will we see more menaces lurking on these platforms? Take for example, a successful fraudster, already achieving a significant income from spamming activities. Equipped with basic knowledge about computer security and software development, he is presented with a tempting environment where people are encouraged to make as many friends online as possible, to interact, share content and pop into conversations whenever it suits them.

We are therefore facing a rather interesting situation since, on one hand you see that millions and millions of people are joining social media websites and want to start sharing links, pictures and other media content, while on the other hand if you take a look at the code provided to interact with the network, you will see how easy it is to develop applications or manipulate different profiles. How can a fraudster resist such temptation?

### Will mobile phones be targeted in the following year?

Nowadays everyone has a mobile phone, and some even more than one. When changing their handset many people are inclined to upgrade to a smart phone, which means that more and more people will have some miniature PCs in their pockets.

With most phones now having a wireless connection, this makes them a very tempting target for the malware writer, even though they aren't capable of processing large amounts of data or broadcasting spam messages. However fraudsters are very adaptable and we are seeing a trend towards the new tactic of 'steal smaller amounts from time to time, rather than all at once'; so perhaps this will become more common in future.

Targeting smart phones is the next logical step, since most users have their phones synchronised with their computers to allow better access to email, contacts and work documents. This opens up the possibility for an attacker to infect both the smart phone and the computer at the same time.

Fake/rogue antivirus products are likely to be a continuing nuisance during 2010. Whilst all Internet security vendors advocate having a security solution installed, this advice is also being copied by the fraudsters. Their tactics include 'warnings' to their potential victims that they are already infected.

This bogus warning is usually accompanied by an offer to provide disinfection for a small fee. They promote their product by claiming to offer the fastest and best solution on the market. Unfortunately this deception often works, as users are becoming increasingly aware of the need for protection, and have not yet taken any action. As a result they may be inclined to accept this 'helpful' prompt?

## Exploring the boundaries of IT security continued...

Some fraudulent vendors even provide their victims with an invoice and a customer support number to call if the victims have any issues with the product. Should the victim call, they follow through with the deceit, by providing somebody to answer and help complete the installation.

Some observers are predicting that there will be a decrease of e-mail spam, now that more people are using social networking for casual communications.

I am not convinced that this will happen. There is no motive for fraudsters to change their tactics now when they are really good at sending email spam. As long as there is email, there is going to be spam. It is true, that some types of spam will move to social media, like porn spam, while others will expand on various platforms, but regrettably spam is here to stay.

Finally, the new wave of social media poses a series of questions. What are the drivers for this behaviour? Is it our desire to own a piece of virtual world, where we can describe who we are, how do we live our lives, who are our friends and family and post our thoughts? Is this intended to be a depository for experiences that will remain for a long time; even after the authors have passed away?

So, besides the advantage of having a bit of immortality, what possible benefits do these social websites have to offer?

Well, from the point of view of a BotNet owner and his IT collaborators, there is the opportunity to add a personal touch to their phishing emails by reading every social network page concerning the individual being targeted and using this 'intelligence' to craft some form of personalised message.

But this will take a lot of time, and....there is also the possibility of targeting an empty account. Then again, what if infected computers around the world would do the exact same thing automatically? Wouldn't this increase significantly the chances of making the fraudulent e-mails look more credible?

Drawing on the military adage; "hope for the best but plan for the worst", there are clear lessons for the network and computer security companies. Whilst nobody relishes the prospect of such menaces, described above, we must continue our work to deal with these risks and make the Internet as safe as possible for all honourable users.



Alexandru Catalin COSOI  
Senior AntiSpam and AntiPhishing Researcher  
eMail: [acosoi@bitdefender.com](mailto:acosoi@bitdefender.com)  
Work Phone: +40 723 399 778  
Personal Phone: +40 742 586 994  
Web: [www.bitdefender.com](http://www.bitdefender.com)