

## Non-OS-dependant malware



All too often people talk about the disadvantages of the Windows operating system: it has too many security flaws, it is not properly patched, it is not security oriented... Until the much talked about Vista system finally reaches our computers, there will still be plenty of time to protest.

However, with the new malware dynamic, the idea that malware is restricted to specific operating systems is becoming anachronistic. It no longer matters whether the victim is a home-user or a company employee. It is now irrelevant whether the system administrator is just someone who lives round the corner or a highly qualified IT manager.

Where some years ago malicious code was designed to multiply rapidly and, in many cases, damage computers, nowadays this modus operandi has all but disappeared. The prime objective nowadays is users' money and you don't need to be an expert programmer to do this, you simply need to be sufficiently malicious to con people out of their savings.

Let's take a look at some of the techniques used in order to trick users. One thing you will notice is that none of them depend on the type of operating system, browser or mail client. They depend, solely and exclusively, on the user.

If we start with the most infamous, then surely we must be talking about the "Nigerian letter" or "419" scam. In these scams, the intended victim is contacted by someone claiming to have inherited large sums of money from a businessman, general or president in an African country and, surprisingly enough, the money is blocked in a bank account. Victims who volunteer to help release the money will find themselves paying endless commissions and advances until boredom or bankruptcy bring it all to an end.

Less well-known, although no less common, are the messages announcing incredible and unexpected lottery wins. The messages purport to have been sent by genuine lottery organizations and needless to say, the prizes announced can reach millions of euros. To receive the prize, all you have to do is call the lottery agent mentioned in the message. He'll supposedly make sure you get the prize. First of course, you will have to pay a series of commissions, exactly as many as it takes you to realize you are the victim of fraud.

Who hasn't received an email message offering better mortgage terms? Such messages are normally false, and simply aim to get the recipient to call the phone number that appears in the text. The trick here is that there are micro-companies who have agreements with the telephone operators

## Non-OS-dependant malware



to earn money from all calls made to these numbers, in addition to premium-rate or toll numbers.

Phishing could also now be considered a 'classic' attack. These email messages simulate those sent by banks, and ask users to confirm their login or credit card details. These messages are becoming increasingly dangerous. Whereas previously the scam relied on spoof web pages which sooner or later would be shut down, now HTML messages have appeared with fields in which users are asked to enter their data directly. In this way the information will be sent directly to the cyber-crook.

These phishing messages don't just use banks, they frequently spoof emails from other money-related services, such as PayPal or e-Bay. The procedure is always the same: a message requesting data on the threat of closing users' accounts.

However, phishing is becoming too well-known and fraudsters are seeing their potential market drastically reduced. For this reason, other, more subtle, techniques are being used. Messages have been detected in which the sender claims to have bought something on eBay and is complaining because he has paid for an item which he has not received. If the user falls for this scam, in order to reply to the sender he will have to enter his eBay user details, which will automatically fall into the hands of the fraudster.

All these scams have something in common: they need a middleman to receive the money from the unsuspecting victims. And what better way of recruiting than an email advertising a great job that simply requires receiving money in your bank account and forwarding it to third parties. Quick and simple. But the transfers received are directly from the bank accounts of victims of the scams mentioned above, and the money is forwarded directly to the fraudsters. The middlemen in these cases are known as 'mules', just like those used to smuggle drugs across borders.

In all these cases it is clear that we are talking about theft, fraud or whatever you want to call it. Users are tricked and their money, data or both are stolen. Things are becoming more subtle however. Now there are messages advising people to buy certain stocks, as, it is claimed, the price is about to rise.

In this case, this is not fraud. There is no theft. Just the naivety of users. Those producing these messages know perfectly well that there is no reason why the stock price should increase, they are simply hoping to push up the price in order to sell their own stocks.

## Non-OS-dependant malware



Fortunately, stocks named in these messages have not witnessed any spectacular increases, although trading in these companies has become busier for a few days. Although the senders of the message make no great profits, they manage to sell some stocks that they probably wanted to get rid of.

And so, with all that said, which of these scams is dependent on the user's operating system? Any email client will display these messages. It doesn't matter whether you have the latest Windows update or whether your Linux system is properly configured or not. It depends solely and exclusively on users clicking on the message; on their gullibility and naivety.

If we really want users on a corporate network to be protected from the latest threats, the solution does not depend on the operating system or patches applied. Protection depends, on the one hand, on user training and on the other, on the protection systems installed. Protection systems, both perimeter and those in workstations and servers, both for Windows and for Linux, must establish a genuine barrier to prevent these types of scams and threats. It is not enough to trust the operating system or users. One will probably do little and the other will probably do the wrong thing.

The classic solution in Linux systems, assigning different privileges to prevent executing malicious programs on systems, may suppose a slight limitation to these types of threats. But the problem does not lie in executable code, but in fraudulent information reaching the user.

The solution, as always, involves security suites that include all the features needed to protect users in a single application: from the classic antivirus to firewalls, or e-mail protection both for Windows and Linux. In this way we can keep users safe as well as their computers.

**Fernando de la Cuadra**  
**International Technical Editor**  
Panda Software (<http://www.pandasoftware.com>)  
E-mail: [Fdelacuadra@pandasoftware.com](mailto:Fdelacuadra@pandasoftware.com)