OPINION

MISGUIDED OR MALEVOLENT? NEW TRENDS IN VIRUS WRITING

Stuart Taylor
Sophos Plc, UK

Recently there have been several reports circulating reviewing the virus scene. Most of these have been looking back at the trends seen in 2003: what types of viruses have been prevalent, when they were prevalent and what platforms have been most affected – no prizes for guessing that *Windows* has taken the brunt of attacks.

One question that keeps coming back to me is ‘Who writes viruses?’. There have been many caricatures of virus writers, some accurate and some not. Are they young or old? Are they ‘nerds’ or professionals? Are they script kiddies or serious writers of metamorphic creations? Are they all men or are there females writing these things? In truth, I suspect that all of the above are true to some extent. However, I think that we may be experiencing a new trend in virus writing.

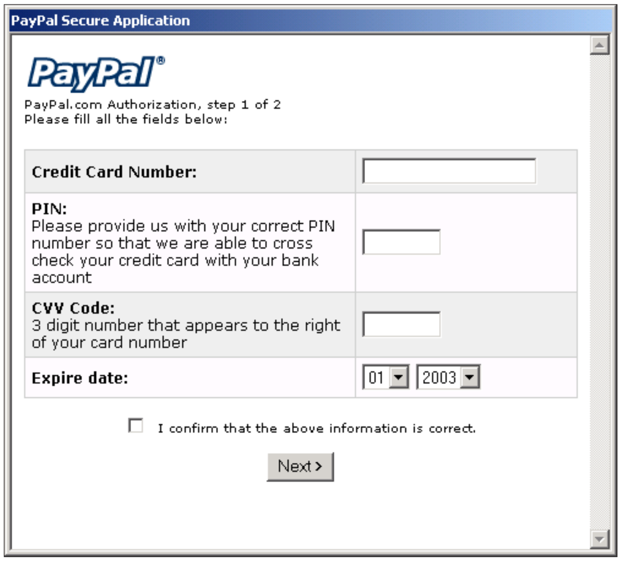
THEFT OF CREDIT CARD DETAILS

In September 2002, a virus writer unleashed the worm W32/Bugbear.A on the world. I recall that *Sophos* released an IDE promptly and we thought nothing more of it. Two days later, however, the media latched onto the idea that the worm could steal credit card details and our support department was flooded with requests for information from users who were worried they might have given away vital information. This was probably the first worm to hit the mainstream media with the concern of theft of credit card information.

In November 2003, I spoke at a two-day conference in the UK on Cyber Fraud. On both days of the conference I awoke to the news from *Sophos* that the company’s virus lab in Sydney had alerted overnight on a new worm that threatened to steal credit card details directly.

The first worm was W32/Mimail.I. This worm attempted to steal credit card details by putting up a fake *PayPal* pop-up which requested credit card information from the recipient, stating that the recipient’s *PayPal* account had expired. *PayPal* is a well-known method of performing a secure transaction on the Internet – this social engineering had been well thought through. A clever trick of W32/Mimail.I was to ask for the CVV (card verification value) code from the back of the credit card.

Clearly some people would have been surprised by the appearance of a pop-up requesting this information and would have exercised caution. The following day the variant W32/Mimail.J attempted to overcome this obstacle by creating a dummy web page on the local disk and bringing up the user’s web browser to view the page, thus giving the recipient the impression of having been taken to a legitimate website.



PayPal.com Authorization, step 1 of 2
Please fill all the fields below:

Credit Card Number:	
PIN: Please provide us with your correct PIN number so that we are able to cross check your credit card with your bank account	
CVV Code: 3 digit number that appears to the right of your card number	
Expire date:	01 ▾ 2003 ▾

□ I confirm that the above information is correct.

W32/Mimail.I produced a fake PayPal pop-up requesting credit card information – even asking for the CVV code from the back of the credit card. Note the misspelling of ‘Expiry date’.

W32/Mimail.J had one more trick up its sleeve, requesting the user’s mother’s maiden name – a favoured security check of most banks. However, at this point the virus writer asked for one piece of information too many – it asked for the user’s Social Security number. This information is very country-specific. The USA and Australia, for instance, both use the term ‘Social Security number’, but other countries use different expressions, such as ‘National Insurance number’ in the UK.

WHO ARE THE WRITERS?

So, who is writing these worms and viruses? Is it still the person who claims to want to expose the flaws in *Microsoft*’s products, or the person who does it just because they can, or the person who wants to convey a political message? Whilst such people are clearly still in the business of writing viruses there is a definite hint that the criminal element of society may be becoming involved with the express purpose of perpetrating fraud.

In his article in last month’s Virus Bulletin (see *VB* January 2004, p.14), Jamz Yaneza concluded that virus writers were moving away from destructive payloads, presumably to allow their creations to spread further before being detected.

I agree with this – we have seen very few worms recently that have been destructive.

Recently we had the mass mailing of Troj/Antikl-Dam. The actual functionality of the attached code is still a mystery as the attachment was harmless, having been truncated to leave no code inside.

The Trojan was seeded via an email containing the following text:

```
Dear customer,
The security of your personal and account information
is extremely important to us. By practicing good
security habits, you can help us ensure that your
private information is protected. Please install our
special software, that will remove all the keyloggers
and backdoors from your computer.
And will help us to prevent credit card fraud in
future.
Thank you.

Best regards,

<name>
```

The <name> in this case was the name of a banking institution, and the emails were sent with a selection of return addresses of various banks, one of which was the Bank of England.

According to news reports on the day, the Bank of England received in excess of 100,000 reports, mainly from out-of-office agents as the Trojan was spammed during the Christmas break when most businesses were closed. The sheer number of messages implied that a spam list had been used, consisting of email addresses of easily double the number of out-of-office replies. Add to this the fact that other banks were targeted as well, and the number of original emails must have been vast. It is possible that this was intended to be a denial of service attack, but it looks more like a well-organised attempt to obtain credit card details fraudulently.

A CRIMINAL ELEMENT

What does all this tell us, and what should we be doing about it? In his 2003 annual review (see http://www.sophos.com/), Graham Cluley said he believed that virus writers had learnt that money could be made from writing viruses. My question is ‘Are they doing it themselves or is there truly a criminal element entering virus writing?’

It is far too early to draw any conclusions but we will monitor the trend over the next year. Anti-virus companies have always worked with law enforcement bodies to try to track down those responsible for propagating viruses, but we are always bound by customer confidentiality. Maybe we are all going to have to work much harder and more openly if we are to prevent this trend from growing.