

**#1 in Overall Security**

If this page does not print out automatically, select **Print** from the **File** menu.

Hackers unleash industrial spy Trojan

Malware targets very small number of high value domains

Robert Jaques, vnunet.com 29 Jun 2005

IT security experts have detected a malware-based hack attack that attempts to gain unauthorised access to the networks of specifically targeted domains.

Security firm [MessageLabs](http://MessageLabs.com), which discovered the attack, explained that the Trojan targets only a small number of email addresses - 17 in this case - rather than mass mailing itself to as many recipients as possible.

The infected emails were transmitted to a highly targeted list of recipients at only four domains, suggesting that the hackers were using the malware for industrial espionage.

The attack is designed to exploit a vulnerability in Microsoft Word caused by a buffer overflow when handling macro names. A Word document containing a long macro name overflows a buffer allowing the embedded Trojan to execute (see Microsoft Security Bulletin MS03-050).

Utilising text content potentially relevant to the target audience, the email encourages the recipients to open an attached Word document claiming to provide further information.

This document contains an embedded UPX packed Trojan that compresses the malware .exe file size in order to make it difficult for antivirus software to detect.

The majority of the emails were bound for addresses at one particular international organisation that operates in the global security arena. This is the second time that [MessageLabs](http://MessageLabs.com) has intercepted attacks aimed at this organisation over the past month.

"The motivation behind today's new email-borne threats is far more sinister than traditional methods of large-scale attacks," said Mark Sunner, chief technology officer at [MessageLabs](http://MessageLabs.com).

"New criminal methods show a preference for selecting a particular target to attack, whether an individual or an organisation, for perhaps financial or competitive gain.

"The architects behind the bespoke Trojan attacks we are witnessing aim to steal confidential corporate information and intellectual property."

Sunner added that some content-based filters may be able to recognise a malformed macro name or a similar exploit condition within such a document, and therefore remove the macro and "defang" the exploit.

However, he went on to warn that there are some buffer overflow exploits found in similar Word documents - such as a VBE exploit - that cannot be safely removed, which is why it is always more effective to dump the entire document.

"Just removing the exploit can still leave the embedded malware present in the document," Sunner warned.

According to trend analysis by [MessageLabs](http://MessageLabs.com), there has been a gradual occurrence of targeted email attacks against businesses and organisations over the past year.

The UK's National Infrastructure Security Coordination Centre has also issued a warning about the threat these industrial strength attacks pose to governments and large corporates.

Email characteristics:

Subject lines: FW or 0627

Body Text: THE TIMES OF INDIA

Monday, June 27, 2005

China's new JL-2 missile prevents US from the Taiwan affairs

[Permalink to this story](#)

www.vnunet.com/2139033

This article was printed from the **VNU Network**
VNU Business Publications
© 2007 All rights reserved

Close [this window to return to the website](#)
