RESEARCH PROJECT

Malformed Email Project

Andreas Marx

At the end of 2001, a rapidly increasing number of email worms were using malformed emails to spread. Popular mail clients, such as *Outlook* and *Outlook Express*, are perfectly able to decode damaged or invalid messages containing attachments. However, we realised that a lot of content security programs, such as email virus scanners, were not scanning such attachments at all – because they were not RFC-compliant.

RFC stands for 'Request for Comments' – a set of technical and organizational notes about the Internet which cover many aspects of computer networking, and many of which represent Internet standards, either by practical use or by agreement. For example, they explain how SMTP (Simple Mail Transfer Protocol) or MIME (Multipurpose Internet Mail Extensions) must be implemented and how they work, so that software based on these standards is interoperable. The RFCs can be found at http://www.ietf.org/rfc.html.

Early in 2002 email security problems attracted the interest of the security community. Many methods by which a content scanner can be bypassed were published, yet still many security programs were unable to find attachments in messages whose formatting was a little out of the ordinary.

As partial fixes, anti-virus companies added detection for known viruses using this method as they were transferred as EML files (in RFC 822 format). However, without analysing the problem properly and trying to fix it in their SMTP/ MIME parser, any subsequent viruses using the same vulnerabilities to hide themselves would not be detected.

It was reasonable to think that there may be more problems which were as yet undiscovered. A little investigation and experimenting showed that there were indeed several more ways in which a virus could get past email scanners.

During February and March 2002 we (Andreas Marx and Mark Ackermans) discussed possible ways in which these known and a lot of unknown email scanner vulnerabilities could be solved in mail content security software within an acceptable length of time. It was from these discussions that the idea of the malformed email project came about. We enlisted the support of *Virus Bulletin* and embarked on the project.

The Test

A test set was created by Mark Ackermans, based heavily on the eicar.com file – at the time of writing (October 2002), this includes about 370 samples which 'hide' attachments, trick scanners or cause buffer overflows which can be used for DoS attacks, for example. However, it includes only email structure vulnerabilities and no other mail-related security issues, such as script exploits. Meanwhile we compiled a list of developers at AV/security companies who needed to be notified – currently this list stands at 89 companies.

On 3 April 2002, most of the AV/security companies on our list were sent an email (see next page), setting out our findings and indicating what we proposed to do to fix the problem (some companies were notified a little later, to allow us to answer incoming messages first and send out the test set, under non-disclosure).

We explained that the purpose of the test set is to stop malware in malformed messages – all files which can be decoded to malware by commonly used mail clients should be detected by mail security products. When malformed message parts are detected, blocking or removing the malformed part of the message is acceptable, although preference is given to virus detection, especially if blocking causes false positives and when blocking can be disabled or is disabled by default.

We thought that two months should be an acceptable length of time for companies to test their own products and to address possible issues, after which time they were to send the fixed products to us for testing. However, due to a very high number of requests for the test set, we chose to extend the deadline by one and a half months – until 22 July 2002. At the time of writing we are still receiving products for testing. (Of course, those products that failed to meet our deadline will be marked clearly as such in the final test results.)

To date, we have collected 270 different products from 43 companies for final testing. The products will be tested in the next few weeks, mainly by *AV-Test.org*'s Marc Schneider, who is working on this project as part of his diploma thesis.

Of course, for testing purposes, a new test set will be used in place of the original version distributed to the companies. This will contain real viruses instead of eicar.com, with similar and published security exploits, in order to ensure that the problems have, indeed, been fixed.

Initial Contact

The following is a copy of the first standard email we sent out to all anti-virus and content security companies, as well as other developers whose products are likely to be affected by these vulnerabilities:

Hello!

We've found out that your products are

VIRUS BULLETIN ©2002 Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, OX14 3YP, England. Tel +44 1235 555139./2002/\$0.00+2.50 No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.

very likely vulnerable to a few MIME and UUEncode problems, which makes attachments "invisible" for your product (e.g. not filtered or scanned), but well-known email programs, will "see" the attachments. For example, Outlook Express uses very liberal decoding - it is able to decode a lot of the malformed attachments correctly, therefore we used OE 5.5 SP2 for our internal tests.

"We" are Andreas Marx, team leader at the Anti-Virus Test Center at the University of Magdeburg, Germany (http://www.av-test.org/) - performing tests for more than 30 international publications; Helen Martin, Editor of Virus Bulletin, England (http://www.virusbtn.com/) and Mark Ackermans, The Netherlands. Other anti-virus organisations are also involved.

A few of these problems are already known about and have been published without informing the vendors first (e.g. http://www.security.nnov.ru/advisories/ content.asp and Bugtraq postings), others are as yet still unknown. Currently, we have about 300 malformed MIME and UUEncode files in our collection and a relatively small nymber of these anomalies are publicly known at this time. We have not tested all files with your product, due to the high number of available products, but your solution is at least vulnerable to a few tested attacks.

The good point is that some of these data are 'too malformed' to be recognised as valid attachments - such files should be stopped by your solution as being an invalid file (some will be stopped, some not). However, a lot of the rest will get through your product fully unscanned and unfiltered, which is indeed a very risky issue. A few viruses are already known which use such malformed attachment encoding - mostly, because of bugs (e.g. Win32/Badtrans.B, Win32/Sircam.A, Win32/FBound.C).

Another good example is Win32/Gibe.A: It inserts spaces in front of the base encoding which seems to result in corruptions by decoders (http://vil.nai.com/vil/content/ v_99377.htm). Most programs (for example, Outlook and WinZip) won't properly decrypt the first line and therefore the worm does not work any more (corrupted sample), but a few programs like Outlook Express will see and decrypt the attachment correctly. The worm is fully able to work.

Another example to by-pass a few programs are too long file names or a "." at the end of the filename (e.g. "test.exe."), even if this was not the main topic we've been working on (see http://online.securityfocus.com/ archive/1/265387 for details). We're almost sure that other virus authors and hackers will find out more of our ways to "bypass" your product, too. Therefore, we have decided to send out this advisory to you and other affected vendors. A few vulnerabilities have already been known for quite a long time, but they are not yet fixed. The CERT/CC is informed as well, but currently too busy, so we've decided to inform you now and not when it is too late.

I hope, we can work together to fix these issues. In this case, and if you agree not to make our test samples and demo scripts and information available to third parties, we'll send you a password-protected or PGP'ed RAR archive with all of the sample files, descriptions of the test set and tools needed to test your product. We will also assist you and answer your questions (please contact Mark with CC: to me).

During the time in which we've prepared the test set, more and more problems were made publicly available. Therefore, we can only suggest that you work carefully on these issues. We think, a good timeframe would be one month to test your product, identify and fix these problems and another one for final testing, if everything is running fine. After these two months, we'll collect all products from the informed vendors and test if all of these holes are closed. These final test results will be published in an upcoming Virus Bulletin issue and on our web site AV-Test.org. No exclusions - all products will be listed and tested. ;-)

I'm looking forward to your feedback.

Andreas Marx

What Happens Next?

The intention is to publish all test results in *Virus Bulletin*, starting in the February 2003 issue. Any review or claim made prior to this publication date that a company's product detects all samples in the test set used in this project, or that it can detect all malformed emails, cannot be verified.

Furthermore, it should be noted that detection of all files in the test set does not guarantee that the program is completely safe – the test set does not contain examples of all known mail security problems.

It is possible that we have missed a few companies or that some developers may have overlooked our initial warning in April and the reminders in the following months. If you are a developer working on content security or related products, and you are interested in gaining access to the test set and further documentation, please contact us (email editor@virusbtn.com). For security reasons, the list of companies that have been notified and those who responded cannot be published at this point.

VIRUS BULLETIN ©2002 Virus Bulletin Ltd, The Pentagon, Abingdon, Oxfordshire, OX14 3YP, England. Tel +44 1235 555139. /2002/\$0.00+2.50 No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form without the prior written permission of the publishers.