RESEARCH PROJECT

Malformed Email Project – Part 2

Andreas Marx, Mark Ackermans

Early in 2002 we embarked on a 'malformed email research project'. The details of how and why the project was started, along with our goals, were discussed in the first part of this series of articles (see *VB* November 2002, p.12). Here, we reveal the companies that were notified and the ways in which they responded. In many cases we have included details as to which versions of a product should be safe against 'malformed emails' according to *the manufacturers'* own tests. The results of our tests (carried out at *AV-Test.org*) will be published later this year.

In early April 2002, companies were informed of the project by email; a test set of malformed emails (version 1.02) was sent to all those who requested it, and the deadline we gave the companies for sending fixed products to us for testing was 6 June 2002 – however, following a large number of requests, this was extended to 22 July 2002. Since its original incarnation, the test set has been updated to reflect techniques seen in new viruses and other forms of malicious code, including W32/Junkmail (see *VB*, November 2002, p.10), W32/Yaha.K and W32/Sobig.A. Updated versions of the test set were sent to participants in May, September and November 2002, and the latest test set (version 1.07) was released in January 2003.

Aladdin, eSafe: *Aladdin* replied to our email within hours. In July 2002 *Aladdin* told us that *eSafe* detects malformed mails as 'unopenable', but the option to block them is disabled by default. We were told that they intended to rewrite their SMTP handling module to improve the handling of malformed mails. We have received no update.

Alwil Software, Avast!: *Alwil Software* responded to our initial email more than two months after it was sent. After sending *Alwil* the test set, we received no further communication from the company.

AMaViS – A Mail Virus Scanner: The *AMaViS* programmers responded to our email almost immediately. They informed us that their software relies on Perl's MIME-tools and that this library needed to be fixed. We shared our test set with the core *AMaViS* development team and, at their suggestion, informed the author of the MIME-tools library and the developer of the Convert-UUlib. The MIME-tools author responded quickly, saying that he knew about the bug and was working on the problem. We received only an auto-generated email from the author of Convert-UUlib.

At the request of the *AMaViS* developers we also notified the author of rip-MIME and Xamime. Updates were available about two months later. In addition we notified the author of qmail-scanner – changes are scheduled to be included in qmail-scanner version 2.0 – and contacted the author of MIMEDefang, who said that he would check the software using a third-party virus scanner engine. However, we received no further information. In August 2002 the authors of *AMaViS* warned in a security bulletin that *AMaViS 0.2.1* would not detect W32/Klez if rip-MIME is used. Their advice was 'upgrade to amavis-perl/amavisd, or fix the rip-MIME call'.

Astaro, Astaro Security: We received a response from *Astaro* within 24 hours. In June 2002 we received a new version of *Astaro Security* software for testing. *Firewall Astaro Security Linux version 3.214* is considered by its developers to provide sufficient protection against malformed emails.

Beginfinite, GWAVA for GroupWise: The *Beginfinite* developers replied to our email within 24 hours, stating: 'Our product actually gets the native attachments from the *GW* API (as opposed to relying on MIME decoding). Therefore we are hopefully "relatively" immune.' In July 2002 we were informed that the test messages caused a few abends, and that these had been reported to *Novell*. The product offers the raw message, the decoded body text and the decoded attachments to a virus scanner to be checked. According to the developer, adding an extra layer of decoding would 'slow down' the mail server 'enormously'. We received no further information about *GWAVA.*

BorderWare, Mail Gateway/MXtreme Firewall: *BorderWare*'s response came within 24 hours. They said that only about 10 per cent of the malformed mail samples were not blocked, according to their own tests. At the beginning of June 2002 *BorderWare Technologies* claimed that *Mail Gateway version 1.3* had passed all of the tests in the malformed email test set. In October 2002 *BorderWare* sponsored a *SecurityFocus* newsletter which included a link to a *BorderWare* web page, on which the claim was made that *MXtreme* 'detects and blocks 100% of invalid messages per University of Magdeburg test suite.' Furthermore, detailed information about the content of the test set was available on the *MXtreme* website – constituting a violation of our non-disclosure agreement. *BorderWare* was removed from the test set distribution list immediately.

Cat Computer Systems, Quick Heal: No reply was received to our original email until some five months later when *Cat*'s lead programmer found out about the project. Five days later, the developers sent us the first fixes for their products, with a detection rate 'up to 80%' of all malformed mails. In September 2002 we received *Quick Heal 6.07 SR* with fixes that should be able to detect all kinds of malformed files.

Clearswift, MAILsweeper: We received a reply from *Clearswift* within a few minutes. In July 2002 we received *MAILsweeper version 4.3_1 RC1* for testing. It should be noted that version 4.2, including all updates, is vulnerable to some malformed email attacks – for example, W32/Yaha.K cannot be found by this version if the AV engine is not scanning the whole EML file. All customers should upgrade to version 4.3 as soon as possible.

Command Software, Command AV: *Command Software* replied to our email within minutes. They told us that most of the messages in the test set were not MIME RFC-compliant. In fact, most MIME messages in our test set contained the error that the 'MIME-Version' header was missing, which caused additional problems for a number of programs. The developers told us that it would be almost impossible for them to fix the issues and certainly not within two months. In late July *Command Software* told us that they were still having problems with a German *Exchange* version and they were unable to send us a fixed version.

Computer Associates, InoculateIT/eTrust AV: *Computer Associates* replied to our message within a few hours. In July 2002 a patch, 'qo21090', for *eTrust AV 6.0* (*Windows* version only) was made available at the *CA* ftp server, but the patch was not mentioned anywhere on the public website. We understand that, following more QA, similar patches should be available for the *Linux* and *Solaris* platforms and that the patches, together with a number of other changes and new features will be included in *eTrust AV 6.1,* due to be released in mid-February 2003.

Computerized Horizons, Declude Virus: *Computerized Horizons* replied to our email within a few hours. In November 2002 the developers informed us that *Declude Virus* (*v1.63*) covers the most recent test sets of malformed messages.

DataEnter, XWall: *DataEnter* replied within a few minutes and, in May 2002, we received a download link of the current fixed *XWall* version for testing.

Finjan, SurfinGate: We received a reply from *Finjan* within 24 hours. *Finjan* explained that they could not fix their product, because it uses the *NAI/McAfee* engine which needed to be updated. In July 2002 we received *SurfinGate version 6.01* (without an updated engine) for testing. Version 4.2.40 of the *NAI/McAfee* virus scan engine is due to be released in late February 2003, when the current *SurfinGate version 7.0* should be updated accordingly.

Fortinet, FortiGate: *Fortinet* responded to our email within a few minutes. In July 2002 *FortiGate 300 Network Protection Gateway* was shipped to us for testing (this release included a beta version of the malformed email protection). A month later we received the final release, which is now available to all customers.

F-Secure, F-Secure Anti-Virus: Developers at *F-Secure* responded to our email within a few minutes, telling us that they were aware of malformed mails and they had made several fixes and hotfixes available to their customers to block such attachments. According to the developers, the fixes were first introduced in *F-Secure AV for Firewalls 6.10* (beta) and *F-Secure AV for Exchange 6.00* (beta). In July 2002 we were informed that *F-Secure AV for Exchange 6.0* (final version), *F-Secure AV for Firewalls 6.10* (final version), *Internet Mail 6.00* (final version with Hotfix 5) and all the Content Scanner Server modules included in these versions were fixed (the *Lotus Notes* AV solution has been discontinued and will not be updated).

G DATA, AntiVirenKit for SMTP Gateways: *G DATA* replied to our email six days after receiving it, and a fixed beta product was submitted for testing in July 2002 – the final version was released in January 2003.

GeCAD Software, RAV AntiVirus: We received a response within 24 hours from *GeCAD*, and we were told in July 2002 that we should test any of the *RAV* products after updating to the latest engine update.

GFI, MailSecurity/MailEssentials: *GFI* replied to our email within a few minutes. The developers said: 'We noticed that the email files which managed to bypass our products are so malformed that they tend to be harmless' (no email program was able to find an attachment) and declared that the program releases available at the time (May 2002) should, therefore, be safe.

Gordano, Messaging Suite: *Gordano* replied five days after our email was sent, informing us that they were already working on some malformed mail issues caused by ItW viruses and that an update was planned for release the following week. In May we were told that the most recent public release of *Messaging Suite* (3037) should protect against malformed mails in our test set.

Grisoft, AVG: *Grisoft* took two weeks to respond to our original email. By July 2002 the developers claimed that all problems besides one (a problem with file extensions) should be fixed with beta version 6.0.379 pre-release of the personal email scanner and *AVG 6.0.377.*

Group Technologies, iQ Suite: *Group Technologies* replied within 48 hours. In July 2002 they informed us that the problems were fixed in version 5.2c of the *Lotus Notes* product (at this time, a release candidate); the first release of the *iQ Suite for Exchange 2000* (planned for Q1/2003) should include all the necessary fixes.

H+BEDV Datentechnik, AntiVir Mailgate: *H+BEDV* replied within 48 hours and within five days told us that a new version that could decode all of the malformed messages was ready. In May 2002 version 2.0.0.4 was released, which fixed most of the issues and in July a further update – version 2.0.0.9 – was released. According to *H+BEDV*, this and all later versions should be safe.

IBM, Lotus Notes/Domino: We received the following email from *Lotus*: 'We would like to work with you to address any issues you have discovered with our products … To date, we have not found *Notes* to be vulnerable to these recently reported types of MIME issues.' We did not hear back from them.

Ikarus Software, Virus Utilities: *Ikarus* replied to our email within 48 hours. In July 2002 We received fixed versions of *Ikarus MailWall/ContentWall* and their *Checkpoint FW-1* appliance '*SecureGuard*', developed by OSST.

Indefense, MailDefense: We received a response to our email from *Indefense* within 24 hours. In July *MailDefense 1.02.10* was submitted for our testing.

Kaspersky Labs, Kaspersky AntiVirus: *Kaspersky Labs* replied to our email within a few minutes. The developers investigating the test set identified some additional problems with the malformed mails in our test set – and another in their email gateway scanner, which was scanning our password-protected test set archive for some 25 hours. Despite some very interesting discussions about all kinds of malformed mail problems, we did not receive fixed versions of *Kaspersky* products for testing.

Marshal Software, MailMarshal: We received a reply to our email within 24 hours. In July 2002 we received *MailMarshal Build 5.0.3.54* for testing, together with some documentation of tests *Marshall Software* has performed with our test set.

MessageLabs, SkyScan AV: *MessageLabs* responded to our email within a few minutes, stating that additional checks would be implemented in their systems with immediate effect, to improve their existing malformed mail checker.

Microsoft, Exchange Server/ISA Server: We contacted *Microsoft* because we thought it could be useful for their developers to investigate these malformed email issues. For example, they could improve their Mail Server APIs to improve detection of malformed mails or they could limit their MIME parser in future product releases so it would no longer be able to catch all of these badly malformed attachments and reassemble them (which would make their products significantly more RFC-compliant). In June 2002 we received the following comment from *Microsoft*: 'If our MIME parser is used it's very robust and essentially can handle wide ranges of commonly found malformed MIME. *Outlook* and *Outlook Express* have very similar MIME parsing capabilities.' (Which is exactly the problem!)

MicroWorld Technologies, eScan/MailScan: *MicroWorld Technologies* replied to our email after a week. In May 2002 the company informed us, 'We have completed all vulnerability tests with 100% detection rates. The updated binaries of *MailScan* will be released as part of Service Pack 4.'

Mirapoint, Secure Messaging: *Mirapoint* replied to our email within 48 hours. *Mirapoint* requested that some of the undetected messages be sent to *Sophos*, as they believed it was the *Sophos* scanning engine that needed to be changed. We did not receive an appliance for testing.

MKS, MKS_VIR: *MKS* responded to our email within 48 hours. According to *MKS*, all products released after 12 July 2002 are 'known' to be safe.

Network Associates, VirusScan/GroupShield/NetShield: We received a response from *NAI* within a few minutes. In July 2002 we received the following versions for our tests: *GroupShield for Domino 5.0a Hotfix 7*, *WebShield for Windows NT SMTP Version MR1a HotFix 6*, *WebShield for Solaris 4.1 HotFix 3*. In addition, the following patches for appliances were available: e50: HotFix 3, e250/e500 (versions 2.1/2.0): Hotfix 11a, e250/e500 (version 2.5): Hotfix 2a. The *Exchange 5.5/2000* requires at least engine version 4.1.70 (beta) to fix the malformed mail issues. A public beta version of the new engine (labelled 4.1.80) was released in December 2002. The final version 4.2.40 should be available at the end of February 2003.

Norman, Virus Control: *Norman*'s developers responded to our email within a few minutes. In July 2002 we received fixes for the *Exchange 2000*, *Lotus Notes*, *Mimesweeper* and *Checkpoint FW-1* versions.

Open Access, MailGate: *Open Access* replied within 24 hours. In July 2002 we received *MailGate 3.5.174* beta for testing.

Panda Software, Panda AV: We received a response from *Panda Software* within a few minutes. In June 2002 we received updated products for *Postfix* (version 0.3) and *QMail* (version 1.01). In July 2002 we received updates for the *Exchange* and *Lotus Notes* products (version 2.51.81 of *Panda Administrator*).

Postini, Postini: Like *MessageLabs*, *Postini* is an email security service provider that does not ship any product to end users. *Postini* replied to our email within 24 hours, telling us that they had made enhancements to their scanner to identify and scan malformed mails, because the AV protection they were relying on (*McAfee*) didn't do so properly. Following the changes, all mails are extracted by *Postini* mail decoder and the AV engine gets only the extracted files for scanning.

Softwin, BitDefender: *Softwin*'s developers replied to our email within a few hours, telling us that they were working on a malformed email protection, to be included in the 7.0 engine, and that a fixed version should be available in less than a month. However, we have received no update.

Sonicwall, SonicWALL: *Sonicwall*'s response to our email arrived within eight days. The company stated: 'Our current product is a standard firewall/VPN concentrator. We have added some capabilities of filtering email attachments, but they are only based on filenames. We are developing additional security products that will scan emails for viruses, worms and other intrusions, but those products are still in development. We will be using your test suite to validate our development.' We have received no further communication. However, the website shows that they offer a virus-scanning product called *SonicWALL Complete Anti-Virus* with *SonicWALL Network Anti-Virus.*

Sophos, MailMonitor: The developers at *Sophos* replied to our email within a few minutes. In July 2002 *MailMonitor for Lotus Notes* (version 2.0.2 beta) and *Exchange 2000* (version 1.0.3) were released and, according to *Sophos*, these should address the malformed mail issues. Ten days later *MailMonitor for SMTP 1.2.0 Beta* for *Windows NT*-based platforms was released, and in October *MailMonitor 1.2.0* (final) was released. In August 2002 *MailMonitor for SMTP 1.2.0 Beta 2* on *Solaris* and *Linux* were available for download from the 'Beta products' section of the *Sophos* website. *MailMonitor for Linux 1.2.1* (final) was released in December 2002.

Stalker, CommuniGate Pro: *Stalker* replied within a few minutes, saying 'Our company manufactures hi-end mail servers … To scan messages, we use plug-in modules that are developed by anti-virus vendors. Currently, we officially support and resell the *McAfee* Plug-in for *CommuniGate Pro*, though there are other plug-ins.' They asked to receive the test set for future enhancements, for example, to block malformed mails completely. In July 2002 we received a version for testing with the comment that detection is dependent on the plug-in provided by *McAfee*.

SurfControl, SurfControl E-mail Filter: *SurfControl* replied to our email five days after it was sent. In July 2002 version 4.0.52e was submitted for our tests.

Sybari, Antigen: We received a reply from *Sybari* three weeks after our email was sent. In July 2002 we were informed that *Sybari* was unable to give us a new version of *Antigen* since the development team was working on a new release which would include new features as well as an improvement in the scanning of malformed emails. A public beta was scheduled to be ready in October 2002. There was no further communication.

Symantec, Norton AV/Symantec AV: *Symantec*'s developers replied to our email within a few hours. In July we received a CD, but this included only the most current SMTP scanner version. In August we received a second CD, this time with all the products we needed for our tests.

Symantec provided the following information about the status of its products: *NAV for Lotus Notes 2.5.1* (*Linux*, *Solaris*, *Windows NT*/*2000*, *AIX*, *AS400* and *iSeries*): no known problems with malformed MIME/dependent on *Notes* decomposer; *SAV/F Exchange v3.03* (*Windows NT*/*2000*): no known problems with malformed MIME with latest update available from September 2002; *SAVSE 3.0* and above (*Windows NT*/*2000*, *Solaris* and *Linux*): no known problems with malformed MIME with latest update available from mid-2002; *SAV SMTP v3* and above (*Solaris* and *Windows NT*/*2000*): no known problems with malformed MIME with latest update available from December 2002; *SWS v2.5* and above (*Solaris* and *Windows NT*/*2000*): no known problems with malformed MIME with latest update available from October 2002.

Trend Micro, InterScan/ScanMail etc.: *Trend* responded to our email within minutes. We received updated *Windows*-based versions of the engine (version 6.350-1101) in August 2002. In September we received two CDs containing all *Trend*'s updated email security products. Engine version 6.510 was released to the public in December 2002 (this is a pre-condition to detect malformed mails with *Trend Micro* products; the new engine is also able to identify and block a few variants with older product releases). In January this year we received new beta builds of a number of products.

According to *Trend*, *ScanMail 6.1 for Exchange 2000* and *ScanMail 3.81 for Exchange 5.5* will be released in mid-March 2003 (for the last version, a special Registry key needed to be set to enable detection) and will include protection against malformed mails; a patch will be available for *ScanMail for Lotus Notes 2.6* to fix the issues; the next release (2.7) should include all changes and will be published in Q2/2003. All products of the *InterScan Messaging Security Suite* are affected by the malformed mail issues and a patch will be released in Q1/2003.

We received the following comment from *Trend Micro*: 'The amount of infections caused by malformed emails is currently low … when actual threats emerge, we have alternative technologies such as Outbreak Prevention Service (OPS), pattern updates, to address the threat.'

Vircom, VOP modusGate/modusMail: *Vircom* replied to our email three weeks after it was sent. Unfortunately, an oversight on our part led to the company being omitted from our mailing list, meaning that they did not receive the updated test set versions or revised deadlines. In October 2002 *Vircom* told us that only six files were still not detected according to our latest available test set and that publicly available updates would be released after finishing the final QA tests.

VirusBuster, VirusBuster: We received a response from *VirusBuster* within 24 hours. The first fixed version of *VirusBuster MailShield 1.10 for Linux* was publicly available in July 2002 and 20 days later version 1.10.02 was released.

WatchGuard Technologies, WatchGuard: *WatchGuard* replied within 24 hours but later declined to offer a *Firebox* appliance for testing, stating, 'It is not our policy to participate in this sort of review except under controlled conditions where our engineers are present to review the configuration of the *Firebox* and test environment.'

Webwasher, WebWasher: *Webwasher* responded three days after our email was sent. *WebWasher 4.1 Build 185* (Beta) was publicly available for *Windows*, *Linux* and *Solaris* in July 2002 and, according to the developers, this release should fix the issues.

ZoneLabs, ZoneAlarm: *ZoneLabs* responded to our email within minutes. In July 2002 we received fixed versions of *ZoneAlarm Freeware 3.1*, *ZoneAlarm Plus 3.1* and *ZoneAlarm Pro 3.1* (the older 2.x releases are no longer supported and will not be fixed).

Others

The following organisations contacted us after reading the introduction to the project in the November 2002 issue of *VB* and have been sent the test set:

- *eAcceleration*, *eAnthology*
- University of Southampton, *MailScanner*
- *Ositis*, *WinProxy*/*AVStripper*
- *eSoft*, *SoftPak*
- *Blackspider*, *BlackSpider AV*

The following companies were notified multiple times, but we have received no response to our mails:

- *Bluetail*
- *BVRP Software*
- *Checkpoint*
- *Computer Mail Services*
- *Critical Path*
- *Cyberguard*
- *Cybersoft*
- *Easylink*
- *Electricmail*
- *Elron Software*
- *Escon*
- *Eset*
- *GreenComputer*
- *Invisimail*
- *IP-Engine*
- *IPSwitch*
- *Lyris*
- *Merak Mail Server Software*
- *MultiTech*
- *Nemx*
- *Novell*
- *PPP-India*
- *Proland*
- *Sald*
- *Sendmail*
- *SSI-Mail*
- *TFS Technology*
- *Tumbleweed*
- *Webshuttle*

We hope these companies will get in contact with us (via the editor of *VB* – editor@virusbtn.com) as soon as possible.

Acknowledgements

We would like to thank the following people for their help, ideas and useful input to improve our reference collection (in no particular order): Alex Shipp (*MessageLabs*), Costin Raiu (*Kaspersky Labs*), Menashe Eliezer (*Finjan*), Peter Ferrie (*Symantec*), Pierre Laliberte (*Vircom*), Sanjay Katkar (*Cat Computer Systems*) and Scott Perry (*Declude*). We would also like to thank *GFI*, *Securiteam* and *Webwasher* for additional test set resources. The first results of our own tests, revealing how the products perform and whether their claims to be safe against malformed emails can be verified, will be released in April 2003.