Sobig.f - a Lesson in Information Security Management

Michael Barwise

On 18th August 2003 a new variant of the Sobig email worm (Sobig.f) was identified.[i] Within its first week of activity it spread faster and further than any previous worm of its type,[ii] and has clearly highlighted some critical deficiencies in corporate information security management.

Sobig.f arrives as an executable attachment to a plain text email, which does not execute automatically when the email body is opened. The attachment must be manually opened to trigger the worm, and its file types are neither sophisticated nor spoofed .The range of alternative email subjects it uses is small: there are only nine alternatives, none of which are highly imaginative or credible. There are only two email body texts, both of which merely state that all the information is contained in the attachment. The worm spoofs the From: field of the infected emails it sends, using a real address stolen from the infected computer. In common with many previous worms, it includes its own SMTP engine and it searches quite exhaustively for email addresses on victim computers.[iii] None of this, however, explains its exceptional performance. So what is special about this worm that makes it so successful? I suggest that the key contributors are not attributes of the worm at all, but failures of information security management.

The most obvious is the lack of, or failure to properly maintain, antivirus protection. Many home and SOHO users simply do not have even basic antivirus protection. Even in the corporate arena, protection may be only nominal. Commercial antivirus packages are generally the sole line of defence, and virus signature updates are often a quite low priority for IT operations staff. The rate at which most virulent worms now propagate makes the window of opportunity for deploying signature files very short indeed: often a matter of a few hours. Not only must much higher priority be placed on updates, but other more robust countermeasures must also be implemented in parallel with antivirus. Very few corporates restrict the types of email attachment that can be received. There ought to be a solid documented business case for admitting any executable file type as an email attachment into the organisation from the Internet. Even excluding executables completely is unlikely to adversely affect most businesses, but this very obvious countermeasure is rarely considered. It would, however, kill most email worms stone dead.

Sobig.f, like the majority of email worms, spreads solely by user intervention, but the propensity of IT users to open emails and attachments without thinking seems to be increasing. Protection against this kind of email worm should not have to rely on “security awareness training” or on emergency briefings about specific threats. Users need to be made generally suspicious of unsolicited, odd-looking or inconsequential emails that do not relate to the business they transact. Unlike some predecessors, this worm does not craft convincing message bodies out of document contents from infected computers, nor does it exhibit much ingenuity in its choice of subject. If you’re paying attention at all, the email is frankly quite suspect. Therefore IT users must be made to wake up and pay attention.

Third, and probably most interesting, is the way this worm can use alerts from misconfigured email gateway antivirus to flood email networks and potentially to spread. Whether or not this was envisaged by the authors, there is some evidence that it has made a significant contribution to the effectiveness of Sobig.f[iv]. Security-conscious enterprises install email gateway antivirus products which scan for and drop or quarantine suspect messages and attachments. Many of the products also attempt to notify the sender that they are the source of potential infection. So far so good. Why should this very sensible action pose any threat? Sadly, it’s down to limited thinking on the part of the developers or deployers of these products. Almost universally, such notifications are sent to the email address in the From: field of the received email. This field is of course the easiest thing in the world to forge, as Sobig.f does. So the alert is misdirected to a recipient who has not so far participated in an exchange of infected messages. Ironically, the IP address in the first Received From: field is much more likely to reflect the true origin of the message. The common implementation has simply picked the wrong header field, turning the notification into useless traffic. An example of the extent of such traffic is cited by Russ Cooper.[v] By the morning of 21st August he had received 8000 copies of Sobig.f and more than 2000 misdirected notifications, representing some twenty percent of the total traffic. This is indeed bad, but there is worse to come.

Just over half the misdirected Sobig.f notifications I received between 20th and 26th August contained (as an attachment) the complete Sobig.f email (including its own malicious attachment), and I don't believe I was singled out for this special treatment. Obviously, the worm could be spread, should the recipient of a notification open the encapsulated attachment. But if it were to arrive at an email gateway that is protected in the same way, a notification would presumably be generated by the antivirus on that gateway. This new notification would be returned to the true origin of the original notification, attaching the original entire message including Sobig.f. An unlimited ping-pong of further notifications could result between the two gateways, causing degradation of service.

Thus we see that, in spite of its virulence, Sobig.f is not miraculous or impossible to protect yourself against. Well thought out managed information security measures at the detail level could easily make this and most other worms a thing of the past. You need to hire exceptionally alert and knowledgeable information security staff, you need to give them time to think, and you need to pay attention to them and accept their advice. The alternative is being wiped out by the next worm that comes along.

---

[i] http://symantec.com/avcenter/venc/data/w32sobig.f@mm.html
[ii] http://www.cnn.com/2003/TECH/internet/08/21/sobig.virus/
[iii] http://symantec.com/avcenter/venc/data/w32sobig.f@mm.html
[iv] for example: Windows NT Bugtraq 21 Aug. 2003 "AV/Spam alert response messages"
[v] ibid

Originally appeared in Computer Weekly, August 2003