



When threatened globally, act locally

By Nicole Manktelow

February 17, 2004

Sluggish networks, odd activity, strange traffic - in the early moments of an online threat, network managers can try to crack the clues. By the time some symptoms show, however, it may already be too late.

"If you were to do a timeline, sometimes it would be over before anyone knew it began," says Jamie Gillespie, senior analyst with the national expert bureau AusCERT (Australian Computer Emergency Response Team).

It was 9.30am when James Nicolson arrived at the office to find staff members at his desk asking about strange email attachments.

"They were asking, 'What's that? Can I open it?'," he says.

Nicolson is sales manager at a company that employs about 20 people and is the key contact for the outsourced IT person. It took a few minutes before he realised a couple of machines were already infected. The emails quickly began to pile up in staff inboxes.

Now, of course, every internet user has heard about Mydoom. The mass-mailing worm swamped the net with record-breaking speed and brought the website of software maker SCO Group to its knees.

"When we realised it was internal on the network, I contacted the provider and asked them to take the email service offline," Nicolson says.

The company uses an antivirus product and updates it regularly but, as is the case with newly discovered viruses, it had to wait for the vendor to analyse the threat and send an update.

"The virus definitions were available by about 11.30am," Nicolson says, although his email service was offline for about five hours as he searched for the infected machines and began cleaning up the mess.

At its peak, Mydoom was present in one out of every 12 emails passing through the internet. It became the world's fastest-spreading mass-mailing worm and analysts say it infected more than 100 million computers in more than 200 countries.

Infected machines were deployed as part of a distributed denial-of-service attack against SCO's main site, bombarding the server with constant requests.

Meanwhile, a less rampant variant took a few stabs at Microsoft's home page.

For some organisations, the first strong indication of trouble comes from the help-desk.

"The end user may not know that they have a problem," says Andrew Lee, a consultant with IBM's security group.

"IT people get calls from staff complaining of slow bandwidth.

"They also get calls from customers complaining that they can't log in to send an order or move money around," he says.

That's when IT managers start looking at network traffic for clues.

"When you see a pile of emails that look similar, as opposed to normal traffic, you start to get a little

suspicious," says Lee.

Virtual private network provider Bulletproof Networks gets a bird's-eye view when online chaos begins.

"We manage customers on a whole swag of networks and, through monitoring customers, we get a good view," says marketing director Lorenzo Modesto.

"Our monitoring alarms pick up increases in latency, and when we see that affect non-related customers on different networks, we know it's a big one," Modesto says.

"We'll see a number of alerts go off. They may be from unrelated clients, on different networks but they will have a common denominator . . . it can be the kind of traffic they are experiencing.

"The engineers will be looking at the traffic. When we realise what it is, we can go through the old alerts to see if it matches an old worm."

Few organisations have this level of monitoring but when a problem such as Mydoom is detected, the steps for defence are essentially the same.

"It depends on the attack but you can either batten down the hatches locally or report the issue to your upstream internet connectivity provider," Modesto says. "Unfortunately, it can take hours to have upstream providers changing firewall rules but local measures can start within a matter of minutes."

For local measures, organisations ideally need tools to identify malicious software and a written procedure to avoid panic and knee-jerk reactions, Lee says.

"Although, admittedly, the response could be to pull the cable out of the machine, the problem is that the customer can get annoyed they cannot get access and (the worm or virus) is still inside your system.

"There are better ways. If you can identify the virus on a particular attachment, you can block it yourself while waiting for the antivirus provider to update signatures.

"You can just block all attachments if you don't want to be overly clever."

Bandwidth problems remain a nasty side effect.

"One of the problems with the latest threats is that even if your protection is perfect, your bandwidth is still being sucked up," Lee says.

"A lot of SMEs have very small pipes and it doesn't take much of a problem for a 1 Mbps pipe to be swamped."

Organisations could consider using external scanning services, such as MessageLabs.

"It is one option to move one layer away from the problem using an organisation that specialises in scanning," Lee says.

Despite growing sophistication, many viruses still spread by convincing recipients to open a malicious attachment.

"For the majority of incidents it does come down to the human factor," says Gillespie.

Some organisations use content filters to weed out all executables from incoming attachments. However, the success of these systems depends on the policies used to control them.

Mydoom sent its file as a .zip compression file, bypassing some blocking policies.

"For Mimesweeper, users needed a policy to be set to check the files within the zip," says Chy Chuawiwat, managing director of Clearswift, maker of the content filter. This is not a default setting.

Clearswift has a policy to block all incoming executables except those that go to the IT department.

Technical manager Steve Irving was notified when an executable was sent to the sales department.

"He looked at the subject lines, headers and From information. It didn't look right. He went next to the antivirus sites to try and find out about it. It wasn't until about 10am that the antivirus companies had started to acknowledge it existed," Chuawiwat says.

It is usually a matter of hours before antivirus vendors can release an update but how many varies greatly from threat to threat, Lee says.

"You can't just knock up something quickly. You must test it to make sure it won't cause a problem."

In all of this, the best offence is self-defence and as essential as antivirus and firewalls are, when new troubles arise, network managers need other analysis tools, like sniffers, to find out what's going on.

"If you've only got 10 people in the company, then probably it's the one person doing all the IT, so they need a tool," says Lee. "Tools are becoming available for SMEs now that are GUI-based, but they still need someone who can work it out . . . the ease of use needs to be improved.

"All a basic sniffer does is display what's going up and down the pipe. But you need intelligence to present this in a meaningful way, so you can see if it is the same name, same subject line, same attachment."

Intrusion Detection Systems are vital for heading off a possible attack, says Gillespie.

"You either stop an attack at the beginning with a firewall and intrusion detection system or learn about it after the fact," he warns.

Intrusion detection systems won't stop an invader, "but at least you can see what's happening," he says.

nicole@auscape.net.au

This story was found at: <http://smh.com.au/articles/2004/02/16/1076779895616.html>