Monthly report

October 2004

Rise of the zombie botnets

Statistics for October

In October, MessageLabs scanned over 84 million emails per day on behalf of its clients.

In October, MessageLabs scanned more than 1.91 billion emails worldwide for spam, of which over 1.47 billion or 76.76% (1 in 1.30), were stopped as spam (565.56 per second).

During the same period, the company also scanned over 2.29 billion emails for viruses, Trojans and other malicious content, and more than 71 million or 3.10% (or 1 in 32.24) were intercepted (27.51 per second).*

The rise of the zombie botnets

It has long been known that one of the largest sources of spam and viruses is the "zombie botnet", the network of virus-compromised computers connected to the Internet that can be remotely controlled by spammers and virus writers to anonymously distribute their wares.

Earlier this year, the botnet problem gained global attention when Comcast, one of the largest residential broadband providers, was found to be single-handedly responsible for the biggest proportion of spam on the Internet. Comcast subscribers were sending out more than 800 million emails per day, according to the statistics at Senderbase, while only around 12% were sent through the company's email servers. The vast majority was spam being relayed through zombie computers that had been compromised to send the unwanted messages.

For ISPs, closing down these zombies can be akin to chasing a moving target. Some are now closing TCP port 25 access that is used to send email via the SMTP protocol. For the relative minority of users who send email from Linux boxes, for example, this poses an immediate problem. It also is a potentially costly exercise for the ISP that pursues this option, as it can require them to provide additional helpdesk support to enable users to reconfigure their servers.

Other spam-mitigating approaches also include "throttling" email traffic so that if a particular connection is seen to be sending a high-volume of email, the connection can be slowed or stopped at a certain threshold, somewhat like passing the emails through a rather viscous tar-pit.

The proliferation of spamming software

It seems that with increasing pressure on ISPs to take drastic anti-spam actions, we are likely to see some benefits in the coming months. In the wake of the US CAN-SPAM legislation, though, we have instead experienced a sharp rise in spam volumes this year, particularly in the US where the epidemic has now become diaspora spanning many continents.

Many new businesses have now appeared on the Internet selling "direct marketing" software that claims to offer compliance with CAN-SPAM. Instead, these packages can include email servers hosted in Asia, which can dynamically change IP address every few minutes to circumvent ISP filters.

The purported author behind one of these spam tools, which enables spam to be propagated through botnets, has recently been named and implicated in the creation of the Sobig family of viruses in 2003. Since early January 2003, MessageLabs has stopped over 17 million copies of Sobig.A through Sobig.F

In a recent document entitled, "Who Wrote Sobig?" the

Virus name	Number intercepted	First intercepted	Expiration date
WS32/SoBig.A-mm	856,416	9 January 2003	Ongoing
WS32/SoBig.B-mm	409,735	17 May 2003	31 May 2003
WS32/SoBig.C-mm	180,560	31 May 2003	8 June 2003
WS32/SoBig.D-mm	4,365	18 June 2003	2 July 2003
WS32/SoBig.E-mm	359,008	25 June 2003	14 July 2003
WS32/SoBig.F-mm	16,670,849	18 August 2003	10 September 2003

Evolution: the Sobig family of email viruses

authors suggested that "through the use of forensics and profiling, [the authors] have identified a very likely suspect and motive."

The botnet problem is further compounded by operations that have now moved offshore, running server farms through which millions of spam messages are sent every day. Often these spammers run rings around authorities by encrypting traffic across virtual private networks, making any potential investigation difficult. Furthermore, many of these countries do not have effective legislation in place to prevent this, and those that are trying to tackle the problem still assume the "one spammer - one server" model, which is no longer the case.

Using viruses to create botnets

Since early 2003, a common device for deploying a Trojan backdoor component has been the staged technique. Initially, this meant that the first-stage virus infection would initiate the download of a second-stage component from a main website, or "mother-ship". The actual payload would often be hidden inside this second (or sometimes third) stage download.

On the plus-side, it is also relatively straightforward for virus fighters to discover the location of these sites and close them down more quickly, thus severing the "umbilical cord" of the botnet from the "mother-ship".

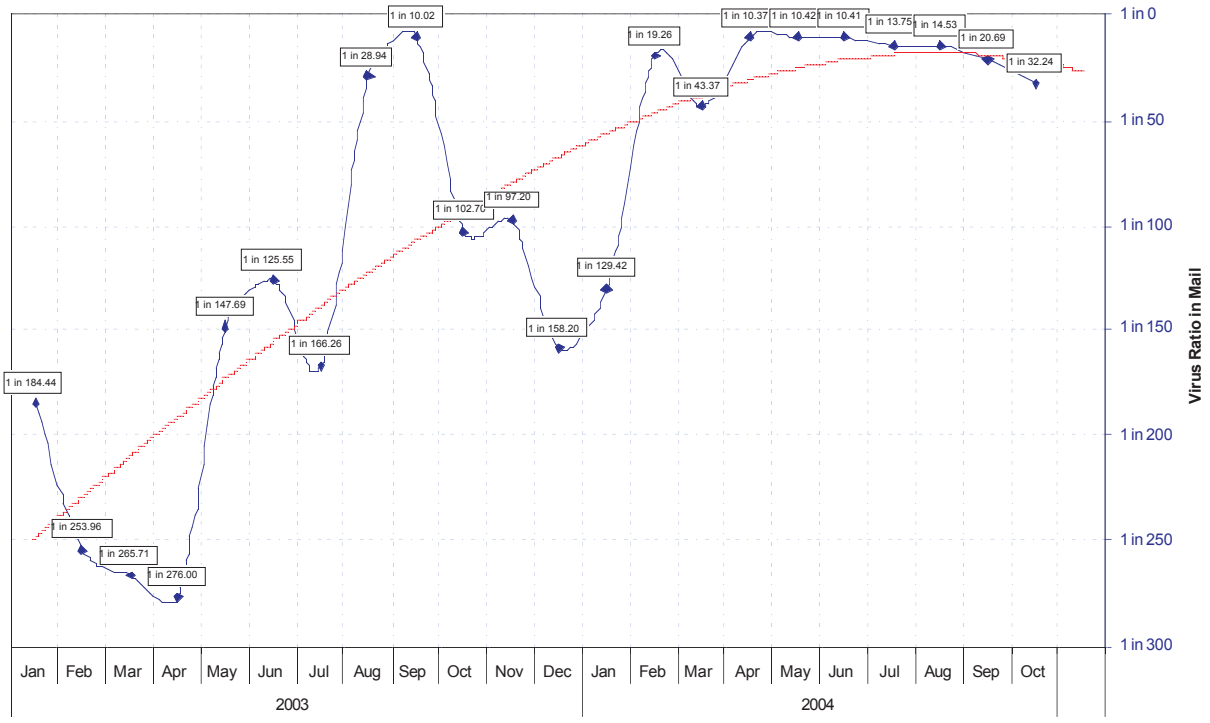
Often the location, or IP address, of these mother-ship sites would be encrypted, but again, they could be analysed, decrypted and shut down. By using these more sophisticated techniques, the bad guys were able to install many different types of backdoors once an initial foothold was gained and they could issue further commands to update the Trojans with new instructions.

It also meant that the virus code itself could be updated and bug-fixed, and that TCP/UDP port numbers or IP addresses could also be changed to further keep the botnet alive.

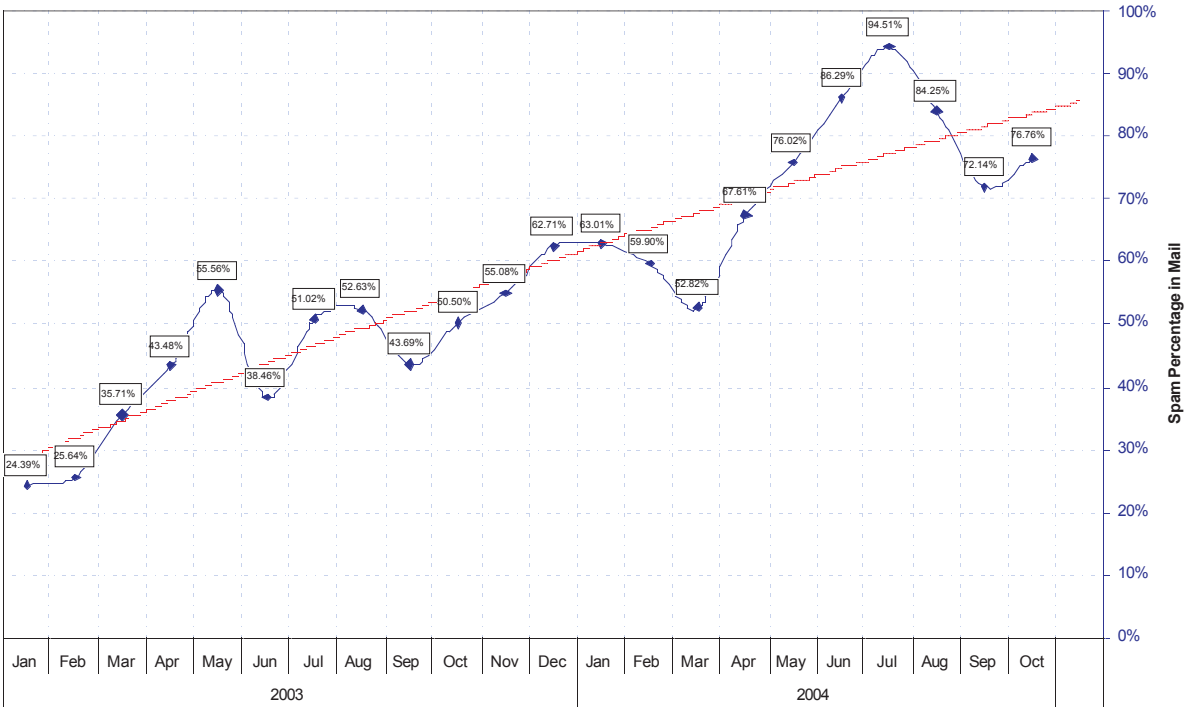
Case study: Sobig, 2003

Sobig was one of those viruses that showed the botnet method could be successful and put to criminal use. Sobig's inventiveness used a second-stage component to control the deployment of the third-stage backdoor "open proxy" service on an unsuspecting user's computer.

These zombies are now being routinely used by spammers to anonymously send junk mail. Approximately 70% of the spam intercepted by MessageLabs over the past 12 months has been sent through zombie botnets.



Viruses: proportion of email carrying viruses (MessageLabs clients)



Spam: proportion of email identified as spam (MessageLabs clients)

One particularly notable side-effect of Sobig was that its proxy component was in fact a genuine legitimate piece of software that was being installed contrary to its licence agreement. This meant it would not be possible for anti-virus software to detect the final stage of its installation without entering into a potential legal wrangle with the software makers of WinGate Proxy Server. This made it all the more important for computers connected to the Internet to have local firewall software installed, which could nip the virus in the bud.

One problem still remained though: the probability of the mother-ship sites being identified and closed down before the virus or Trojan was able to fully activate. This is largely what happened in the case of Sobig.F, the most eminent incarnation of the original progenitor.

Overcoming the umbilical problem: peer-to-peer botnets

After Sobig.F hit in August 2003, it became obvious that it wasn't a typical virus or Trojan and that its motive was for financial and ultimately criminal gain. The perpetrators behind it needed another way to hide the addresses of these mother-ships, which had become the single-point-of-failure in the virus' design.

Other techniques had been tried and, to varying degrees, succeeded, by using IRC (internet chat) to control zombies from Internet chat rooms, such as with the Fizzer virus.

Today, a more contemporary approach seems already to have evolved: rather than communicating via a mother-ship, zombies can scan the Internet, searching for other similar zombies. Once contact between zombies has been established, they can exchange information about all the other zombies that they have previously discovered.

This dynamic approach is certainly a step beyond the typical peer-to-peer networking model, which would use a network of servers through which the peers would communicate, such as the peer-to-peer file sharing services used to exchange music files.

Case study: Sinit

The first example of this technique was with a Trojan called Backdoor-BAM (aka Calyps, Backdoor.Sinit or Sinit). With this Trojan, there were no mother-ships, which meant there was no hard-coded list of IP addresses of computers that, once shut down, could deactivate the botnet. As the Sinit botnet grew, any code that was introduced would become replicated to all of the other hosts in the botnet. Furthermore, this was not akin to an underground network that anyone could log into. Access was limited through the use of special digital

keys, which carefully controlled access to it. This meant that the only person that could use the network was the person who created the Trojan or had access to the keys.

Any code that is introduced into the network in this way, either as dynamic link library or executable, may subsequently be loaded by the Trojan itself, thus making it extensible and flexible.

Although there are perhaps some limitations in the random "scatter-gun" approach these Trojans use to search for the IP addresses of other Trojans, it is only a matter of time before these algorithms are tuned to focus more carefully on local subnets before seeking IP addresses further afield.

Perhaps what makes this botnet model particularly interesting is that no matter how embryonic it may be, there is no single-point-of-failure to it in that there are no mother-ship sites that once closed leads to the end of the zombie network.

Sinit was undoubtedly created as a part of some lucrative and enterprising scheme. Although the fruits of these motives may be less clear, the primitive copies of Sinit have been around since late 2003, and its network has undoubtedly evolved considerably in that time. Some estimates have suggested a botnet in excess of tens of thousands of computers.

The unabated growth in spam and viruses has already propelled many businesses to adopt a managed email security solution. Challenged with maintaining a holistic security solution and keeping pace with the increasingly sophisticated nature of these threats has put many IT departments under pressure, in terms of resources and budget. In an age when minimising and managing acceptable levels of risk are at the forefront of today's business decisions, it becomes obvious that protecting your email results in protecting your business.

*** The information relating to MessageLabs' services contained in this newsletter is based on data generated internally by MessageLabs and has not been subject to an independent review by a third party.**

About MessageLabs Intelligence

MessageLabs Intelligence is a respected source of data and analysis for email security issues, trends and statistics. MessageLabs provides a range of information on global email security threats based on live data feeds from our control towers around the world. The information relating to MessageLabs' services contained in this report, is based on data generated internally by MessageLabs and has not been subject to an independent review by a third party.