Name of Publication: Community Times
Date of Publication: 9/3/2004
Page(s) in Publication: 30

The Viral Future

F-Secure were first to detect and warn of the Mydoom email worm. Mr. Juhani Kivela works as Regional Manager at the F-Secure Corporation's Growth Country Group and speaks about the future of malware.

The Mydoom email worm, which was identified in January this year, has already spread more than Sobig.F. The Sobig.F worm spread massively in August 2003 and until now has held the title of the fastest spreading email worm in history. Email worms are currently the most common virus type in the world. Automatic network worms can spread even faster, but they are not nearly as common. Mydoom masks infected emails to look like a system error and in addition to sending itself to email addresses found from users' files, the worm also creates new addresses by guessing common user names. Its timely release during the middle of business hours in the US also lead it to contaminate several large corporate networks.

An F-Secure Radar Level 2 Alert first warned about the Mydoom worm, the worst email worm incident in virus history, on January 26th, at 23:05 UTC. Three hours later the alert was raised to Radar 1. F-Secure shipped detection of the virus at 23:09 UTC – in 1 hours 50 minutes from the moment the first sample of the worm was received.

Based in Finland, Mr Juhani Kivela is currently responsible to manage F-Secures business in Middle East and Central & Eastern Europe. In speaking about their work in the Middle East Mr

Although Mydoom (aka Novarg) is now very widespread, it does not pose an immediate threat to infected computers. Mydoom launches a worldwide denial-of-service attack from every infected computer against the website www.sco.com, which belongs to SCO, a well-known Unix vendor. In fact, some have already nicknamed the virus 'ScoBig.' However, this attack should not affect the rest of the Internet. Mr Kivela referred to the Mydoom outbreak by saying, "In several ways. It has been the fastest spreading email worm in history. Mydoom has targeted SCO, a well know Unix vendor. A later version of Mydoom, referred to as Doomjuice is special as it infects machines which are already infected by Mydoom, does not spread over email, and instead of attacking sco.com it tries to perform an attack on microsoft.com."

> "TVs and even cars are starting to have connections to net. As soon as they are online, there will be a high risk for malicious code to be run on them too."

Current estimates show that between 20% - 30% of all email traffic worldwide is generated by this worm. F-Secure is especially urging Internet Service Providers to start dropping infected emails instead of delivering them to end users. F-Secure is releasing information for ISPs on how to reliably detect infected emails from mail queues with minimum processing power. For details, see the virus screenshots of the Mydoom worm are available in the F-Secure Virus Description Database at http://www.f-secure.com/v-descs/novarg.shtml

When speaking about how users might combat viruses on the whole, Mr Kivela said, "The big majority of viruses and worms are still spread via email attachments. An efficient way to be protected is not to open any suspicious email, especially emails coming from unknown senders should be deleted without even previewing them. Users should be careful when entering his/her email address in any unknown website; the email address should be presented clearly. In addition to up-to-date anti-virus software each user should also have personal firewall software installed. This software prevents intrusion attempts and protects against attempts to steal valuable data from the PC. F-Secure's Client Security is an integrated package that protects the user against modern combined threats." In relation to using email as a means to spread, Mr Kivela spoke about how best to combat junk email, "In the last twelve months, these email worms that are spread by junk email have been multiplied millions and millions of times and helped their propagation tremendously. Against junk emails the most efficient solution is a spam filter. The filter can locate in various parts of the network: the user workstation, corporate mail gateways or at ISP site. F-Secure will come out during next quarter with a selection of tools to reduce incoming spam."

Though viruses may appear to be predominantly associated with computer usage, there is the likelihood of their spreading to any telecommunications device (or via any telecommunications device) Mr Kivela responded to this point by saying, "Viruses can live and spread when there is transmission of data between devices who have processing and communication capabilities. As different kind of devices used by masses of people are getting more 'clever,' the probability to have problems with viruses is getting higher. The natural next target could be the smart phone. TVs and even cars are starting to have connections to net. As soon as they are online, there will be a high risk for malicious code to be run on them too."

Whether or not users will ever be in a position to effectively guard against malicious software is a point that Mr Kivela spoke about this by saying, "It seems that it will be a continual process, and it is very difficult to look at, many people are pessimistic about ever completely resolving the situation. Anti-virus software will help and