F-SECURE CORPORATION DATA SECURITY SUMMARY

July to December 2005

In the second half of the year, we can report that the trend towards mass assaults using network worms has dropped significantly with two major outbreaks, one in September causing larger disruptions internationally and the second, a worm flooding email systems in late November. Nevertheless, the virus count continued to rise with alarming force increasing from 110,000 to approximately 150, 000 by the end of the year.

July 2005 started out for data security professionals visiting the DEFCON conference in Las Vegas - the largest computer underground event in the world was held. As usual, the participants came from both sides of the fence and everything in between with thousands of black, grey and white hat hackers as well as security professionals, law enforcement members and undercover agents.

In slightly less exotic Helsinki: the Assembly'05 demo party was the scene of 5000 geeks gathering together for four days. The event was of particular interest to the data security lab specialists since many of the techniques used in demo coding are written in low-level assembler, and to fit within tight limits using really advanced compression techniques.

Overall, it was a tough year for high profile malware authors around the world, at least according to the number of convictions. In July three men in their early 20s heading an international extortion ring were arrested in raids in Russia apparently after launching big DDoS attacks from botnets against gambling sites, then emailing them and asking $50,000 for not doing it again.

Despite the money trail routing itself to Russia via the Caribbean and Latvia, the UK police were nevertheless able to trace it, leading eventually to the arrests. Various other virus authors were reached by the long arm of the law including the VBS/Lasku virus author in Finland, the Peep backdoor author arrested in Taiwan and most notoriously, the Sasser and Netsky author, Sven Janschen who equally notoriously received a thirty hour community service order and suspended sentence for creating a worm that caused damage in the millions of dollars before it was brought under control.

Spam is bad for your health

Sometimes, things are handled differently in attempting to stop the spread of malware and spam. In July, Russian media reported the owner of the American Language Center, Vardan Kushnir, had been killed. According to the reports, Kushnir had suffered massive head trauma when he was found in his apartment in Moscow. The American Language Center provides English language courses for Russian speaking people and reportedly organized the largest spam campaign in Russian history.

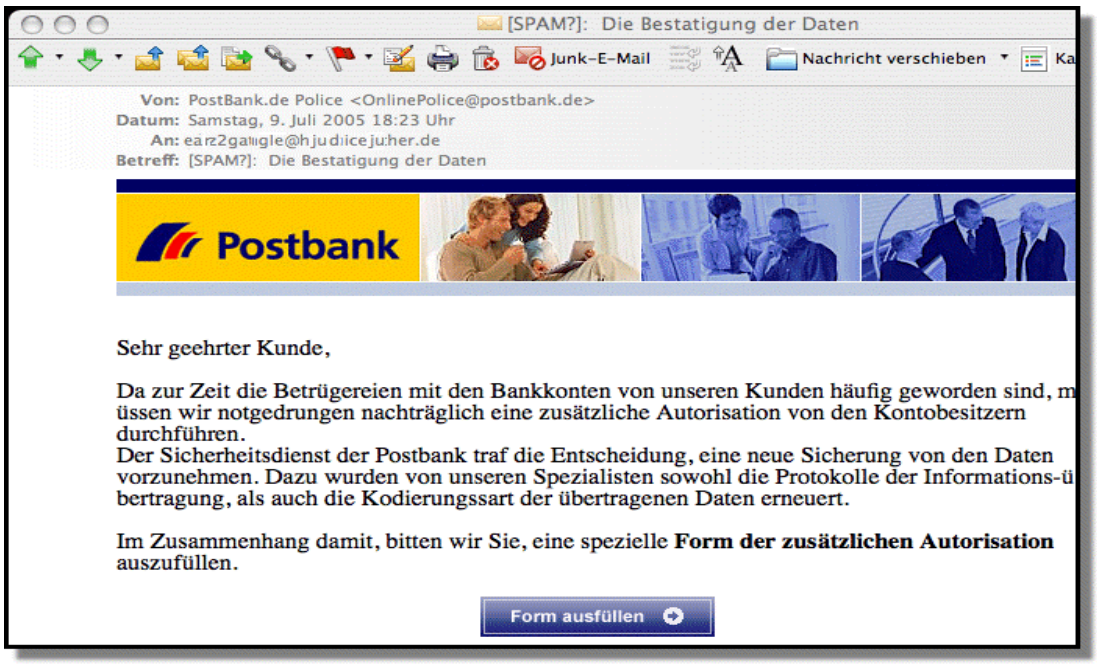
Spam was sent to over 20 million e-mail addresses belonging to Russian speaking people. The campaign was so pervasive that you can hardly find a Russian who has never received a message advertising the American Language Center. The killing of Kushnir might not, however, be related to his company’s spamming although many people might have wished him dead after receiving yet another spam email from his company. Russian authorities are currently investigating the crime with suspects in the thousands.

Phishing is obviously worth it

In July, the Financial Times Deutschland reported that German banks lost 70 million Euros due to phishing attacks over the last year and this figure is growing fast. If this is the case in one country we can extrapolate that phishing is not only big business but is also clearly worth it to the criminal fraternity.

As phishing becomes more widespread, however, so too do the authorities' ability to detect it. As a result, typical larger phishing targets, such as those made onCitibank, eBay, Paypal and US Bankhave been replaced by more focused attacks against smaller targets in order to find users who still can still be fooled to respond to a phishing email.

This has resulted, for example, in a series of attacks against German banks, with increased activity against organizations like Deutsche Bank and Postbank. As a result, both Deutsche Bank and Postbank will be introducing one-time passwords, which are needed to authorize online transactions.



There is some evidence that the criminal organizations behind phishing attacks have been jumping from one geographical area to another looking for more targets. First we saw them in the US, then in Australia and then the UK. In Germany, the attacks were localized in the German language as was the case earlier in 2005 when phishing cases localized in Danish were detected in Denmark.

It didn't take long afterwards in August for a large-scale attack against Nordea in Sweden. Nordea is the largest bank in the Nordic countries. It also operates one of the largest Internet banks in the world, with over 4 million Internet customers in eight countries.

In this particular case somebody spammed a large amount of spoofed emails with links pointing to a fake bank. Once again, the attack was localised in the target language but this time, the scam was aimed at breaking through Nordea's one-time password system.

The system in use by Nordea Sweden consists of a scratch sheet, where you scratch the paper to uncover the next available pin code for login. Attacking a site like this is quite a bit more challenging than attacking banks authenticating users with a bank account number and a constant 4-number pin code as was the case in Germany.

The fake mails explained that Nordea was introducing new security measures, which could be accessed at www.nordea-se.com or www.nordea-bank.net (both fake sites hosted in South Korea). The fake sites looked fairly real. They were asking the user for his personal number, access code and the next available scratch code. Regardless of what was entered, the site

would complain about the scratch code and ask for the next one. In reality, the phishers were trying to hook several scratch codes for their own use.

Nordea Sweden took the threat seriously and immediately shut down their whole Internet bank while they looked into the assault and immobilised it. Apparently this was done in order to prevent the scammers from using the codes to move money around.

Overall, by September, the number of phishing attempts overall had levelled out but this was also marked by an increase in the volume of spam. This marked rise appears to be caused by a large number of matchmaking spams. So it would seem that the activities of a single determined spammer can still make a difference.

Typosquatting for careless typists

Earlier this year we saw evidence of typosquatting with the Google surfers mispelling it as ‘googkle’ leading them to all manner of malware ridden sites instead. In the autumn, an even larger exploit concerning typosquatting was launched – no surprises there but the sheer scale of the domains created to trick the unwary was impressive – 150 of them, many of which were targeted to data security companies.

Among other typosquats we found:"www-f-secure.com" and "wwwf-secure.com" which at the moment point to a web site called "nortpnantivirus.com". The good news is that at least this site isn't used for phishing or for downloading trojans. Other typosquats related to security firms include the following: f-secue.com, mesagelabs.com, mcafeeantiviru.com, bitdefneder.com, pestpatorl.com, wwwbullguard.com, pandafirewall.com, sendamil.org and centralcomand.com.

Terror attacks, natural disasters and exploitation

In a year characterised by a large number of natural disasters and terror attacks, another important and regrettable trend repeated itself – members of the malware community using other people’s misery for profit.

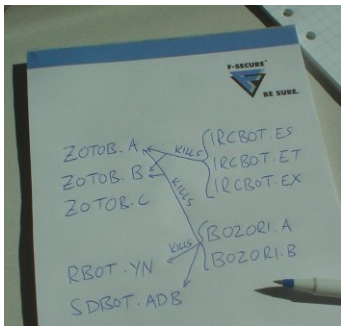
After the 9/11 attack against the World Trade Center in New York, malware was launched using the event to trick users into running malicious attachments. Just two weeks after the September attack the e-mail worm W32/Vote.A@mm was found and exactly a year after the event another e-mail worm, W32/Chet@mm, was found. While Vote.A didn't spread very well the Chet worm was widespread and prompted an F-Secure Radar 2 warning.

In July of this year, the same pattern repeated itself with the underground terrorist attack in London. Shortly after the bombing the first trojan was detected as an attachment in e-mail messages. The ZIP file contained the file "London Terror Moovie.avi <124 spaces> Checked By Norton Antivirus.exe'. F-Secure detected the trojan as 'SpamTool.Win32.Delf.h' and promptly sent out an update.

In September there were reports of a spam message with subject fields like "Katrina killed as many as 80 people". The message seems to contain a news article on the devastation caused by hurricane Katrina but actually directed the reader to a website called "nextermest.com. Further investigation reveals that the site is just a placeholder that refreshes to a page that tries to download the Trojan-Downloader.JS.Small.bq malware.

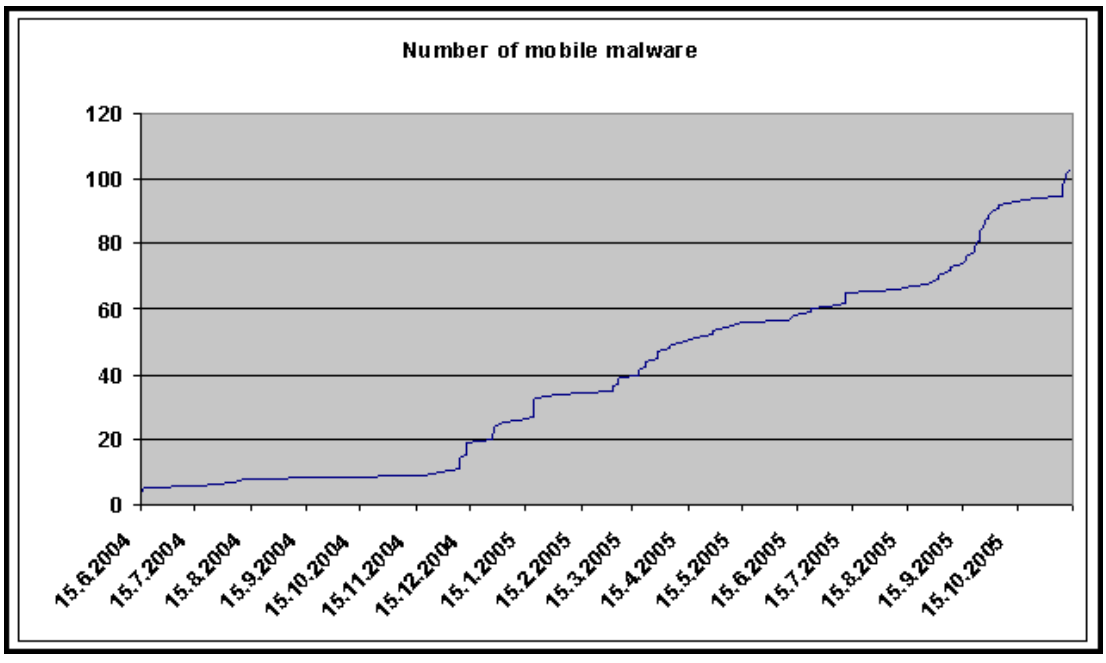
Major virus outbreak in August

In August the Data Security Laboratory in Helsinki's headquarters mapped the course of a botwar that took on the proportions of an international incident before it was stopped. It started with a new virus round about lunch exploiting a Microsoft patch vulnerability: the MS05-039 PnP hole. As the virus progressed, CNN was struck as was the Financial Times, The New York Times and ABC.



The attack which centres around the Zotob virus is also aided by assaults by bot variants which interestingly compete with each other over infected machines actively removing the resident infection and replacing it with their own. Specifically, there are two groups that are fighting: IRCBot and Bozori vs Zotobs and the other Bots.Widespread disruption, particularly in the media was eventually brought under control and F-Secure's report makes the headlines in over 500 different journals in the days that follow. Not long after the outbreak, two young men were arrested regarding the Zotob PnP worm case.Moroccan authorities arrested "Diabl0", aka Farid Essebar and Turkey authorities arrested "Coder", aka Atilla Ekici. The suspects are aged 18 and 21, respectively.

Mobile malware proliferation



Interest in mobile malware continues to grow in step with the increasing media coverage, To date, F-Secure has received an increasing number of queries about just how many known mobile malwares are out there. At the time of writing the total count has already exceeded 100 – a landmark in the progress of viruses and their assault on the mobile environment.

Symbian-related malware is the vast majority of all mobile malware. The large number just shows how popular Symbian devices are, thus making them the most interesting target for malware authors.

As all currently known Symbian trojans and worms display several warnings, it would be easy to blame any user who got phone infected for being stupid or ignorant. However, it seems that the explanation why people get infected by Cabir and other Bluetooth worms show that it is not so straightforward.

Firstly, a great deal of Symbian software requires Bluetooth to be visible in order to work properly. And some of these programs either switch on the Bluetooth without asking the user, or display the activation question in such a manner that the user is likely to answer yes.
Then there are several social networking applications that use Bluetooth such as YOU-WHO and CrowdSurfer.
Which enable people to use Bluetooth for social networking and gaming and these naturally lower the bar for accepting any connections and files from unknown persons.

And finally most Cabir variants are quite aggressive in spreading, and keep sending the Bluetooth connection request, even when the user clicks ‘no’ to them. Eventually, the user gets frustrated and start clicking yes to all questions with inevitable results.

F-Secure Mobile Anti-Virus has been able to handle 61 (74%) cases of Symbian malware with generic detection. Which means that the Anti-Virus has been able to detect and stop the malware without the need for database updates.

Commwarrior continues to spread

Nevertheless certain viruses continue to spread unchecked, most obviously the infamous Commwarrior which has now been reported in infection cases in twenty countries so far spanning from as far afield as India and South Africa.

In August F-Secure received a sample of new Symbian trojan Doomboot.A that drops Commwarrior.B and damages the phone such that it does not boot anymore. While other trojans have dropped several different Cabir variants, Doomboot.A is the first known trojan that drops Commwarrior and uses a new technique to break the phone.

Like most of the Symbian trojans Doomboot.A also pretends to be a pirate copied Symbian game. So people who don't download and install pirate copied games or applications are safe from nasty surprises.

What makes Doomboot troubling is the unpleasant combination of Doomboot and Commwarrior’s effects on the phone. The Doomboot.A causes the phone not to boot anymore and Commwarrior causes so much Bluetooth traffic that the phone will run out of battery in less than one hour. Thus the user who gets his phone infected with Doomboot.A has less than one hour to figure out what is happening and disinfect his phone, or he will lose all data.

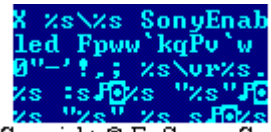
In September,an otherwise unremarkable Symbian Trojan, SymbOS/Cardtrap.A is, put a new spin on mobile malware by being able to cross infect a PC if the user inserts the phone memory card to his PC.

When infecting a Symbian phone, the Cardtrap.A copies two Windows worms (Win32/Padobot.Z and Win32/Rays) to the memory card of the phone. Padobot.Z is copied with an autorun.inf file in an attempt to start automatically if the card is inserted to a PC using Windows. Rays is copied with the filename SYSTEM.EXE and the same icon as the System folder. This is done as a social engineering technique so that the user would click on Rays instead of the System folder. Luckily, both Padobot.Z and Rays are detected by F-Secure Anti-Virus, and we have added detection and disinfection for them also for F-Secure Mobile Anti-Virus.

Viruses spread to MP3 players and game consoles

At the end of August, reports came through of a commercial MP3 player being shipped out with a virus. The manufacturer, Creative reported it had accidentally shipped almost 4000 MP3 players with a Windows virus. This happened in Japan with the 5GB Zen Neeons players. The filesystem on the players contains one file that is infected with the Wullik.B (also known as Rays.A) email worm. The worm does not, however, infect PCs unless the user browses the player's files and clicks on the infected file.

In October this was followed up by a malware alert for Sony Playstation appearing in a firmware dowgrade tool that turned out to be a trojan rendering the PSP unusable. The infamous patcher from PSP Team removes a few important system files from the flash, which makes the system unbootable. This tool has been reported to be the first "PSP virus" by many sources. Since it does not replicate in any way, however, by the F-Secure definition it can called a trojan at most. It definitely falls under the malware umbrella term, however. It is worth mentioning here that, according to Sony, running any unauthorized code on the PSP will immediately void the warranty. Hot on the heels of the first PSP Trojan in October, the data security lab received reports about the first trojan for the Nintendo DS handheld gaming console.This simple trojan, known as "DSBrick" overwrites critical memory areas, preventing the console from booting.



Back with Sony again, the big news in November was the discovery of a rootkit detected in some Sony BMG music CDs placed there by the company itself to enforce the copy control policies of its audio CDs. The rootkit, which acts as a covert method for monitoring customer behaviour through Digital Rights Management software is installed when the user inserts the CD to a Windows-based PC, and accepts a license agreement. Unknown to the user, the rootkit is installed after which, there's no direct way to uninstall it. The system also opens a possible backdoor for viruses (or any other malicious program) to use the rootkit to hide themselves. The good news is that F-Secure's BlackLight scanner introduced this year in March is able to detect both the Sony DRM rootkit system and any other malware that hides using it.

Speaking about the Sony case, Risto Siilasmaa, CEO of F-Secure said: "The real story, and the very valuable lesson, here is that many companies are linking their products to ICT technology. This means that they need to educate themselves on data security issues, build processes to handle claims of vulnerabilities, train their PR people to deal with these kinds of situation and so on. Hundreds of consumer electronics companies will find themselves in the same boat with Sony."

Also in late November F-Secure issued a Radar Level 1 alert about a New Sober variant that caused the year's largest email worm outbreak with everal millions of infected emails reported by Internet operators. The mails contained faked messages from such claimed sources as the FBI and CIA asking its recipients to open an attachment containing the Sober variant worm.

The first Sober was found in October 2003, over two years ago and F-Secure believes all 25 variants of this virus have been written by the same individual, operating from somewhere in Germany. Interestingly, the author seems to be from the old school of virus writers seeking for fame not fortune since there appears to be no clear financial motive behind the exploit.

Successful product releases and the move from software to hardware

Back in June, F-Secure released F-Secure Client Security 6.0 and, after a summer break, the reviews have started to flow in. Most significantly for F-Secure, Infoworld review of F-Secure Anti-Virus Client Security 6.0 in September put F-Secure ahead of all the major competitors in a large review.

To quote the magazine: "Support for real-time protection also varies among vendors. McAfee's, Trend Micro's, and Tenebril's versions allow the malware to install, but prevent it from executing, thus leaving it installed but neutered until a removal scan is started. Others, such as Sunbelt CounterSpy, block most malware installs while missing others, and, like Trend Micro, remove existing traces on next scan. F-Secure did the best job of preventing initial installations, blocking all spyware and malware attacks."

Also in September, F-Secure launched its flagship consumer product, F-Secure Internet Security 2006 and shipped out 42,000 boxes of the product destined for retailers across Europe. The latest version contains a wealth of new features that will undoubtedly result in favourable reviews still this year.

And also in September, F-Secure made a significant decision to change the dynamic of company production: after 17 years as a software company F-Secure started selling its first hardware product, ever.

The box is called F-Secure Messaging Security Gateway™. It's a 1U-sized rack-mountable appliance that sits next to your email server and filters spam and viruses from the message traffic, automatically. The appliance is a result of collaboration with US manufacturer Proofpoint and initial response has been favourable.