Data Security Summary
January to June 2005

White Paper
July 2005

Spam wars, PC viruses, mobile viruses, phishing and typosquatting, FS AVCS 6.0 launch and multiple awards

Despite the efforts of companies like F-Secure to eradicate spam from email servers and private mailboxes, the volumes continued to rise in the first half of 2005. Indeed, spam accounts for 85 percent of mail traffic globally, so concerted efforts on behalf of antivirus vendors and legislators to stop this modern plague are needed.

Nevertheless, Microsoft's Bill Gates made optimistic statements about eradicating spam predicting in January 2004 that technology will help us finally win the battle against spam by 2006. One of the first steps in that direction was announced by Microsoft in April 2005 with the corporation's first foray into offering data security management software – a consumer subscription service called Windows OneCare. The service is scheduled to include antivirus, antispyware, firewall, PC maintenance, and data backup and restore functionality. For its part, F-Secure welcomed the fact that the IT giant is starting to develop similar service-centric security concepts to the ones that it has successfully pioneered over the past five years.

Viruses Infections under control in first half of 2005

The virus situation is actually looking pretty good. The amount of virus outbreaks is down almost 50% compared to same time in the previous year. Nevertheless, the number of viruses has consecutively grown an average of 40 percent per year for the past two years – all this in step with the growth of spam. Industry pundits put this marked growth in relation to two phenomena, the ongoing increase in processing power allowing PC users to advertently or inadvertently propagate spam and spam scams, and the fact that more and more people have broadband connections keeping them on line potentially 24/7.

According to world famous security expert, Bruce Schneier who paid a visit to the F-Secure headquarters in May, anti virus protection is a 'done deal' equivalent to inoculating against the common cold. Despite what he described as the 'insane amount' of new viruses emerging everyday he was happy to note that the technology already exists to fight it. For F-Secure, this stands true – in its efforts to offer the best security possible the company opened two completely refurbished state of the art data security labs, the first in mid March in its San José office and the second at the end of May at its headquarters in Helsinki.

Nevertheless, black hats benefiting from cheap bandwidth, a good technology infrastructure, and poor policing in certain countries are able to launch increasingly bold exploits that aim to circumvent traditional prevention techniques.

One particular trend in malware-writing from the black hats is the rapid increase in new trojans and bots. Unlike the more indiscriminate assaults by viruses and worms, trojans can be delivered with precision to target organisations via email attachments or links to websites. Once a system is infiltrated, remote hackers can go about stealing information and planning further attacks from the inside. The stealth aspect of Trojans, meaning that they don't replicate under their own power, conceals the fact that they are significantly on the rise as a highly effective tool for criminal exploits.

Phishing is another good example of the modern criminal mind because it combines the global reach of spam messaging with the subtle psychology of the confidence trickster. In addition to the typical phishing targets, such as eBay, Paypal and large American and British banks, we're seeing a move towards smaller markets. This is probably happening as most customers of a bank like Citibank have already received a hundred different phishing messages and will not be fooled by another one.

Given the possibility that a phishing message gets past all relevant filters and into your email inbox, the only true protection is your own common sense. Recognizing the mail for what it is, the best policy is simply to delete it.

Another more sinister evolution of phishing is the term pharming or the exploitation of a vulnerability in the DNS server software that allows a hacker to acquire the Domain Name for a site, and to redirect traffic from that web site to another web site. DNS servers are the machines responsible for resolving Internet names into their real addresses - effectively the "signposts" of the Internet.

If the web site receiving the traffic is a fake web site, such as a copy of a bank's website, it can be used to "phish" or steal a computer user's passwords, PIN number or account number. So, for all on-line transactions, set the alarm bells ringing if you receive invalid server certificates especially when attempting to enter any site where you deposit confidential information or perform money transactions.

Worms, hostage-takers and bogus WLANS

At the beginning of May this year a new email worm Sober variant was reported in the wild in Europe sending variable messages in English and German. In this case, the authors were banking on the German public's interest in football, and specifically the forthcoming World Cup with some predictable results. The worm was released on the same day ticket sales for the next World Cup began. Sober.P sent a message out in German confirming successful ticketing application to the soccer world championships encouraging recipients to open an enclosed and infected file. FIFA was quick to respond with a public warning but not before its system experienced some heavy traffic as a result. The worm itself compromised thousands of PCs with reports coming in from 40 countries.

As with everything else these days, the malware community has become very adept at blending, automating and adding new layers of sophistication to their threats. In May there were reports of a data stealing Trojan called Agent.aa Trojan (aka Trojan-PSW.Win32.Agent.aa or Bancos.NL) which monitors active Internet Explorer instances. When a web page containing certain domain names is visited from an infected computer, the Trojan logs data from the web page, including key strokes and also takes screenshots of browser windows. Unsurprisingly, domain names in this particular exploit are mostly online banks but what sets this Trojan apart is the sheer volume of banks listed: 2764 different sites in total from over 100 different countries.

At the end of May there were also reports of a piece of malware that can take hostages and demand a ransom. The Trojan called Gpcode (also known as PGPCoder) encrypts user's files with certain extensions and then asks for a ransom to "fee" (decrypt) them - a good example of adapting new technology to fit a more commonly recognized model of criminal activity in the 'real world'. Luckily, Gpcode had a very simple encryption algorithm, so it was possible to create a decryptor for the encrypted files and F-Secure Anti-Virus was able to detect and decrypt files encrypted by Gpcode.

A further demonstration of the criminal mind in action to take advantage of gaps in modern technology came out in March when it was discovered at a conference in London that hackers had created malicious WLAN hotspots with a forged log-in web page. People using the hotspot to access websites automatically found themselves to be the target of malware. While the exploit came to light, it raises worrying implications on the use of free wireless hotspots for business travellers hopping from one connection to another often with important data in their laptops.

This exploit seems to be the model for more to come. With this in mind, the best way to protect yourself against such attacks, is to have up-to-date operating system and browser, with the latest anti-virus and firewall software installed. Also, it is important to have any critical connections secured over VPN, and not to use any unsecured service connection requiring your user name and password.

Also in March, F-Secure was actively engaged in promoting its new BlackLight Rootkit software at the monumental CeBIT fair in Hannover, Germany. Blacklight addresses the problem of rootkits, which allow hackers to create backdoors in systems completely under the radar of traditional anti virus software. While this exploit is not common, it has been implicated in a number of high profile corporate espionage cases in the States. Now, thanks to BlackLight technology, system administrators have a new tool in their armoury against their increasingly cunning opponents.

If only to demonstrate the impact of the new release in the malware community, a spyware manufacturer released a version of their Trojan marketing it as "Hidden from by F-Secure BlackLight Rootkit Elimination Technology!". The spyware used a simple trick: identifying the BlackLight process and not hiding from it. Never versions of BlackLight have been modified so that it can't be hidden from in this manner.

As evidence of the ingenuity of the online criminal fraternity in their attempts to trick unwary web surfers is the raise in malicious typo squatting websites. In the case in point, if you happen to mistype www.google.com (one variation being www.googkle.com) you will be lead to a site that will start a huge chain of web pages with exploits in various. As a result, the poor mistypist will have seriously malware and spyware infected computer. So, our advice to you is keep your browsers up to date and practice your touch typing.

The advance of mobile malware

Image Copyright © F-Secure Corporation

Mobile viruses continue to make news although it appears that the majority of them continue exhibit 'proof of concept' ie malware authors are putting their toe in the water to demonstrate that mobile viruses are possible. So far, the worst damage has been shown by a Trojan called Skulls, a malicious SIS file Trojan that replaces the system applications with non-functional versions, so that all but the phone's basic functionality is disabled. Once again, as evidence of malware author ingenuity, F-Secure received reports this spring of a Symbian Trojan Skulls.L that pretends to be a pirate copied version of F-Secure Mobile Anti-Virus showing a dialogue text "F-Secure Antivirus protect you against the virus. And don`t forget to update this!"

Users are advised not to download F-Secure Anti-Virus files from any other server than the official F-Secure site. For your information, all official F-Secure Anti-Virus installation packages are Symbian signed, so that when installing it, the user does not get the warning about a missing installation package signature. If you are trying to install F-Secure Mobile Anti-Virus and you get a warning about a missing signature, simply abort the install.

Equally, in spring there were numerous reports of Cabir sightings in the wild this spring in more than 23 countries, as far afield as New Zealand and Switzerland. Cabir is a worm that runs in Symbian mobile phones that support Series 60 platform. Cabir replicates over Bluetooth connections and appears in the infected phone's messaging inbox as a SIS file containing the worm. The minute the unwitting user clicks on it and chooses to install, the worm activates and starts looking for new devices to infect over Bluetooth.

More worryingly for smartphone owners is the arrival of Commwarrior – a mobile virus that spreads both via Bluetooth and MMS messages, which was first reported in the wild in Ireland already in January 2005. Commwarrior

could potentially be much bigger trouble than Cabir because of its capability to spread via MMS thus allowing it to jump from one country to another easily. Up to the first half of the year, reports on phones infected with Commwarrior came from 15 different countries, including USA, Ireland, India, Italy, Germany, The Philippines and of course, Finland.

When Commwarrior arrives via MMS, the user sees a message that contains a social engineering text and an attachment. The problem with viruses spread by MMS is the trust factor; people are more likely to open a file from someone they know thus giving the virus access to their own contacts file and ever onwards.

Commwarrior infected phones can be easily disinfected with by surfing to mobile.f-secure.com and downloading F-Secure Mobile Anti-Virus - or manually with a third party file manager. And telecom operators can scan the MMS traffic for viruses using a suitable tool, for example F-Secure Mobile Filter.

Award winning and malware conquering across the board

In the first six months of the year, F-Secure's products was awarded more than eight times in important trade magazines from around Europe as well as receiving a number of other positive reviews – all validating the excellence of F-Secure as the connoisseur's choice of anti-virus software. As a company we actively solicit the critical review of our products to enable our customers to make informed choices. Achieving awards validates the quality of our products and proves in an unbiased manner to our customers that with F-Secure they can be sure of the highest levels of protection on the market.

For all that's latest in our review successes, go to:
http://www.f-secure.com/news/awards/

And with the highest protection in mind, F-Secure launched its flagship product Anti-Virus Client Security 6 in June at the same time introducing a new approach to tackling modern day threats known as 'Behavior Adaptive Security' allowing protection to be kept at the highest level no matter how people use their computers and networks. A practical example of how this adaptive technology works is the automatic security level change when a roaming user connects his laptop to a network outside corporate premises.

Another example is the monitoring of suspicious activities beyond 'normal parameters' so that no software is allowed to take control over the computer without the users' approval. In this manner, F-Secure has created the means to anticipate security threats beyond the control of traditional anti virus prevention and raise the threshold to a new unprecedented level.

Examples of malware exploits in the first half of 2005 indicate that the malware community are ingenious in their ability to create workarounds to traditional AV solutions and invent unprecedented attacks in order to achieve their criminal goals. Based on our award-winning track record and an innovative approach to evolving security threats we are confident, however, that subsequent releases like F-Secure Anti-Virus Client Security 6.0 prove to industry specialists and customers alike that we will continue to fulfill the highest requirements in the market.

