Mobile Phones, and the MalWare threat.

Over the last 12 months, but particularly in the last 6 months, there has been a significant increase in the amount of malicious code in circulation for the mobile phone users of the world.

In the first half of 2005, more than 50 different viruses or worms were identified for mobile phone platforms. Many of these are variants on each other, and the actual number of new, original pieces of MalWare is still low.

One of the biggest reasons for the growth in the numbers has been the adoption of common operating systems across the handsets from many different manufacturers. A few years ago, mobile phones were relatively simple devices with a single function in mind, and a small, relatively obscure proprietary operating system on each one. This made it difficult for software developers outside the manufacturer themselves to develop any 3rd party products for these devices.

However, these manufacturers recognised this issue, and came up with a number of general purpose type operating systems for the new multifunction mobile phone devices that makes it easier to develop 3rd party applications. These operating systems include Symbian, the Microsoft Mobile O/S, and Linux. The fact that these general-purpose operating systems are now being used also means that it is easy for the MalWare authors to develop for these phones. In fact, many of the software development kits available for these phones make it almost as easy to develop applications for the mobile platform as for the traditional PC environment.

We are seeing many of the same techniques that started the spread of viruses and worms in the PC world being used to spread the MalWare in the mobile arena today. Most of the original viruses for PCs, and still many today, require that users execute a piece of malicious code that has been sent to them. While many would think that this would not be something that one would normally do, the statistics from the PC world tell us that many, many people will still open an email attachment, especially if the From email address looks like one they know. This piece of Social Engineering is one of the oldest tricks in the virus writers book, and the techniques used to Social Engineer the target into running the attachment are getting better.

For instance, in the case of the CommWarrior worm for the Symbian mobile phone operating system, the worm uses Social Engineering with message titles such as “MS-DOS Emulator”, “Anti-Virus Software”, SymbianOS Update”, and “Porno Images” to get the target to execute the attachment. Due to the fact that the worm uses the local contacts database in the infected phone, there is a high likelihood that targets will accept that the message is coming from someone that they know, and will open the attachment. When installed on a phone, it attempts to connect to any Bluetooth devices in range, and transfer itself. It also uses the MMS (multimedia version of SMS) interface to send itself to other contacts.

While there has been no major outbreak of a mobile phone virus or worm to date, it is widely accepted as only being a matter of time before there is one. A number of major research organisations have made statements that they expect a major outbreak to occur within the next 12-18 months.

Most of the malicious code that has appeared to date has required user intervention to execute the attachment, much the same as many of the email viruses in existence in the PC world today. User education and awareness can do a lot to limit the rate of spread of this type of malicious code. However, it will probably not be too long before we see some security vulnerabilities as we have seen in operating systems on all other platforms. If, and when, this is the case, and someone crafts a worm that exploits this vulnerability, without the user's intervention (as was the case with the highly infectious Blaster and Slammer worms), we will have a serious issue.

There is a very high density of mobile phones in countries like Ireland, and more and more of these are of the Smartphone variety. People awareness of security issues on the PC platform is getting better all the time, and there are very few PCs left today without some form of anti-virus software. A very infectious worm could infect millions of handsets around the globe in a very short space of time.

There could be a very serious negative impact as a result of this. There is only a limited amount of bandwidth within the mobile phone network, and if this is being taken up with the attempted propagation of worms and viruses, other services, including voice calls will suffer. This is a particular area for the mobile operators to focus on to ensure that emergency calls etc can still be made during a worm outbreak on the network.

Another thorny area will be that of costs. If a worm such as CommWarrior appears in a very virulent strain, and infects a large number of handsets, there is going to be a very large cost to each phone owner for all the data being transferred on the network. MMS messages are a preferred route for much of this infection, but there is also the Bluetooth connection for attempting infection. This is limited in range, and free to the owner, and as such is seen as a lower rate of infection model.

We have seen recent viruses in the PC world that are holding the owners to ransom. In these infections, the files on a PC are encrypted by the virus, and can only be accessed again after paying money to the author, who will send you the decryption key. For many, the loss of all the data on a mobile phone would be a disaster, and thus this extortion attempt is often successful.

As with PCs, a few simple steps will help keep your phone virus free. Do not open attachments, or MMS messages, even from people you know, unless you know what it is, are expecting it, and know the name of the file. Secure your Bluetooth settings on your mobile. Each phone is slightly different, but it is important not to allow unauthenticated connection attempts, and better not to broadcast. When anti-virus software becomes more readily available, investigate its use.