A Report On The Topic

“MOBILE VIRUS AND WORMS”

Submitted To : -

Sonali Madam
Kotadia

Submitted By

Bhawik
Acknowledgement

We would like to express our gratitude to all those who gave us the possibility to complete this report. We would like to appreciate the effort of the people who helped us in our report. We would like to acknowledge the labor of miss Sonali Agrawal (our teacher) for assisting us.
CONTENTS

• Introduction
• What is a Virus
• Motive to create virus
• Differences with PC virus
• Virus actions
• Case study of different viruses
• Futuristic threats
• Conclusion and recommendation
Introduction

All of us are familiar with cell phones. The use of cell phones to access internet and share executable files have increased. With the growing number of functionalities, the amount of personal data at risk is high. With the growth of the smart phone, mobile phones with Internet connectivity that work like a handheld computer, phone users have also seen the advent of the mobile phone virus. If not handled properly, it may prove to be fatal to our privacy. It is not just PCs that are vulnerable to virus attacks these days--now we also have to protect your phone from mobile phone virus and PDA, too. Advanced mobile phones run the same kind of applications as desktop and laptop computers, and they have multiple wireless connections so they too get infected by mobile phone virus and spread cell phone virus.
There are currently about 100 mobile viruses that can disable a phone or create bills of hundreds of dollars by sending pricey picture messages. The first mobile virus spreading "in the wild" emerged less than two years ago. While this is still a tiny number compared with personal computer viruses, the threat is expected to increase.

**Virus, What is it?**

A virus is a computer program that can copy itself and infect a computer without permission or knowledge of the user. It may have a negative effect, such as causing a program to operate incorrectly or corrupting a computer's memory. The term "virus" is also commonly but erroneously used to refer to other types of malware, adware, and spyware programs that do not have the reproductive ability. A true virus can only spread from one computer to another (in some form of executable code) when its host is taken to the target computer; for instance because a user sent it over a network or the Internet, or carried it on a
removable medium such as a floppy disk, CD, DVD, or USB drive. Viruses can increase their chances of spreading to other computers by infecting files on a network file system or a file system that is accessed by another computer. A worm is one that exploit security vulnerabilities to spread it to other computers without needing to be transferred as part of a host, and a Trojan horse is a program that appears harmless but has a hidden agenda. Worms and Trojans, like viruses, may cause harm to either a computer system's hosted data, functional performance, or networking throughput, when they are executed. Some viruses and other malware have symptoms noticeable to the computer user, but many are surreptitious.

MOBILE VIRUS

A mobile virus is an electronic virus that targets mobile phones or wireless-enabled PDAs. As wireless phone and PDA networks become more numerous and more complex, it has become more difficult to secure them against electronic attacks in the form of viruses or other malicious software (also known as malware). Malware is
software designed to infiltrate or damage a computer system without the owner's informed consent.

A mobile phone virus is a computer virus specifically adapted for the cellular environment and designed to spread from one vulnerable phone to another. Although mobile phone virus hoaxes have been around for years, the so-called Cabir virus is the first verified example.

Motive to create virus

Viruses are written for a variety of reasons

- Curiosity
- Challenge
• To gain wider attention
• Some new antivirus companies want to enter new market.

Differences with PC Virus

Although similar OSes are being used, differences exist:
- Large numbers of mobile users are less “tech literate”.
- Implies that it is difficult to “rollout security patches” to phones already sold.
- Mobiles are always “connected” and switched on.
- “Environment” keeps changing as the user keep changing its mode of using cell phones.

Cell phones also have OS
Symbian OS
Windows Mobile
Palm OS
J2ME
Linux based
Blackberry based

Virus Actions
• Send SMS & MMS to all numbers found within mobile phone.
• Damage by deleting & modifying mobile phone.
• Starting to make calls to pay-per-minute numbers.
• Prevents phone from booting.
• Drains phone’s battery.

Case Studies
First symbian virus: CARIBE

CommWarrior (MMS : worm)

Caribe (blue tooth : worm)

Skuller (Most numerous family,OS vulnerability : Trojans)
In 2004 a group of professional virus writers known as 29A created the first virus for smartphones called Caribe. Caribe is the first network worm capable of spreading via Bluetooth. It infects mobile phones which run Symbian OS. Creators stated it was purely proof of concept just to show malicious code could be created for Symbian OS. Source code was published on the Internet → many modified version surfaced.
Most dangerous
Symbian virus: COMWAR

The second worm found for mobile devices was the Comwar. The worm spread via Bluetooth and MMS. The executable worm file is packed into a Symbian archive (*.SIS). Once launched the worm will search for accessible Bluetooth devices and send the infected .SIS archive under a random name to these devices.
The Skuller Trojan

Skuller was the first real Trojan for the Symbian OS. The Trojan appeared as a program which would offer new wallpapers and icons for Symbian OS. Installing the program led to the standard application icons to be replaced with a skull and crossbones. At the same time it would overwrite the original application → application ceased to work. Once the smartphone has been infected it caonly be used to make calls.
How skuller works?

Classification (examples)
<table>
<thead>
<tr>
<th>Name</th>
<th>Date</th>
<th>OS</th>
<th>Functionality</th>
<th>Technology used</th>
<th>Number of variants</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Worm.SymbOS.Cabir</strong></td>
<td>June 2004</td>
<td>Symbian</td>
<td>Spreads via Bluetooth</td>
<td>Bluetooth</td>
<td>15</td>
</tr>
<tr>
<td><strong>Virus.WinCE.Duts</strong></td>
<td>July 2004</td>
<td>Windows CE</td>
<td>Infects files</td>
<td>(File API)</td>
<td>1</td>
</tr>
<tr>
<td><strong>Backdoor.WinCE.Brador</strong></td>
<td>August 2004</td>
<td>Windows CE</td>
<td>Provides remote network access</td>
<td>(Network API)</td>
<td>2</td>
</tr>
<tr>
<td><strong>Trojan.SymbOS.Mosquit</strong></td>
<td>August 2004</td>
<td>Symbian</td>
<td>Sends SMS messages</td>
<td>SMS</td>
<td>1</td>
</tr>
<tr>
<td><strong>Trojan.SymbOS.Skuller</strong></td>
<td>November 2004</td>
<td>Symbian</td>
<td>Replaces files, icons, system applications</td>
<td>OS vulnerability</td>
<td>31</td>
</tr>
<tr>
<td><strong>Worm.SymbOS.Lasco</strong></td>
<td>January 2005</td>
<td>Symbian</td>
<td>Spreads via Bluetooth, infects files</td>
<td>Bluetooth, File API</td>
<td>1</td>
</tr>
<tr>
<td><strong>Trojan.SymbOS.Locknut</strong></td>
<td>February 2005</td>
<td>Symbian</td>
<td>Installs corrupted applications</td>
<td>OS vulnerability</td>
<td>2</td>
</tr>
<tr>
<td><strong>Trojan.SymbOS.Dampig</strong></td>
<td>March 2005</td>
<td>Symbian</td>
<td>Replaces system applications</td>
<td>OS vulnerability</td>
<td>1</td>
</tr>
<tr>
<td><strong>Worm.SymbOS.ComWar</strong></td>
<td>March 2005</td>
<td>Symbian</td>
<td>Spreads via Bluetooth and MMS, infects files</td>
<td>Bluetooth, MMS, File API</td>
<td>7</td>
</tr>
</tbody>
</table>
Futuristic Developments

- Location Tracking
- Camera and Microphone Bug
- Leaking Sensitive Information
- DDOS attack on Mobile Service Provider
Common protection against mobile malware

1) Non-discoverable Bluetooth - Switch to Bluetooth hidden mode. If your phone has Bluetooth capability, ensure that the Bluetooth capability is switched to hidden or invisible mode unless you specifically need it to be visible. This will help prevent other Bluetooth-enabled devices from finding your phone (unless you grant them the necessary permission) and will therefore help protect your phone from worms that spread using the Bluetooth wireless technology.

2) Install antivirus

3) Firmware Updates.

4) Don’t use untrusted sites & softwares.

5) Infection Scanners at public locations.
What is Antivirus?

Antivirus software are computer programs that attempt to identify, neutralize or eliminate malicious software. Antivirus mainly prevents and removes computer viruses, including worms and trojan horses.

WE RECOMMEND

- Kaspersky
- F-Secure
- McAfee
CONCLUSION

We should not accept files from unknown people without confirmation. We should not download unknown files from internet. Since the advent of the Internet, computer virus hoaxes have competed with computer viruses. The same is true of the mobile phone virus. There are real hoaxes, just as there are real viruses. One recent one had folks believing that calls from Pakistan to Afghanistan would transmit an actual physical virus that could cause users to become sick. Mainly, we simply need to be worried about the viruses that might make
our mobile phone sick. Installing antivirus programs makes good sense, especially if we want to keep our smart phones healthy. There are so many antivirus applications for PocketPC, Symbian Series 60, Windows Mobile are already available in market.

REFERENCES

• www.viruslist.com
• www.mobile.f-secure.com
• www.free-av.com
• www.zdnet.com.au
• www.scribd.com
• www.physorg.com
• www.hoax-slayer.com/mobile-phone-virus-hoax.html
• www.wisegeek.com
• Operating system principles