

Malicious Code & Wireless Networks



By: Brett L. Neilson
hamcom@brettneilson.com



Who am I?

- Brett L Neilson – KC7IIB
- Author
 - Maximum Wireless Security
 - Maximum Security 4th Edition
- By Day
 - Networking Security Professional
 - Intrusion Prevention
 - RF Field Technician Systems Admin



Overview

- Wireless technology, networks & devices
- Defining wireless threats
- Why malicious code will spread on wireless networks
- Economic impact & potential damages
- Protecting against malicious threats

Wireless technology & networks

What is wireless?

- Merriam Webster says:
 - Wireless: *adjective*
 - 1: Having no wire or wires
- Basic Components of a wireless system
 - Antenna
 - The conduit of sorts
 - Transmitter
 - Sends the RF
 - Receiver
 - Receives the RF

So who is using it?

- Everybody
 - TV / Radio / Satellite
 - Police / Fire / EMS
 - Cell Phones / Pagers
 - Building access cards
 - Automatic Toll Collection (Toll Tags)

Mobile Data Terminals (MDT)

- Very popular with Police and Fire
- Allows instant access to dispatcher data
- More secure???
 - Up until recently legal to monitor
- New features include
 - Live video monitoring



Cellular Technologies

1G (First Generation)

- 1983 to present
- Analog cellular service
- Voice only

2G (Second Generation)

- 1995 to present
- Digital / PCS Services
- Data speeds (9.6 – 19Kbps)
- Text messaging

2.5G (Not quite 3G)

- 2001 to present
- Digital / PCS Services
- Data speeds (56Kbps)
- Email messaging

3G (Third Generation)

- 2002 and beyond (In progress)
- Data speeds (144+Kbps)
- Video and Audio

802.11 Networks


802.11 1 to 2 Mbps 2.4 GHz	802.11a 54 Mbps 5.15-5 GHz
802.11b 11 Mbps 2.4 GHz	802.11g 20 Mbps 2.4 GHz

Wireless Devices

- PDA
 - Palm & iPAQ
 - Strong Growth in 2000
 - Slowly shrinking thereafter
 - Renewed interest due to advances
 - New suppliers entering the market
- Converged Devices
 - PDA & Phone combined into one
 - All the features w/ all the connectivity
 - Designed for size not security
- Wireless (Security) Cameras
- RFID devices



Defining the wireless threats

- WarDriving
 - Searching and Logging
- Data Snooping
 - Capturing data
- Jamming
 - Disrupting legitimate signals
- Insertion Attacks
 - Unauthorized clients and APs
 - AirSnarf – The Shmoo Group (DC11)
 - Control AP 

Defining the wireless threats

- Malicious Code
 - Virus
 - A piece of code that can replicate itself
 - SMS - URLs & Attachments
 - Worm
 - A program that can copy itself to other disks
 - Masquerades as valid program
 - Trojan
 - A program that launches other programs or code
 - Bundled with a valid program

The Big Virus War

Variant	Virus		
	<u>Bagle</u>	<u>Mydoom</u>	<u>Netsky</u>
A	01/23/04	01/27/04	02/16/04
B	02/17/04		02/18/04
C	02/27/04		02/25/04
D	02/28/04		02/29/04
E	02/28/04	02/16/04	03/01/04
F	03/01/04	02/24/04	03/02/04
G	03/01/04	03/03/04	03/04/04
H	03/02/04	03/03/04	03/05/04
I	03/02/04	04/13/04	03/07/04
J	03/02/04	04/16/04	03/08/04
K	03/03/04		03/08/04
L	03/09/04		03/10/04
M	03/11/04		03/11/04

Variant	Virus		
	<u>Bagle</u>	<u>Mydoom</u>	<u>Netsky</u>
N	03/13/04		
O	03/13/04		03/17/04
P	03/15/04		03/21/04
Q	03/18/04		03/29/04
R	03/18/04		03/31/04
S	03/18/04		04/05/04
T	03/18/04		04/06/04
U	03/26/04		04/08/04
V	03/29/04		04/15/04
W	04/05/04		04/16/04
X	04/19/04		04/20/04
Y			04/20/04
Z			04/21/04

Emerging threats

- Liberty Trojan (PLAM) - September 2000
 - Deleted applications and was unable to replicate itself
- Timophonica (Spain) - January 2001
 - First automatic dialer
- 911 - April 2001
 - Caused phones to repeatedly dial 911
 - Sent to over 100,000 phones
- Flooder - August 2001
 - Sends unwanted SMS messages
- Phage & Vapor – September 2001
 - Deletes files and hides applications

Why Malicious Code will spread

Why Malicious Code will spread...

- In nature, viruses infect all organisms, even the tiniest bacteria.
 - Small Pox, Plague, SARS
- Likewise, computer viruses infect all platforms that reach any level of sophistication.
 - Melissa, LoveBug, Klez, SQL-Slammer

Four main factors

- 1) Protection is poor or non-existent
- 2) Power of new devices
- 3) Standardization of networks
- 4) Increased connection of devices

Protection is poor or non-existent

- Very little built in protection
 - Nokia 9000 series has malicious code protection
 - Other vendors are working on solutions
- Data transmissions are protected but unchecked
 - Currently no carrier has the ability to scan SMS or MMS delivery servers for malicious code.
 - Current security only offers limited protection and next to no scanning abilities

Power of new devices

- PDAs are now able to run PC like applications
 - Increased power means increased automation
 - Automation is often targeted by virus writers.
- Devices are often synchronized on a regular basis
 - Thus opening a door for the spread of malicious code
- Common language for developing apps
 - Makes it easier to create malicious code

Standardization of networks

- The more standard the easier malicious code will spread
 - Same as in the wired world
- The trend is moving away from proprietary standards and is focusing more on protocol (TCP/IP) related standards
- Email messaging standards brought us Melissa and LuvBug
 - Standardized wireless networks are sure to do the same

Increased connection of devices

- More connectivity than ever
 - Bluetooth
 - WiFi 802.11
 - Cellular
- Allows for multiple ways to the internet and email
- Increased SMS/MMS popularity and exposure due to links and attachments

Economic Impact and Potential Damages

Damages

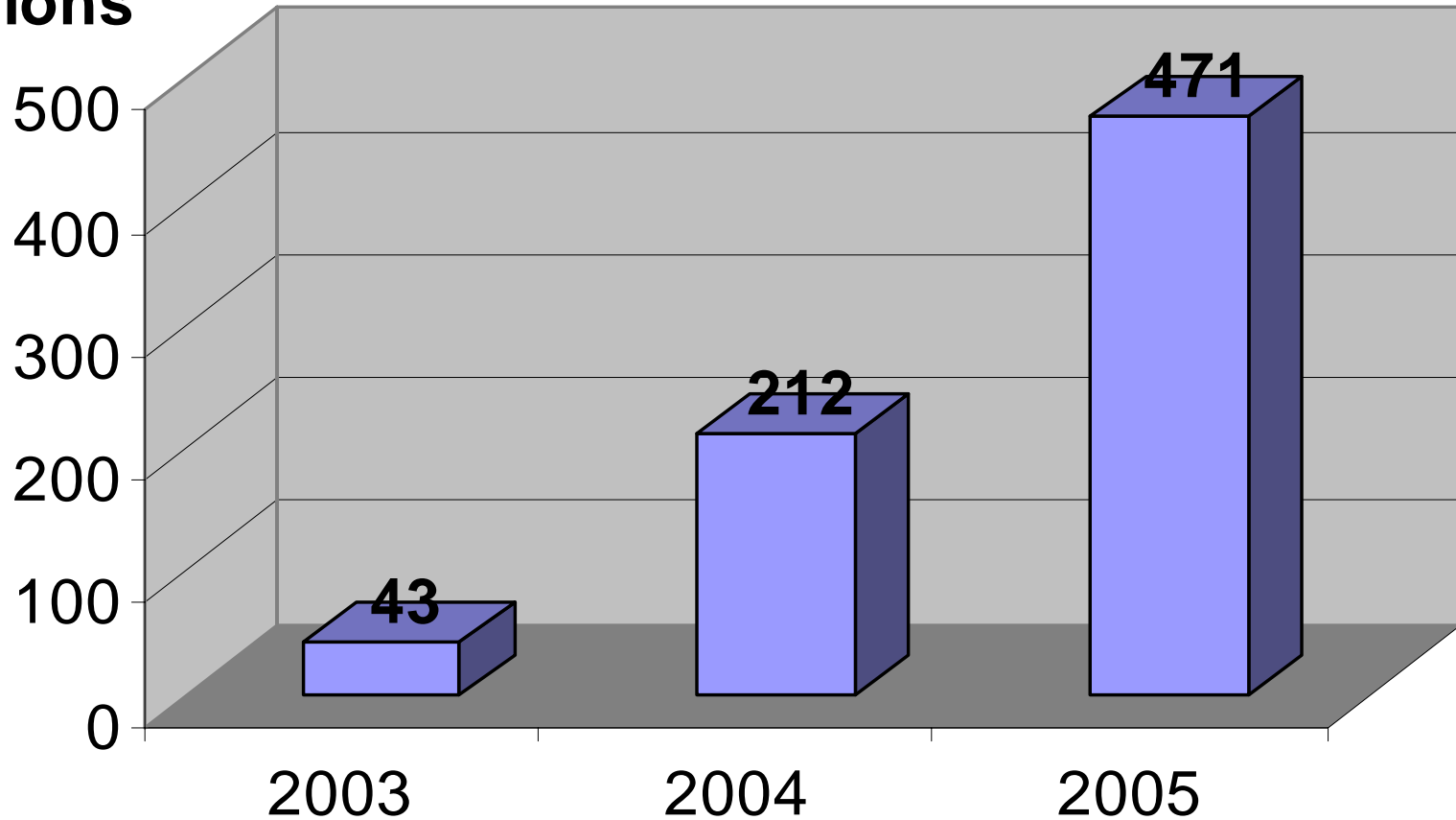
- Users receive unwanted messages
- Some devices send unwanted messages
- Data in devices is erased, deleted or stolen
- Device becomes unusable
- Network slowdowns (congestion)
- Network performance suffers
- Network intrusion

Impact

- Customer complaints
- Higher turnover from unhappy customers
- Cost from unwanted traffic
 - May not be just dollars
- Dropped calls & sessions
- Un-infecting or cleaning devices & servers/network
- Purchasing new technology

So what's the financial impact?

Millions



Gartner 2003



So what needs to be done?

Protecting against malicious threats

- Protection must be implemented at every point possible
 - Devices, Switches, Towers, COs, Access Points, etc.
- Mobile operators & administrators need to start offering scanning services to their clients and need to start scanning their servers and data streams.
 - Already happening in the broadband (DSL & Cable) realm
 - Yet to be seen in the WISP market
- Delivering a solution now rather than latter could save millions of dollars in lost revenue and expenses.
 - AV Vendors & Coders need to start step up to the plate
- Mobile operators, network administrators & device manufactures need to have plans for addressing thousands if not millions of simultaneous infections on their networks. (Nachi, SQLSlammer)

Conclusion

- Top four reasons malicious code will spread
 1. Current protection of wireless networks/devices is minimal
 2. Increased computing power of devices
 3. Standardization
 4. Growing connectivity options
- Not changing security could result in large economic losses
 - \$471 Million per 5 Million users estimated for 2005
- Mobile Operators, Administrators, Manufactures and Developers should act now and think proactively in a effort to better protect their systems and infrastructure.

Malicious Code & Wireless Networks



By: Brett L. Neilson
hamcom@brettneilson.com

