

# Мобильные угрозы. Вчера, сегодня, завтра

**Андрей Никишин**  
«Лаборатория Касперского»  
Директор направления



F

Closest 14 discoverable bluetooth devices  
(currently 106 devices in range, total 5042)

- #
- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.
- 9.
- 10.
- 11.
- 12.
- 13.
- 14.

- Nokia Smart Phone
- Lifebook T4010  
Laptop
- Nokia 6310mj  
Cellular
- Nokia Eric  
Cellular
- Nokia 6680mj  
Nokia Smart Phone
- Nokia 6630 david  
Nokia Smart Phone
- 703SH  
Cellular
- K700i  
Sony Cellular
- Nokia 6310i  
Cellular
- Gentoo-Linux rulez  
Nokia Smart Phone
- Dsilva  
Cellular
- Volkmar2  
Nokia Smart Phone
- diva  
Computer
- Nokia 6230i  
Nokia Cellular

Bluetooth viruses  
11 files received)

irus name

- 1.
- 2.
- 3.

- ;/Commwarrior.B  
1 infected devices  
10-Mar-2006 09:31:57  
(00:0e:ed:b2:a2:b3)
- SymbOS/Skulls.A  
1 infected devices  
09-Mar-2006 10:31:45  
(00:0e:ed:b2:a2:b3)
- EICAR test file  
1 infected devices  
08-Mar-2006 18:36:06  
(00:60:57:9f:aa:db)

11-Mar-2006 12:02:16

11-Mar-2006 12:02:22 - btaddr: | names | both - 11213

Search for discoverable devices: Enabled (Disable) Bluetooth Honeypot: Enabled (Disable) Alert infected phones: Disabled (Enable)

# Сегодня. Москва

## ❖ 12 марта (2 часа)

- Маршрут от м.Пушкинская по Тверской, внутри Охотного ряда, затем пешком на Новый Арбат и до м.Баррикадная.
- Найдено 199 устройств с включенным ВТ

## ❖ 17 марта (2 часа)

- Метро, с 9-30 утра. От Сходненской до Новокузнецкой, затем час в Министерстве Печати и обратно на метро до Сходненской (11-11:30)
- Найдено 101 устройство

# Сегодня. Москва

## ❖ Устройства по типам

- 158 **Phone/Mobile**
- 95 **Phone/Smart phone**
- 20 **Phone/Cordless**
- 7 Computer/Palm sized PDA
- 5 **Audio-Video/Hands free**
- 4 Computer/Laptop
- 4 Computer/Desktop
- 2 Imaging/Printer
- 2 Phone/Uncategorised
- 1 **Audio-Video/Headset**
- 1 Computer/Handheld PDA
- 1 Phone/Wired modem or voice gateway

## ❖ Доступные сервисы

- Audio - 16
- Capturing - 18
- Limited discoverable mode - 3
- Networking - 150
- **Object Transfer - 291**
- Rendering - 5
- **Telephony - 271**

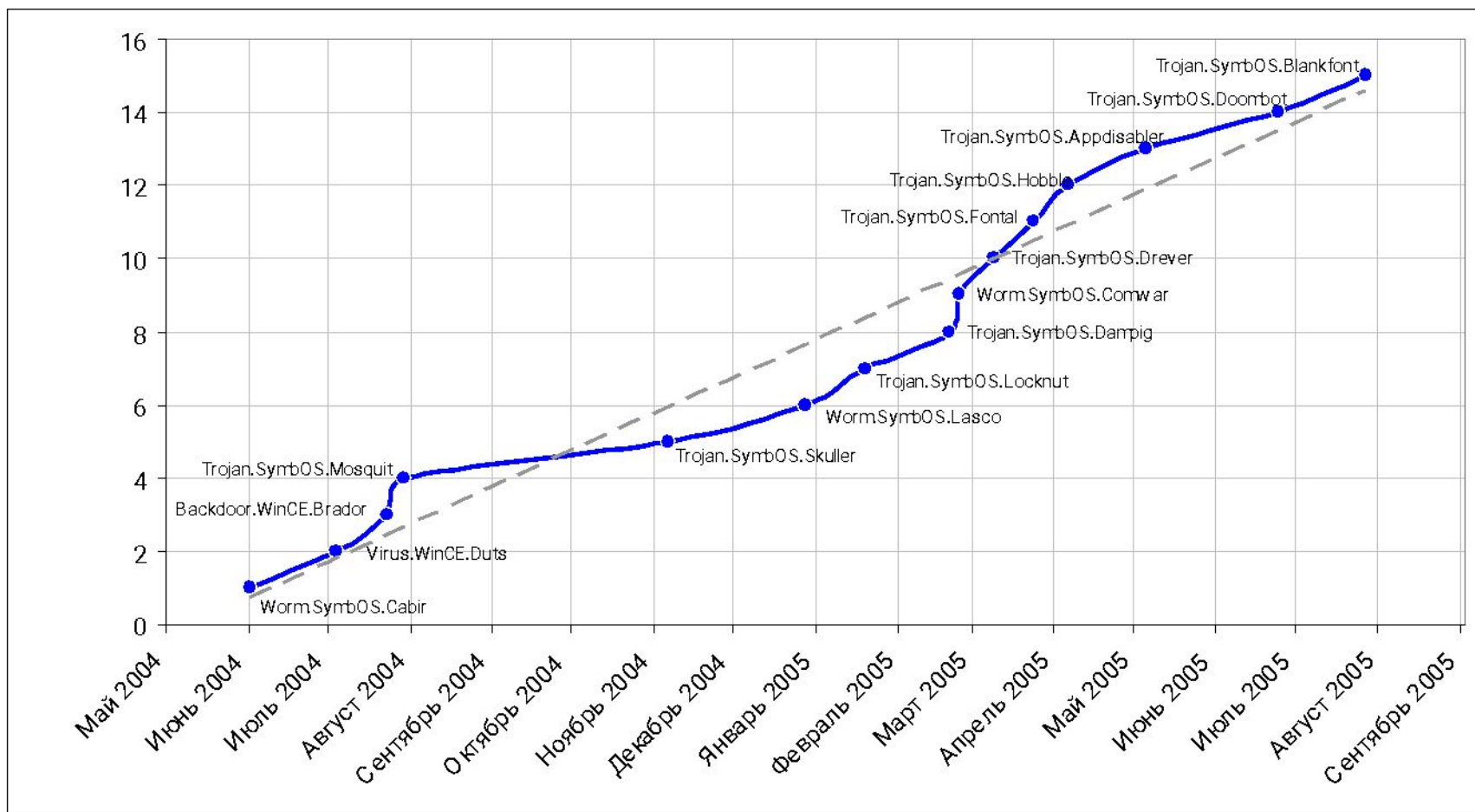
# Вчера

- ❖ Июнь 2004
- ❖ Worm.SymbOS.Cabir
- ❖ Автор – член хакерской группы 29A Vallez
  - Цель – показать возможность создания вредоносной программы для смартфонов
  - Распространяется через BlueTooth
  - Symbian OS

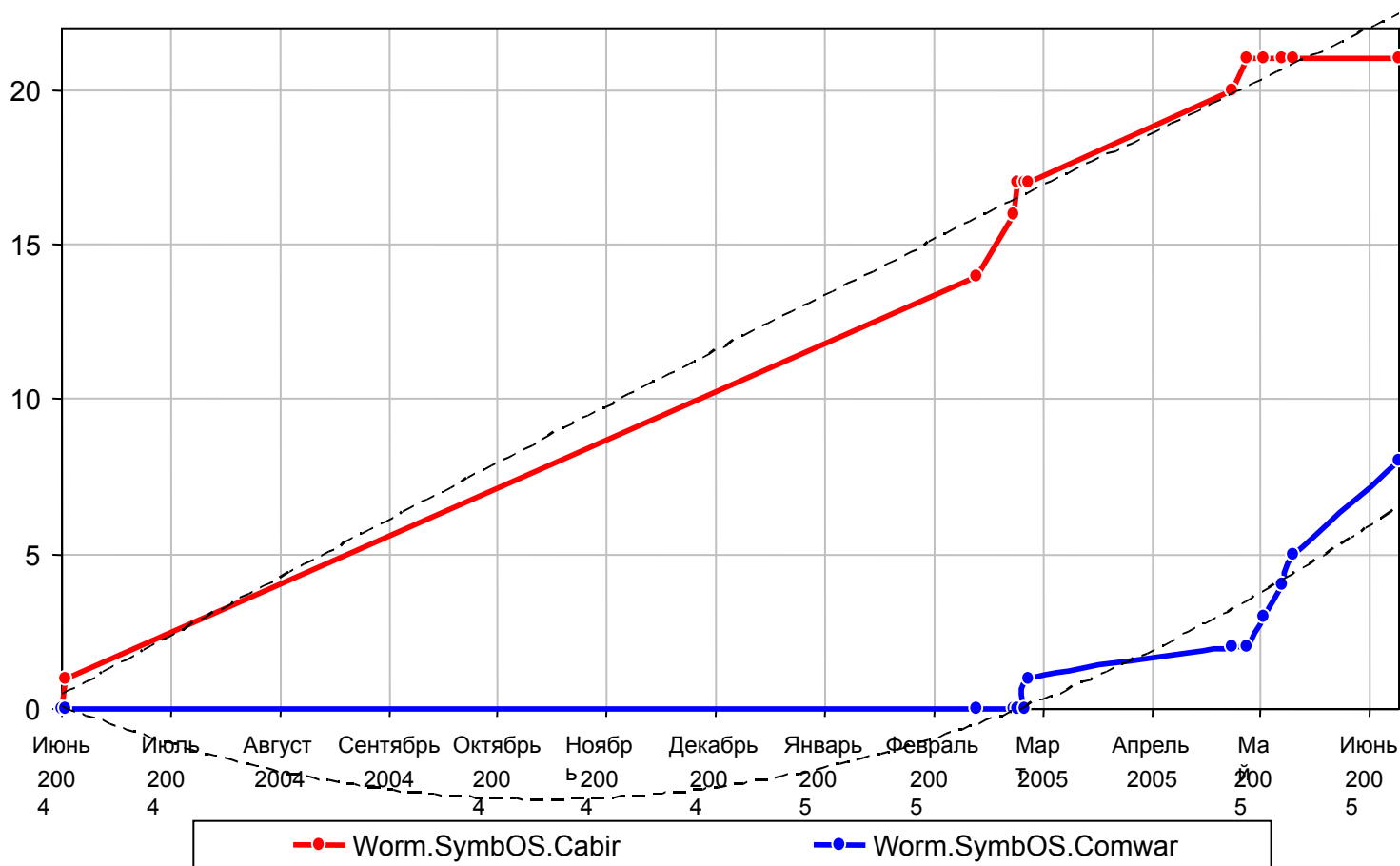
# Сегодня

- ❖ Более чем 20 семейств червей и вирусов
- ❖ Более сотни вариантов
- ❖ В среднем 10 новых троянов в неделю

# Количество семейств мобильных вредоносных программ



# Количество стран\*, в которых встречались зараженные смартфоны





# Что делают вредоносные программы

❖ Распространяются через Bluetooth, MMS

❖ По

❖ За

❖ Да

❖ Из

❖ пр

❖ Ус

❖ шр

❖ Борются с антивирусами

❖ Устанавливают другие вредоносные программы

❖ Блокируют работу карт памяти

❖ Воруют информацию



НОМ

# Сегодня

- ❖ Январь 2005. Первый зараженный смартфон в Москве
- ❖ Август 2005. Заражен смартфон сотрудника
- ❖ Декабрь 2005 – Январь 2006. Примерно 10 инцидентов с Sabir среди наших сотрудников



РЕ

ДЕ

РА

ОД

Т

НО

ВЭ



Buy It

PDF SPEC SHEET

\*Connectivity features require the use of a Beyond iCEBOX and a SANI Network Card, sold separately



# Вопросы, пожалуйста

**Андрей Никишин**  
«Лаборатория Касперского»  
Директор направления