Операционные системы

Антивирусные технологии

Вирус. Flame

- Обнаружен в 2012
- Количество инфицированных ~1000
- Текущий статус – неактивен
- Комплексная программа по кибер-шпионажу

Вирус. NetTraveler

- Заражено 350 целей в 40 странах мира (гос структуры)
- Основная цель – кибершпионаж
- Текущий статус - активен

Вирус. Stuxnet

- Червь
- Количество инфицированных 300 000
- Использовал 4 0-day уязвимости
- Имел валидную цифровую подпись
- Статус-неактивен
- Перехват и модификация трафика между контроллерами

Вирус. Flashfake

- Категория – троян/ботнет
- Количество зараженных 700 000
- Статус – детектируется и нейтрализуется

Вирус. The Mask/Coreto

- Мультиплатформенное вредоносное ПО для кибершпионажа
- 380 зараженных пользователей из 31 страны среди гос структур

Вирус. ZEUS

- Количество инфицированных более 15 миллионов
- Статус – активна. Угроза детектируется и устраняется, но выходят постоянно новые версии этой угрозы
- Онлай-банкинг троян/ботнет
- Заражение мобильных ОС (Android, Blackberry)
- Первые случаи распространения были произведены через социальные сети
- “Thanks to KAV and to Avira for new quests, i like it! NOD32 and SAV is stupid!”

Антивирусное ПО

Антивирус «Лаборатории Касперского»

- KAV
- KIS
- KES
- LA
- WSEE (Windows Servers Enterprise Edition)
- CIP (Critical Infrastructure Protection)

ODS (On-demand scan)

- Сканирование выбранных областей
- Запуски по расписанию
- Оптимизации сканирования уже обработанных файлов (iChecker, iSwift)

OAS (On-Access scan)

- Сканирование только при обращении к файлам
- Оптимизации сканирования
- Информирование, удаление, дизенфекция

Anti-Rootkit

- Возможность запуска и установки антивируса на зараженном компьютере
- Уничтожение rootkit’ов

DeviceControl

- Набор правил по работе с флеш-устройствами

HIPS (Host-based Intrusion Prevention System)

- Система возможных прав для приложений
- Система групп приложений (доверенные, ограниченные, сильно ограниченные, недоверенные)

Firewall

- Отслеживание входящего и исходящего трафика

Active disinfection

WebAv + WebControl + MailAv

- Отслеживание скачиваемых файлов
- Ограничение трафика по типу контента
- Просмотр трафика почтовых клиентов

Система обновления антивируса

- Обновление баз антивируса
- Обновление самого антивируса

System watcher

KSN (Kaspersky security network)