Тема 12. Поняття антивірусної програми. Огляд найпоширеніших антивірусних програм та їх класифікація.

Поняття антивірусної програми

Антивірусна програма (антивірус) — програма для знаходження і лікування програм, що заражені комп'ютерним вірусом, а також для запобігання зараження файлу вірусом.

Перші, найпростіші антивірусні програми з'явилися майже одразу після появи вірусів. Зараз розробкою антивірусів займаються великі компанії. Як і в творців вірусів, у цій сфері також сформувались оригінальні засоби — але вже для пошуку і боротьби з вірусами. Сучасні антивірусні програми можуть знаходити десятки тисяч вірусів.

Антивірусне програмне забезпечення складається з комп'ютерних програм, які намагаються знайти, запобігти розмноженню і видалити комп'ютерні віруси та інші шкідливі програми.

З усіх методів антивірусного захисту можна виділити дві основні групи:

- ***Сигнатурні методи*** - точні методи виявлення вірусів, засновані на порівнянні файлу з відомими зразками вірусів
- ***Евристичні методи*** - приблизні методи виявлення, які дозволяють з певною вірогідністю припустити, що файл заражений.

Слово сигнатура в даному випадку є калькою на англійське signature, що означає "підпис" або ж у переносному розумінні "характерна межа, щось ідентифікуюча". Власне, цим все сказано. Сигнатурний аналіз полягає у виявленні характерних ідентифікуючих рис кожного вірусу і пошуку вірусів шляхом порівняння файлів з виявленими рисами.

Сигнатурою вірусу вважатиметься сукупність рис, що дозволяють однозначно ідентифікувати наявність вірусу у файлі (включаючи випадки, коли файл цілком є вірусом). Всі разом сигнатури відомих вірусів складають антивірусну базу.

Задачу виділення сигнатур, як правило, вирішують люди - експерти в області комп'ютерної вірусології, здатні виділити код вірусу з коду програми і сформулювати його характерні риси у формі, найбільш зручній для пошуку. Як правило - тому що в найбільш простих випадках можуть застосовуватися спеціальні автоматизовані засоби виділення сигнатур. Наприклад, у разі нескладних по структурі троянів або черв'яків, які не заражають інші програми, а цілком є шкідливими програмами.

Практично в кожній компанії, що випускає антивіруси, є своя група експертів, що виконує аналіз нових вірусів і поповнює антивірусну базу новими сигнатурами. З цієї причини антивірусні бази в різних антивірусах відрізняються. Проте, між антивірусними компаніями існує домовленість про обмін зразками вірусів, а значить рано чи пізно сигнатура нового вірусу потрапляє в антивірусні бази практично всіх антивірусів. Кращим же антивірусом буде той, для якого сигнатура нового вірусу була випущена раніше всіх.

Одна з поширених помилок щодо сигнатур полягає в тому,що кожна сигнатура відповідає рівно одному вірусу або шкідливій програмі. І як наслідок, антивірусна база з великою кількістю сигнатур дозволяє виявляти більше вірусів. Насправді це не так. Дуже часто для виявлення сімейства схожих вірусів використовується одна сигнатура, і тому вважати, що кількість сигнатур рівна кількості вірусів, що виявляються, вже не можна.

Співвідношення кількості сигнатур і кількості відомих вірусів для кожної антивірусної бази своє і цілком може опинитися, що база з меншою кількістю сигнатур насправді містить інформацію про більшу кількість вірусів. Якщо ж пригадати, що антивірусні компанії обмінюються зразками вірусів, можна з високою часткою упевненості вважати, що антивірусні бази найбільш відомих антивірусів еквівалентні.

Важлива додаткова властивість сигнатур - точне і гарантоване визначення типу вірусу. Ця властивість дозволяє занести в базу не тільки самі сигнатури, але і способи лікування вірусу. Якби сигнатурний аналіз давав тільки відповідь на питання, є вірус чи ні, але не давав би відповіді, що це за вірус, очевидно, лікування було б не можливе - дуже великим був би ризик зробити не ті дії і замість лікування отримати додаткові втрати інформації.

Інша важлива, але вже негативна властивість - для отримання сигнатури необхідно мати зразок вірусу. Отже, сигнатурний метод непридатний для захисту від нових вірусів, оскільки до тих пір, поки вірус не потрапив на аналіз до експертів, створити його сигнатуру неможливо. Саме тому всі найбільш крупні епідемії викликаються новими вірусами. З моменту появи вірусу в мережі Інтернет до випуску перших сигнатур зазвичай проходить декілька годин, і весь цей час вірус здатний заражати комп'ютери майже безперешкодно. Майже - тому що в захисті від нових вірусів допомагають додаткові засоби захисту, розглянуті раніше, а також евристичні методи, використовувані в антивірусних програмах.

Якщо сигнатурний метод заснований на виділенні характерних ознак вірусу і пошуку цих ознак у файлах, що перевіряються, то евристичний аналіз ґрунтується на (вельми правдоподібному) припущенні, що нові віруси часто виявляються схожі на які-небудь з вже відомих. Постфактум таке припущення виправдовується наявністю в антивірусних базах сигнатур для визначення не одного, а відразу декількох вірусів. Заснований на такому припущенні евристичний метод полягає в пошуку файлів, які не повністю, але дуже близько відповідають сигнатурам відомих вірусів.

Позитивним ефектом від використання цього методу є можливість виявити нові віруси ще до того, як для них будуть виділені сигнатури. Негативні сторони:

- Вірогідність помилково визначити наявність у файлі вірусу, коли насправді файл чистий - такі події називаються помилковими спрацьовуваннями.
- Неможливість лікування - і через можливі помилкові спрацьовування, і через можливе неточне визначення типу вірусу, спроба лікування може привести до більших втрат інформації, чим сам вірус, а це неприпустимо.
- Низька ефективність - проти дійсно новаторських вірусів, що викликають найбільш масштабні епідемії, цей вид евристичного аналізу малопридатний.

Інший метод, заснований на евристиці, виходить з припущення, що шкідливі програми так чи інакше прагнуть завдати шкоди комп'ютеру. Метод заснований на виділенні основних шкідливих дій, таких як, наприклад:

- Видалення файлу
- Запис у файл
- Запис в певні області системного реєстру
- Відкриття порту на прослуховування
- Перехоплення даних що вводяться з клавіатури
- Розсилка листів та ін.

Зрозуміло, що виконання кожної такої дії окремо не є приводом рахувати програму шкідливою. Але якщо програма послідовно виконує декілька таких дій, наприклад, записує запуск себе ж в ключ автозапуску системного реєстру, перехоплює дані, що вводяться з клавіатури і з певною частотою пересилає ці дані на якусь адресу в Інтернет, означає, що ця програма щонайменше підозріла. Заснований на цьому принципі евристичний аналізатор повинен постійно стежити за діями, які виконують програми.

Перевагою описаного методу є можливість виявляти невідомі раніше шкідливі програми, навіть якщо вони не дуже схожі на вже відомі. Наприклад, нова шкідлива програма може використовувати для проникнення на комп'ютер нову вразливість, але після цього починає виконувати вже звичні шкідливі дії. Таку програму може пропустити евристичний аналізатор першого типу, але цілком може виявити аналізатор другого типу.

Негативні риси ті ж, що і раніше:

- Помилкові спрацьовування.
- Неможливість лікування.
- Невисока ефективність.

В першу чергу, кожен антивірус повинен містити ***модуль оновлення***. Це пов'язано з тим, що основним методом виявлення вірусів сьогодні є сигнатурний аналіз, який покладається на використання антивірусної бази. Для того, щоб сигнатурний аналіз ефективно справлявся з найостаннішими вірусами, антивірусні експерти постійно аналізують зразки нових вірусів і випускають для них сигнатури.

Другий важливий допоміжний модуль - це ***модуль планування***. Існує ряд дій, які антивірус повинен виконувати регулярно,зокрема: перевіряти ваш комп'ютер на наявність вірусів і оновлювати антивірусну базу. Модуль оновлення якраз і дозволяє набудувати періодичність виконання цих дій.

У міру збільшення кількості модулів в антивірусі виникає необхідність в додатковому ***модулі для управління і настройки***. У простому випадку - це ***загальний інтерфейсний модуль***, за допомогою якого можна в зручній формі дістати доступ до найбільш важливих функцій:

- Настройки параметрів антивірусних модулів.
- Настройки оновлень.
- Настройки періодичного запуску оновлення і перевірки.
- Запуску модулів вручну, на вимогу користувача.
- Звітам про перевірку.
- Іншим функціям, залежно від конкретного антивіруса.

Серед інших допоміжних засобів в багатьох антивірусах є спеціальні технології, які захищають від можливої втрати даних в результаті дій антивіруса. Таким засобом є карантин, в який антивірус розміщує файл, що не вдалося вилікувати, тоді якщо опиниться, що файл був видалений помилково або була втрачена важлива інформація, завжди можна буде виконати відновлення з резервної копії.

Загальний огляд сучасних антивірусних програм

Avira AntiVir — серія антивірусних програм від німецької компанії Avira GmbH. Всі продукти серії засновані на антивірусному двигуні Luke Filewalker, який було вперше представлено у 1988 році. 17 жовтня 2008 було випущено значно покращену версію продукту, завдяки чому швидкість сканування збільшилась на 20%. Це було досягнуто завдяки «прибиранню» з вірусної бази старих версій вірусних сигнатур. AntiVir може постійно стежити за файлами і архівами, які можуть бути потенційними переносниками вірусів. Відшукуються також і макроси, які упроваджуються в офісні документи.

NOD32 — антивірусний пакет, що випускається словацькою фірмою ESET. Перша версія була випущена в кінці 1987 році. Назва спочатку розшифровувалася як Nemocnica na Okraji Disku («Лікарня на краю диска», перифраз назви популярного тоді в Чехословаччині телесеріалу «Лікарня на околиці міста»).

NOD32 — це комплексне антивірусне рішення для захисту в реальному часі. ESET NOD32 забезпечує захист від вірусів, а також від інших загроз, включаючи троянські програми, черв'яки, spyware, adware, фішинг-атаки. В ESET NOD32 використовується патентована технологія ThreatSense, призначена для виявлення нових загроз, які виникають в реальному часі, шляхом аналізу виконуваних програм на наявність шкідливого коду, що дозволяє попереджати дії авторів шкідливих програм.

При оновленні баз використовується ряд серверів-дзеркал, при цьому також можливе створення внутрішньомережевого дзеркала оновлень, що призводить до зниження навантаження на інтернет-канал. Для отримання оновлень з офіційних серверів необхідні ім'я користувача і пароль, які можна отримати, активувавши свій номер продукту на сторінці реєстрації регіонального сайту.

Нарівні з базами вірусів NOD32 використовує евристичні методи, що забезпечує краще виявлення ще невідомих вірусів.

Велика частина коду антивірусу написана на мові асемблера, тому для нього характерне мале використання системних ресурсів і висока швидкість перевірки з налаштуваннями за замовчуванням.

AVG — антивірусне програмне забезпечення розроблене чеською компанією AVG Technologies (раніше відома під назвою Grisoft). Антивірус має сканер файлів, має змогу перевіряти електронну пошту, та моніторинг системи. Програма містить пошуковий механізм Virus Stalker, яких сертифікований незалежними дослідницькими лабораторіями.

AVG Antivirus існує у двох версіях:

AVG Antivirus Free Edition

AVG Antivirus Pro Edition

Антивірус Касперського (раніше відомий як Antiviral Toolkit Pro; коротко називається KAV — від англ. Kaspersky Antivirus) — антивірусне програмне забезпечення, що розробляється Лабораторією

Касперського. Надає користувачеві захист від вірусів, троянських програм, шпигунських програм, руткітів, adware, а також невідомих погроз за допомогою проактивного захисту, що включає компонент HIPS.

Базовий захист

- Перевірка файлів, веб-сторінок, поштових і ICQ-повідомлень
- Блокування посилань на заражених і фішингові веб-сайти
- Проактивний захист від невідомих погроз, заснований на аналізі поведінки програм
- Самозахист антивірусу від спроб виключення з боку шкідливого ПО
- Регулярні і екстрені оновлення — завжди актуальний захист комп'ютера
- Віртуальна клавіатура для безпечного введення логінів, паролів і номерів кредитних карт на веб-сторінках
- Спеціальний Ігровий профіль для тимчасового відключення оновлень, перевірки за розкладом і повідомлень
- Перевірка операційної системи і встановлених програм на наявність уразливостей
- Налаштування операційної системи і інтернет-браузера для безпечної роботи в інтернеті
- Відновлення працездатності системи після вірусної атаки
- Інструменти створення Диска аварійного відновлення системи
- Видалення тимчасових файлів інтернет-браузера

Kaspersky Internet Security 2010

Базовий захист та:

- Контроль роботи програм і обмеження їх доступу до важливих областей ОС і особистих даних користувача
- Доступ до паролів, логінів і інших особистих даних — лише для довірених програм
- Захист від спаму і фішингу в поштових програмах
- Блокування банерної реклами на веб-сторінках
- Батьківський контроль (обмеження використання інтернету дітьми)
- Аналіз мережевої активності в режимі реального часу за допомогою інструменту Моніторинг мережі
- Запуск підозрілих файлів і веб-сайтів в Безпечному середовищі
- Захищена область для тек і файлів з важливими даними, доступна лише для довірених програм
- Налаштування правил доступу програм до системних і онлайну-ресурсам
- Навчання модуля Анти-спам на прикладі вже наявних листів для ефективнішої фільтрації спаму-повідомлень

Avast! Professional Edition увібрав в себе всі високопродуктивні технології для забезпечення однієї мети: надати вам найвищий рівень захисту від комп'ютерних вірусів. Даний продукт є ідеальне рішення для робочих станцій на базі Windows. Нова версія ядра антивіруса avast! забезпечує високий рівень виявлення укупі з високою ефективністю, що гарантує 100%-е виявлення вірусів "In-the-Wild" і високий рівень виявлення троянів з мінімальним числом помилкових спрацьовувань. Механізм антивірусного ядра сертифікований ICSA, постійно бере участь в тестах VirusBulletin і отримує нагороди VB100%. Зовнішній вигляд призначеного для користувача інтерфейсу відображається за допомогою так званих скінів, тому у вас є можливість набудувати зовнішній вигляд панелі продуктів avast! по-своєму бажанню.

Вдосконалений призначений для користувача інтерфейс (тільки у версії Professional).

На додаток до простого, призначеного для користувача інтерфейсу Professional Edition представляє вдосконалений, призначений для користувача інтерфейс, забезпечуючи вас можливістю розширеного сканування.

На відміну від простого інтерфейсу, сканування проводиться за допомогою так званих "завдань". Спочатку ви визначаєте завдання, включаючи різні параметри - області сканування, що сканувати, як сканувати і т.д. Визначивши завдання, ви можете його запустити на виконання. Кожне

завдання генерує список результатів, з яким ви можете працювати пізніше.

Інша важлива особливість, тісно пов'язана із завданнями, - сканування за розкладом. Воно дає вам можливість задавати час для запуску завдання на виконання, одноразово або періодично.

КОНТРОЛЬНІ ЗАПИТАННЯ

1. Що називається антивірусною програмою?
2. Назвіть дві основні групи методів антивірусного захисту.
3. Опишіть принципи роботи, переваги та недоліки сигнатурного та евристичного методів антивірусного захисту.
4. З яких основних модулів складається сучасне антивірусне програмне забезпечення?
5. Що таке карантин?
6. Які ви знаєте сучасні найпоширеніші антивірусні програми?
7. Охарактеризуйте можливості більшості сучасних антивірусних програм.
8. Який антивірус встановлений на вашому робочому комп’ютері? Охарактеризуйте його основні можливості.