VirusTotal — це безкоштовна послуга для **дослідження підозрілих файлів і посилань**; дозволяє швидко виявляти віруси, хробаки, трояни й інші види шкідливих програм.

**Ботне́т** ([англ.](https://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0) *botnet* від robot і network) — це комп'ютерна мережа, що складається з деякої кількості хостів, із запущеними ботами — автономним програмним забезпеченням. Найчастіше бот у складі ботнета є програмою, яка приховано встановлюється на комп'ютері жертви і дозволяє зловмисникові виконувати певні дії з використанням ресурсів інфікованого комп'ютера. Зазвичай використовуються для протиправної діяльності — розсилки [спаму](https://uk.wikipedia.org/wiki/%D0%A1%D0%BF%D0%B0%D0%BC), [перебору паролів](https://uk.wikipedia.org/wiki/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4_%C2%AB%D0%B3%D1%80%D1%83%D0%B1%D0%BE%D1%97_%D1%81%D0%B8%D0%BB%D0%B8%C2%BB) на віддаленій системі, атак на [відмову в обслуговуванні](https://uk.wikipedia.org/wiki/%D0%92%D1%96%D0%B4%D0%BC%D0%BE%D0%B2%D0%B0_%D1%81%D0%B5%D1%80%D0%B2%D1%96%D1%81%D1%83), отримання персональної інформації про користувачів, крадіжка номерів кредитних карт та паролів доступу.

**Социальная инженерия** — это метод управления действиями [человека](https://ru.wikipedia.org/wiki/%D0%A7%D0%B5%D0%BB%D0%BE%D0%B2%D0%B5%D0%BA_%D1%80%D0%B0%D0%B7%D1%83%D0%BC%D0%BD%D1%8B%D0%B9) без использования технических средств. Метод основан на использовании слабостей [человеческого фактора](https://ru.wikipedia.org/wiki/%D0%A7%D0%B5%D0%BB%D0%BE%D0%B2%D0%B5%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D1%84%D0%B0%D0%BA%D1%82%D0%BE%D1%80) и считается очень разрушительным.

**Скимминг** (от англ. skimming) — кража данных карты при помощи специального считывающего устройства ([скиммера](http://www.banki.ru/wikibank/%D1%EA%E8%EC%EC%E5%F0/" \o "скиммера)). Злоумышленники копируют всю информацию с магнитной полосы карты (имя держателя, номер карты, срок окончания срока ее действия, CVV- и [CVC-код](http://www.banki.ru/wikibank/CVC2/)), узнать [ПИН-код](http://www.banki.ru/wikibank/%CF%C8%CD-%EA%EE%E4/) можно с помощью мини-камеры или накладок на клавиатуру, установленных на [банкоматах](http://www.banki.ru/wikibank/%C1%E0%ED%EA%EE%EC%E0%F2/). Стать жертвой скимминга можно не только снимая наличные, но и оплачивая покупки в торговых точках. Для копирования данных официанты, кассиры, служащие гостиниц используют переносные скиммеры или устройства, прикрепленные к терминалу.

**Руткит** ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) *rootkit*, то есть «набор [root](https://ru.wikipedia.org/wiki/Root" \o "Root)'а») — набор [программных средств](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0) (например, исполняемых файлов, скриптов, конфигурационных файлов), для обеспечения:

* маскировки объектов (процессов, файлов, директорий, драйверов)
* управления (событий, происходящих в системе)
* сбора данных (параметров системы)

В систему руткит может быть установлен различными способами: загрузка посредством эксплойта, после получения шелл-доступа (в таком случае, может использоваться средство типа wget или исходный [FTP-клиент](https://ru.wikipedia.org/wiki/FTP-%D0%BA%D0%BB%D0%B8%D0%B5%D0%BD%D1%82) для загрузки руткита с удаленного устройства), в исходном коде или ресурсах программного продукта.

**Завантажувачі** або **Дропери** ([англ.](https://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0) *Dropper*) — родина [зловмисного програмного забезпечення](https://uk.wikipedia.org/wiki/%D0%97%D0%BB%D0%BE%D0%B2%D0%BC%D0%B8%D1%81%D0%BD%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%B5_%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F" \o "Зловмисне програмне забезпечення), призначення якого — несанкціоноване і приховане від користувача встановлення на комп'ютер-жертву шкідливих програм, що містяться в самому тілі дропера або завантажуючи через мережу.

Даний тип шкідливих програм звичайно без будь-яких повідомлень (або з оманливими повідомленнями про помилку в архіві, невірну версію операційної системи тощо) завантажує з мережі й зберігає на диску жертви файли з їхнім подальшим виконанням.

Антивирусы

1. Сигнатуры – последовательность байт, контрольные суммы.
2. Еврестичный поиск – поиск закономерностей в программе (есть подозрение что данный файл заражен)
3. Поведiмковий анализатор – следит за тем что делает программа в системею. Блокирует прогу, делает откат в ос
4. Репутацiйна та хмарна технология – сигнатуры отправляются на сервер , после у пользователя спрашивается, вы качали этот файл и хотите его открыть. Назначает рейтинг файла.

Способы воровства финансовой инфы

1. Троянские программы (скрины монитора, нажатия на клавиши)
2. Фишинг
3. Скимминг
4. Дзвонки злодеев

Защита от финасовой кражи

1. Антивирус
2. Учетка без прав админа