Сучасні питання кібербезпеки

доцент
Горбенко В.І.
ауд.19, корп.1

Троянські програми

Троянська програма (Trojan Horse) — це шкідливе програмне забезпечення, яке маскується під легальне або корисне ПЗ, щоб отримати доступ до системи користувача або виконати небажані дії без його відома. На відміну від вірусів, троянські програми не здатні самостійно розмножуватись, їх перша мета — бути інстальованими на комп’ютер жертву, для чого використовується обман і засоби соціальної інженерії.

Період	Подія / приклад	Характеристика
1980-ті	Перші "жарти" — програми, які знищували дані під виглядом корисних утиліт	Початок концепції
1990-ті	Поширення через дискети й e-mail (*AIDS Trojan, NetBus, Sub7*)	Перші програми для віддаленого доступу
2000-ті	*Zeus*, *SpyEye* — трояни для крадіжки банківських даних	Професіоналізація кіберзлочинності
2010-ті – 2020-ті	*Emotet*, *TrickBot*, *Agent Tesla*	Комерціалізація (Malware-as-a-Service), інтеграція з ботнетами

Класифікація троянських програм

Тип трояну	Характеристика	Приклади
Remote Access Trojan (RAT)	Надає зловмиснику повний контроль над системою (екран, камера, файли, клавіатура)	*DarkComet*, *NanoCore*
Banking Trojan	Викрадає облікові дані банківських акаунтів, перехоплює введення з клавіатури	*Zeus*, *TrickBot*
Downloader / Dropper	Завантажує й інсталює інше шкідливе ПЗ	*Emotet*, *SmokeLoader*
Spyware (шпигун)	Збирає дані користувача — історію браузера, натискання клавіш, скріншоти	*Agent Tesla*, *FormBook*
Backdoor	Відкриває “чорний хід” у систему для подальшого доступу	*Back Orifice*, *Gh0st RAT*
Ransom Trojan	Блокує систему або шифрує дані, вимагаючи викуп	*FakeAV*, *Ransomlock*
SMS Trojan (мобільний)	Відправляє платні SMS-повідомлення без відома користувача.	*Trojan-SMS.AndroidOS.FakeInst*
Rootkit Trojan	Маскує присутність інших програм у системі.	*ZeroAccess*, *TDSS*

Принцип дії

1. Маскування — троян подається як безпечна програма (оновлення, документ, фото, комп’ютерна гра).

2. Інфікування — користувач сам запускає файл.

3. Встановлення — троян створює копії себе у системних каталогах, змінює автозапуск.

4. Приховування — шифрування коду, зміна імен, використання rootkit-технологій.

5. Виконання шкідливих дій — крадіжка даних, відкриття порту, контроль камери, знищення файлів.

6. Комунікація з командним сервером (C&C) — передача даних або отримання команд.

Приклади:

1. “Zeus” (2007) — троян, який викрадав банківські логіни через фальшиві веб-сторінки.

2. “Emotet” (2014–2021) — троян, який маскувався під листи державних установ.

3. “Agent Tesla” (2020–) — шпигун, що краде паролі й пересилає їх на пошту зловмисника.

Методи виявлення та захисту

Захід	Суть
Антивірусне ПЗ з аналізом поведінки	Виявлення аномальної активності
Сегментація мережі	Обмеження поширення шкідливого коду
Контроль привілеїв користувача (UAC, Least Privilege)	Мінімізація шкоди
Моніторинг мережевого трафіку (IDS/IPS)	Виявлення зв’язку з C&C серверами
Соціальна грамотність користувачів	Усвідомлення фішингових ризиків
Оновлення систем і додатків	Усунення експлойтів, що використовуються троянами

Malware-as-a-Service (MaaS)

Malware-as-a-Service (MaaS) — комерційна модель, коли розробники шкідливого ПЗ пропонують його іншим злочинцям як послугу: готові інструменти, інфраструктура, техпідтримка — за гроші або частку від прибутку. Це робить потужні інструменти доступними тим, хто не вміє їх писати.

Malware-as-a-Service (MaaS) — це одна з ключових причин, чому кіберзлочинність сьогодні стала масовою, професійною й масштабною.

Ролі в екосистемі MaaS

- Розробники (operators) — створюють і підтримують шкідливий код, інфраструктуру C2, адмін-панель.
- Покупці/афіліати (customers/affiliates) — орендують інструмент або працюють за партнерською моделлю (отримують частину «прибутку» за здійснені атаки).
- Хостинг/інфраструктурні провайдери — bulletproof-хости, VPN, проксі, криптобіржі (опосередковано).
- Посередники/маркетплейси — форумні майданчики, закриті телеграм-канали, дарк-маркет — місця продажу та реклами MaaS.
- Сервіси “під ключ” — фішинг-kits, крадені бази даних, крипто-каси, шифрувальники (ransomware) як окрема послуга.

Види послуг

Ransomware-as-a-Service (RaaS) — готовий рансомвар з адмін-панеллю, шлюзом оплати та “кейтерінгом” (вибір жертв). Це бізнес-модель кіберзлочинності, яка поширює доступ до атак програм-вимагачів. Функціонує як легальний SaaS-сервіс, але замість легітимного програмного забезпечення пропонує інструменти та інфраструктуру для проведення атак із вимаганням.

Структура та Ролі

Складається з двох основних груп, які мають чіткі ролі та розподіл прибутків:

A. Оператори RaaS (The Developers)

Розробники або кіберзлочинні угруповання, що створюють, підтримують і постійно оновлюють основний код програми-вимагача, інфраструктуру для переговорів, платіжні системи (часто у крипті) та мережу командно-контрольних серверів (C2).

- Продукт: Готовий, протестований, часто поліморфний код (змінюється для уникнення виявлення).
- Інфраструктура: Веб-портали для афіліатів, панелі керування, служби підтримки (для афіліатів та, іноді, для жертв).
- Оновлення: Постійне оновлення коду для обходу нових засобів кіберзахисту.

B. Афіліати (The Affiliates)

Це кіберзлочинці-виконавці, які не мають навичок написання коду, але вміють проникати в мережі. Вони купують або орендують доступ до RaaS-платформи.

- Діяльність: Знаходять ціль (компанію), здійснюють початкове проникнення (через фішинг, експлуатацію вразливостей, викрадення облікових даних) і розгортають надане програмне забезпечення-вимагача.
- Переговори та Викуп: Часто вони також ведуть переговори з жертвою та надають їй інструкції щодо сплати викупу.

Бізнес-Модель RaaS

RaaS-модель працює за принципом франшизи або партнерської програми:

Крок 1: Залучення Афіліатів

Оператори RaaS рекламують свої послуги на підпільних форумах. Вони можуть стягувати плату за підписку (наприклад, $500–$2000 на місяць) або вимагати початковий внесок (Deposit) за доступ до своїх інструментів.

Крок 2: Надання Інструментів (The Kit)

Афіліат отримує доступ до "RaaS Kit", який включає:

- Виконуваний файл програми-вимагача з можливістю налаштування (наприклад, вказати цільову директорію).
- Панель керування для відстеження стану атаки (скільки жертв заражено, хто заплатив).
- Шаблони повідомлень для фішингу та інструкції з розгортання.

Крок 3: Атака та Шифрування

Афіліат використовує свої навички, щоб доставити та розгорнути програму-вимагача в мережі жертви. Програма шифрує дані.

Крок 4: Сплата та Розшифрування

Жертва сплачує викуп (як правило, у криптовалюті, наприклад, Bitcoin або Monero) на гаманець, контрольований Оператором RaaS.

Крок 5: Розподіл Прибутку (The Cut)

Після отримання викупу Оператори RaaS автоматично або вручну розподіляють прибуток за попередньо узгодженою схемою. Найпоширеніші моделі:

1. Розподіл Відсотка (Revenue Share): Це найпопулярніша модель. Оператори RaaS забирають 20%–40% від загальної суми викупу, а решта надходить Афіліату.
2. Фіксована Ціна: Афіліат платить фіксовану суму за використання інструменту, а весь викуп забирає собі (менш поширено).

Ефективність та небезпечність RaaS

• Масштаб: RaaS дозволяє тисячам низькокваліфікованих злочинців (афіліатів) проводити високотехнологічні атаки, які раніше були під силу лише елітним APT-групам.

• Спеціалізація: Оператори зосереджуються виключно на розробці та уникненні виявлення, а афіліати — на проникненні та монетизації. Це максимізує ефективність.

• Економіка: Модель RaaS мінімізує ризики для Операторів, оскільки юридичні та технічні ризики доставки (виявлення, ідентифікація) лежать на Афіліатах.

RaaS є основною рушійною силою більшості великих інцидентів із програмами-вимагачами у 2025 році

Індикатори компрометації (на високому рівні)

(ознаки, які варто моніторити)

• раптові масові операції з файлами / зміни великих масивів даних;
• повідомлення про неможливість відкрити файли + нотиси про викуп;
• незвична мережева активність із зовнішніми доменами;
• незрозумілі процеси, скрипти чи завдання, яких раніше не було;
• резервні копії, які несподівано недоступні або видаляються.

Засоби захисту та реагування (для організацій)

Стратегія має бути багатошаровою. Ключові елементи:

Профілактика

- Оновлення ПЗ (patch management) — швидко закривати відомі вразливості.
- Управління привілеями (least privilege) — мінімізувати права користувачів.
- Багатофакторна аутентифікація (MFA) для доступів (особливо RDP, VPN, тощо).
- Контроль доступу та сегментація мережі — для зупинки поширення.
- Політики щодо резервних копій — регулярні бекапи, ізоляція копій від мережі; періодичні перевірки відновлюваності.
- Навчання персоналу — тренінги із розпізнавання фішингу/соціальної інженерії.
- Контроль встановлення ПЗ (whitelisting) та блокування запуску скриптів з неперевірених джерел.

Виявлення

- EDR/XDR — інструменти для виявлення аномальної поведінки кінцевих точок.
- SIEM і логування — централізований збір подій та аналіз.
- Threat intelligence feeds — автоматичне підвантаження IOC для блокування.

Реагування

- План реагування на інциденти (IRP) — призначені ролі, процедури, контакти.
- Ізоляція уражених систем — зупинити поширення.
- Відновлення з бекапів — тестовані процедури.
- Співпраця з правоохоронними органами та CERT.
- Комунікація — внутрішня і зовнішня, про інцидент і про кроки відновлення.

BaaS — Botnet-as-a-Service

BaaS — комерційна модель, коли оператор/власник ботнету здає в оренду мережу заражених пристроїв («ботів») іншим злочинцям для виконання завдань: DDoS, масових розсилок, проксінгу трафіку тощо.

Ролі в BaaS

- **Оператор ботнету** — створює/підтримує ботнет (інфікує пристрої, керує C2-інфраструктурою).
- **Клієнт/орендатор** — платить за використання ботнету для виконання конкретного завдання.
- **Інфраструктурні провайдери** — bulletproof-хостинг, проксі, TOR/VPN, криптопослуги для платежів.
- **Посередники/маркетплейси** — дарк-форум/телеграм-канали, де продають послуги.

Послуги(product set)

- DDoS-атаки на замовлення — від коротких ударів до тривалих кампаній.
- Спам/фішинг-розсилки — використання ботів для масової розсилки листів.
- Проксі/анонімізація трафіку — маршрутизація через ботнет як «маленький VPN».
- Клікфрод / фальсифікація трафіку — створення фальшивих переглядів або кліків.
- Розповсюдження іншого malware — ransomware, banking-trojans тощо.
- Майнинг-послуги (оренда ресурсів для майнінгу) — менш поширено.

Загальний життєвий цикл BaaS

- Набір ботів — оператор інфікує пристрої через вразливості, фішинг, небезпечні програми, IoT-уразливості.
- Управління — ботнет управляється через C2-сервери або через децентралізовані механізми.
- Оренда — клієнт замовляє атаку/послугу, платить (часто в крипті), отримує інтерфейс/інструкції.
- Виконання — ботнет виконує завдання (DDoS/розсилка/проксі), результати збираються.
- Підтримка — оператор оновлює ботнет, обходить фільтри, додає нові боти.

Мотивація використання BaaS

- Масштаб без навичок: покупцю не треба вміти створювати ботнет — він просто орендує.
- Розподіл ризиків: оператор/афіліат розділяють відповідальність і прибуток.
- Масовість атак: один ботнет може обслуговувати багатьох клієнтів.

Ознаки компрометації визначаються на рівні IT-операцій та адміністраторів:

- аномально велике вихідне мережеве навантаження із кінцевих точок;
- незрозумілі або регулярні вихідні з’єднання на підозрілі домени/IP;
- процеси або служби, які запускаються вночі і витрачають CPU/пам’ять;
- одночасна підвищена активність на багатьох пристроях в одному сегменті;
- повідомлення від провайдера про скарги на спам або DDoS-джерела.

Глибше розслідування виконується через EDR/IDS/NetFlow/SIEM.

Профілактичні заходи захисту

- Патч-менеджмент: швидко закривати відомі вразливості (особливо на периферійних пристроях, IoT).
- Обмеження зовнішніх сервісів: блокувати непотрібні порті та сервіси (RDP, SMB) на рівні мережі.
- Сегментація мережі: ізолювати IoT і гостеві сегменти від критичних ресурсів.
- Контроль встановлення ПО (whitelisting), політики щодо установлення програм.
- EDR/XDR та сетевий моніторинг: виявлення аномалій поведінки кінцевих точок і трафіку.
- Політика парольного менеджменту і MFA: щоб ускладнити розповсюдження через викрадені облікі.
- Резервні копії та IR-план: готовність до інциденту.

РЕАКЦІЯ: ізоляція уражених вузлів; блокування підозрілих доменів/IP на perimeter; співпраця з ISP і CERT для sinkholing C2; аналіз логів і відновлення з бекапів; повідомлення постраждалих і регуляторів (за вимогами).

Phishing-kits / Credential-as-a-Service (CaaS)

Одна з причин, чому фішинг залишається надзвичайно ефективним: нападник вже не мусить писати код — він купує «під ключ» готовий інструмент:

- **Phishing-kit** — набір файлів і шаблонів, який дає змогу швидко створити фейковий сайт (наприклад, під виглядом банку, поштового сервісу чи соцмережі) і збирати введені жертвами логіни/паролі.
- **Credential-as-a-Service (CaaS)** — сервісна модель: кіберзлодій пропонує повний сервіс (шаблон, хостинг, панель збору, дешифрування, опції доставки), часто за підпискою або частку від зібаних облікових даних.

Ролі в екосистемі

- Автор kits / оператори — роблять шаблони, пакують панелі керування, підтримку.
- Покупці / афіліати — запускають кампанії (розсилка листів, SMS, реклами).
- Хостинг-провайдери / bulletproof host — забезпечують розміщення фейкових сайтів, інколи із слабким реагуванням на жалоби.
- Посередники (маркети, Telegram-канали, форуми) — ринок продажу і реклами kit'ів.
- Сервіси обробки даних / воркфлоу — де зібрані облікові дані фільтруються, перевіряються, продаються.

Типовий життєвий цикл

- Придбання kit — покупець купує/орендує шаблон з панеллю збору.
- Настроювання — мінімальна кастомізація (логотип, домен, мова) — зазвичай GUI-налаштування.
- Доставка — фішингові листи, SMS (SMiShing), дзвінки, підроблені реклами або зкомпрометовані сайти з redirect.
- Збір облікових даних — користувач вводить логін/пароль на фейковому сайті; дані записуються у панелі оператора.
- Верифікація й продаж — оператор/афіліат перевіряє «збиті» облікиа (credential stuffing), відправляє на продаж або відразу використовує (email takeover).
- Поновлення / масштабування — оновлення шаблонів, нові цілі, повторення кампаній.

Склад phishing-kit:

- HTML/CSS/JS шаблони фейкових форм входу, іноді з копією сторінки служби.
- Серверна частина для збирання даних (скрипт, що отримує введені поля).
- Панель керування (backend) для перегляду зібраних логінів, статистики, керування кампаніями.
- Механізми обфускації (перенаправлення, короткі URL, use of cloud storage) щоб уникати блокувань.
- Інструменти для доставки (спам-листинги, шаблони листів) — іноді як окремий модуль.

Продавці часто додають «how-to» документацію і «customer support» — як у SaaS.

Бізнес-моделі

- Прямий продаж — одноразовий платіж за kit.
- Оренда / підписка — доступ до панелі та оновлень на місяць/рік.
- Affiliate / share — оператор отримує % від «збору» або продає доступ афіліатам за плату.
- Пакетні пропозиції — базовий kit + послуги з phishing-розсилки або куплених списків e-mail.

Засоби, завдяки яким kit’и обходять блокування / виявлення:

- Використовують короткі/легкодоступні домени, проксі чи cloud-storage (швидка зміна URL).
- Маскують сторінку (не завжди повна копія), щоб уникнути автоматичних сигнатур.
- Інтегрують captcha-bypass рішення або підмінюють перевірки.
- Часто роблять геоблоки (показують фішинг лише для конкретних регіонів) щоб зменшити скарги.

Індикатори компрометації та ознаки фішингової кампанії

- Несподівані листи з натиснути сюди / термінова дія із зовнішніми короткими URL.
- Сторінки входу з доменами, що близькі до легітимних (typosquatting) або з нетиповими TLD.
- URL, які ведуть через сервіси переадресації або зберігання (cloud storage) перед показом форми.
- Наявність у лінку довгих рядків/параметрів, підозрілих redirect.
- Масові підозрілі спроби логінів із різних джерел (credential stuffing).
- Поява невідомих записів у логах SMTP/HTTP, що корелюються з повідомленнями користувачів.

Виявлення і захист

- Фільтрація e-mail: SPF / DKIM / DMARC, антифішинг-шлюзи, репутаційні фільтри;
- URL-розгортання / проксі-сканування;
- WAF / блокування доменів;
- MFA (обов’язково): другий фактор суттєво підвищує рівень безпеки;
- EDR / SIEM: виявлення нетипових спроб входу, масових змін IP/USER-agent;
- Блокування коротких URL-сервісів у критичних повідомленнях (політика).

Організаційні заходи

- Навчання користувачів, тестові фішинг-кампанії (етичні) - пильність персоналу
- Політика «повідомити і заблокувати»

Види послуг

• Phishing-kits / Credential-as-a-Service — шаблони фейкових сайтів та панелі збору облікових даних.

• Crypters / Packers — інструменти для зашифрування/обфускації шкідливого коду, щоб обійти AV.

• Payload/Loader-services — завантажувачі, які доставляють основний malware.

• Data-as-a-Service — продаж викрадених баз або доступів (RDP, VPN тощо).

• Technical Support & Updates — інструкції, оновлення, “how-to” для операторів.

Бізнес-моделі

• Підписка (subscription): фіксована щомісячна/щорічна плата за доступ.

• Франшиза / партнерська програма (affiliate): оператор дає інструмент, отримує відсоток від кожного “успішного” кейсу.

• Платіж за використання (pay-per-use): оренда ботнету чи завантажувача на годину/день.

• Одноразова купівля: ліцензія на комплект інструментів.

• Комбінації: наприклад, низька підписка + вищий відсоток від прибутку.

Платежі: часто у криптовалюті (Bitcoin, Monero) або через міксер-сервіси, щоб приховати сліди.