Шкідливе програмне забезпечення

План лекції

Вступ
1. Джерела шкідливого програмного забезпечення
2. Шляхи розповсюдження, вектори атак
3. Види шкідливого програмного забезпечення
4. Ознаки ураження ШПЗ
Висновки

Рекомендована література

Основна

1. Даник Ю.Г., Грищук Р.В. Основи кібернетичної безпеки: монографія. Житомир: ЖНАЕУ, 2016. 636 с.
2. Манжай О.В., Манжай І.А. Правові засади захисту інформації: підручник / вид. друге, переробл. та доповн. Харків: Промарт, 2020. 162 с. з іл. URL: https://univd.edu.ua/science-issue/issue/4315.
3. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікованої) програми підвищення кваліфікації: практикум / О.В. Манжай, В.В. Носов. К.: ВАІТЕ, 2021. 106 с.
4. Робочий зошит для учасників тренінгу з питань кібергігієни. Загальна короткострокова програма підвищення кваліфікації / О.М. Барановський, В.В. Гузій, Д.І. Майорников, О.В. Манжай, В.В. Носов. К.: ВАІТЕ, 2021. 262 с.

Допоміжна

5. Носов В.В., Манжай О.В. Зміст та методологія практичного навчання з питань кібергігієни // Протидія кіберзлочинності та торгівлі людьми (18 травня 2021 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків: ХНУВС, 2021. С. 72–73.
6. Манжай О.В., Манжай І.А. Що таке кібергігієна? // Протидія кіберзлочинності та торгівлі людьми (18 травня 2021 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; ГС «Глобальний центр взаємодії в кіберпросторі». Харків : ХНУВС, 2021. С. 65–67.

Інформаційні ресурси в Інтернеті

7. Освітній серіал «Основи кібергігієни». URL: https://osvita.diia.gov.ua/courses/cyber-hygiene.

Текст лекції

Вступ

Шкідливе програмне забезпечення (ШПЗ) – це програмне забезпечення (ПЗ), яке використовується зловмисниками для проведення атак на комп'ютерні системи. Наслідками активності ШПЗ може бути знищення, блокування, модифікація, копіювання інформації або порушення роботи комп'ютерних систем і мереж.

1. Джерела шкідливого програмного забезпечення

ШПЗ може створюватись як окрема програма, а може базуватися на корисних програмах. Наприклад, програми легального віддаленого доступу та адміністрування можуть бути використані як шкідливі.

ШПЗ можна купити на спеціалізованих форумах та сайтах в мережі Інтернет, вартість коливається від кількох десятків доларів то кількох тисяч. Досить часто ШПЗ надається як сервіс (Malware-as-a-service), де клієнт платить місячну/денну/тижневу плату за користування ШПЗ. На рис. 1 наведений фрагмент реклами ШПЗ на хакерському форумі.

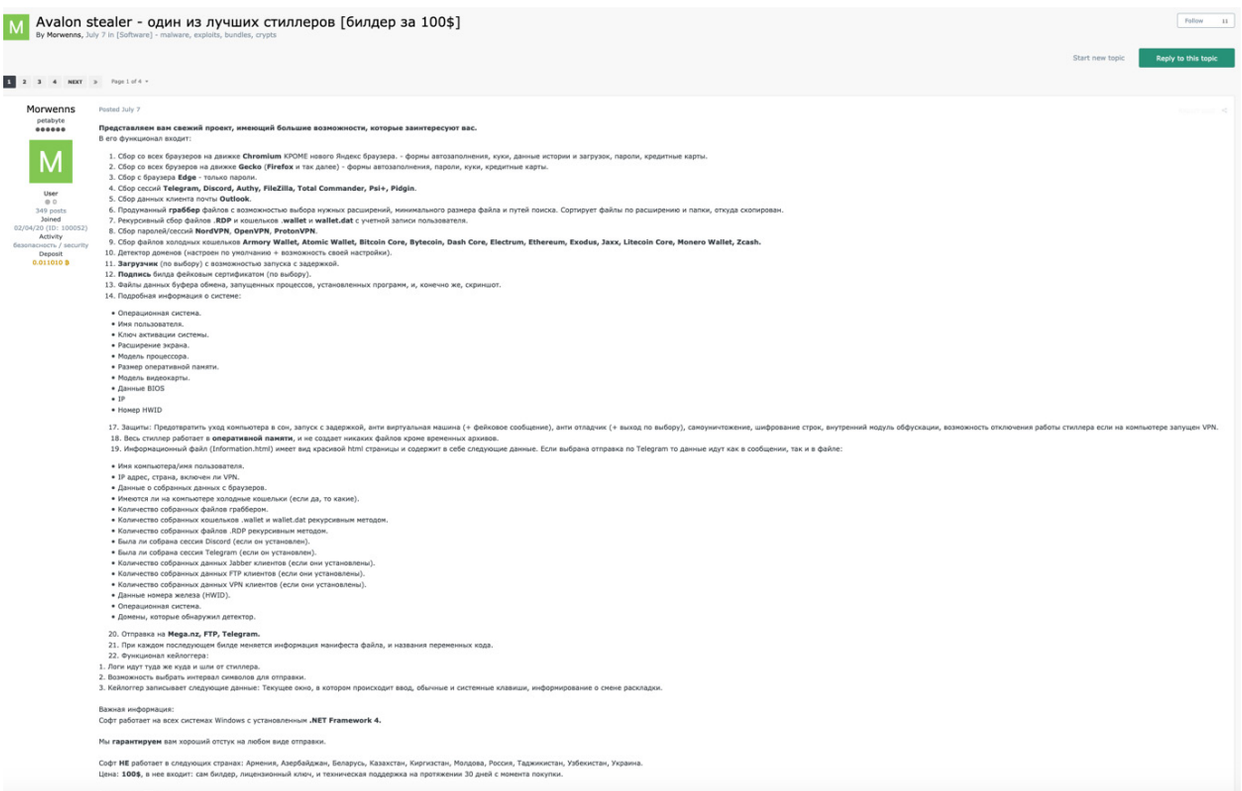

Рис. 1. Реклама ШПЗ

У вільному доступі існують різноманітні інструменти конструювання ШПЗ для отримання несанкціонованого віддаленого доступу до систем, зокрема це – Metasploit-Framework, Veil-Framework (рис. 2) та інші.

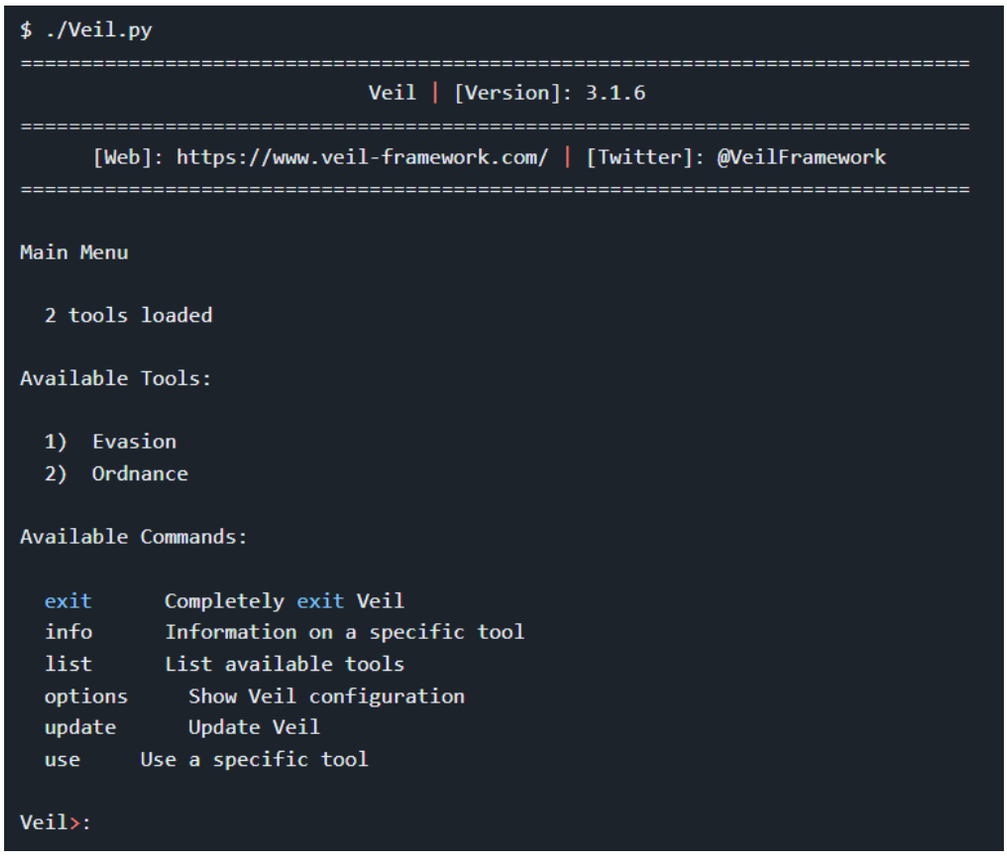

Рис. 2. Меню Veil-Framework

2. Шляхи розповсюдження, вектори атак

Спам. Існує кілька найпоширеніших шляхів розповсюдження ШПЗ, серед них безперечним лідером є масова розсилка повідомлень, зазвичай рекламного характеру, людям, які не дали згоди на їх отримання, – спаму.

Зловмисники можуть надсилати спам, атакуючи певні галузі, наприклад, страхові компанії, медичні установи, державні структури або певних користувачів. Бази адресів для спаму зазвичай купуються на хакерських форумах.

Таргетовані або цільові спам-кампанії спрямовані на конкретних осіб або організації. Це – більш складний тип атаки, оскільки таргетовані спам-кампанії передбачають попереднє вивчення майбутньої жертви, наприклад, її активності в соціальних мережах, родинних зв'язків, уподобань, хобі, життєвих проблем тощо. Ця інформація дозволяє зловмиснику створювати переконливе повідомлення, щоб змусити жертву запустити ШПЗ.

Зловмисники надсилають через вкладення до електронного листа спеціально створені файли, наприклад, MS Word/Excel, PDF, PNG, ZIP, EXE, які після активізації вже завантажують ШПЗ із віддаленого серверу та запускають на комп'ютері жертви (рис. 3).

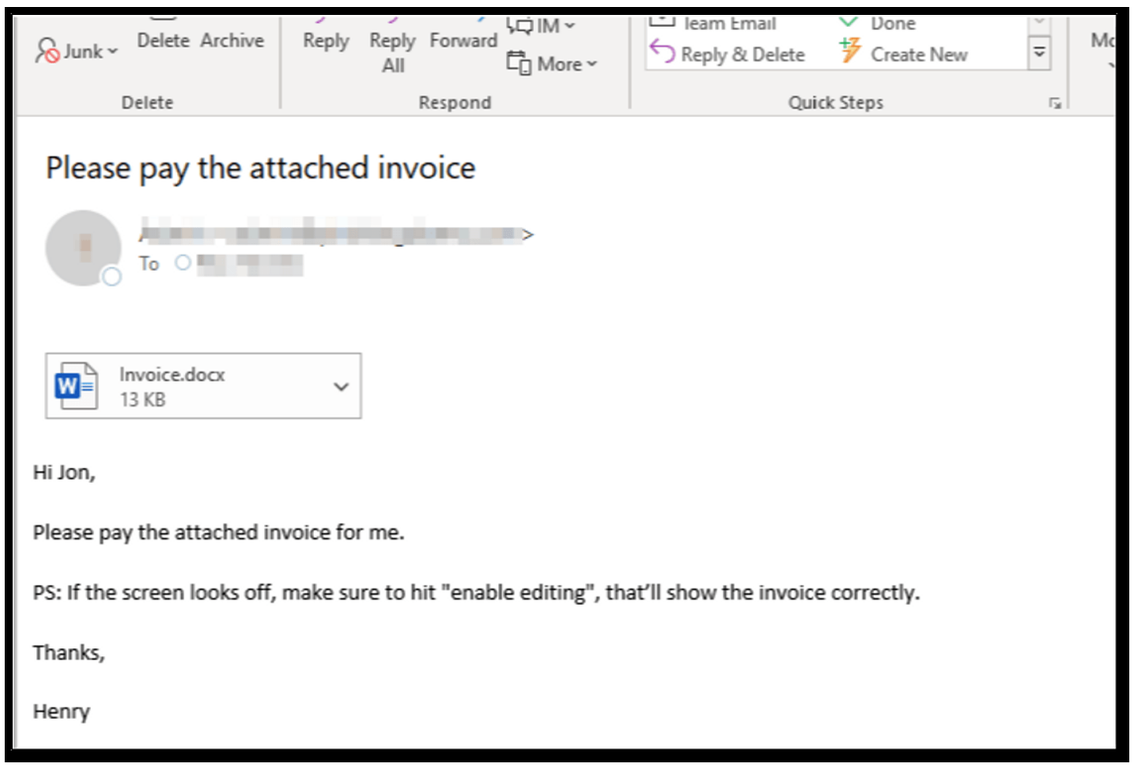

Рис. 3. Вкладення файлу MS Word, який містить макрос завантаження ШПЗ

Іншим способом є надсилання шкідливого файлу із «фейковим» або з так званим «подвійним розширенням». У такому випадку зловмисники змінюють розширення файлу, а також змінюють іконку файлу на відповідне розширення. Це створює враження, що файл є безпечним та може бути відкритий. Наприклад, файл note.txt.exe насправді є виконуваним файлом, а не текстовим, і якщо у користувача вимкнено функцію показувати розширення файлів, у нього складеться враження, що він відкриває текстовий файл, натомість запускаючи при цьому ШПЗ.

Щоб увімкнути функцію «Показувати розширення файлів»:*

- Натисніть кнопку «Пуск» і виберіть пункт меню «Мій комп'ютер».
- Далі в меню оберіть пункт «Сервіс», потім пункт «Властивості папки».
- У вікні «Властивості папки», виберіть вкладку «Вигляд».
- Знайдіть пункт «Приховувати розширення для зареєстрованих типів файлів» і зніміть з нього галочку.

* може дещо відрізнятися залежно від версії операційної системи.

Для того, щоб змусити жертву відкрити вкладений шкідливий файл, зловмисники застосовують засоби соціальної інженерії.

Як альтернатива, злочинці можуть вставляти посилання на завантаження ШПЗ безпосередньо в повідомленні та маскувати його під виглядом легітимної програми чи додатку. На рис. 4 показані приклади фішингових листів, які використовували тему світової пандемії коронавірусу 2020 р. для розповсюдження ШПЗ.

Фішинг – вид онлайн-шахрайства, який базується на методах соціальної інженерії та має на меті шляхом обману змусити користувача здійснити дії, які б він не здійснив у звичних умовах, наприклад, розкрити свої персональні дані, завантажити, встановити чи запустити шкідливе програмне забезпечення. Фішинг може бути здійснений у різних формах: електронні листи, надіслані нібито від імені легальних компаній, фейкові веб-сайти, дзвінки нібито співробітників банку тощо.

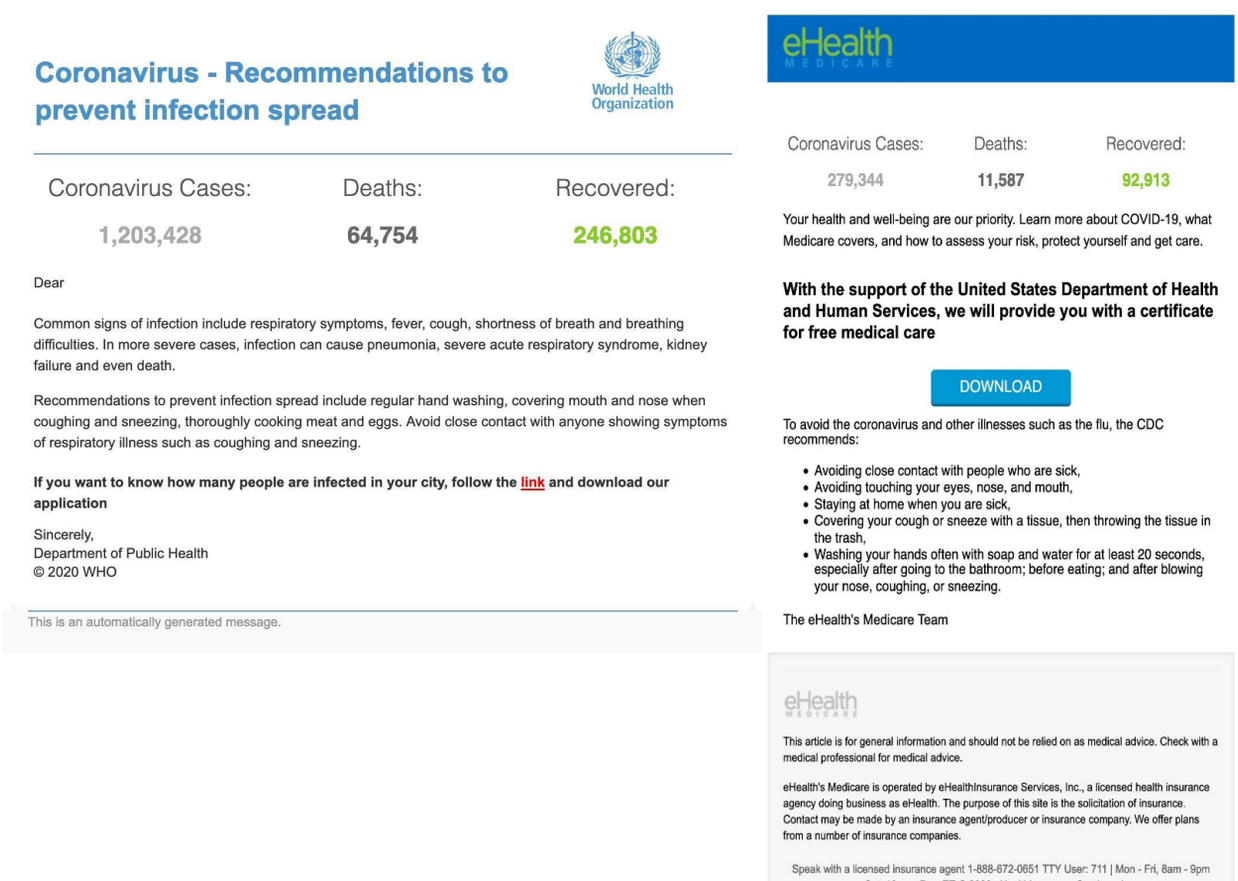

Рис. 4. Приклади фішингових листів

Програми нелегальної активації комерційного ПЗ. Іншим, не менш поширеним способом розповсюдження ШПЗ є поширення так званих «креків» для комерційного програмного забезпечення або власне примірників «зламаного» комерційного програмного забезпечення, яке «не потребує купівлі ліцензії».

> **«Крек»** (від англ. «crack») – це програма, яка генерує код активації для комерційного програмного забезпечення чи змінює систему перевірки ліцензії комерційного програмного забезпечення і тим самим порушує авторські права виробника.

У такому випадку зловмисники додають шкідливий програмний код у модифіковане комерційне програмне забезпечення. Нічого не підозрюючи, користувач встановлює таку програму, а разом з нею – і ШПЗ, за допомогою якого зловмисники отримують доступ до системних файлів. На рис. 5 показаний приклад розповсюдження програми-вимагача (ransomware) під виглядом програми активації ОС Windows.

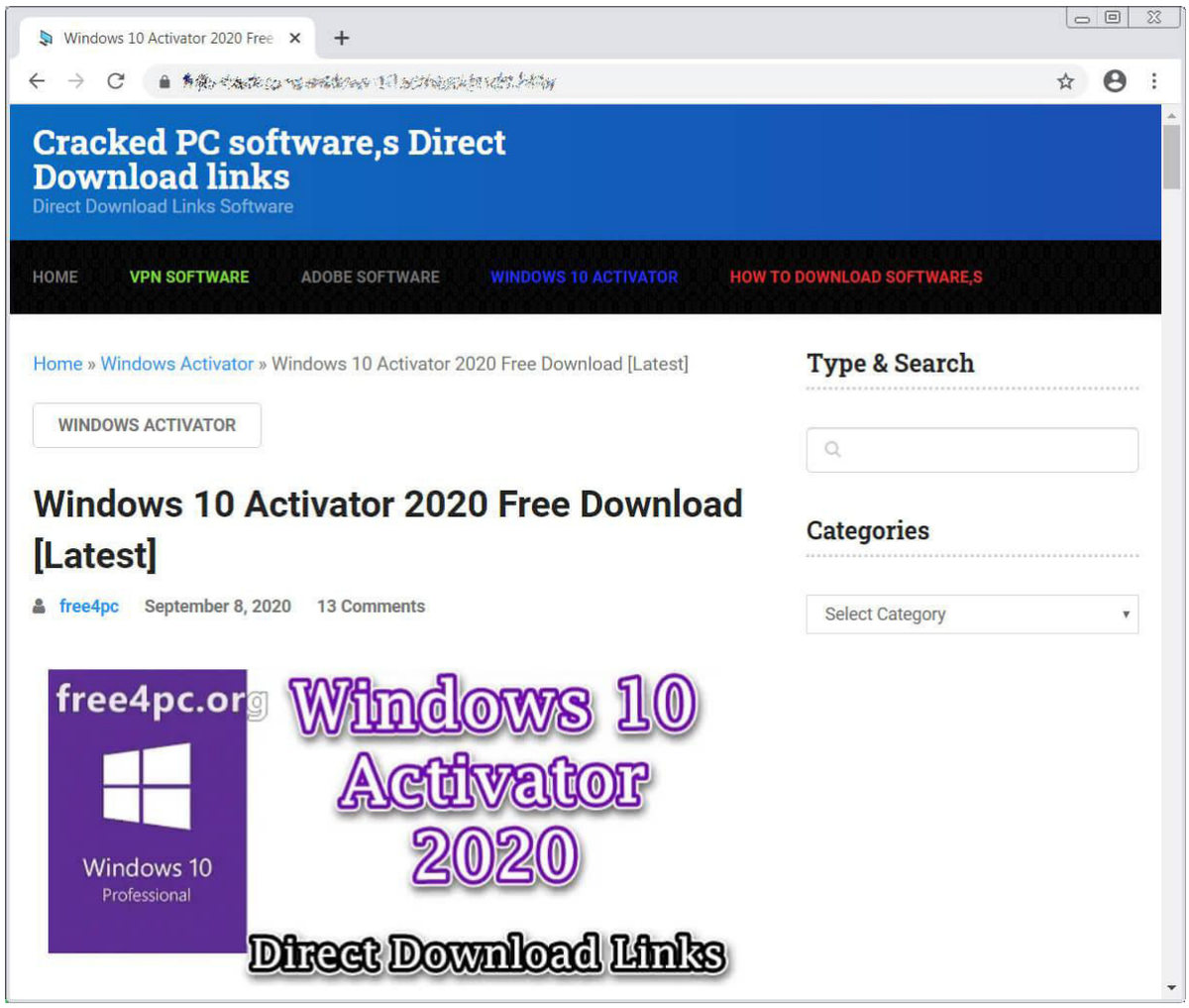

Рис. 5. Приклад розповсюдження програми-вимагача (ransomware) під виглядом програми активації ОС Windows

Безкоштовне ПЗ. Різновидом цього способу є поширення ШПЗ під виглядом «freeware»-програм. Це, як правило, так звані «корисні» програми, такі як ліхтарики для мобільних телефонів, калькулятори, конвертери валют тощо. Найбільш поширеними вони є для мобільних пристроїв. На рис. 6 зображено програми для фітнесу, які приховано встановлювали на мобільний пристрій ШПЗ для крадіжки банківської інформації.

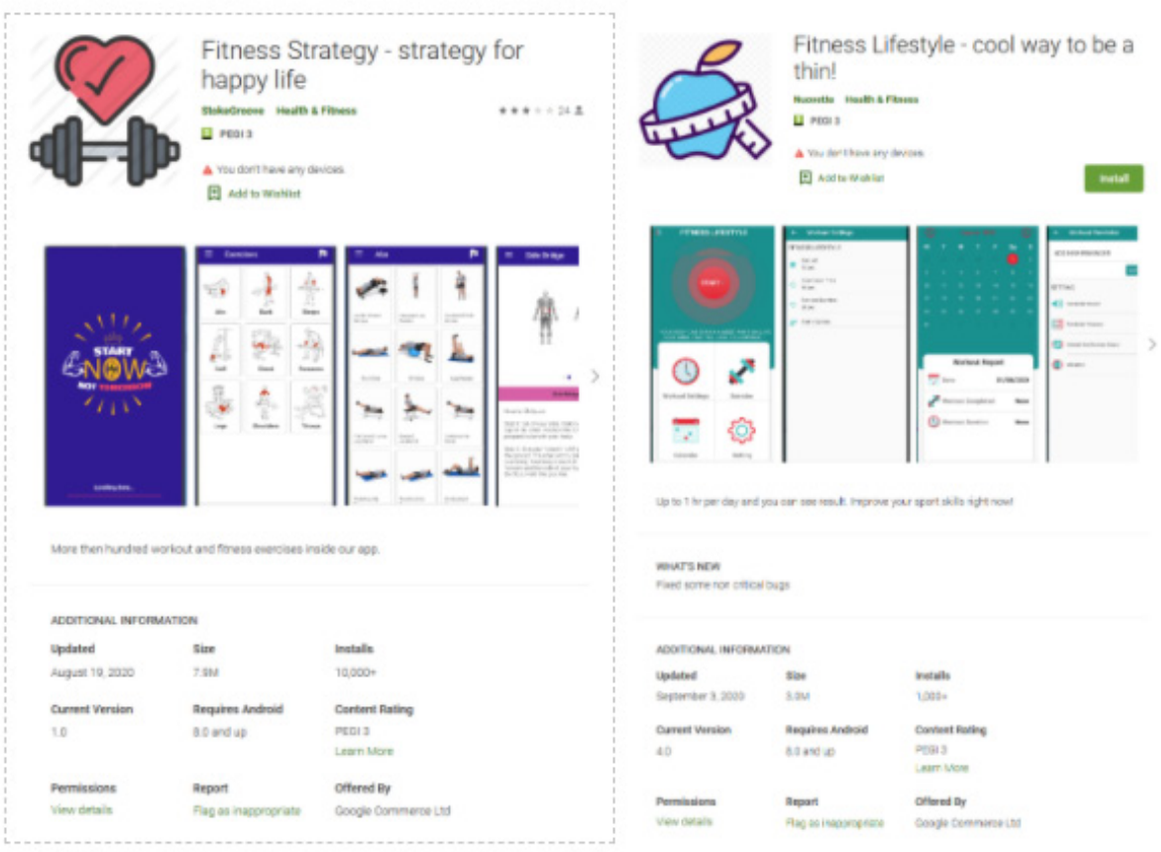

Рис. 6. ШПЗ під виглядом корисного ПЗ

Для зменшення ризику встановлення ШПЗ під виглядом корисної безкоштовної програми необхідно:

- уникати ПЗ з малим рейтингом та поганими відгуками користувачів у репозиторії (магазині) додатків;
- при встановленні ПЗ звертати увагу на дозволи доступу до ресурсів операційної системи, які запитує додаток. Очевидно, що програмі ліхтарика не потрібний доступ до текстових повідомлень, камери, мікрофону чи фото, щоб ефективно працювати;
- ознайомитись з інформацією про розробника ПЗ: наскільки він відомий на ринку ПЗ, чи існують інші додатки й який у них рейтинг, чи є власний сайт тощо.

Таргетовані атаки із використанням «нетрадиційних методів». Сюди можна віднести «випадково загублені флешки», фізичний доступ зловмисника до комп'ютера, складні прийоми соціальної інженерії: коли телефонують користувачеві та просять встановити ту чи іншу програму, наприклад, під виглядом співробітників банку. На окрему увагу заслуговує загроза від інсайдерів, які вербуються для встановлення ШПЗ, відключення антивірусів та міжмережевих екранів (рис. 7).

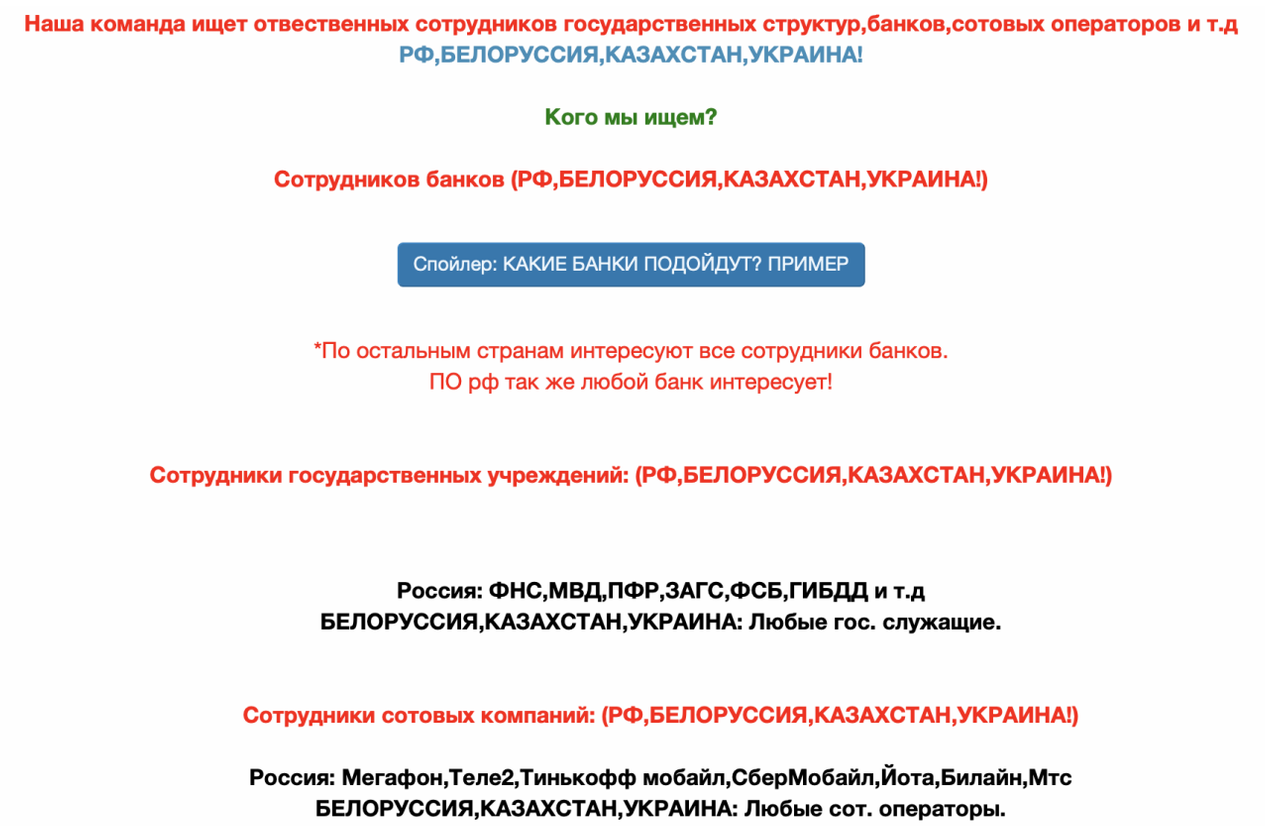

Рис. 7. Оголошення про пошук інсайдерів

3. Види шкідливого програмного забезпечення

Складність класифікації ШПЗ полягає в широкому функціоналі таких програм. Наприклад, ШПЗ *Agent Tesla* виконує функції кейлогера (keylogger), викрадача інформації (stealer) та є вдосконаленим трояном віддаленого доступу (RAT). З огляду на базові функції ШПЗ можна поділити на види, про які йдеться нижче.

Вірус. Основна функція – самореплікація (саморозмноження) в комп'ютерній системі, за рахунок якої він стає здатним впроваджувати свій код в інші програми, тим самим заражаючи їх. Заражене ПЗ стає здатним далі також самореплікувати код вірусу в інші ПЗ. Чистий вірус не має жодної іншої логіки, крім самореплікації.

Наразі найпоширенішими вірусами є макровіруси (інструкції, які приєднані до файлів офісних документів), що впроваджуються у файли типу .docx, .xlsx та інші.

Троян. Основна функція – обманювати жертв за рахунок застосування оболонки безпечного ПЗ. Порівняно із вірусом (а також з безліччю інших ШПЗ), троян не має як таких алгоритмів виконання, а є лише оболонкою для інших ШПЗ.

Хробак. Основна функція – самореплікація в комп'ютерній мережі, завдяки якій він стає здатним дублювати себе як у межах однієї системи, створюючи численні копії в каталогах, так і переміщаючись в інші системи комп'ютерної мережі, створюючи в кожній окремій свою копію.

На відміну від вірусу, що має точно такий самий механізм самореплікації, хробак не впроваджується в уже наявне ПЗ, а створює свою копію як окремий файл.

Шифрувальник (вимагач). Основна функція – шифрування файлів на системі жертви таким чином, щоб жертва не могла відновити все раніше зашифроване, що призводить до втрати всіх файлів. Часто шифрувальника також називають вимагачем, оскільки трапляються випадки, коли ШПЗ пропонує за викуп надати ключ розшифрування (рис. 8).

Рис. 8. Повідомлення шифрувальника (вимагача)

Локер. Основна функція – блокування дій жертви під час роботи в системі. У такому разі жертва або не може посувати мишкою, або не може переглядати файли, або зовсім може не мати доступу до файлової системи. Локера також іноді називають вимагачем, коли таке ШПЗ блокує екран жертви і виводить на екран поле введення пароля розблокування і реквізити з необхідністю «викупити» можливість далі користуватися системою.

На відміну від шифрувальника, що блокує доступ до файлів за допомогою їхнього шифрування, локери використовують блокування інтерфейсу, не шкодячи самим файлам.

На відміну від вірусів, троянів і хробаків, які не мають у своєму виконанні деструктивної логіки, шифрувальники представляють логіку руйнування.

Програма віддаленого доступу. Програма віддаленого доступу сама по собі не є ШПЗ, проте може використовуватися як така. Програми віддаленого доступу забезпечують передачу даних від однієї системи до іншої. Супутні дії (у тому числі деструктивні) можуть розглядатися як комбінація застосувань кількох програм. Програми віддаленого доступу, що використовуються як ШПЗ, також називають RAT (Remote Access Trojan).

Стілер. Основна функція – автоматична крадіжка інформації з системи жертви. Стілери мають багато реалізацій, починаючи від програм-шпигунів (Spyware), що зчитують інформацію в потоковому режимі з клавіатури та веб-камери, закінчуючи стілерами, що розміщені для автоматичного запуску на флешці або у мікропроцесорі Arduino.

Руткіт. Основна функція – приховування дій, видалення слідів або забезпечення відмовостійкості заданих програм. Руткіт не має конкретної деструктивної логіки, на відміну від шифрувальників, локерів та стілерів, але водночас забезпечує приховування їхніх дій або запобігання передчасному їхньому вимкненню, тобто забезпечують безперебійність виконання конкретно заданих зовнішніх функцій.

Буткіт. Основна функція – виклик програм до завантаження операційної системи, внаслідок чого буткіт стає здатний ефективно приховувати раніше запущені процеси, які не можна буде побачити стандартними засобами ОС.

Ботнет. Основна функція – це кооперування безлічі заражених жертв (ботів) з метою здійснення запланованої дії, що вимагає багато обчислювальних ресурсів. Прикладом таких ШПЗ можуть слугувати майнери криптовалют, які обчислюють необхідний ґеш у завданні типу Proof-of-Work. Також прикладом ботнетів може слугувати атака розподіленої відмови в обслуговуванні (DDoS).

Ботнет може бути як централізованим, так і децентралізованим. Остання форма також може бути поділена на два види – підконтрольний і

безконтрольний ботнет. У першому випадку існує контролюючий вузол, у той час як у другому випадку контролю дій не існує зовсім.

Спамер. Основна функція спамера – створення, видача або заміна рекламних банерів у браузерах, застосунках, сайтах, а також можливе надсилання повідомлень у месенджерах, соціальних мережах і поштою. Цей вид ШПЗ також називають рекламними програмами (Adware).

Установник (завантажувач, дропер/лоадер). Основна функція – автоматичне завантаження і запуск програм (рис. 9). Певною мірою установники схожі з програмами віддаленого доступу – вони створені для транспортування даних. Але на відміну від програми віддаленого доступу, дії якої здійснюються ручним способом і спрямовані від зловмисника до жертви, установники діють повністю автономно за конкретно заданим алгоритмом, а їхні дії протилежні віддаленому доступу і спрямовані від жертви до зловмисника.

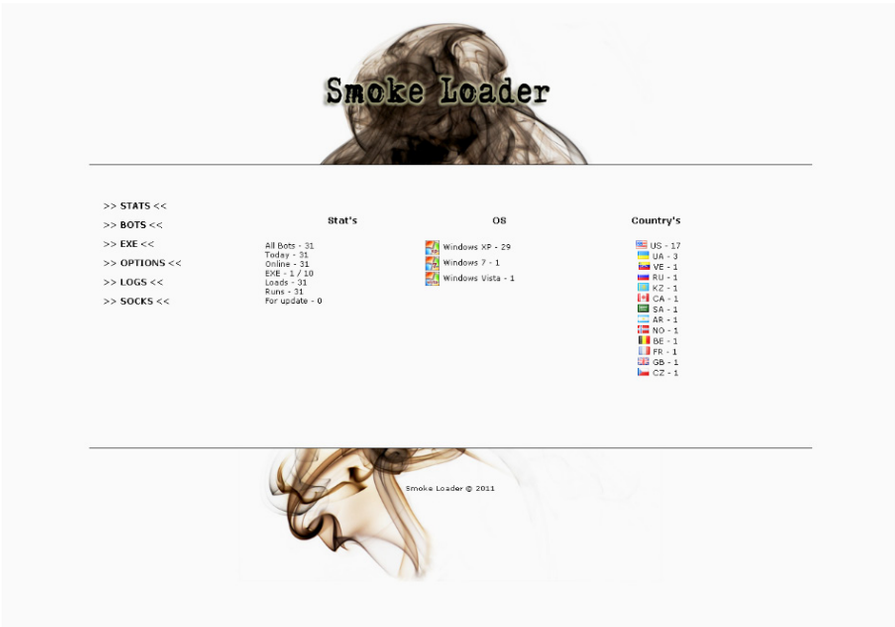

Рис. 9. Меню налаштування ШПЗ типу установника

Логічна бомба. Основна функція – зчитування умови, за якої відбуватиметься розпакування та/або запуск певного ПЗ. На відміну від безлічі інших ШПЗ, логічна бомба не самодостатня і потребує додаткової логіки виконання (шкідливого навантаження).

Очищувач. Основна функція – безповоротне видалення всіх можливих файлів на системі жертви.

Ініціалізатор. Основна функція – забезпечення автоматичного запуску ШПЗ операційною системою після свого старту. Є одним із найпоширеніших помічників за рахунок своєї відносної простоти і можливості відтворювати виконання програм навіть після перезапуску системи.

За функціями ШПЗ можна також розділити на 3 категорії (табл. 1):

- **виконувачі** – безпосередньо виконують шкідливу дію щодо системи або користувача;
- **розповсюджувачі** – здійснюють доставку ШПЗ від однієї системи до іншої;
- **помічники** – забезпечують відмовостійкість, живучість та прихованість інших ШПЗ.

Таблиця 1. Категорії ШПЗ за функціями

ВИКОНУВАЧІ	РОЗПОВСЮДЖУВАЧІ	ПОМІЧНИКИ
Шифрувальник	*Троян*	*Вірус*
Локер	*Хробак*	*Логічна бомба*
Стілер	*Програма віддаленого доступу (ПВД)*	*Руткіт*
Спамер		*Буткіт*
Ботнет	*Установник*	*Ініціалізатор*
Очищувач		

Часто ШПЗ є композицією кількох видів і категорій програм, зокрема:

- Виконувач + Розповсюджувач:
  - Хробак + Шифрувальник
  - Троян + Стілер
  - Хробак + Ботнет
  - Троян + Спамер
  - ПВД + Стілер
- Виконувач + Помічник:
  - Буткіт + Локер
  - Руткіт + Спамер
  - Вірус + Ботнет
- Виконувач + Виконавець:
  - Шифрувальник + Локер
  - Спамер + Стілер
- Помічник + Розповсюджувач:
  - Руткіт + ПВД
  - Вірус + Установник
- Помічник + Помічник:
  - Руткіт + Вірус
  - Вірус + Руткіт
- Розповсюджувач + Розповсюджувач:
  - Троян + Хробак
  - Хробак + Троян
  - Троян + ПВД
  - ПВД + Троян
  - Хробак + ПВД

- Виконувач + Помічник + Розповсюджувач:
  - Ботнет + Буткіт + Хробак
  - Стілер + Логічна бомба + Троян
  - Спамер + Вірус + Установник
- інші композиції.

4. Ознаки ураження ШПЗ

Поміж загальних ознак, таких як повільна робота комп'ютера (мобільного пристрою), поява рекламних повідомлень, постійні безпричинні перезавантаження, відключений антивірус, значна мережева активність, брак системних ресурсів, поява на робочому столі чи екрані смартфону невідомих іконок або іконок програм, які ви не встановлювали, тощо, можна виділити кілька специфічних ознак.

Підозріла активність акаунтів у соціальних мережах, поштових акаунтів тощо.

- вам прийшло повідомлення, що хтось намагався увійти до ваших акаунтів Facebook, Twitter, Gmail тощо;
- ви помітили IP-адреси, з яких не здійснювали доступ до своїх акаунтів, чи підозрілі прилади, які здійснювали доступ;
- ви помітили імейли, дописи, пости, фото, які особисто не додавали або не надсилали.

Дії:

- негайно змінити усі паролі, встановити двофакторну автентифікацію (2FA);
- перевірити систему антивірусом чи іншою програмою із виявлення ШПЗ;
- звернутися по допомогу до спеціалістів з інформаційної безпеки (IT-департамент, приватні організації).

Вам надійшло повідомлення від вашого банку про списання або спробу списання коштів.

Дії:

- звернутися до служби підтримки банку та повідомити про підозрілу активність, заблокувати банківський рахунок та платіжні картки;
- змінити паролі до банківських рахунків, встановити 2FA;
- перевірити систему, в тому числі мобільний пристрій, антивірусом чи
- іншою програмою із виявлення ШПЗ;
  звернутися по допомогу до спеціалістів з інформаційної безпеки (IT-департамент, приватні організації).

Ви помітили підозрілу активність операційної системи:

- система завантажена та зависає;
- файли стали недоступними;
- ви помітили файли із підозрілим розширенням;
- на робочому столі та в папках з'явилися підозрілі файли, а вам надійшло повідомлення, що ваші файли зашифровано.

Дії:

- вимкнути комп'ютер та звернутися по допомогу до спеціаліста.

Якщо файли все ж були зашифровані, можна спробувати визначити тип вимагача та пошукати дешифратор, хоча ймовірність повернути файли за відсутності резервних копій мінімальна.

Як визначити, яким типом вимагача (ransomware) була уражена система:

- визначити розширення, яке додає файлам ransomware: це може бути «.KICK», «.crash», «.harma», «.PLUT», «.wal», «.txt», «.FREDD» та сотні інших;
- із відкритих джерел встановити, чи було випущено дешифратор для цього типу ransomware, АБО скористатися сайтом https://id-ransomware.malwarehunterteam.com.

Ознаки ураження ШПЗ мобільного пристрою:

- пристрій працює значно повільніше, ніж зазвичай, зависає, батарея розряджається значно швидше, ніж зазвичай;
- з'явилися іконки програм, яких не встановлювали; замість звичного веб-браузера запускається інший;
- невідомі програми просять надати їм root-права (root-права – це права суперкористувача на пристроях під управлінням операційної системи «Android». Основними цілями root-прав є зняття обмежень виробника чи оператора зв'язку, маніпулювання системними програмами й можливість запуску застосунків, що вимагають прав адміністратора);
- програми просять надати їм права чи доступ до ресурсів, які не властиві їх функціональному призначенню (наприклад, ви встановили програму «Ліхтарик» і помітили, що вона просить доступ до функції відправки або зчитування СМС, ваших фотографій тощо);
- ви помітили списання коштів із мобільного рахунку або/а також підписки на платні сервіси.

Висновки

Як мінімізувати ризики та що робити, якщо я став(ла) жертвою ШПЗ:

1. Використання лише ліцензійного програмного забезпечення та користування програмним забезпеченням останніх версій. Увімкніть автоматичні оновлення для операційних систем, програм. Встановлюйте та використовуйте лише те програмне забезпечення, якому довіряє ваша організація (як приклад, використання «AppLocker»).
2. Не відкривайте підозрілі додатки до імейлів; не встановлюйте підозрілі розширення для інтернет-браузерів чи інші програми із сумнівною репутацією. Вимкніть використання макросів (використовуються в багатьох офісних продуктах, наприклад, у Microsoft Office, CorelDRAW, Notepad++). Якщо ви завантажили документ з невідомого джерела або він прийшов від невідомого чи підозрілого адресата та просить активувати макрос – **не робіть цього.** Якщо це можливо, під час використання віддаленого доступу дозволити підключення лише визначеним користувачам за допомогою «білого списку» IP-адрес (IP-whitelisting). Не користуйтеся чужими чи знайденими зовнішніми носіями інформації (флешками, дисками тощо).