4. ЗАХИСТ ВІД ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

4.1. Найпоширеніші види шкідливого програмного забезпечення.

4.2. Основні технології захисту.

4.3. Віртуальні машини (пісочниця).

4.1. Найпоширеніші види шкідливого програмного забезпечення.

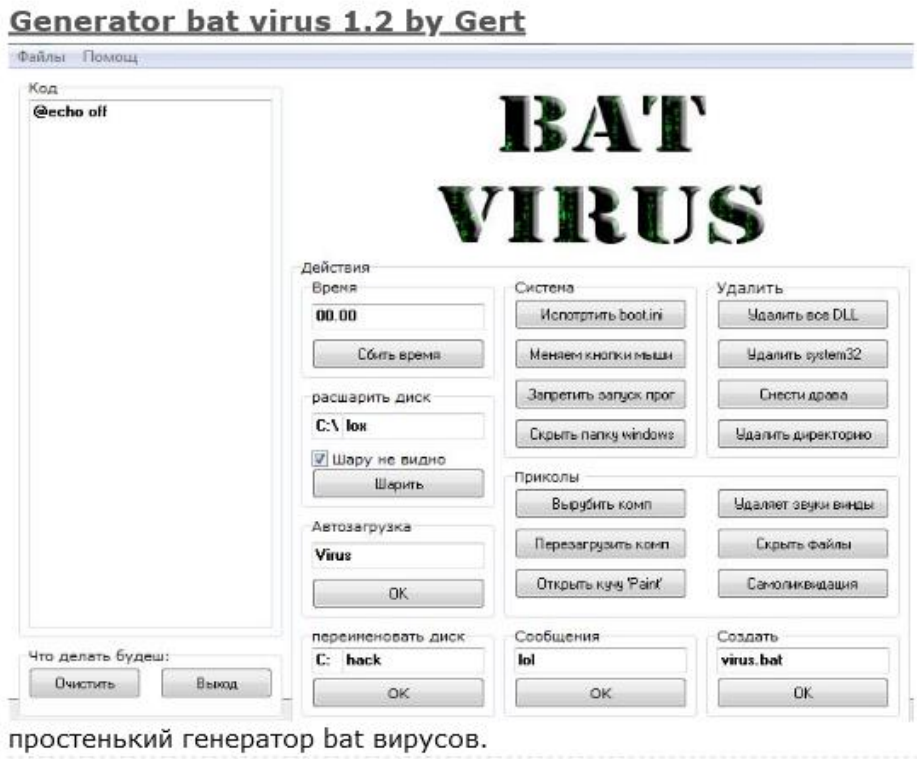
Ідея вірусу в комп'ютерах була вперше запропонована математиком Джоном фон Нейманом у 1949 році з його тезою про те, що програмне забезпечення може відтворювати себе. У наступні десятиліття з'явилися нові теоретичні підходи та були поставлені експерименти з кодом. Перший «практичний» вірус Creeper був розроблений в 1971 році і поширився через Arpanet. До 1980 у світі налічувалося понад 200 вірусів, а до 1990 – близько 3000.

```
BBN-TENEX 1.25, BBN EXEC 1.30
@FULL
@LOGIN RT
JOB 3 ON TTY12 08-APR-72
YOU HAVE A MESSAGE
@SYSTAT
UP 85:33:19    3 JOBS
LOAD AV    3.87    2.95    2.14
JOB  TTY   USER        SUBSYS
1    DET   SYSTEM      NETSER
2    DET   SYSTEM      TIPSER
3    12    RT          EXEC
@
I'M THE CREEPER : CATCH ME IF YOU CAN
```

Комп'ютерний вірус – це невелика програма, яка здатна до саморозмноження й виконання різних деструктивних дій. На початку епохи комп'ютерних вірусів розробка вірусоподібних програм носила чисто дослідницький характер, поступово перетворюючись на відверто вороже протистояння користувачів та безвідповідальних, і навіть кримінальних «елементів». В ряді країн карне законодавство передбачає відповідальність за комп'ютерні злочини, в тому числі за створення та розповсюдження вірусів.

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Віруси діють тільки програмним шляхом. Вони, як правило, приєднуються до файлу або проникають всередину файлу. У цьому випадку кажуть, що файл заражений вірусом. Вірус потрапляє в комп'ютер лише разом із зараженим файлом. Для активізації вірусу потрібно завантажити заражений файл, і тільки після цього вірус починає діяти самостійно. Деякі віруси під час запуску зараженого файлу стають резидентними (постійно знаходяться в оперативній пам'яті комп'ютера) і можуть заражати інші файли та програми, що завантажуються. Інші різновиди вірусів відразу після активізації можуть спричиняти серйозні пошкодження, наприклад, форматувати жорсткий диск.

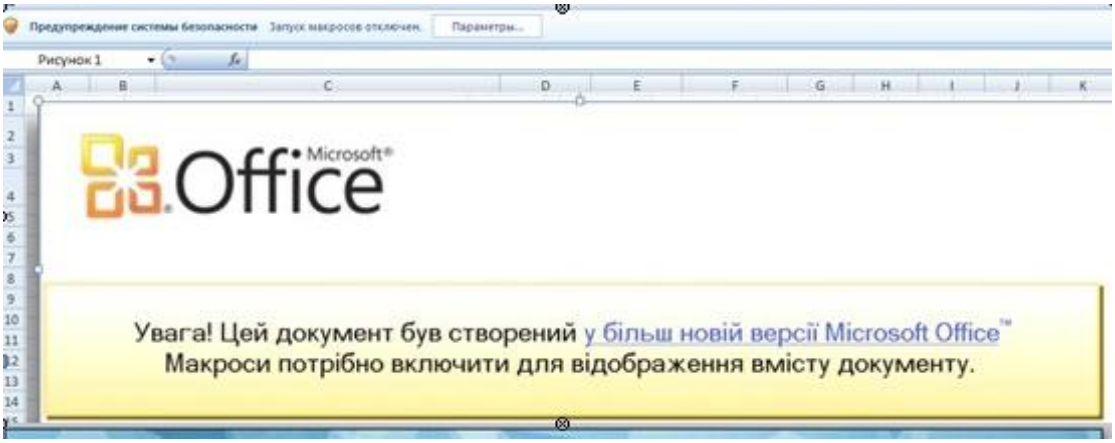


простенький генератор bat вирусов.

Дія вірусів може проявлятися по різному: від різних візуальних ефектів, що заважають працювати, до повної втрати інформації. Більшість вірусів заражують виконавчі програми, тобто файли з розширенням .exe та .com.

У даний час не існує єдиної системи класифікації та іменування вірусів (хоча спроба створити стандарт була зроблена на зустрічі CARO у 1991 році). Прийнято розділяти віруси:

- по уражаємих об’єктах (файлові віруси, завантажувальні віруси, скриптові віруси, макровіруси, віруси, що вражають вихідний код);
- по уражаємим операційним системам і платформам (DOS, Microsoft Windows, Unix, Linux);
- за технологіями, використовуваними вірусом (поліморфні віруси, стелс-віруси, руткіти);
- за мовою, на якій написано вірус (асемблер, високорівнева мова програмування, скриптова мова та ін.);
- по додатковій шкідливої функціональності (бекдори, кейлоггери, шпигуни, ботнети та ін.).

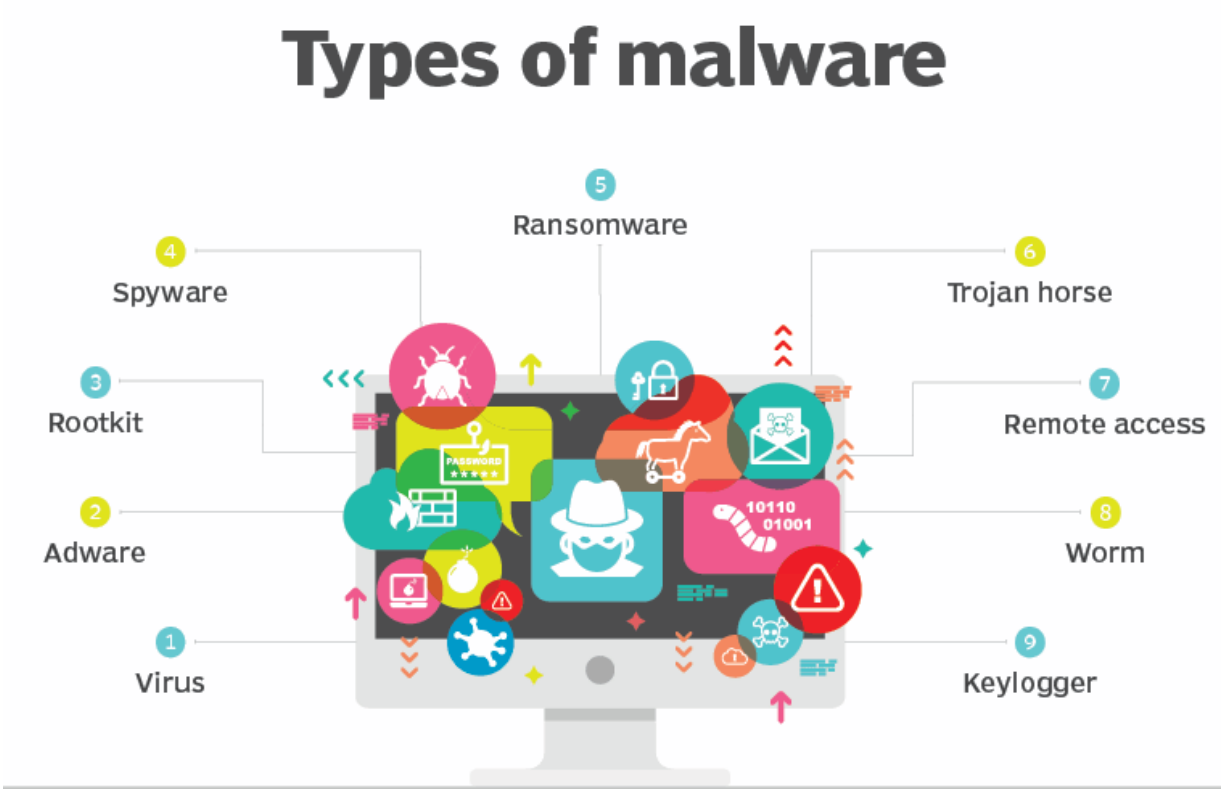


Термін «комп’ютерний вірус» часто неправильно використовується як загальний термін для позначення всіх підозрілих програм, плагінів або коду, які заражають програмне забезпечення, комп’ютери та файли. Насправді правильним загальним терміном для таких програм є шкідливе програмне забезпечення, категорія комп’ютерних вірусів є лише одним із типів. У світі поширений англійський термін – malware, malicioussoftware (шкідливе програмне забезпечення). Однак у вжитку укорінилась загальна назва «вірус», як синонім до шкідливих програм, це є поняттям слова вірус у широкому сенсі.

Інші основні типи шкідливих програм:

- бекдор програми – надають віддалений доступ до комп’ютера для зловмисників;
- хробаки – окремий вид шкідливих програм, головною задачею яких є розмноження серед комп’ютерів в мережі;

- адваре – рекламні модулі;
- дропери – по суті, це програми, які встановлюють троянські програми на комп'ютери користувачів;
- даунлоадери – маленькі троянські програми, у яких є усього одна функція – завантажити велику троянську програму.



Троянська програма – це програма, яка має приховані функції. Така назва виникла тому що перші програми цього типу потрапляли на комп'ютери під виглядом корисних програм, які користувачі завантажували й запускали власноруч. Зараз такий варіант розповсюдження також присутній, часто користувачі самі запускають подібні програми, намагаючись завантажити зламані неліцензійні версії програмного забезпечення чи програми для генерації зламаних серійних ключів.

Хробак – це програма, яка розмножується, від одного комп'ютера до іншого. Механізми можуть бути дуже різними: електронна пошта, локальна мережа чи USB-накопичувач. Так, хробак може скопіювати свої файли на флешку та створити відповідний файл автозавантаження і як тільки ви під'єднаєте флешку до комп'ютера, на ньому одразу ж активізується хробак.

При цьому слід зазначити, що хробаки які розповсюджуються через пошту чи через флешки, практично ні в чому не відрізняються, вони лише використовують різні шляхи поширення.

Бекдор – програма «чорний хід», зазвичай шкідливі програми цього типу дають зловмиснику віддалений доступ та можливість керування комп’ютером користувача. Методи їх дії бувають різними, наприклад така програма може відкрити мережевий порт, за допомогою якого зловмисник отримає повний доступ до ураженого комп’ютера: зможе надсилати різні команди, запускати інші програми.

Дропер – це по суті інсталятор троянської програми. Оскільки троянська програма це багатокомпонентний елемент, який потребує встановлення в системі певних драйверів та інших компонент, то цю задачу виконує дропер. Після того як дропер було активовано в системі, він встановлює всі частини троянської програми та активує її.

Завантажувальник – це по-суті троянська програма, мета якої – завантажити з мережі Інтернет іншу троянську програму. Характерна риса таких програм – вони дуже маленького розміру (кілька десятків кілобайт), а отже можуть завантажитись і активізуватись дуже швидко. І вже після вкорінення в системі, даунлоадер завантажує основну троянську програму. При цьому може бути завантажений, як дропер, так і окремі компоненти троянця, які будуть методично інсталюватись на комп’ютер. Отже, якщо у вас на комп’ютері був знайдений завантажувальник, то варто шукати й інші троянські програми.

Діалери – це програми-дзвонилки, вони були дуже популярні у часи активного використання модемів і телефонних ліній. Сучасні модифікації діалерів використовують дещо інші механізми, зокрема, це можуть бути дзвінки через Skype, відкриття певних спеціалізованих сайтів.

Руткіт – це спеціальний вид троянських програм, головна мета якого – максимально глибоко інсталюватись у систему, щоб його було якомога важче знайти і видалити. Як правило, руткіти містять драйвери операційних систем і працюють на досить низькому рівні. Руткіти використовуються для маскування всіх інших компонентів троянця від детектування. Тобто руткіт у системі призваний приховати роботу інших компонентів трояна. Головна проблема в тому, що руткіти дуже важко знайти і ще важче видалити з системи. Далеко не кожна антивірусна програма може з цим впоратись.

Умовно шкідливе ПО або потенційно небажані програми (PUA, Potentially Unwanted Application) – це широка категорія програмного забезпечення, яке не можна однозначно віднести до шкідливого ПЗ за аналогією з такими безумовно шкідливими програмами, як віруси або трояни. Ці програми можуть інсталювати додаткове небажане ПЗ, змінювати поведінку або налаштування цифрового пристрою, а також виконувати неочікувані для користувача дії або не підтверджені ним.

Категорії програмного забезпечення, які можна розглядати як умовно шкідливе: ПЗ, що відображає рекламу або виконує завантаження інших програм, різноманітні браузерні панелі інструментів, ПЗ з оманливою поведінкою, пакетне ПЗ, ПЗ для відстеження користувацьких операцій, майнери криптовалют, програми для очищення реєстру (тільки в операційних системах Windows), будь-яке інше сумнівне ПЗ або програмне забезпечення із застосуванням противоправних або принаймні неетичних практик ведення бізнесу (незважаючи на те, що його використання може сприйматися як правомірне), яке кінцевий користувач може розцінити як небажане, коли він дізнається про особливості роботи цього ПЗ після інсталяції.

Потенційно небезпечна програма – це легітимне програмне забезпечення (можливо, комерційне), яке може несанкціоновано використовуватись зловмисниками для досягнення їх цілей. Рекламний модуль – адваре програми, мабуть найменш небезпечні з усіх шкідливих програм, але через дуже широку розповсюдженість і просто величезну зухвалість їх авторів в останній час вони стали досить неприємними. Задача рекламного модуля – показати вам рекламу. Це може відбуватись у різних проявах, наприклад у вас можуть самостійно відкриватись певні сторінки у браузері, які ви не відкривали – це будуть сайти з

дивною рекламою або просто сайти, які ви не збирались відвідувати. Тобто зловмисники таким чином підвищують відвідуваність певного сайту або провокують вас подивитись певну інформацію. Також рекламні модулі можуть показувати різні банери чи навіть вставляти банери на той сайт, де їх не було, або ж підмінювати рекламні повідомлення на сайтах. Наприклад якщо ви шукаєте певну інформацію у Гугл, то видача пошукового запиту містить 2 категорії – безкоштовні пошукові запити та рекламні повідомлення, рекламні модулі можуть підміняти одні рекламні повідомлення на інші й в результаті ви будете бачити не ту інформацію яку запитували, а те, що хоче вам показати власник рекламного модуля. Даний механізм підміни пошукових видач отримав назву «чорного SEO».

Основні джерела зараження ПК та мобільних пристроїв.

Найголовнішим джерелом вірусів буде той канал, який забезпечує максимальний обмін інформацією Вашого ПК з іншими. Тож, головним джерелом зараження є глобальна мережа Інтернет.

На жаль віруси існують практично для всіх каналів зв’язку і зловмисники охоче використовують ті, якими більш активно користуємось ми. Зараз найбільше користувачі використовують вебсайти та електронну пошту. Існують віруси, які розповсюджуються через Skype та інші месенджери. У свій час існували популярні віруси для RRS клієнтів, однак вони використовуються не

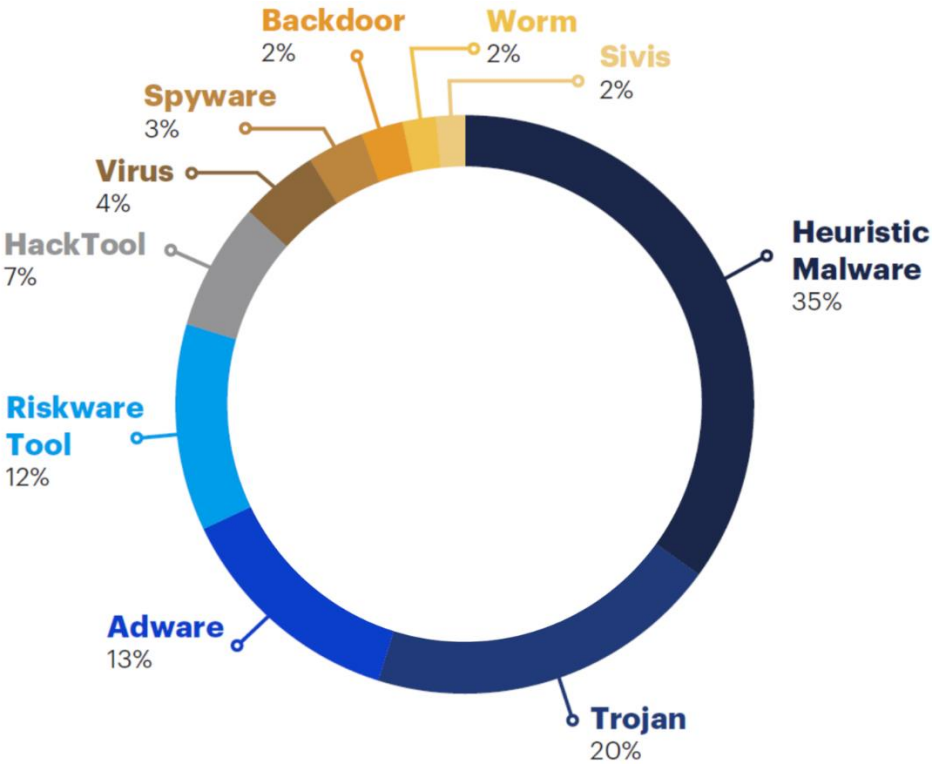
так широко. А от браузерами для відвідування сайтів користуються всі без виключення і як наслідок це джерело є найбільш популярним.

Другим по популярності джерелом зараження є електронна пошта. На початку 2000-их років практично всі загрози шли саме з електронної пошти. Зараз об’єм заражень через е-мейли не на стільки високий, однак все ж зустрічаються масові розсилки, в яких користувачі отримують листи, які маскуються під звичайну пошту від знайомих чи колег. І наприклад якщо вірус заразив комп’ютер Вашого знайомого і від нього пише вам листа, то вірогідність того що ви відкриєте цього листа дуже висока. Часто відбуваються масові СПАМ-розсилки, які маскують під повідомлення від банків, і взагалі під певну корисну інформацію: фото, архіви, які Вам пропонують подивитись. Звичайно ж після відкриття такого файлу нічого корисного для вас крім зараження Вашого ПК не відбудеться.

Третім за популярністю способом зараження ПК є змінні накопичувачі, перш за все це флеш диски та USB-накопичувачі. Перші комп’ютерні віруси взагалі почали свою історію саме зі змінних накопичувачів, тільки тоді це були дискети – гнучкі магнітні диски. Різниця лише у тому, що старі віруси не завжди могли запускатись автоматично і чекали коли користувачі самі запустять певну програму з диску, сучасні ж віруси можуть запускатись автоматично одразу після підключення флешки до комп’ютера.

За масовістю – найбільш розповсюдженими є рекламні модулі. На другому місці за популярністю є троянські програмі.

Із 2015 року небувалої активності набули програми-криптувальники, які шифрують дані та вимагають викуп для розблокування. На жаль, для шифрувальників використовують криптостійкі алгоритми і гарантувати розшифрування ніхто не може. Головна порада — не платити викуп. Відправивши гроші кіберзлочинцям, ви лише підтвердите, що вимагацьке ПЗ влучило в ціль; водночас ніхто не гарантує, що ви отримаєте потрібний ключ дешифрування.



Ознаки зараження комп’ютера вірусами:

- поява незвичайних системних повідомлень, наприклад, що програма з незнайомою назвою виконала неприпустиму операцію і буде закрита;
- повідомлення про брак системних ресурсів;
- поява рекламних банерів у той час, коли ви не працюєте в Інтернеті;
- поява вікон із попередженням про блокування та прохання надіслати SMS на вказаний номер;

- повідомлення від антивірусних програм, які ви не встановлювали на свій комп’ютер;
- різке зменшення вільного місця на жорсткому диску, хоча ви нічого великого не записували і не встановлювали громіздких програм;
- збільшення трафіку під час роботи в Інтернеті. Це особливо помітно тим, хто оплачує доступ до Інтернету залежно від обсягу інформації. Для тих, хто користується безлімітними тарифами, може бути помітним зменшення швидкості доступу до мережі;
- поява на флешці файлів, які ви туди не записували (особливо з розширенням .exe). Поява на знімному носії файлу autorun.inf та папки Recycler. При штатному безпечному видаленні флешки операційна система повідомляє про те, що пристрій не може бути зупинено прямо зараз, хоча файли на флешці не відкриті в жодній програмі;
- повідомлення від встановлених антивірусних програм про виявлення загрози.

4.2. Основні технології захисту.

Сигнатурний аналіз.

Із самого початку появи антивірусних програм, програмісти зрозуміли, що вірус потрібно детектувати за певною характеристикою, і, оскільки, спочатку віруси були досить незначними, і володіли достатньо унікальним кодом, використовували так звану сигнатуру. Сигнатура – це послідовність байт у певній програмі чи контрольна хеш сума деякого блоку програми, яка характеризує його. Тобто, антивірус знаходив у програмі деяку частину коду, яка була характерною лише для певного вірусу і якщо така частина була знайдена в певній програмі, то вважалось, що програма заражена вірусом, або вона є троянською програмою чи рекламним модулем. Сигнатура (signature – підпис) може розглядатися у більш широкому сенсі – унікальна послідовність, ланцюг, інформація, які характеризують певну загрозу. Це може бути і алгоритм, певна послідовність байт, може бути контрольна сума, сигнатура поведінки програми у системі.

У чому проблема сигнатурного пошуку? Для того щоб створити сигнатуру для певного вірусу, потрібно щоб він був у вірусної лабораторії. Не можна створити сигнатуру для вірусу якого ще не має, оскільки не має тієї унікальної послідовності яку можна додати у вірусну базу. Це основна проблема сигнатурного детектування вірусів. З іншого боку, у сигнатур є свої переваги. Якщо антивірус за допомогою сигнатур знайшов вірус, значить він знайшов у файлі чітку послідовність характерну для певного вірусу, він може назвати цей вірус, по цьому імені можна знайти опис того, що ця програма робить, а виходячи з такої інформації можна знати як даний вірус нейтралізувати, які операції потрібно зробити, які шкідливі функції він виконує, і як можна виправити наслідки їх дій. Тобто сигнатура характеризує якийсь конкретний вірус і дає переваги у подальшій його обробці антивірусом.

Із часом стало очевидно, що боротися з вірусами лише за допомогою сигнатурного аналізу не можливо, оскільки якщо ви сьогодні оновили вірусні бази, а завтра з’явився новий вірус, то Ваш антивірус не зможе його детектувати. Отже, антивірусна програма постійно перебуває позаду.

Евристичний аналізатор.

Наступною технологією, яка з'явилась досить давно є евристичний пошук, зараз ця технологія використовується в антивірусних програмах разом із сигнатурними методами.

У вірусів окрім унікальних характеристик є певні загальні властивості, певна модель поведінки яка їх характеризує, особливості, які притаманні для шкідливих програм і не характерні для звичайних програм. Евристичний аналізатор аналізує код програми, знаходить у ньому певні закономірності, притаманні для різних класів шкідливих програм і на основі цього приймає рішення щодо можливого визначення програми шкідливою. Часто антивірус повідомляє, що «Даний файл є підозрілим, можливо в ньому є такий-то вірус…». Сенс у тому, що евристичний аналізатор не знає точно який це вірус, не знає точно чи вірус це взагалі. В чому перевага евристичних аналізаторів? Вони дозволяють визначати загрози, які ще не були додані у сигнатурні бази, нові, ще невідомі загрози. Навіть якщо у вас не було можливості оновити вірусні бази, евристичний аналізатор зможе заблокувати ймовірні загрози.

Які недоліки евристичного аналізу? Перш за все це вірогідність хибного спрацювання. Евристичний аналізатор може знайти у програмі певну підозрілу діяльність, але її наявність ще не робить програму шкідливою. Можливо програмісти використовували при написанні програми схожі методи з тими, які використовували зловмисники. Тобто, евристичний аналізатор теоретично може помилитися, при чому, з досить великою долею вірогідності.

Автори вірусів активно протидіють евристичними аналізаторами. З’явились анти-евристичні прийоми, різні коди анти-аналізатори, щоб антивірусна програма не змогла перевірити цей код. використовувались й інші прийоми, щоб не дати можливості перевірити такі файли.

Поведінковий аналізатор.

Він схожий на роботу евристичного аналізатора, однак із тією різницею, що аналізується не код програми, а її поведінка в процесі роботи. Тобто, в системі запустилась програма і вона виконує певні дії. Наприклад, програма зберегла файл у системній папці і звернулась до Інтернет, щось завантажила, намагається цей закачаний файл запустити. Поведінковий аналізатор слідкує за діями програм і намагається зрозуміти чи є діяльність програм штатною, чи характерна для шкідливих програм. Якщо поведінковий аналізатор вважає що дана програма поводить себе як шкідлива, він може її заблокувати і навіть «відкотити» назад певні зміни у операційній системі, які зробила шкідлива програма. Поведінкові аналізатори можуть блокувати ще невідомі загрози.

Наприклад, якщо є певний алгоритм поведінки коли програма запускається, створює запис у реєстрі Windows і після цього одразу розсилає листи прикріпляючи копію себе – то це поштовий хробак. Логіка прозора – який би не був код поведінка хробака буде така сама, і тому не важливо як і на якій мові написана програма, чи є в ній шифрування чи ні, присутні анти-евристичні прийоми чи ні – діяти програма буде однаково. Тому її можна заблокувати.

Недоліки поведінкових аналізаторів. Нажаль, поведінковий аналізатор перевіряє програму тоді, коли вона вже працює. Тобто, якщо ви просто скопіюєте файли з флешки, то поведінковий аналізатор не зможе їх перевірити. У спокійному стані можна використовувати лише евристику та сигнатури. Якщо ж ви запустите програму, то спрацює поведінковий аналізатор, і добре, якщо вдасться шкідливу програму зупинити до того, як вона виконає певні шкідливі дії.

Отже, поведінковий аналізатор не забезпечує абсолютний захист. Цей модуль забезпечує дуже високий додатковий рівень захисту, але все ж таки є додатковим і саме так його варто розглядати.

Репутаційні технології.

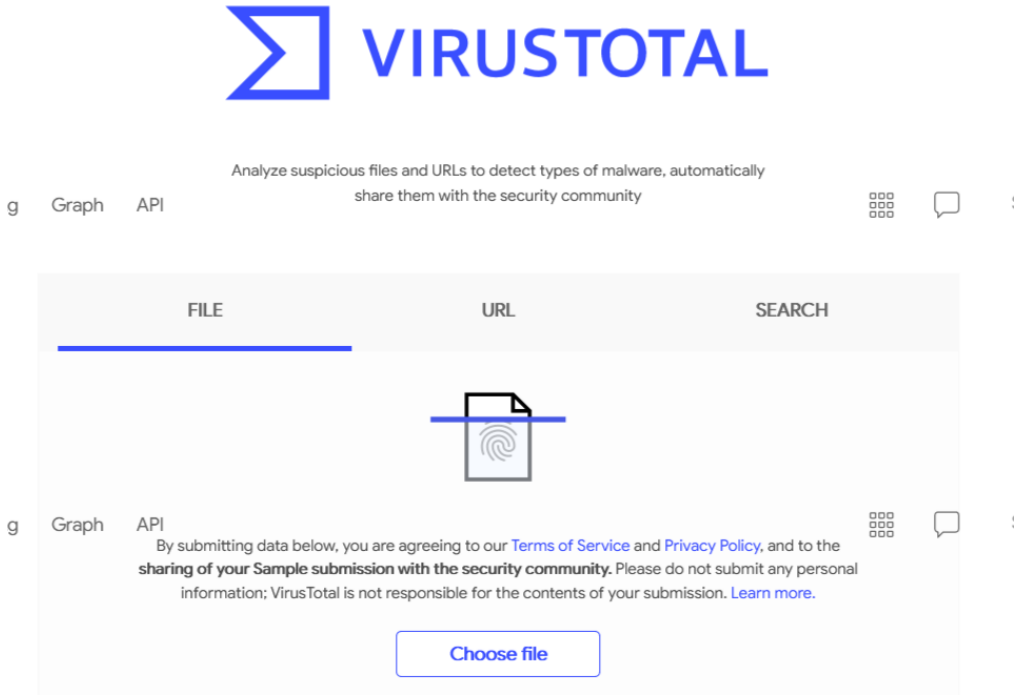
Дуже важливий момент – з розвитком Інтернет стало очевидно, що частина функцій антивірусного захисту може здійснюватися не на комп'ютері користувача, а на серверах антивірусної компанії. Антивірусні компанії запустили так звані хмарні антивірусні сервіси, а також репутаційні технології, які можна віднести до хмарних сервісів.

У чому суть репутаційних технологій? Коли на ваш комп'ютер вперше потрапляє новий файл, то для нього підраховується унікальна сигнатура, наприклад хеш-сума, певна послідовність байт, яка характеризує тільки цей файл. Вона передається на сервер і антивірус «консультується» з ним щодо наявної інформації про файл. Якщо сервер надає відповідь, що це новий файл і він до цього не зустрічався ні у кого з інших користувачів, то ви приймаєте рішення чи є ця програма шкідливою й можете залишити свій голос, сформувати репутацію цього файлу. Наприклад, користувач зазначає: «так, цей файл хороший, я його качав і хочу його запустити». Програма запускається, працює й аналізується поведінковим аналізатором. Якщо раптом виявиться що файл все таки шкідливий, на сервер передається інформація про те, що файл небезпечний і користувач помилився й для файлу сформується відповідний рейтинг. У подальшому користувач, який завантажує цей файл, навіть якщо його ще не додали в сигнатурні бази і не детектують евристичним чи поведінковим аналізатором, зможе побачити низький рейтинг довіри до файлу, і це дозволить бути більше обізнаним про можливу загрозу.

Що дають репутаційні технології? В роботі антивірусних компаній є певний виробничий процес: вірус має потрапити на комп'ютери користувачів заразити їх, після чого він потрапляє в антивірусну компанію, або антивірусна компанія сама його знайде, або користувач надішле зразок власноруч в антивірусну компанію. Часто антивірусні компанії проводять обмін зразками

вірусів. Далі буде потрібен певний час на аналіз такого файлу, який може зайняти години або дні. Після чого буде створена певний сигнатура, яка буде протестована всередині антивірусної компанії, що також займає певний час, далі створюється оновлення вірусних баз і користувачі мають ці оновлення скачати. Тобто з моменту створення загрози і першого зараження до моменту готовності антивірусу захищати користувача від даної загрози пройде певний час. Це можуть бути години, а можуть бути і дні, тобто сигнатурний метод немов запізнюється. Репутаційні аналізатори дозволяють боротись з загрозами практично в режимі реального часу, перший користувач, який стикається з файлом, вже отримає інформацію про нього, як мінімум, на рівні повідомлення, що це новий файл. За перші 5 хвилин існування у файлу вже буде певна репутація. Відповідно всі наступні користувачі вже будуть оповіщені про рівень загрози.

Хмарні технології.



Суть хмарних технологій полягає у тому, що сигнатурна перевірка файлів відбувається не у вас на комп'ютері, а на сервері антивірусної компанії. Всі відомі файли не потрібно передавати на аналіз, передаються лише нові, які визначаються на основі унікальної хеш-суми. І сервер відповідає, чи знає він про ці файли з відповідними хеш-сумам. Відповідно до рішення сервера

антивірус на вашому комп’ютері буде приймати рішення дозволити запускати ці файли чи ні. Якщо ж новий файл невідомий, то він буде переданий на сервер антивірусної компанії, де буде повністю досліджений усіма найпотужнішими антивірусними технологіями. Хмарні технології дозволяють перенести навантаження, потрібне для аналізу файлу, з вашого комп’ютера на сервер компанії, де він буде опрацьований більш якісно й не завантажуючи вашу систему.

Не існує найкращого універсального антивірусу. Він підбирається під ситуацію, під користувача, під комп’ютер на якому буде встановлений, під задачі, для яких буде використовуватись. Хороший антивірус той, який постійно працює. Якщо антивірус гальмує систему і ви його періодично вимикаєте, то це погано, адже чи не найголовнішою опцією антивірусної програми є те, що вона має постійно працювати. виключений антивірус інколи навіть гірше ніж відсутність антивірусу взагалі.

Варто наголосити, що вибір антивірусу є пошуком компромісу. Не складно зробити антивірус який буде максимально захищати від всіх загроз, можна вбудувати туди поведінковий аналізатор, зібрати сигнатури загроз із усього світу але є одна проблема – цей антивірус буде дуже сильно гальмувати роботу системи, буде займати дуже багато пам’яті, постійно видавати повідомлення, що певний файл є підозрілим. І тому його неможливо буде використовувати. Антивірусні компанії постійно йдуть на компроміс між якістю детектування і продуктивність, між автоматизацією і здатністю обробити певні загрози більше ефективно.

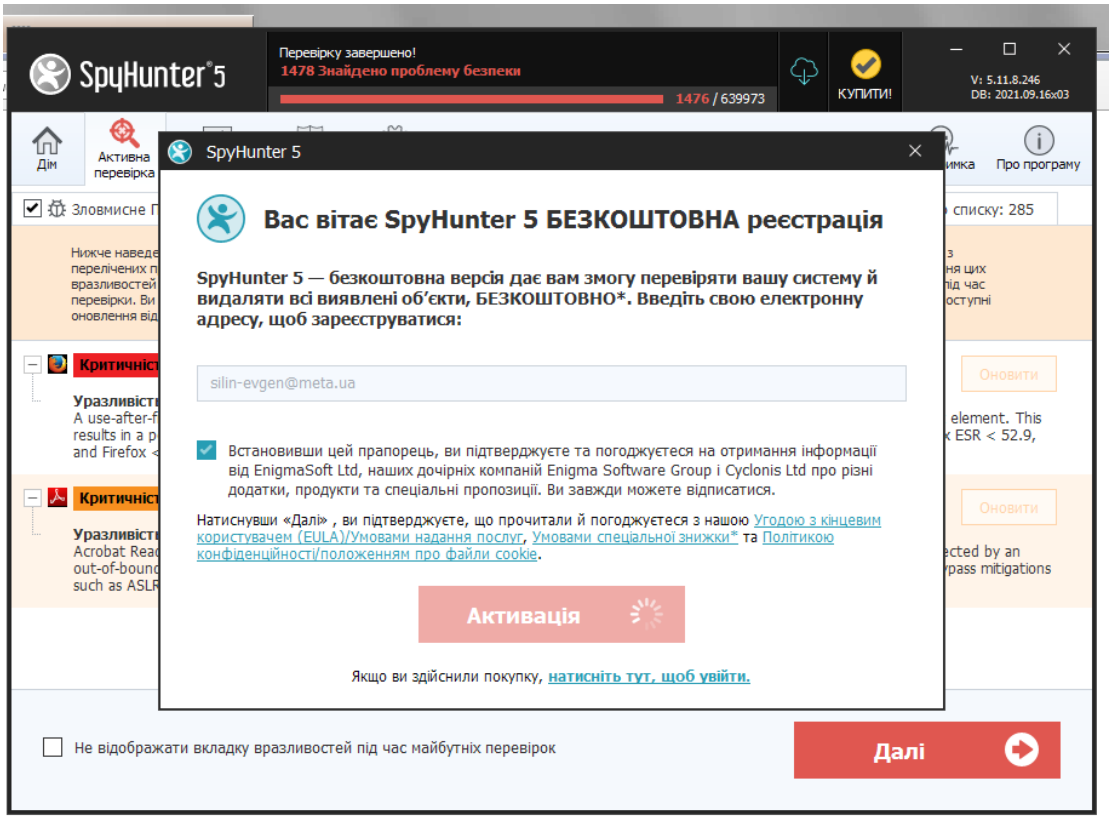
Отже, ви маєте обрати антивірус виходячи із того на скільки вам зручно ним користуватись, наскільки гарно він детектує загрози, які характерні саме для Вашого комп’ютера, виходячи із ресурсів якими ви користуєтесь, виходячи із регіону в якому перебуваєте.

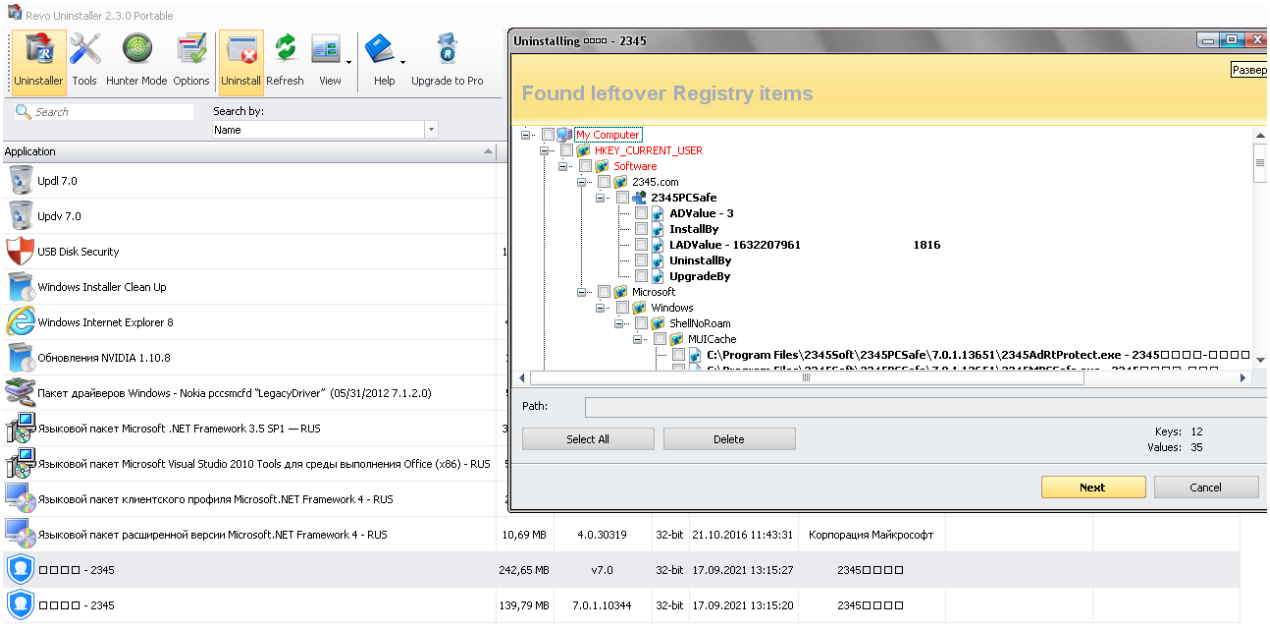
Тести антивірусного програмного забезпечення:

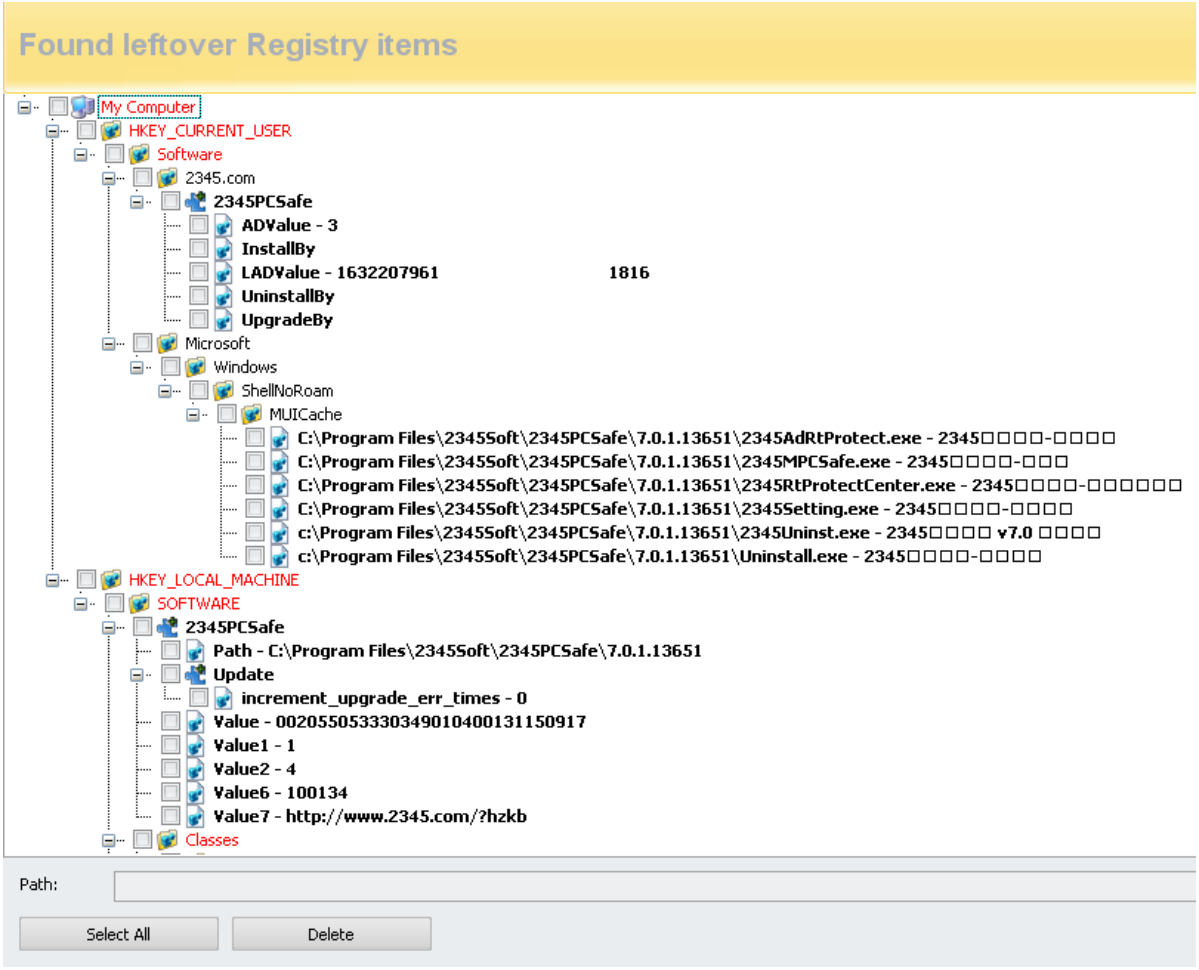
- https://www.av-test.org/en/antivirus/home-users/,
- https://www.av-comparatives.org/.

Producer		Certified	Protection	Performance	Usability
AhnLab	V3 Internet Security 9.0	TOP PRODUCT	6	6	6
Avast	Free AntiVirus 21.7 & 21.8	TOP PRODUCT	6	6	6
Avast	One Essentials 21.7 & 21.8	TOP PRODUCT	6	6	6
AVG	Internet Security 21.7 & 21.8	TOP PRODUCT	6	6	6
Avira	Internet Security for Windows 1.1	TOP PRODUCT	6	6	6
Bitdefender	Internet Security 25.0	TOP PRODUCT	6	6	6
BullGuard	Internet Security 21.0	TOP PRODUCT	6	6	6
eset	Internet Security 14.2	TOP PRODUCT	6	6	6
F-Secure	SAFE 18	TOP PRODUCT	6	6	6
G DATA	Total Security 25.5	TOP PRODUCT	6	6	6
K7 SECURITY	Total Security 16.0	TOP PRODUCT	5.5	6	6
kaspersky	Internet Security 21.3	TOP PRODUCT	6	6	6
Malwarebytes	Premium 4.4.5 & 4.4.7	TOP PRODUCT	5.5	6	6
McAfee	Total Protection 25.0	TOP PRODUCT	6	6	6
Microsoft	Defender 4.18	TOP PRODUCT	6	6	6
eScan Enterprise Security	eScan Internet Security Suite 14.0		5	6	5.5
NortonLifeLock	Norton 360 22.21	TOP PRODUCT	6	6	6
PC Matic	PC Matic 3.0		5.5	6	4.5
TOTAL AV	Total AV 5.15	TOP PRODUCT	6	6	6
TREND MICRO	Internet Security 17.0	TOP PRODUCT	6	6	6
VIPRE	VIPRE AdvancedSecurity 11.0	TOP PRODUCT	6	6	6

ESET AV Remover допоможе видалити практично будь-яке антивірусне програмне забезпечення, інстальоване в системі. Необхідно завантажити відповідний інструмент та запустити файл на виконання: https://www.eset.com/ua/support/av-remover/.







Для смартфонів характерні ті ж самі загрози, що і для персональних комп'ютерів, оскільки телефон, по суті, і є комп'ютером. Сьогодні існує величезна кількість загроз: віруси, троянські програми, мережеві хробаки, рекламні модулі орієнтовані на абсолютно різні платформи для мобільних пристроїв.

Краще встановлювати додатки лише з PlayMarket. Водночас, під час встановлення програми вам буде показуватись список привілеїв, які бажає отримати програма. Потрібно дуже уважно читати, що саме потребує програма. Тут має бути проста логіка. Наприклад, якщо ви встановлюєте гру, навіщо вона просить доступ до відправки sms. Звичайно, у цьому випадку це дуже підозріло і краще відмовитись від встановлення даної програми.

У налаштуваннях можна дозволити встановлення додатків не з офіційного магазину. Це пункт меню Налаштування / Безпека / Невідомі джерела. Навіть якщо ви досвідчений користувач та бажаєте встановити програму не з PlayMarket дуже важливо цей дозвіл давати саме на момент

встановлення вами програми. Під час звичайного користування смартфоном чи планшетом доцільно не вмикати цю опцію, оскільки у цьому випадку шкідливі програми не зможуть встановитись у той час, коли ви помилково перейдете за фішинговим посиланням.

Коли ви встановлюєте програмне забезпечення на смартфон, система запитує у вас дозвіл на цю операцію. На цей момент програма ще може бути не шкідливою. Але в подальшому вона може автоматично оновитися, отримати нові функцію, частина яких може бути шкідливими. Тому радимо не вмикати функцію автоматичного оновлення програм, та оновлювати необхідні вам програми вибірково, під вашим контролем, і тільки тоді, коли це дійсно необхідно. Тож ні в якому разі не вмикайте дозвіл на встановлення програм з невідомих джерел на тривалий термін.

Дії при ураженні шкідливим ПЗ.

1) Важливо розуміти, що, залежно від типу обгортки (приманки), процес інфікування може запуститися автоматично, а може очікувати остаточного підтвердження. Просто закрити документ або вкладку не завжди буде правильним рішенням. Деякі приманки розраховані на запуск саме під час закриття доданку.

Можливо, процес інфікування вже розпочався, тому потрібно якнайшвидше розірвати канал передачі інформації – висмикнути кабель із мережевої карти або вимкнути Wi-Fi. Існує можливість, що ви обірвете завантаження основної частини вірусу.

2) Зробіть резервні копії (якщо вони відсутні) найважливіших файлів та документів. У подальшому проведіть додаткову антивірусну перевірку цих даних, перш ніж їх використовувати.

3) Після того як документи будуть скопійовані (або резервні копії у вас завжди наявні), не закриваючи документа-приманки, не натискаючи ні «Ок», ні «Скасувати», вимикайте систему довгим натисканням на кнопку або ж висмикуйте кабель живлення – не завершуючи роботу штатно (це необхідно, щоб обірвати запущені процеси вірусу, якщо він уже активний). Якщо ви

плануєте звернутися за допомогою до IT-фахівця, тоді ліпше систему перевести в режим так званого гібридного сну (hibernation). Такий підхід допоможе в розслідувані інциденту.

4) Завантажити систему з live CD/USB, підготовленого на іншій системі, та провести антивірусну перевірку.

У випадку зараження вірусом-шифрувальником:

1) Зробіть фотографію (знімок екрана) повідомлення з вимогою викупу на вашому екрані.

2) Якщо це можливо, використайте антивірусне програмне забезпечення або продукти захисту від шкідливих програм, щоб видалити вимагацьке програмне забезпечення з вашого пристрою. Можливо, доведеться перезавантажити систему у безпечному режимі.

3) видалення вимагацького ПЗ не призведе до дешифрування ваших файлів, але дозволить вам виконати наступні дії без зашифровування нових файлів.

4) Якщо у вас була резервна копія, відновіть інформацію.

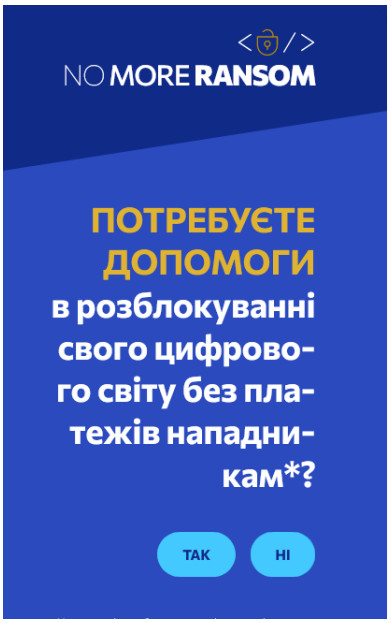
5) Не платіть викуп. Заплативши, ви фінансуватимете злочинність і заохочуватимете злочинців до нових незаконних дій. Немає жодних гарантій того, що ви отримаєте доступ до своїх даних або пристрою, і в майбутньому ви, найімовірніше, станете знову мішенню злочинців.

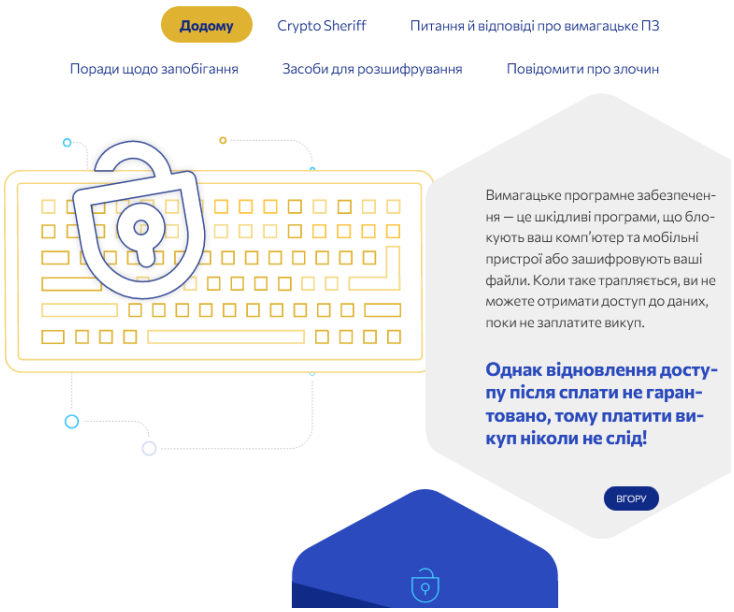
6) Якщо у вас немає резервної копії даних, відвідайте www.nomoreransom.org (https://www.nomoreransom.org/uk/index.html), щоб перевірити, чи не уражений ваш пристрій вимагацьким ПЗ, для якого сервіс пропонує безкоштовні засоби для розшифрування. Повідомлення з вимогою викупу стане в пригоді в цьому процесі.

Розшифрування можливо в таких випадках:

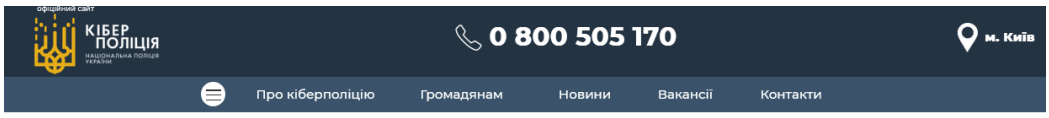
- автори шкідливого ПЗ помилилися в реалізації, вможлививши злом шифру. Таке мало місце з вимагацькими програмами Petya та CryptXXX;
- автори шкідливого ПЗ шкодують про свої дії й публікують ключі або головний ключ, як це було у випадку TeslaCrypt;

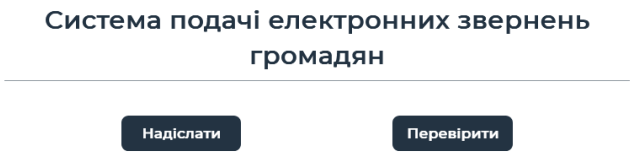
- правоохоронні органи захоплюють сервер з ключами й діляться ними. Одним з таких прикладів є CoinVault.





7) Повідомте про це Кіберполіцію України. Чим більше інформації ви надасте, тим вірогідніше, що правоохоронні органи зможуть зупинити злочинну діяльність.



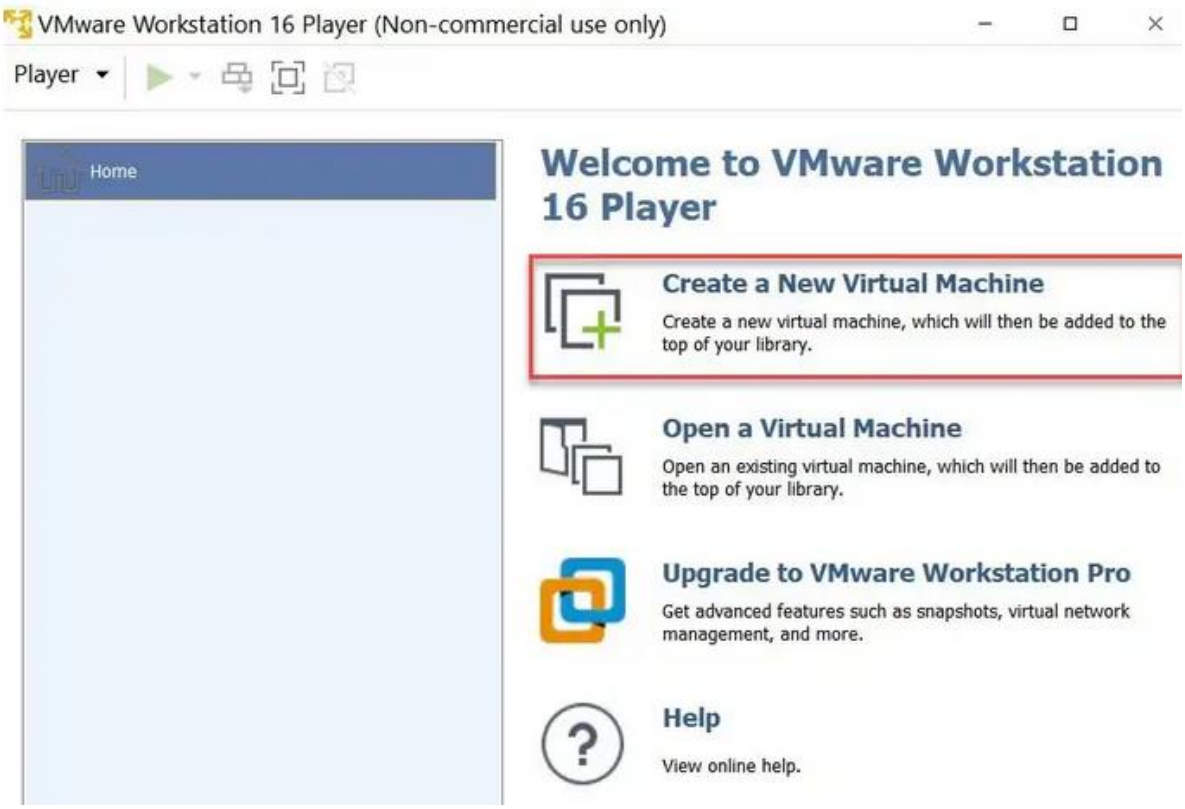


4.3. Віртуальні машини (пісочниця).

Віртуальна машина – це система для емуляції іншої платформи, вона допомагає користувачеві експлуатувати пристрій при встановленні декількох операційних систем, незалежних один від одного, завдяки чому один апарат може поєднати властивості двох і більше ПК. Створюються такі пристрої на реальних комп'ютерах в якості умовних. Це програма, що імітує копію існуючого апаратного забезпечення з усіма його компонентами (БІОС, жорсткий диск, периферійні пристрої). З допомогою спеціальних утиліт можна

запустити на одному комп’ютері кілька віртуальних машин з однаковими або різними операційними системами.

Операційна система, на якій встановлено віртуальну машину, називається основною або хост-ОС (від англ. host – головний, базовий, ведучий), а операційна система самої віртуальної машини називається гостьовою. Кожна гостьова ОС запускається в окремому вікні на основній ОС, аналогічно до звичайної програми. Все віртуальне обладнання, яке живить гостьову ОС, керується спеціальним механізмом, який називається гіпервізором. Гіпервізор відомий як менеджер віртуальної машини: він виділяє фізичні ресурси для кожної з систем і гарантує, що вони не перериватимуть роботу одна одної. Як правило, гіпервізори реалізуються на програмному рівні, але існують і такі, що вже вбудовані в прошивку системи.



Більшість віртуальних машин зберігають свої дані, включаючи операційну систему й додатки, в спеціальному файлі під назвою віртуальний диск, який містить файлову систему і представлений гостьовій ОС як звичайний фізичний жорсткий диск. Такий файл або набір файлів може

зберігатися на основному або віддаленому комп’ютері, бути частиною віртуальної машини або монтуватися в ОС фізичної машини.

Основними варіантами домашнього використання віртуальних машин є наступні.

Створення персонального віртуального середовища, ізольованого від хостової системи, що дозволяє використовувати на одному комп’ютері кілька копій робочих оточень, повністю ізольованих один від одного.

Створення переносних віртуальних машин, готових до використання на будь-який інший сумісній з архітектури платформі. Якщо Вам необхідно продемонструвати роботу певної програми, при цьому вона або оточення операційної системи повинні бути відповідним чином налаштовані – віртуальні машини кращий варіант в цьому випадку.

Отримання безпечних для користувача оточень для Інтернет. При роботі в мережі Інтернет віртуальна машина є більш виграшним варіантом, оскільки шкідлива програма після отримання контролю над операційною системою в віртуальній машині, може завдати шкоди тільки всередині неї, не зачіпаючи при цьому хостову ОС. Але останнім часом почали з’являтися віруси, які виявляють свою присутність в віртуальній машині й не видають себе в цьому випадку, однак поки таких шкідливих програм одиниці, і в будь-якому випадку шкоди важливим даним завдано не буде, поки заражені об’єкти не будуть перенесені в хостову ОС. Тому застосування віртуальних машин в цьому випадку аж ніяк не виключає використання антивірусного ПЗ.

Створення середовищ для експериментів із потенційно небезпечним програмним забезпеченням. На віртуальній машині можна без жодного ризику встановлювати прикладне ПЗ, яке може при певних умовах пошкодити систему або дані. В цьому випадку віртуальна машина виступає в ролі «пісочниці», в якій «граються» програми.

Можливість навчання роботі з операційними системами, відмінними від вашої хостової.