Загальна (сертифікована) короткострокова програма
«Інформаційна безпека та кібербезпека в органах влади»

Соціальна інженерія. Шкідливе програмне забезпечення

Артем СЕРЕНОК

к.держ.упр., доцент кафедри цифрових технологій та е-урядування ННІ “Інститут державного управління” ХНУ ім. В.Н. Каразіна
тренер з відкритих даних Національної мережі тренерів з відкритих даних
Національний консультант у сфері е-урядування в Донецькій області від ПРООН в Україні

Структура загальної (сертифікованої) короткострокової програми (дистанційно) «Інформаційна безпека та кібербезпека в органах влади»

- Основи інформаційної безпеки
- Інститути й інструменти забезпечення інформаційної безпеки України
- Стандарти Європейського Союзу і НАТО у сфері інформаційної безпеки
- Кіберзлочинність
- Безпека електронних платіжних систем
- Безпека роботи в Інтернет
- Соціальна інженерія
- Безпека мобільних пристроїв
- Захист інформації в мережах. Захист персональних даних

Термінологія

Кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об’єктів.

Соціальна інженерія – це наука, що вивчає людську поведінку та фактори, які на неї впливають.

Соціальна інженерія – це психологічне маніпулювання людьми, щоб змусити їх вчинити певні дії (наприклад повідомити свої персональні дані, перейти та завантажити файл за посиланням тощо), які особа не вчинила б, якщо б нею не маніпулювали.

Чому хакери використовують методи соціальної інженерії?

1. Це дешево
2. Це ефективно
3. Соціальна інженерія ефективна проти будь-якої операційної системи та версії програмного забезпечення

Методи соціальної інженерії

Фішинг - метод СІ коли зловмисник під виглядом іншої особи, організації, відомого сервісу намагається отримати від потерпілого його персональні дані чи іншу конфіденційну інформацію або змусити вчинити певні дії, які особа не вчинила б за звичайних умов, наприклад, завантажити та встановити шкідливе програмне забезпечення (ШПЗ).

Методи соціальної інженерії

Вішинг - це різновид фішінгу, який здійснюється через телефон.

Методи соціальної інженерії

SMS-фішинг - це різновид фішінгу, який здійснюється через SMS-розсилки

Методи соціальної інженерії

“КВІ ПРО КВО” (від. лат. Quid pro quo) - метод СІ, що поєднує в собі ознаки фішингу та вішингу.

Методи соціальної інженерії

“Дорожнє яблуко” (від англ. Road Apple) або “Троянський кінь” - метод атаки, який передбачає підкинути співробітнику компанії (організації) фізичний носій інформації (флеш-накопичувач, оптичний диск) із ШПЗ.

Як тільки співробітник вставить такий носій до ПК, то запуститься шкідливий код, який активує бекдор та надасть атакуючому доступ до мережі.

Методи соціальної інженерії

Зворотна соціальна інженерія - це вид СІ за якої особа сама звертається до шахрая та повідомляє свої конфіденційні дані.

Методи соціальної інженерії

Складна атака через проміжну ціль (від англ. “Supply chain attack”) - поняття, що використовується для опису складної, декілька ступеневої атаки, під час якої хакер атакує не напряму організацію, яка його цікавить, а менш захищену проміжну організацію чи установу, а вже через неї компроментує ту ціль, яка від самого початку його цікавила.

Термінологія

Шкідливе програмне забезпечення (ШПЗ) – програмне забезпечення, яке перешкоджає роботі комп’ютера, збирає конфіденційну інформацію або отримує доступ до приватних комп’ютерних систем.

Може проявлятися у вигляді коду, скрипту, активного контенту, й іншого ПЗ.

Більша частина шкідливого ПЗ створена з метою викрадення чи блокування персональної інформації та отримання несанкціонованого доступу до неї.

Звідки береться ШПЗ?

Шкідливе програмне забезпечення може розроблятися зловмисниками «з нуля», а може базуватися на легітимному модифікованому «програмному забезпеченні», зазвичай це троянські програми, які базуються на легальних програмах віддаленого доступу та адміністрування.

Досить часто ШПЗ надається як сервіс (Malware-as-a-service), де клієнт платить місячну/денну/тижневу плату за користування ШПЗ, яке надається «під ключ». Такий підхід значно знижує бар'єр входу та робить ШПЗ доступним для широкого кола осіб.

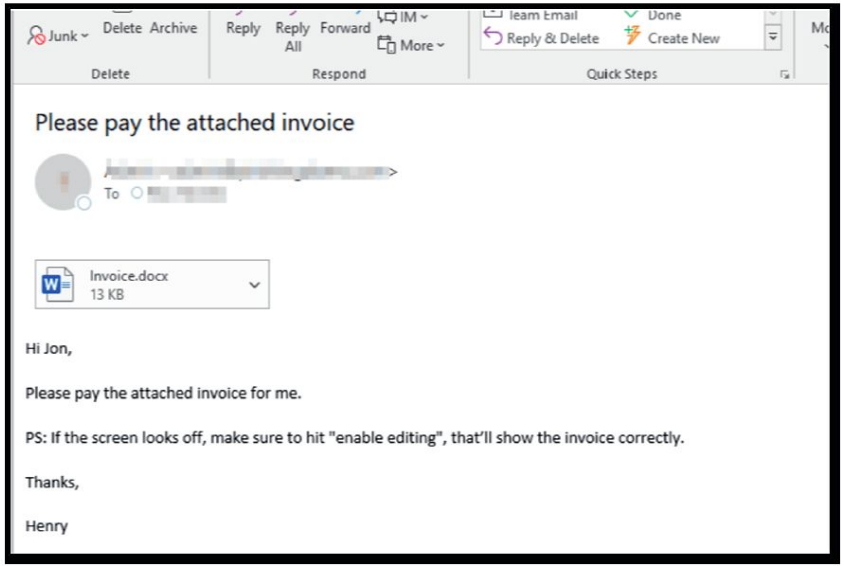
ШЛЯХИ РОЗПОВСЮДЖЕННЯ ШПЗ, ВЕКТОРИ АТАК

- **звичайний спам** – надсилається масово широкому колу осіб.
- **таргетовані або цільові спам-кампанії**, це коли хакер надсилає спеціально створений лист, адресований конкретній особі або організації.

Таргетована або цільова атака – це вид кібератаки, спрямований на конкретну ціль, це може бути компанія, державна структура чи користувач.

Таргетована атака відрізняється від масової тим, що перед її здійсненням атакуючий детально вивчає свою ціль, збирає про неї всі наявні дані та, виходячи з цього, планує та організовує атаку.

ШЛЯХИ РОЗПОВСЮДЖЕННЯ ШПЗ, ВЕКТОРИ АТАК



ШПЗ у вигляді вкладення до e-mail, це може бути файл MS Word/Excel, PDF, PNG тощо із спеціальним вставленним скриптом, який після його активізації завантажить ШПЗ із віддаленого серверу та запустить на комп’ютері жертви.

ШЛЯХИ РОЗПОВСЮДЖЕННЯ ШПЗ, ВЕКТОРИ АТАК

Надсилання шкідливого файлу із «фейковим або так званим подвійним розширенням». У такому випадку хакери змінюють розширення файлу та змінюють іконку файлу на відповідну розширенню. Це створює враження, що файл є безпечним та може бути відкритий у комп’ютері. Наприклад, файл note.txt.exe насправді є виконуваним файлом, а не текстовим,

ШЛЯХИ РОЗПОВСЮДЖЕННЯ ШПЗ, ВЕКТОРИ АТАК

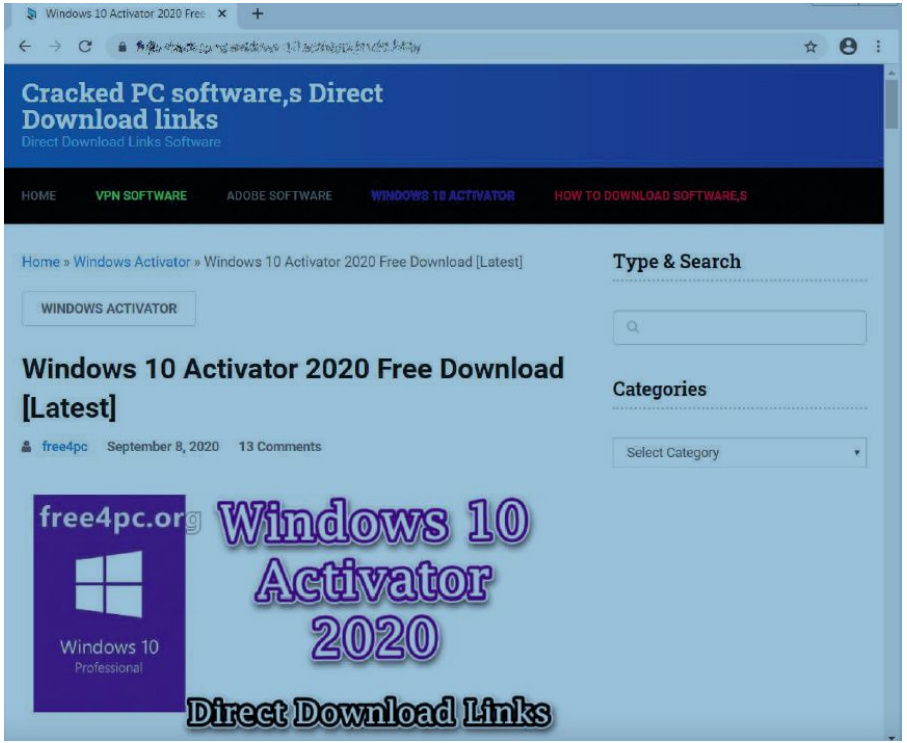
Фíшинг – це вид онлайн шахрайства, який базується на методах соціальної інженерії та має на меті, шляхом обману, змусити користувача здійснити дії, які б він не здійснив у звичних умовах, наприклад, розкрити свої персональні дані, завантажити, встановити чи запустити шкідливе програмне забезпечення.

Фішинг може бути здійснений у різних формах – електронні листи, надіслані нібито від імені легальних компаній, фейкові вебсайти, дзвінки нібито співробітників банку, тощо.

ШЛЯХИ РОЗПОВСЮДЖЕННЯ ШПЗ, ВЕКТОРИ АТАК

Розповсюдження ШПЗ під виглядом примірників «зламаного» комерційного програмного забезпечення, яке «не потребує ліцензії».

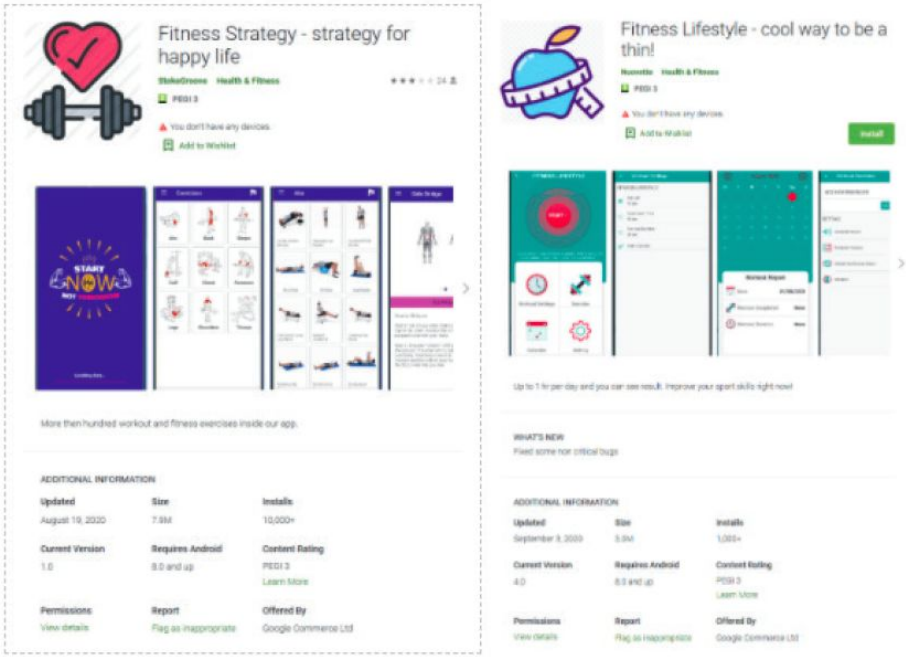
«Кряк» (від англійського “crack”), це програма, яка генерує код активації для комерційного програмного забезпечення чи змінює систему перевірки ліцензійності комерційного програмного забезпечення і тим самим порушує авторські права виробника.



ШЛЯХИ РОЗПОВСЮДЖЕННЯ ШПЗ, ВЕКТОРИ АТАК

Поширення ШПЗ під виглядом “freeware” программ.

Це, як правило, так звані «корисні» програми, такі як ліхтарики для мобільних телефонів, калькулятори, конвертери валют тощо. Найбільш поширеними вони є для мобільних пристроїв.



ШЛЯХИ РОЗПОВСЮДЖЕННЯ ШПЗ, ВЕКТОРИ АТАК

Таргетовані атаки із використанням «нетрадиційних методів». Сюди можна віднести «випадково загублені флешки», фізичний доступ хакеру до комп'ютера, складні прийоми соціальної інженерії, коли телефонують користувачеві та просять встановити ту чи іншу програму, наприклад, під виглядом співробітників банку.

Окремої уваги заслуговує загроза від інсайдерів, які вербуються хакерами для встановлення вірусів, відключення антивірусів та фаєрволів.

Рекомендації, як визначити, що програма підозріла і може завдати шкоди Вашому пристрою:

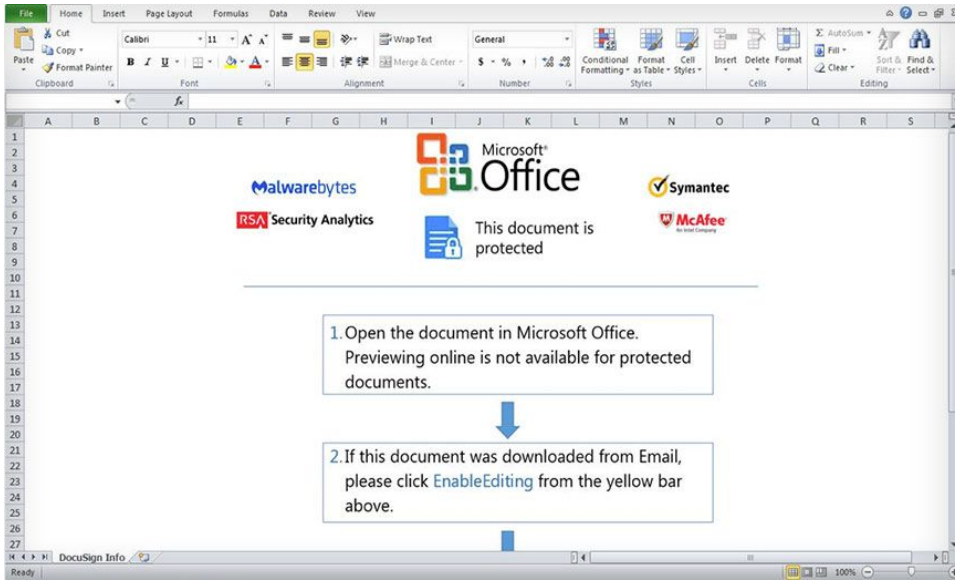
- Подивитися рейтинг програми та почитати відгуки.
- Подивитися інформацію, до яких функцій операційної системи програма отримує доступ або просить надати доступ. Очевидно, що програмі ліхтарик, не потрібний доступ до ваших текстових повідомлень, камери, мікрофону чи фотографій, щоб ефективно працювати.
- Подивитися інформацію щодо розробника. Чи це відома фірма, чи невідомий розробник? Чи існує взагалі якась інформація щодо розробника у відкритих джерелах? Чи завантажив розробник в “Google Play Market” інші програми, скільки, який їх рейтинг? Чи є у розробника власний сайт тощо.
- Не встановлюйте програми із низьким рейтингом та малою кількістю завантажень.
- Пам’ятайте, що краще заплатити кілька сотень гривень за ліцензійну програму, ніж потім втратити тисячі із власного банківського рахунку.

ВИДИ ШПЗ

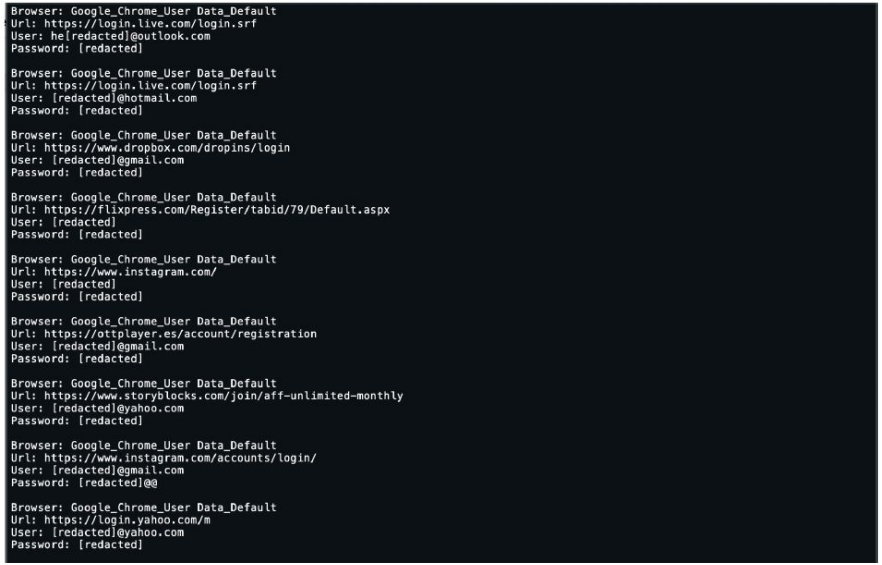
Завантажувач (дропер/лоадер) (Eng. malware loaders or droppers)

Функцією дропера є завантаження та запуск головного модуля ШПЗ. Лоадер, як правило, мають малий розмір, в декілька десятків або сотень кілобайт, та мінімальний функціонал – завантаження та запуск «головного модуля» ШПЗ.

Дропер може бути у вигляді простого скрипту, який завантажує інше ШПЗ за заздалегідь визначеним посиланням (наприклад JS loader) або мати більш складний функціонал та систему управління (control panel), розташовану на віддаленому сервері.



ВИДИ ШПЗ



Викрадач інформації «Інфостілер або стілер» (Eng. Information stealers)

Це вид шкідливого програмного забезпечення, створеного з метою викрадення персональних даних користувачів, у тому числі логінів та паролів, які зберігаються в інтернет-браузерах, месенджерах та різноманітних мережевих клієнтах.

Інфостілери не забезпечують віддаленого доступу до інфікованої системи, але виступають ефективним інструментом для збору конфіденційної інформації та первинного вектору атаки на комп’ютерні мережі.

ВИДИ ШПЗ

Keylogger “кейлогер” (англ. key (stroke) клавіша, англ. logger – реєструючий пристрій) – це програмний продукт або апаратний пристрій, що реєструє кожне натискання клавіш клавіатури комп’ютера. На даний момент функціонал кейлогерів значно розширився і вони можуть перехоплювати інформацію з вікон програм, кліків миші, буферу обміну; робити фотознімки екрану і активних вікон; моніторити файлову активність тощо; перехоплювати дані з монітору, вебкамери, принтера тощо.

ВИДИ ШПЗ

«JS-сніфери» шкідливі програмні скрипти, які «вставляються» в програмний код зламаних вебсайтів та використовуються для викрадення даних платіжних карток. JS-сніфер – це зазвичай декілька рядків програмного коду, який зловмисники встановлюють на сторінках із формами онлайн-оплати і які активуються, коли користувач вводить дані платіжних карток.

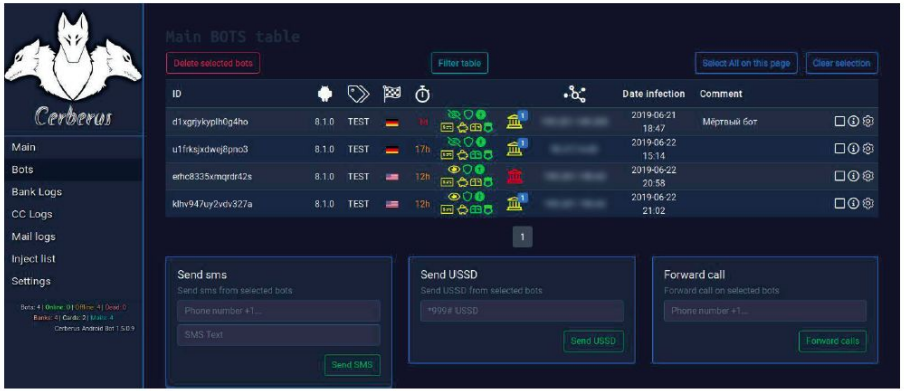
Ризик «JS сніферів» у тому, що кінцевий користувач практично не має інструментів захисту, адже уражається інфраструктура з боку вебсайту (серверу).

ВИДИ ШПЗ

Троянські програми віддаленого доступу RAT (remote access trojans)

Троянські програма або троян забезпечує хакеру віддалений доступ до інфікованої системи. В такому випадку атакуючий може отримати контроль над усіма файлами, завантажувати файли, модифікувати їх, виконувати від імені користувача дії на комп’ютері, переглядати веб-браузер, користуватися поштовим клієнтом та іншим програмним забезпеченням. Троянські програми часто працюють на базі легітимних протоколів операційної системи RDP, VNC і часто розроблені на базі легітимного програмного забезпечення для віддаленого адміністрування комп’ютерів. Це часто призводить до того, що антивірусні програми трактують їх як офіційне програмне забезпечення.

ВИДИ ШПЗ

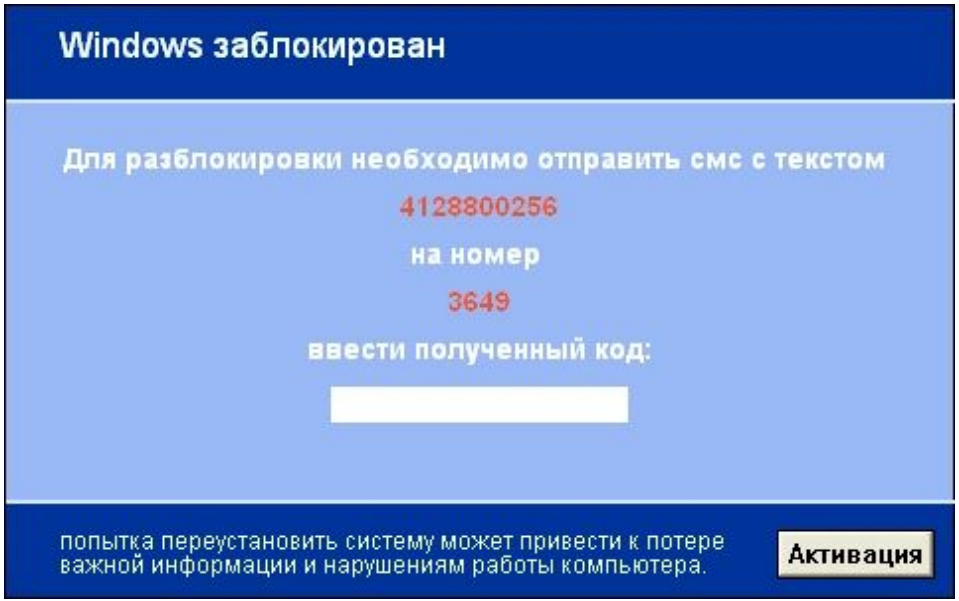


Банківські трояни (banking trojans)

Вид шкідливого програмного забезпечення, створений з метою викрадення коштів із банківських рахунків. Банківські трояни, це комплексне, багатофункціональне ШПЗ, яке поєднує в собі функції кейлогера та стілера, троянської програми. Після потрапляння на комп'ютер жертви, банківський троян моніторить активність користувача та збирає персональні дані. Як тільки користувач логіниться в особистий кабінет онлайн-банкінгу, ШПЗ перехоплює сесію веб-браузера, застосовуючи man in- the-middle атаку. За такого сценарію, банківський троян відображає точну копію банківської сторінки і, нічого непідозрюючи, користувач вводить свої персональні дані (логін, пароль, код 2FA авторизації), які передаються на север хакера. Далі хакер, використовує викрадену сесію для переказу коштів на підконтрольний йому рахунок. Користувач, як правило, бачить у своєму браузері повідомлення, що зв'язок із банком на даний момент неможливий чи, навпаки, йому відображається повідомлення, що браузер намагається встановити з'єднання із сервером банку.

ВИДИ ШПЗ

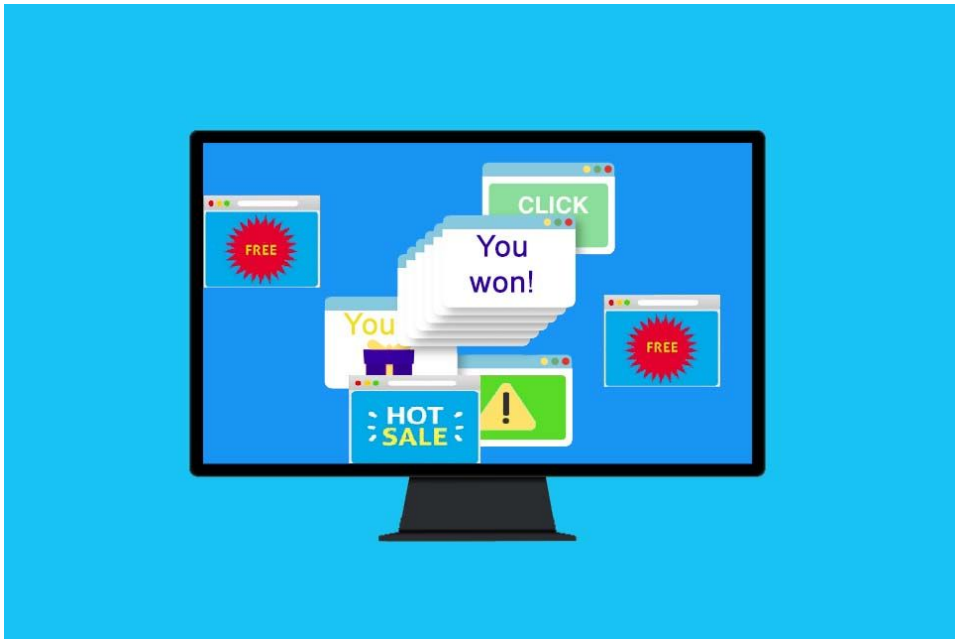
Ransomware (програма-вимагач, програма-шантажист) – це тип шкідливої програми, яка після потрапляння на комп’ютер шифрує файли та злочинці вимагають викуп за їх розшифрування.



ВИДИ ШПЗ

Шкідливе програмне забезпечення для знищення інформації без можливості її відновлення (Destructive malware) головною ціллю ШПЗ є знищення важливих та критичних файлів, щоб унеможливити доступ до операційної системи. Файли, як правило, стираються і дисковий простір перезаписується декілька разів, щоб унеможливити відновлення файлів. Атаки з використанням destructive malware порівняно рідкі, мають або «хуліганський» підтекст, або є частиною “state sponsored”-атак на критичні об’єкти інфраструктури.

ВИДИ ШПЗ



Рекламне шкідливе програмне забезпечення (Adware)

ШПЗ основною ціллю, якого є показ користувачеві реклами, а також збору інформації маркетингового характеру про користувача.

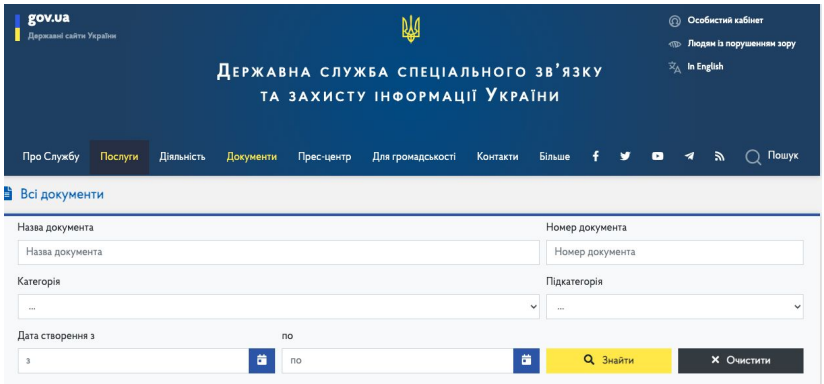
ВИДИ ШПЗ

Майнери (miners) – ШПЗ, яке без відома жертви використовує потужності її комп’ютера для майнингу криптовалюти. Майнери активізуються лише тоді, коли вражена система не завантажена іншими ресурсозатратним завданнями, щоб не викликати підозру користувача.

ЯК МІНІМІЗУВАТИ РИЗИКИ ТА ЩО РОБИТИ, ЯКЩО Я СТАВ(ЛА) ЖЕРТВОЮ ШПЗ

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

Перелік програмного забезпечення, дозволеного для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, наведений на веб-сайті Державної служби спеціального зв'язку та захисту інформації України.



ЯК МІНІМІЗУВАТИ РИЗИКИ ТА ЩО РОБИТИ, ЯКЩО Я СТАВ(ЛА) ЖЕРТВОЮ ШПЗ

Не відкривайте підозрілі додатки до емейлів; не встановлюйте підозрілі розширення для інтернет-браузерів чи інші програми із сумнівною репутацією. Вимкніть використання макросів (використовуються в багатьох офісних продуктах, наприклад 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).

Order #20180329

PM Purchase Manager
9/17/2018 7:25 AM

To: Sales

Quotation_Request_20180329_0...
466.46 KB

Dear Sir / Madam,

We have been referred to you by an agent and they said you are the best in this field.
Attached is our Purchase order for your quotation. Please review the products and specifications as it is very important to u
possible send us your catalogue for our referrence.

Also indicate your payment and delivery terms.

Regional Sales Manager

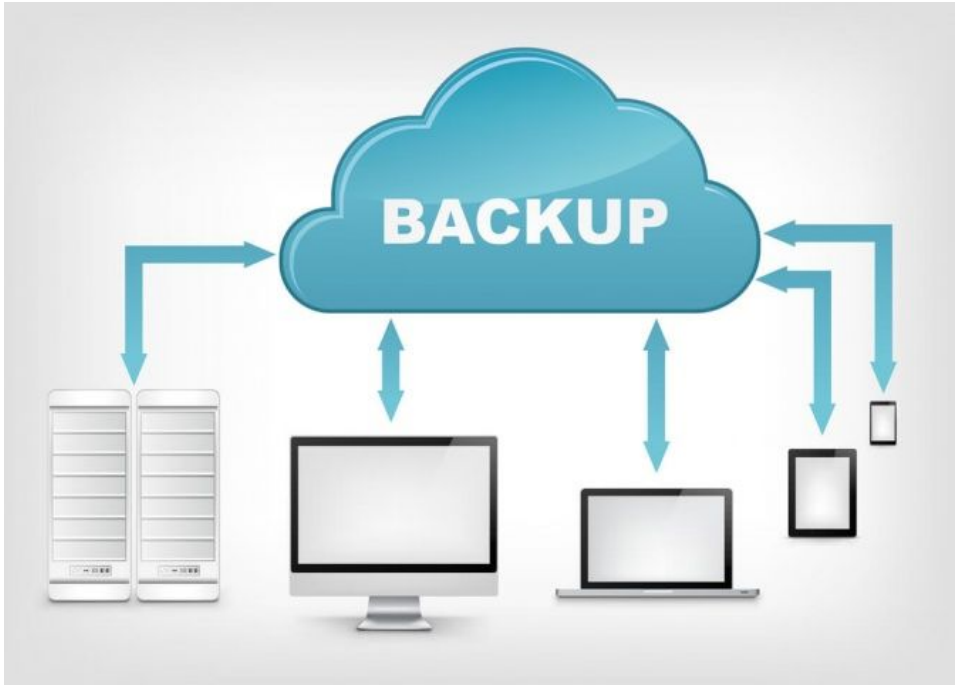
Head Office

Stabilimento:

ЯК МІНІМІЗУВАТИ РИЗИКИ ТА ЩО РОБИТИ, ЯКЩО Я СТАВ(ЛА) ЖЕРТВОЮ ШПЗ

Створюйте backups де це можливо і коли це можливо [анімація як створити бекап].

Backups (бекап) – процес створення копії даних з носія (жорсткого диска, дискети тощо), призначений для відновлення цих даних у разі їх пошкодження або видалення



Дякую за увагу!