банк ПІВДЕННИЙ

Методи і підходи до захисту коштів клієнта

bank.com.ua

14.11.2018

Історія і причини зростання кібершахрайства

Історія

З 2013 року бурхливе зростання інцидентів із несанкціонованими платежами за системами «Банк-Клієнт» юридичних осіб.

З 2017 року ситуація «стабілізувалася» - грабують стабільно.

₴

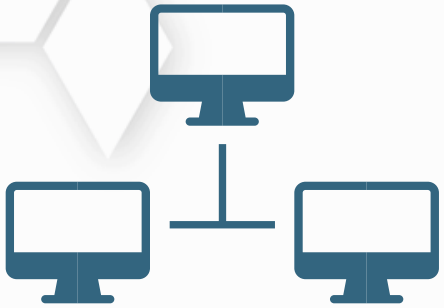
Платежі від декількох десятків тисяч до десятків мільйонів гривень.



Причини:

- Низький рівень безпеки
- Простота і доступність
- Високий рівень доходу і низький рівень ризику для кіберугруповувань

Хто під прицілом?



Компанії, юридичні особи
(системи ДБО, БД підприємств)



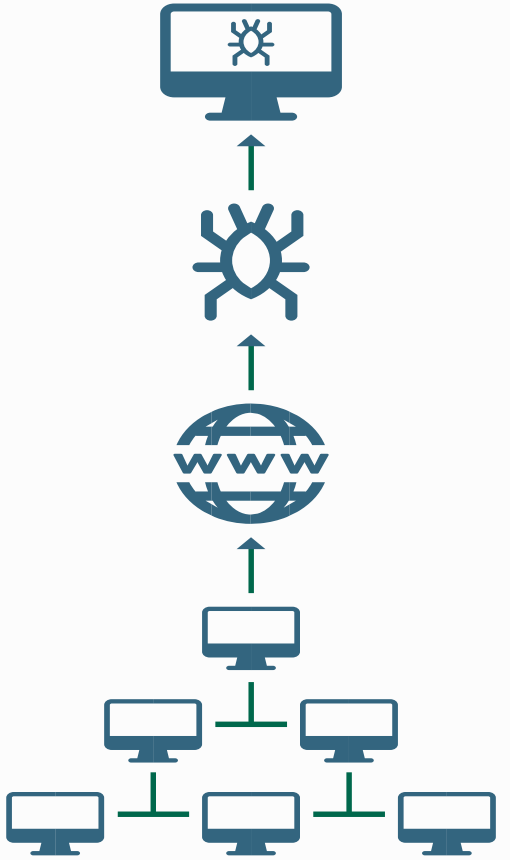
Фізичні особи
(кошти на платіжних картках)



Для компаній – що реально відбувається?

«По ту сторону барикад»,
або Методи і прийоми хакерів

- Заражений лист
- Зараження комп'ютера, встановлення зв'язку із сервером
- Завантажуються автоматизовані засоби розвідки
- Продаж заражених комп'ютерів злочинним групам
- Вивчення, аналіз грошових потоків, підготовка до виведення коштів
- Крадіжка облікових даних, ключів ЕЦП



Для компаній – що реально відбувається?

«Нас хакнули?!»

- Що бачать співробітники компанії?

«Ой, комп'ютер із «Банк-Клієнтом» «зависнув». Пішов на перезавантаження і не завантажується».

- Як діють співробітники компаній?

«Кличуть «айтішника», за день-два він все затирає і відновлює комп'ютер».
Рідко хто дзвонить у банк перевірити стан рахунку і останні платежі.

- Які результати в підсумку? – ГРОШЕЙ НЕМАЄ.



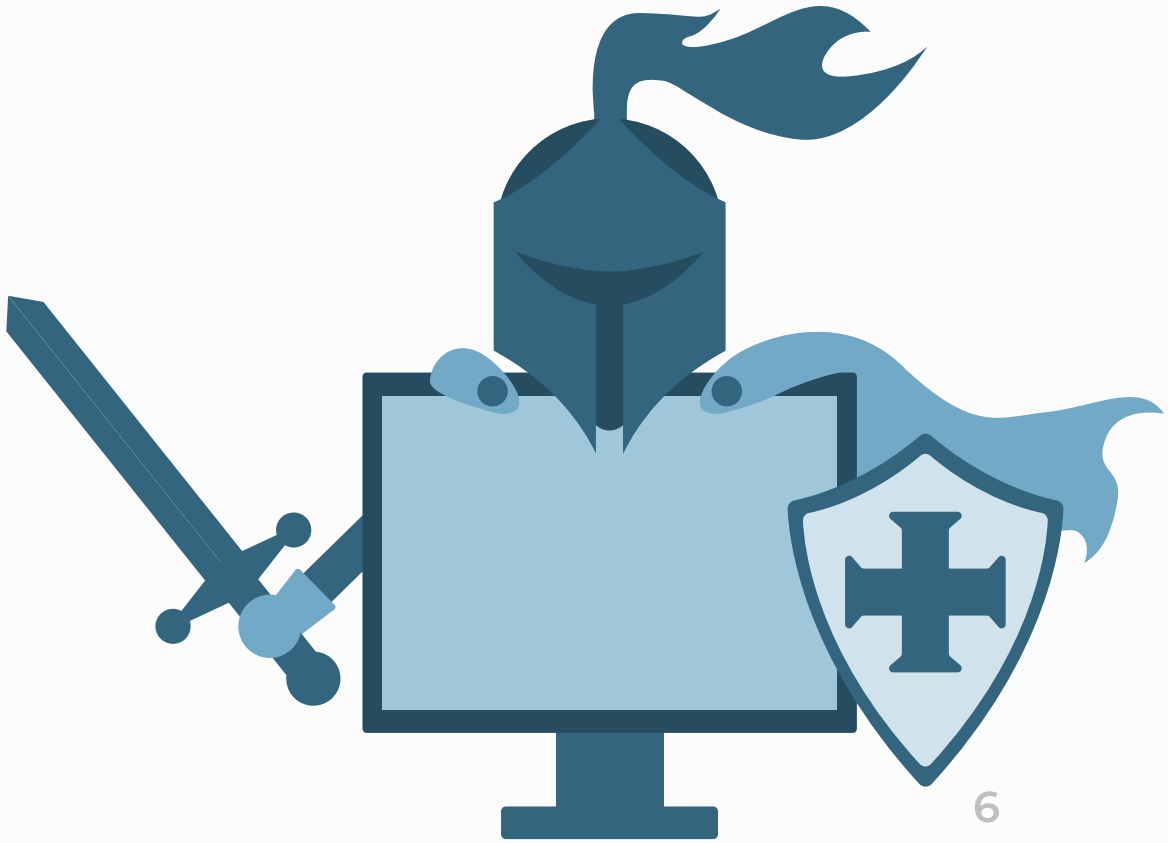
Для компаній – що потрібно робити компанії?

Що робити відразу:

- Дзвонити в банк операціоністу, з'ясувати, чи немає несанкціонованих операцій

Якщо злочин стався:

- блокувати роботу «Банк-Клієнт»;
- надіслати офіційний лист в банк;
- перевірити рахунки і заблокувати роботу інших систем «Банк-Клієнт» на комп'ютері;
- скомпрометований комп'ютер вимкнути і більше не вмикати.



Для компаній – що потрібно робити компанії?

Як «заморозити» гроші?
Як «наздогнати» гроші?

Час – гроші, кожна хвилина є вирішальною!

- Банк вживає оперативні заходи із затримання коштів у банку-одержувачі.
- Підключається кіберполіція та інші органи.



Для компаній – що потрібно робити компанії?

Гроші «наздогнали». Як повернути?

- Юридичні аспекти повернення
- Державний фінансовий моніторинг:
  - затримання коштів на 2 дні;
  - продовження затримання до 25 днів.
- Інші варіанти
- Арешт викрадених коштів на банківському рахунку злочинців за рішенням суду
- Вимагати негайного виконання від слідчого



Для компаній – як запобігти?

Дорогий варіант:

Надійна IT-архітектура на підприємстві
На практиці: дорого, мало у кого є

Простіший варіант:

Комп'ютер – гаманець із грошима!

Як захистити його:

- Комп'ютер для роботи з банком – тільки для роботи з банком!
- Забрати права адміністратора
- Виключно ліцензійне ПЗ
- Комерційний антивірус
- Файрвол
- «Білий список» дозволеного програмного забезпечення
- Закрити USB
- Windows-> MacOS



Інструменти банку

Як банк «Південний» захищає ваші гроші:

- SMS-оповіщення
- вхід до iFOBS із певних IP-адрес.
- SMS-confirmation
- Послуга «Право авторизаційного підпису»
- Послуга «Ліміти і авторизація»



Які ще інструменти існують?

Токени:

- Що це?
- Види токенів: апаратні/програмні
- Плюси і мінуси токенів
- Якими наявними послугами банку можна замінити токени?



Для фізичних осіб – що відбувається?

І знову про картки та про поточні рахунки

- Види карток та їхня захищеність (смуга, чип, CVV2)
- Платежі в інтернеті
- 3D Secure (SMS-підтвердження інтернет-операцій)



Як ЦЕ відбувається у людей?
Методи і прийоми хакерів

- Соціальна інженерія, OLX
- Накладки на банкомати
- Фішингові сайти

Рекомендуємо: Сайт міжбанківської асоціації EMA.COM.UA

Для фізичних осіб – що робити?

Це відбулося. Що робити?

- Звернутися в банк
- Заява в кіберполіцію

Робота над помилками.
Як себе убезпечити – просто і ефективно

- Не передавати PIN-код, CVV-код, слово «пароль»
- Картки з чипом
- SMS-підтвердження операцій в інтернеті (3D Secure)
- Окрема картка для операцій в інтернеті
- Безпечний смартфон
- Пильність



банк
ПІВДЕННИЙ

Ваш фінансовий партнер

вул. Краснова, 6/1
м. Одеса, 65059, Україна
Контакт-центр: 0 800 30 70 30
307030@pivdenny.ua

bank.com.ua