ЛАБОРАТОРНА РОБОТА №1. РОЗПІЗНАВАННЯ ФІШІНГУ.

Мета вивчення: отримати теоретичні знання та практичні навички розпізнавання фішингу.

Обсяг навчального часу: 1 година.

Обладнання: комп'ютер (планшет, смартфон), наявність підключення до мережі Інтернет.

План заняття:

1. Отримати теоретичні знання аналізу повідомлень щодо фішингового вмісту.
2. Пройти тест від Jigsaw щодо вміння розпізнавати фішингові повідомлення.

Інформаційні джерела:

тест на вміння розпізнавати фішингові листи:

- https://phishingquiz.withgoogle.com/?hl=uk,

перевірка документів та URL на шкідливий вміст:

- https://virustotal.com/;
- https://iris-h.malwageddon.com/submit;
- https://cape.contextis.com/submit/;
- https://urlscan.io/.

ЗАВДАННЯ:

1. Ознайомитися з методикою розпізнавання фішингу, перевірити отриманні знання за допомогою тесту від Jigsaw – підрозділу Google (https://phishingquiz.withgoogle.com/?hl=uk). Зробити скріншот із результатами Вашого тестування та додати до звіту.

2. Перевірити за допомогою відповідних ресурсів принаймні один файл та одне посилання з вашої електронної пошти.

ВИМОГИ ДО ЗВІТУ:

1. Скрін екрану з результатами проходження тесту від Jigsaw.

ХІД РОБОТИ.

1. Фішингові листи – це різновид соціальної інженерії, спосіб прихованої маніпуляції діями обраної людини. Щоб примусити жертву відреагувати на фішинговий лист, а не видалити його одразу, зловмисники підбирають відповідного адресанта – лист може прийти начебто від державної фіскальної служби або від організації-підрядника, із яким співпрацює компанія жертви. Текст фішингового листа, як правило, пропонує ознайомитися з документами, частіше – пов'язаними з фінансовими операціями.

Під час створення листа зловмисники можуть використовувати інформацію, яку вони знаходять у відкритих джерелах (Google, Facebook тощо). Припустимо, жертва на своїй сторінці в соціальній мережі показує всім, що вона дуже захоплюється авіамоделюванням або є палким фанатом певного музичного гурту – в такому разі їй можуть надіслати листа із пропозицією переглянути свіжий каталог моделей чи придбати квитки на найближчий концерт із суттєвою знижкою, або завантажити рідкісний концертний запис. Ймовірність того, що, зацікавлена такою приманкою, жертва перейде за посиланням або відкриє документ, значно вища, ніж у випадку типових масових сповіщень, наприклад, від банків.

Правила захисту від фішингу в електронних листах.

1) Не довіряти нікому, або правило 30 секунд. Не поспішайте відкривати приєднані файли чи переходити за посиланням, зупиніться і дайте собі 30 секунд на коротку перевірку нового листа.

Зазвичай, безпосередньо під час розсилки і кілька годин потому більшість звичайних антивірусів не розрізняють загрозу, яку вам надіслали під виглядом документів. Але навіть цільовий, персональний фітинг, досить часто легко відрізнити за деталями, яких, на жаль, часто не помічають.

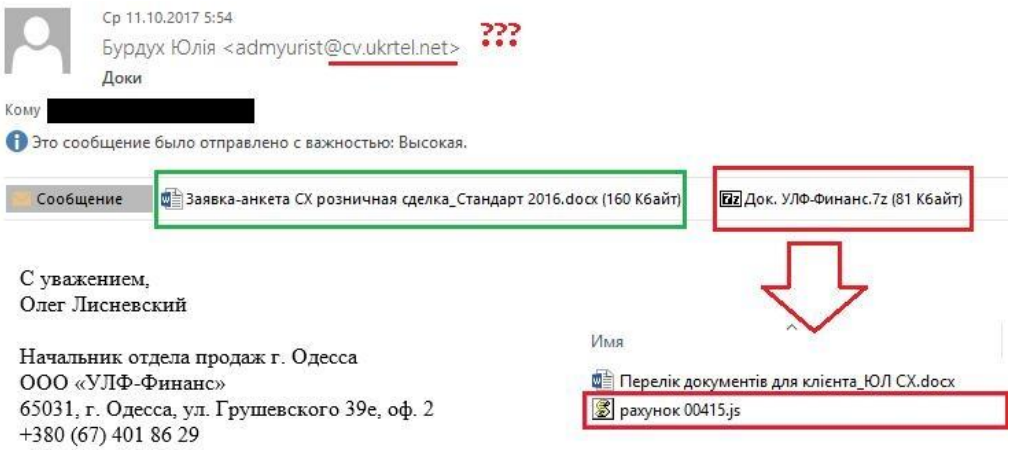
Надайте собі відповіді на такі запитання:

- Від кого надійшов лист? Яка його тема?
- Кому надіслано листа? Вам чи відділу, де ви працюєте?
- Чи є вкладення?

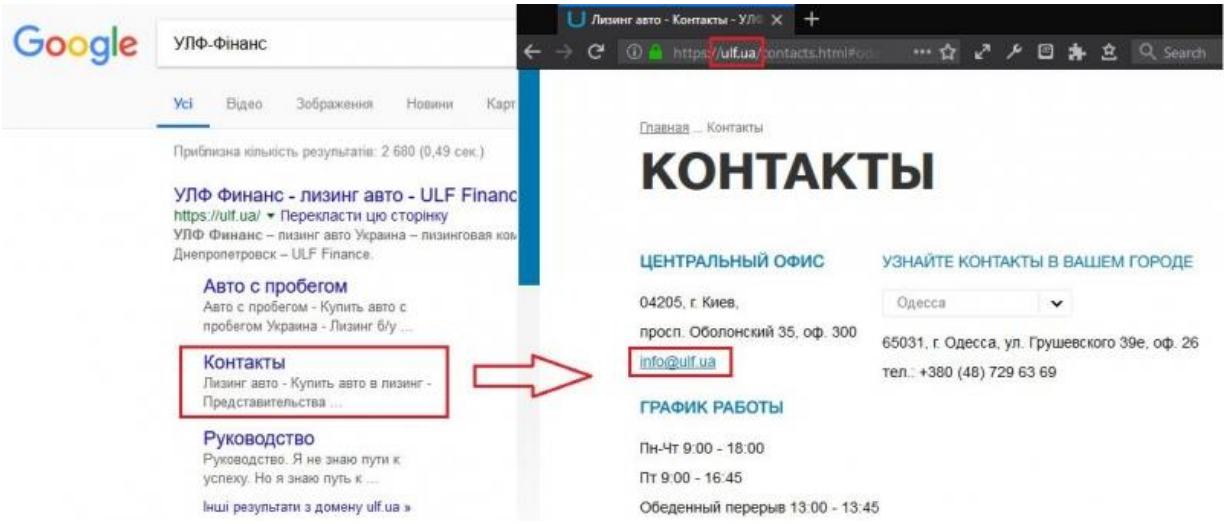
- Текст листа – чи збігається він із темою листа?
- Про що вас намагаються попросити? Чи маєте ви право це робити?
- Чи є в кінці листа підпис тієї особи, яка начебто писала його вам?
- Чи співпадає поштова скринька, з якої ви отримали цього листа, з доменним ім’ям тієї організації, що вказана в підписі?
- Чи співпадає зазначена в підписі листа організація з тою, що вказана в темі листа або ж у його тексті?
- Чи помічаєте ви грубі граматичні та/або орфографічні помилки в тексті листа?
- Чи містить текст листа будь-які посилання?

Мета цього поверхневого огляду – пересвідчитися, що лист адресовано дійсно вам, що він стосується саме вас. Правило просте: повідомлення, яке прямо вас не стосується та не пов’язане з вашою роботою, яким би спокусливим або ж, навпаки, яким би незрозумілим воно не здавалося, помітити як небажане та видалити.

Навіть якщо ви держслужбовець і ваша робота полягає в розгляді звернень громадян – так, ви, дійсно, маєте реагувати на кожного листа, але навіть тоді, ви не мусите відкривати приєднання чи посилання листа, який надійшов вам іншою мовою. Якщо щось не збігається – приміром, підпис із скринькою, від якої надійшов лист, або ім’я в заголовку листа не співпадає із тим, що вказане в підписі, чи текст листа містить грубі помилки і так далі – не відкривайте приєднання, не переходьте за посиланням



Відправник Юлія, скринька належить до cv.ukrtel.net. Тема «Доки» – викликає невелику підозру. Лист містить два приєднання – документ і архів. Можливо, так і має бути (насправді так роблять, аби обманути фільтри пошти, сам документ – порожній, там лише текст, а ось архів містить приманку, що завантажує вірус). Підпис – Олег замість Юлії, в офіційному діловому спілкуванні таке зустрічається дуже рідко. Назва компанії – «УЛФ-Фінанс» у місті Одеса дозволить пошукати контакти цієї компанії в Google:

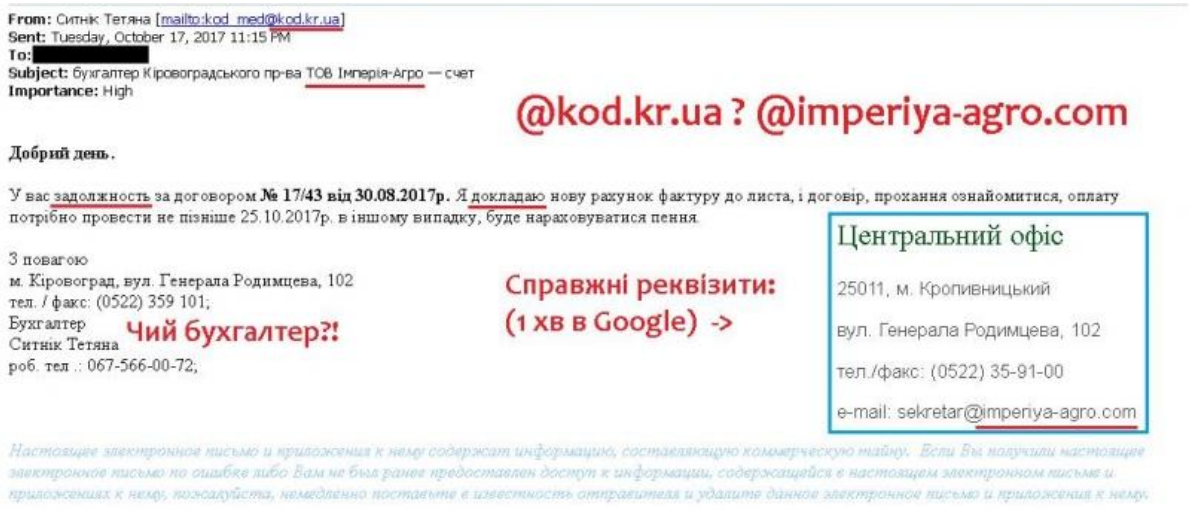


Адреса в підписі та на офіційному сайті співпадають, а домен – ні. Але ж у більшості сучасних компаній адреси їхніх електронних скриньок матимуть таку ж саму назву, як і офіційний сайт. Наприклад, офіційний сайт організації – ulf.ua, отже, листи від них можуть надходити лише з адрес на кшталт user@ulf.ua. А в цьому випадку ми маємо зразок фейкового (несправжнього) листа, це фішинг:

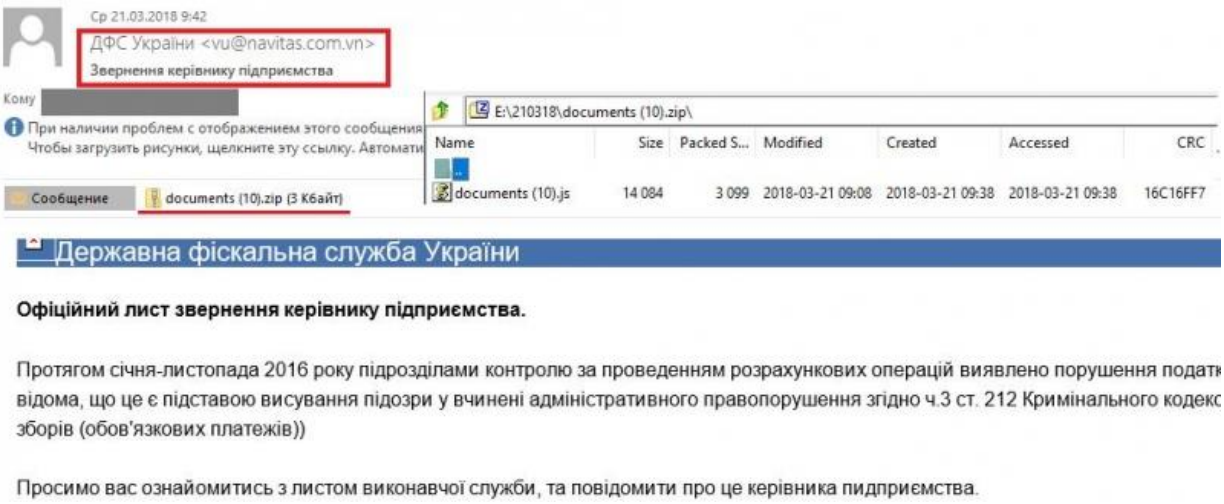
- адреса скриньки, від якої надійшов лист, не співпадає з офіційними контактами організації;
- неформальний текст у темі, жаргонізми;
- чужий підпис, його туди просто вставили.

ви можете пересвідчитися, що вам надсилали документи саме з тієї організації, яка вказана в підписі, але в жодному разі не користуйтеся контактами в підписі. Якщо лист писали зловмисники, їм ніхто не заважав указати там свої номери, а отже, щойно ви зателефонуєте до них, вони одразу вас запевнять, що цей підозрілий документ надіслано саме вам. Тому треба

звернутися за телефонами, які вказані на офіційному сайті, й перепитати, чому Олег зі скриньки Юлії надіслав якісь незрозумілі документи.

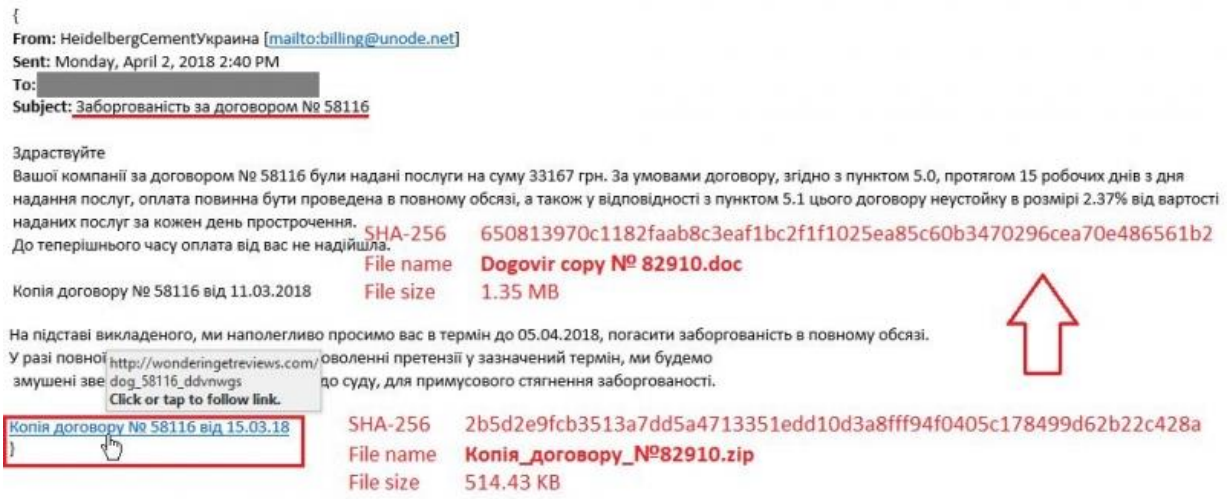


Перша і головна ознака фішингу – скринька, від якої надійшов лист, не має абсолютно нічого спільного з доменом, який зареєстрований на компанію, що фігурує в темі листа. Далі, в підписі відсутня інформація про компанію. Вказали лише посаду і телефон людини. Хто вона? До якої організації належить? Дуже велика кількість помилок.



Скринька не співпадає з офіційними контактами ДФС. Відсутній формалізований підпис. Це фейк. Зловмисники дуже полюбляють надсилати фішинг від імені всіляких державних установ або контрольних органів. Основна їхня мета – залякати жертву і примусити її відкрити приєднання.

Фішингові листи часто містять посилання на фейкові сторінки чи ресурси.



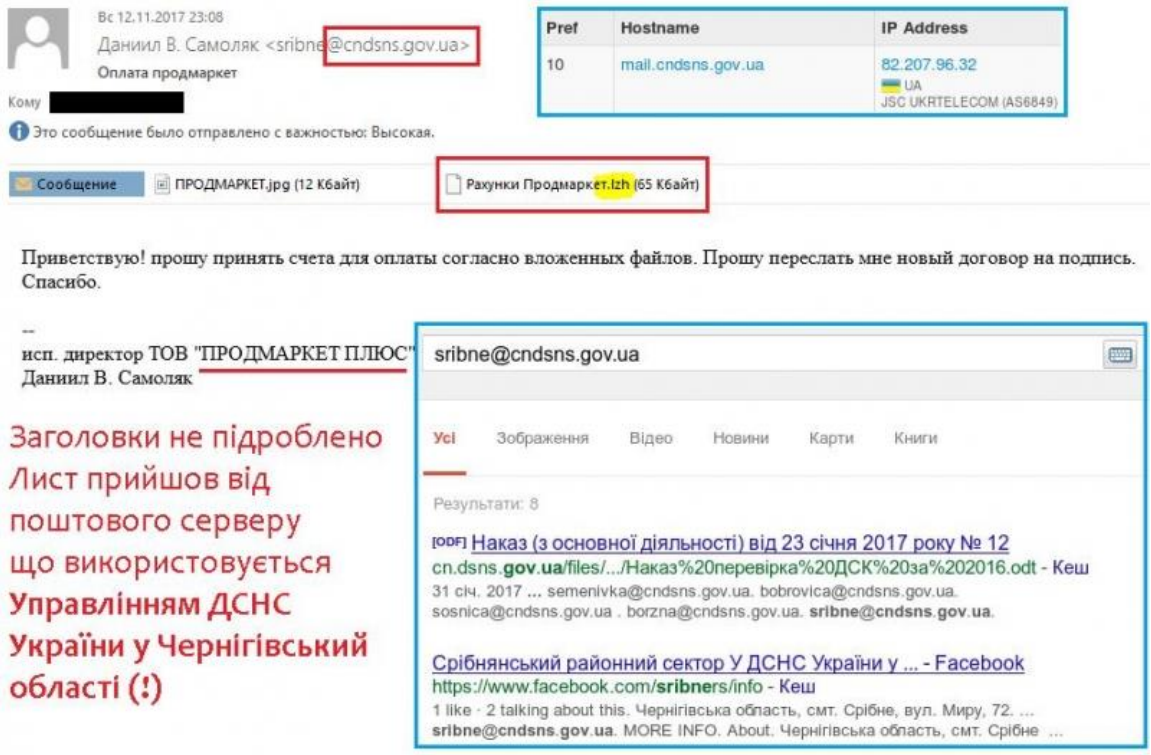
«Здраствуйте» на початку і ламана українська в тексті. Скринька не співпадає з офіційними контактами вказаної організації. Але зверніть увагу на посилання – це улюблений прийом.

Справа в тому, що в листі можна взяти будь-який текст і вставити в нього посилання на певне джерело в Інтернеті. Зловмисники беруть текст правильного джерела, припустимо rada.gov.ua, але ставлять на нього посилання на якийсь сервер, що розповсюджує віруси. Люди, як правило, не читають текст справжнього посилання, вони бачать лише те, що лежить на поверхні.

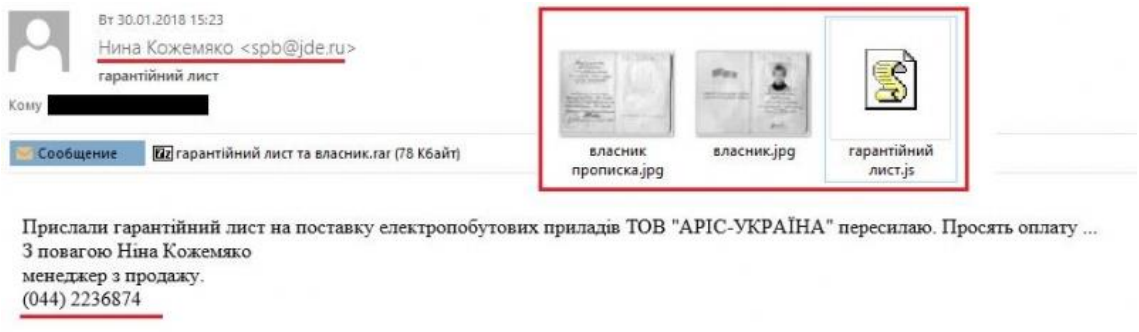
Щоб захиститися від таких трюків, варто просто не клікати одразу на посилання, а навести на нього курсор (як на знімку екрана вище). Або можна також через контексте меню скопіювати посилання та вставити його у блокнот, щоб порівняти зі справжнім сайтом організації, на який вас відправляють.

Також відомі випадки, коли офіційна скринька (або ж навіть цілий поштовий сервер) реальної організації були скомпрометовані, і вам може надійти лист, який пройде всі фільтри.

Лист дійсно надійшов від ДСНС. Нападники досить примітивно скористалися доступом до одного з регіональних серверів ДСНС– вони від скриньки служби розсилають фішинг із підписом «продмаркет плюс».



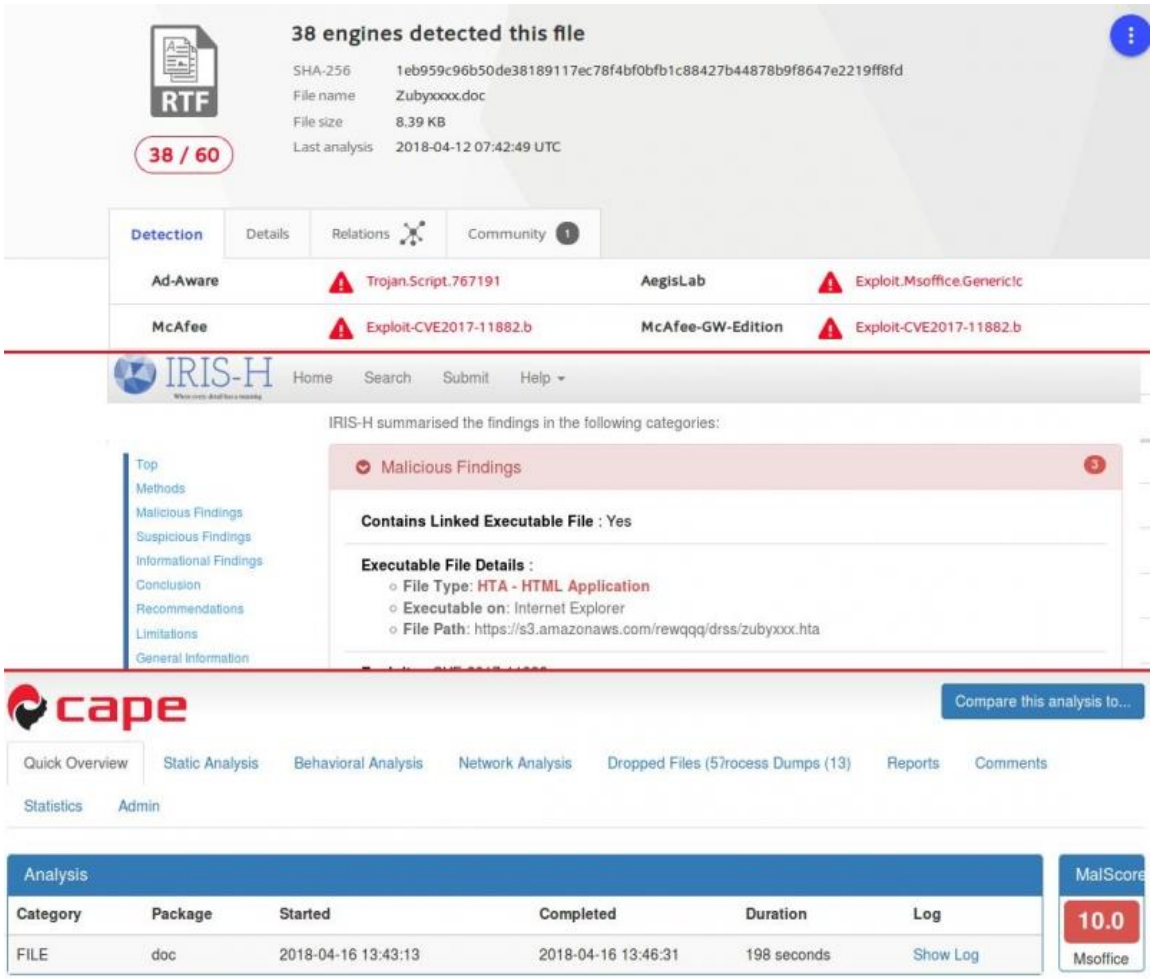
2) Перевіряти посилання та файли, перш ніж відкрити.



Червоним обведено зміст архіву. Третій файл — скрипт-приманка. Перш ніж відкривати документ або переходити за посиланням, ви можете безкоштовно та швидко перевірити їх на публічних сервісах:

- https://virustotal.com/ – перевірка файлів різних типів багатьма антивірусами (за контрольними сумами);
- https://iris-h.malwageddon.com/submit – перевірка документів MS Office;
- https://cape.contextis.com/submit/ – статичний та динамічний аналіз файлів;
- https://urlscan.io/ – перевірка URL на шкідливий вміст.

Зазначені ресурси є публічними та безкоштовними. Основна мета – переконатися, що зміст листа безпечний, до того, як запускати його на вашому комп’ютері.



Куди звернутися по допомогу:

Повідомити про кіберзлочини, кібершахрайство тощо: кіберполіція callcenter@cyberpolice.gov.ua;

Повідомити про кібератаки, кіберінциденти, у тому числі фішингові розсилання на органи влади, бізнес, громадян: урядова команда реагування на комп’ютерні надзвичайні події e-mail: incidents@cert.gov.ua, форма повідомлення на сайті: https://cert.gov.ua/contact-us, через сторінку у Facebook: https://www.facebook.com/UACERT;

Повідомити про кібератаки, кіберінциденти, у тому числі фішингові розсилання на державні органи влади: оперативний центр реагування на кіберінциденти e-mail: soc@scpc.gov.ua, тел.: (044) 281-87-37;

Оперативно-технічна служба Державного центру кіберзахисту: (044) 281-88-01.

Повідомити про ресурси в інтернеті, які розповсюджують дезінформацію: департамент кіберполіції Національної поліції України: https://t.me/stopdrugsbot.

Повідомити про загрозу нацбезпеці України в інтернеті, зокрема спроби та факти кіберрозвідки інших держав, кібертероризму та кібершпигунства – ситуаційний центр забезпечення кібербезпеки СБУ:

incident@dis.gov.ua – про виявлені кіберінциденти на об'єктах критичної інфраструктури та в органах державної влади;

cvd@dis.gov.ua – про виявлені вразливості в інформаційно-телекомунікаційних системах на об'єктах критичної інфраструктури та в органах державної влади.

Результат тестування в Jigsaw: