кримінального правопорушення, пов’язаного з корупцією, вимагає вказування у процесуальних документах належність цієї особи до категорії службових осіб, до якої відноситься дане діяння. Оскільки дещо різниться кваліфікація кримінальних правопорушень в залежності від обіймання особою посади, що пов’язана із виконанням нею функцій представника влади, організаційно-правових або адміністративно-господарських обов’язків.

Список використаних джерел:

1. Кримінальний кодекс України: Закон України від 05.04.2001. № 2341-III. Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/card/2341-14 (дата звернення: 06.11.2021).

2. Коментар до статті 364. Зловживання владою або службовим становищем. Юридичні послугу Online. URL: http://yurist-online.com/ukr/uslugi/yuristam/kodeks/024/361.php (дата звернення: 06.11.2021).

3. Про затвердження Змін до Роз'яснення щодо застосування окремих положень Закону України "Про запобігання корупції" стосовно заходів фінансового контролю: Рішення Національного агенства з питань запобігання корупції від 08.02.2019. № 368. URL: https://rp.gov.ua/upload-files/Activity/Corruption/NAZK_08022019_368.pdf (дата звернення: 06.11.2021).

4. Про державну службу: Закон України від 10.12.2015. № 889-VIII. Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/card/889-19 (дата звернення: 06.11.2021).

Чехута М.
здобувач вищої освіти ННІП ПФПНП Дніпропетровського державного університету внутрішніх справ

Науковий керівник:
Гаркуша А.
Доцент кафедри кримінального процесу Дніпропетровського державного університету внутрішніх справ, к.ю.н., доцент, майор поліції

ДЕЩО ПРО КІБЕРЗЛОЧИННІСТЬ

Поки ми користуємося своїми ноутбуками і телефонами за нашою інформацією розгортається справжнє полювання. Хакери вигадують все більш складні віруси, а ті хто з ними борються створюють все більш складний захист. Виглядає приблизно як піраміда до основних так званих масових загроз відносяться фішингові листи ,трояни - це більшість атак в інтернеті, які ні на кого не націлені, складають приблизно 90% . трохи вище знаходиться цільові атаки тобто націли на конкретних людей або організації включають в себе

приблизно 9.9%, а верхівку вінчає новинка нашого століття кібер-зброя0.1%. Кожен хакер сам вирішує, яку нішу йому зайняти для нескінченої війни з фахівцями по кібер -безпекці. Більшість атак не на когось конкретного не націлена, це як зазвичай трояни або фишенгові листи які гуляють по мережі, їх жертвами стають в основному ті, що не потурбували про свою безпеку або кібер грамотності. Прикладом є коли на пошту приходить фішинговий лист з різними посиланнями(архівами), або як приклад лист чоловікові від жінки або жінці від чоловіка з провокаційним змістом для того, щоб людина перейшла за посиланням внизу листа. Коли переходить по тому посиланню або в архів, який йому відправили в даному повідомленні то не чого не відбувається, а "заражені" думають що це якась помилка і цей лист адресовано не йому ,потім спокійно закривають його і забуває про це. Через деякий час він виявляє, що на карті стало менше грошей або стерли всю зарплату. Така атака побудована на неуважності і називається « IDN homograph attack»[1].Раніше браузери були вразливі, ми могли зайти на сайти які були створені через спеціальну програму, які генерують злі url хакери підставляли сайти на які потрібно створити копію, і вже створюється хитра копія url.

Сьогодні радує те що кібер грамотність зростає і вже не кожен переходитиме за невідомими посиланнями. Погана новина в тому, що це стали розуміти і хакери і тепер вони почали діяти по-іншому «DRIVE-BY DOWENLOAO» -ЦЕ новий тип атак, ти просто заходиш на сайт і виникає зараження системи. Сьогодні смартфон це перше що ми бачимо з ранку і останнє що ми бачимо перед сном. Якщо раніше шахраї могли вкрасти гроші з рахунку мобільного телефону, то тепер коли у більшості встановлений додаток банків, можна вивести набагато більше грошей. Є багато варіантів як це зробити: один з них це фейкові програми. Видимість програм таких як “GOOGL Play” для багатьох це гарант якості, перевірене джерело. Це спонукає шахраїв створювати більш законні схеми шахрайства. Прикладом є додаток «Ancestry» - воно ніби допомагає знайти предків. Вводиш ім'я, дату і місце народження і додаток просить піднести палець, щоб знайти когось із родичів (для того щоб скачати вашу біометрію і порівняти з біометрією наприклад вашого прадіда). Більшість людей навіть не замислюються що наших далеких родичів не можна знайти по відбитку пальців, і до того ж що у людей не ідентичні відбитки і не можна знайти тільки по відбитку пальців.

Є також шахрайство з банкоматами. Шахраї встановлюють на картоприймачу «ATM SKIMMER» цей приймач зчитує дані з магнітної смуги, його можна впізнати через те, що він опуклий і виходить з меж стін банкомату. Банки звернули на це увагу і зробили «анти SKIMMER», але є проблема вони схоже на ті самі приймачі шахраїв. Зараз їх роблять прозорими, щоб було видно що всередині немає проводів, сканерів і плат. Після отримання ваших даних шахраї просто виготовляють копію вашої карти та знімають гроші де їм завгодно.

Розберемо з чого складається все угруповання цілком. На чолі стоїть кілька людей: експерт з баз даних, фахівці розвідки банківських систем,

програміст який написав «зловред», чистильник для того щоб очистити цифрові сліди і фішер який буде відправляти листи – разом вони складають кібер ОЗУ. Код вірусу пакується у вкладенні і розсилається фішером листами на пошту бухгалтерам банків. Тема листів, імена вкладень, такі щоб їх хотілося відкрити. Відкрив файл-значить відкрив шкідливий код. Вірус який проникає в сервери, що відповідають за управління банкоматами, вони подають їм команди і точний час для видачі грошей. Таким чином постраждало близько 100 організацій. Після операції підключався чистильник і очищав цифрові сліди в системі банків. і в такий спосіб вони звели у банків один мільярд 200 мільйонів доларів і це найбільше цифрове пограбування в історії, це відбувалося в Іспанії. [4]

Першими хто зайнявся розслідування такої атаки була лабораторія Касперського[2] вони перші зрозуміли, що це шкідлива атака, провели розслідування і відновили послідовність дій хакерів.

Цифровий світ в якому ми зараз живемо здається зручним, все стає цифрованим, все підключається до інтернету, ну разом з цим приходять і нові загрози.

Список використаних джерел

1. Wikipedia-free enceklopedia // IDN homograph attack //15.10.2021//URL: https://en.wikipedia.org/wiki/IDN_homograph_attack

2. The BELL//Новин// Катана из Аликанте. Как удалось раскрыть крупнейшее цифровое ограбление в истории// 1 .06.2018//URL: https://thebell.io/katana-iz-alikante-kak-udalos-raskryt-krupnejshee-tsifrovoe-ograblenie-v-istorii

3. ANTI-MALWERE//Лабораторія Касперського//URL: https://www.anti-malware.ru/companies/kaspersky-lab

4. КореспонденТ.net.// Кибер ОПГ. Главная угроза в мире по версии NYT//URL: https://korrespondent.net/world/4383169-kyber-oph-hlavnaia-uhroza-v-myre-po-versyy-NYT