УДК 343.72:004.773+343.97
Марков В'ячеслав Валерійович
кандидат юридичних наук, старший науковий співробітник,
декан факультету № 4 Харківського національного університету внутрішніх справ
https://orcid.org/0000-0003-2024-657X
Рвачов Олексій Михайлович
старший викладач кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-3500-9393
Гельдт Станіслав Володимирович
курсант 1 курсу факультету № 4
Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ ЧАТ-БОТІВ ДЛЯ ЗАЛУЧЕННЯ НАСЕЛЕННЯ ДО ПРОТИДІЇ КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ, ЩО ВЧИНЯЮТЬ ЗЛОВМИСНИКИ З ВИКОРИСТАННЯМ ЗАСОБІВ ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ ТА ЕЛЕКТРОННИХ КОМУНІКАЦІЙ

В останні роки спостерігається стала тенденція щодо збільшення серед населення як світу, так і України, користувачів інтернету.

Так в жовтні 2020 року організації «We Are Social» та «Hootsuite» опублікували звіт «Digital 2020» в якому зазначено, що більше 4,66 мільярдів людей з 7,81 мільярдів населення світу користуються інтернетом, а аудиторія соціальних мереж перевалила за відмітку в 4,14 мільярда [1].

За даними дослідження щодо проникнення інтернету в Україні, що було проведено у III кварталі 2020 року дослідницьким холдингом «Factum Group Ukraine» на замовлення «Інтернет Асоціація України» 71 % населення України є регулярними користувачами інтернету [2].

Українські користувачі інтернету не тільки використовують його для спілкування, отримання корисної інформації, навчання та роботи, а серед іншого також за допомогою інтернету користуються дистанційними банківськими послугами.

Національний банк України підрахував, що за перше півріччя 2020 року українці здійснили 2 306,6 мільйонів безготівкових операцій з використанням

платіжних карток на загальну суму 982,8 мільярда гривень, у тому числі 296,2 млн. операцій з переказу коштів з «картки» на «картку» на суму 415,5 мільярдів грн., 501,8 млн. операцій з оплати товарів/послуг у мережі Інтернет на суму 226,2 мільярдів грн., 396,6 млн. операцій з переказу коштів з «картки» на банківський рахунок у мережі Інтернет (погашення кредитів, поповнення депозитів тощо) на суму 65,9 мільярдів грн [3].

Такі обсяги коштів, які зберігають та пересилають українці в безготівковій формі, привертають увагу не тільки комерсантів, які все більше пропонують своїм клієнтам сплатити кошти за товари та послуги онлайн, але й представників кримінального світу.

За підрахунками Української міжбанківської асоціації членів платіжних систем ЕМА, сумарний дохід інтернет-шахраїв за перше півріччя склав 116,5 млн грн. 93 % від цієї суми вони отримали, застосовуючи методи соціальної інженерії [4].

До основних способів незаконного заволодіння коштами користувачів інтернету, що вчиняють зловмисники з використанням сучасних електронних комунікацій, можна віднести наступні:

1) направлені на користувачів терміналів мобільного (рухомого) зв’язку (мобільних телефонів, смартфонів та інтернет-плашетів):

а) розсилка фейкових повідомлень через SMS-повідомлення;

б) фейкові телефонні дзвінки від начебто:

– банківських працівників;

– операторів мобільного зв’язку;

– правоохоронців;

– податківців;

– лікарів;

– соціальних працівників;

– працівників державних установ;

– тощо;

2) направлені на користувачів інтернету незалежно від виду пристрою, яким вони користуються для отримання доступу до мережі Інтернет:

а) розсилка повідомлень через вебсайти та програмні додатки:

– інтернет-мессенджерів;

– соціальних комп'ютерних мереж;

– електронної пошти;

б) використання фейкових вебсайтів [5, с. 151]:

– інтернет-магазинів;

– поповнення рахунків мобільних операторів;

– переказу коштів;

– банківських установ;

– маркетплейсів;

– продажу білетів на транспорті засоби, що здійснюють міжнародні пасажирські перевезення;

– компаній, що надають послуги з доставки товарів;

– компаній, що проводять розіграші товарів та послуг;

– організацій, що проводять онлайн-опитування чи дослідження;

– державних установ, що здійснюють соціальні виплати від держави;

– тощо;

в) розміщення на інтернет-ресурсах (наприклад, в соціальних комп'ютерних мережах, маркетплейсах) шахрайських оголошень про:

– продаж товарів чи послуг;

– збір благодійної допомоги, наприклад, на лікування чи для постраждалих від аварій, пожеж тощо;

г) надсилання користувачам чи розміщення на популярних інтернет-ресурсах програм чи файлів, що мають прихований від користувача шкідливий функціонал.

Для ошукування громадян кібершахраї використовують не тільки методи соціальної інженерії, але й інформаційні приводи про події, які нещодавно відбулися або повинні відбутися найближчим часом, такі як:

– спортивні змагання чи виступи відомих артистів для продажу білетів на ці заходи;

– соціальні виплати від держави для різних верст населення (багатодітним родинам, пенсіонерам, підприємцям, особам похилого віку тощо);

– ювілеї відомих комерційних установ (наприклад, банківських установ, ІТ-компаній тощо);

– взлом популярних вебсайтів (наприклад, соціальних комп'ютерних мереж, поштових серверів, державних реєстрів чи баз даних тощо);

– витік конфіденційних даних у компаній, які мають велику кількість клієнтів (наприклад, банків, кур'єрських компаній тощо);

– появу ефективних методів профілактики та лікування популярних хвороб, продаж за привабливими цінами чи безкоштовну роздачу експрес-тестів чи ліків від цих хвороб (наприклад, гострої респіраторної хвороби COVID-19, спричиненої короновірусом SARS-CoV-2) [6, с. 186].

Однією із причин втрати коштів інтернет-користувачем також може бути кібероніманія – неконтрольовані особою покупки товарів в інтернет-магазинах, без реальної необхідності їх придбання та без урахування власних фінансових можливостей, постійна участь в онлайн-аукціонах [7, с. 130].

На теперішній час українські інтернет-користувачі використовуючи наступні офіційні вебресурси державних установ можуть перевірити наявні в них дані про певну особу (наприклад, продавця чи покупця), телефонного абонента тощо щодо можливість їх причетності к шахрайствам:

1) на вебсайті Української міжбанківської асоціації членів платіжних систем ЕМА у розділі «BlackList EMA» (https://www.ema.com.ua/citizens/blacklist/) перевірити:

– посилання на вебсайти;

2) на вебсайті Департаменту кіберполіції Національної поліції України у розділі «Стоп Фрауд» (https://cyberpolice.gov.ua/stopfraud/) перевірити:

– номери банківських платіжних карток;

– номери мобільних телефонів;

– посилання на вебсайти;

3) на вебсайті МВС України:

– перевірити за серією та номером паспорта чи він не викрадений чи втрачений;

3) на вебсайті Державної міграційної служби України у розділі «Перевірка недійсних документів» (https://nd.dmsu.gov.ua/) перевірити за серією та номером чи є недійсним:

– паспорт громадянина України;

– паспорт громадянина України у формі картки;

– паспорт громадянина України для виїзду закордон;

– тимчасове посвідчення громадянина України;

– інші типи документів, що видають особам у підрозділах міграційної служби;

4) на вебсайті Міністерства юстиції України в Єдиному державному реєстрі юридичних осіб, фізичних осіб-підприємців та громадських формувань (https://usr.minjust.gov.ua/content/free-search) перевірити:

– чи займається підприємницькою діяльністю та якою самою певна фізична чи юридична особа, її юридичину адресу, хто є керівником організації;

– чи існує певна державна чи комунальні організація, установа чи підприємство, їх контактні дані.

В останні декілька років в Україні були виявлені непоодинокі факти, коли зловмисники використовували сучасні засоби електронних комунікацій для:

– незаконного збуту наркотиків у безконтактний спосіб;

– поширення порнографічних фото та відеофайлів, у тому числі дитячої порнографії;

– рекламування електронних ресурсів, що здійснювали продаж незаконних товарів та послуг;

– поширення фейкових новин і повідомлень від імені державних установ, політичних діячів, відомих публічних осіб;

– поширення неправдивої та конфіденційної інформації;

– тощо.

В 2018-2020 роках в Україні почали все частіше з’являтися для популярних інтернет-месенджерів чат-боти, що були розроблені приватними особами, громадськими об’єднаннями, державними, комунальними та комерційними установами чи організаціями. Основне призначення багатьох із цих чат-ботів – це швидка передача користувачем певної невеликої інформації власнику чат-боту, або швидкий пошук та отримання користувачем певної інформації з великих баз даних.

19 вересня 2019 року на засіданні Координаційної ради з протидії наркоманії Харківської міської ради, активними учасниками якого є представники факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ, було презентовано Telegram чат-бот «СтопНаркотик» (https://t.me/StopDrugsBot), який було розроблено курсантами та працівниками факультету № 4 [8, с. 213].

На теперішній час за безпосередньої допомоги користувачів Telegram чат-боту «СтопНаркотик» вдалося заблокувати більше 1800 електронних адрес у месенджері Telegram, що використовували зловмисники для незаконного збуту наркотиків через мережу Інтернет.

За більше року роботи чат-боту «СтопНаркотик» його авторський колектив декілька разів приймав рішення та проводив так звані «Дні протидії кібершахраям». В ці дні користувачам чат-боту замість надсилання електронних посилань на адреси, що використовують зловмисники для незаконного збуту наркотиків та на які необхідно залишити електронні скарги адміністрації месенджера Telegram, надсилались електронні адреси, що використовувались зловмисниками для:

– начебто продажу підроблених банкнот України різного номіналу;

– виманювання у користувачів банківських платіжних карток конфіденційної інформації для несанкціонованого списання коштів через фейкові чат-боти державного банку;

– розміщення фейкових новин і повідомлень від імені державних установ, політичних діячів, відомих публічних осіб;

– поширення неправдивої та конфіденційної інформації про жінок;

– поширення «порад» щодо того, як здійснювати насильство над жінками, у тому числі сексуальне [9, с. 306].

Завдяки об'єднанню зусиль небайдужих інтернет-користувачів чат-боту «СтопНаркотик» певну кількість електронних адрес, що використовували зловмисники у своїй протиправній діяльності, вдалося або заблокувати, або ці електронні адреси отримали позначку «Scam» (шахрайство).

На теперішній час на факультеті № 4 Харківського національному університеті внутрішніх справ ведуться роботи щодо створення під егідою МВС України всеукраїнського чат-боту «СтопШахрай», адмініструванням якого буде займатися Харківський національний університет внутрішніх справ.

Планується, що зазначений чат-бот повинен мати наступні функціоналі можливості:

1) отримувати від громадян та працівників правоохоронних органів електронні адреси, що використовують зловмисники з метою скоєння кібершахрайств, продажу заборонених товарів та послуг, поширення недостовірної та небезпечної інформації тощо;

2) участь користувачів чат-боту у спільному залишенні скарг на електронні адреси, що використовують зловмисники у своїй протиправній діяльності;

3) перевірка користувачами чат-боту наявної в них інформації про певних осіб, щодо їх можливої приналежності до шахрайств (за номером мобільного телефону, номером банківської картки, електронної адресою у месенджері тощо).

Використання чат-ботів є одним із методів залучення населення до протидії кримінальним правопорушенням, що вчиняють зловмисники з використанням засобів обчислювальної техніки та електронних комунікацій.

Список використаних джерел

1. Digital 2020 October Global Statshot Report (October 2020) v01 // slideshare : site. 20.10.2020. URL: https://www.slideshare.net/DataReportal/digital-2020-

october-global-statshot-report-october-2020-v01 (дата звернення: 20.11.2020).

2. Проникнення інтернету в Україні. Жовтень 2019 // Інтернет асоціація України : офіційний сайт. URL: https://inau.ua/sites/default/files/file/1910/dani_ustanovchyh_doslidzhen_iii_kvartal_2019_roku.pdf (дата звернення: 20.11.2020).

3. Розподіл безготівкових операцій з використанням платіжних карток у І півріччі 2020 року // Офіційне інтернет-представництво Національного банку України. 06.08.2020. URL: https://bank.gov.ua/admin_uploads/article/06-08-20_Cashless_operations_ua.jpg?v=4 (дата звернення: 20.11.2020).

4. Нобіуз В. Онлайн-покупки, або Як не заплатити шахраям // Mind.ua : сайт / ТОВ «Фьючер Медіа». 27.11.2020. URL: https://mind.ua/openmind/20218797-onlajn-pokupki-abo-yak-ne-zaplatiti-shahrayam (дата звернення: 20.11.2020).

5. Зуб Л. В., Рвачов О. М. Сучасні загрози сімейній онлайн безпеці: класифікація та профілактика виникнення // Актуальні питання протидії кіберзлочинності та торгівлі людьми : збірник матеріалів Всеукр. наук.-практ. конф. (23 листоп. 2018 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2018. С. 149-154. URL: http://univd.edu.ua/general/publishing/konf/23_11_2018/pdf/45.pdf (дата звернення: 20.11.2020).

6. Рвачов О. М., Ковтун В. О. Сучасні кібершахрайства щодо протизаконного заволодіння коштами з банківських рахунків громадян // Протидія кіберзлочинності та торгівлі людьми : зб. матеріалів Міжнарод. наук.-практ. конф. (27 травня 2020 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2020. С. 185-189. URL: http://www.univd.edu.ua/general/publishing/konf/27_05_2020/pdf/53.pdf (дата звернення: 20.11.2020).

7. Бєляєва Є. Г., Рвачов О. М. Мережа Інтернет як джерело підвищеної небезпеки для дітей // Актуальні питання протидії кіберзлочинності та торгівлі людьми : збірник матеріалів Всеукр. наук.-практ. конф. (23 листоп. 2018 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2018. С. 128-131. URL: http://univd.edu.ua/general/publishing/konf/23_11_2018/pdf/38.pdf (дата звернення: 20.11.2020).

8. Рвачов О. М., Лактіонов В. В., Дацюк Д. О. Сучасні методи активного залучення населення до протидії збуту наркотичних засобів, психотропних речовин або їх аналогів через мережу Інтернет // Протидія кіберзагрозам та торгівлі людьми (26 листоп. 2019 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2019. С. 210-217. URL: http://www.univd.edu.ua/general/publishing/konf/26_11_2019/pdf/65.pdf (дата звернення: 20.11.2020).

9. Марков В. В., Рвачов О. М., Ковтун В. О. Досягнення та перспективи розвитку факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ // Шлях успіху і перспективи розвитку (до 26 річниці заснування Харківського національного університету внутрішніх справ)

: матеріали Міжнар. наук.-практ. конф. (м. Харків, 20 листоп. 2020 р.) / [редкол.: Д. В. Швець (голова), О. М. Бандурка, С. М. Гусаров та ін.] ; МВС України, Харків. нац. ун-т внутр. справ. Харків : ХНУВС, 2020. С. 303-310. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/9722/Shliakh%20uspikhu_2020.pdf?sequence=3&isAllowed=y (дата звернення: 20.11.2020).

Одержано 20.11.2020

УДК [351.74(100):004.9](075.8)

Могілевський Леонід Володимирович
доктор юридичних наук, професор,
проректор Харківського національного університету внутрішніх справ
http://orcid.org/0000-0002-6994-6086

ВЕЛИКІ ДАНІ У ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Великі дані виступають тут у ролі ультимативного інструменту розслідування кіберзлочинів і запобігання їм. Упроваджуючи чергову схему, зловмисники всюди залишають цифрові сліди. Окремо ці малі зміни зазвичай ігноруються. Однак на рівні Великих даних злочин з використанням мережевих технологій виглядає як характерний патерн. Повністю приховати його не вдасться, як би ретельно не маскувалися окремі прояви.

Стало набагато легше відстежити нелегальні ключі активації програмних продуктів. Раніше самі розробники виявляли тільки вкрадені однокористувальні ліцензії, коли їх намагалися одночасно використовувати кілька людей. Зараз обмін даними дозволяє побачити, що корпоративний ключ однієї з програм був украдений або відбувається перевірка генератора ключів.

За допомогою візуалізації великих обсягів спільних даних можна побачити незвичайні сплески активності на серверах реєстрації, що може вказувати на тестування вкрадених або згенерованих ключів. Без засобів візуалізації ці аномалії, скоріш за все, залишалися б непоміченими.

Традиційними засобами вебмоніторингу протидіяти піратству сьогодні вже навряд чи можливо. У світі існує понад 600 млн сайтів; з використанням