ЗАСТУПНИК СЕКРЕТАРЯ
РАДИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

вул. Петра Болбочана, 8, м. Київ, 01601, телефон: (044) 255-06-50, телефакс: (044) 255-05-85

_____ № _____

_____

Голові Правління Інтернет Асоціації України

САВЧУКУ О.М.

Щодо фільтрації фішингових доменів

Шановний Олександре Михайловичу!

За дорученням Секретаря Ради національної безпеки і оборони України О. ДАНІЛОВА в Апараті РНБО України опрацьовано Ваші листи від 08.02.2023 № 13/1, від 24.02.2023 № 19/1 та від 28.02.2023 № 25/2 щодо впровадження в Україні системи фільтрації фішингових доменів. За результатами опрацювання повідомляємо.

Указом Президента України від 26 серпня 2021 року № 447 затверджено Стратегію кібербезпеки України, у розділі 1 якої визначено, що забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» Національний координаційний центр кібербезпеки здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку.

У рамках проведення координаційних заходів Національним координаційним центром кібербезпеки організовано роботу відповідних суб'єктів з метою створення системи фільтрації фішингових доменів.

Розпорядженням Кабінету Міністрів України від 27.03.2019 № 177-р у структурі Державної служби спеціального зв'язку та захисту інформації України, яка згідно із законодавством є одним із основних суб'єктів

національної системи кібербезпеки, створено Національний центр оперативно-технічного управління мережами телекомунікацій (далі – НЦУ).

Порядком оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану, затвердженим постановою Кабінету Міністрів України від 29.06.2004 № 812, зокрема передбачено, що:

1. **В умовах** надзвичайних ситуацій, надзвичайного та **воєнного стану оператори телекомунікацій**, центральні органи виконавчої влади (крім спеціальних споживачів), підприємства, установи та організації, у власності, користуванні, господарському віданні чи оперативному управлінні яких є засоби та мережі телекомунікацій, **надають можливість використовувати ресурси своїх мереж для** попередження, локалізації та ліквідації наслідків надзвичайних ситуацій, оповіщення населення, проведення мобілізації, **забезпечення потреб національної безпеки**, оборони, охорони правопорядку *(пункт 6)*.

2. **Основними завданнями НЦУ в умовах** надзвичайних ситуацій, надзвичайного та **воєнного стану є** загальне управління центрами управління мережами, **забезпечення можливості оперативно-технічного управління телекомунікаційними мережами з метою їх** сталого функціонування та **використання в інтересах** управління державою, попередження, локалізації та ліквідації наслідків надзвичайних ситуацій, оповіщення населення, забезпечення проведення мобілізації, **задоволення потреб національної безпеки**, оборони, охорони правопорядку *(пункт 26)*.

Отже в умовах воєнного стану та з метою задоволення потреб національної безпеки, відповідно до повноважень, визначених частиною восьмою статті 32 Закону України «Про електронні комунікації», а також постановою Кабінету Міністрів України від 29.06.2004 № 812, НЦУ видано розпорядження від 30.01.2023 № 67/850 «Про впровадження системи фільтрації фішингових доменів», яке є обов’язковим для виконання постачальниками електронних комунікаційних мереж та/або послуг.

Загальновідомо, що створення фішингових вебсайтів, які мають на меті збір персональних даних громадян та інформації про банківські картки, є одним із найпоширеніших видів шахрайства в інтернеті. Зловмисники реєструють фішингові домени та розміщують на них інтернет-сторінки, що імітують офіційні вебресурси банківських і фінансових установ, підприємств, які надають послуги громадянам, інтернет-магазинів тощо. Інформація, яку вводять користувачі інтернет на таких фішингових сторінках, у подальшому використовується зловмисниками з метою викрадення коштів та в інших шахрайських схемах.

В Україні після початку повномасштабної агресії рф значно зросла кількість випадків інтернет-шахрайства. Серед тем, які використовують зловмисники, активно використовується тематика фінансової допомоги

громадянам України від державних органів та міжнародних організацій. За результатами аналізу, діяльність більшості шахрайських груп, які працюють в Україні, координується злочинцями з рф, які надають типові шаблони фішингу, способи виведення коштів тощо. Крім того, в рамках гібридної війни спецслужби рф створюють фішингові сайти з метою збору персональних даних громадян України, волонтерів, військовослужбовців та членів їх сімей під виглядом заявок на допомогу. Отже, на сьогодні це є реальною загрозою національній безпеці.

Питання протидії шахрайству неодноразово розглядалося під час координаційних нарад сектору безпеки, правоохоронних органів та засідань НКЦК. За результатами дослідження способів протидії фітингу та вивчення досвіду міжнародних партнерів було визначено як найбільш перспективний підхід – фільтрацію фішингових доменів на рівні рекурсивних DNS серверів із використанням технології RPZ-зон.

З метою врахування позиції суб'єктів, що здійснюють діяльність у сфері електронних комунікацій, до роботи над розробкою та впровадженням системи фільтрації фішингових доменів було залучено представників усіх зацікавлених сторін.

Так, 14 вересня 2022 року в Апараті РНБО України було проведено міжвідомчу нараду з питань технічних та організаційних можливостей захисту громадян України від банківського та фінансового шахрайства шляхом фільтрації шкідливих доменів на рівні DNS за участю представників Національного банку України, Національної комісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку, Державної служби спеціального зв'язку та захисту інформації України, НЦУ, Департаменту кіберполіції Національної поліції України, Української асоціації операторів зв'язку «ТЕЛАС», Української міжбанківської асоціації членів платіжних систем ЄМА, а також представників великих постачальників електронних комунікаційних послуг (ТОВ «Лайфселл», ПрАТ «Київстар», ПрАТ «ВФ Україна», ПрАТ «Датагруп», ТОВ «Мережа Ланет», АТ «Укртелеком», ТОВ «ТриМоб»).

Учасники наради підтримали пропозицію щодо побудови системи фільтрації фішингових доменів на рівні рекурсивних DNS серверів. Відповідно до протокольного рішення було створено робочу групу при Апараті РНБО України, що включила дві підгрупи – з технічних та організаційно-правових питань. Протокол наради додатково було надіслано для використання в роботі народному депутатові України Федієнку О.П., заступникові голови Комітету Верховної Ради України з питань цифрової трансформації (на той час).

За результатами роботи підгрупи з організаційно-правових питань було розроблено та погоджено учасниками Регламент роботи системи фільтрації фішингових доменів (далі – Регламент). У пропозиціях та зауваженнях до проєкту цього документа представники постачальників електронних

комунікаційних послуг зазначили відсутність обґрунтованої необхідності державного регулювання питань роботи системи фільтрації фішингових доменів на рівні законів.

На період дії правового режиму воєнного стану з метою захисту громадян від шахрайства в банківській і фінансовій сфері, пов'язаного із використанням фішингових інтернет-ресурсів, учасники підгрупи запропонували механізм упровадження системи фільтрації фішингових доменів через відповідне розпорядження НЦУ. За результатами роботи підгрупи з технічних питань було здійснено тестування роботи системи фільтрації фішингових доменів з відповідними системами та мережами постачальників електронних комунікаційних послуг.

Дія Регламенту поширюється на постачальників послуг широкосмугового доступу до інтернету, які надають кінцевим користувачам послугу з отримання інформації про домени (DNS). Відповідні роз'яснення надавалися НЦУ на запити постачальників електронних комунікаційних послуг.

На виконання розпорядження НЦУ від 30.01.2023 № 67/850 до системи фільтрації фішингових доменів вже підключилися понад 250 постачальників електронних комунікаційних послуг. Системою фільтрації фішингових доменів зареєстровано понад 200 тисяч унікальних переходів на сторінку з попередженням користувачам про загрози фішингових ресурсів. За попередніми оцінками, це дозволило попередити втрати громадян України на суму понад 5 млн гривень. За результатами аналізу діяльності шахрайських груп, вони були змушені змінити свої техніки, тактики і процедури. Щонайменше одна з шахрайських груп припинила свою діяльність в Україні та спрямувала її на громадян росії та білорусі.

Робота системи фільтрації фішингових доменів не впливає на стабільність функціонування інформаційно-комунікаційних систем та мереж постачальників електронних комунікаційних послуг. Її недоступність у випадку технічного збою або кіберінциденту не може мати наслідком порушення функціонування чи нестабільну роботу систем і мереж інтернет-провайдерів.

Для захисту системи фільтрації фішингових доменів від наслідків імовірного несанкціонованого доступу до елементів системи фільтрації фішингових доменів упроваджено сучасні засоби кіберзахисту, моніторингу подій безпеки. Механізми «білих списків» та контролю цілісності списку фільтрації під час обробки та передавання мінімізують ризики помилкової фільтрації нефішингових доменів. Учасники системи фільтрації фішингових доменів мають інтерфейс доступу до активного списку фільтрації фішингових доменів, можливість в режимі реального часу слідкувати за його оновленнями, надавати пропозиції щодо додавання та виключення доменів зі списку.

Також слід зазначити, що впровадження системи фільтрації фішингових доменів не потребує додаткових фінансових витрат чи придбання обладнання постачальниками електронних комунікаційних послуг.

Таким чином, система фільтрації фішингових доменів підтверджує свою доцільність і ефективність у протидії банківському та фінансового шахрайству з використанням фішингових інтернет-ресурсів. Аналогічний підхід до фільтрації шкідливих доменів на рівні рекурсивних DNS серверів із використанням технології RPZ-зон використовується в країнах ЄС, Великій Британії та США.

Викладене вище свідчить про своєчасність прийняття рішення щодо впровадження системи фільтрації фішингових доменів, а також про достатність правових підстав для цього в умовах воєнного стану.

Водночас інформуємо, що з метою забезпечення функціонування системи фільтрації фішингових доменів після припинення чи скасування воєнного стану в установленому порядку буде вжито додаткових заходів правового регулювання, а Ваші пропозиції щодо необхідності більш точного визначення термінів буде обов’язково враховано під час розробки наступних версій Регламенту.

З повагою

Заступник Секретаря
Ради національної безпеки
і оборони України **Сергій ДЕМЕДЮК**