Прим. № 1

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

НАЦІОНАЛЬНИЙ ЦЕНТР ОПЕРАТИВНО-ТЕХНІЧНОГО УПРАВЛІННЯ
МЕРЕЖАМИ ТЕЛЕКОМУНІКАЦІЙ

Р О З П О Р Я Д Ж Е Н Н Я

м. Київ

30.01.2023 № 67/850

Про впровадження системи фільтрації фішингових доменів

Відповідно до статті 32 Закону України «Про електронні комунікації», Указу Президента України від 24.02.2022 № 64/2022 «Про введення воєнного стану в Україні», затвердженого Законом України від 24.02.2022 № 2102-IX «Про затвердження Указу Президента України «Про введення воєнного стану в Україні» (зі змінами), на виконання звернення Ради національної безпеки і оборони України щодо впровадження системи фільтрації фішингових доменів як складової Національного сервісу доменних імен (DNS)

НАЛЕЖИТЬ:

1) Постачальникам електронних комунікаційних мереж та/або послуг:
   1.1 Протягом **30 календарних днів** здійснити реєстрацію в системі фільтрації фішингових доменів та забезпечити подальше здійснення фільтрації фішингових доменів на рекурсивних DNS-серверах згідно з Регламентом роботи системи фільтрації фішингових доменів (додається);
   1.2 Про реєстрацію в системі фільтрації фішингових доменів та початок здійснення фільтрації фішингових доменів згідно з Регламентом повідомити на електронну адресу оперативного чергового НЦУ – ncu@cip.gov.ua .

2) Оперативному черговому НЦУ надіслати розпорядження до Національної комісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку, для доведення до постачальників електронних комунікаційних мереж та/або послуг і розміщення на офіційному веб-сайті.

Додаток: Регламент роботи системи фільтрації фішингових доменів. Версія 1.0, на 8 арк.

Начальник Центру Олександр ТИТАРЕНКО

Оперативний черговий НЦУ
+380 44 281 67 12

РЕГЛАМЕНТ
роботи системи фільтрації фішингових доменів
Версія 1.0

ЗМІСТ

1. Загальні положення

Цей Регламент описує основні принципи та процедури взаємодії з системою фільтрації фішингових доменів (далі – Система).

Метою створення Системи є фільтрація фішингових доменів у мережах операторів електронних комунікацій на рівні рекурсивних DNS серверів із використанням технології RPZ зон з метою протидії шахрайству в банківській і фінансовій сфері, пов'язаному із використанням фішингових інтернет ресурсів.

Система є складовою Національного сервісу доменних імен (DNS), створення якого передбачено пунктом 54 Плану реалізації Стратегії кібербезпеки України, схваленого рішенням Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України», введеним в дію Указом Президента України від 1 лютого 2022 року № 37.

Система не застосовується для фільтрації доменів та обмеження доступу до інтернет ресурсів, які використовуються для поширення шкідливого програмного забезпечення, пропаганди, дезінформації тощо, а також до інтернет ресурсів, обмеження доступу до яких здійснюється відповідно до Закону України "Про санкції".

2. Терміни та визначення

У цьому документі наведені нижче терміни вживаються в такому значенні:

провайдер DNS – постачальник електронних комунікаційних мереж та/або послуг, який надає кінцевому користувачу (пов'язану) послугу з отримання інформації про домени (DNS);

лендінгова сторінка – інтернет-сторінка, на яку здійснюється перенаправлення запитів кінцевого користувача в ході обробки DNS сервером провайдера DNS зони RPZ, яка містить перелік фішингових доменів, які фільтруються Системою, та яка містить інформацію про причини такого перенаправлення;

уповноважені державні органи – основні суб'єкти національної системи кібербезпеки, визначені Законом України "Про основні засади забезпечення кібербезпеки", підрозділ Апарату Ради національної безпеки і оборони України, який відповідає за забезпечення діяльності Національного координаційного центру кібербезпеки;

учасники Системи – уповноважені державні органи, провайдери DNS та інші суб'єкти господарювання, які мають санкціонований доступ до інформації в Системі з метою захисту власних електронних комунікаційних мереж;

домен – символьне позначення областей в мережі Інтернет, що базується на ієрархічній структурі, що дозволяє визначити доменні імена;

доменне ім'я – символьне позначення, яке служить для адресації вузлів мережі Інтернет і розташованих на них мережевих ресурсів (веб-сайтів, серверів електронної пошти, мережевих сервісів) в зручній для людини формі;

IP адреса – мережева адреса вузла в комп'ютерній мережі, побудованій за протоколом IP;

DNS – комп'ютерна розподілена система для отримання інформації про домени;

RPZ (Response Policy Zones) – стандартизований механізм застосування політик обробки запитів на серверах DNS. RPZ зона — зона DNS, в якій застосовується відповідна політика фільтрації доменів.

Інші терміни у цьому документі вживаються у значеннях, визначених законодавством України.

3. Принципи фільтрації доменів

Одним із поширених видів шахрайства в інтернет є створення фішингових ресурсів, які мають на меті збір персональних даних громадян та інформації про банківські картки. Зловмисники реєструють фішингові домени та розміщують на них інтернет-сторінки, що імітують офіційні веб-ресурси банківських і фінансових установ, державних та міжнародних організацій, які надають фінансову допомогу або інші послуги громадянам, інтернет-магазинів тощо. Інформація, яку вводять громадяни на таких фішингових інтернет-сторінках, в подальшому використовується зловмисниками з метою викрадення коштів та в інших шахрайських схемах. Система фільтрації фішингових доменів дозволяє захистити користувачів інтернет від подібного шахрайства шляхом перенаправлення їх з фішингового домену на безпечну лендінгову сторінку.

Основні засади функціонування Системи:

1. Використання стандартизованого механізму для фільтрації фішингових доменів, а саме методу DNS RPZ.

2. Фільтрація фішингового домену відбувається у період з моменту його виявлення до видалення (призупинення дії) домену на рівні реєстратора доменних імен.

3. Фільтрація відбувається на рівні рекурсивних DNS серверів українських постачальників електронних комунікаційних мереж та/або послуг.

4. З метою підвищення обізнаності користувачів інтернет реалізовано безпечну лендінгову сторінку, на яку здійснюється перенаправлення запитів до фішингових ресурсів. Ця сторінка забезпечує інформування користувачів про потенційний ризик, а також механізм зворотного зв'язку.

5. Для обліку доменів та централізованого зберігання використовується окрема подія платформи MISP, для систематизації переліку фішингових доменів використовується необхідний набір тегів.

6. Для забезпечення максимальної ефективності Системи необхідно мінімізувати час з моменту виявлення шкідливого домену до моменту фільтрації. Частота оновлення RPZ зони – до 15 хвилин з моменту внесення змін до переліку фішингових доменів.

7. Синхронізація RPZ зони відбувається від авторитетного серверу до рекурсивних серверів провайдерів DNS з використанням стандартизованих механізмів – AXFR (повна передача зони DNS RFC5936) та IXFR (інкрементальна передача зони DNS RFC1995).

Основні компоненти Системи:

1. Платформа MISP (адреса публікації https://fmisp.ncscc.gov.ua)

Платформа MISP забезпечує доступ учасників Системи до актуального переліку фішингових доменів. Перелік фішингових доменів реплікується в автоматичному режимі із MISP-NBU. Учасники Системи можуть використовувати платформу MISP для надання пропозиції до переліку фішингових доменів.

2. Авторитетний сервер DNS (IP адреса публікації 185.13.250.11)

Авторитетний сервер DNS здійснює обслуговування RPZ зони "fraud-rpz.ua.db", яка автоматизовано оновлюється у відповідності до переліку фішингових доменів у платформі MISP, та виступає провайдером для реплікації RPZ зони для рекурсивних DNS серверів учасників Системи.

3. Лендінгова сторінка (IP адреса публікації 185.13.250.10)

Інтернет-сторінка, на яку здійснюється перенаправлення запитів кінцевого користувача до фішингового домену.

4. Рекурсивні DNS сервери учасників Системи

Рекурсивні сервери учасників Системи, що здійснюють обслуговування клієнтських запитів із застосуванням політик RPZ.

За потреби учасники Системи можуть використовувати проміжні DNS сервери для централізованого розповсюдження RPZ зони у середині своєї мережі.

За погодженням з власником Системи допускається, щоб провайдери DNS синхронізували RPZ зону від інших провайдерів DNS, наприклад, по регіональному чи ієрархічному принципу.

4. Організація взаємодії з Системою

Для отримання доступу до Системи провайдер DNS здійснює реєстрацію в Системі шляхом надсилання заявки на адресу fraud-filter@ncscc.gov.ua.

Заявка провайдера DNS на реєстрацію в Системі повинна містити: назву провайдера DNS та код СДПРОУ/ІПН, ПІБ та адресу електронної пошти уповноваженої особи, IP адресу(-и) власного DNS серверу, який здійснює

синхронізацію зони RPZ. Додатково провайдер DNS може вказати перелік власних підмереж (AS) для доступу до статистичних даних щодо роботи Системи, назву і версію програмного забезпечення власного DNS серверу для отримання технічних рекомендацій з його налаштування.

Відповідно до наданих провайдером DNS в заявці на реєстрацію даних в платформі MISP за адресою https://fmisp.ncscc.gov.ua створюється користувач з правами "org admin", який має права створювати додаткових користувачів з представників своєї організації.

Учасники Системи відповідають за підтримку реєстраційних даних в актуальному стані.

Після реєстрації, провайдер DNS налаштовує на власному DNS сервері синхронізацію зони RPZ "fraud-rpz.ua.db".

Реєстрація в Системі уповноважених державних органів здійснюється на підставі листа-запиту до Апарату Ради національної безпеки і оборони України, що містить ПІБ та адресу електронної пошти уповноваженої особи.

5. Внесення доменів до зони RPZ

Відповідальність за ведення переліку фішингових доменів покладається на галузеву команду реагування на кіберінциденти у банківській системі України Національного банку України CSIRT-NBU (далі – CSIRT-NBU). Для зберігання та розповсюдження переліку фішингових доменів використовується платформа MISP.

Команда CSIRT-NBU розглядає звернення від основних суб'єктів забезпечення кібербезпеки України та учасників Системи щодо внесення доменів до переліку фільтрації. Команда CSIRT-NBU проводить періодичний перегляд статусів доменів із метою мінімізації переліку. Фільтрації підлягають тільки активні домени, не заблоковані реєстраторами доменних імен.

Пропозиції учасників Системи щодо внесення доменів до зони RPZ надаються на адресу fraud-filter@ncscc.gov.ua та/або через механізм "proposals" в екземплярі MISP за адресою https://fmisp.ncscc.gov.ua.

Пропозиції щодо внесення доменів до зони RPZ розглядаються протягом робочого часу. Строк обробки пропозиції щодо внесення домену до зони RPZ – дві години з часу надання пропозиції.

Користувачі інтернет, які виявили фішинговий домен, мають право надати пропозиції щодо внесення доменів до зони RPZ через учасників Системи та/або Урядову команду реагування на комп'ютерні надзвичайні події України CERT-UA.

6. Вилучення доменів із зони RPZ

Пропозиції щодо вилучення доменів із зони RPZ можуть надаватися усіма учасниками Системи. Остаточне рішення про вилучення доменів із зони RPZ приймає CSIRT-NBU.

Пропозиції учасників Системи щодо вилучення доменів із зони RPZ надаються на адресу fraud-filter@ncscc.gov.ua та/або через механізм “proposals” в екземплярі MISP за адресою https://fmisp.ncscc.gov.ua.

Власник або адміністратор домену, який вважає, що його домен помилково внесено до зони RPZ, надсилає мотивовану заявку на виключення домену на електронну адресу, вказану на лендінговій сторінці. Заявка повинна містити ідентифікацію особи та підтвердження права власності на домен.

Пропозиції щодо вилучення домену із зони RPZ розглядаються під час робочого часу. Строк оновлення RPZ зони складає до 15 хвилин з моменту внесення змін до переліку доменів.

7. Білі списки доменів

З метою зменшення ризику помилкового внесення не фішингових доменів до зони RPZ Система використовує механізм білих списків доменів. До білого списку внесені домени, які заборонено фільтрувати за допомогою Системи.

Пропозиції щодо додавання доменів до білого списку можуть надаватися усіма учасниками Системи. Остаточне рішення про внесення доменів до білого списку приймає CSIRT-NBU.

Користувачі інтернет мають право надати пропозиції щодо внесення доменів до білого списку через учасників Системи.

8. Вимоги до лендінгової сторінки

Лендінгова сторінка повинна містити:

- попередження користувачу інтернет про небезпеку переходу на фішинговий ресурс;
- доменне ім'я або URL фішингової сторінки, на яку здійснюється перехід
- поточну дату та час
- адресу електронної пошти для подання заявки на виключення домену із зони RPZ.

Додатково лендінгова сторінка може містити рекомендації з кібербезпеки для користувачів інтернет.

9. Статистика та звітність

При переході на лендінгову сторінку у Системі зберігається технічна інформація, що включає дату і час, IP адресу (підмережу), з якої здійснюється перехід, доменне ім'я або URL фішингової сторінки, на яку здійснюється перехід, user-agent тощо.

Система має інтерфейс для доступу до інформації щодо переходів на лендінгову сторінку.

Провайдерам DNS за запитом надається інформація щодо переходів на лендінгову сторінку з їх підмереж за умови надання списку їх підмереж (AS) під час реєстрації.

З метою аналізу та відповідного реагування уповноваженим державним органам надається доступ до інформації щодо переходів на лендінгову сторінку.

CSIRT-NBU раз на півроку публікує та надає до НКЦК узагальнені статистичні дані щодо використання та ефективності роботи Системи.

10.Інше

Провайдери DNS не несуть відповідальності за точність інформації в зоні RPZ, фільтрацію доменів у відповідності до цього Регламенту.

Власником Системи є Національний координаційний центр кібербезпеки в особі структурного підрозділу Апарату Ради національної безпеки і оборони України, який відповідає за забезпечення діяльності НКЦК.

Текст цього Регламенту публікується за адресою https://fmisp.ncscc.gov.ua/reglament/. В разі внесення змін до цього Регламенту власник Системи повідомляє учасників Системи не менше ніж за 10 робочих днів до набирання чинності таких змін шляхом направлення повідомлень на електронну пошту учасників, зазначених ними під час реєстрації в Системі.

Адреса технічної підтримки: fraud-filter@ncscc.gov.ua.