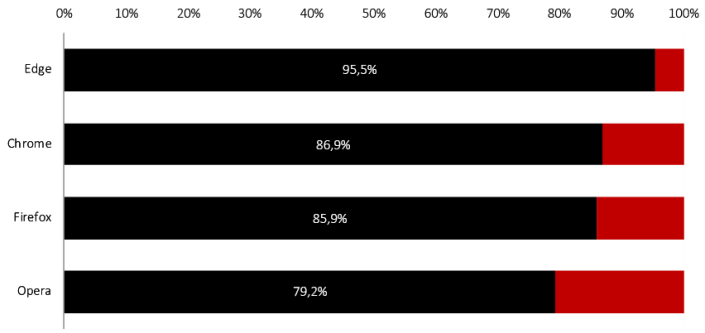
Другий квартал 2020 р. ЗВІТ ПРО ПОРІВНЯЛЬНЕ ТЕСТУВАННЯ

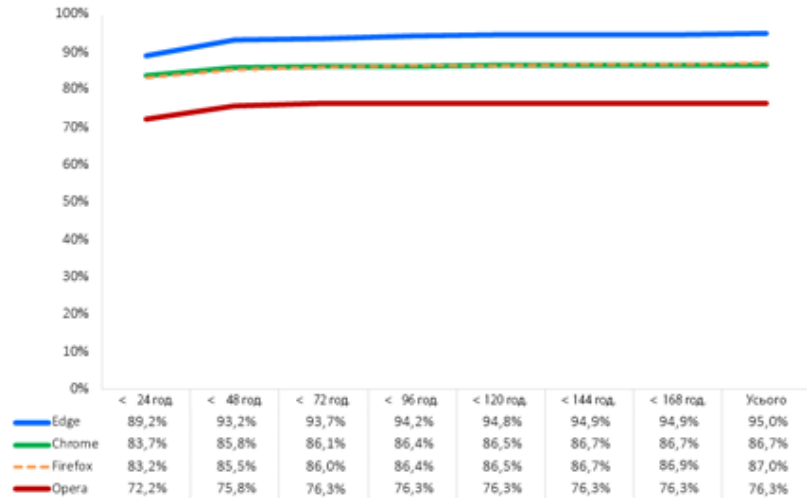
Огляд

Протягом другого кварталу 2020 р. NSS Labs виконувала незалежне тестування захисту від фішингу, який забезпечується веб-браузерами: протягом 18 днів було виконано 47 274 окремих тести (для одного веб-браузера) з використанням 2443 унікальних URL-адрес. Задля забезпечення захисту від фішингу в браузері Microsoft Edge застосовується фільтр SmartScreen для захисника Windows, у браузерах Google Chrome і Mozilla Firefox застосовується API безпечного перегляду Google, а в браузері Opera застосовується поєднання сторонніх списків заблокованих веб-сайтів.



Браузер Microsoft Edge забезпечує найліпший захист, блокуючи 95,5% URL-адрес фішингу, при цьому він забезпечує найвищий рівень захисту в першу годину після виникнення загрози (89,2%). Рівень захисту, який забезпечується браузером Google Chrome, посідає друге місце: цей браузер блокує в середньому 86,9% атак, при цьому цей показник для браузера Mozilla Firefox становить 85,9%, внаслідок чого цей браузер посідає третє місце. Браузер Opera блокує 79,2% атак.

Резюме результатів

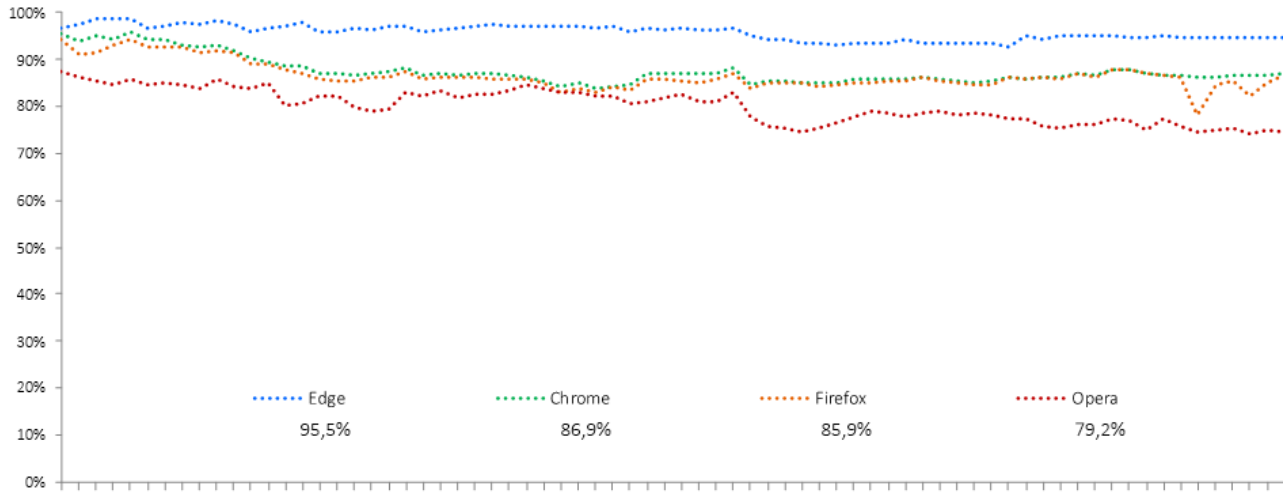


	< 24 год.	< 48 год.	< 72 год.	< 96 год.	< 120 год.	< 144 год.	< 168 год.	Усього
Edge	89,2%	93,2%	93,7%	94,2%	94,8%	94,9%	94,9%	95,0%
Chrome	83,7%	85,8%	86,1%	86,4%	86,5%	86,7%	86,7%	86,7%
Firefox	83,2%	85,5%	86,0%	86,4%	86,5%	86,7%	86,9%	87,0%
Opera	72,2%	75,8%	76,3%	76,3%	76,3%	76,3%	76,3%	76,3%

Системи визначення репутації URL-адрес скорочують час, який є у зловмисників для досягнення своїх цілей, способом попередження користувачів, що та або інша URL-адреса є відомим фішинговим веб-сайтом. Однак оскільки користувачі відвідують широкий спектр різних веб-сайтів, багато з яких є новими, системи визначення репутації URL-адрес не можуть просто блокувати всі нові URL-адреси. Оскільки зловмисники про це знають, їхні операції фішингу постійно змінюються, при цьому основна кількість нових атак відбувається в перші кілька годин початку зловмисної операції.

NSS Labs оцінила спроможність браузерів блокувати зловмисні URL-адреси негайно після їхнього виявлення нами в Інтернеті. Ми продовжували тестувати їх кожні шість годин задля виявлення часу, який потрібен постачальнику для організації захисту, якщо взагалі здійснювався будь-який захист.

Зміна захисту від фішингу в динаміці часу



Протягом тестування щодня додавалися нові фішингові URL-адреси, при цьому видалялися URL-адреси, які більше не були доступними або не здійснювали фішингових атак. Кожна точка даних представляє собою оцінку захисту, який забезпечується в конкретний момент часу. Якщо URL-адреса заблокована на початку атаки, оцінка послідовності захисту в динаміці часу, який забезпечується тим або іншим браузером, покращується. Натомість, якщо браузер не заблокував таку URL-адресу, оцінка погіршується.

Тестування проводилося на основі методики тестування веб-браузерів версії 4.0 (доступній за посиланням www.nsslabs.com).

Загальна інформація

Фішинг – це тип методу проникнення в захищені системи, так званого «соціального інжинірингу», при застосуванні якого зловмисники переконують об'єкт атаки надати їм конфіденційну особисту інформацію. Деякі приклади конфіденційної інформації включають номери кредитних карт, номери полісів соціального страхування, інформацію щодо імені користувача та паролю для входу у випадку банківських рахунків. Каналами фішингових атак є електронна пошта, миттєві повідомлення, SMS-повідомлення та посилання в соціальних мережах. Нерідко цільова сторінка фішингового веб-сайту також робить спробу проникнення в комп'ютер відвідувача та встановлення зловмисного програмного забезпечення (цей метод також можна описати, як «короткочасне проникнення»).

Фішингові атаки є значним ризиком як для фізичних осіб, так і для організацій, оскільки представляють собою загрозу розголошення або отримання конфіденційної особистої та корпоративної інформації. За даними робочої групи з питань боротьби з фішингом (APWG) у першому кварталі 2020 р. загалом зареєстровано 165 772 окремих фішингових операції з використанням електронної пошти.[1] Фішингові атаки набувають дедалі складнішого характеру, внаслідок чого їх усе важче виявляти та попереджати.

Захист веб-браузерів проти фішингу

Захист проти фішингу реалізовано в програмі, вбудованій у веб-браузер, яка запитує репутацію URL-адреси в репутаційного сервера в хмарі. Цей репутаційний сервер виконує очищення Інтернету способом виявлення фішингових веб-сайтів, присвоєння їм оцінки та їхнього додавання до списку заблокованих веб-сайтів. У такий спосіб, коли веб-браузер отримує інструкцію відвідати URL-адресу, система захисту проти фішингу браузера (наприклад, «безпечний перегляд», SmartScreen тощо) запитує дані про репутацію цієї URL-адреси в хмарного репутаційного сервера. Якщо результати свідчать, що даний веб-сайт є «поганим», веб-браузер спрямовує користувача до повідомлення з попередженням, у якому роз'яснюється, що URL-адреса є зловмисною. Деякі системи визначення репутації також мають додатковий освітній вміст. Навпаки, якщо виявлено, що той або інший веб-сайт є «хорошим», веб-браузер не вживає будь-яких заходів, а користувачу навіть невідомо, що браузером щойно проводилася перевірка безпеки.

Із чого складалося тестування – фішингові URL-адреси

У цьому звіті наведено дані за період тестування, який тривав протягом 18 днів із 21 квітня 2020 р. до 8 травня 2020 р. Усі заходи з тестування виконувалися на об'єкті для проведення тестувань компанії NSS, розташованому в м. Остін, штат Техас. Під час тестування інженери NSS виконували постійний моніторинг підключення до мережі Інтернет задля забезпечення доступності для браузерів, що піддаються тестуванню, фішингових URL-адрес, а також репутаційних служб браузерів у хмарі.

Основна увага приділялася актуальності. Отже, оцінці піддавалася більша кількість веб-сайтів, ніж у кінцевому рахунку було збережено в якості набору результатів, тому що до тестування постійно додавалися нові URL-адреси, а мертві веб-сайти видалялися.

Загальна кількість зловмисних URL-адрес у тестуванні

Кожним веб-браузером багато разів тестувалася загальна кількість із 4020 непідтверджених URL-адрес, при цьому загальна кількість окремих тестів, які безперервно проводилися протягом 430 годин, склала 222 527 тестів (кожні шість годин упродовж 18 днів). Інженери NSS видалили зразки, які не відповідають критеріям перевірки, включно зі зразками, щодо яких було зареєстровано спроби проникнення (не входять до обсягу цього тестування). Зрештою до 189 096 окремих дійсних тестів фішингу було включено 2443 унікальних дійсних фішингових URL-адрес (47 274 на один веб-браузер), що забезпечувало похибку менше 2 відсотків (<2%) при рівні впевненості 95%.

Середня кількість зловмисних URL-адрес, що додаються щодня

В середньому до тестового набору щодня додавалися 136 нових підтверджених URL-адрес. У деякі дні ці цифри дещо відрізнялися внаслідок коливань рівнів злочинної активності.

Блокування фішингових URL-адрес

NSS оцінила спроможність браузерів блокувати зловмисні URL-адреси негайно після їхнього виявлення в Інтернеті. Інженери повторювали ці тести кожні шість годин задля виявлення часу, який потрібен постачальнику для організації захисту, якщо взагалі здійснювався будь-який захист.

Новий браузер Microsoft Edge, випущений 15 січня 2020 р., ґрунтується на браузері Chromium. Він є сумісним із усіма підтримуваними версіями Windows і macOS. Внаслідок завантаження цього браузера будуть замінені успадковані версії Microsoft Edge на ПК під керуванням Windows 10.

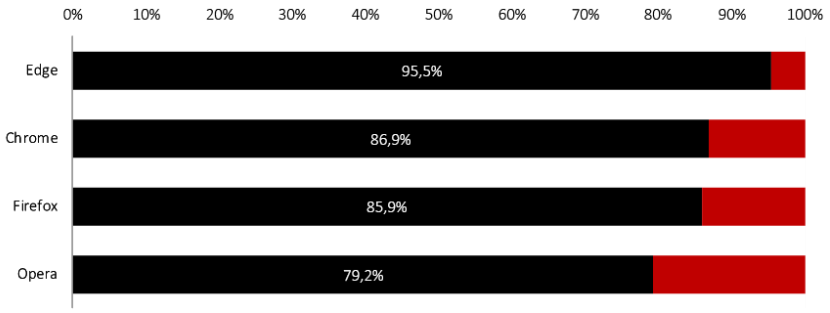
https://support.microsoft.com/uk-ua/help/4501095/download-the-new-microsoft-edge-based-on-chromium

[1] Звіт APWG про тенденції фішингової активності

Рівень блокування фішингових URL-адрес

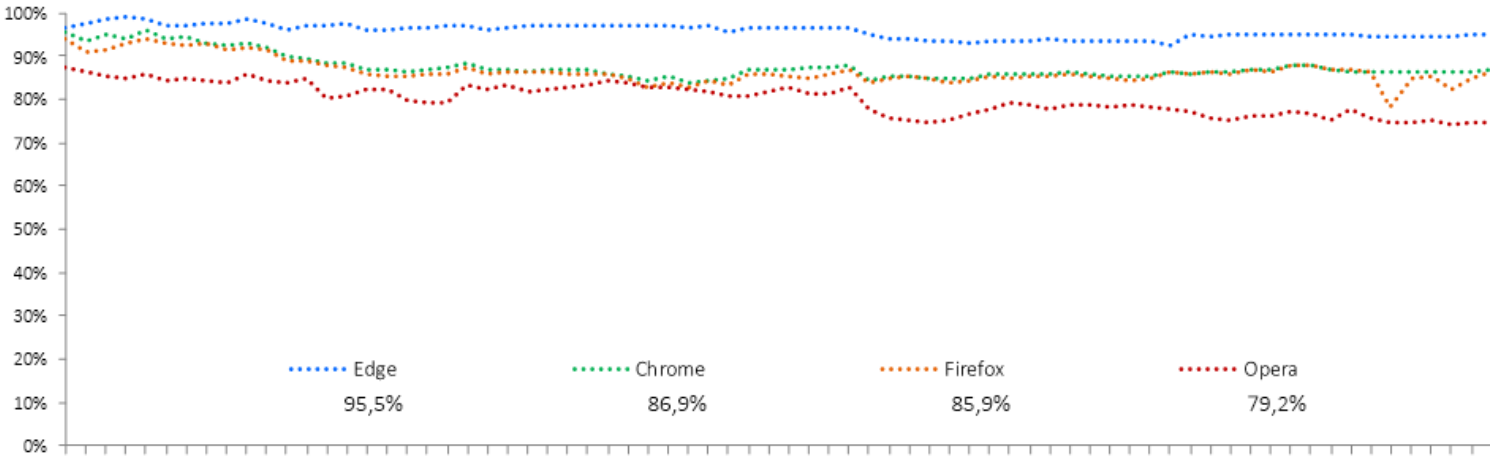
У Google Chrome і Mozilla Firefox застосовується API безпечного перегляду Google. Задля забезпечення захисту проти загроз фішингу та зловмисних програм у Microsoft Edge застосовується фільтр SmartScreen для захисника Windows, включно з репутаційною службою програм. У браузері Opera використано поєднання списку заблокованих веб-сайтів Netcraft,[2] PhishTank[3] і Metamask,[4] а також список заблокованого зловмисного програмного забезпечення служби Yandex.[5]

Спроможність попереджати потенційних жертв, що вони незабаром потраплять на зловмисний веб-сайт, є унікальною можливістю для цих веб-браузерів боротися з фішингом та іншою злочинною діяльністю. Оскільки фішингові веб-сайти живуть недовго, виявляти, підтверджувати, класифікувати та якомога швидше додавати до репутаційної системи такі веб-сайти конче важливо. Це пояснює співвідношення між середнім часом до блокування та показником виявлення. Задля досягнення високих показників виявлення надійна репутаційна система має бути як точною, так і швидкою. Розробники браузерів чітко розуміють це співвідношення, при цьому протягом перших 24 годин блокується значно більше фішингових веб-сайтів, ніж після закінчення цього періоду.



Індивідуальна продуктивність блокування кожного браузера постійно вимірювалася, при цьому реєструвався загальний рівень блокувань усіх URL-адрес, що тестувалися, за браузерами. Загальний рівень блокувань браузером обчислюється, як кількість успішних блокувань, розділена на загальну кількість тестів. Наприклад, коли тести проводяться кожні шість годин, URL-адреса, яка перебувала в Інтернеті протягом 48 годин, тестується вісім разів. Браузер, який блокує її в шести (з максимум восьми) сеансах тестування, досягає рівня блокування 75%.

Послідовність захисту в динаміці часу



Протягом тестування щодня додавалися нові фішингові URL-адреси, при цьому видалялися URL-адреси, які більше не були доступними або ефективними. Кожна точка даних представляє собою оцінку захисту, який забезпечується в конкретний момент часу. Якщо URL-адреса заблокована на початку атаки, оцінка послідовності захисту в динаміці часу, який забезпечується тим або іншим браузером, покращується. Натомість, якщо браузер не заблокував таку URL-адресу, оцінка погіршується.

[2] http://www.netcraft.com/

[3] http://www.phishtank.com/

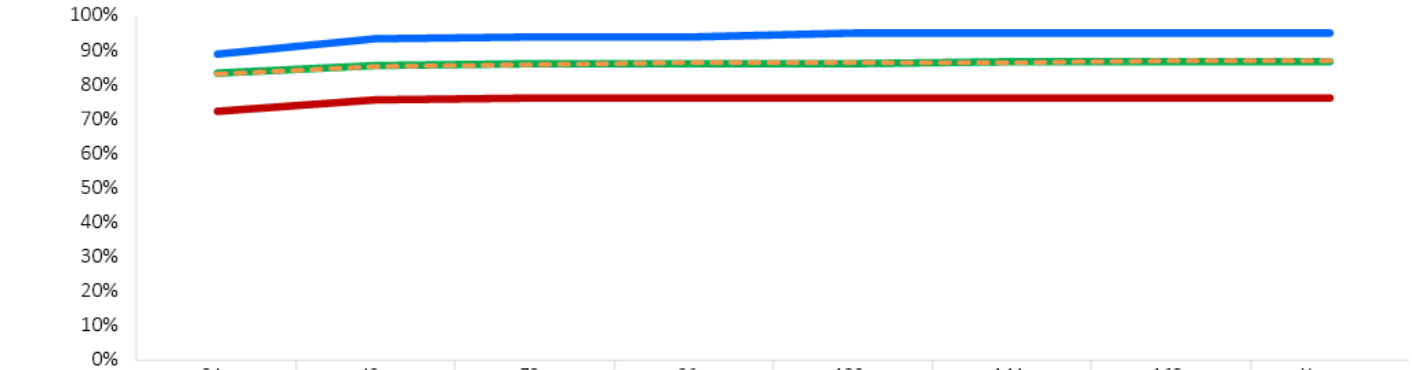
[4] https://github.com/metamask/eth-phishing-detect

[5] https://yandex.com

Зведена таблиця захисту від фішингу

Критичним є негайний захист проти нових фішингових URL-адрес. Тією мірою, якою виявляються фішингові веб-сайти, вони фіксуються. Часто це робиться впродовж відносно короткого часу. Продукти, які вчасно не додають захист, можуть запізнитися при подоланні загрози. У зведеній таблиці нижче показано, скільки часу знадобилося кожному браузеру для блокування фішингового веб-сайту після введення загрози в цикл тестування. Сукупні рівні захисту розраховуються щодня протягом семиденного періоду до моменту блокування загроз.

Під час тесту спочатку браузер Microsoft Edge забезпечував захист проти фішингових атак на рівні 89,2%. Google Chrome і Mozilla Firefox досягали початкових рівнів захисту 83,7% і 83,2% відповідно. Початковий рівень захисту Opera склав 72,2%. Станом на кінець сьомого дня тестування всі веб-браузери демонстрували підвищення рівня захисту. Підвищення у випадку браузера Microsoft Edge становило 5,7% і загалом склало 94,9%. Рівень захисту Mozilla Firefox підвищився на 3,7% і склав 86,9%, а рівень захисту Google Chrome підвищився на 3% до позначки 86,7%. Рівень захисту Opera підвищився на 4,1% і загалом склав 76.3%



	< 24 год.	< 48 год.	< 72 год.	< 96 год.	< 120 год.	< 144 год.	< 168 год.	Усього
Edge	89,2%	93,2%	93,7%	94,2%	94,8%	94,9%	94,9%	95,0%
Chrome	83,7%	85,8%	86,1%	86,4%	86,5%	86,7%	86,7%	86,7%
Firefox	83,2%	85,5%	86,0%	86,4%	86,5%	86,7%	86,9%	87,0%
Opera	72,2%	75,8%	76,3%	76,3%	76,3%	76,3%	76,3%	76,3%

Тестове середовище

- BaitNET™ (NSS Labs Proprietary)
- 64-bit Microsoft Windows 10 Pro (версія 1909 збірка: 18363.592)
- Ubuntu 18.04.3 LTS
- Kali (Kernel випуск 4.19.0-kali5-amd64)
- VMware vCenter (версія 6.7u2 збірка 6.7.0.30000)
- VMware vSphere (версія 6.7.0.20000)
- VMware ESXi (версія 6.7u3 збірка 14320388)
- VMware Tools 10.3.5
- Wireshark версія 2.6.3
- WinPcap 4.1.3
- Filezilla Server 0.9.6
- SSH Secure Shell 3.2.9 (збірка 283)
- GNU Wget 1.19.4
- Curl 7.58.0

Продукти, що тестувалися

- Google Chrome: Версія 81.0.4044.113 – 81.0.4044.138
- Microsoft Edge: Версія 83.0.478.10 – 84.0.502.0
- Mozilla Firefox: Версія 75.0 – 76.0.1
- Opera: Версія: 67.0.3575.137 – 68.0.3618.125

Розробники

Діпті Гіміре (Dipti Ghimire), Томас Скайбакмоен (Thomas Skybakmoen), Вікрам Фатак (Vikram Phatak)

Методика тестування

Методика тестування NSS Labs Web Browser Security (WBS) версії 4.0 доступна за адресою www.nsslabs.com.

Контактна інформація

NSS Labs, Inc.

3711 South Mopac Expressway
Building 1, Suite 400
Остін, Техас 78746

info@nsslabs.com

www.nsslabs.com