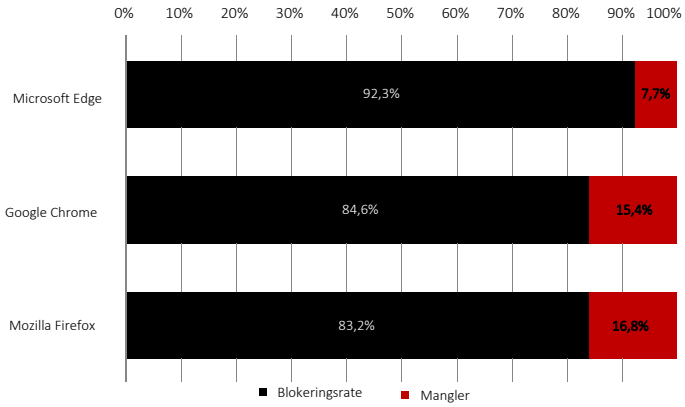
2. KVARTAL 2021 Webbrowsere vs. Phishing

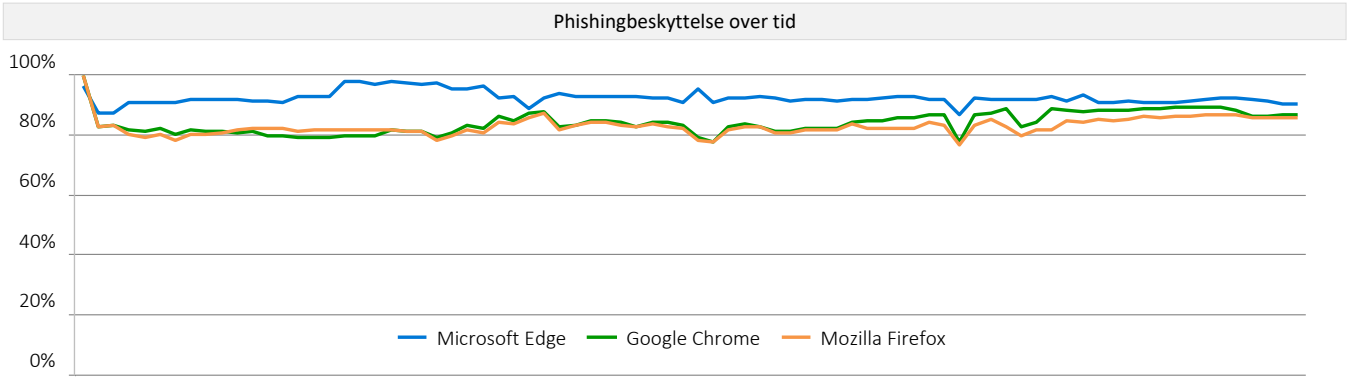
Oversigt

I løbet af 2. kvartal 2021 udførte CyberRatings.org en uvildig test af phishingbeskyttelse, som webbrowsere tilbyder. Testene kørte i 20 dage med 80 separate testkørsler. Som beskyttelse mod phishing bruger Microsoft Edge Microsoft Defender SmartScreen; Google Chrome og Mozilla Firefox bruger Google Safe Browsing API.
Microsoft Edge gav den bedste beskyttelse ved at blokere 92,3% af phishing-URL'er og havde samtidig den højeste zero-hour-beskyttelsesrate (93,5%). Google Chrome havde den næsthøjeste beskyttelse ved i gennemsnit at blokere 84,6%, efterfulgt af Mozilla Firefox med 83,2%.

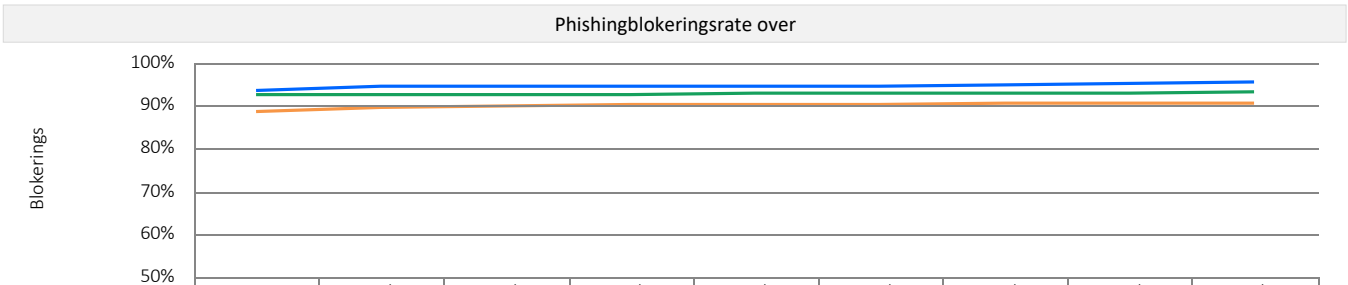


Oversigt over

URL-omdømmesystemer forkorter den tid, som angribere har til at opnå deres mål, ved at forhindre eller advare brugere om, at en URL er et kendt phishing-websted. Men eftersom brugere besøger mange forskellige websteder, hvoraf mange er nye, kan URL-omdømmesystemer ikke bare blokere alle nye URL'er. Med den viden ændres angribernes phishingkampagner konstant, og størstedelen af nye angreb opstår i de første få timer, efter et angreb er startet.



I løbet af testen blev der dagligt tilføjet nye phishing-URL'er, og URL'er, der ikke længere kunne kontaktes eller ikke længere leverede phishing-angreb, blev fjernet. Hvert datapunkt repræsenterer beskyttelse på et bestemt tidspunkt. Hvis en URL blev blokeret tidligt, blev browserens score for konsistent beskyttelse over tid forbedret. Hvis browseren derimod ikke blokerede URL'en, blev scoren dårligere.



	0 t.	1d	2d	3d	4d	5d	6d	7d	I alt
Microsoft Edge	93,5%	94,4%	94,5%	94,5%	94,5%	94,7%	94,9%	95,1%	95,4%
Google Chrome	92,4%	92,6%	92,7%	92,7%	92,8%	92,8%	92,8%	92,9%	93,2%
Mozilla Firefox	88,7%	89,7%	90,0%	90,4%	90,4%	90,4%	90,5%	90,6%	90,6%

Vi målte browsernes evne til at blokere skadelige URL'er lige så hurtigt, som vi fandt dem på internettet. Dette fortsatte hver 6. time for at afgøre, hvor længe det vil tage en leverandør at tilføje beskyttelse. Tallet nedenfor viser svartiden for hver browser om at blokere et phishingwebsted, da truslen blev introduceret i testcyklussen.

Phishing-angreb

Phishing er en type social engineering-angreb, der forsøger at narre et offer til at afgive følsomme personlige oplysninger til angriberen. Eksempler på følsomme oplysninger er kreditkortnumre, cpr-numre og login og adgangskoder til bankkonti. Mails, chatbeskeder, sms'er og link på sociale medier er alle vektorer for phishingangreb. Landingssiden for et phishingwebsted forsøger ofte at udnytte en besøgendes computer og installere skadelig software (også kaldet 'drive-by exploit').

Phishingangreb udgør en betydelig risiko for både private og organisationer, da de truer med at kompromittere eller erhverve følsomme personlige oplysninger og forretningsdata. Anti-Phishing Working Group (APWG) rapporterede i alt 396.688 unikke mailbaserede phishingkampagner i 4. kvartal af 2020.[1]

Webbrowseres beskyttelse mod phishing

Phishing-beskyttelse leveres af et program i en webbrowser, der anmoder om en URL's omdømme fra en cloudtjeneste, der har gransket internettet for at finde phishing-websteder og føjet dem til en blokeringsliste. Når en webbrowser så forsøger at besøge en URL, omdirigerer browserens phishing-beskyttelse (dvs. Safe Browsing, SmartScreen osv.) brugeren til en advarselsbesked, der forklarer, at URL'en er skadelig. Nogle omdømmesystemer har også ekstra uddannelsesindhold. Omvendt, hvis et websted er besluttet på at være "godt", gør webbrowseren ingenting.

Google og Firefox bruger Google Safe Browsing API for begge URL-omdømmer og for at advare brugere mod at downloade bestemte filtyper. Microsoft Edge bruger Microsoft Defender SmartScreen, som yder URL-baseret beskyttelse mod angreb via en integreret cloudbaseret URL-omdømmetjeneste samt programomdømme til blokering af skadelige filer.

Antal skadelige URL'er tilføjet dagligt i gennemsnit

I gennemsnit blev 50 nye, validerede URL'er føjes til testen per dag. Tallene varierede på nogle dage, hvis den kriminelle aktivitet var høj.

Samlet antal skadelige URL'er i testen

26.976 rå, uvaliderede URL'er blev testet flere gange med hver webbrowser. Der blev udført i alt 80 separate testcyklusser uden afbrydelse i 480 timer (hver 6. time i 20 dage). Vores teknikere fjernede prøver, der ikke bestod valideringskriterierne, inkl. dem, der er skadet af exploits (ikke del af denne test). I sidste ende blev 996 unikke, gyldige phishing-URL'er inkluderet i det endelige sæt af 61.605 separate, gyldige phishingtests (20.535 test per webbrowser), hvilket gav en fejlmargen på 3,1 procent (3,1%) med et konfidensniveau på 95%.

Testkomposition – phishing-URL'er

Data i denne rapport spænder over en testperiode på 20 dage mellem 11. maj og 31. maj 2021. Under testen overvågede vores teknikere rutinemæssigt forbindelsen for at sikre, at browserne under testen kunne tilgå phishing-URL'erne samt browseromdømmetjenester i clouden.

Der blev lagt vægt på friskheden med nye URL'er, der konstant blev føjet til testen, og døde websteder, der blev fjernet.

Sådan evaluerede vi resultaterne

Vi målte hver browsers evne til at blokere skadelige URL'er lige så hurtigt, som de blev fundet på internettet. Teknikerne gentog disse tests hver 6. time for at bestemme, hvor længe det tog en leverandør at tilføje beskyttelse, hvis de overhovedet gjorde det.

Hver browsers effektivitet blev målt kontinuerligt, og den overordnede blokeringsrate for alle URL'er, som browseren testede, blev registreret. Hver browsers overordnede blokeringsrate blev beregnet som antallet af vellykkede blokeringer delt med det samlede antal testsager. F.eks. med tests, der blev udført hver 6. time, blev en URL, der var online i 48 timer, testet 8 gange. En browser, der blokerer den på 6 (ud af maks. 8) testkørsler, opnåede en blokeringsrate på 75%.

Testmiljø

- Microsoft Windows 10 Pro, 21H1

Testede produkter

- Google Chrome: Version 90.0.4430.212 - 91.0.4472.19
- Microsoft Edge: Version: 91.0.864.19 - 91.0.864.37
- Mozilla Firefox: Version 88.0.1 - 88.0.1

1 APWG's rapport om trends inden for phishingaktivitet

Forfattere

Thomas Skybakmoen, Vikram Phatak

Testmetodik

CyberRatings Web Browser Security Test Methodology v1.0 er tilgængelig på www.cyberratings.org

Kontaktoplysninger

CyberRatings.org
2303 Ranch Road 620 South
Suite 160, #501
Austin, TX 78734

info@cyberratings.org
www.cyberratings.org