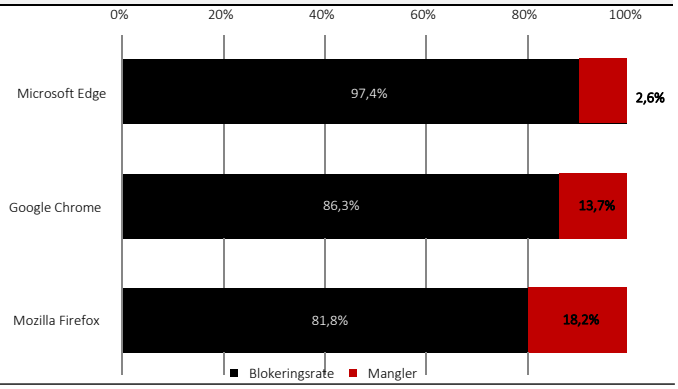
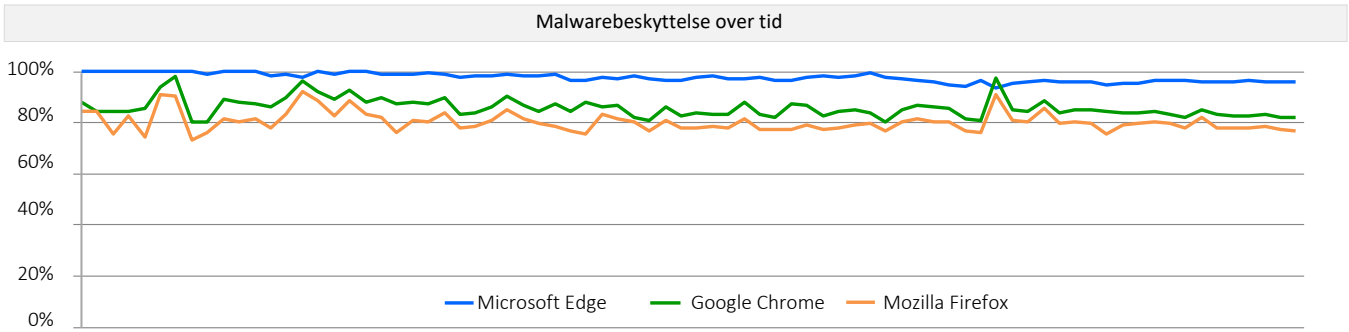
Q2 2021 Webbrowsere vs. Malware

Oversigt

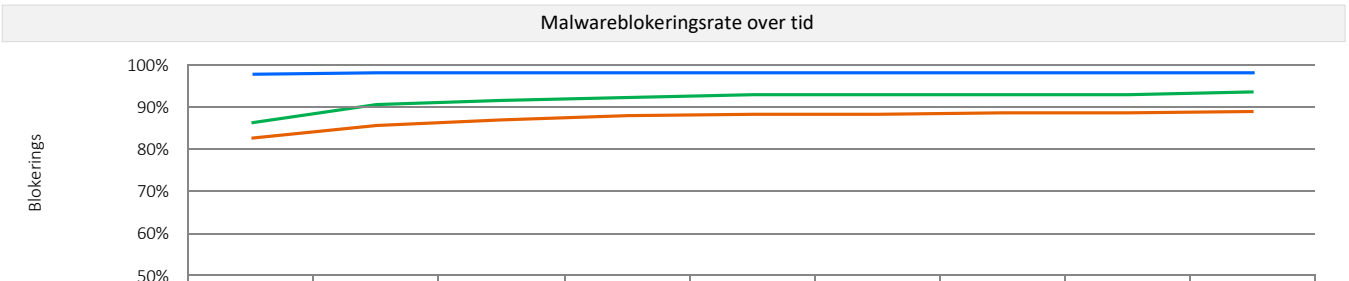
I løbet af 2. kvartal 2021 udførte CyberRatings.org en uvildig test af malwarebeskyttelse, som webbrowsere tilbyder. Testene kørte i 20 dage med 80 separate testkørsler. Som beskyttelse mod malware bruger Microsoft Edge Microsoft Defender SmartScreen; Google Chrome og Mozilla Firefox bruger Google Safe Browsing API. Microsoft Edge gav den bedste beskyttelse ved at blokere 97,4% af malware og havde samtidig den højeste zero-hour-beskyttelsesrate (97,7%). Google Chrome havde den næsthøjeste beskyttelse ved i gennemsnit at blokere 86,3%, efterfulgt af Mozilla Firefox med 81,8%.



Evnen til at advare potentielle ofre om, at de er på vej ind på et skadeligt websted, giver webbrowsere en unik mulighed for at bekæmpe malware. Websteder, der narrer (social engineer) brugere til at downloade malware, har korte levetider, så det er afgørende, at webstedet opdages og føjes til omdømmesystemet hurtigst muligt. Et godt omdømmesystem skal som sådan både være nøjagtigt og hurtigt for at realisere høje fangstrater.



I løbet af testen blev der hele tiden tilføjet ny malware. URL'er, der enten ikke længere kunne kontaktes, eller hosting-malware blev fjernet. Hvert datapunkt beregnes fra målinger, der foretages på et specifikt tidspunkt. Hvis malwaren blev blokeret tidligt, blev browserens score-beskyttelse over tid forbedret. Hvis browseren derimod ikke blokerede malwaren, blev scoren dårligere.



	0 t.	1d	2d	3d	4d	5d	6d	7d	I alt
Microsoft Edge	97,7%	97,9%	97,9%	97,9%	97,9%	97,9%	97,9%	97,9%	97,9%
Google Chrome	86,4%	90,6%	91,7%	92,5%	92,9%	93,1%	93,1%	93,1%	93,6%
Mozilla Firefox	82,8%	85,9%	87,1%	88,0%	88,3%	88,4%	88,6%	88,7%	89,1%

Oversigt over

Tallet ovenfor viser, hvor længe hver browser var om at blokere malware, da prøven blev introduceret i testcyklussen. Kernebeskyttelsesteknologien i Microsoft Edge er SmartScreen, som yder URL-baseret beskyttelse mod angreb via en integreret cloudbaseret URL-omdømmetjeneste samt programomdømme til blokering af skadelige filer. Google Chrome og Mozilla Firefox bruger Google Safe Browsing API for begge URL-omdømmer og for at blokere eller advare brugere mod at downloade bestemte filtyper.

Malware-angreb

Social engineered malware (SEM)-angreb bruger vildledelse til at narre brugere til at downloade malware: Hijackede mailkonti og konti til sociale medier udnytter den implicitte tillid mellem kontakter og narrer ofrene til at tro, at links til skadelige filer er pålidelige. Andre vildledelser inkluderer pop op-beskeder, der opfordrer brugere til at installere programmer (såsom Adobe Flash Player) eller advarer en bruger om, at dennes computer er inficeret, eller at den kræver en opdatering.

Når malwaren er installeret, er ofrene sårbare over for logintyveri, identitetstyveri, kompromitteret bankkonto osv.

Webbrowseres beskyttelse mod malware

For at beskytte mod malware gransker cloudbaserede omdømmesystemer internettet for skadelige websteder og kategoriserer derefter indholdet. Webbrowsere spørger derefter de cloudbaserede omdømmesystemer om specifikke URL'er, filer eller programmer. Hvis resultaterne indikerer, at der er malware til stede, omdirigerer webbrowseren brugeres til en advarselsbesked, der forklarer, at URL'en, filen eller programmet er skadeligt. Nogle omdømmesystemer har også ekstra uddannelsesindhold.

Google Chrome og Mozilla Firefox bruger Google Safe Browsing API til både URL-omdømme og programomdømme for at blokere skadelige filer. Microsoft Edge bruger Microsoft Defender SmartScreen, som yder beskyttelse mod angreb via en cloudbaseret URL-omdømmetjeneste samt programomdømme til blokering af skadelige filer.

Gennemsnit antal skadelige malwareprøver tilføjet dagligt

I gennemsnit blev 49 nye, validerede malwareprøver føjet til testen per dag. Tallene varierede på nogle dage, hvis den kriminelle aktivitet var høj eller lav.

Samlet antal skadelige prøver testet

18.621 rå, uvaliderede prøver blev testet flere gange med hver webbrowser. Der blev udført i alt 78 separate testcyklusser uden afbrydelse i 468 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 950 unikke, gyldige malwareprøver inkluderet i det endelige sæt af 48.672 separate, gyldige malwaretests (16.224 test per webbrowser), hvilket gav en fejlmargen på under 3,2 procent (< 3,2%) med et konfidensniveau på 95%.

Sådan testede vi – malwareprøver

Data i denne rapport spænder over en testperiode på 20 dage mellem 11. maj og 31. maj 2021. Under testen overvågede CyberRatings-teknikere rutinemæssigt forbindelsen for at sikre, at browserne under testen kunne tilgå malwaren samt omdømmetjenesterne i clouden.

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

Sådan evaluerede vi resultaterne

Vi målte hver browsers evne til at blokere malware lige så hurtigt, som den 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 malwareprøver, 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 malwareprøve, 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

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