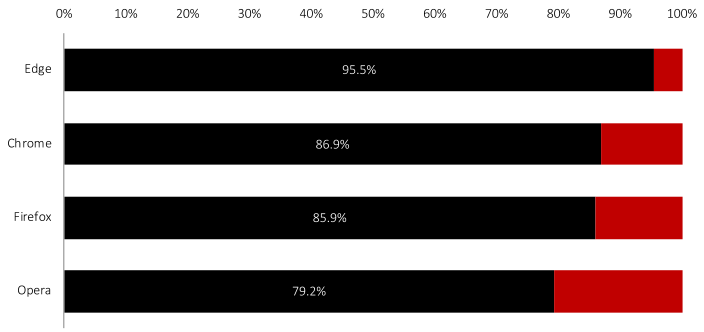
2. kvartal 2020 KOMPARATIV TESTRAPPORT

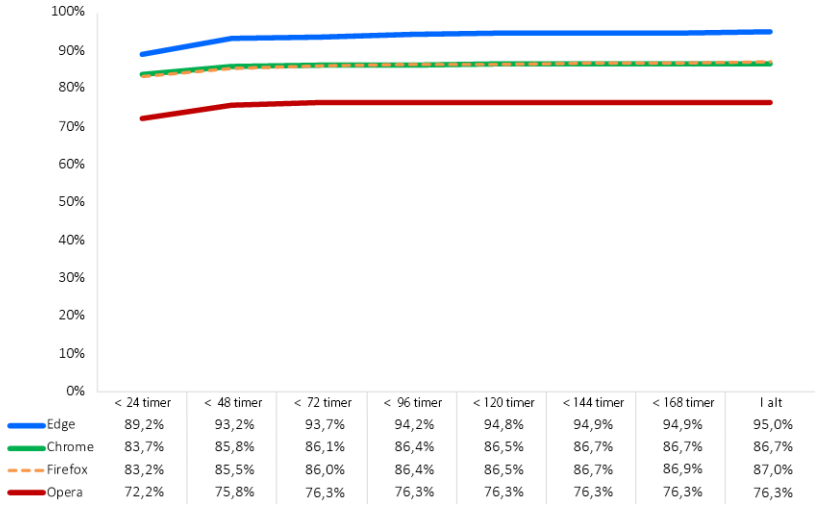
Oversigt

I løbet af 2. kvartal 2020 udførte NSS Labs en uvildig test af phishingbeskyttelse, som webbrowsere tilbyder: 47.274 separate tests (per webbrowser) ved hjælp af 2.443 unikke phishing-URL'er over 18 dage. Som beskyttelse mod phishing bruger Microsoft Edge Microsoft Defender SmartScreen; Google Chrome og Mozilla Firefox bruger Google Safe Browsing API; og Opera bruger en kombination af blokeringslister fra tredjepart.

Microsoft Edge gav den bedste beskyttelse ved at blokere 95,5% af phishing-URL'er og havde samtidig den højeste zero-hour-beskyttelsesrate (89,2%). Google Chrome havde den næsthøjeste beskyttelse ved i gennemsnit at blokere 86,9%, efterfulgt af Mozilla Firefox med 85,9%. Opera blokerede 79,2%.



Oversigt over resultater

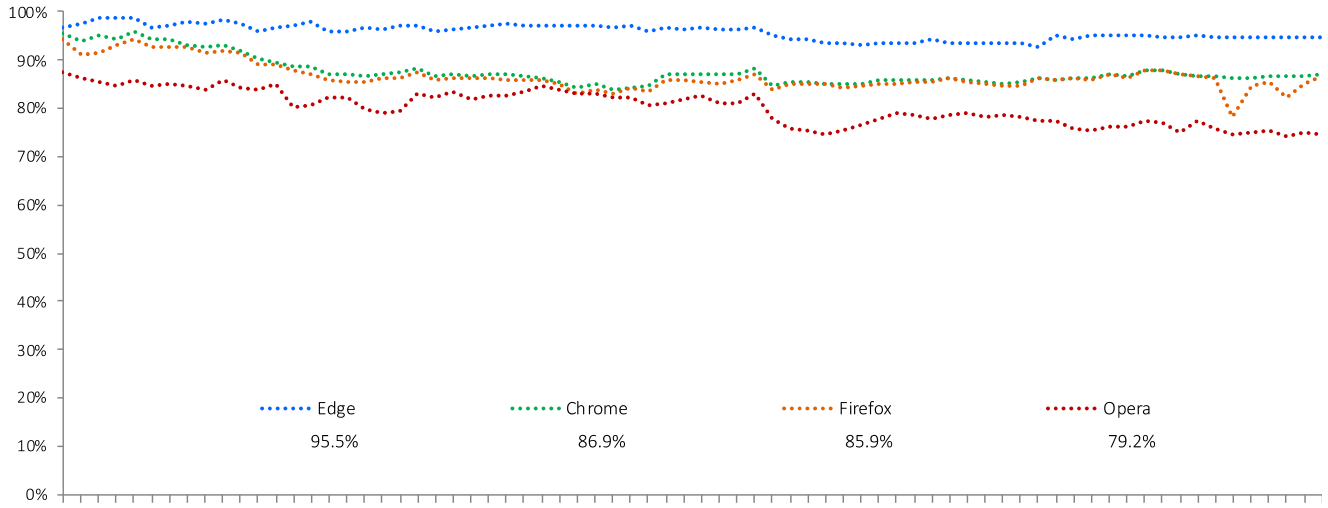


	< 24 timer	< 48 timer	< 72 timer	< 96 timer	< 120 timer	< 144 timer	< 168 timer	I alt
Edge	89,2%	93,2%	93,7%	94,2%	94,8%	94,9%	94,9%	95,0%
Chrome	83,7%	85,8%	86,1%	86,4%	86,5%	86,7%	86,7%	86,7%
Firefox	83,2%	85,5%	86,0%	86,4%	86,5%	86,7%	86,9%	87,0%
Opera	72,2%	75,8%	76,3%	76,3%	76,3%	76,3%	76,3%	76,3%

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.

NSS Labs evaluerede browsernes evne til at blokere skadelige URL'er lige så hurtigt, som vi fandt dem på internettet. Vi fortsatte med at teste dem hver 6. time for at bestemme, hvor længe det tog en leverandør at tilføje beskyttelse, hvis de overhovedet gjorde det.

Phishingbeskyttelse over tid



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.

Testen var baseret på Web Browser Test Methodology v4.0 (findes på www.nsslabs.com).

Denne rapport er fortrolig og er udtrykkeligt begrænset til NSS Labs' licenserede kunder.

Baggrund

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 loginoplysninger og adgangskoder til bankkonti. Mails, chatbeskeder, sms'er og link på sociale medier er alle vektorer for phishingangreb. Landingssiden for et phishingwebsted forsøger også ofte at udnytte en besøgendes computer og installere en 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 165.772 unikke mailbaserede phishingkampagner i 1. kvartal af 2020.[1] Phishingangreb bliver mere og mere komplekse og sofistikerede, hvilket gør dem sværere at detektere og vanskeligere at forhindre.

Webbrowseres beskyttelse mod phishing

Phishingbeskyttelse foretages af et program i webbrowseren, der anmoder om en URL's omdømme fra en omdømmeserver i clouden. Omdømmeserveren finkæmmer internettet for at finde phishingwebsteder og tildeler derefter hver URL en score og føjer den til en blokeringsliste. Når en webbrowser så instrueres til at besøge en URL, anmoder browserens phishingbeskyttelse (f.eks. Safe Browsing, SmartScreen osv.) om URL'ens omdømme fra den cloudbaserede omdømmeserver. Hvis resultaterne så indikerer, at et websted er "dårligt", omdirigerer webbrowseren brugeren til en advarselsbesked om, at URL'en er skadelig. Nogle omdømmesystemer har også ekstra uddannelsesindhold. Og omvendt, hvis et websted vurderes som "godt", gør browseren ikke noget, og brugeren forbliver uvidende om, at browseren netop udførte et sikkerhedstjek.

Testkomposition – phishing-URL'er

Data i denne rapport spænder over en testperiode på 18 dage mellem 21. april 2020 og 8. maj 2020. Hele testen blev udført i NSS-testcentret i Austin, Texas. Under testen overvågede NSS-teknikere rutinemæssigt forbindelsen for at sikre, at browserne under testen kunne tilgå phishing-URL'erne samt browseromdømmetjenester i clouden.

Fokus var på friskhed, og dermed blev et stort antal websteder evalueret, end der slutligt blev bevaret som del af resultattestsættet, eftersom nye URL'er konstant blev føjet til testen, og døde websteder blev fjernet.

Samlet antal skadelige URL'er i testen

I alt 4.020 rå, uvaliderede URL'er blev testet flere gange med hver webbrowser. Der blev udført i alt 222.527 separate tests uden afbrydelse i 430 timer (hver 6. time i 18 dage). NSS-teknikere fjernede prøver, der ikke bestod valideringskriterierne, inkl. dem, der er skadet af exploits (ikke del af denne test). I sidste ende blev 2.443 unikke, gyldige phishing-URL'er inkluderet i 189.096 separate, gyldige phishingtests (47.274 per webbrowser), hvilket gav en fejlmargen på under 2 procent (<2%) med et konfidensniveau på 95%.

Antal skadelige URL'er tilføjet dagligt i gennemsnit

I gennemsnit blev 136 nye, validerede URL'er føjes til testen per dag. Tallene varierede på nogle dage, hvis den kriminelle aktivitet var høj.

Blokering af phishing-URL'er

NSS evaluerede browsernes 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.

Den nye Microsoft Edge er baseret på Chromium og blev udgivet 15. januar 2020. Den er kompatibel med alle understøttede versioner af Windows og macOS. Ved at downloade browseren erstattes den ældre version af Microsoft Edge på Windows 10-pc'er.

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

[1] APWG's rapport om trends inden for phishingaktivitet

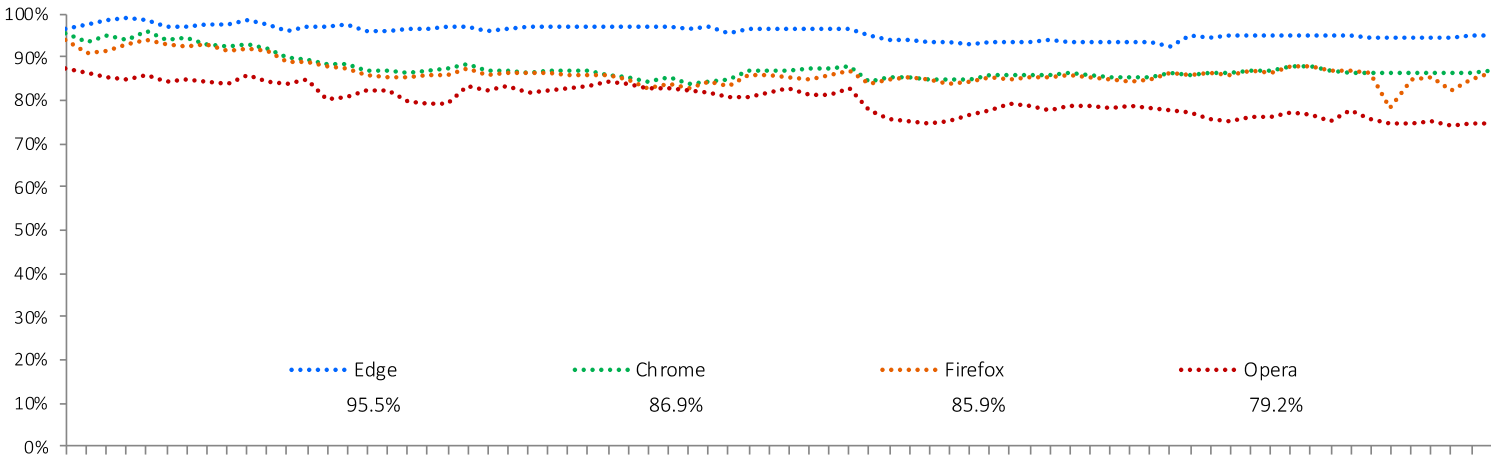
Phishingblokeringsrate

Google Chrome og Mozilla Firefox bruger Googles Safe Browsing API. Microsoft Edge bruger Microsoft Defender SmartScreen, inkl. programomdømmetjenesten, for at yde beskyttelse mod phishing og malwaretrusler. Opera bruger en kombination af blokeringslister fra Netcraft,[2] PhishTank[3] og Metamask[4] samt en malware-blokeringsliste fra Yandex.[5] 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 phishing og andre kriminelle aktiviteter. Eftersom phishingwebsteder ikke lever længe, er det afgørende, at webstedet opdages, valideres, klassificeres og føjes til omdømmesystemet så hurtigt som muligt. Dette forklarer sammenhængen mellem den gennemsnitlige blokeringstid og fangstraten. Et godt omdømmesystem skal både være nøjagtigt og hurtigt for at realisere høje fangstrater. Browserudviklere forstår tydeligt denne relation, og betydeligt flere phishingwebsteder blokeres i de første 24 timer af detekteringen end efterfølgende.



Hver browsers individuelle blokeringseffektivitet blev målt kontinuerligt, og den overordnede blokeringsrate for alle URL'er, som browserne testede, blev registreret. En browsers overordnede blokeringsrate beregnes 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, vil have en blokeringsrate på 75%.

Konsistent beskyttelse over tid



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-URL'er, 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.

Histogram for phishingbeskyttelse

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

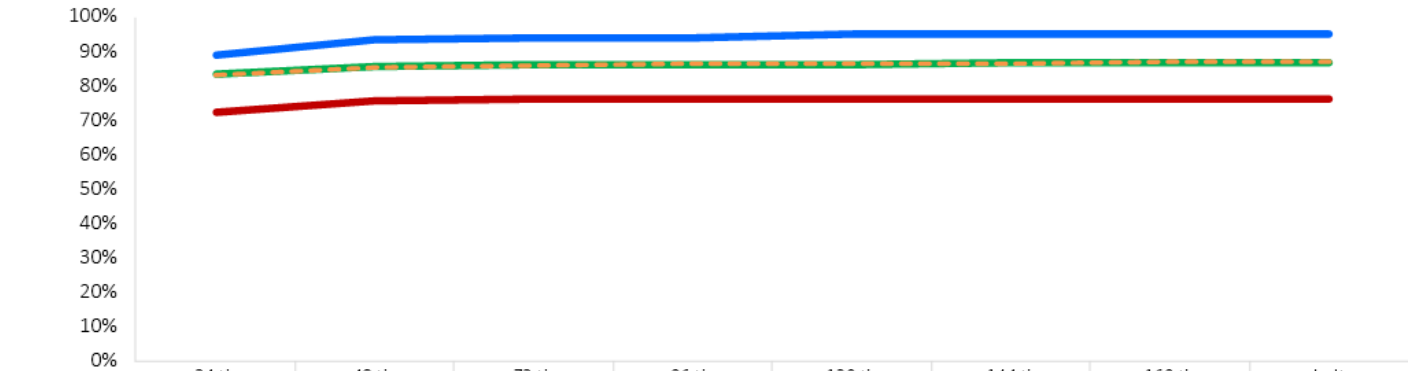
[3] http://www.phishtank.com/

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

[5] https://yandex.com

Direkte beskyttelse mod nye phishing-URL'er er kritisk. Idet phishingwebsteder opdages, lukkes de og ofte inden for relativt kort tid. Produkter, der ikke formår at tilføje beskyttelse i tide, er muligvis for længe om at bekæmpe en trussel. Histogrammet nedenfor viser, hvor længe hver browser var om at blokere et phishingwebsted, da truslen blev introduceret i testcyklussen. Inden for 7 dage beregnes kumulative beskyttelsesrater hver dag, indtil trusler blokeres.

Under testen demonstrerede Microsoft Edge en indledende beskyttelsesrate på 89,2% mod phishingangreb. Google Chrome og Mozilla Firefox opnåede en indledende beskyttelsesrate på henholdsvis 83,7% og 83,2%. Operas indledende beskyttelsesrate var 72,2%. Inden udgangen af den 7. dag med test oplevede alle webbrowsere en stigning i beskyttelsen. Microsoft Edge steg med 5,7% til 94,9%. Mozilla Firefox steg med 3,7% til 86,9%; Google Chrome steg med 3% til 86,7%. Opera steg med 4,1% til 76,3%



	< 24 timer	< 48 timer	< 72 timer	< 96 timer	< 120 timer	< 144 timer	< 168 timer	I alt
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%

Testmiljø

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

Testede produkter

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

Forfattere

Dipti Ghimire, Thomas Skybakmoen, Vikram Phatak

Testmetodik

NSS Labs Web Browser Security (WBS) Test Methodology v4.0 findes på www.nsslabs.com.

Kontaktoplysninger

NSS Labs, Inc.

3711 South Mopac Expressway
Building 1, Suite 400
Austin, TX 78746

info@nsslabs.com

www.nsslabs.com

Dette og andre relaterede dokumenter findes på: www.nsslabs.com. For at modtage en licenseret kopi eller rapportere misbrug skal du kontakte NSS Labs.

© 2020 NSS Labs, Inc. Alle rettigheder forbeholdes. Ingen del af denne publikation må gengives, kopieres/scannes, gemmes på et søgesystem, mailes eller på anden måde udbredes eller sendes uden udtrykkelig skriftlig godkendelse fra NSS Labs, Inc. ("os" eller "vi").

Læs ansvarsfraskrivelsen i dette felt, fordi den indeholder vigtige oplysninger, der binder dig. Hvis du ikke accepterer disse betingelser, bør du ikke læse resten af denne rapport, men bør i stedet straks returnere rapporten til os. "Du" eller "din" betyder den person, der tilgår denne rapport, og enhver entitet, på hvis vegne han/hun skaffede denne rapport.

1. Oplysningerne i denne rapport kan ændres af os uden varsel, og vi afviser enhver forpligtelse til at opdatere dem.

2. Oplysningerne i denne rapport er ifølge os nøjagtige og pålidelige på udgivelsestidspunktet, men det er ikke garanteret. Al brug af og tillid til denne rapport sker på eget ansvar. Vi er ikke ansvarlige for nogen skader, tab eller udgifter af nogen art, der opstår som følge af en fejl eller udeladelse i denne rapport.

3. VI STILLER INGEN GARANTI, HVERKEN UDTRYKKELIGT ELLER UNDERFORSTÅET. ALLE UNDERFORSTÅEDE GARANTIER, INKL. UNDERFORSTÅEDE GARANTIER AF SALGBARHED, EGNETHED TIL ET BESTEMT FORMÅL OG IKKE-KRÆNKELSE, AFVISES OG UDELUKKES HERMED AF OS. VI ER UNDER INGEN OMSTÆNDIGHED ANSVARLIGE FOR DIREKTE, FØLGEMÆSSIGE, HÆNDELIGE, PØNALE, EKSEMPLARISKE ELLER INDIREKTE SKADER ELLER FOR TAB AF PROFIT, INDTJENING, DATA, COMPUTERPROGRAMMER ELLER ANDRE AKTIVER, SELV HVIS VI ER BLEVET UNDERRETTET OM MULIGHEDEN HERFOR.

4. Denne rapport udgør ikke en godkendelse, anbefaling eller garanti af nogen af produkterne (hardware eller software), der er testet, eller den hardware og/eller software, der blev brugt til at teste produkterne. Testen garanterer ikke, at der ikke er fejl eller defekter i produkterne, eller at produkterne vil opfylde dine forventninger, krav, behov eller specifikationer, eller at de vil fungere uden afbrydelse.

5. Denne rapport udgår ikke nogen godkendelse, sponsorat, tilhørsforhold eller bekræftelse af eller med nogen organisationer, der nævnes i rapporten.

6. Alle varemærker, servicemærker og varenavne, der anvendes i denne rapport, er varemærker, servicemærker eller varenavne tilhørende deres respektive ejere.