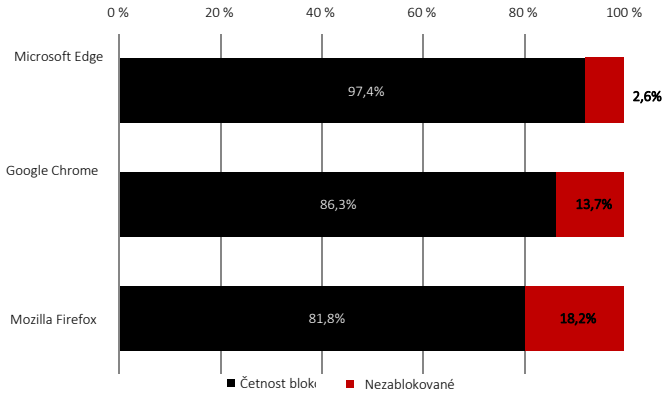
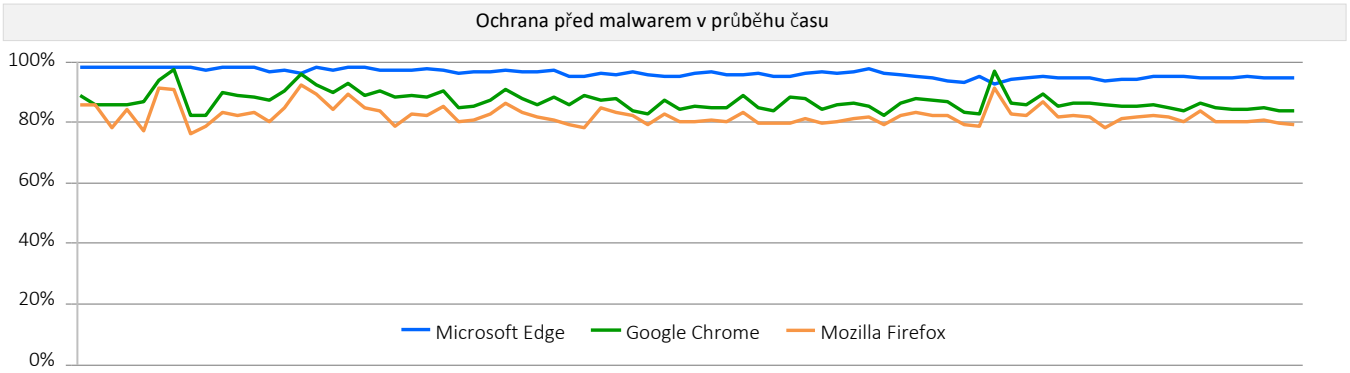
Q2 2021 Webové prohlížeče vs. malware

Přehled

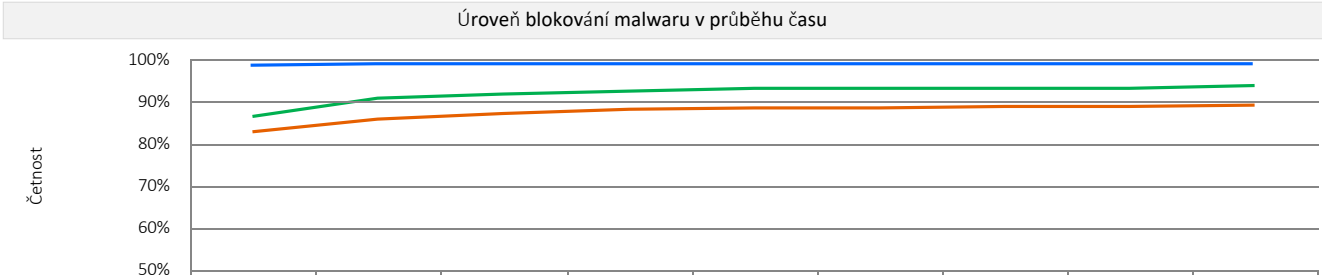
Během 2. čtvrtletí 2021 provedla společnost CyberRatings.org nezávislý test ochran před malwarem nabízených webovými prohlížeči. Testy probíhaly po dobu 20 dní a zahrnovaly 80 diskrétních zkoušek. K ochraně proti malwaru využívá Microsoft Edge nástroj Microsoft Defender SmartScreen; Google Chrome a Mozilla Firefox využívají Google Safe Browsing API. Microsoft Edge nabízel nejlepší ochranu a zablokoval 97,4 % malwaru a zároveň zajistil nejvyšší úroveň ochrany typu zero-hour (97,7 %). Google Chrome zajistil druhou nejvyšší ochranu a zablokoval v průměru 86,3 %, následovaný prohlížečem Mozilla Firefox s hodnotou 81,8 %.



Schopnost varovat případné oběti, že se chystají otevřít škodlivou webovou stránku poskytuje webovým prohlížečům jedinečnou pozici v boji s malwarem. Webové stránky, které podvodem navádí (pomocí sociálního inženýrství) uživatele ke stažení malwaru mají krátkou životnost, takže je klíčové, aby byla daná stránka objevena a přidána do systémů hodnocení pověsti co nejrychleji. Proto musí být dobrý systém hodnocení pověsti přesný i rychlý, aby zajistil vysoké úrovně záchytu.



V průběhu testu byl neustále přidáván nový malware. Adresy URL, které již nebyly dostupné nebo obsahovaly malware byly odebrány. Každý datový bod byl vypočítán z měření uložených v konkrétním bodě v čase. Pokud byl malware včas zablokován, hodnocení ochrany prohlížeče se v průběhu času zlepšilo. Alternativně, pokud prohlížeč malware nezablokoval, hodnocení se zhoršilo.



	0 h	1d	2d	3d	4d	5d	6d	7d	Celkem
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%

Shrnutí výsledků

Obrázek výše ukazuje, jak dlouho trvalo každému prohlížeči zablokování malware po zavedení vzorku do testovacího cyklu. Klíčovou technologií ochrany v prohlížeči Microsoft Edge je SmartScreen, která zajišťuje ochranu před útoky na základě adres URL prostřednictvím integrované, cloudové služby hodnocení pověsti adres URL a také hodnocení pověsti aplikací týkající se blokování škodlivých souborů. Google Chrome a Mozilla Firefox využívají rozhraní Google Safe Browsing API pro hodnocení pověsti adres URL i blokování nebo varování uživatelů před stahováním některých typů souborů.

© 2021 CyberRatings.org. Všechna práva vyhrazena.

Útoky malwaru

Útoky malwaru se sociálním inženýrstvím (SEM) využívají podvody k oklamání uživatelů a stažení malwaru: Uloupené e-mailové účty a účty na sociálních médiích využívají výhod implicitní důvěry mezi kontakty a vyvolávají u obětí nezaslouženou důvěru, že odkazy na škodlivé soubory jsou důvěryhodné. Další klamy zahrnují vyskakovací zprávy doporučující uživatelům, že je třeba nainstalovat aplikace (například Adobe Flash Player) nebo varují, že počítač uživatele je nakažen nebo že vyžaduje aktualizaci.

Po instalaci malwaru jsou oběti zranitelné vůči krádeži přihlašovacích údajů, krádeži identity, narušení bezpečnostní bankovního účtu apod.

Ochrana webových prohlížečů proti malwaru

K ochraně proti malwaru hledají cloudové hodnotící systémy na Internetu škodlivé webové stránky a pak příslušným způsobem vytváří kategorie obsahu. Webové prohlížeče se následně ptají cloudových hodnotících systémů na konkrétní adresy URL, soubory nebo aplikace. Pokud výsledky naznačují, že je přítomen malware, webový prohlížeč přesměruje uživatele na výstražnou zprávu vysvětlující, že adresa URL, soubor nebo aplikace jsou škodlivé. Některé systémy hodnocení také zahrnují dodatečný vzdělávací obsah.

Google Chrome a Mozilla Firefox využívají rozhraní Google Safe Browsing API pro hodnocení adres URL a hodnocení aplikací k blokování škodlivých souborů. Microsoft Edge využívá nástroj Microsoft Defender SmartScreen, který zajišťuje ochranu před útoky prostřednictvím cloudových služeb hodnocení týkající se adres URL a také hodnocení aplikací týkající se blokování škodlivých souborů.

Průměrný počet denně přidávaných vzorků škodlivého malwaru

V průměru bylo do testovací sady denně přidáváno 49 nových ověřených vzorků malwaru. Čísla se v některých dnech liší, jelikož úrovně škodlivé činnosti kolísaly.

Celkový počet otestovaných škodlivých vzorků

18 621 hrubých, neověřených vzorků bylo několikrát otestováno z každého prohlížeče v průběhu celkem 78 zkušebních cyklů, prováděných bez přerušení v průběhu 468 hodin (každých 6 hodin po dobu 20 dní). Naši inženýři odebrali vzorky, které nesplnili kritéria ověřování, včetně těch zkreslených exploity (nejsou součástí tohoto testu). Nakonec bylo do konečné sady 48 672 diskrétních, platných testů malwaru (16 224 testů na webový prohlížeč) přidáno 950 jedinečných, platných vzorků malwaru, což zajistilo chybovost menší než 3,2 procenta (< 3,2 %) v intervalu jistoty 95 %.

Jak jsme testovali – vzorky malwaru

Data v této zprávě zahrnují období testování v délce dvaceti (20) dnů od 11. května po 31. května 2021. Během testu inženýři CyberRatings rutinně monitorovali konektivitu, aby zajistili, že testované prohlížeče měly přístup k malwaru i službám hodnocení v cloudu.

Důraz jsme kladli na aktuálnost s neustále přidávanými novými vzorky do testu a odstraňovanými starými vzorky.

Jak jsme hodnotili výsledky

Změřili jsme schopnost každého prohlížeče blokovat malware stejně rychle, jako se objevují na internetu. Inženýři opakovali tyto testy každých šest hodin, aby určili, jak dlouho bude dodavateli trvat přidání ochrany, pokud vůbec.

Výkon každého prohlížeče byl měřen nepřetržitě a byla uložena celková úroveň blokování všech testovaných vzorků malwaru v prohlížeči. Celková úroveň blokování všech prohlížečů byla vypočtena jako počet úspěšných bloků podělená celkovým počtem testovacích případů. Například u testů prováděných každých 6 hodin, byl vzorek malwaru, který byl online po dobu 48 hodin, testován osmkrát (8). Prohlížeč, který jej zablokoval v 6 (z maximálně 8) zkoušek dosáhl úrovně blokování 75 %.

Zkušební prostředí

- Microsoft Windows 10 Pro, 21H1

Testované produkty

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

© 2021 CyberRatings.org. Všechna práva

Autoři

Thomas Skybakmoen, Vikram Phatak

Metodologie testu

Metodologie testu zabezpečení webového prohlížeče společnosti CyberRatings v1.0 je dostupná na webu www.cyberratings.org

Kontaktní informace

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

info@cyberratings.org
www.cyberratings.org

© 2021 CyberRatings.org. Všechna práva vyhrazena. Žádná část této publikace nesmí být reprodukována, kopírována/skenována, ukládána na úložný systém, zasílána e-mailem nebo jinak šířena nebo přenášena bez výslovného písemného souhlasu společnosti CyberRatings.org. („nás“ nebo „my“).

1. Údaje v této zprávě můžeme kdykoliv změnit bez upozornění a zříkáme se jakékoliv povinnosti je aktualizovat.

2. Informace v této zprávě jsou námi považovány za přesné a spolehlivé v okamžik publikace, ale nejsou zaručeny. Veškeré využívání a spoléhání na tuto zprávu je na vaše výhradní riziko. Nejsme zodpovědní za jakékoliv škody, ztráty nebo výdaje jakéhokoliv druhu vyplývající z jakýchkoliv chyb nebo opomenutí v této zprávě.

3. NEPOSKYTUJEME ŽÁDNÉ ZÁRUKY, VYJÁDŘENÉ NEBO PŘEDPOKLÁDANÉ. VŠECHNY PŘEDPOKLÁDANÉ ZÁRUKY, VČETNĚ PŘEDPOKLÁDANÝCH ZÁRUK OBCHODOVATELNOSTI, VHODNOSTI PRO DANÝ ÚČEL A NEPORUŠOVÁNÍ PRÁV JSOU TÍMTO ODMÍTNUTY VYLOUČENY. V ŽÁDNÉM PŘÍPADĚ NEBUDEME ODPOVĚDNÍ ZA JAKÉKOLIV PŘÍMÉ, NÁSLEDNÉ, NÁHODNÉ, TRESTNÍ, VZOROVÉ NEBO NEPŘÍMÉ ŠKODY NEBO JAKÉKOLIV ZTRÁTY ZISKU, OBRATU, DAT, POČÍTAČOVÝCH PROGRAMŮ NEBO DALŠÍCH PROSTŘEDKŮ, I KDYŽ JSME BYLI NA TAKOVOU MOŽNOST UPOZORNĚNI.

4. Tato zpráva nepředstavuje doporučení, podporu nebo záruku žádných testovaných produktů (hardwaru nebo softwaru) nebo hardwaru a/nebo softwaru používaného při testování produktů. Testování nezaručuje, že v produktech nejsou žádné chyby nebo vady nebo že produkty splní vaše očekávání, požadavky, potřeby nebo specifikace nebo že budou pracovat bez přerušení.

5. Tato zpráva nepředpokládá jakoukoliv podporu, sponzorství, vztah nebo ověřování prostřednictvím nebo u společností uváděných v této zprávě.

6. Všechny ochranné známky, známky služby a obchodní názvy používané v této zprávě jsou ochranné známky, známky služeb a obchodní názvy příslušných vlastníků.