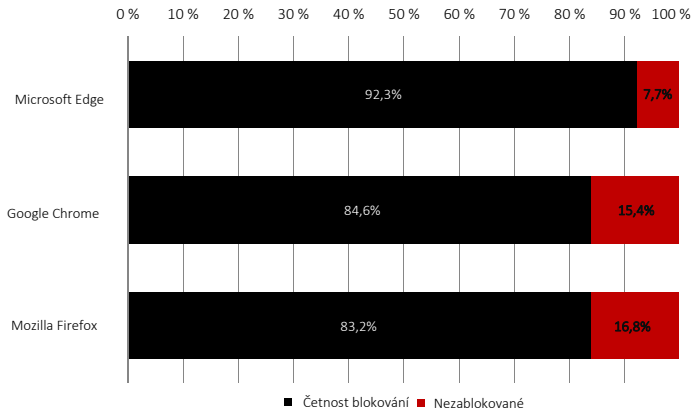
Q2 2021 Webové prohlížeče vs. phishing

Přehled

Během 2. čtvrtletí 2021 provedla společnost CyberRatings.org nezávislý test ochran před phishingem nabízených webovými prohlížeči. Testy probíhaly po dobu 20 dní a zahrnovaly 80 diskrétních zkoušek. K ochraně proti phishingu využívá Microsoft Edge nástroj Microsoft Defender SmartScreen; Google Chrome a Mozilla Firefox využívají Google Safe Browsing API.

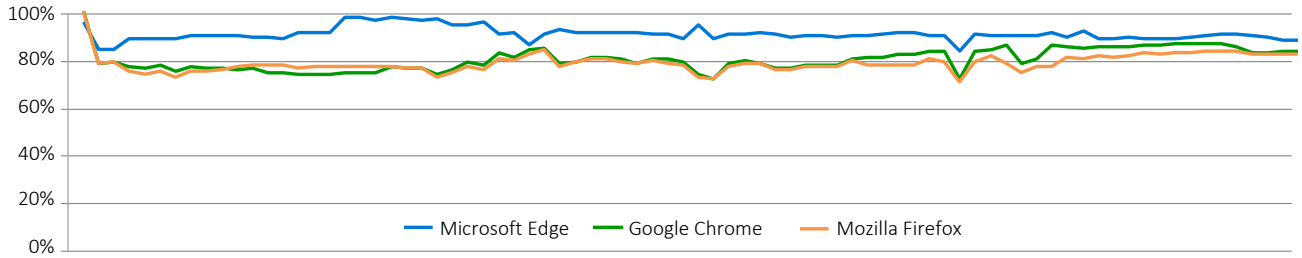
Microsoft Edge nabízel nejlepší ochranu a zablokoval 92,3 % phishingových adres URL a zároveň zajistil nejvyšší úroveň ochrany typu zero-hour (93,5 %). Google Chrome zajistil druhou nejvyšší ochranu a zablokoval v průměru 84,6 %, následovaný prohlížečem Mozilla Firefox s hodnotou 83,2 %.



Shrnutí výsledků

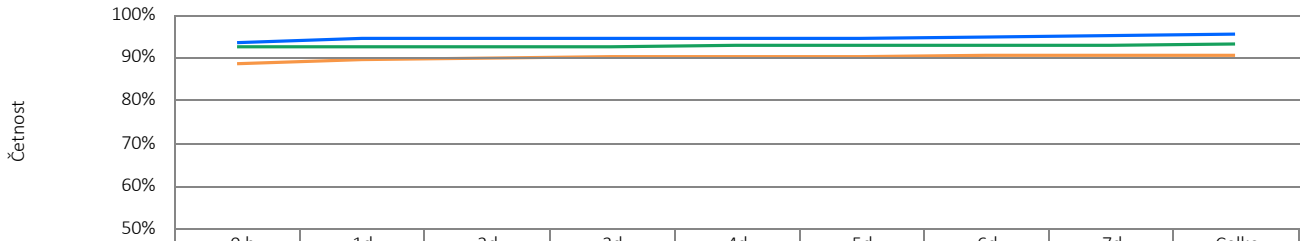
Systémy hodnocení adres URL zkracují čas, za který musí útočníci dosáhnout svých cílů, zabráněním/varováním uživatelů, že adresa URL je známou phishingovou stránkou. Jelikož však uživatelé navštěvují širokou řadu webových stránek, mnoho z nichž je nových, systémy hodnocení adres URL nemohou jednoduše blokovat všechny nové adresy URL. V tímto vědomím se phishingové kampaně útočníků neustále mění s většinou nových útoků nastávajících během prvních pár hodin po spuštění útoku.

Ochrana před phishingem v průběhu času



V průběhu testu byly nové phishingové adresy URL přidávány každý den a adresy URL, které již nebyly dosažitelné nebo již neprodukovaly phishingové útoky, byly odebrány. Každý datový bod představuje ochranu v konkrétním bodě v čase. Pokud byla adresa URL brzy zablokována, hodnocení konzistence ochrany prohlížeče se v průběhu času zlepšilo. Alternativně, pokud prohlížeč adresu URL nezablokoval, hodnocení se zhoršilo.

Úroveň blokování phishingu v průběhu času



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

Změřili jsme schopnost prohlížečů blokovat škodlivé adresy URL stejně rychle, jako je objevujeme na internetu. To pokračovalo každých šest hodin, abychom určili, jak dlouho bude dodavateli trvat přidání ochrany. Obrázek výše ukazuje dobu odezvy každého prohlížeče k zablokování phishingové stránky po zavedení hrozby do testovacího cyklu.

Phishingové útoky

Phishing představuje typ útoku se sociálním inženýrstvím, který se pokouší přesvědčit oběť, aby poskytla citlivé osobní údaje útočníkovi. Do příkladů citlivých informací patří čísla kreditních karet, čísla sociálního zabezpečení a přihlášení a hesla bankovních účtů. E-mailové, okamžité zprávy, SMS zprávy a odkazy na stránky sociálních sítí, to jsou všechno vektory phishingových útoků. Výchozí stránka phishingové webové stránky se často pokouší tiše využít počítač návštěvníka a nainstalovat škodlivý software (tzv. exploit náhodného kolemjdoucího).

Phishingové útoky představuje značné riziko pro osoby a organizace a hrozí narušením nebo získáním citlivých osobních a podnikových údajů. Antiphishingová pracovní skupina (APWG) nahlásila celkem 396 688 jedinečných e-mailových phishingových kampaní ve čtvrtém čtvrtletí roku 2020.[1]

Ochrana webových prohlížečů proti phishingu

Ochrana proti phishingu je zajišťována aplikací ve webovém prohlížeči, která žádá o hodnocení adresy URL z cloudové služby, jež prohledávala Internet a hledala phishingové webové stránky a přidávala je na seznam blokovaných. Tímto způsobem se pak webový prohlížeč pokusí o návštěvu adresy URL a ochrana před phishingem prohlížeče (tj. Safe Browsing, SmartScreen apod.) přesměruje uživatele na výstražnou zprávu vysvětlující, že adresa URL je škodlivá. Některé systémy hodnocení také zahrnují dodatečný vzdělávací obsah. Naopak pokud je webová stránka označena jako „dobrá“, neprovede webový prohlížeč žádnou akci.

Google a Firefox využívají rozhraní Google Safe Browsing API pro hodnocení pověsti adres URL k varování uživatelů před stahováním některých typů souborů. Microsoft Edge využívá nástroj Microsoft Defender SmartScreen, který 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.

Průměrný počet denně přidávaných adres škodlivých URL

V průměru bylo do testovací sady denně přidáváno 50 nových ověřených adres URL. Čísla se v některých dnech liší, jelikož úrovně škodlivé činnosti kolísaly.

Celkový počet škodlivých adres URL v testu

26 976 hrubých, neověřených adres URL bylo několikrát otestováno z každého prohlížeče v průběhu celkem 80 zkušebních cyklů, prováděných bez přerušení v průběhu 480 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 61 605 diskrétních, platných phishingových testů (20 535 testů na webový prohlížeč) přidáno 996 jedinečných, platných phishingových adres URL, což zajistilo chybovost menší než 3,1 procenta (< 3,1 %) v intervalu jistoty 95 %.

Složení testu – phishingové adresy URL

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

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

Jak jsme hodnotili výsledky

Změřili jsme schopnost každého prohlížeče blokovat škodlivé adresy URL 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 adres URL 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, byla adresa URL, která byla online po dobu 48 hodin, testována 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

[1] Zpráva trendů phishingové aktivity APWG

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