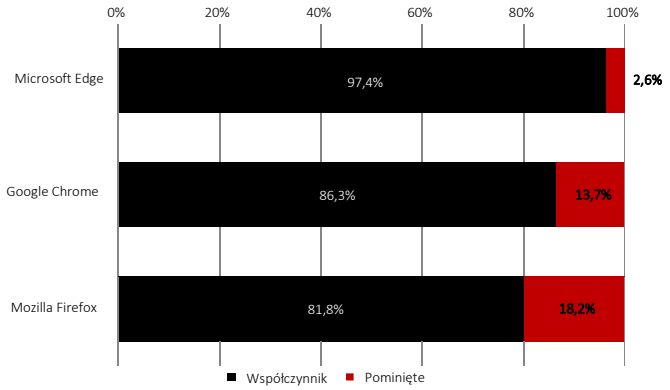
Q2 2021 Przeglądarki internetowe kontra złośliwe oprogramowanie

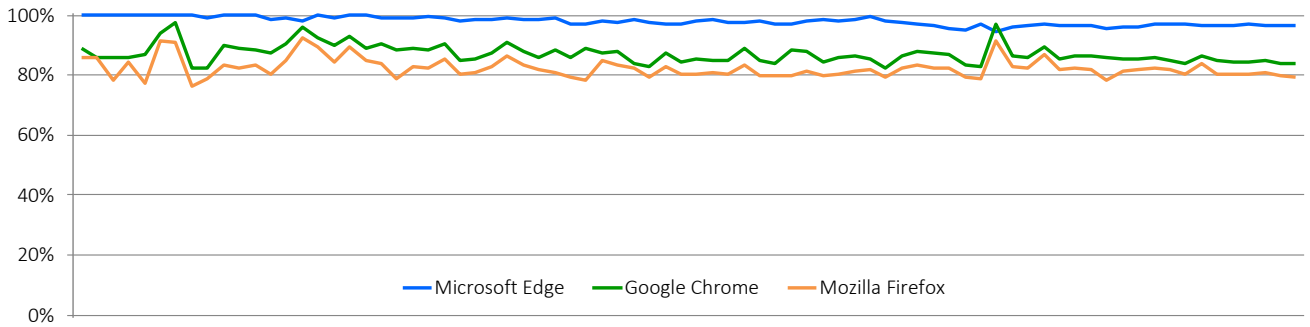
Omówie

W drugim kwartale 2021 roku strona internetowa CyberRatings.org przeprowadziła niezależny test zabezpieczeń przed złośliwym oprogramowaniem oferowanych przez przeglądarki internetowe. Testy trwały 20 dni, a łącznie odbyło się 80 oddzielnych przebiegów testowych. Przeglądarka Microsoft Edge chroni klientów przed złośliwym oprogramowaniem przy użyciu rozwiązania Microsoft Defender SmartScreen, a przeglądarki Google Chrome i Mozilla Firefox wykorzystują interfejs API Google Safe Browsing. Przeglądarka Microsoft Edge zapewniała najlepszą ochronę, blokując 97,4% złośliwego oprogramowania, a jednocześnie gwarantowała najdoskonalszy współczynnik ochrony przed oprogramowaniem typu zero-hour (97,7%). Przeglądarki Google Chrome i Mozilla Firefox uplasowały się kolejno na drugim i trzecim miejscu z wynikami odpowiednio 86,3% i 81,8%.



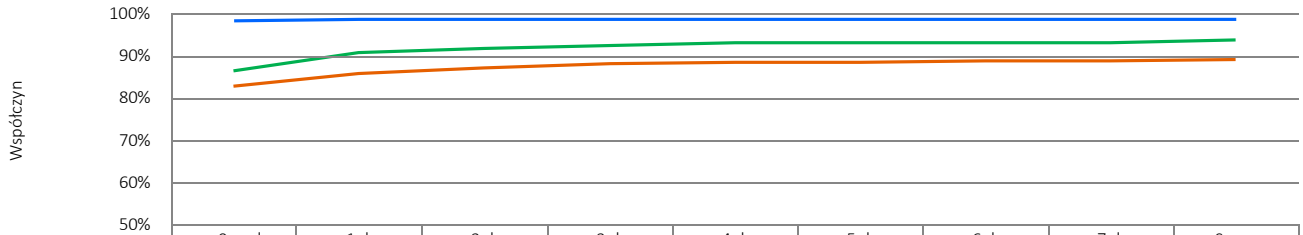
Przeglądarki, które mają możliwość ostrzegania potencjalnych ofiar o złośliwym oprogramowaniu na stronach internetowych, mogą w znacznym stopniu zwiększyć ich bezpieczeństwo. Z uwagi na to, że strony internetowe, będące dziełem inżynierii społecznej, z których wprowadzeni w błąd użytkownicy pobierają złośliwe oprogramowanie, są publikowane tylko na chwilę, jak najszybsze wykrywanie i dodawanie do systemu reputacji takich witryn to kluczowe kwestie. Dlatego właśnie dobry system reputacji to taki, który osiąga wysoką częstotliwość wykryć szybko i z dużą dokładnością.

Ochrona przed złośliwym oprogramowaniem w czasie



Podczas testu stale dodawano nowe złośliwe oprogramowanie. Adresy URL, które przestawały być dostępne lub nie zawierały dłużej złośliwego oprogramowania, usuwano. Każdy punkt danych obliczano na podstawie pomiarów zarejestrowanych w określonym czasie. Jeśli złośliwe oprogramowanie zostało zablokowane na wczesnym etapie, ocena zabezpieczeń przeglądarki poprawiała się, a spadała, gdy przeglądarce nie udawało się zablokować złośliwego oprogramowania.

Współczynnik blokowania złośliwego oprogramowania w czasie



	0-godz.	1 d.	2 d.	3 d.	4 d.	5 d.	6 d.	7 d.	Suma
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%

Podsumowanie

Rysunek powyżej przedstawia czas, po jakim przeglądarka zablokowała złośliwe oprogramowanie od chwili wprowadzenia próbki do cyklu testowego. Najważniejszym zabezpieczeniem w przeglądarce Microsoft Edge jest bazujące na adresach URL rozwiązanie SmartScreen chroniące przed atakami dzięki zintegrowanej usłudze w chmurze do weryfikacji reputacji adresów URL i reputacji aplikacji blokującej złośliwe pliki. Przeglądarki Google Chrome i Mozilla Firefox wykorzystują interfejs API Google Safe Browsing zarówno do weryfikacji reputacji adresów URL, jak i do blokowania niektórych typów plików lub ostrzegania przed nimi użytkowników.

Ataki złośliwego oprogramowania

Ataki socjotechniczne przy użyciu złośliwego oprogramowania (SEM, social engineered malware) podstępem przekonują użytkowników do pobierania złośliwego oprogramowania: Przejęte konta e-mail i konta w mediach społecznościowych wykorzystują zaufanie do osób z list kontaktów i oszukują ofiary, które uznają łącza do złośliwie spreparowanych plików za zaufane. Oszuści stosują też wyskakujące okienka z monitami o instalację aplikacji (np. Adobe Flash Player), ostrzeżeniami o infekcji komputera lub konieczności przeprowadzenia aktualizacji.

Skutkami instalacji złośliwego oprogramowania może być kradzież poświadczeń lub tożsamości czy włamanie na rachunek bankowy.

Zabezpieczenia przeglądarek przed złośliwym oprogramowaniem

Aby zapewniać ochronę przed złośliwym oprogramowaniem, systemy reputacji w chmurze przeszukują Internet w poszukiwaniu złośliwych stron internetowych i odpowiednio kategoryzują treści. Następnie przeglądarki internetowe wysyłają zapytania do systemów reputacji w chmurze dotyczące określonych adresów URL, plików lub aplikacji. Jeśli wynik świadczy o obecności złośliwego oprogramowania, przeglądarka internetowa przekieruje użytkownika do komunikatu ostrzegawczego z informacją o tym, że adres URL, plik lub aplikacja zawiera złośliwy kod. Niektóre systemy reputacji obejmują również dodatkowe treści edukacyjne.

Przeglądarki Google Chrome i Mozilla Firefox wykorzystują interfejs API Google Safe Browsing do weryfikacji reputacji adresów URL i aplikacji blokujący złośliwe pliki. Przeglądarka Microsoft Edge wykorzystuje rozwiązanie Microsoft Defender SmartScreen chroniące przed atakami dzięki usłudze do weryfikacji reputacji adresów URL i reputacji aplikacji blokującej złośliwe pliki.

Średnia liczba próbek złośliwego oprogramowania dodawana dziennie

Średnio dziennie do zestawu testowego dodawano 49 nowych zweryfikowanych próbek złośliwego oprogramowania. Zmienność w tym zakresie wynikała z fluktuacji w natężeniu działalności przestępców.

Łączna liczba sprawdzonych próbek złośliwego oprogramowania

18 621 nieobrobionych, niezweryfikowanych próbek sprawdzono wiele razy każdą przeglądarką w ciągu łącznie 78 cykli testowych na przeglądarkę przeprowadzonych bez przerw na przestrzeni 468 godzin (co 6 godzin przez 20 dni). Nasi informatycy usunęli próbki, które nie przeszły kryteriów weryfikacji, także te zanieczyszczone programami wykorzystującymi luki (nie były one wykorzystywane podczas testów). Ostatecznie 950 unikatowych pozycji spełniających kryteria próbek złośliwego oprogramowania uwzględniono w ostatecznym zbiorze 48 672 odrębnych, spełniających kryteria testów złośliwego oprogramowania (16 224 testy na przeglądarkę). Margines błędu wyniósł mniej niż 3,2 procenta (<3,2%) przy poziomie pewności 95%.

Sposób testowania — próbki złośliwego oprogramowania

Dane w raporcie pochodzą z okresu testowego dwudziestu (20) dni od 11 maja do 31 maja 2021 roku. Podczas testu informatycy CyberRatings rutynowo monitorowali łączność, aby zapewnić przeglądarkom stały dostęp do złośliwego oprogramowania i usług do weryfikacji reputacji w chmurze.

Nacisk położono na świeżość, dlatego do testu stale wdrażano nowe próbki, a usuwano martwe.

Sposób oceny wyników

Sprawdzone zostały możliwości blokowania złośliwego oprogramowania każdej przeglądarki w najkrótszym możliwym czasie od ich wykrycia w Internecie. Informatycy powtarzali testy co sześć godzin, aby określić, jak długo zajmie dostawcy ewentualne dodanie zabezpieczeń.

Wyniki każdej przeglądarki były regularnie sprawdzane, a ogólny współczynnik blokowania testowanych próbek złośliwego oprogramowania rejestrowano. Wzorem na ogólny współczynnik blokowania każdej przeglądarki był iloraz udanych blokad i łącznej liczby przypadków testowych. Przykładowo: w przypadku przeprowadzania testów co 6 godzin próbkę złośliwego oprogramowania dostępną online przez 48 godzin sprawdzano osiem (8) razy. Przeglądarka, która zablokowała próbkę w 6 z 8 przebiegów testowych, osiągnęła współczynnik blokowania 75%.

Środowisko testowe

- Microsoft Windows 10 Pro, 21H1

Testowane produkty

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

Autorzy

Thomas Skybakmoen, Vikram Phatak

Metodologia testów

Metodologia testów zabezpieczeń przeglądarek internetowych CyberRatings v1.0 jest dostępna pod adresem www.cyberratings.org

Dane kontaktowe

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

info@cyberratings.org
www.cyberratings.org