

1 Wstęp

Bezpieczeństwo przeglądarek internetowych z pewnością stało się jednym z najważniejszych czynników decydujących o bezpiecznym korzystaniu z Internetu, zarówno przez indywidualnego użytkownika sieci jak również firmy - poprzez jej pracownika. Przeglądarka ze względu na swoją powszechność jest obecnie jednym z najczęściej atakowanych typów oprogramowania. Nieautoryzowana instalacja oprogramowania czy podstawianie nieprawdziwego adresu URL to jedne z najczęściej stosowanych technik w atakach sieciowych, które niestety okazują się być bardzo skuteczne. Efektem ich wykorzystania mogą być zarówno ataki na pojedynczych użytkowników (np.: *phishing*) jak również budowanie olbrzymich sieci, nad którymi została przejęta kontrola i które mogą być wykorzystywane do dalszych ataków (np.: atak typu DDoS, rozsyłanie spamu).

Dyskusji nad bezpieczeństwem przeglądarek właściwie zawsze towarzyszy próba odpowiedzi na pytanie, która z nich jest najbardziej bezpieczna, a która najmniej? Zdajemy sobie sprawę, że odpowiedź na tak postawione pytanie nie jest łatwe. Niemniej jednak mamy nadzieję, że wyniki naszej analizy mogą stać się pomocne w dalszej, rzeczowej dyskusji o bezpieczeństwie przeglądarek, która powinna być ważnym elementem dyskusji na temat bezpiecznego korzystania z Internetu.

2 Dane statystyczne

Jako podstawę informacji o lukach w przeglądarkach potraktowaliśmy raporty firmy Secunia¹ (<http://www.secunia.com/>). Bazując na metodologii tej firmy, wprowadziliśmy podziały luk na załatane, częściowo załatane i niezałatane.

Pełne załatanie luki jest równoznaczne z tym, że została udostępniona poprawka producenta i luka już nie występuje. Częściowe załatanie może przykładowo oznaczać, że luka została naprawiona w niektórych systemach operacyjnych lub została zmieniona domyślna konfiguracja, lecz w pewnych okolicznościach lukę nadal można wykorzystać. Podzieliliśmy luki także w zależności od ich wagi. Do kategorii „krytyczne” zostały zaliczone wszystkie luki, pozwalające na zdalne i anonimowe przejęcie kontroli nad systemem, nie wymagające określonych działań użytkownika².

Skupiliśmy się na przeglądarkach, których udział w rynku przekracza 1%³, co w praktyce oznaczało cztery przeglądarki – Microsoft Internet Explorer (MSIE), Mozilla, Mozilla Firefox oraz Opera. Przeglądarka Mozilla Firefox została świadomie potraktowana jako oddzielny produkt, gdyż jej rozwój jest coraz bardziej niezależny od macierzystej Mozilli.

¹ Wybór tego zestawu statystyk podyktowany został faktem, że to jedyne tego typu kompletne zestawienie interesujących nas danych.

² Odpowiada to lukom określanym jako 'extremally critical' oraz 'highly critical' w systematyce Secunii, gdzie dodatkowo wprowadzono podział ze względu na dostępność kodu wykorzystującego lukę.

³ Wszelkie statystyki dotyczące udziału poszczególnych przeglądarek pochodzą z badań GemiusTraffic przygotowywanego przez Gemius S.A. i publikowanego na stronach serwisu <http://www.ranking.pl/>. Dotyczą okresu 13-19 grudnia 2004r.

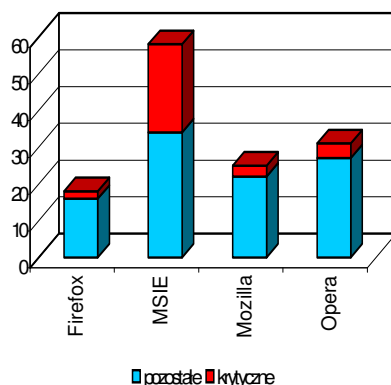
Oczywiście, ponieważ spora część kodu obu przeglądarek jest wspólna, wiele błędów okazywało się wspólnych dla obu produktów.

W raporcie uwzględniliśmy luki wykryte od stycznia 2003 do grudnia 2004 roku. Okres ten został wybrany arbitralnie, a jednym z argumentów jest fakt, że w powszechnie używanych obecnie produktach nie ma luk starszych niż pochodzące z tego okresu, na które nie byłaby dostępna odpowiednia łata. Tworząc zestawienie luk, braliśmy pod uwagę cykl życia danego produktu w rozważanym okresie. Jeżeli po wykryciu luki ukazywała się nowa wersja przeglądarki, pozbawiona już tej słabości, lukę taką traktowaliśmy jako załataną. W przypadku Internet Explorera pod uwagę braliśmy wyłącznie wersję 6. MSIE 5, mimo że jest nadal w powszechnym użyciu, nie jest wspierana przez producenta i porównywanie jej z aktualnymi przeglądarkami nie miałyby sensu.

3 Wskaźniki dotyczące bezpieczeństwa

Aby spróbować odpowiedzieć na pytania postawione we wstępie zaproponowaliśmy posłużenie się dwoma wskaźnikami. Poniżej znajdują się ich krótkie opisy wraz z wyliczonymi wartościami. Przed wyciągnięciem ostatecznych wniosków podjęliśmy próbę wstępnej interpretacji uzyskanych wyników.

3.1 Bezwzględna liczba luk, procent luk krytycznych.



Wykres 1 - Bezwzględna liczba luk, w tym luk krytycznych

Liczba wszystkich ujawnionych luk dotyczących danej przeglądarki oraz procent luk krytycznych.

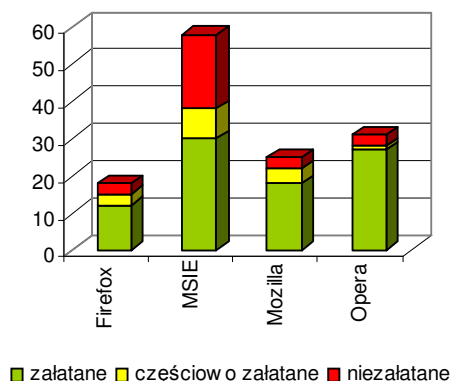
Tabela 1- Bezwzględna liczba luk, luk krytycznych i procent luk krytycznych

Przełęczarka	Liczba luk	Liczba luk krytycznych	Procent luk krytycznych
Firefox	18	2	11%
MSIE	58	24	41%
Mozilla	25	3	12%
Opera	31	4	13%

Jak wynika z powyższych danych najwięcej luk dotyczy przeglądarki MSIE, mniej związanych jest z Operą i Mozillą, zaś najmniej z Firefox. 41% wszystkich luk w MSIE to luki krytyczne, w przypadku pozostałych przeglądarek wartość ta wynosi od 11% do 13%.

3.2 Poziom załatania przeglądarki

Wskaźnik ten opisany został jako procent udziału luk załatanych we wszystkich lukach dotyczących danej przeglądarki (podajemy również liczbę niezalatanych luk). Obliczyliśmy również poziom załatania przeglądarki dla luk krytycznych.



Wykres 2- Bezwzględna liczba luk w rozbiciu na załatane, częściowo załatane i niezalatane

Tabela 2- Poziom załatania

Przełgądarka	Procent luk załatanych	Liczba luk niezalatanych	Procent luk krytycznych załatanych	Liczba luk krytycznych niezalatanych
Firefox	83%	3	100%	0
MSIE	66%	20	83%	4
Mozilla	88%	3	100%	0
Opera	90%	3	100%	0

Najniższą wartość tego wskaźnika ma przeglądarka MSIE, następne w kolejności są Firefox, Mozilla i Opera. W przypadku luk krytycznych, dla trzech ostatnich przeglądarek wartość wynosi 100%, czyli wszystkie luki krytyczne są załatane. Wartość wskaźnika dla MSIE wynosi 83%, co znaczy, że 4 luki pozostają niezalatane.

4 Wnioski i rekomendacje

Do oceny bezpieczeństwa przeglądarek internetowych posłużyliśmy się dwoma wskaźnikami: liczbą bezwzględną luk wraz z procentem luk krytycznych oraz poziomem załatania przeglądarki.

Z pierwszego ze wskaźników wynika, że najwięcej luk bezpieczeństwa w kodzie odkryto w przeglądarce MSIE. Dotyczy to szczególnie najbardziej istotnych luk - 41% wykrytych luk w oprogramowaniu MSIE to luki krytyczne, których wykorzystanie pozwala na zdalne i anonimowe przejęcie kontroli nad systemem, nie wymagające określonych działań użytkownika. W przypadku tego wskaźnika, w naszym zestawieniu najlepiej wypada Firefox.

Wskaźnik przedstawiający poziom załatania systemu wydaje się dosyć dobrze obrazować aktualny stan bezpieczeństwa oprogramowania. Niestety producenci żadnej z przeglądarek nie załatali wszystkich znanych luk systemowych. Po trzy niezalutane luki mają Firefox, Mozilla i Opera, 20 takich luk ma MSIE. Naszym zdaniem luki krytyczne powinny być w 100% załatane przez producenta. Jedyną przeglądarką, która nie spełnia tego założenia to MSIE. Mozilla i Opera posiadają największy odsetek załutanych luk – odpowiednio 90% i 88%.

Ciekawym, uzupełniającym wskaźnikiem poziomu bezpieczeństwa związanego z używaniem danej przeglądarki mógłby być wskaźnik opisujący, jak dużo czasu potrzebował producent na załatanie luki. Niestety ze względu na trudności związane z dotarciem do danych na temat szczegółowych dat wykrycia, opublikowania i załutania luki, nie udało nam się przygotować takiego zestawienia.

Równie interesująca mogłaby okazać się próba odpowiedzi na pytanie, jak popularność danej przeglądarki wpływa na ilość odkrytych w jej kodzie luk. Przy obecnej dominacji MSIE na rynku przeglądarek (ponad 75% użytkowników sieci korzysta z tej właśnie przeglądarki) postawienie tezy, że jest taka zależność i jest ona wprost proporcjonalna, ustawia MSIE w rankingu bezpieczeństwa zdecydowanie wyżej od pozostałych przeglądarek, aczkolwiek, co warto zauważyć, tylko w przypadku ogólnej liczby luk. Jeśli chodzi o luki krytyczne, przewaga ta nie jest już tak duża.

Tabela 3 - Popularność przeglądarki a liczba luk

Przeglądarka	Popularność	Liczba luk / Popularność	Liczba luk krytycznych / Popularność
<i>Firefox</i>	3,5%	5,14	0,57
<i>MSIE</i>	75,1%	0,77	0,32
<i>Mozilla</i>	1,9%	13,16	1,58
<i>Opera</i>	4,3%	7,21	0,93

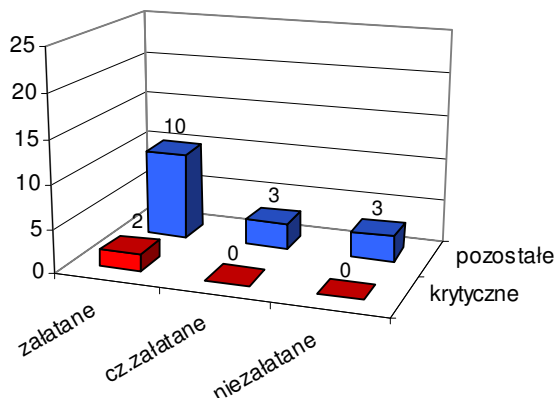
Przydatność wykorzystania tego wskaźnika w ocenie bezpieczeństwa przeglądarek naszym zdaniem należy traktować z ostrożnością, przynajmniej do czasu, kiedy można by się posłużyć większą ilością danych na ten temat, np.: jeśli znacząco zmieniałyby się popularność poszczególnych przeglądarek, a i korelacja między liczbą luk i popularnością aplikacji zostałaby potwierdzona.

W dziedzinie bezpieczeństwa obowiązuje zasada najsłabszego ogniwa. Naszym zdaniem w przypadku oceny bezpieczeństwa przeglądarek tym najsłabszym ogniwem jest liczba luk krytycznych. Tak jak pisaliśmy wcześniej, producent powinien uczynić wszystko, aby w momencie wystąpienia luki krytycznej została ona załutana. Również wysoka wartość bezwzględnej liczby luk krytycznych jest bardzo niebezpieczna. Założenie, że wszyscy z użytkowników, lub choćby ich zdecydowana większość, załutają swoje systemy, niesie ze sobą zbyt dużą dozę optymizmu. Dlatego produkt, który dużo takich luk posiada, szczególnie niezalutanych, jest produktem narażonym na skuteczne ataki. Z naszej analizy wynika, że bezpieczeństwo trzech przeglądarek: Firefox, Mozilla i Opera układa się na podobnym poziomie. Wybór jednej z nich powinien opierać się o indywidualne preferencje, takie jak funkcjonalność czy dodatkowych funkcje (poczta elektroniczna, przeglądarka newsów itp.)

5 Dodatkowe informacje dotyczące bezpieczeństwa przeglądarek.

W tym rozdziale umieściliśmy kilka dodatkowych informacji dotyczących bezpieczeństwa poszczególnych przeglądarek, podając między innymi adresy stron producentów przeglądarek, na których znajdują się informacje na temat ich bezpieczeństwa.

5.1 Firefox



Wykres 3 - Firefox - rozkład luk załatanych, częściowo załatanych, niezałatanych w odniesieniu do luk krytycznych i pozostałych

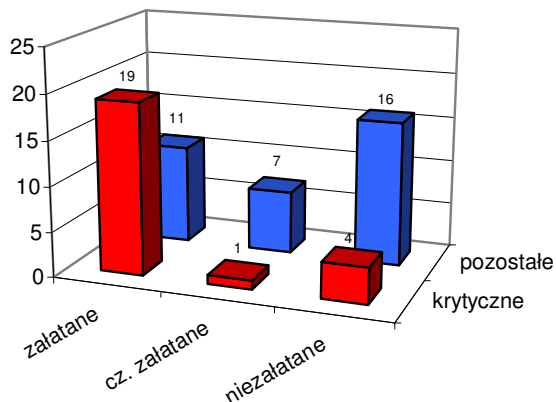
Firefox jest stosunkowo „młoda” przeglądarką. Dopiero niedawno ukazała się jej wersja 1.0.; wcześniej projekt żył jako Phoenix, Mozilla Firebird, i Firefox 0.x. Ujawnione luki, opisane przez Secunię, dotyczą wersji 0.x i 1.x z roku 2004.

Najstarsza niezałatana luka w przeglądarce Firefox pochodzi z 30 sierpnia 2004 roku i dotyczy wersji na platformę Mac OS X. Umożliwia zmianę treści zakładek, co może służyć do przeprowadzania ataków typu *phishing*. Ostatnia niezałatana luka, dotycząca użytkowników systemów Windows, została ujawniona 18 września 2004 roku i umożliwia podmianę plików cookies oraz zakłócanie uwierzytelnionych sesji na niektórych stronach.

Raporty Secunia dotyczące przeglądarki Firefox: <http://secunia.com/product/4227/>

Strona producenta dotycząca bezpieczeństwa: <http://www.mozilla.org/security/>

5.2 MS Internet Explorer



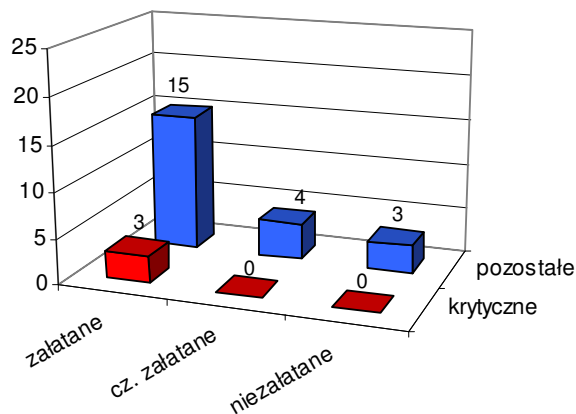
Wykres 4 - MSIE - rozkład luk załatanych, częściowo załatanych, niezałatanych w odniesieniu do luk krytycznych i pozostałych

Najstarsza niezałatana luka w MSIE pochodzi z 13 marca 2003 roku i dotyczy obsługi archiwów .mht. Pozwala na spowodowanie zamknięcia przeglądarki. Najstarsza niezałatana krytyczna luka, datowana jest na 14 sierpnia 2003 roku, dotyczy jednej z wtyczek ActiveX i może pozwalać na wykonanie dowolnego kodu przy przeglądaniu stron WWW.

Raporty Secunia dotyczące przeglądarki MSIE: <http://secunia.com/product/11/>

Strona producenta dotycząca bezpieczeństwa: <http://www.microsoft.com/security/>

5.3 Mozilla



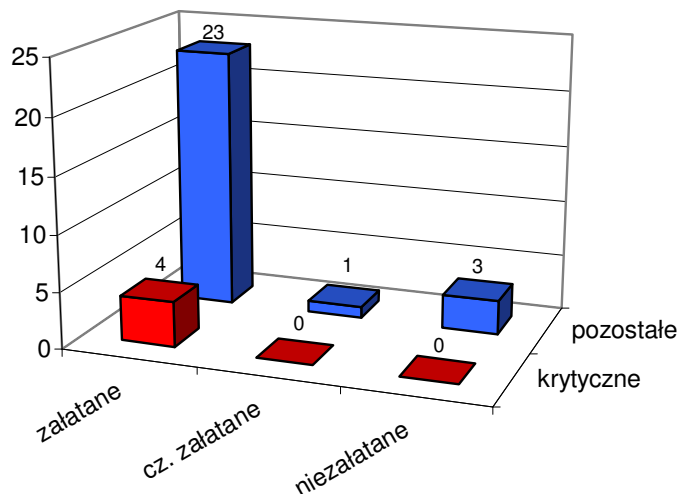
Wykres 5 - Mozilla - rozkład luk załatanych, częściowo załatanych, niezałatanych w odniesieniu do luk krytycznych i pozostałych

Najstarsze niezalātane luki w przeglądarce Mozilla opisane s przy okazji opisu Firefoxa. W sierpniu 2004 roku Mozilla Foundation ogłosiła nagrodę 500\$ za znalezienie kaŹdej luki zwizanej z bezpieczestwem w ich oprogramowaniu. Akcja ta obejmuje zarówno produkt Mozilla jak i Mozilla Firefox.

Raporty Secunia dotyczce przegldarki Mozilla 1.7.x: <http://secunia.com/product/3691/>

Strona producenta dotyczca bezpieczestwa: <http://www.mozilla.org/security/>

5.4 Opera



Wykres 6 - rozkład luk załatanych, częściowo załatanych, niezalātanych w odniesieniu do luk krytycznych i pozostałych

Najstarsza niezalātana luka w Operze pochodzi z 20 paŹdziernika 2004 roku i jest zwizana z moŹliwością podmiany zawartości wyskakujcych okien przez kod strony, która nie wygenerowała okna, co moŹe ułatwiać ataki typu *phishing*.

Raporty Secunia dotyczce przegldarki Opera: <http://secunia.com/advisories/12713/>

Strona producenta dotyczca bezpieczestwa:
<http://www.opera.com/support/service/security/>

5.5 Inne Źródła informacji o bezpieczestwie przegldarek

Wiele uwagi zostało poŹwięcone przegldarkom w najnowszym, piątym wydaniu listy najpowaŹniejszych zagroŹe dla systemów Windows i Unix, SANS Top 20. Poza wymieniem istniejcych luk w oprogramowaniu, w dokumencie tym znalazły się takŹe rady dla uŹytkownikw i sposoby podniesienia bezpieczestwa, w szczeglnoŹci do zastosowania w Internet Explorerze.

Polsk wersj jzykow dokumentu, przygotowan przez CERT Polska, znaleźc moŹna pod adresem <http://www.sans.org/top20/top20-v50-polish.pdf>.

Polecamy także dokumenty przygotowane przez US-CERT:

- [Cyber Security Tip ST04-012: Understanding Active Content and Cookies](#)
- [Cyber Security Tip ST04-16: Recognizing and Avoiding Spyware](#)
- [Cyber Security Tip ST05-001: Evaluating Your Web Browser's Security Settings](#)