Złodzieje znaleźli sposób na obejście tego zabezpieczenia banku. Mogą cię okraść

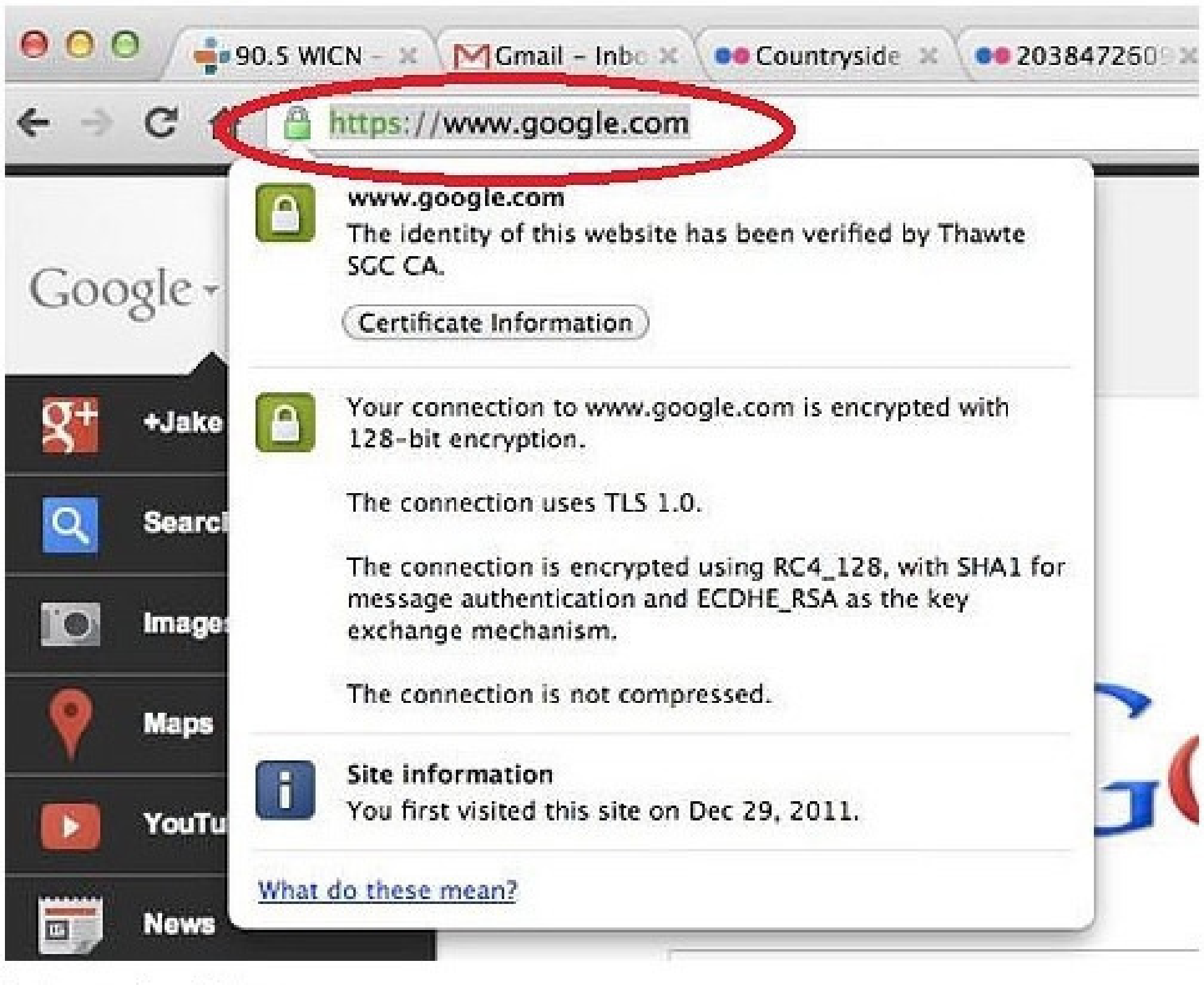
Robert Kędzierski
16.06.2016 09:48

Podziel się

5 najlepszych antywirusów na Androida (Fotomontaż Robert Kędzierski/ Fot. Thom Weerd/psdreams.com)

Ataki skierowane przeciwko klientom bankowości elektronicznej stały się jeszcze bardziej niebezpieczne. Złodzieje znaleźli sposób na obejście bardzo ważnego zabezpieczenia.

Zaufana Trzecia Strona donosi o nowym sposobie cyberprzestępców na wykradanie pieniędzy z naszych kont. Nauczyli się jak omijać ważne zabezpieczenie, które do tej pory miało gwarantować bezpieczeństwo transakcji przeprowadzanych online. Chodzi o certyfikat SSL potwierdzający zaszyfrowanie połączenia z bankiem.



www.google.com
The identity of this website has been verified by Thawte SGC CA.

Certificate Information

Your connection to www.google.com is encrypted with 128-bit encryption.

The connection uses TLS 1.0.

The connection is encrypted using RC4_128, with SHA1 for message authentication and ECDHE_RSA as the key exchange mechanism.

The connection is not compressed.

Site information
You first visited this site on Dec 29, 2011.

What do these mean?

Fot. www.hongkiat.com

Przeczytaj też: Przestępcy są groźni, bo... są grzeczni.

Przestępcy obchodzą zabezpieczenie

Do tej pory przestępcy działali dość ordynarnie. Używali phishingu - kierowali klientów na fałszywą stronę banku i wyłudzali dane logowania licząc, że uda się wyciągnąć od niezbyt zorientowanego w kwestiach technicznych klienta kod SMS. To pozwala zalogować się na konto, zmienić dane któregoś z odbiorców zaufanych i wyprowadzić wszystkie oszczędności z naszego konta.

Ten sposób na kradzież przestaje być skuteczny w przypadku bardziej świadomych klientów, którzy słyszeli o dwóch ważnych zasadach dotyczących bezpieczeństwa. Po pierwsze: adres banku musi być autentyczny (np. www.pko.pl, a nie www.pko.xyz). Po drugie symbol kłódki przed nazwą strony. Na fałszywych stronach go nie ma, a tylko obecność takiego symbolu gwarantuje, że połączenie z bankiem jest szyfrowane i nikt nie może "podsłuchać" naszej korespondencji, a więc przejąć naszego loginu. Inne ataki polegają na fizycznej podmianie numeru konta, kiedy kopiujemy go jako tekst (np. z wiadomości e-mail) i wklejamy do odpowiedniego pola na stronie banku. Jeden z polskich użytkowników stracił w ten sposób 40 tys. zł.

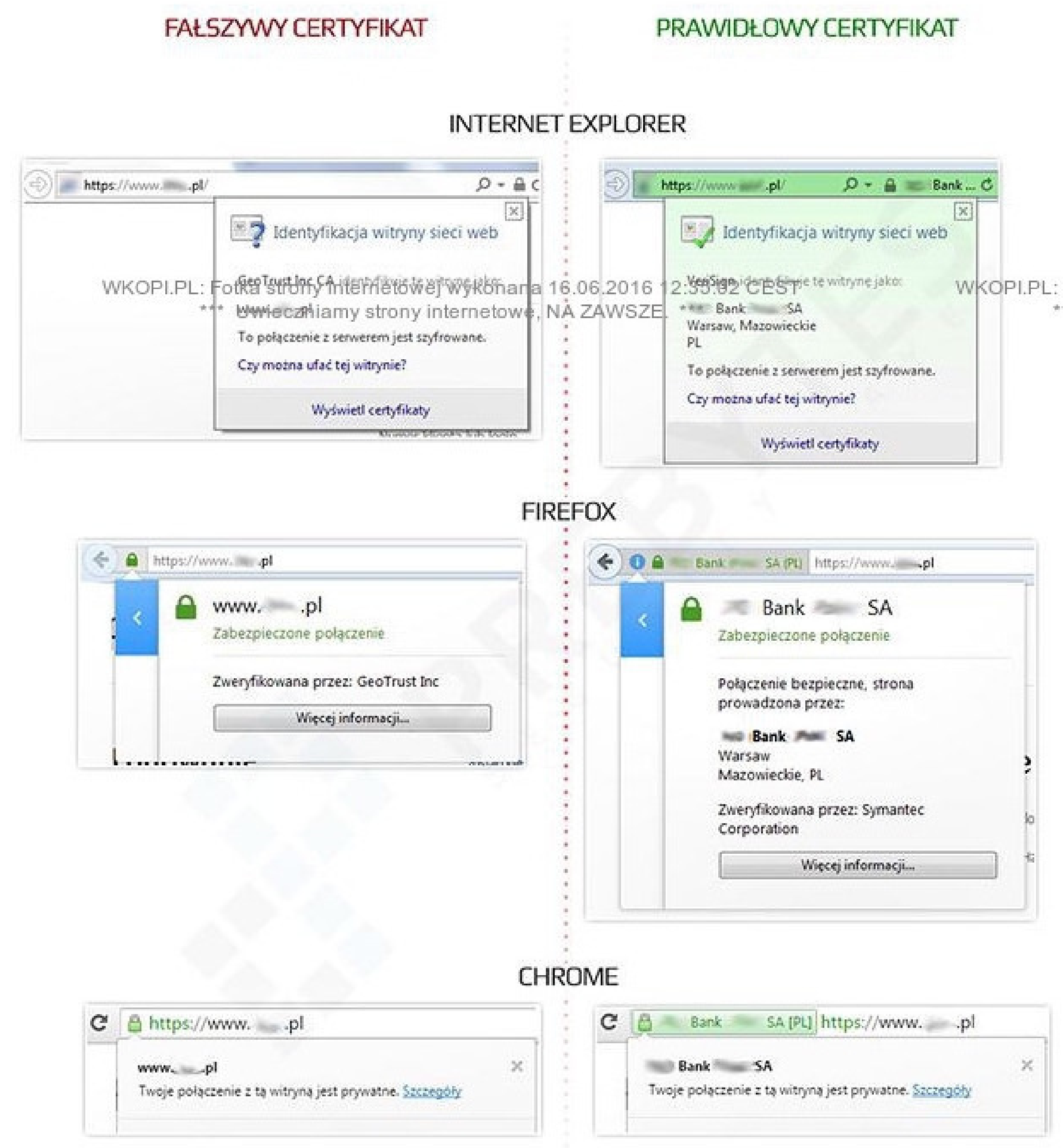
Nie ufaj kłódce

Fałszywe strony nie mogły do tej pory wyświetlić ikony kłódki przed nazwą adresu. Najnowszy wirus sprawia jednak, że kłódka się pojawia.

Komputer ofiary jest zarażany w taki sposób, by jednocześnie zmienić konfigurację serwerów DNS i zainstalować fałszywy certyfikat. Użytkownik zostanie więc skierowany na podstawioną przez przestępców stronę (nawet jeśli samodzielnie wpiszę poprawny adres strony). Zobaczy też ikonkę z kłódką wyświetlaną dzięki fałszywemu certyfikatowi.

Jak się bronić?

Obrona przed atakiem tego typu jest dość prosta, ale wymaga jednego: świadomości. Jak wyjaśnia firma Prebytes, specjalizująca się cyberbezpieczeństwie, autentyczny certyfikat różni się od fałszywego.



https://www.[redacted].pl/
Identyfikacja witryny sieci web
GeoTrust Inc CA identyfikuje tę witrynę jako:
www.[redacted].pl
To połączenie z serwerem jest szyfrowane.
Czy można ufać tej witrynie?
Wyświetl certyfikaty

https://www.[redacted].pl/ Bank ...
Identyfikacja witryny sieci web
VeriSign identyfikuje tę witrynę jako:
[redacted] Bank [redacted] SA
Warsaw, Mazowieckie
PL
To połączenie z serwerem jest szyfrowane.
Czy można ufać tej witrynie?
Wyświetl certyfikaty

https://www.[redacted].pl
www.[redacted].pl
Zabezpieczone połączenie
Zweryfikowana przez: GeoTrust Inc
Więcej informacji...

[redacted] Bank [redacted] SA (PL) https://www.[redacted].pl
[redacted] Bank [redacted] SA
Zabezpieczone połączenie
Połączenie bezpieczne, strona prowadzona przez:
[redacted] Bank [redacted] SA
Warsaw
Mazowieckie, PL
Zweryfikowana przez: Symantec Corporation
Więcej informacji...

https://www.[redacted].pl
www.[redacted].pl
Twoje połączenie z tą witryną jest prywatne. Szczegóły

[redacted] Bank [redacted] SA [PL] https://www.[redacted].pl
[redacted] Bank [redacted] SA
Twoje połączenie z tą witryną jest prywatne. Szczegóły

Fot. Prebyte/Związek Banków Polskich

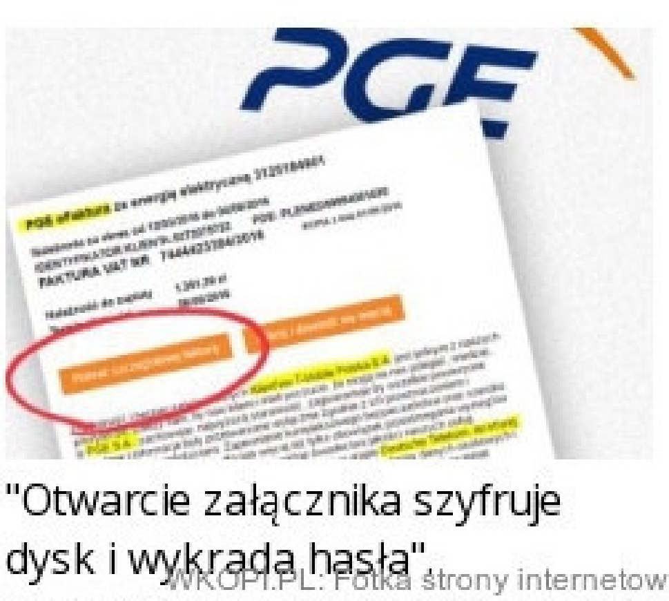
W pierwszym wypadku po kliknięciu ikonki kłódki zobaczymy dodatkowe informacje potwierdzające fakt, że certyfikat został wydany dla banku, z którego korzystamy. "Fałszywa" kłódka takich informacji nie wyświetla.

Niestety spora część konsumentów może nie zwrócić na to uwagi - w końcu samodzielnie wpisali adres swojego banku, nie klikali linka z wiadomości o zablokowaniu konta.

Podziel się Tweetnij

cyberprzestępcy, bankowość elektroniczna, wirusy, hakerzy

POLECAMY



"Otwarcie załącznika szyfruje dysk i wykrada hasła". Podrobione faktury PGE

Nowa fala fałszywych maili. Wyjątkowo perfidne. NIE SĄ od Allegro!

KOMENTARZE (4)

Złodzieje znaleźli sposób na obejście tego zabezpieczenia banku. Mogą cię okraść

Zaloguj się Skomentuj

najnowsze popularne

ssamiec 22 minuty temu 0

Jak się bronić?
Nie logować się do banku spod windowsa.

Odpowiedz

Abigail Sarah Poisson pół godziny temu Oceniono 1 raz -1

kolejne pie...nie w bambuko, po co pisac o czyms, na czym sie nie zna?

Pokaż odpowiedzi (2) Odpowiedz

NAJCZĘŚCIEJ CZYTANE

1. Milik strzela, Ty zarabiasz. Nie, nie chodzi o zakłady bukmacherskie
2. Nie spłacasz kredytu? Firma pożyczkowa opublikuje twoje nagie
3. To definitywny koniec najstarszego polskiego supermarketu. Przegrał z
4. Ukochany bank Putina umiera. Dobiły go igrzyska w Soczi. Potrzebny
5. Dzień Wolności Podatkowej czyli pomieszanie z poplątaniem