Okres	19-26.03.2009

Mozilla Firefox	
Krótki opis zagrożenia	W przeglądarce Internetowej Mozilla Firefox ujawniono luki związane z bezpieczeństwem, które mogą pozwolić osobie nieupoważnionej m.in. na uzyskanie dostępu do informacji zapisanych na dysku komputera użytkownika.
Poziom zagrożenia	**Wysoki**
Opis sposobu usunięcia	Należy zainstalować najnowszą wersję przeglądarki (3.0.8) opublikowaną na stronie: http://www.firefox.pl
Dodatkowe informacje dla zaawansowanych	Informacje dostępne wyłącznie w języku angielskim: http://www.mozilla.org/projects/security/known-vulnerabilities.html

Mozilla Firefox	
Krótki opis zagrożenia	W Internecie wykryto atak przeprowadzany na użytkowników przeglądarki Mozilla Firefox. Polega on na sprowokowaniu Użytkownika do zainstalowania specjalnej wtyczki w przeglądarce. Wtyczka ta działa jak typowy koń trojański, pobierając m.in informacje dotyczące logowania do wielu instytucji finansowych. Obecna wersja nie jest uczulona na polskie instytucje, ale zapewne może się to szybko zmienić.
Poziom zagrożenia	**Wysoki**
Opis sposobu usunięcia	Odinstalowanie wtyczki z przeglądarki, a następnie usunięcie jej plików.
Dodatkowe informacje dla zaawansowanych	Informacje dostępne wyłącznie w języku angielskim: http://www.bitdefender.com/VIRUS-1000451-en--Trojan.PWS.ChromeInject.B.html

Wirusy	
Krótki opis zagrożenia	W dniu 01.04.2009 aktywowany zostanie robak internetowy *Conficker* wykorzystujący do ataku na stacje Użytkowników lukę w systemach operacyjnych Microsoft Windows opisaną w biuletynie z dn. 23.10.2008. Na dzień dzisiejszy nie ma możliwości oceny skutków jego działania, gdyż zainfekowane komputery dnia 01.04.2009 pobiorą z serwerów w Internecie instrukcję dotyczące działań które mają wykonać.
Poziom zagrożenia	**Wysoki**
Opis sposobu usunięcia	Szczegóły dotyczące usunięcia robaka znajdują się tutaj: http://blogs.msdn.com/rockyh/archive/2009/01/14/conficker-removal-with-msrt.aspx
Dodatkowe informacje dla zaawansowanych	Informacje dostępne wyłącznie w języku angielskim (na przykładzie wersji ikh): http://vil.nai.com/vil/content/v_153464.htm

Wirusy	
Krótki opis zagrożenia	W ostatnim czasie pojawiły się nowe wersje konia trojańskiego (Trojan-Spy.Win32.Zbot) mogące stanowić zagrożenie dla komputera użytkownika. Oprogramowanie to, w szczególności, stara się uzyskać informacje na temat danych wrażliwych wpisywanych przez Użytkowników (dane kart kredytowych, informacje o dostępie do kont bankowych). Aby zabezpieczyć się przed infekcją należy w szczególności nie uruchamiać załączników przesłanych poczta e-mail od nieznanych osób i jeśli to możliwe nie pracować na komputerze w trybie użytkownika administracyjnego, a także posiadać aktualne oprogramowanie antywirusowe
Poziom zagrożenia	**Wysoki**
Opis sposobu usunięcia	Zależny od wersji wirusa. Przykład modyfikacji wprowadzanych w systemie przez opisywane oprogramowanie znajduje się tutaj (w języku angielskim): http://support.kaspersky.com/faq/?qid=208280039
Dodatkowe informacje dla zaawansowanych	Informacje dostępne wyłącznie w języku angielskim (na przykładzie wersji ikh): http://www.viruslist.com/en/viruses/encyclopedia?virusid=21782783

Krótki opis zagrożenia	W ostatnim czasie pojawił się nowy wirus (Mebroot, Mabroot) instalujący się na komputerach użytkownika w sektorze rozruchowym dysku, co powoduje jego automatyczne uruchomienie przy każdym starcie komputera. Wirus ten może służyć to gromadzenia oraz przesyłania intruzowi nazw użytkowników oraz haseł np. do bankowości internetowej. Aby zabezpieczyć się przed infekcją należy w szczególności nie uruchamiać załączników przesłanych poczta e-mail od nieznanych osób i jeśli to możliwe nie pracować na komputerze w trybie użytkownika administracyjnego
Poziom zagrożenia	**Wysoki**
Opis sposobu usunięcia	Szczegółowy opis usunięcia wirusa znajduje się na stronie Banku.

Słownik trudnych pojęć

Wirus komputerowy	Jest to najczęściej prosty program komputerowy, który w sposób celowy powiela się bez zgody użytkownika. Wirus komputerowy w przeciwieństwie do robaka komputerowego do swojej działalności wymaga *nosiciela* w postaci programu komputerowego, poczty elektronicznej itp. Wirusy wykorzystują słabość zabezpieczeń systemów komputerowych lub właściwości systemów oraz niedoświadczenie i beztroskę użytkowników.
Koń trojański	Program, który nadużywa zaufania użytkownika, wykonując bez jego wiedzy dodatkowe, szkodliwe czynności. Konie trojańskie często podszywają się pod pożyteczne programy, takie jak np. zapory sieciowe, wygaszacze ekranu lub udają standardowe usługi systemowe, takie jak np. logowanie. Koń trojański jest trudny do wykrycia i może być poważnym zagrożeniem dla bezpieczeństwa systemu.
Phishing	Oszukańcze pozyskanie poufnej informacji osobistej, jak hasła czy szczegóły karty kredytowej przez udawanie osoby lub strony www godnej zaufania, której te informacje są pilnie potrzebne. Jest to rodzaj ataku opartego na socjotechnice.
Serwer DNS	Usługa działająca w sieciach komputerowych pozwalająca na zamianę adresów łatwych do zapamiętania przez użytkowników komputerów (np. www.ingbank.pl) na adresy IP (193.201.34.65), czyli takie, które są zrozumiałe przez urządzenia tworzące sieć komputerową i jednoznacznie identyfikują dane urządzenie.