Okres	12-19.03.2009

Microsoft Windows	
Krótki opis zagrożenia	W systemach operacyjnych Microsoft Windows wykryto podatność pozwalającą intruzowi na przejęcie kontroli nad komputerem Użytkownika. Aby intruz mógł z sukcesem przejąć kontrolę nad komputerem Użytkowniku, wystarczy że ten uruchomi na swoim komputerze odpowiednio spreparowany plik, przesłany przez intruza za pomocą poczty elektronicznej lub pobrany przez Użytkownika ze strony WWW.
Poziom zagrożenia	**Wysoki**
Opis sposobu usunięcia	Należy zainstalować poprawkę opublikowaną na stronie firmy Microsoft. Poprawka zostanie zainstalowana automatycznie na komputerach ze skonfigurowaną usługą automatycznej aktualizacji. Na komputerach, dla których nie ustawiono usługi automatycznej aktualizacji poprawkę należy pobrać i zainstalować ręcznie według załączonej instrukcji: http://www.microsoft.com/technet/security/bulletin/MS09-006.mspx
Dodatkowe informacje dla zaawansowanych	Informacje dostępne wyłącznie w języku angielskim: http://secunia.com/advisories/34117/

Internet Explorer	
Krótki opis zagrożenia	W przeglądarce Internetowej Internet Explorer w wersji 7 ujawniono lukę związaną z bezpieczeństwem, która może pozwolić osobie nieupoważnionej na przejęcie kontroli nad komputerem Użytkownika. W celu wykorzystania tej luki intruz musi zachęcić Użytkownika do wejścia na odpowiednio przygotowaną stronę www, np. wysyłając wiadomość e-mail z załączonym odsyłaczem (linkiem). Wejście na taką stronę spowoduje, uruchomienie bez wiedzy Użytkownika programu, który może wykonać dowolne operacje na jego komputerze (np. udostępnić usługi, wysłać pocztę)
Poziom zagrożenia	**Wysoki**
Opis sposobu usunięcia	Należy zainstalować poprawkę opublikowaną na stronie firmy Microsoft. Poprawka zostanie zainstalowana automatycznie na komputerach ze skonfigurowaną usługą automatycznej aktualizacji. Na komputerach, dla których nie ustawiono usługi automatycznej aktualizacji poprawkę należy pobrać i zainstalować ręcznie według załączonej instrukcji: http://www.microsoft.com/technet/security/Bulletin/MS09-002.mspx
Dodatkowe informacje dla zaawansowanych	Informacje dostępne wyłącznie w języku angielskim: http://secunia.com/advisories/33845/

Microsoft Windows	
Krótki opis zagrożenia	W systemach operacyjnych Microsoft Windows wykryto podatność pozwalającą intruzowi na przejęcie kontroli nad komputerem Użytkownika. Warunkiem wystarczającym do jej wykorzystania przez intruza jest podłączenie do Internetu komputera niezabezpieczonego przez oprogramowanie typu firewall (np. Windows Firewall)
Poziom zagrożenia	**Wysoki**
Opis sposobu usunięcia	Należy zainstalować poprawkę opublikowaną na stronie firmy Microsoft. Poprawka zostanie zainstalowana automatycznie na komputerach ze skonfigurowaną usługą automatycznej aktualizacji. Na komputerach, dla których nie ustawiono usługi automatycznej aktualizacji poprawkę należy pobrać i zainstalować ręcznie według załączonej instrukcji: http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx
Dodatkowe informacje dla zaawansowanych	Informacje dostępne wyłącznie w języku angielskim: http://secunia.com/advisories/31883/

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 (3.0.7) 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

Internet Explorer	
Krótki opis zagrożenia	W przeglądarkach internetowych Internet Explorer w wersjach 5.x oraz 6.x wykryto podatność przy korzystaniu z serwerów FTP polegającą na możliwości skasowania, pobrania lub zmiany nazwy plików na nim umieszczonych. W wyniku działania intruza, Użytkownik może pobrać z serwera inny plik niż oczekiwał (ze zmienioną nazwą – np. wirus komputerowy).
Poziom zagrożenia	**Średni**
Opis sposobu usunięcia	Na dzień publikacji biuletynu producent nie udostępnił uaktualnienia. Aby ograniczyć możliwość wykorzystania podatności nie należy uruchamiać nieznanych łączy internetowych (zwłaszcza odnoszących się do serwerów FTP), w szczególności przysłanych pocztą e-mail od nieznanych nadawców.
Dodatkowe informacje dla zaawansowanych	Informacje dostępne wyłącznie w języku angielskim: http://secunia.com/advisories/29346/

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.