Jak usunąć złośliwe oprogramowanie z telefonu komórkowego po ataku Trojana Zeus (ZitMo)?

Po ostatnim ataku Trojana Zeus określanego mianem ZitMo (Zeus in the Mobile), który skierowany był na Klientów polskich banków, część zaatakowanych Klientów mogła dokonać instalacji tego złośliwego oprogramowania na swoich telefonach. Komunikacja zainfekowanego telefonu z C&C, czyli centrum zarządzania odbywa się poprzez wiadomości SMS wysyłane i odbierane z określonego numeru telefonu. Atakujący ma możliwość zdalnego zarządzania telefonem. Może on przekierować wszystkie przychodzące wiadomości SMS na jego numer telefonu i na dodatek wiadomości te nie są widoczne na telefonie ofiary.

Jak usunąć złośliwe oprogramowanie z telefonu? Najlepiej wykonać tak zwany „***factory reset***”, czyli przywrócenie ustawień fabrycznych. Można z tym zwrócić się do dostawcy telefonii komórkowej, gdzie wyspecjalizowani pracownicy są w stanie wykonać bezpiecznie taką operację. Należy jednak pamiętać, że takie działanie powoduje usunięcie wszystkich danych zapisanych w telefonie! Osobom, którym takie rozwiązanie nie odpowiada przedstawiamy inne rozwiązanie przygotowane na podstawie artykuł „Halo, tu ZITMO - czyli jak usunąć malware z telefonu” umieszczonego na stronie CERT-u http://www.cert.pl/news/3283.

Instalacja Trojana Zeus była przygotowana na trzy systemy operacyjne wykorzystywane w telefonach Symbian, BlackBerry i Windows mobilny.

Usunięcie Trojana z sytemu Symbian wymaga skorzystania z menedżera aplikacji, gdzie szukamy aplikację „***Certificate*”**. Następnie z menu wybieramy opcję ***Usuń/Odinstaluj*** a następnie potwierdzamy zamiar usunięcia aplikacji ***Tak***. W przypadku pojawienia się ostrzeżenia o konieczności zamknięcia aplikacji odpowiadamy twierdząco ***OK***. W czasie usuwania aplikacji zostaniemy proszeni o podanie hasła, którym cyberprzestępcy zabezpieczyli złośliwą aplikację. CERT podaje, że hasłem jest, **45930** gdy infekcja miała miejsce w lutem 2011 r.

Usunięcie Trojana z systemu BlackBerry wymaga wybrania z menu ***Opcje*** a następnie ***Aplikacje***. Powinna pojawić się aplikacja o nazwie „***sertificate”***. Wybierając właściwości aplikacji mamy możliwość usunięcia niechcianego oprogramowanie poprzez naciśnięcie przycisku ***Usuń***. Zostanie wyświetlone okienko potwierdzające usunięcie gdzie wybieramy ***Usuń***. Po wykonaniu tej operacji Trojan Zeus zostanie usunięty z naszego telefonu.

Usunięcie Trojana z telefonów z systemem Windows mobilny nie jest proste. Złośliwe oprogramowane nie jest widoczne na liście zadań w menadżerze procesów, co znacznie utrudnia usunięcie złośliwego oprogramowania. W tym wypadku najlepiej skorzystać z przywrócenia ustawień fabrycznych.