**Operacja Buhtrap – cel: kradzież pieniędzy z rosyjskich firm**

**Operacja Buhtrap skierowana jest przeciwko rosyjskim firmom, a jej celem jest kradzież danych potrzebnych do wykonania transakcji bankowych. Jak podają eksperci z firmy ESET, zagrożenie pozwala cyberprzestępcom szpiegować systemy komputerowe i kradnie wrażliwe dane m.in. te dotyczące kart używanych jako tokeny sprzętowe potrzebne do logowania podczas korzystania z bankowości online.**

Celem kampanii są oszustwa finansowe. Według ekspertów ESET zagrożenie korzysta z kilku fałszywych certyfikatów firm w Rosji. Wykorzystuje również specjalne techniki, aby uniknąć wykrycia przez rozwiązania do zabezpieczenia komputerów i sieci firmowych. Atak przebiega w następujący sposób: cyberprzestępcy wysyłają do rosyjskich firm wiadomości spamowe z fałszywymi załącznikami takimi jak fałszywe faktury lub umowy z MegaFon – dużym rosyjskim operatorem telefonii komórkowej, próbując w ten sposób skłonić ofiary do otwarcia szkodliwych załączników. Następnie złośliwe oprogramowanie wykorzystuje lukę CVE-2012-0158 w Microsoft Word. Po przeniknięciu do komputera ofiary, odczytuje dane podczas korzystania z tokenów sprzętowych, w trakcie dokonywania transakcji bankowych online.

Narzędzia zainstalowane na komputerze ofiary pozwalają cyberprzestępcom sterować zdalnie komputerem i rejestrować działania użytkownika.

Złośliwe oprogramowanie próbuje uzyskać hasło do konta systemowego użytkownika, a nawet utworzyć nowe. Instaluje również keyloggera (program rejestrujący znaki wprowadzane za pośrednictwem klawiatury), aplikację odczytującą dane zapisywane w schowku oraz skrypt do rejestrowania informacji dotyczących tokenów sprzętowych. Zagrożenie ma również możliwość pobrania i zainstalowania dodatkowego złośliwego oprogramowania.

- Jeden zarażony komputer w sieci pozwala cyberprzestępcom, przy wykorzystaniu różnych narzędzi, dotrzeć do innych maszyn i je zainfekować. Złośliwy program daje cyberprzestępcom możliwość szpiegowania użytkowników i ustalenia, czy tzw. oszukańcza transakcja w banku może zostać zrealizowana – mówi Kamil Sadkowski, analityk zagrożeń firmy ESET.

Eksperci ESET przypuszczają, że kampania ta trwa już ponad rok, a złośliwe oprogramowanie ulega ciągłej ewolucji w celu uniknięcia wykrycia i maksymalizacji zysku. Operacja Buhtrap uświadamia jak ważne są zabezpieczenia przed złośliwym oprogramowaniem.

