**Jak cyberprzestępcy wykorzystują wizerunek Starbucksa**

**Cyberprzestępcy często używają podrobionych wiadomości e-mail do nakłaniania ludzi, by klikali szkodliwe załączniki. Pomagają w tym dwa triki - podszycie się pod znaną firmę (bank, portal społecznościowy itp.) oraz chwytliwy temat.**

Eksperci z Kaspersky Lab wykryli atak wykorzystujący sfałszowane wiadomości od sieci kawiarni Starbucks, w którym cyberprzestępcy zastosowali obydwie wymienione sztuczki.

Z treści wiadomości wykrytych przez ekspertów odbiorca dowiaduje się, że przed kilkoma godzinami jego przyjaciel złożył w Starbucksie zamówienie, by uczcić specjalną okazję. Co ciekawe, tajemniczy przyjaciel chce pozostać anonimowy i pragnie zrobić niespodziankę, jednak w załączniku wiadomości rzekomo znajduje się kompletne przygotowane przez niego menu. Wszystkie wiadomości wykorzystane w ataku są wysyłane z flagą "ważne". Adres nadawcy różni się w każdej wiadomości i najprawdopodobniej jest generowany losowo (zawsze w domenie @google.com lub @yahoo.com).

Załącznik wiadomości zawiera plik wykonywalny .exe, a cyberprzestępcy nie zadali sobie nawet trudu, by ukryć go przy użyciu archiwum lub chociażby podwójnego rozszerzenia. Najprawdopodobniej byli przekonani, że odbiorca będzie tak szczęśliwy po przeczytaniu treści, że bez żadnych podejrzeń będzie chciał zobaczyć załącznik. Niestety załączony plik to już bardzo poważna sprawa, zupełnie niepasująca do luźnej treści i otoczki sfałszowanych e-maili. Jest to szkodliwy program wykrywany przez Kaspersky Lab jako Rootkit.Win32.Zbot.sapu i stanowi modyfikację jednej z najniebezpieczniejszych rodzin szkodliwego oprogramowania - ZeuS. Przy użyciu tego typu szkodliwych aplikacji cyberprzestępcy kradną od użytkowników informacje poufne, takie jak szczegóły dotyczące bankowości internetowej (loginy, hasła, numery kont, adresy e-mail itd.). Wersja ZeuSa wykorzystana w omawianym ataku pozwala cyberprzestępcom dodatkowo zakłócać pracę programów antywirusowych i innych rozwiązań bezpieczeństwa.

„Atak jest swego rodzaju ciekawostką, ponieważ przy dość prymitywnej formie (brak jakiegokolwiek zamaskowania szkodliwego załącznika) niesie ze sobą bardzo poważne zagrożenie w postaci jednej z wersji ZeuSa, który do dziś traktowany jest jako jeden z najniebezpieczniejszych szkodliwych programów” - powiedział **Maciej Ziarek**, ekspert ds. zagrożeń IT, Kaspersky Lab Polska. „Aby ustrzec się tego typu zagrożeniami, należy z rezerwą i czujnością podchodzić do wiadomości zawierających załączniki, szczególnie gdy są to e-maile, których nie oczekujemy".

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky Lab jako źródła.

Wszystkie informacje prasowe Kaspersky Lab Polska są dostępne na stronie <http://www.kaspersky.pl/news>.