Sophos ostrzega przed spamem prowadzącym do witryn infekujących komputery fałszywym oprogramowaniem AV.

Sophos, firma specjalizująca się w technologiach ochrony informacji, ostrzega internautów, aby zachowali szczególną ostrożność wobec szeroko zakrojonej kampanii spam, która ma na celu infekowanie pecetów fałszywym oprogramowaniem antywirusowym. Jeśli odbiorca otworzy pliki HTML dołączone do wiadomości spam, jego przeglądarka zostanie przekierowana do zhakowanej witryny zawierającej złośliwy iFrame (tzw. pływającą ramkę), który umożliwia uruchomienie fałszywego oprogramowania antywirusowego.

E-maile przechwycone przez SophosLabs mają różne tematy, począwszy od opłat za karty kredytowe na darmowych zdjęciach z wakacji skończywszy.

Tematy zainfekowanych maili:

* Pozwolenie na parking i / lub potwierdzenie zamówienia karty korzyści
* Zapraszam do obejrzenia moich zdjęć!
* Potwierdzenie spotkania
* Twój rachunek elektroniczny jest gotowy
* Twoje zamówienie VistaPrint zostało potwierdzone

"Scam tego typu może być bardzo skuteczny w przekazywaniu dochodów bezpośrednio w ręce hakerów, dlatego wszyscy musimy mieć się na baczności", powiedział Graham Cluley, starszy konsultant ds. technologii w Sophos. "Ataki mają na celu skłonienie ludzi do płacenia za coś, czego w ogóle nie zamawiali. Gdy komputer użytkownika zostanie zainfekowany fałszywym antywirusem, oprogramowanie będzie kontynuowało bombardowanie użytkownika zmyślonymi komunikatami ostrzegawczymi, zachęcając do zapłaty lub zainstalowania kolejnego złośliwego oprogramowania w celu rzekomego usunięcia zagrożeń z komputera. Jeśli użytkownicy są zaniepokojeni o bezpieczeństwo swoich maszyn, powinni się udać bezpośrednio na właściwą stronę poświęconą bezpieczeństwu IT."

Sophos wykrywa złośliwe załączniki e-mail jako Troj / JSRedir-CH, i fałszywy atak antywirusowy jako Mal / FakeAV-EI.

Ataki fałszywego oprogramowania antywirusowego zazwyczaj są bardzo efektywne, jako że hakerzy wykorzystują ludzką naiwność, słabo zabezpieczone strony i wypróbowane triki polegające na straszeniu użytkowników problemami związanymi z bezpieczeństwem na ich komputerze. To wszystko może doprowadzić do pobrania szkodliwego oprogramowania i przekazania hakerom poufnych danych.

Więcej informacji można znaleźć na blogu Grahama Cluleya:
http://www.sophos.com/blogs/gc/g/2010/08/25/malicious-spammers

Wideo przedstawiając dalsze informacje o atakach fałszywych programów antywirusowych można znaleźć na kanale Sophos w serwisie YouTube:
http://www.youtube.com/watch?v=2DzBdhqB73I

Sophos