Cyberprzestępcy dzięki stronie www zaprojektowanej na wzór interfejsu systemu Windows, nieświadomych użytkowników naciągają na zakup fałszywego antywirusa. Niebezpieczna witryna na kilku kolejnych stronach przedstawia proces rzekomego skanowania komputera, ilość obecnych w systemie infekcji oraz w końcowym etapie pobranie groźnego pliku z fałszywym antywirusem.

Łukasz Nowatkowski dyrektor techniczny **G Data Software**: „Cyberprzestępcy do perfekcji opanowali metody, pozwalające na zmanipulowanie potencjalnej ofiary. Powyższy atak przede wszystkim bazuje na przyzwyczajeniu użytkownika do interfejsu Windowsa. Przekierowany na tak przygotowaną stronę, **nieświadomy ataku Internauta** bardzo często wpada w panikę i akceptuje warunki postawione przez internetowych złodziei. Odruchowo wykonuje polecania zawarte w wyskakujących okienkach, co ostatecznie prowadzi do podania nr konta bankowego, hasła lub po prostu przelewu pieniędzy na wskazane konto. Powodzenie ataku naturalnie zależy od świadomości Internatów na obecne w sieci zagrożenia oraz zastosowane programy ochronne.

Aby minimalizować ryzyko ataków konieczne jest stosowanie pakietów antywirusowych wyposażonych w dodatkowe moduł takie jak firewall, **AntiPhishing, AntiSpam, WebFilter** oraz moduł skanowania zawartości http.

Kolejne kroki ataku:
I krok: Komunikat po wejściu na niebezpieczną stronę

II krok: Wizualizacja rzekomego procesu skanowania

III krok: Komunikat o obecności infekcji w Twoim systemie i polecenie instalacji fałszywego pliku

IV krok: Kolejny komunikat podkreślający rangę zagrożenia i powagę sytuacji

IV krok: Propozycja pobrania groźnego pliku, który zainfekuje nasz system groźnym malware i proponować będzie zakup fałszywego antywirusa

G Data Software