W weekend klienci Lenovo zostali zaskoczeni w najmniej spodziewanym momencie – podczas pobierania sterowników ze strony chińskiego producenta, tysiące Internautów otrzymało również pasażera na gapę – konia trojańskiego Bredolab. Wielu z nich wciąż o tym nie wie.

Hakerzy odkryli piętę achillesową Lenovo

Lenovo jest kolejnym przykładem na to, jak nieustępliwi stają się hakerzy. Nawet takie olbrzymy jak ten chiński gigant nie są całkowicie odporne na ataki spragnionych pieniędzy cyberprzestępców. Dla wielu Internautów ściągających ze strony Lenovo sterowniki, niedziela 20 czerwca okazała się pechowa, bowiem tego dnia po południu strona zaczęła rozprzestrzeniać złośliwy skrypt, który przekierowywał użytkowników do domeny o nazwie volgo-marun.cn. Tutaj następowała automatyczna instalacja złośliwego pliku .exe na dysku twardym Internautów. Wirus jest nową odmianą konia trojańskiego Bredolab.

„Firmy muszą być bardzo czujne i od razu reagować na takie zagrożenia, w końcu od tego zależy ich reputacja na rynku" – mówi Tomasz Zamarlik z polskiego oddziału G Data Software. „Każda firma powinna być przygotowana na ewentualność takiego ataku i - co za tym idzie - mieć przygotowany odpowiedni plan reagowania kryzysowego. Sytuacje kryzysowe takie jak ta zdarzają się niezmiernie rzadko, lecz w skali długoterminowej szkody potrafią być bardzo duże, szczególnie w przypadku dużych korporacji takich jak Lenovo. Wszystkim, którzy odwiedzili witrynę Lenovo, zalecamy przeskanowanie komputera programem antywirusowym ze zaktualizowaną bazą sygnatur wirusów".

Internet Explorer najbardziej podatny

Cyberprzestępcy odpowiedzialni za atak umieścili w kodzie strony specjalną komendę iframe. Uruchamia ona skrypt, instalujący się automatycznie na komputerach Internautów odwiedzających witrynę. Po załadowaniu na komputer, wirus kopiuje się do folderu %Programs%Startupmonskc32.exe.

Użytkownicy przeglądarek Chrome oraz Firefox mogą spać spokojnie, bowiem próba wejścia na oszukańczą witrynę kończy się wyświetleniem napisu, ostrzegającego, iż strona została sklasyfikowana jako niebezpieczna. Trochę mniej szczęścia mają internauci korzystający z Internet Explorer, bowiem to głównie na nią nacelowany był ów atak. Hakerzy celowo wykorzystali luki w zabezpieczeniach Internet Explorera. W chwili pojawienia się zagrożenia, radziło sobie z nim tylko 10 spośród 40 najbardziej popularnych antywirusów. Obecnie firmy pracują nad aktualizacją swoich baz sygnatur w celu ochrony przed Bredolab.

Teraz strona Lenovo nie stanowi już zagrożenia. Lenovo usunęło ze strony złośliwy kod, lecz mimo to nie wydało jeszcze w tej sprawie żadnego oświadczenia. Blog firmowy też w tej sprawie milczy.

Someday Interactive