Sophos, firma specjalizująca się w technologiach ochrony informacji, udostępnił dziś darmowe narzędzie do ochrony przed luką Windows w obsłudze plików skrótu .LNK, która pozwala na automatyczny rozruch niebezpiecznego kodu w przypadku, gdy przeglądamy pamięć USB z poziomu Eksploratora Windows.

Sophos Windows Shortcut Exploit Protection Tool zapewnia ochronę przed groźną dziurą we wszystkich wersjach systemu Windows. Exploit, znany także pod nazwą CPLINK, umożliwia skrótom (plikom .lnk) uruchomienie na komputerze złośliwego oprogramowania - bez jakiejkolwiek interakcji z użytkownikiem.

Darmowe narzędzie Sophos, dostępne do pobrania ze strony http://www.sophos.com/shortcut, przechwytuje pliki skrótów zawierające exploit, ostrzegając przed wykonywalnym kodem. Oznacza to koniec zagrożeń ze strony złośliwego kodu, wykorzystującego lukę .lnk.

"Jak dotąd widzieliśmy robaki Stuxnet i Dulkis, a także trojana Chymin usprawniającego rozprzestrzenianie i infekowanie komputerów. Stuxnet trafił na nagłówki, ponieważ jest wycelowany w systemy Siemens SCADA, które sterują krytyczną infrastrukturą krajową, taką jak elektrownie. Należy jednak pamiętać, że zagrożeni rootkitem są wszyscy użytkownicy," powiedział Graham Cluley, starszy konsultant ds. technologii w Sophos. "Szczegóły o tym, jak wykorzystać tę lukę bezpieczeństwa są dostępne w sieci, a to oznacza, że hakerzy bez najmniejszych trudności mogą ją wykorzystać do kolejnych ataków."

Sophos udostępnił nagranie YouTube demonstrujące, jak narzędzie przechwytuje atak:
http://www.youtube.com/watch?v=Gucn5xWZ1m8

"Nikt nie wie kiedy Microsoft wyda stosowną łatę dla tej luki bezpieczeństwa," ciągnął dalej Cluley. "Darmowe narzędzie Sophos może działać na równi z każdym oprogramaniem antywirusowym, zapewniając podstawową ochronę przed exploitem. W przeciwieństwie do propozycji Microsoft, nie wyłącza wyświetlania ikon skrótów, co oznacza mniej stresów podczas pracy z komputerem."

Klienci Sophos są już objęci ochroną przed exploitem wykrywanym jako Exp/Cplink-A lub Troj/Cplink.

Więcej informacji oraz zrzuty ekranu darmowego narzędzia Sophos, można znaleźć na blogu Grahama Cluleya pod adresem:
http://www.sophos.com/blogs/gc/g/2010/07/26/shortcut-exploit-free-tool

Sophos