Eksperci z Sophos, firmy specjalizującej się w technologiach ochrony informacji, ostrzegają użytkowników komputerów przed rootkitem, który samoczynnie instaluje się z pamięci USB, nawet gdy funkcja autouruchamiania jest wyłączona.

Rootkit W32/Stuxnet-B wykorzystuje lukę Windows w obsłudze plików skrótu .LNK, która pozwala na automatyczny rozruch niebezpiecznego kodu w przypadku, gdy przeglądamy pamięć USB z poziomu Eksploratora Windows. Rootkit instaluje się bez wiedzy użytkownika i sprytnie maskuje swoją obecność.

Jak to działa, doskonale widać na przygotowanym przez Sophos filmie YouTube:
http://www.youtube.com/watch?v=1UxN7WJFTVg&feature=player_embedded

"Zagrożenia takie jak doskonale znany już robak Conficker, w przeszłości rozprzestrzeniały się bardzo skutecznie za pośrednictwem USB, ale po części zostały zneutralizowane poprzez wyłączenie funkcji autoodtwarzania. Istnieje ryzyko, że więcej szkodliwego oprogramowania wykorzysta lukę odnalezioną przez twórców rootkita Stuxnet", wyjaśnił Graham Cluley, starszy konsultant ds. technologii w Sophos. "Luka jest wciąż analizowana przez specjalistów z branży security, ale pojawiają się bardzo niepokojące sygnały, że złośliwy kod może zainfekować dane specyficzne dla systemów SCADA Siemens - oprogramowania sterującego krytyczną infrastrukturą krajową."

Co ciekawe, podejrzane pliki sterownika posiadały podpis cyfrowy Realtek Semiconductor Corp, znanego dostawcy sprzętu komputerowego.

"Ważne jest, aby nie przesadzić z reakcją na to zagrożenie, jako że exploit został niedawno wykryty, a specjaliści od bezpieczeństwa nie ustalili jeszcze ryzyka dla systemów SCADA. Ale sam fakt, że systemy SCADA są w ogóle zaangażowane oznacza, że każdy będzie przyglądał się sprawie z bliska. Oczy będą też skierowane w kierunku firmy Microsoft, aby zobaczyć, jaka będzie reakcja na to, co wydaje się być kolejną luką w ich kodzie, którą sprytnie wykorzystali hakerzy."

Po więcej informacji i pełny opis działania ataku zapraszamy na blog Chestera Wisniewskiego, pod adresem:
http://www.sophos.com/blogs/chetw/g/2010/07/15/windows-day-vulnerability-shortcut-files-usb/
http://www.sophos.com/blogs/chetw/g/2010/07/16/windows-day-attack-works-windows-systems/

Sophos