W czerwcu groźny robak o nazwie Stuxnet zainfekował systemy informatyczne kilku dużych korporacji. Kilka dni temu badacze ds. bezpieczeństwa dokonali przełomowego odkrycia: prawdziwym celem Stuxnet był najprawdopodobniej irański reaktor atomowy w Bushehr.

Złośliwe, ale jednak arcydzieło
Stuxnet od razu po pojawieniu się został nazwany najbardziej wyrafinowanym spośród istniejących wirusów. Żaden inny program nie wykorzystywał czterech nieznanych wcześniej luk systemowych na raz. Stuxnet rozprzestrzenił się szczególnie intensywnie na terenie Indii, Indonezji oraz Iranu. O jego niszczącym potencjale świadczy zaś fakt, iż jego łupem padło aż 60 procent wszystkich komputerów w Iranie.

Analiza złośliwego kodu, dane o nieprawdopodobnie dużej liczbie zarażonych komputerów na terenie Iranu oraz fakt, iż w tym samym czasie nagle przełożono na inny termin otwarcie elektrowni atomowej w mieście Bushehr, doprowadziły niemieckiego naukowca Ralpha Langnera do wniosku, iż Stuxnet został stworzony w celu zniszczenia konkretnej irańskiej elektrowni. Świadczy o tym natura samego programu, który pozostaje uśpiony do momentu, aż trafi na podatny grunt. Wtedy uaktywnia się powodując szkody. Takim sygnałem do aktywacji jest rozpoznanie przez Stuxnet maszyn z oprogramowaniem marki Siemens, często używanym w przemyśle. Tym samym Stuxnet i jego złośliwy kod pozwalają zdalnie przejąć kontrolę nad systemami informatycznymi w zakładach przemysłowych.

Atak motywowany politycznie?
„Przeprowadzenie takiego ataku wymagało wielu specjalistycznych umiejętności" – mówi Langner. „Weźmy pod uwagę wszystkie wykorzystywane luki, ukradzioną przez twórców Stuxnet dokumentację potrzebną do zaprojektowania ataku, itp. Zostało to wykonane przez wysoko wykwalifikowany zespół ekspertów, w którym przynajmniej część osób posiadała wiedzę na temat działania informatycznych systemów kontrolnych w przemyśle. To nie była robota domorosłego hakera siedzącego w piwnicy swoich rodziców. Wydaje mi się, że rodzaj zasobów niezbędnych do przeprowadzenia takiego ataku wskazuje na udział konkretnego państwa".

Na swojej stronie Langner pisze, że przestawione przez niego wnioski mają charakter spekulacji i nie istnieją niezbite dowody na to, że jest dokładnie tak jak mówi. Langner nie ma stuprocentowej pewności co do celu ataku, jak i co do tego, jakich zniszczeń mógłby dokonać.

Prawdziwy przełom
Stuxnet stanowi prawdziwy przełom w podejściu do kwestii bezpieczeństwa – komentuje Łukasz Nowatkowski z G Data Software. Program okazał się dużo bardziej niebezpieczny niż się na początku spodziewano. Jak pokazują wydarzenia ostatnich miesięcy, Internet coraz częściej staje się środkiem ataków motywowanych politycznie. Stuxnet jest pierwszym tak wyraźnym sygnałem, że ewentualna wojna w cyberprzestrzeni jest coraz bliższym scenariuszem. Niedawne ataki hakerów na Google, na infrastrukturę informatyczną Estonii czy też na stronę partii szwedzkich demokratów wpisują się w ten sam wątek. Jest to bodziec dla wielkich firm oraz instytucji, aby dołożyły wszelkich starań na rzecz poprawy bezpieczeństwa".

1.Wiadomości na temat Stuxnet, że niedawno się pojawił, od razu wywołał ogromne zainteresowanie specjalistów, bo…, został ochrzczony…, ale najnowsze badania wykazały, że jego celem, jest uśpiony dopóki…,
2.Oprogramowanie Siemens, SCADA, wypowiedź naukowców, trzeba szybko wypracować odpowiednie środki zaradcze na tego typu …, wyszukane oprogramowanie, zbudowane przez....,
3.Komentarz G Data: coraz częściej spotyka się ataki motywowane politycznie oraz w wymierzone w konkretne cele: szwedzka partia SD, RIAA, Eneken Tikk i cybernetyczna wojna

Someday Interactive