Mandiant wyśledził chińską jednostkę wojskową odpowiedzialną za cyberataki

Najnowszy raport firmy Mandiant omawia działania kolejnej grupy cyberprzestępczej z Chin, tym razem bez wątpienia powiązanej z chińską armią PLA lub będącej jej przykrywką.

Marcin Marciniak, IDG News Service
20.02.2013, godz. 16:33

Firma Mandiant, specjalizująca się w zagadnieniach bezpieczeństwa informacji opublikowała raport, w którym informuje, że wyśledziła działalność grupy hakerskiej o nazwie APT1. Grupa ta prowadziła ciągłe i zaawansowane ataki technologiczne klasy APT (ang. Advanced Persistent Threat) przeciw różnym podmiotom. Wspomniana grupa charakteryzuje się nadzwyczaj silną aktywnością w cyberprzestrzeni, posiada również możliwości i zasoby, które wskazują na bardzo prawdopodobne wsparcie instytucji rządowych ChRL.

Działania podjęte w celu lokalizacji i identyfikacji grupy hakerskiej doprowadziły na ślad jednostki wojskowej chińskiej armii PLA oznaczonej "Jednostka 61398", która charakteryzuje się podobną misją, zbliżonymi możliwościami oraz zasobami. Dodatkowo wspomniana jednostka wojskowa znajduje się w tym samym precyzyjnie określonym obszarze, skąd pochodziły ataki grupy APT1. Specjaliści mówią, że jednostka 61398 jest zlokalizowana w budynku o powierzchni 12 tys mkw, znajdującym się przy Datong Road w Szanghaju. Oficjalnie działalność tej jednostki wojskowej jest owiana tajemnicą, ale specjaliści firmy Mandant uważają, że jej zadaniem jest przeprowadzanie ataków na systemy komputerowe.

Czy grupa hakerska jest przykrywką chińskiej armii?
Podobieństwa między jednostką wojskową a grupą określaną APT1 nie ograniczają się do zwykłych podejrzeń. Grupa ta posiada zastanawiająco złowieszczą historię działania - specjaliści Mandianta obserwowali przejęcie kontroli nad IT w 141 firmach z 20 głównych branż. Aż 87% z tych ataków kierowano przeciw anglojęzycznym firmom określanym przez chiński rząd jako strategiczne.

Ministerstwo Spraw Zagranicznych ChRL twierdzi, że Chiny przeciwstawiają się działaniom hakerskim i wspierają regulacje zabraniające ataków cybernetycznych. Rząd chiński wielokrotnie protestował przeciw zarzutom o organizację ataków kierowanych przeciw agencjom prasowym oraz redakcjom różnych czasopism.

Własne narzędzia do kradzieży informacji
Grupa APT1 wykorzystywała narzędzia niespotykane nigdzie indziej, w tym

organizację ataków kierowanych przeciw agencjom prasowym oraz redakcjom różnych czasopism.

Własne narzędzia do kradzieży informacji
Grupa APT1 wykorzystywała narzędzia niespotykane nigdzie indziej, w tym dwa programy przeznaczone do kradzieży wiadomości e-mail (GETMAIL oraz MAPIGET, przeznaczone do kradzieży z zasobów serwerów Microsoft Exchange). Po uchwyceniu przyczółków w sieci ofiary, infrastruktura IT była dokładnie penetrowana, kradziono dokumentację technologiczną, opisy własnościowych procesów, wyniki testów prototypów, plany biznesowe, dokumenty z wyceną produktów i usług, umowy o współpracy oraz listy kontaktów zarządu.

O zagadnieniach związanych z grupami hakerskimi z ChRL można przeczytać także w artykule Chińscy hakerzy - prawdy i mity, CW 29/2011.

Drukuj