Amerykańscy dyplomaci zarzucili chińskim firmom ochroniarskim powiązanym z wojskiem, rekrutowanie hakerów. Wśród zatrudnionych miała znaleźć się także grupa odpowiedzialna za stworzenie robaka komputerowego Blaster. Według doniesień WikiLeaks, chińskie firmy posiadają dostęp do kodu źródłowego systemu Microsoft Windows.

Komunikat dotyczący bezpieczeństwa, wydany przez Departamentu Stanu w USA 29. czerwca 2009 roku, informował, że pekińska firma ochroniarska Topsec od czerwca 2002 do marca 2003 zatrudniała znanych chińskich hakerów. Jeden z przestępców internetowych został zidentyfikowany jako Lin Yong pseudonim „Lion", pełnił on funkcję starszego inżyniera do spraw bezpieczeństwa, odpowiadał za zarządzanie służbami bezpieczeństwa i szkoleniami.

Topsec jest czołowym chińskim dostawcą systemów bezpieczeństwa, szkoleń i rozwiązań wspierających Chińską Armię Ludowo – Wyzwoleńczą (PLA). Prezes i założyciel firmy He Weidong powiedział w wywiadzie, że częściowo finansował ją rząd chiński.

Inna firma z siedzibą w Pekinie – Venustech korzystała z usług grupy hakerów o nazwie XFocus. Przestępcy w połowie 2003 roku napisali robaka komputerowego Blaster. W lipcu 2003, kilka tygodni po odkryciu luk w Microsoft WIndows, XFocus stworzyła kod programu, który stał się następnie podstawą Blastera. Amerykański nastolatek Jeffrey Lee Parson wykorzystał wiedzę grupy i stworzył inną wersję Blastera, który nazwał „XFocus"- na cześć twórców. Parsona aresztowano, oskarżony przyznał się do winy i został skazany na osiemnaście miesięcy więzienia.

Rząd chiński wspiera działania firm łączonych z hakerami, w ramach narodowego projektu sieci badań naukowych. Kilka firm w Chinach, które podpisały umowy z amerykańskim deweloperem w 2003 r., ma teraz dostęp do kodu źródłowego Windows, tym samym ma do niego dostęp rząd Chin.

„Amerykańscy badacze i analitycy systemów bezpieczeństwa przypuszczali już jakiś czas, że wojsko chińskie ma szerokie możliwości jeśli chodzi o działania w sieci. Podejrzewali nawet, że Chińczycy powołali specjalne jednostki militarne odpowiedzialne za cyber ataki na wroga" - dodaje Łukasz Nowatkowski, ekspert ds. bezpieczeństwa IT z firmy G Data Software.

G Data Software