Dwóch badaczy postanowiło zbadać, kim tak naprawdę są słynni rosyjscy hakerzy, będący od dawna zmorą Interentu. „Cały cyberprzestępczy biznes w Rosji obraca się wokół wyłudzania pieniędzy od osób z Zachodu" – mówi Fiodor Jaorczkin z instytutu InfraGard.

Odkrycia badaczy zupełnie zaskakują

Fiodor Jaroczkin oraz „Grugq", badacze z amerykańskiego instytutu do spraw bezpieczeństwa narodowego InfraGard, wniknęli na okres sześciu miesięcy w środowisko rosyjskich hakerów. Cel badania był prosty: dowiedzieć się kim są ludzie, którzy stoją za światowymi atakami hakerskimi, w jaki sposób działają i co jest głównym motywem skłaniającym ich do tworzenia i rozprzestrzeniania złośliwych programów. W tym celu dołączyli do kilkunastu rosyjskojęzycznych cyberprzestępczych forów, aby śledzić aktywność ich użytkowników. Dostęp do nich jest całkowicie wolny, trzeba jednak rozumieć cyberprzestępczy slang.

Odkrycia badaczy zupełnie zaskakują. Okazuje się, że sprawy mają się zupełnie odwrotnie w relacji do tego, co zwykło się sądzić o rosyjskich hakerach. Większość złośliwych skryptów wcale nie wychodzi z rąk wysoce zorganizowanych siatek przestępczych, ani też rządowych agencji, lecz tworzona jest przez zwykłych amatorów, o większym lub mniejszym poziomie zdolności informatycznych. Wielu z nich jest po prostu studentami, którzy znaleźli sposób na łatwy zarobek. Cały cyberprzestępczy biznes w Rosji obraca się wokół wyłudzania pieniędzy od osób z Zachodu. Jak mówi Jaroczkin: „Przeciętny rosyjski student przekonany jest, że wszyscy mieszkający na Zachodzie opływają w gotówkę, toteż nie ma skrupułów, aby takiej osobie odebrać część pieniędzy, których ma przecież pod dostatkiem".

Duże firmy powinny ciągle mieć się na baczności

Ponadto, przytłaczająca część zaatakowanych to wcale nie duże międzynarodowe korporacje, lecz pojedyncze osoby prywatne. „Jest to dobra wiadomość dla dużych przedsiębiorstw, lecz nie znaczy to, że mogą one teraz zaniechać wysiłków na rzecz bezpieczeństwa swoich sieci – komentuje Łukasz Nowatkowski z G Data Software. Zagrożenie istnieje nadal, gdyż często osoby prywatne przynoszą ze sobą zainfekowane pliki z komputerów domowych do pracy. Tego typu pośrednia forma ataku może wyrządzić takie same szkody jak bezpośredni atak na infrastrukturę informatyczną przedsiębiorstwa."

Cyberprzestępcze fora zdołały również wypracować system oceny podobny do znanego nam z wielu internetowych aukcji. Polega to na tym, że za każdym razem, gdy ktoś kupuje od hakera plik z wykradzionymi numerami kart kredytowych, kupujący wystawia sprzedawcy ocenę, zależną od tego, ile z nich tak naprawdę działało i na ile jest z transakcji zadowolony. Jeśli zdarzy się, że duża ich cześć jest do niczego, to nie dzieje się nic, ponieważ sprzedający cyberprzestęcy oferują gwarancję i wadliwy towar jest natychmiast zastępowany nową serią numerów kart.

Badacze doszli do wniosku, że głównym motywem, jakim kierują się Ci drobni cyberprzestępcy jest po prostu chęć szybkich zysków. Nie ma w tym żadnej ideologii, jest za to czysta kalkulacja. Dla zainteresowanych istnieje też możliwość zarabiania na cyberprzestępczych programach partnerskich – im więcej użytkowników napędzą na złośliwą stronę partnerzy, tym większe otrzymują wynagrodzenie.

Wyniki badania przedstawione zostały w lipcu na forum konferencji Hack In The Box w Amsterdamie, omawiającej sprawy bezpieczeństwa IT.

Someday Interactive