**Hakerzy syryjskiej armii elektronicznej oskarżeni o kradzież danych i konspirację.**

**Dwóch mężczyzn zostało oskarżonych o rzekomy udział w hakerskich kampaniach skierowanych przeciwko krytykom reżimu Baszara al-Assada w Syrii.**

**Mężczyźni - Ahmad Umar Agha (znany również jako "Pro") i Firas Dardar ("Cień") - zostali oskarżeni przez sąd federalny Virginii o konspirację kryminalną i kradzież tożsamości.**

Agha i Dardar są obywatelami Syrii, a ich domniemane ataki zostały popełnione pod sygnaturą słynnej "Syryjskiej Armii Elektronicznej".

Jednym z najbardziej znanych ataków prowadzonych przez Syryjską Armię Elektroniczną było włamanie na konto Twitter Associated Press w 2013 roku i opublikowanie wiadomości, że w Białym Domu nastąpiła eksplozja, a prezydent Barack Obama został ranny.

Ten fałszywy alarm sprawił, że na giełdzie powstały nagłe zachwiania cen, pozwalające na upłynnienie 136 miliardów dolarów z Dow Jones.

Innymi ofiarami Syryjskiej Armii Elektronicznej są Forbes, Microsoft, Facebook, CNN, The Guardian, The Telegraph i Washington Post oraz wiele innych znanych firm.

Chociaż wiele ataków na media społecznościowe wydawało się być bardziej po to, aby publikować żartobliwe posty, niż stwarzać niebezpieczeństwo, nie znaczy to, że wszystkie ich skutki były całkowicie niegroźne.

Na przykład Syryjska Armia Elektroniczna włamywała się do systemów komputerowych międzynarodowych firm w celu kradzieży informacji oraz - w niektórych przypadkach - wymuszenia dużych sum pieniędzy.

„W typowym ataku, użytkownik zostaje wprowadzony w błąd starannie spreparowanym e-mailem phishingowym w celu kradzieży danych logowania”, komentuje Mariusz Politowicz, inżynier techniczny Bitdefender w firmie Marken, „możemy zauważyć, że ataki phishingowe są coraz bardziej zaawansowane i wykorzystują wyrafinowane metody socjotechniczne. Co mogą zrobić firmy aby ich uniknąć? Należy się upewnić, że pracownicy posiadający dostęp do poczty e-mail lub CMS naszej witryny, używają uwierzytelniania dwuskładnikowego, aby zmniejszyć prawdopodobieństwo phisingu. Odnośnik phishingowy może również prowadzić do pobrania oprogramowania szpiegowskiego, keyloggera lub trojana” - dodaje.

Jeśli kradzież danych uwierzytelniających użytkownika zakończy się powodzeniem, hakerzy używają nazwy użytkownika i hasła do zalogowania się, po czym mogą skompromitować konta w mediach społecznościowych, zlikwidować witryny internetowe, stworzyć zamieszanie w DNS lub rozpocząć dalsze ataki phishingowe.

Ahmad Umar Agha i Firas Dardar byli od dawna poszukiwani przez służbę FBI. Zostali wpisani na listę Cyber ​​Most Wanted FBI w 2016 r. Zaoferowano nawet nagrodę w wysokości 100 000 USD za informacje, które doprowadzą do ​​ich aresztowania.

Nie wyobrażajmy sobie jednak, że dwaj podejrzani hakerzy będą bronić się w sądzie w USA w najbliższym czasie. Obaj uważają że są niewinni i nikt nie zamierza ich aresztować, dlatego nadal przebywają w Syrii. Z tego powodu na razie wydają się być poza zasięgiem władz USA.

dź treść