Tajna cybermisja na Ukrainie

10 marca 2022

Pomimo trwającej od 2 tygodni rosyjskiej agresji, internet na Ukrainie ciągle działa. Zaskakiwać może, że Kreml, bardzo chętnie korzystający z cyberataków, dotychczas go nie wyłączył. Okazuje się, że na kilka miesięcy przed rosyjską napaścią Stany Zjednoczone zorganizowały tajną misję, w ramach której amerykańscy eksperci pomogli zabezpieczyć ukraińską cyberprzestrzeń.

Od kilku lat USA pomagają Ukrainie zabezpieczyć sieci komputerowe. Na Ukrainie pracują żołnierze US Army's Cyber Command, niezależni specjaliści opłacani przez Waszyngton eksperci oraz eksperci z firm IT. Jednak pod koniec ubiegłego roku wysiłki te zostały wyraźnie zintensyfikowane i skupione na konkretnym zagrożeniu. Media donoszą, że w październiku i listopadzie liczba amerykańskich ekspertów pracujących na Ukrainie uległa nagłemu zwiększeniu. Mieli oni przygotować ukraińskie sieci na spodziewane ataki w obliczu coraz bardziej prawdopodobnej wojny. Misja najwyraźniej się powiodła, gdyż Ukraina ciągle ma łączność ze światem.

Okazuje się na przykład, że agresor chciał sparaliżować ukraińskie koleje. Amerykanie znaleźli w sieci komputerowej ukraińskich kolei państwowych malware, które pozwalało napastnikom na jej wyłączenie poprzez skasowanie kluczowych plików.

Niestety, podobne oprogramowanie zostało też zainstalowane – czego Amerykanie nie zauważyli – na komputerach straży granicznej i przeprowadzony cyberatak zwiększył chaos na granicy ukraińsko-rumuńskiej.

Amerykanie nie ograniczyli się do działań informatycznych. Wiadomo, że we współpracy z ukraińskimi firmami odpowiadającymi za ukraińską sieć szkieletową, budowali

dodatkową infrastrukturę, która miała zabezpieczyć najważniejsze potencjalne cele rosyjskich cyberataków.

W ostatnim tygodniu lutego na sieć ukraińskiej policji i innych agend rządowych przeprowadzono silny atak DDoS. Wiadomo, że w ciągu kilku godzin Amerykanie skontaktowali się z Fortinetem, kalifornijską firmą sprzedającą wirtualne maszyny przeznaczone do przeciwdziałania takim atakom, zdobyli fundusze, w zaledwie 15 minut uzyskali zgodę Departamentu Handlu na transfer technologii i zainstalowali oprogramowanie Fortinetu na komputerach policji. Atak został odparty w ciągu ośmiu godzin od rozpoczęcia.

Ataki hakerskie są często kierowane przeciwko komercyjnemu oprogramowaniu, a znaczną jego część produkują amerykańskie i europejskie firmy, które teraz poświęcają część swoich zasobów na pomoc Ukrainie. Wiadomo na przykład, że microsoftowe Threat Intelligence Center od wielu miesięcy chroni ukraińskie sieci przed rosyjskimi atakami. Jeszcze 24 lutego, na kilka godzin przez rosyjską napaścią, inżynierowie Microsoftu wykryli nowe szkodliwe oprogramowanie i dokonali jego inżynierii wstecznej. W ciągu trzech godzin udało im się stworzyć łatę i ostrzec ukraińskie władze przed licznymi atakami na wojskowe sieci. O sytuacji powiadomiono Biały Dom, który poprosił Microsoft, by ten podzielił się szczegółami z Polską innymi krajami europejskimi w obawie, że i ich sieci mogły zostać zarażone tym samym kodem. Menedżerowie Microsoftu przyznają, że jeszcze kilka lat temu takie działania zajęłyby całe tygodnie lub miesiące. Teraz wystarczają godziny.

Amerykańska prasa donosi, że niektórzy z wysokich rangą menedżerów Microsoftu uzyskali szybko certyfikaty bezpieczeństwa i biorą teraz udział w spotkaniach National Security Agency (NSA) i Cyber Command.

Eksperci obserwujący rozwój wydarzeń w ukraińskiej cyberprzestrzeni, są zdumieni tym, co widzą. Rosja zdobyła sobie reputację kraju, który potrafi skutecznie przeprowadzić

silne niszczące cyberataki. Tymczasem od czasu napaści na Ukrainę nie obserwuje się wzmożenia tego typu aktywności. Nie wiadomo, co się stało. Być może Rosjanie próbowali, ale dzięki wzmocnieniu ukraińskiej infrastruktury napotkali na trudności. Na pewno próbowali przejąć facebookowe konta wysokich rangą ukraińskich oficerów i znanych osobistości, by rozpowszechniać fałszywe informacje. Na kontach tych pojawiły się filmy z rzekomo poddającymi się ukraińskimi oddziałami. Facebook zablokował zaatakowane konta i poinformował ich właścicieli.

Nie można wykluczyć, że Kreml zlekceważył siłę ukraińskiej cyberprzestrzeni podobnie, jak zlekceważył ukraińską armię.

Autorstwo: Mariusz Błoński
Na podstawie: NYTimes.com
Źródło: KopalniaWiedzy.pl