Cyberdefence 24

aut. Andrzej Kozłowski 04.10.2017

CHIŃCZYCY STOJĄ ZA ATAKIEM NA EQUIFAX? [KOMENTARZ]

Trwające śledztwo w sprawie włamania do firmy Equifax prowadzi do zaskakujących wniosków. Eksperci podejrzewają, że za atakiem stoi aktor państwowy, a działania są bardzo podobne do operacji z 2015 roku wymierzonych w Office of Personal Management. Może to oznaczać, że sprawcą są Chiny.

Pierwsze wnioski wynikające ze śledztwa wskazują na wykorzystanie wielu zespołów hakerskich, które używały do swoich działań narzędzi, wskazujących na chińskie pochodzenie. Eksperci jednak przestrzegają przed wyciąganiem pochopnych wniosków. Grupy hakerów z Państwa Środka wielokrotnie w przeszłości dokonywały wielu włamań kradnąc praktycznie wszystko od danych medycznych po wojskowe sekrety. Eksperci wskazują na szereg podobieństw z włamaniem do jednej z największej firmy zajmującej się ubezpieczeniami Anthem, a wcześniej do U.S. Office of Personal Management. Oba wydarzenia przypisuję się chińskim hakerom.

Cała operacja rozpoczęła się 6 marca, kiedy firma Apache opublikowała poprawkę umożliwiającą załatanie dziury w aplikacji Apache Struts służącej do budowania webowych aplikacji Java. Większość Amerykanów nie zauważyła tego wydarzenia, ale za to zwróciło ono uwagę hakerów na całym świecie. W przeciągu 24 godzin na stronie poświęconej cyberbezpieczeństwu FreeBuc.com pojawiła się informacja o luce. Została ona również dodana do Metasploita – otwartego narzędzia służącego do przeprowadzania testów penetracyjnych. 10 marca hakerzy skanując Internet w poszukiwaniu podatności w systemach komputerowych znaleźli niezabezpieczony serwer amerykańskiego giganta kredytowego firym Equifaxu w Atlancie.

Czytaj więcej: Ogromy wyciek danych w Stanach Zjednoczonych. 150 milionów osób zagrożonych

W krótkim czasie hakerzy spenetrowali sieci i system firmy Equifax. Według śledczych atak miał wyglądać w następujący sposób. Początkowo włamała się pierwsza grupa, która została w raporcie ze śledztwa określana jako „ekipa wejścia". Następnie do akcji wkroczył zaawansowany zespół hakerów, co zdaniem niektórych ekspertów może wskazywać na udział podmiotu państwowego. Po pewnym czasie udało się uzyskać dostęp do dziesiątek baz danych, utworzono również 30 oddzielnych punktów dostępu do systemów komputerowych firmy Equifax. Hakerzy mieli wystarczająco dużo czasy żeby odpowiednio zmodyfikować swoje narzędzia, aby jeszcze efektywniej wykorzystać luki w oprogramowaniu używanym przez Equifax oraz przeszukać bazy danych w poszukiwaniu najbardziej wartościowego materiału. Nie skupiali się tylko na kolekcjonowaniu informacji o zwykłych obywatelach, ale szukali danych osób dysponujących majątkiem przekraczającym milion dolarów amerykańskich.

Hakerzy zostali wykryci 29 lipca, ale szkody poczynione przez nich spowodowały, że firma musiała wyłączyć portal służący do składania skarg na 11 dni, żeby zespoły zajmujące się bezpieczeństwem mogły załatać wszystkie dziury.

Zdarzenie to miało miejsce pomimo tego, że Equifax zainwestował miliony w zaawansowane środki bezpieczeństwa, posiada własny SOC oraz rozmieścił w swoich systemach programy wykrywania wtargnięć. Według śledczych odejście kluczowych osób zajmujących się bezpieczeństwem oraz inne niewymienione powody mogły negatywnie wpłynąć na bezpieczeństwo. Część śledczych z kręgów rządowych podejrzewa, że hakerom mógł ktoś pomagać z wewnątrz firmy, czemu zaprzeczają przedstawiciele Equifaxu.

Czytaj więcej: Edukacja podstawą systemu cyberbezpieczeństwa [ANALIZA]

Na zaangażowanie aktora państwowego miałby wskazywać też fakt, że wykradzione dane nie pojawiły się na żadnym z tzw. rynków w Darknecie, co jest normalne w przypadku działania cyberprzestępców, którzy dążą do uzyskania jak największych zysków. Uzyskane we włamaniu dane, jak np. numer ubezpieczenia społecznego, są niezwykle cennym źródłem dla każdego wywiadu, który szuka przykrywki dla swoich pracowników. Część ekspertów pozostaje jednak sceptyczna wobec tych doniesień. Wynajęta przez Equifax firma Mandiant w przygotowanym raporcie napisała, że nie posiada wystarczających danych pozwalających na wskazanie winnego. Wykrycie sprawców jest utrudnione przez działanie hakerów, którzy wystrzegali się używania oprogramowania, które mogłoby naprowadzić śledczych na ich trop. Jedno z narzędzi jak podaje Bloomberg, które udało się zanalizować to China Chopper posiadające interfejs w języku chińskim. Nie przesądza to jednak w żaden sposób udziału hakerów Państwa Środka, ponieważ jest ono również używane poza Chinami.

Jeżeli faktycznie potwierdzą się informację o chińskiej ingerencji albo zostanie zebrana wystarczająca liczba danych, żeby oskarżyć Chiny, będzie to jawne złamanie porozumienia z 2015 roku, kiedy to prezydenci Barack Obama i Xi Jinping uzgodnili m.in. że państwa nie będą prowadziły działań szpiegowskich wymierzonych w prywatne podmioty.

Może to również oznaczać, że Chiny obierają bardziej konfrontacyjny kurs względem Stanów Zjednoczonych prezydenta Trumpa, ponieważ ciężko sobie wyobrazić, że tego typu działania hakerskie nie były dokonywane w porozumieniu z rządem Państwa Środka. W szczególności, że Xi Jinping reformuje siły zbrojne w kierunku większej centralizacji jak również zwiększenia kontroli nad jednostkami do operacji w cyberprzestrzeni. Jednak w środowisku wirtualnym, mało co może być pewne, dlatego nie można wykluczyć, że ktoś używa chińskich metod, tym samym przeprowadzając operacje pod tzw. fałszywą flagą.