NAPASTNICY STOJĄCY ZA INFEKCJĘ CCLEANERA PRAWDOPODOBNIE OSIĄGNĘLI SWÓJ CEL [KOMENTARZ EXATELA]

Świat powoli zapomniał już o wirusie NotPetya, który dokonał olbrzymich strat. Hakerzy jednak nie kazali nam długo czekać na kolejne zagrożenie o światowym zasięgu. Tym razem nosicielem infekcji został popularny CCleaner. Każdy, kto pobrał i zainstalował renomowany program (w wersji CCleaner 5.33.6162 oraz CCleaner Cloud version 1.07.3191.), nieświadomie instalował również złośliwe oprogramowanie. Skala ataku jest gigantyczna. CCleaner ma ponad 2 miliardy pobrań, z czego wersja ze złośliwym oprogramowaniem została zainstalowana 2 miliony razy.

Nie tak dawno żyliśmy olbrzymim atakiem na Ukrainie. Wirus NotPetya spowodował gigantyczne straty sięgające setek milionów dolarów. Atak polegał na przejęciu serwerów firmy M.E.Doc tak, by w ramach aktualizacji programu przemycać złośliwe oprogramowanie. Ponieważ aplikacja była zaufana, aktualizacje pochodziły z oficjalnych serwerów, a administratorzy nie spodziewali się w nich złośliwego kodu. Atak mógł więc pozostać niezauważony miesiącami. Dodatkowo złośliwy kod miał takie same uprawnienia jak legalna aplikacja. To wszystko umożliwiło, by NotPetya została uruchomiona jednym *prikazem*, siejąc spustoszenie i niszcząc zawartości tysięcy dysków. Oczywiście przejęcie serwera firmy tak, by być w stanie zatruwać aplikacje u źródła, jest wyjątkowo trudne. Natomiast jeżeli już się powiedzie, wykrycie złośliwego oprogramowania jest bardzo ciężkie.

Czytaj też: Ransomware Petya nie zaszkodził polskiej gospodarce [Komentarz Exatela]

Rzeczywistość zmienia się bardzo szybko. Mogliśmy więc już zdążyć zapomnieć o atakach na Ukrainie, a już jesteśmy świadkami podobnego ataku. Tym razem sprawa wyszła na jaw dzięki specjalistom z firmy Cisco. Otóż atakującym udało się przejąć serwery firmy Pirform, która była właściciel popularnego programu CCleaner. W efekcie każdy, kto pobrał i zainstalował renomowany program CCleaner (w wersji CCleaner 5.33.6162 oraz CCleaner Cloud version 1.07.3191.), nieświadomie instalował również złośliwe oprogramowanie. Skala ataku jest gigantyczna. CCleaner ma ponad 2 miliardy pobrań, z czego wersja ze złośliwym oprogramowaniem została zainstalowana 2 miliony razy. Pod adresem IP 216.126.225.148 znajdował się serwer C&C, czyli serwer kontrolowany przez hakerów. To na ten adres spływały dane z zarażonych komputerów. Dla pewności atakujący wyposażył złośliwy kod w system DGA (Domain Generation Algorithm), który na wypadek braku dostępu do serwera umożliwiał komunikacje przy pomocy specjalnie spreparowanych domen. Najciekawsze jednak w tej historii jest to, co atakujący zrobił z tą gigantyczną zarażoną armią komputerów, bo… nie zrobił praktycznie nic. Przez miesiąc – od 15 sierpnia do 11 września – chociaż wszystkie zarażone komputery czekały na rozkaz z C&C, nie znamy nawet choćby jednego przypadku, by taki został wydany. W fazie spekulacji pozostaje pytanie dlaczego. Możliwe, że atakujący czekał na dogodny moment do przeprowadzania spektakularnego ataku i np. zaszyfrowania wielu milionów komputerów na całym świecie. Na szczęście atak został wykryty i zablokowywany. Możliwe jednak, że nie znamy

całej historii i choć zarażone oprogramowanie trafiło do milionów użytkowników na całym świecie, to prawdziwym celem ataku była np. jedna konkretna instytucja. Zaatakowana instytucja została przejęta, ale jej członkowie nie mają ochoty chwalić się tym z opinią publiczną. Patrząc na ogrom umiejętności hakerskich, profesjonalizm atakujących, jakość kodu (choćby zaszycie mechanizmów DGA) skłaniam się do teorii, że choć nie wiemy, jaki był prawdziwy cel ataku, to prawdopodobnie został on osiągnięty. Na koniec pozostaje jeszcze doradzić, co zrobić, jeżeli zainstalowaliśmy CCleanera ze złośliwym kodem. Wystarczy pobrać najnowszą wersję tego programu, a aplikacja sama usunie pozostałość działalności hackerów.

Niniejsza historia po raz kolejny uczy, że kluczową kwestią – gdy chcemy zapewnić cyberbezpieczeństwo – jest zasada ograniczonego zaufania. Atak może przyjść z praktycznie każdej strony. By móc się ochronić, należy nie tylko korzystać z produktów i narzędzi tworzonych przez zaufanych producentów, ale również wykorzystywać zaufane oprogramowanie zabezpieczające, monitorowane i obsługiwane przez zaufany zespół specjalistów. Wtedy moment wykrycia ataku będzie znacznie szybszy, a reakcja znacznie bardziej skuteczna.

Autor: Jan Kostrzewa – Analityk Bezpieczeństwa SOC Exatel.