Bitdefender

Złośliwe oprogramowanie QakBot na celowniku międzynarodowego zespołu pod przewodnictwem USA

31.08.2023

Władze USA współpracujące z międzynarodowymi organami ścigania zlikwidowały niesławną sieć złośliwego oprogramowania QakBot. Ogłoszona 29.08.2023 roku międzynarodowa operacja „Duck Hunt" miała na celu rodzinę szkodliwego oprogramowania, która w ciągu ostatnich 18 miesięcy spowodowała straty o wartości ponad 58 milionów dolarów. W ramach tej akcji Federalne Biuro Śledcze (FBI) i Departament Sprawiedliwości (DoJ) uzyskały nakazy sądowe nakazujące potajemne usuwanie szkodliwego oprogramowania QakBot z zainfekowanych komputerów z systemem Microsoft Windows i przejmowanie serwerów używanych do kontrolowania botnetu.

Złośliwe oprogramowanie QakBot – czym jest?

QakBot, znany wcześniej jako Qbot i Pinkslipbot, pojawił się po raz pierwszy w 2007 roku jako trojan bankowy, przekształcił się w potężną odmianę złośliwego oprogramowania, która umożliwia sprawcom przygotowanie zainfekowanych sieci na infekcje ransomware. Szkodnik rozprzestrzenia się głównie za pośrednictwem wiadomości e-mail phishingowych podszywających się pod legalne przedmioty, takie jak zlecenia pracy lub faktury, często poprzez wywoływanie poczucia pilności.

Amerykański prawnik z południowego dystryktu Kalifornii, Martin Estrada, powiedział, że QakBot był zaangażowany w 40 różnych atakach ransomware w ciągu ostatnich 18 miesięcy.

Don Alway, zastępca dyrektora odpowiedzialny za biuro terenowe FBI w Los Angeles, opisał, w jaki sposób śledczy federalni uzyskali dostęp do internetowego panelu sterowania wykorzystywanego przez cyberprzestępców do monitorowania i kontrolowania botnetu.

Za zgodą sądu władze poinstruowały wszystkie zainfekowane maszyny, aby odinstalowały QakBota i zerwały połączenie z botnetem.

Wysiłki te były częścią szerszej strategii neutralizacji szkodliwego oprogramowania, które w zeszłym roku zainfekowało ponad 700 000 komputerów, w tym 200 000 systemów w USA.

Sukces międzynarodowej koalicji ekspertów do spraw cyberbezpieczeństwa

Złośliwe oprogramowanie QakBot na celowniku międzynarodowego zespołu pod przewodnictwem USA

Sukces operacji opierał się na współpracy międzynarodowej. Departament Sprawiedliwości ściśle współpracował z organami ścigania z Francji, Niemiec, Łotwy, Holandii, Rumunii i Wielkiej Brytanii. Wspólnie przejęli ponad 50 serwerów podłączonych do sieci złośliwego oprogramowania i skradzioną kryptowalutę o wartości około 9 milionów dolarów.

„Plik Qakbot Uninstall nie naprawił innego złośliwego oprogramowania, które było już zainstalowane na zainfekowanych komputerach" – czytamy w oświadczeniu Departamentu Sprawiedliwości . „Zamiast tego zaprojektowano go tak, aby zapobiegać instalowaniu dodatkowego złośliwego oprogramowania QakBot na zainfekowanym komputerze poprzez odłączenie komputera ofiary od QakBota botnetu".

Nie jest to pierwsze wykorzystanie przez rząd Stanów Zjednoczonych nakazów sądowych do likwidacji operacji szkodliwego oprogramowania i przywrócenia zainfekowanych systemów. W zeszłym roku Departament Sprawiedliwości przeprowadził podobną operację przeciwko cieszącemu się złą sławą rosyjskiemu złośliwemu oprogramowaniu „Snake", znanemu z kradzieży danych.

„Operacja „Polowanie na kaczki" stanowi kolejny kamień milowy w wojnie z cyberprzestępczością i pokazuje, co można osiągnąć, współpracując podmioty krajowe i międzynarodowe na rzecz wspólnej sprawy. Dzięki takim akcjom rządy dają sygnał cyberprzestępczemu światkowi, który polega na tym, że działania hakerów nie są całkowicie bezkarne i bardzo szybko mogą zmienić rolę z myśliwego na zwierzynę

ściganą przez międzynarodowy zespół specjalistów” – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło: https://bitdefender.pl/zlosliwe-oprogramowanie-qakbot/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 31.08.2023
Z pozdrowieniami Piotr Rozmiarek
E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender
Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.