aut. Szymon Palczewski 24.04.2020

ZIDENTYFIKOWANO GRUPĘ IRAŃSKICH HAKERÓW. POSIADALI "CYBERBROŃ" OD NSA

Były specjalista Kaspersky'iego oraz Google zidentyfikował nieznaną dotychczas grupę hakerską sponsorowaną przez państwo, która prawdopodobnie działa na zlecenie irańskiego rządu. Cyberprzestępcy posługiwali się narzędziem NSA, pozyskanym w wyniku działalności Shadow Brokers.

W 2017 roku grupa cyberprzestępców znana jako Shadow Brokers udostępniła zbiór narzędzi hakerskich skradzionych z amerykańskiej National Security Agency (NSA). Zestaw cyberbroni nazwano „Lost in Translation", a wiele z nich było wykorzystywane przez Stany Zjednoczone do prowadzenia operacji przeciwko innym państwom – przypomina serwis ZDNet.

Wśród opublikowanych narzędzi hakerskich znajduje się plik „sigs.py", który wzbudza szczególne zainteresowanie specjalistów do spraw cyberbezpieczeństwa. Wynika to z faktu, że jest czymś, co wielu ekspertów uważa za „skarbnicę operacji cyberszpiegowskich".

Jak donosi ZDNet, narzędzie, o którym mowa jest skanerem złośliwego oprogramowania, który służył NSA do wyszukiwania obecności grup hakerskich (APT) na zhakowanym komputerach i urządzeniach.

Zainteresowanie plikiem „sigs.py" wynika z faktu, że wielu specjalistów zdało sobie sprawę, iż nie byli w stanie wykryć aktywności tylu grup APT, co NSA za pomocą jednego narzędzia. Jak poinformował Costin Raiu, ekspert Kaspersky, 15 sygnatur z pliku sigs.py wciąż pozostaje bez atrybucji. „Ostatnim, który udało się powiązać był SIG27, czyli DarkUniverse / ItaDuke" – czytamy na Twitterze specjalisty. To wszystko wskazuje, że NSA posiada lepszy wgląd w zagraniczne operacje hakerskie w porównaniu do wielu współczesnych i świetnie wyposażonych firm cyberbezpieczeństwa.

Nowe odkrycie

Juan Andres Guerrero-Saade, były specjalista Kaspersky oraz Google odkrył, że prawdopodobnie dokonano złego powiązania SIG37 z Iron Tiger, czyli podejrzanej o cyberszpiegostwo chińskiej grupy hakerskiej – informuje ZDNet. Według eksperta narzędziem tym posługiwała się nowa grupa, która, jego zdaniem, może mieć siedzibę w Iranie.

Juan Andres Guerrero-Saade nazwał ugrupowanie Nazar APT, co odzwierciedla strukturę wykrytego złośliwego oprogramowania. Co więcej, podkreślił, że udało mu się zidentyfikować ofiary, których urządzenia zostały zainfekowane wirusem, pasującym do sygnatury SIG37.

„Złośliwe oprogramowanie jest bardzo stare i atakuje głównie starsze wersje systemu Windows, takie jak Windows XP i poprzednie wersje" – podkreślił specjalista, cytowany przez ZDNet. – „Za każdym razem, gdy wszyscy mówią o Iranie jako o napastniku, zaczynamy myśleć o zachodnich ofiarach".

Czytaj też: Irańscy hakerzy atakują WHO