aut. Szymon Palczewski 09.02.2021

„PRINCE OF PERSIA”. IRAN WRACA DO KORZENI CYBERSZPIEGOSTWA

Iran wznowił jedną z pierwszych swoich kampanii w cyberprzestrzeni, kierując cyberataki na podmioty z całego świata. Ponadto, wykryto odrębną operację hakerską, której celem są organizacje oraz osoby, uznawane przez rząd w Teheranie za zagrożenie dla władzy. Podjęte działania należy klasyfikować w kategorii cyberszpiegostwa.

Specjaliści CheckPoint wykryli dwie kampanie cyberszpiegowskie prowadzone przez grupy hakerów, działających na zlecenie rządu w Teheranie. Wśród celów znajdują się zarówno krajowe jak i zagraniczne podmioty, które są uznawane przez reżim za zagrożenie dla państwa i ładu społecznego.

Eksperci podkreślili, że irańscy hakerzy nie zaprzestali prowadzenia szeroko zakrojonych operacji szpiegowskich wymierzonych w obywateli oraz osoby i organizacje, które są przez władze uznawane za niebezpieczne, w tym m.in. dysydentów politycznych, siły opozycji, zwolenników ISIS czy mniejszości kurdyjskiej.

> *Cyberwojna od dawna stała się powszechną praktyką w arsenale rządów, armii i agencji wywiadowczych na całym świecie. To, co kiedyś było „czarną sztuką”, zarezerwowaną dla elity i kierowaną przez nielicznych, teraz stało się krainą możliwości dla prawie każdego państwa na całym świecie. Iran nie jest wyjątkiem od tego trendu.*
>
> Raport „Infy – After Lightning Comes Thunder”

Inwigilacja wewnętrznych „wrogów”

Pierwsza z kampanii jest prowadzona przez grupę „Domestic Kitten” (znaną również jako APT-C-50), powiązaną z rządem w Teheranie. Jej głównym celem są obywatele Iranu. Do tej pory hakerzy byli odpowiedzialni za „10 unikalnych operacji, skierowanych do ponad 1200 osób”, podczas których dokonano ponad 600 infekcji. Obecnie specjaliści wykryli kolejne 4 aktywne kampanie, z których ostatnia rozpoczęła się w listopadzie 2020 roku.

Jak wskazują specjaliści CheckPoint, w ramach operacji ofiary są zachęcane do zainstalowania określonego programu lub aplikacji, które w rzeczywistości zawierają w sobie złośliwe oprogramowanie. Do tego celu hakerzy wykorzystują m.in. specjalnie przygotowane blogi tematyczne, kanały w komunikatorach (np. Telegram) czy wiadomości SMS.

Wirus (nazwany przez ekspertów FurBall) użyty podczas kampanii pozwala na przechwytywanie wiadomości elektronicznych, dzienników połączeń, nagrywanie dźwięku poprzez dostęp do mikrofonu urządzenia, rejestrowanie rozmów, kradzież plików multimedialnych (np. filmów i zdjęć), pobieranie zainstalowanych aplikacji, śledzenie lokalizacji oraz pozyskanie dokumentów z pamięci zewnętrznej nośnika.

FurBall hakerzy starają się ukryć pod postacią różnych aplikacji lub witryn internetowych. Specjalistom udało się zidentyfikować kilka z nich. Szczególnie niebezpieczne są:

- VIPRE Mobile Security – fałszywa aplikacja bezpieczeństwa mobilnego;
- ISIS Amaq – witryna informacyjna dla agencji informacyjnej Amaq;
- Exotic Flowers – zmodyfikowana wersja gry z Google Play;
- MyKet – sklep z aplikacjami na Androida;
- Iranian Woman Ninja – aplikacja do tapet.

Ponadto, eksperci odkryli również różne metody prowadzenia kampanii. Przykładowo w niektórych operacjach wykorzystano wiadomości SMS z zainfekowanym załącznikiem, podczas gdy w innych wirus był ukryty na jednym z blogów internetowych. Złośliwe oprogramowanie było także rozpowszechniane za pomocą komunikatora „Telegram" – wskazuje CheckPoint.

„Prince of Persia"

Druga kampania, o której informują specjaliści, to reaktywacja jednej z pierwszych irańskich operacji w cyberprzestrzeni, czyli „Infy", znanej również jako „Prince of Persia". Jej ślady zostały wykryte już w 2007 roku i potwierdzają, że głównym celem hakerów były podmioty z Iranu oraz Europy. Podczas cyberataków naruszono bezpieczeństwo urządzeń wykorzystywanych przez m.in. duńskich dyplomatów czy dziennikarzy w czasie wyborów w Iranie. Oczywiście działania były silnie wspierane przez rząd w Teheranie.

> *Wygląda na to, że po długim przestoju irańscy cyberprzestępcy byli w stanie przegrupować się, wyeliminować swoje problemy i radykalnie wzmocnić swoje działania, a także podnieść sprawność techniczną i możliwości.*
>
> Raport „Infy – After Lightning Comes Thunder**"**

W pierwszej połowie 2020 roku specjaliści CheckPoint, we współpracy z ekspertami firmy SafeBreach Labs, wykryli nową wersję złośliwego oprogramowania o nazwie „Foudre", które w przeszłości było głównym narzędziem hakerów podczas „Infy". Jednak zostało ono zmodyfikowane, na co wskazuje odmienny sposób działania – zamiast zmuszać ofiarę do kliknięcia w załącznik lub link, wirus uruchamiał makro, gdy ofiara zamknęła dany plik.

„Foudre" znajduje się w spreparowanych dokumentach elektronicznych. Przykładowo, w jednym z nich widnieje zdjęcie Mojtaba Biranvand, gubernatora miasta Dorud w prowincji Lorestan w Iranie. Jest on napisany w języku perskim i zawiera informacje na temat biura gubernatora oraz jego numer telefonu. W rzeczywistości, kiedy ofiara otwiera plik, uruchamiana jest specjalna procedura instalacji wirusa. Gdy użytkownik zamknie dokument, złośliwe oprogramowanie jest w pełni zdolne do działania

na urządzeniu.

Zainfekowanie nośnika pozwala na m.in. kradzież plików z folderów, a także pamięci zewnętrznej oraz nagrywanie dźwięku czy przechwytywanie obrazu z ekranu.

Kto tym razem był celem hakerów? Specjaliści zidentyfikowali podmioty z takich krajów jak: Azerbejdżan, Kanada, Niemcy, Wielka Brytania, Irak, Indie, Rosja, Rumunia, USA, Turcja, Holandia oraz Szwecja.

Czytaj też: Phishing ukryty w świątecznych życzeniach. Iran sięgnął po najprostsze środki