**Irańska grupa Nimbus Manticore rozszerza operacje szpiegowskie na Europę**

**Nimbus Manticore - irańska grupa hakerów wspieranych przez państwo - rozszerza swoją działalność na Europę Zachodnią – ostrzegają eksperci firmy Check Point Research. Ugrupowanie celuje w konkretne firmy z sektorów obronnego, telekomunikacyjnego i lotniczego w celu prowadzenia działań szpiegowskich.**

Nimbus Manticore to wyspecjalizowana grupa APT (advanced persistent threat) powiązana z irańskimi służbami. Bywa określana również jako UNC1549 lub Smoke Sandstorm, wcześniej związana z kampanią „Iranian Dream Job”. Od początku 2025 r. Check Point Research obserwuje kolejne fale jej aktywności. Grupa znana jest przede wszystkim z ukierunkowanych kampanii spear-phishingowych (**celowanych ataków e-mail/SMS)**, które mają uśpić czujność wybranych osób, poprzez dostarczanie własnych implantów, m.in. Minibike.

Choć Nimbus Manticore konsekwentnie atakuje cele na Bliskim Wschodzie – szczególnie w Izraelu i Zjednoczonych Emiratach Arabskich – ostatnie operacje pokazują rosnące zainteresowanie Zachodnią Europą, zwłaszcza Danią, Szwecją i Portugalią. Sektory, na których skupia się grupa – telekomunikacja (zwłaszcza dostawcy satelitów), kontraktorzy obronni, przemysł lotniczy i linie lotnicze – ściśle odpowiadają priorytetom strategicznym Korpusu Strażników Rewolucji Islamskiej (IRGC), skoncentrowanym na gromadzeniu wywiadu o wrażliwych dostawcach w okresach nasilonych napięć geopolitycznych.

Po raz pierwszy Minibike został opisany w 2022 r. i od tego czasu stale ewoluował – zyskał techniki zaciemniania kodu, architekturę modułową oraz zapasową infrastrukturę C2. Najnowsza aktywność pokazuje znaczący skok w poziomie zaawansowania: wykorzystywanie nieznanych dotąd technik ładowania plików DLL z alternatywnych ścieżek poprzez modyfikację parametrów wykonania procesu. Wariant nazwany MiniJunk demonstruje, jak Nimbus Manticore nieustannie rozwija swoje złośliwe oprogramowanie, by unikać wykrycia. Obok MiniJunk grupa wykorzystuje także MiniBrowse, co pozwala jej nie tylko utrzymywać długotrwały dostęp do systemów ofiar, ale też skutecznie kraść dane i pozostawać w ukryciu.

**Fałszywe portale rekrutacyjne i spear phishing**

Nimbus Manticore stosuje fałszywe portale rekrutacyjne i zaawansowany spear phishing, aby zwabić ofiary. Złośliwe pliki dostarczane są jako element procesów rekrutacyjnych, a przestępcy podszywają się przy tym pod duże lokalne i globalne firmy z sektora lotniczego. - *Zidentyfikowaliśmy korelację między stronami dostarczającymi malware a sektorami, do których są skierowane* – informuje Check Point Research. Przykładem jest fałszywy portal rekrutacyjny firmy telekomunikacyjnej będzie celował w pracowników i organizacje właśnie z tej branży.

- *Przez ostatni rok Nimbus Manticore rozwinął swój arsenał złośliwego oprogramowania, metody dostarczania i strategię ataków. Przekształcając Minibike w MiniJunk, wdrażając MiniBrowse i udoskonalając spear phishing, aktor ten pokazał odporność i zdolność ukrywania się nawet podczas intensywnych konfliktów geopolitycznych* – podkreślają eksperci firmy Check Point.

**Zespół badaczy ostrzega, że rozszerzenie działalności grupy na Europę w sektorach obrony, telekomunikacji i lotnictwa oznacza narastającą irańską kampanię cyberszpiegowską zgodną z priorytetami IRGC** *(Islamic Revolutionary Guard Corps/***Korpusu Strażników Rewolucji Islamskiej).** Aby przeciwdziałać tym zagrożeniom, organizacje potrzebują ochrony blokującej ataki, zanim dotrą do pracowników. - *Jednym ze sposobów skutecznej walki z tego rodzaju atakami jest instalacja systemów wykrywania i zapobiegania spear phishing, które zatrzymują ataki już na poziomie poczty* – czytamy w raporcie.

Szczegóły ataków [dostępne są tutaj](https://research.checkpoint.com/2025/nimbus-manticore-deploys-new-malware-targeting-europe/).