aut. Szymon Palczewski 09.01.2020

KOREA PÓŁNOCNA ZBROI SIĘ W CYBERPRZESTRZENI. ZAGROŻENIE DLA INSTYTUCJI FINANSOWYCH NA CAŁYM ŚWIECIE?

Hakerzy Pjongjangu regularnie modyfikują swoją taktykę działania oraz ulepszają narzędzia stosowane podczas cyberataków. Cyberprzestępcy koncentrują się na minimalizacji ryzyka wykrycia, czego potwierdzeniem są ostatnie prowadzone przez nich kampanie. Jedno jednak nie ulega zmianie – celem nadal pozostają instytucje finansowe z całego świata oraz rynki kryptowalut.

Północnokoreańscy hakerzy od lat stosują różne taktyki działania w ramach kampanii wymierzonych w instytucje finansowe. W ostatnim czasie cyberprzestępcy znacznie zmodyfikowali swoje narzędzia, ulepszając je w taki sposób, aby zminimalizować możliwość wykrycia – donosi serwis CyberScoop, powołując się na informacje pozyskane od Kaspersky Lab.

Hakerzy, należący do grupy Lazarus, w ciągu ostatnich dwóch lat znacznie zmienili swoją taktykę działania. Cyberprzestępcy zaczęli wykorzystywać fikcyjne firmy, jak na przykład „JMT Trading", za pomocą których przesyłali skradzione fundusze do kraju. Podczas kampanii hakerzy tworzyli również fałszywe strony internetowe, między innymi „UnionCryptoTrader", służące jako jedno z narzędzi, używanych do realizacji złośliwej operacji.

Jak donosi CyberScoop, w zeszłym roku specjaliści Kaspersky Lab podczas analizy jednego z incydentów odkryli, że metody oraz instrumenty działania grupy Lazarus zostały znacznie ulepszone. Zwłaszcza, jeśli chodzi o narzędzia hakerskie przeznaczone do atakowania urządzeń z systemem Windows oraz macOS.

Najnowsze badania działalności grupy Lazarus wskazują, że nieustannie celem północkoreańskich hakerów są instytucje finansowe oraz rynek kryptowalut. Ofiarami złośliwych kampanii Pjongjangu są podmioty pochodzące z Wielkiej Brytanii, Rosji, Chin, a nawet Polski. Cyberprzestępcy stale rozwijają swoją działalność, starając się równocześnie modyfikować wykorzystywane narzędzia oraz stosowaną taktykę działania.

„Cybergang kontynuuje operacje, ale działa z większą ostrożnością, stosując udoskonalone taktyki i procedury, jak również wykorzystując komunikator Telegram jako jeden z nowych wektorów ataków" – czytamy na oficjalnej stronie Kaspersky Lab. Specjaliści firmy wskazują, że od pewnego czasu hakerzy grupy Lazarus tworzą między innymi fałszywe witryny internetowe związane z kryptowalutą, które zawierają fikcyjne załączniki do kanałów Telegrama. W ten sposób cyberprzestępcy rozsyłają złośliwe oprogramowanie za pomocą popularnego komunikatora.

Podobnie, jak w kampaniach prowadzonych wiele lat temu cyberatak składa się głównie z dwóch faz. Po pierwsze, nieświadomi użytkownicy pobierają zainfekowany plik, który następnie ściąga na dane urządzenie kolejny szkodliwy element, zapewniający cyberprzestępcom pełną kontrolę nad danym

sprzętem.

Eksperci Kaspersky Lab podkreślają, że od pewnego czasu grupa zaczęła przywiązywać dużą wagę do zacierania swoich śladów i zminimalizowania możliwości zostania wykrytym. Obecnie szkodliwe oprogramowanie jest dostarczane w sposób dużo bardziej dyskretny. „W atakach na cele działające w systemie macOS, moduł pobierający szkodliwe funkcje został wzbogacony o mechanizm uwierzytelniania, zmieniono środowisko programistyczne i przyjęto bezplikową technikę infekcji" – czytamy na oficjalnej stronie firmy.

Z kolei jeśli chodzi o kampanie wymierzone w użytkowników systemu Windows, zamiast dotychczas wykorzystywanego złośliwego oprogramowania Fallchill, hakerzy opracowali wirusa, który działa wyłącznie w określonych systemach po sprawdzeniu ich pod kątem określonych parametrów.

Hakerzy północnokoreańskiej grupy Lazarus wyróżniają się głównie cyberatakami ukierunkowanymi w sektor finansowy oraz prowadzeniem kampanii cyberszpiegowskich. Jednym z podstawowych celów cyberprzestępców jest generowanie zysków dla władzy, które są następnie przeznaczane na między innymi rozwój programu nuklearnego. Analiza ostatnich lat działalności grupy Lazarus pokazuje, jak dużą wagę hakerzy przywiązują do zapobiegania wykrycia swojej działalności.

Czytaj też: Cyberatak na sieć kantorów Travelex. Brytyjskie służby wszczęły dochodzenie