PÓŁNOCNOKOREAŃSCY HAKERZY Z POTĘŻNYM ARSENAŁEM. LAZARUS FINANSUJE BUDOWĘ BRONI MASOWEGO RAŻENIA?

Narzędzie hakerskie TrickBot, znane już z ataków na branżę finansową, zostało ulepszone i znacznie zmodyfikowane przez północnokoreańską grupę hakerską Lazarus. Poza atakami na banki, umożliwia kradzież danych uwierzytelniających a także pranie pieniędzy. Podejrzewa się, że działalność grupy finansuje budowę broni jądrowej.

Narzędzie znane jako TrickBot aktywnie przekształciło się w pełni funkcjonalną platformę do ataków o nazwie „Anchor" twierdzą eksperci z SentinelLABS Research Team. Po przebadaniu oprogramowania określili je jako „złożone i ukryte narzędzie do ukierunkowanego wydobywania danych z bezpiecznych środowisk". Platforma, jak wskazują eksperci w raporcie prezentującym wyniki badań, łączy w sobie zbiór narzędzi - od pierwszego narzędzia instalacyjnego do tego mającego na celu usunięcie szkodliwego oprogramowania na zaatakowanym komputerze. W opinii ekspertów Anchor przedstawia się jako kompleksowa platforma zaprojektowana do atakowania środowisk korporacyjnych przy użyciu zarówno niestandardowych, jak i istniejących narzędzi. Wygląda na to, że grupa specjalizująca się głównie w atakach na sferę finansową dynamicznie rozwija swoje narzędzia i dysponuje już bardzo silnym arsenałem cyberbroni – czy będzie to broń na miarę broni nuklearnej, której budowa jest finansowana z działalności grupy?

Pierwsze doniesienia o TrickBot pojawiły się jesienią 2016 roku, natomiast w listopadzie tego roku, oprogramowywanie zostało przetestowane. Jeszcze w tym samym roku, za pomocą tego narzędzia, północnokoreańscy hakerzy zaczęli atakować banki, a pierwszymi ofiarami padły instytucje australijskie, nowozelandzkie, brytyjskie, niemieckie i kanadyjskie. Rok później narzędzie rozwinięto i za jego pomocą cyberprzestępcy byli w stanie przeglądać Google Chrome, Mozillę Firefox, Microsoft Edge i inne aplikacje zawierające hasła i dane uwierzytelniające. Do 2019 roku narzędzie było już w pełni zautomatyzowane. Moduł zbierający umożliwił automatyczne zbieranie informacji o sieci oraz zbieranie danych uwierzytelniających. Narzędzie, zdaniem ekspertów, było w pełni gotowe do przeprowadzenia zaawansowanych operacji oszustw bankowych – prania pieniędzy czy oszustw podatkowych.

Zdaniem ekspertów z SentinelLABS Research Team, platforma Anchor jest obecnie używana do dużych napadów w cyberprzestrzeni i operacji kradzieży kart w punktach sprzedaży. Jedną z grup, która w szczególności zainteresowana jest pozyskaniem środków finansowych jest Lazarus, który podejrzewany jest o finansowanie północnokoreańskiego programu nuklearnego.

Grupa Lazarus powiązana z rządem Korei Północnej jest prawdopodobnie złożona z członków koreańskich służb specjalnych – Koreańskiej Agencji Wywiadowczej, według różnych szacunków liczy około 20 osób. Działalność grupy odnotowano już w 2009 roku. W dużej mierze grupa zainteresowana jest giełdami kryptowalut, instytucjami finansowymi, organizacjami pozarządowymi, ale także zajmuje

się rozpoznaniem osobowym na zlecenie Korei Północnej. Grupa prawdopodobnie nie tylko samofinansuje się, ale również ma za zadanie zarabiać pieniądze dla reżimu. Podejrzewa się, że grupa odpowiedzialna jest za liczne ataki na giełdy kryptowalut i użytkowników, aby osiągnąć ten cel. Zgodnie z danymi które przekazało ONZ, o czym informowaliśmy w sierpniu, Korea Północna mogła wygenerować około 2 miliardy dolarów dzięki zaawansowanym cyberatakom, których celem była kradzież środków z systemów bankowych oraz giełd kryptowalutowych. Według ONZ zdobyte w ten sposób fundusze Pjongjang przeznaczył na rozwój programu broni masowego rażenia. Była to odpowiedz reżimu na nałożone sankcje, które miały na celu ograniczyć jej zdolności do dalszego finansowania programów nuklearnych oraz projektów rakiet balistycznych. Szacuje się, że tylko w okresie od stycznia 2017 roku do września 2018 północnokoreańscy hakerzy wykradli 571 milionów dolarów w kryptowalutach z pięciu czołowych giełd Azji.