aut. Szymon Palczewski 29.07.2020

EWOLUCJA LAZARUS GROUP. HAKERZY PJONGJANGU Z NOWĄ BRONIĄ I STRATEGIĄ

Północnokoreańscy hakerzy stworzyli specjalistyczne oprogramowanie ransowmare, które zostało wykorzystane w ich najnowszej kampanii. Operacje prowadzone przez Lazarus Group stają się coraz bardziej zaawansowane i trudniejsze do wykrycia oraz zwalczania. Eksperci ostrzegają, że celem hakerów może być każdy podmiot gospodarczy, niezależenie od tego, gdzie się znajduje.

Specjaliści Kaspersky Lab wykryli kampanię ransomware prowadzoną przez północnokoreańskich hakerów, należących do Lazarus Group. Cyberprzestępcy posługiwali się nieznanym wcześniej złośliwym oprogramowaniem VHD.

Wirus „przedziera się przez dyski podłączone do komputera ofiary, szyfruje pliki i usuwa wszystkie foldery z informacjami o woluminie systemowym" – czytamy w oficjalnym komunikacie Kaspresky. Co więcej, oprogramowanie może zawieszać procesy, które mogą potencjalnie chronić ważne pliki przed modyfikacją (takie jak Microsoft Exchange lub SQL Server).

Analiza VHD wykazała, że ransomware ma do swojej dyspozycji listy adresów IP komputerów ofiary, a także dane uwierzytelniające do kont z uprawnieniami administratora. „Jeśli złośliwe oprogramowanie zdołało połączyć się przy użyciu protokołu SMB z folderem sieciowym innego komputera, kopiowało się i uruchamiało samo, szyfrując również to urządzenie" – wskazują specjaliści Kaspersky.

Eksperci podkreślają, że tego typu działanie jest nietypowe dla „masowego oprogramowania ransomware". Wynika to z faktu konieczności wcześniejszego rozpoznania infrastruktury ofiary.

Przeprowadzone badania wykazały, że w ramach operacji hakerom udało się uzyskać dostęp do systemów ofiar poprzez wykorzystanie podatnej na ataki bramy VPN. Następnie pozyskali prawa administratora na zaatakowanych komputerach, dzięki czemu mogli zainstalować backdoory. Przejęcie kontroli nad systemami pozwoliło hakerom na zainfekowanie urządzeń ransomware VHD przy użyciu programu ładującego, który został napisany specjalnie do tego zadania. Specjaliści nie wskazali jednak konkretnej liczby ofiar oraz żadnych konkretnych informacji na ich temat.

„Dalsza analiza zastosowanych narzędzi wykazała, że backdoor jest częścią wieloplatformowego frameworka MATA" – czytamy w komunikacie Kaspersky. – „Doszliśmy do wniosku, że jest to kolejne narzędzie Lazarus".

Jak informowaliśmy wcześniej, MATA jest strukturą złośliwego oprogramowania, która zawiera między innymi kilka modułów ładujących oraz zainfekowane wtyczki. Ta wszechstronna platforma może być przeznaczona dla systemów operacyjnych Windows, Linux i macOS.

Pierwsze ślady MATA zostały wykryte przez specjalistów w pierwszym kwartale 2018 roku. Twórca złośliwego oprogramowania wykorzystywał je do prowadzenia agresywnej infiltracji sieci

przedsiębiorstw na całym świecie. Obecnie MATA stała się elementem kampanii północnokoreańskich hakerów.

Czytaj też: Polska celem Korei Północnej. Hakerzy wykradali dane i środki finansowe

Eksperci podkreślają, że hakerzy posługujący się VHD posiadają większe zdolności i doświadczenie niż inne grupy działające w środowisku. Jak wskazują, oprogramowanie nie jest dostępne na forach cyberprzestępczych, ale specjalnie opracowane na potrzeby operacji ukierunkowanych.

W tym miejscu warto podkreślić, że do tej pory hakerzy Lazarus Group koncentrowali się na kampaniach wymierzonych w sektor finansowy, których głównym celem była kradzież pieniędzy na rzecz Pjongjangu. Tak pozyskane środki rząd przeznaczał między innymi na rozwój programu atomowego i zbrojenia. Dla Korei Północnej cyberataki są jednym ze sposobów na obchodzenie sankcji nałożonych przez społeczność międzynarodową.

Omawiana kampania wskazuje jednak, że Pjongjang rozszerza swoją strategię w cyberprzestrzeni. Celem hakerów jest już nie tylko kradzież zasobów finansowych, ale także operacje ransomware, czyli wyłudzanie środków poprzez okup. Taki stan rzeczy sprawia, że nawet małe instytucje oraz przedsiębiorstwa w różnych częściach świata są narażone na cyberataki, dlatego też powinny rozważyć zastosowanie bardziej zaawansowanych technologii bezpieczeństwa.