aut. Szymon Palczewski 29.06.2020

WIELCY AMERYKAŃSKIEGO BIZNESU DOTKNIĘCI RANSOMWARE. SPÓŁKI Z LISTY FORTUNE 500 ZHAKOWANE

Amerykańskie firmy z sektorów kluczowych dla państwa padły ofiarą kampanii ransmoware. Wśród podmiotów dotkniętych cyberatakami znajdują się spółki z listy Fortune 500. Eksperci Symantec wykryli złośliwą operację dzięki wykorzystaniu innowacyjnego narzędzia bazującego na uczeniu maszynowym. „Hakerzy odpowiedzialni za kampanię wydają się być wykwalifikowani i doświadczeni" – podkreślają eksperci.

Specjaliści firmy Symantec zidentyfikowali kampanię złośliwych cyberataków wymierzonych w amerykańskie firmy. Hakerzy próbowali zainfekować urządzenia oprogramowaniem ransomware o nazwie WastedLocker.

„Celem ataków jest sparaliżowanie infrastruktury IT ofiary poprzez zaszyfrowanie większości serwerów i komputerów dla wielomilionowego okupu" – czytamy na oficjalnym blogu Symantec. Według specjalistów kampania dotknęła co najmniej 31 organizacji.

Operacja hakerska rozpoczyna się od JavaScript. Wirus podszywa się pod aktualizację systemu, co umożliwia cyberprzestępcom uzyskanie dostępu do danego urządzenia. Jest on zamieszczany na legalnych stronach internetowych. Specjaliści wykryli ponad 150 różnych witryn, które służyły jako narzędzie do rozpowszechniania ładunku z wirusem.

Następnie hakerzy wykorzystują złośliwe oprogramowanie Cobalt Strike w celu kradzieży danych uwierzytelniających i uzyskania pełnego dostępu do sieci. Ostatnią fazą jest zainstalowanie WastedLocker.

Kampania została wykryta przez zespół specjalistów Symantec dzięki użyciu Targeted Attack Cloud Analytics, czyli innowacyjnego rozwiązania, które wykorzystuje uczenie maszynowe do wykrywania wzorców złośliwej aktywności w sieci.

„To odkrycie pozwoliło nam zidentyfikować kolejne organizacje, które były celem WastedLocker oraz przeanalizować dodatkowe narzędzia, taktyki i procedury stosowane przez hakerów" – wskazują specjaliści Symantec. – „To pomogło nam wzmocnić ochronę przed kolejnymi przejawami cyberataków".

Giganci na celowniku

Do tej pory udało się zidentyfikować 31 organizacji, które padły ofiarą złośliwej kampanii. Wszystkie znajdowały się w Stanach Zjednoczonych. Zdecydowana większość to duże korporacje, a także 11 spółek giełdowych, z których 8 to firmy z listy Fortune 500.

„Zaatakowano podmioty z różnych sektorów” – podkreślają eksperci. – „Najwięcej działań wymierzonych było w sektor produkcji, gdzie poszkodowanych jest 5 firm”. Hakerzy uderzyli również w branżę technologii informacyjnych (4 przedsiębiorstwa), telekomunikacji (3) oraz media (3).

Gdyby specjalistom nie udało się zneutralizować złośliwej kampanii, cyberataki mogłyby doprowadzić do milionowych strat, wstrzymania produkcji, a nawet do „efektu domina” w zakresie łańcucha dostaw.

„Hakerzy odpowiedzialni za kampanię wydają się być wykwalifikowani i doświadczeni, potrafią przeniknąć do najlepiej chronionych korporacji, ukraść dane uwierzytelniające i swobodnie poruszać się po sieciach” – czytamy na blogu Symantec.