aut. Szymon Palczewski 05.10.2020

„DEKADA CYBERSZPIEGOSTWA" W EUROPIE WSCHODNIEJ. RZĄDOWE TAJEMNICE WYKRADANO PRZEZ LATA

Przez prawie dekadę hakerzy niepostrzeżenie prowadzili kampanię cyberszpiegowską wymierzoną w instytucje rządowe państw w regionie Europy Wschodniej oraz Bałkanów. Jedną z ofiar cyberprzestępców były białoruskie organizacje państwowe, w tym Rada Ministrów. Jak to możliwe, że przez niemal 10 lat prowadzenia operacji szpiegowskich hakerzy nie zostali wykryci?

Specjaliści firmy ESET odkryli nową grupę APT, która od 2011 roku wykradała poufne dane oraz dokumenty, przeprowadzając cyberataki wymierzone w rządy państw w Europie Wschodniej oraz na Bałkanach. Cyberprzestępcy przez 9 lat pozostawali w ukryciu, co skutecznie uniemożliwiało ekspertom wykrycie ich działalności. „To bardzo rzadkie" – wskazują specjaliści ESET w specjalnym komunikacie. Obecnie niewiadomo skąd pochodzą hakerzy.

Grupa została nazwana „XDSpy" i specjalizuje się w cyberszpiegostwie. Jej hakerzy naruszyli zabezpieczenia wielu agencji rządowych oraz prywatnych firm. „Jak dotąd grupa nie przyciągnęła większej uwagi opinii publicznej, z wyjątkiem alertu białoruskiego CERT-u w lutym 2020 roku" – powiedział badacz ESET Mathieu Faou, który pracował nad analizą grupy oraz jej narzędzi.

Wówczas CERT.BY poinformował o kampanii „rozsyłania szkodliwego oprogramowania" za pomocą skrzynek e-mailowych „autentycznych osób, a nie fikcyjnych postaci". Cyberataki trwały od 11 do 13 lutego bieżącego roku.

„Wiadomości zawierające złośliwe oprogramowanie zostały napisane w języku rosyjskim, osoby atakujące wykorzystały standardową technikę socjotechniczną" – podkreślił w tamtym czasie białoruski CERT w specjalnym komunikacie. Głównym tematem zainfekowanych wiadomości był między innymi początek pandemii koronawirusa w tym kraju.

Główny cel hakerów stanowili wówczas pracownicy agencji i organizacji rządowych w łącznej liczbie ponad 100 osób. Złośliwe e-maile trafiały na adresy powiązane z Radą Ministrów, Radą Republiki, Ministerstwa Gospodarki, Ministerstwa Finansów, Ministerstwa Przemysłu, Ministerstwa Informacji; Państwowym Komitetem Normalizacji oraz organów ścigania.

Jak widać na powyższym przykładzie, XDSpy wykorzystuje wiadomości spear-phishingowe, aby naruszyć konkretne cele. Zainfekowane e-maile zawierają załącznik lub plik – zwykle było to archiwum ZIP lub RAR. Po kliknięciu w pozostawiony przez hakerów ładunek na urządzeniu ofiary instalowany był „XDDown", czyli główny składnik wirusa.

Pod koniec czerwca 2020 roku hakerzy zintensyfikowali swoje działania, wykorzystując lukę w przeglądarce Internet Explorer CVE-2020-0968.

„Grupa wykorzystała tematykę związaną z COVID-19 co najmniej dwa razy w 2020 roku, ostatni raz miesiąc temu podczas trwających kampanii spear phishingowych" – zaznaczył Mathieu Faou. Zdaniem specjalisty XDSpy jest wcześniej „nieudokumentowaną grupą". Wynika to z faktu, że nie znaleziono żadnych podobieństw między używanymi przez cyberprzestępców narzędziami z innymi rodzinami złośliwego oprogramowania wykorzystywanych w przeszłości.

„Cele grupy XDSpy znajdują się w Europie Wschodniej i na Bałkanach. Są to przede wszystkim agencje rządowe, w tym wojsko, ministerstwa spraw zagranicznych i firmy prywatne" – czytamy w oficjalnym komunikacie firmy ESET.

Analiza działalności hakerów doprowadziła specjalistów do interesujących wniosków. Ich zdaniem cyberprzestępcy funkcjonują w strefie czasowej UTC + 2 lub UTC + 3, w której znajdują się również ofiary cyberataków. „Zauważyliśmy także, że pracują tylko od poniedziałku do piątku, co sugeruje, iż robią to zawodowo" – czytamy w raporcie „XDSpy: Stealing government secrets since 2011", opracowanym przez ESET.

Przez prawie dekadę działalność hakerów XDSpy nie została wykryta. Dlaczego teraz udało się zidentyfikować operacje grupy? „Moim zdaniem, grupa przyciągnęła uwagę w 2020 roku, ponieważ zwiększyła intensywność cyberataków" – wyjaśnił w rozmowie z CyberScoop Mathieu Faou. – „Ich działalność (hakerów – przyp. red.) stała się głośniejsza i eksperci zaczęli przyglądać się prowadzonym operacjom".

Czytaj też: Fala ataków ransowmare na brytyjskie szkoły i uniwersytety