FBI przejęła kontrolę nad routerami Cisco i Netgear

3 lutego 2024

Chińscy cyberprzestępcy z grupy Volt Typhoon wstrzyknęli szkodliwy kod do setek przestarzałych routerów Cisco i Netgear SOHO. FBI twierdzi, że hakerzy atakują krytyczną infrastrukturę informatyczną USA. Napastnicy pobrali moduł VPN na podatne urządzenia i utworzyli zaszyfrowany kanał komunikacyjny z botnetem KV Botnet. Jednocześnie grupa rzekomo planowała ataki na stacje uzdatniania wody, sieci energetyczne, rurociągi naftowe i gazowe oraz systemy transportowe.

Specjalistom FBI udało się zneutralizować botnet. Aby zidentyfikować zainfekowane urządzenia, wysyłane były polecenia specyficzne dla botnetu. Odpowiadały na nie tylko zainfekowane routery. Następnie uzyskano pozwolenia na masowy zdalny dostęp do zainfekowanego sprzętu.

Funkcjonariusze organów ścigania zebrali informacje o aktywności szkodliwego oprogramowania, a następnie usunęli wirusa z pamięci routerów, nie wpływając na inne dane. W ten sposób FBI faktycznie przejęło kontrolę nad pozaresortowym sprzętem sieciowym, aby zneutralizować zagrożenie, co samo w sobie jest precedensem.

Amerykańska Agencja ds. Cyberbezpieczeństwa i Ochrony Infrastruktury twierdzi, że włamania cybernetyczne z Chin stają się coraz bardziej wyrafinowane. Aby chronić routery, zaleca się korzystanie z funkcji automatycznej aktualizacji oprogramowania i ograniczanie dostępu do interfejsu zarządzania tylko z urządzeń podłączonych do sieci lokalnej.

„Chińscy hakerzy atakują krytyczne części amerykańskiej infrastruktury cywilnej, przygotowując się do wyrządzenia prawdziwych szkód w przypadku konfliktu” – powiedział Wray.

Dyrektor FBI Christopher Wray powiedział Kongresowi USA, że specjalistom udało się udaremnić sabotaż grupy hakerów. Napastnicy zamierzali wykorzystać szkodliwe oprogramowanie wbudowane w routery w przypadku zaostrzenia konfliktu ze Stanami Zjednoczonymi. Władze chińskie zaprzeczają udziałowi w Volt Tajfun.

Autorstwo: tallinn
Źródło: ZmianyNaZiemi.pl