Bitdefender

# Zhakowane drony nowym cyberzagrożeniem

10.03.2023

Badacze bezpieczeństwa cybernetycznego zidentyfikowali 16 luk w zabezpieczeniach kilku dronów firmy DJI, co mogło umożliwić atakującym rozbicie urządzeń oraz zlokalizowanie ich pilotów. Komercyjne drony są coraz częściej wykorzystywane nie tylko przez ekipy telewizyjne, artystów i miłośników fotografii, lecz także przez wojsko, dlatego niewystarczające zabezpieczenia mogą skutkować bardzo groźnymi sytuacjami.

Podobnie jak wszystkie inne urządzenia elektroniczne, drony są podatne na luki w zabezpieczeniach. Specjaliści do spraw cyberbezpieczeństwa postanowili przetestować ich odporność na włamania. Niestety jeden z najpopularniejszych producentów, czyli DJI nie podołał temu sprawdzianowi.

## Niepokojące wyniki testów

Zespół kierowany przez Nico Schillera z Horst Görtz Institute for IT Security na Ruhr University Bochum w Niemczech oraz profesora Thorstena Holza z CISPA Helmholtz Center for Information Security ujawnił luki w zabezpieczeniach podczas Sympozjum Bezpieczeństwa Sieci i Systemów Rozproszonych.

Naukowcy przyjrzeli się następującym modelom dronów: DJI Mini 2, DJI Air 2 i DJI Mavic 2. Ich metoda symulowanego ataku na urządzenia, zwana „fuzzingiem", polegała na wielokrotnym podawaniu dronom losowych typów danych wejściowych w poszukiwaniu tych, które zakłócą ich poprawną pracę, np. powodując awarię.

„Często całe oprogramowanie układowe urządzenia mamy dostępne w celu fuzzowania. Tutaj jednak tak nie było" – powiedział Schiller. – „Po podłączeniu drona do laptopa najpierw przyjrzeliśmy się, jak możemy się z nim komunikować i jakie interfejsy były nam do tego celu potrzebne".

Po opracowaniu dedykowanego algorytmu dla procesu fuzzingu badaczom udało się zakłócić funkcjonalność dronów, prowadząc do ich awarii podczas lotu, a także do zmiany numerów seryjnych. Następnie naukowcy przekazali swoje odkrycia producentowi dronów. Zgodnie z ich raportem firma DJI usunęła wszystkie 16 luk w systemie bezpieczeństwa, zanim ujawniono je publicznie.

## Zhakowane drony nowym cyberzagrożeniem dla społeczeństwa

Zhakowane drony stanowią poważne niebezpieczeństwo nie tylko jako obiekty, które w niekontrolowany sposób mogą spaść na ziemię, są również potencjalnym zagrożeniem na nowoczesnym polu bitwy. Zlokalizowanie pilota tego typu urządzenia jest jak najbardziej możliwe dzięki posłużeniu się inżynierią odwrotną oprogramowania układowego – co pokazali badacze.

„Luki w zabezpieczeniach dronów mogą doprowadzić do bardzo niebezpiecznych sytuacji. Firmy produkujące te urządzenia najczęściej blokują możliwość przelotu nad niektórymi obiektami, np. więzieniami i lotniskami. Zgodnie z raportem Nico Shillera hakerzy mogli ominąć te zabezpieczenia. Nietrudno sobie wyobrazić próby ataków terrorystycznych przy wykorzystaniu tanich komercyjnych dronów, które piloci próbują skierować w stronę silników lądujących lub startujących

samolotów” – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło:https://bitdefender.pl/zhakowane-drony-nowym-cyberzagrozeniem/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.

Data udostępnienia: 10.03.2023

Z pozdrowieniami Piotr Rozmiarek

E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender

Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.