**Rosjanie ponownie atakują europejskie instytucje. Ofiarą tym razem Eurocontrol**

**Europejska Organizacja ds. Bezpieczeństwa w Lotnictwie (Eurocontrol) stała się celem ataków typu DDoS ze strony pro-rosyjskich cyberprzestępców. W rezultacie funkcjonalność strony internetowej organizacji została zakłócona na kilka godzin. W ciągu ostatnich 16 miesięcy nastąpił niebezpieczny wzrost liczby ataków na lotniska i ruch lotniczy– ostrzegają eksperci Check Point Research.**

Eurocontrol jest agencją Unii Europejskiej zajmującą się zarządzaniem ruchem lotniczym w Europie. Według przedstawicieli organizacji ataki hakerskie, zostały szybko wykryte, a następnie podjęto odpowiednie działania w celu przywrócenia funkcjonalności stron.

Zgodnie z oświadczeniem Eurocontrol, atak nie wpłynął na bezpieczeństwo lotów ani na funkcjonowanie systemów zarządzania ruchem lotniczym. Stanowi jednak poważne ostrzeżenie dla instytucji publicznych i prywatnych w Europie, aby zwiększyć swoje środki bezpieczeństwa cyfrowego i chronić się przed potencjalnymi atakami ze strony cyberprzestępców. W ciągu roku liczba ataków w tym sektorze wzrosła o 530% - informowała europejska agencja Eurocontrol.

Z danych Check Point wynika, że Killnet - w ciągu ostatnich 16 miesięcy – uderzał w domeny rządowych instytucji, policji i infrastruktury transportowej również naszego kraju. Na celowniku znalazł się m.in. porty lotnicze. Po tym, jak w lipcu 2022 zaatakowano kilkanaście portów lotniczych w Europie (Niemczech), co najmniej pięć systemów lokalnych lotnisk w Polsce było zablokowanych, zmuszając operatorów do szybkiego działania i wprowadzania nowych zabezpieczeń. *- Motywem hakerów są względy finansowe. Co trzeci atak kończy się utratą poufnych danych. Wymagane jest pilne wzmocnienie bezpieczeństwa systemów sieci lotnicznych –* wskazują eksperci Check Point Software.

Zaledwie dwa lata temu - w 2021 roku - Eurocontrol ostrzegał, że liczba ataków cybernetycznych na sektor lotnictwa wzrosła w ciągu roku przeszło pięciokrotnie. Jak widać, sytuacja wciąż nie ulega zmianie.

- *W ciągu ostatnich 16-18 miesięcy obserwujemy gwałtowny wzrost liczby powiązanych z państwami grup haktywistycznych, z których wiele popiera narrację rosyjską lub irańską. Ze strony rosyjskiej widzimy grupy takie jak Killnet, Noname057(16) czy Anonymous Russia, które agresywnie atakują różne organizacje w UE i Ameryce Północnej, w tym strony internetowe dotyczące infrastruktury krytycznej, takiej jak usługi użyteczności publicznej, lotniska, opieka zdrowotna i inne* – wyjaśnia Sergey Shykevich, specjalista cyberbezpieczeństwa z Check Point Software Technologies.

- *Chociaż prawie wszystkie ataki tych grup* (haktywistycznych – przyp. red) *koncentrują się na atakach DDoS skierowanych przeciwko publicznie dostępnym witrynom internetowym, w ciągu ostatniego miesiąca obserwujemy próby przejścia w kierunku operacji hakerskich, wycieków oraz wykorzystania programów wykradających informacje i innych rodzin złośliwego oprogramowania* – ostrzega ekspert Check Pointa.