TYSIĄCE PODMIOTÓW ZAGROŻONYCH PRZEZ CYBERATAKI NA ZLECENIE RZĄDÓW

Jak ostrzega firma Microsoft, cyberataki to narzędzie wybierane przez tych, którzy chcą wywierać wpływ na przebieg demokratycznych wyborów. Koncern poinformował równocześnie, że 10 tysięcy podmiotów korzystających z jego usług jest zagrożonych tego typu działaniami.

Przedstawiciele firmy stwierdzili, iż klienci, którzy są zdaniem Microsoftu zagrożeni aktywnością hakerów działających na zlecenie obcych rządów, zostali już o tym ryzyku ostrzeżeni.

Wiceprezes Microsoftu ds. bezpieczeństwa klientów i zaufania Tom Burt napisał, iż około 84 proc. ataków skierowanych na konkretne podmioty korzystające z usług firmy to działania przeciwko dużym organizacjom, takim jak międzynarodowe korporacje. Pozostałe 16 proc. cyberataków kierowanych jest przeciwko konsumenckim kontom poczty elektronicznej.

Według Burta, niektóre podmioty z grupy 10 tys. klientów firmy narażonych na sponsorowane przez inne państwa ataki hakerskie już ucierpiały w wyniku działań cyberprzestępców. Inne organizacje i firmy jedynie znalazły się na celowniku hakerów. Burt nie podał jednak szczegółowych danych liczbowych, jeśli chodzi o poszczególne grupy.

Microsoft ocenia, że różne państwa z powodzeniem wykorzystują cyberataki jako narzędzie gromadzenia informacji wywiadowczych, wywierania wpływu na geopolitykę bądź "osiągania innych celów". Według Burta wzmożoną aktywność obserwuje się obecnie ze strony pięciu grup hakerskich sponsorowanych przez Iran, Koreę Północną i Rosję. To m.in. grupa Holmium związana z Iranem, wymieniana również przez firmę FireEye jako APT33, która zajmuje się atakami przede wszystkim przeciwko celom zlokalizowanym w USA, Arabii Saudyjskiej i Korei Południowej. Ofiary hakerów z tego ugrupowania to najczęściej firmy z sektora obronnościowego, lotniczego i energetycznego.

Inna grupa hakerska zidentyfikowana przez Microsoft jako Strontium, znana również jako Fancy Bear czy APT28 to cyberprzestępcy pochodzący z Rosji, o których inna firma - CrowdStrike - informuje, iż działają od co najmniej 2008 roku i najprawdopodobniej współpracowali w przeszłości z rosyjskim wywiadem wojskowym GRU. APT28 to także grupa, która w 2016 roku przed wyborami prezydenckimi w USA jako jedna z dwóch siatek cyberprzestępczych dokonała ataku na Narodowy Komitet Partii Demokratycznej. Cyberprzestępcy z Fancy Bear mają na swoim koncie również ataki na niemiecki Bundestag, francuską stację telewizyjną TV5 Monde i Światową Agencję Antydopingową. Firma wskazała również na wzmożoną działalność mniej znanych grup hakerskich takich jak rosyjska Yttrium, irańska grupa Mercury oraz pochodząca z Korei Północnej Thallium.

SZP/PAP