HAKERZY ZMIENIAJĄ TAKTYKĘ CYBERATAKÓW NA PRZEDSIĘBIORSTWA

Hakerzy przeprowadzający cyberataki na przedsiębiorstwa zmieniają swoją taktykę, aby skuteczniej zaskakiwać swoje cele. Na popularności traci phishing, z kolei rośnie zainteresowanie naruszaniem bezpieczeństwa usług brzegowych.

Eksperci Fortinetu spadek natężenia kampanii phishingowych uzasadniają skutecznością działań edukacyjnych prowadzonych przez firmy, które dotąd były najczęściej wybieranym celem tego rodzaju cyberataków. Polegają one na dystrybucji złośliwego oprogramowania za pomocą specjalnie spreparowanych załączników do poczty elektronicznej lub na skłanianiu ofiar do kliknięcia w link, infekujący komputer bądź wykradający dane do logowania w usługach cyfrowych firmy.

Cyberprzestępcy częściej skupiają się obecnie na publicznych usługach brzegowych, takich jak infrastruktura internetowa czy protokoły komunikacji sieciowej. W ostatnim kwartale firma Fortinet zaobserwowała coraz częstsze wykorzystywanie luk, pozwalających na zdalne wykonanie kodu w atakowanych systemach, a metoda ta zyskała na popularności na całym świecie. Według specjalistów, choć ten sposób ataku nie jest nowy, może stanowić zaskoczenie dla działów IT w firmach, które spodziewają się przede wszystkich ataków phishingowych i na nie najbardziej przygotowują swoich pracowników.

Celem działania hakerów jest zdobycie większych środków finansowych, o czym świadczy coraz częściej obserwowana współpraca grup cyberprzestępczych i pojawienie się złośliwego oprogramowania szyfrującego dla okupu jako usługi dostępnej w tzw. dark webie. Eksperci ostrzegają, że narzędzia cyberprzestępców są nieustannie udoskonalane, w celu utrudnienia wykrycia cyberataków i przeprowadzania coraz bardziej wyrafinowanych operacji.

Skuteczną strategią działania pozostaje atakowanie starszych, nieaktualizowanych systemów. Fortinet odkrył, że hakerzy obecnie częściej atakują luki znane od 12 lub więcej lat, niż te podatności bezpieczeństwa, które zostały świeżo wykryte.

Firma uważa, że aby sprawniej zapobiegać aktywności hakerów niezbędne jest przyjęcie całościowego podejścia do zabezpieczania swoich środowisk sieciowych przez firmy - zarówno, jeśli chodzi o infrastrukturę lokalną, jak i tę rozproszoną. Pomóc może również wdrożenie narzędzi bezpieczeństwa opartych o sztuczną inteligencję i automatyzację działań, które znacząco zmniejszają szanse na włamanie do infrastruktury. Jak podkreśla Fortinet, kluczową kwestią w przeciwdziałaniu cyberatakom jest dynamiczna, proaktywna i inteligentna identyfikacja zagrożeń, gdyż tylko ona pozwala na zaobserwowanie ewolucji metod ataków i zapewnienie tzw. cyfrowej higieny w firmach.