**Cyberataki na przeglądarki stały się zmorą 2024 roku. Hakerzy wymusili w tym roku najwyższy okup sięgający 75 mln dolarów!**

**W 2024 roku cyberprzestępcy skupili się na atakach na przeglądarki internetowe, wykorzystując ich podatności - podsumowują kończący się rok eksperci Check Point Software. W mijającym roku wymuszono najwyższy okup (na rzecz grupy Dark Angels), który wyniósł aż 75 milionów dolarów. Ataki były szczególnie dotkliwe dla sektora opieki zdrowotnej i administracji rządowej, które doświadczyły łącznie 67% wszystkich ataków ransomware. Średni koszt naprawy skutków ataku dla firm oszacowano na 2,57 mln dolarów.**

Podczas, gdy w 2024 roku firmy coraz bardziej polegały na platformach SaaS, aplikacjach chmurowych, pracy zdalnej i politykach BYOD (Bring Your Own Device), systematycznie rosła liczba ataków napędzanych przez sztuczną inteligencję, ransomware jako usługa (RaaS) oraz podatności typu zero-day w przeglądarkach internetowych. Tradycyjne rozwiązania, takie jak zabezpieczenia punktów końcowych, SaaS czy poczty e-mail, okazały się niewystarczające. Zaawansowane technologie, polityka ochrony przeglądarek (w biurach i prywatnie) stała się kluczowym elementem dla firm chcących zabezpieczyć swoje cyfrowe miejsca pracy.

Alarmująca była również skala tegorocznych ataków phishingowych i socjotechnicznych realizowanych we współpracy z AI. Cyberprzestępcy wykorzystywali generatywną sztuczną inteligencję do tworzenia wiadomości phishingowych niemal nie do odróżnienia od autentycznych komunikatów. Z raportu *GlobeNewswire* wynika, że aż 89% zagrożeń w przeglądarkach pochodziło właśnie z phishingu, a atakujący skuteczniej omijali tradycyjne filtry zabezpieczające.

RaaS (ransomware jako usługa) w 2024 roku stał się niespotykanie popularnym środkiem działania przestępców. Średnia żądana kwota okupu w pierwszej połowie 2024 roku wynosiła ponad 5,2 mln dolarów! Ale w mijającym roku padł również rekord okupu zapłaconego hakerom - 75 milionów dolarów.

Check Point Software Technologies odnotował ponadto wzrost podatności zero-day w przeglądarkach, takich jak Chrome i Edge. Szczególnie głośna była luka CVE-2024-7971 w silniku JavaScript V8 Chrome, która pozwalała hakerom na zdalne uruchamianie złośliwego kodu. Skutki były dotkliwe – przestoje operacyjne, wycieki danych oraz kosztowne procesy odzyskiwania.