

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **84** ze dne **26.9.2024**

Vyděrači hledají citlivé údaje v ukradených datech, aby zlomili oběti, které odmítají zaplatit

Společnost Sophos zveřejnila novou studii s názvem "Utahování šroubů: Nátlakové techniky ransomwarových gangů", která podrobně popisuje, jak kyberzločinci využívají ukradená data ke zvýšení nátlaku na oběti, které odmítají zaplatit. Tyto techniky zahrnují například zveřejňování osobních údajů nebo vyhrožování, že nahlásí úřadům informace o podezřelých obchodních aktivitách odhalené v ukradených datech.

"V prosinci 2023, v souvislosti s narušením bezpečnosti kasina MGM, začal Sophos upozorňovat na sklon ransomwarových gangů zneužívat média jako nástroj nejen ke zvýšení tlaku na své oběti, ale také k převzetí kontroly nad celým příběhem a přesunutí viny. Gangy si také vybírají vedoucí představitele firem, které označují za 'zodpovědné' za ransomwarové útoky. V jednom z nalezených příspěvků útočníci zveřejnili fotografii majitele firmy s ďábelskými rohy a jeho číslo sociálního pojištění. V jiném příspěvku útočníci vyzývali zaměstnance, aby od své společnosti požadovali 'odškodnění', a v dalších případech útočníci vyhrožovali, že budou o úniku dat informovat zákazníky, partnery a konkurenci. Tyto snahy vytvářejí hromosvod obvinění, zvyšují tlak na firmy, aby zaplatily, a potenciálně prohlubují poškození pověsti v důsledku útoku," řekl Christopher Budd, ředitel výzkumu hrozeb ve společnosti Sophos.

Bezpečnostní experti společnosti Sophos našli na dark webu i několik příspěvků ransomwarových útočníků, kteří podrobně popisují své plány na hledání informací v ukradených datech, které by mohly být použity jako páka, pokud společnost nezaplatí. V jednom příspěvku například ransomwarový útočník WereWolves uvádí, že veškerá ukradená data podléhají "trestněprávnímu posouzení, obchodnímu posouzení a posouzení z hlediska důvěryhodnosti informací pro konkurenci". V dalším příkladu ransomwarová skupina Monti uvedla, že našla zaměstnance cílové společnosti, který hledal materiály týkající se sexuálního zneužívání dětí, a pohrozila, že pokud společnost nezaplatí výkupné, obrátí se s těmito informacemi na policii.

Útočníci aktivně v ukradených datech pátrají

Tyto příspěvky zapadají do širšího trendu, kdy se zločinci snaží vydírat společnosti stále citlivějšími údaji o zaměstnancích, klientech nebo pacientech, včetně záznamů o duševním zdraví a zdravotních záznamů dětí, informací o sexuálních problémech pacientů a snímků nahých pacientů. V jednom případě ransomwarová skupina Qiulong zveřejnila osobní údaje dcery generálního ředitele a odkaz na její profil na Instagramu.

"Ransomware gangy jsou stále invazivnější a odvážnější v tom, jak a čím se vyzbrojují. Tlak na společnosti se ještě zvyšuje, protože nejen kradou data a vyhrožují jejich únikem, ale aktivně je analyzují a hledají způsoby, jak maximalizovat škody a vytvořit nové příležitosti k vydírání. To znamená, že organizace se musí obávat nejen špionáže a ztráty obchodního tajemství nebo nezákonné činnosti zaměstnanců, ale také propojení těchto problémů s kybernetickými útoky," řekl Budd.

Zdroj: AVcentrum ČR