Ubytovací služby pod útokem nových e-mailových podvodů

11.6.2024 - | PROTEXT

Podvržené e-maily jsou zasílány na veřejné e-mailové adresy hotelů a napodobují obvyklé dotazy či stížnosti hostů nebo se tváří jako naléhavé žádosti společnosti Booking.com o vyřízení připomínek uživatelů.

Ve skutečnosti však jde o e-maily od útočníků, kteří chtějí vylákat od zaměstnanců hotelu například přihlašovací údaje nebo je přimět, aby si stáhli malware.

Podvodníci vytvářejí e-maily s věrohodnými důvody tak, aby vypadaly jako skutečné žádosti nebo stížnosti zákazníků, jejichž řešení je běžnou součástí povinností hotelového personálu. V pohostinství se samozřejmě klade velký důraz na dobrou pověst, a proto se zaměstnanci snaží na tyto e-maily rychle reagovat. Tato snaha zvyšuje pravděpodobnost, že kliknou na nebezpečný odkaz nebo otevřou škodlivou přílohu, a tím se chytí do nastražené pasti. Útočníci přitom odesílají podvodné e-maily prostřednictvím známých bezplatných e-mailových služeb, jako je Gmail, které hosté normálně používají. Pro zaměstnance hotelů je tak obtížnější rozlišovat mezi běžnými legitimními a klamnými nebezpečnými zprávami.

Podvodné e-maily lze obecně rozdělit do dvou kategorií. První z nich obsahují fiktivní stížnosti bývalých „hostů“. Popisují negativní zkušenosti, jako je hrubé chování personálu nebo neuklizené pokoje, někdy s odkazy na fotografie nebo videa. Cílem je přimět zaměstnance, aby klikali na odkazy nebo otevírali přílohy obsahující malware. Do druhé kategorie patří e-maily, které napodobují dotazy potenciálních hostů. Ptají se na vybavení, ceny či dostupnost pokojů nebo žádají o pomoc s plánováním cesty. Cílem útoků je shromáždit citlivé informace a prodat je na darknetových fórech nebo je rovnou použít pro další útoky, například na hosty napadených hotelů.

„Útočníci využívají k dosažení svých cílů často nejzranitelnější aspekty podniku. V pohostinství spoléhají na starostlivost zaměstnanců hotelových služeb, kteří se snaží vycházet vstříc zákazníkům. Napodobováním dotazů nebo stížností hostů manipulují se snahou personálu rychle řešit problémy, čímž zvyšují pravděpodobnost, že se stanou obětí podvodného jednání. Na ochranu proti těmto útokům by měly podniky v hotelovém průmyslu zavést robustní systémy filtrování e-mailů, pravidelně školit zaměstnance, jak rozpoznat pokusy o zneužití, a zavést postupy pro preventivní ověřování pravosti naléhavých žádostí,“ řekla Anna Lazaricheva, analytička spamu ve společnosti Kaspersky.

Podle výroční zprávy o spamu a phishingu, kterou vydala společnost Kaspersky, představují phishing a malware šířené prostřednictvím e-mailů i nadále významnou kybernetickou hrozbu. V loňském roce zablokoval Kaspersky Mail Anti-Virus 135 980 457 škodlivých e-mailových příloh, zatímco systém Anti-Phishing zabránil 709 590 011 pokusům o přístup k phishingovým odkazům. Odesílatelé phishingových a škodlivých e-mailů se často vydávají za důvěryhodné subjekty a využívají sofistikované taktiky sociálního inženýrství, aby přiměly příjemce k vyzrazení důvěrných údajů nebo k aktivaci škodlivých odkazů.

Odborníci společnosti Kaspersky na ochranu před phishingovými útoky a úniky dat doporučují:

https://www.ceskenoviny.cz/tiskove/zpravy/ubytovaci-sluzby-pod-utokem-novych-e-mailovych-podvodu/2530506