

ESET: Podvodníci z online bazarů se nově zaměřili na ubytovací platformy Booking.com a Airbnb

10.10.2024 - Lucie Mudráková, Vítězslav Pelc | ESET software

Společnost ESET zveřejnila nové informace o kybernetických zločincích využívajících online nástroj Telekopí (Telekopye), který funguje v rámci platformy Telegram. Útočníkům slouží k vytváření podvodné komunikace a koordinaci jednotlivých členů různě velkých kyberkriminálních uskupení, a to především k organizování podvodů na internetových trzích, jako je Vinted, eBay, Facebook Marketplace, Bazoš či Sbazar. Podle posledních informací se podvodníci navíc zaměřili také na populární služby pro rezervace ubytování Booking.com a Airbnb. V rámci těchto podvodů zneužívají legitimní účty hotelů a pronajímatelů ubytování s cílem přimět oběti k zadání údajů z platebních karet do formulářů na falešných webových stránkách. Útočníci byli nejvíce aktivní v období letní sezóny, kdy počet těchto podvodů více než dvojnásobně překročil počet podvodů na online trzích. S ohledem na popularitu obou platformů útočníci cílí na uživatele z celého světa.

Organizovaná síť podvodníků podle expertů z ESETu vylepšila také proces výběru obětí a zacílení na rezervační stránky služeb Booking.com a Airbnb. Phishingové podvodné webové stránky, které útočníci dokáží díky nástroji Telekopí vytvořit, jsou tak ještě uvěřitelnější, než tomu bylo v podvodech na bazarových platformách. Telekopí (kombinace slov Telegram a kopí neboli také Telekopye) je nástroj, který funguje jako tzv. Telegram bot. Umožňuje i méně technicky zdatným útočníkům vytvářet phishingové stránky z přednastavených šablon, generovat QR kódy a falešné screenshoty a rozesílat podvodné e-maily či SMS zprávy.

„Zatímco v případě podvodů na internetových bazarech bývají útočníci nejvíce aktivní kolem výplatních dnů, kdy předpokládají, že lidé budou více utrácet své peníze, v případě podvodů na ubytovacích platformách využili hlavně období letních prázdnin. S ohledem na velký nárůst tohoto nového typu podvodů se lze domnívat, že je nový scénář pro podvodníky natolik atraktivní, že v něm budou pokračovat i v budoucnu. Cílem podvodů jsou uživatelé bez ohledu na to, odkud pocházejí. A protože jsou služby jako Booking.com nebo Airbnb oblíbené i mezi českými uživateli, měli by být při rezervacích pobytů přes tyto platformy opatrní, a to především kolem větších svátků a prázdnin,“ říká Radek Jizba, expert z výzkumného týmu pražské pobočky společnosti ESET.

„Uživatelům bych doporučil, aby se před vyplněním jakýchkoli formulářů souvisejících s rezervací dovolené vždy ujistili, že neopustili oficiální webovou stránku nebo aplikaci dané platformy. Pokud jste přesměrováni na jinou, externí URL adresu, kde byste měli dokončit rezervaci a následně provést platbu, měli byste zbystřit. Takové chování může poukazovat na možný podvod,“ dodává Jizba.

Nástroj Telekopí používají podle informací společnosti ESET desítky podvodných skupin, kdy každá z nich může mít až tisíc členů. Právě díky tomuto nástroji dokázali útočníci proměnit podvody na bazarových platformách v nezákonný organizovaný byznys. Útoky přicházejí nejčastěji z Ruska, Ukrajiny a Uzbekistánu, odkud pocházejí jak autoři nástroje Telekopí, tak jednotliví podvodníci, kteří ho využívají. Podle bezpečnostních expertů z ESETu ale mohou pocházet i ze zemí EU. Finanční škody spojené s těmito podvody činí již více než 100 milionů korun.

Podvodníci ze skupin organizovaných kolem nástroje Telekopí označují své oběti jako tzv. mamuty. V

rusky mluvících zemích je to označení pro někoho, „kdo se snadno nachytá“. Podvodníci, které experti z ESETu označují jako neandrtálce, potřebují díky Telekopí k uskutečnění podvodů jen minimální nebo žádné technické znalosti, o vše se postará samotný nástroj.

Podle dat společnosti ESET začaly podvody s rezervacemi na ubytovacích platformách nabírat na síle až v letošním roce. K prudkému nárůstu došlo v červenci, kdy počet těchto případů poprvé překonal počet podvodů s využitím Telekopí na online tržištích, a to více než dvojnásobným počtem detekcí. V srpnu a září 2024 byl pak počet podvodů pro obě sledované kategorie na podobné úrovni.

Oběťmi jsou tentokrát uživatelé rezervující pobyty v prázdninových destinacích, přičemž útočníci podle expertů z ESETu cílí tyto útoky globálně. Na rozdíl od podvodů v prostředí online tržišť, kde se podvodníci zaměřují na širokou škálu různých provozovatelů, se podvody kolem rezervací pobytů soustředily především kolem dvou zmíněných platforem – Booking.com a Airbnb. Jen za letošní rok přitom podvody na těchto dvou platformách dosáhly třetiny všech detekovaných podvodů pomocí Telekopí.

Podle nejnovějšího scénáře zasílají podvodníci obětem e-mail či zprávu v oficiálním chatu ubytovací platformy, ve které tvrdí, že došlo k problému s platbou za rezervaci. Zpráva obsahuje odkaz na falešnou, ale velmi dobře vytvořenou a legitimně vypadající webovou stránku napodobující jednu ze dvou zmíněných platforem. Stránka obsahuje předvyplněné informace o rezervaci, jako je termín příjezdu a odjezdu, cena a místo. Informace uvedené na podvodných stránkách navíc odpovídají skutečným rezervacím, které uživatelé vytvořili. Cílem podvodníků je opět přimět oběti k tomu, aby prostřednictvím formulářů na falešných stránkách zadali údaje ke své platební kartě.

„Podvodníci využívají již dříve kompromitované účty legitimních hotelů a pronajímatelů ubytování na těchto platformách. Přístupy k těmto účtům pravděpodobně získávají nákupem ukradených přihlašovacích údajů na kyberzločineckých fórech. Díky přístupu k nim vyhledávají uživatele, kteří si nedávno rezervovali pobyt, za který buď ještě nezaplatili, nebo zaplatili poměrně nedávno, a na ty se zaměří,“ vysvětluje Jizba. „Tím, že zločinci mohou k získaným účtům takto přistupovat, jsou tyto podvody mnohem obtížněji odhalitelné. Oběti na informacích nevidí nic podezřelého, a také webové stránky vypadají naprosto legitimně. Jedinými viditelnými znaky, které naznačují, že něco není v pořádku, jsou URL adresy webových stránek, které neodpovídají napodobovaným, legitimním webům,“ dodává Jizba z ESETu.

Jelikož útočníci v rámci těchto podvodů zneužívají kompromitované účty poskytovatelů ubytování, bezpečnostní experti uživatelům nedoporučují kontaktovat tyto poskytovatele napřímo, jelikož se nejedná o spolehlivý způsob ověření, že je žádost o platbu legitimní. V případě pochybností by měli kontaktovat oficiální zákaznickou podporu platformy Booking.com či Airbnb.

Pro ochranu svých účtů vždy používejte silné a unikátní heslo a ověření přihlášení dalším faktorem. Vícefázové ověřování by mělo být zapnuté u všech účtů, kde je to možné. Se správou hesel může uživatelům pomoci také specializovaný program, který hesla uchovává v zašifrované podobě a automaticky je dosazuje při přihlašování do jejich účtů. Správci hesel, jak se tyto programy nazývají, bývají součástí komplexních bezpečnostních řešení.

Fungování nástroje Telekopí a pozadí podvodů na internetových bazarech představil ESET ve spolupráci s Policií ČR poprvé v srpnu 2023. Koncem roku 2023 poté ve dvou společných operacích zatkla česká a ukrajinská policie desítky kyberzločinců využívajících Telekopí, a to včetně klíčových hráčů těchto podvodů. Obě operace byly zaměřeny proti bližší nespecifikovanému počtu skupin, které podle odhadů policie od roku 2021 nashromáždily nejméně 100 milionů korun.

Bezpečnostní experti z ESETu pak nejnovější informace o využití nástroje Telekopí prezentovali na

letošní konferenci Virus Bulletin 2024. Podrobné technické informace najdete také na webu welivesecurity.com.

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost najdete například v online magazínu Dvojklík.cz nebo v online magazínu o IT bezpečnosti pro firmy Digital Security Guide. Nejčastějším rizikům pro děti na internetu se věnuje iniciativa Safer Kids Online, která má za cíl pomoci nejen jejich rodičům, ale také například učitelům či vychovatelům zorientovat se v nástrahách digitálního světa.

Společnost ESET ve spolupráci s kyberbezpečnostními odborníky dále připravuje podcast True Positive. Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET.

Společnost ESET již od roku 1987 vyvíjí bezpečnostní software pro domácí i firemní uživatele. Drží rekordní počet ocenění a díky jejím technologiím může více než miliarda uživatelů bezpečně objevovat možnosti internetu. Široké portfolio řešení od ESET pokrývá všechny populární platformy, včetně mobilních, a poskytuje neustálou proaktivní ochranu při minimálních systémových nárocích.

ESET dlouhodobě investuje do vývoje. Jen v České republice nalezneme tři výzkumná a vývojová centra, a to v Praze, Jablonci nad Nisou a Brně. Společnost ESET má lokální zastoupení v Praze, celosvětovou centrálu v Bratislavě a disponuje rozsáhlou sítí partnerů ve více než 200 zemích světa.

<https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/eset-podvodnici-z-online-bazaru-se-nove-z-amerili-na-ubytovaci-platformy-bookingcom-a-airbnb>