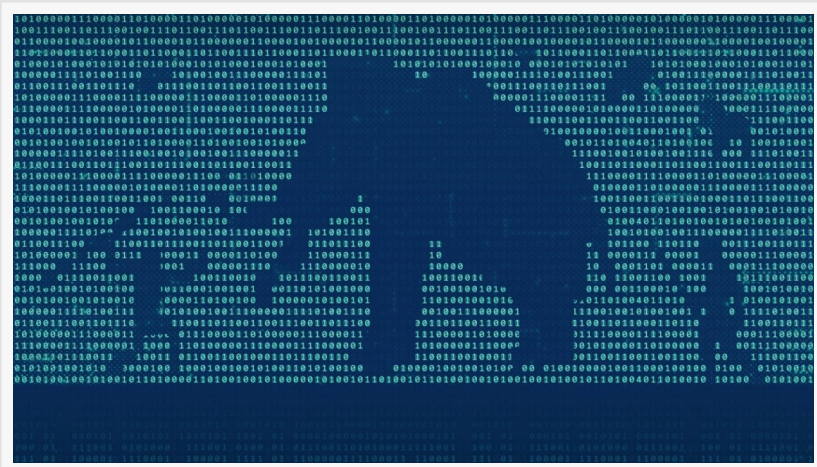
ESET Research: Telekopye scammer network targets Booking.com and Airbnb



DUBAI, DUBAI, UNITED ARAB EMIRATES, October 22, 2024 /EINPresswire.com/ -- ESET researchers discovered that the organized scammer network Telekopye has expanded its operations to target users of popular accommodation booking platforms like Booking.com and Airbnb. They have also increased the sophistication of their victim selection and of targeting the two booking sites, where the phishing pages are even more believable than regular online marketplace ones. Telekopye is a toolkit that operates as a Telegram bot turning online marketplace scams into illicit organized business. It is used by dozens of scam groups with up to thousands of members to steal millions of euros from their victims. ESET Research presented the latest findings about Telekopye at the 2024 Virus Bulletin conference.

In the Telekopye scammer network, the scammers refer to the targeted buyers and sellers as Mammoths. The scammers, called Neanderthals by ESET researchers, require little to no technical knowledge – Telekopye takes care of everything in a matter of seconds. According to ESET telemetry, the booking scams started gaining traction in 2024. The accommodation-themed scams saw a sharp uptick in July, surpassing Telekopye's marketplace scams for the first time, with more than double the detections. In August and September, the two categories continued at similar levels.

The growing popularity of online marketplaces has attracted fraudsters preying on unsuspecting buyers and sellers, looking to score credit card information rather than bargains. As this booking scam increase coincides with the summer holiday season in the targeted regions – prime time for taking advantage of people booking stays – it remains to be seen if this trend continues. Based on the 2024 data, these newer scams have amassed approximately half of the detection numbers of the marketplace variants. The newer scams focus mainly on two platforms – Booking.com and Airbnb – compared to the wide variety of online marketplaces targeted by Telekopye.

In this new scam scenario, scammers send an email to a targeted user of one of these platforms, claiming an issue with their booking payment. The email contains a link to a well-crafted, legitimate-looking web page mimicking the abused platform. The page contains prefilled information about a booking, such as the check-in and check-out dates, price, and location – and the information provided on the fraudulent pages matches real bookings made by the targeted users.

"The scammers achieve this by utilizing compromised accounts of legitimate hotels and accommodation renters on the platforms, which they most likely obtain through purchasing stolen credentials on cybercriminal forums. Using their access to these accounts, the scammers single out users who recently booked a stay and haven't paid yet – or paid very recently – and target them," explains ESET researcher Radek Jizba, who discovered and analyzed Telekopye. "This approach makes the scam much harder to spot, as the information provided is personally relevant to the victims and the websites look as expected. The only visible signs of something being amiss are the websites' URLs, which do not match the impersonated, legitimate websites," he adds.

Besides diversifying their target portfolio, Neanderthals have also tried to improve their tools and operations to increase their gains.

"Before filling out any forms related to your booking, always make sure you haven't left the official website or app of the platform in question. Being directed to an external URL to proceed with your booking and payment is a strong indicator of a scam," advises Jizba.

In late 2023, after ESET Research had published its two-part series on Telekopye, Czech and Ukrainian police arrested tens of cybercriminals utilizing Telekopye, including the key players, in two joint operations. Both operations were aimed against a further unspecified number of Telekopye groups, which had accumulated at least €5 million since 2021, based on police estimates.

For a more detailed analysis about the latest Telekopye activities, check out the latest ESET Research whitepaper "Marketplace scams: Neanderthals hunting Mammoths with Telekopye" on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X) for the latest news from ESET Research.

About ESET
ESET® provides cutting-edge digital security to prevent attacks before they happen. By combining the power of AI and human expertise, ESET stays ahead of known and emerging cyberthreats — securing businesses, critical infrastructure, and individuals. Whether it's endpoint, cloud or mobile protection, our AI-native, cloud-first solutions and services remain highly effective and easy to use. ESET technology includes robust detection and response, ultra-secure encryption, and multifactor authentication. With 24/7 real-time defense and strong local support, we keep

users safe and businesses running without interruption. An ever-evolving digital landscape demands a progressive approach to security: ESET is committed to world-class research and powerful threat intelligence, backed by R&D centers and a strong global partner network. For more information, visit www.eset.com or follow us on LinkedIn, Facebook, and X.

Sanjeev Kant
Vistar Communications
+ +971 55 972 4623
email us here