Cybergefahr im Hype: Hamster Kombat zieht Hacker an

Cyberkriminelle missbrauchen das beliebte Blockchain-Game "Hamster Kombat", um Daten von Nutzern auf Android und Windows zu stehlen.

24.07.2024 – 09:30

In der heutigen digitalen Welt sind Online-Spiele wie „Hamster Kombat“ mehr als nur Unterhaltung. Sie bringen Millionen von Nutzern zusammen und schaffen gleichzeitig neue Möglichkeiten für Cyberkriminalität. Das Telegram-basierte Clicker-Spiel hat in den letzten drei Monaten erstaunliche 240 Millionen Spieler gewonnen. Dieser enorme Zulauf zieht jedoch nicht nur Liebhaber des Spiels an, sondern weckt auch das Interesse von Hackern, die Nutzen aus dieser Beliebtheit ziehen wollen.

Das Spiel im Überblick

„Hamster Kombat“ ist ein einfach gehaltenes Clicker-Spiel, bei dem Nutzer durch Klicken auf einen Bildschirmbutton virtuelle Münzen sammeln können. Diese Währung dient zur Finanzierung von Power-ups oder kurzzeitigen Verbesserungen im Spiel und ermöglicht es den Spielern, durch das Erfüllen bestimmter Aufgaben, wie dem Beitritt zum Telegram-Kanal, zusätzliche Münzen zu verdienen. Das Besondere an diesem Game ist, dass es ausschließlich über den Telegram-Messenger gespielt wird. In naher Zukunft soll außerdem ein Airdrop stattfinden, der den Spielern die Möglichkeit gibt, die neue Kryptowährung HMSTR zu erhalten.

Bedrohungen durch Cyberkriminalität

Trotz seines unterhaltsamen Konzepts birgt das Spiel erhebliche Risiken. Forscher von ESET haben aufgedeckt, dass Cyberkriminelle gefälschte App-Stores und Malware entwickeln, um Daten von Android- und Windows-Nutzern zu stehlen. Diese Angriffe zielen vorrangig darauf ab, persönliche Informationen und Krypto-Wallets zu kompromittieren. Lukas Stefanko, Forscher bei ESET, weist darauf hin: „Die Popularität von Hamster Kombat macht es attraktiv für Missbrauch. Das heißt: Auch in Zukunft wird das Spiel wahrscheinlich weitere Betrüger anziehen.“

Die verschiedenen Typen von Bedrohungen

- Eine bedrohliche Android-App, die sich als „Hamster Kombat“ tarnt und als Spyware fungiert. Diese App kann Benachrichtigungen stehlen und SMS-Versand initiieren, was den Hackern erlaubt, im Namen der Nutzer unbemerkt Dienste zu abonnieren.
- Gefälschte Hilfs-Tools für Windows, die Nutzer mit vermeintlich nützlichen Spielhilfen anlocken. Diese Tools enthalten versteckte Schadsoftware, die auf sensible Informationen abzielt, wie Krypto-Wallets und Passwörter.

Reaktion der Community

Trotz der wachsenden Bedrohung durch Cyberkriminalität sind viele Spieler von der Einfachheit und dem potenziellen Verdienst des Spiels begeistert. Diese Faszination für die Möglichkeit, mit dem neuen Kryptocoin Geld zu verdienen, treibt die Nutzerzahlen weiter in die Höhe. Allerdings ist die Versuchung, an solch populären Trends teilzuhaben, nicht ohne Risiko. In einer Zeit, in der Daten die neue Währung darstellen, ist es unerlässlich, dass Nutzer sich über die Gefahren bewusst sind und Maßnahmen zum Schutz ihrer Informationen ergreifen.

Ein Trend mit Perspektiven

Die Herausforderungen, die mit der Explosion von Spielen wie „Hamster Kombat“ einhergehen, spiegeln einen größeren Trend in der Gaming-Industrie wider. Die Kombination aus mobiler Zugänglichkeit und der potenziellen finanziellen Belohnung zieht sowohl ehrliche Spieler als auch Kriminelle an, was eine ständige Wachsamkeit erfordert. Die Nutzer sind nun gefordert, sich nicht nur um ihre Unterhaltung, sondern auch um ihren Datenschutz zu kümmern.

Für weitergehende Informationen zu den Bedrohungen rund um „Hamster Kombat“ können Interessierte den Blogbeitrag „Hamster im Fadenkreuz“ auf WeLiveSecurity.com besuchen.

Pressekontakt:

ESET Deutschland GmbH

Christian LuegHead of Communication & PR DACH+49 (0)3641 3114-269 christian.lueg@eset.de

Michael KlattePR Manager DACH+49 (0)3641 3114-257 Michael.klatte@eset.de

Philipp PlumPR Manager DACH+49 (0)3641 3114-141 Philipp.plum@eset.de

Folgen Sie ESET: **www.ESET.de**

ESET Deutschland GmbH, Spitzweidenweg 32, 07743 Jena, Deutschland

Original-Content von: ESET Deutschland GmbH, übermittelt durch news aktuell

– **NAG**

Details