**Hakerzy zaatakowali inwestorów kryptowalut. Skradziono ponad 9 milionów dolarów w kryptowalutach.**

**Hakerzy okradli w ciągu 6 miesięcy ponad 9 milionów dolarów grupie 30 tys. inwestorów kryptowalut. To wszystko dzięki Inferno Drainer, jednemu z najbardziej przebiegłych i dochodowych mechanizmów wykradania kryptowalut – alarmują eksperci Check Point Research.**

*- Ostatnie ataki pokazują jak bardzo cyberprzestępczość się sprofesjonalizowała. Inferno Drainer nie tylko kradnie kryptowaluty; rozwija on oszustwa na wzór startupu, z siecią partnerów, własną infrastrukturą i ciągłymi aktualizacjami. Ekosystem kryptowalut musi wreszcie zdać sobie sprawę, jak zaawansowane i uporczywe stały się te zagrożenia* – uważa Eli Smadja, menedżer w Check Point Software Technologies.

Check Point odkrył, że działalność Inferno Drainera przyniosła w ostatnim półroczu **ponad 30 000** ofiar w ponad **30 blockchainach**. Rekordowa jednorazowa strata użytkownika sięgnęła **761 000 dolarów**, czyli ponad 2,9 mln PLN! Szacuje się, że wszystkie kradzieże przypisywane Inferno Drainer mogą przekraczać łącznie nawet **250 milionów dolarów**.

Inferno Drainer to przykład modelu **Drainer-as-a-Service (DaaS)** – zorganizowanej usługi przestępczej, w której operatorzy udostępniają zestawy narzędzi phishingowych swoim „partnerom”, zapewniając im infrastrukturę, dedykowane skrypty i bieżące wsparcie techniczne. Według analityków Check Point Research, obecna wersja oprogramowania cechuje się niespotykanym poziomem zaawansowania technologicznego.

Wersja z 2025 roku wprowadza szereg nowoczesnych mechanizmów utrudniających wykrycie i przeciwdziałanie atakom. Posiada szyfrowaną komunikację C&C w łańcuchu Binance Smart Chain, czy **jednorazowe smart kontrakty**, które ulegają samozniszczeniu po pojedynczym użyciu. **Narzędzie umożliwia wykorzystanie protokołu OAuth2 i bezpiecznych proxy** do omijania filtrów przeglądarek, portfeli i narzędzi antyphishingowych, a**wielowarstwowe szyfrowanie AES i głęboka obfuskacja kodu**, chroni przed analizą ekspertów ds. bezpieczeństwa.

**Jak działa atak?**

Ataki Inferno Drainer bazują głównie na manipulacji użytkownikiem. Wg analityków Check Point Research można je opisać w trzech punktach:

l Hakerzy przejmują linki zaproszeń na Discordzie lub podszywają się pod popularne boty (np. Collab.Land).

l Podszywając się pod interfejsy weryfikacyjne, nakłaniają ofiary do podłączenia portfela i podpisania „niewinnej” transakcji.

l W rzeczywistości użytkownicy autoryzują złośliwe smartkontrakty lub udzielają nieświadomie stałego dostępu do tokenów.

W niektórych przypadkach użytkownicy przesyłają tokeny na wcześniej przygotowane adresy, bez jakiejkolwiek interakcji, co uniemożliwia portfelowi ostrzeżenie o zagrożeniu.

**Jak się chronić?**

Eksperci z Check Point Research zalecają użytkownikom regularne sprawdzanie adresów URL i korzystanie tylko z oficjalnych źródeł – najlepiej zapisywać je jako zakładki, używanie „burner wallets” do testowania airdropów i nowych projektów, sprawdzanie czy bot Discorda ma oznaczenie Verified App. Niezbędna jest również analiza każdego wniosku o podpisanie transakcji – doradzają eksperci.