Bitdefender

Północnokoreańscy hakerzy czerpią zyski z witryn hazardowych zawierających złośliwe oprogramowanie

16.02.2024

Eksperci ds. cyberbezpieczeństwa zauważyli nową nielegalną działalność generującą przychody wśród północnokoreańskich hakerów: tworzenie witryn hazardowych zawierających złośliwe oprogramowanie i sprzedawanie ich innym cyberprzestępcom.

Witryny hazardowe zamienione w MaaS

Innymi słowy, aktywność tę można postrzegać jako konkretną gałąź złośliwego oprogramowania jako usługi (MaaS), która zapewnia dostęp do w pełni rozwiniętej fałszywej witryny internetowej zamiast pojedynczego szkodliwego oprogramowania.

Odkrycia dokonała południowokoreańska Narodowa Służba Wywiadowcza (NIS), która wskazała, że kilka południowokoreańskich grup cyberprzestępczych kupiło już szkodliwe strony internetowe od północnokoreańskich sprawców.

Organizacja Korei Północnej stojąca za nową formą oszustwa hazardowego

Według doniesień ekspertów do spraw cyberbezpieczeństwa z Korei Południowej grupą odpowiedzialną za tworzenie i rozpowszechnianie witryn hazardowych zawierających złośliwe oprogramowanie jest „Gyeongheung" – organizacja informatyczna powiązana z Pokojem nr 39 Partii Pracy w Korei Północnej. Ta ostatnia to tajna północnokoreańska organizacja partyjna, która rzekomo finansuje fundusze typu slush w walutach obcych i zarządza nimi dla przywódców kraju.

Aby ominąć sankcje Rady Bezpieczeństwa ONZ zabraniające zatrudniania pracowników z Korei Północnej, członkowie Gyeongheung sfałszowali chińskie dowody osobiste i ukradli referencje zawodowe pracownikom branży IT.

Eksperci uważają, że ogromne zyski już zostały zgromadzone

Cyberprzestępcy mogą wynająć złośliwą witrynę hazardową za około 5000 dolarów miesięcznie. Jeśli potrzebują pomocy technicznej od twórców witryny, muszą wydać dodatkowe 3000 dolarów. Według doniesień w przypadku witryn internetowych, które mogą gromadzić dużą ilość danych bankowych z kont Paypal obywateli Chin, najemcy

usług cyfrowych muszą zapłacić właścicielom dodatkową opłatę w wysokości od 2000 do 5000 dolarów.

NIS uważa, że sprawcy niedawnego oszustwa związanego z witryną hazardową zgromadzili już wielomilionowe zyski.

Funkcja zautomatyzowanych zakładów wzbogacona złośliwym oprogramowaniem kradnącym dane

Według agencji NIS fałszywe witryny internetowe ukrywały złośliwy kod w automatycznej funkcji obstawiania zakładów, która była wykorzystywana do zbierania danych osobowych od niczego niepodejrzewających graczy. Podmioty zagrażające próbowały już sprzedać około 1100 bitów danych osobowych obywateli Korei Południowej.

„Najnowszy sposób zdobywania nielegalnych środków przez północnokoreańskich hakerów jasno pokazuje, że internauci zainteresowani hazardem powinni dokładnie weryfikować platformę, z której chcą korzystać. Jeśli planujesz uczestniczyć w grach losowych, lub dokonywać zakładów, to unikaj witryn powiązanych z jakimikolwiek podmiotami z krajów rządzonych przez władze autorytarne. Zamiast tego wybieraj te zalegalizowane w Twoim kraju. Pamiętaj także o tym, aby odpowiednio zabezpieczyć swoje urządzenie za pomocą skutecznego systemu antywirusowego, które uchroni Cię przed złośliwym oprogramowaniem” – mówi Krzysztof Budziński z firmy Marken Systemy Antywirusowe, polskiego dystrybutora Bitdefender.

Źródło: https://bitdefender.pl/polnocnokoreanscy-hakerzy-czerpia-zyski-z-witryn-hazardowych-zawierajacych-zlosliwe-oprogramowanie/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 16.02.2024
Z pozdrowieniami Piotr Rozmiarek
E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender
Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.