Bitdefender

Mołdawianin poddany ekstradycji do USA w związku z rynkiem skradzionych danych uwierzytelniających za pomocą E-Roota

25.10.2023

Sandu Diaconu, 31-letni obywatel Mołdawii, został poddany ekstradycji z Wielkiej Brytanii do Stanów Zjednoczonych, aby stanąć przed sądem w związku z jego rzekomym administrowaniem osławionym rynkiem E-Root, który specjalizował się w handlu skradzionymi danymi uwierzytelniającymi.

Ekstradycja, której powodem była sprzedaż danych za pomocą E-Roota

Ekstradycja Mołdawianina nastąpiła na podstawie nakazu wydanego

przez Westminster Magistrates' Court we wrześniu 2023 r. Współoskarżony, którego tożsamość została zatajona w dokumentach sądowych, rzekomo prowadził obok Diaconu nielegalny bazar internetowy w latach 2015–2020.

Według biura prokuratora amerykańskiego Middle District of Florida E-Root była platformą działającą od dawna, używaną do sprzedaży dostępu do zainfekowanych komputerów na całym świecie, w tym serwerów należących do podmiotów z siedzibą w USA.

Operacje na rynku za pomocą E-Root

Cyberprzestępcy w E-Root mogą wyszukiwać różne zhakowane dane uwierzytelniające, takie jak Secure Socket Shell (SSH) i dostęp do protokołu Remote Desktop Protocol (RDP). Platforma posiadała także zaawansowane funkcje filtrowania, umożliwiające złoczyńcom filtrowanie według ceny, regionu, systemu operacyjnego, otwartych portów i dostawcy usług internetowych (ISP).

Federalne dochodzenie dotyczące rynku ujawniło, że według Departamentu Sprawiedliwości Stanów Zjednoczonych w serwisie E-Root wystawiono na sprzedaż ponad 350 000 danych uwierzytelniających.

Dochodzenie federalne i wpływ na ofiary

Ofiarami jest wiele przedsiębiorstw i firm na całym świecie oraz co

najmniej jedna agencja samorządu lokalnego w Tampie. Ujawniono, że wiele poszkodowanych podmiotów padło później ofiarą ataków oprogramowania ransomware, a niektóre dane uwierzytelniające wymienione na rynku były powiązane z oszustwami związanymi z kradzieżą podatku tożsamości.

Płatności na platformie E-Root zostały ułatwione poprzez system płatności internetowych Perfect Money. Zarzuca się również, że Diaconu, działające pod pseudonimem „WinD3str0y", prowadził siostrzaną witrynę internetową, umożliwiającą konwersję Bitcoinów na Perfect Money, aby pomóc ukryć tożsamość użytkowników rynku.

Pomimo tych skomplikowanych ustaleń dokumenty sądowe ujawniły luki w operacji, ponieważ administratorzy prowadzili obszerną dokumentację dotyczącą kupujących, co ułatwiało władzom prześledzenie nielegalnej działalności.

Upadek E-Root

Upadek E-Root nastąpił pod koniec 2020 r. w wyniku wspólnej operacji, a władze brytyjskie zatrzymały Diaconu w maju 2021 r. podczas próby opuszczenia kraju. Zarzuty postawione Diaconu i jego współoskarżonemu obejmują spisek mający na celu popełnienie oszustwa związanego z urządzeniami dostępowymi i komputerami, spisek dotyczący prania pieniędzy, spisek dotyczący oszustw drogą elektroniczną, oszustwa dotyczące urządzeń dostępowych i oszustwa komputerowe.

Diaconowi obecnie grozi do 20 lat więzienia federalnego, jeśli zostanie skazany pod każdym względem. Po raz pierwszy stawił się przed amerykańskim sędzią 16 października. Pozostaje w areszcie i nie przyznał się do postawionych mu zarzutów.

Zalecenia zespołu Bitdefender dotyczące bezpieczeństwa poświadczeń

- Unikaj ponownego używania hasła: Upewnij się, że każde konto ma unikalne hasło, aby zapobiec naruszeniu bezpieczeństwa jednego konta i naruszeniu innych.

- Używaj silnych haseł: używaj kombinacji wielkich i małych liter, cyfr i znaków specjalnych, aby tworzyć solidne hasła.

- Włącz uwierzytelnianie dwuskładnikowe (2FA): Dodaj dodatkową warstwę zabezpieczeń, wymuszając drugą formę identyfikacji oprócz hasła.

- Regularnie aktualizuj hasła: zmieniaj hasła okresowo, aby zmniejszyć ryzyko nieautoryzowanego dostępu.

- Użyj Menedżera haseł: Specjalistyczne narzędzia, takie jak Menedżer haseł Bitdefender, mogą pomóc w śledzeniu złożonych haseł i zapewnieniu ich bezpiecznego przechowywania.

- Uważaj na próby wyłudzenia informacji: zachowaj czujność, aby

uniknąć oszustw kradnących Twoje dane uwierzytelniające za pośrednictwem fałszywych e-maili lub wiadomości.

- Aktualizuj oprogramowanie: upewnij się, że Twój system operacyjny, aplikacje i oprogramowanie zabezpieczające są aktualne i zawierają najnowsze poprawki zabezpieczeń.

„Informacje dotyczące zatrzymania i ekstradycji Mołdawskiego hakera są pozytywnym sygnałem dla całej branży cyberbezpieczeństwa, ponieważ świadczą o coraz bliższej współpracy między poszczególnymi krajami, której celem jest wspólne działanie przeciwko zorganizowanym grupom hakerskim" – mówi Dariusz Woźniak z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło: https://bitdefender.pl/moldawianin-poddany-ekstradycji-do-usa-w-zwiazku-z-rynkiem-skradzionych-danych-uwierzytelniajacych-za-pomoca-e-roota/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 25.10.2023
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.