**MacOS na celowniku hakerów. Narzędzie do wykradania danych już w sprzedaży.**

**• Eksperci Check Point Research obserwowali nowy złośliwy szczep złośliwego oprogramowania - XLoader, będący pochodną malware’u Formbook**

**• XLoader z powodzeniem atakował urządzenia z systemem Windows. Dziś analitycy potwierdzili istnienie wersji zagrażającej użytkownikom Mac OS.**

**• Malware ma możliwość zbierania danych logowania, wykonywania zrzutów ekranu, rejestrowania naciśnięć klawiszy i instalacji kolejnych złośliwych plików**

**Oprogramowanie znane z Windowsa dostępne już na MacOS. Tym razem nie jest to powód do zadowolenia, a niepokoju dla użytkowników komputerów Apple; chodzi bowiem o niebezpieczny malware potrafiący wykradać dane użytkowników! Za jedyne 49 dolarów hakerzy mogą kupić w darknecie licencje na nowe złośliwe oprogramowanie, które umożliwia przechwytywanie danych logowania, zbieranie zrzutów ekranu, rejestrowanie naciśnięć klawiszy i uruchamianie złośliwych plików – ostrzegają eksperci Check Point Research.**

Komputery Apple z systemem MacOS w powszechnej opinii uważane są za najbezpieczniejsze. I chociaż jest w tym sporo prawdy, to eksperci od bezpieczeństwa cybernetycznego zwracają uwagę, że bezpieczeństwo danych zależy głównie od użytkownika i jego praktyk. W ostatnich latach na urządzeniach z systemem MacOS [pojawiły się kolejne rodziny złośliwego](https://www.macworld.co.uk/feature/mac-viruses-list-3668354/) oprogramowania, które choć uciążliwe, zwykle okazywały się niegroźne dla bezpieczeństwa danych.

Niestety, horyzont zagrożeń cybernetycznych jest niezwykle zmienny, a przed użytkownikami komputerów z nadgryzionym jabłkiem jawi się nowe zagrożenie, które początkowo wymierzone było przeciwko systemowi Windows.

Eksperci cyberbezpieczeństwa z Check Point Research poinformowali, że wykryli nowy złośliwy szczep złośliwego oprogramowania, będący pochodną malware’u Formbook, znanego z atakowania użytkowników Windowsa. W 2018 roku Formbook przestał być dystrybuowany przez hakerów, natomiast dwa lata później wydany został zastępujący go XLoader. Dziś, ku zaskoczeniu ekspertów, XLoader jest w stanie zaatakować również użytkowników Maców.

*- W ramach naszych działań mających na celu śledzenie cyberprzestępczości zaobserwowaliśmy interesujące zmiany w znanej rodzinie złośliwego oprogramowania „Formbook”, który wyewoluował w nowy szczep złośliwego oprogramowania. „XLoader” to złośliwy program, który jest znacznie bardziej dojrzały i wyrafinowany niż jego poprzednicy: funkcjonuje na różnych systemach operacyjnych, w tym komputerach z MacOS. –* informuje Yaniv Balmas, szef działu badań cybernetycznych w Check Point Software.

Osoby niezainteresowane tematyką cyberbezpieczeństwa szokować może fakt, że w darknecie sprzedawane są specjalne licencje XLoader w cenie zaczynającej się od 49 dolarów! Twórcy oprogramowania wyposażyli je w możliwość zbierania danych logowania, wykonywania zrzutów ekranu, rejestrowania naciśnięć klawiszy i instalacji kolejnych złośliwych plików. Ofiary hakerów są zwykle nakłaniane do pobrania XLoadera za pośrednictwem sfałszowanych wiadomości e-mail zawierających złośliwe dokumenty Microsoft Office.

- *Historycznie złośliwe oprogramowanie MacOS nie było tak powszechne. Zwykle należało do kategorii oprogramowania szpiegującego, nie powodując jednak zbyt dużych szkód. Myślę, że wśród użytkowników MacOS panuje błędne przekonanie, że platformy Apple są bezpieczniejsze niż inne, powszechniej używane. Prawda jest jednak taka, że ​​złośliwe oprogramowanie na MacOS staje się coraz powszechniejsze i bardziej niebezpieczne. Nasze ostatnie odkrycia są natomiast doskonałym przykładem i potwierdzają ten rosnący trend. Osobiście spodziewam się, że po rodzinie złośliwego oprogramowania Formbook pojawią się kolejne zagrożenia.* – wyjaśnia ekspert Check Point Software.

Check Point Research obserwowało aktywność Xloadera od 1 grudnia 2020 r. do 1 czerwca 2021 r. wykrywając go w 69 krajów. Ponad połowa (53%) ofiar mieszka w Stanach Zjednoczonych.