**Raport SophosLabs: aplikacje typu fleeceware groźne także dla właścicieli iPhone’ów**



 **Kraków, 10 kwietnia 2020** – Badacze z firmy **Sophos** znaleźli **ponad 30 aplikacji** typu **fleeceware** dostępnych w **oficjalnym sklepie Apple App Store**. Zazwyczaj są to proste narzędzia, które mają wiele darmowych lub tanich odpowiedników, np. edytory zdjęć, horoskopy czy skanery kodów QR. Niebezpieczne programy mają już łącznie ponad **3,6 mln pobrań.**[[1]](#footnote-1)Ich zainstalowanie może drogo kosztować – **po kilku dniach** obciążają użytkowników **subskrypcjami o wartości nawet kilku tysięcy złotych** lubobowiązkowymi zakupami w aplikacji.

**„Darmowe” programy za kilka tysięcy**

Z aplikacji typu fleeceware można korzystać za darmo tylko w okresie próbnym. Po nim naliczane są wysokie **opłaty za subskrypcję** – nawet ponad **40 zł na tydzień**, czyli około **2000 zł rocznie.** Do tego często dochodzą **obowiązkowe** opłaty za **zakupy** **w aplikacji**, bez których nie działa ona prawidłowo. Wbrew powszechnemu przekonaniu użytkowników, **subskrypcji** **nie anuluje** samo **usunięcie aplikacji**.

Po raz pierwszy Sophos ostrzegał przed fleeceware we wrześniu ubiegłego roku, gdy taki schemat działania odkryto w aplikacjach na **system Android**.[[2]](#footnote-2) W styczniu br. firma znalazła kolejnych 20 niebezpiecznych programów, które ze sklepu Google Play pobrało **prawie 600 mln użytkowników**.[[3]](#footnote-3) Teraz zagrożeni są **także użytkownicy** **systemu iOS**. Proceder jest przy tym bardzo opłacalny – wiele aplikacji typu fleeceware znajduje się **wśród najbardziej dochodowych programów w App Store** (np. zajmujący 11. miejsce Zodiac Master Plus).

**Legalne, ale nieuczciwe**

Aplikacje zachęcają **fałszywymi pięciogwiazdkowymi recenzjami** i **agresywnymi reklamami**, m.in. w popularnych serwisach społecznościowych, takich jak YouTube, Instagram czy TikTok. Oficjalnie nie są uznawane za nielegalne i **pozornie nie stanowią zagrożenia**, bo nie zawierają złośliwego kodu. Ich działanie jest jednak **nieuczciwe**, gdyż **wykorzystują zaufanie i nieuwagę** użytkowników, ukrywając informacje o opłatach „drobnym drukiem” w pomijanych zazwyczaj regulaminach.

– C*zujność należy zachować już podczas wybierania aplikacji. Decydujmy się na te, które znamy, a dokładnie sprawdzajmy szczególnie te, o których dowiedzieliśmy się z reklamy. Starannie czytajmy wszelkie informacje dotyczące regulaminu i warunków subskrypcji, nie podawajmy też pochopnie danych swojej karty kredytowej. Jeśli już zainstalowaliśmy aplikację tego typu pamiętajmy, że aby anulować opłaty nie wystarczy usunąć programu. Listę swoich aktywnych subskrypcji oraz szczegółowe wskazówki jak je unieważnić znajdziemy na stronie Apple App Store oraz Google Play* – radzi **Łukasz Formas, Kierownik zespołu inżynierów w firmie Sophos.**

**Więcej informacji** o odkrytych aplikacjach typu fleeceware oraz sposobach anulowania subskrypcji można znaleźć [tutaj](https://news.sophos.com/en-us/2020/04/08/iphone-fleeceware/).

**Informacje o firmie**

Jako światowy lider zabezpieczeń nowej generacji, Sophos chroni przed najbardziej zaawansowanymi cyberzagrożeniami ponad 400 tys. firm różnej wielkości w ponad 150 krajach. Rozwiązania Sophos wykorzystują chmurę i sztuczną inteligencję, aby zabezpieczać urządzenia końcowe (laptopy, serwery i urządzenia mobilne) oraz sieci przed ewoluującymi metodami cyberprzestępców. Przy wsparciu SophosLabs – globalnego zespołu badającego zagrożenia – firma odpowiada na zagrożenia takie jak ransomware, malware, exploity, eksfiltracja danych, phishing czy indywidualnie dokonywane włamania przez cyberprzestępców. Platforma do zarządzania w chmurze Sophos Central integruje całe portfolio produktów nowej generacji Sophos w jeden system „zsynchronizowanej ochrony”, dostępny przez zestaw interfejsów API i obejmujący m.in. rozwiązanie Intercept X dla urządzeń końcowych oraz zaporę sieciową nowej generacji z rodziny XG Firewall. Firma oferuje również usługi łączące posiadaną technologię oraz aktywne przeciwdziałanie zagrożeniom (Managed Threat Response), szczególnie istotne w zmieniającym się dynamicznie świecie.

Sophos dąży do rozwijania i oferowania rozwiązań nowej generacji, aby zapewnić każdemu przedsiębiorstwu najwyższej klasy ochronę, zachowując jednocześnie prostotę zarządzania i umożliwiając redukcję kosztów. Wykorzystuje do tego m.in. zaawansowane funkcje infrastruktury chmurowej, uczenie maszynowe, interfejsy API, automatyzację i zarządzanie sposobami reagowania na zagrożenia. Firma sprzedaje swoje produkty i usługi za pośrednictwem globalnej sieci ponad 47 tys. partnerów i dostawców usług zarządzanych (MSP). Z innowacyjnych technologii Sophos mogą skorzystać także konsumenci indywidualni dzięki rodzinie rozwiązań Sophos Home. Firma ma siedzibę w Oksfordzie w Wielkiej Brytanii.

Więcej informacji można znaleźć na stronie www.sophos.com

1. Źródło: <https://sensortower.com/ios/rankings/top/iphone/us/all-categories?date=2020-01-11> [↑](#footnote-ref-1)
2. <https://news.sophos.com/en-us/2019/09/25/fleeceware-apps-overcharge-users-for-basic-app-functionality/> [↑](#footnote-ref-2)
3. <https://news.sophos.com/en-us/2020/01/14/fleeceware-apps-persist-on-the-play-store/> [↑](#footnote-ref-3)