NOWE SPOSOBY DZIAŁANIA CYBERPRZESTĘPCÓW. PODRĘCZNIKI SZKOLNE ZAGROŻENIEM

Cyberprzestępcy wykorzystują podręczniki i wypracowania w celu przemycania szkodliwego oprogramowania - wynika z raportu firmy Kaspersky. Eksperci wykryli ponad 50 tys. potencjalnie niebezpiecznych plików podszywających się pod gotowe eseje oraz podręczniki szkolne i akademickie online.

Według danych ze sporządzonego przez firmę raportu "Powrót do szkoły" wykryto 53 531 szkodliwych plików podszywających się pod gotowe teksty oraz książki do szkoły. Od sierpnia 2018 r. do lipca 2019 r. zostały one wykorzystane w 356 662 atakach na 104 819 użytkowników.

Autorzy opracowania zwracają uwagę, że wiele podręczników można znaleźć online, a rodzice i uczniowie unikają wysokich kosztów, pobierając je, podobnie jak wypracowania, z nielegalnych stron internetowych lub serwisów pozwalających na współdzielenie plików. Jest to jednak ryzykowne, gdyż cyberprzestępcy mogą wykorzystać je do rozprzestrzeniania szkodliwego oprogramowania.

Pod podręczniki szkolne, które w większości stanowiły nielegalnie rozprowadzane książki do języka angielskiego (2 080), matematyki (1 213) oraz literatury (870), podszywało się łącznie 17 755 zagrożeń. Ogromną większość z nich stanowiły narzędzia pobierające różne pliki: od irytującego, ale niegroźnego oprogramowania reklamowego po niebezpieczne oprogramowanie kradnące pieniądze - wynika z danych raportu.

Pozostałe 35 776 zagrożeń podszywało się pod eseje oraz referaty na różne tematy. Według badaczy, w 35,5 proc. przypadków najpopularniejszym szkodliwym oprogramowaniem był ośmioletni robak – przestarzały rodzaj rzadko spotykanego obecnie zagrożenia. Robak ten był aktywnie rozprzestrzeniany za pośrednictwem konkretnego wektora ataków – pamięci USB. Po dokładniejszej analizie eksperci doszli do wniosku, że robak „rezyduje” na komputerach punktów oferujących studentom usługi wydruku. Takie urządzenia nierzadko od lat działają bez aktualizacji zabezpieczeń i pod kontrolą starych systemów operacyjnych. Robak przedostał się na nie prawdopodobnie za sprawą dokumentu, który ktoś przyszedł wydrukować.

Raport zwraca uwage, że infekcja, która trafi na komputer szkolnej sieci, może łatwo się rozprzestrzenić. Nie wszystkie szkoły są przygotowane na to, aby skutecznie reagować na tego rodzaju incydenty, zwłaszcza, że placówki edukacyjne nie są postrzegane jako typowy cel oszustów.

Według ekspertów uczniowie, studenci i rodzice mogą uchronić się przed szkodliwym oprogramowaniem podszywającym się pod materiały edukacyjne m.in. nie otwierając załączników do wiadomości e-mail, które wydają się podejrzane lub pochodzą od nieznanej osoby; szukając książek wyłącznie w księgarniach lub w zaufanych bibliotekach online. Należy też zwracać uwagę na rozszerzenie pobieranego pliku, który w przypadku pobierania np. podręcznika nie powinien posiadać rozszerzenia .exe. Firma Kaspersky zwraca też uwagę na konieczność stosowania rozwiązań

zabezpieczających oraz aktualnych wersji systemu operacyjnego na wszystkich komputerach w sieci szkolnej czy akademickiej.