HAKERZY OBCHODZĄ ZABEZPIECZENIA OUTLOOKA. DUŻY PROBLEM MICROSOFTU

Hakerzy obchodzą łatkę zabezpieczającą w programie Microsoft Outlook, która została wdrożona przez koncern w 2017 roku. Jej celem miała być naprawa podatność funkcji "Strona domowa".

Funkcja "Strona domowa" może służyć użytkownikom Outlooka jako domyślny ekran widoczny w programie. Pozwala ona na ładowanie zewnętrznych treści pobieranych z sieci, np. obrazków pochodzących z publicznie dostępnej strony internetowej czy serwera. Stanowi zarazem furtkę dla cyberprzestępców, którzy kilka lat temu zorientowali się, iż mogą wykorzystać funkcję do pozyskania danych logowania do kont poczty elektronicznej zarejestrowanych w programie.

Atak odbywa się poprzez załadowanie na "Stronie domowej" złośliwych treści, które zawierają skrypt umożliwiający złamanie zabezpieczeń Outlooka i przejęcie kontroli nad systemem operacyjnym działającym na komputerze ofiary. Z perspektywy użytkownika działania hakerów mogą być w praktyce niewykrywalne, gdyż wyglądają jak prawdziwy ruch sieciowy programu do obsługi poczty. Według serwisu Wired cyberprzestępcy nie tracą możliwości pozyskiwania danych z atakowanego Outlooka nawet po zrestartowaniu urządzenia, na którym zainstalowano program.

Microsoft w 2017 roku oznaczył podatność Outlooka jako lukę niskiego ryzyka i poinformował, że nie dysponuje danymi na temat jej wykorzystania przez cyberprzestępców podczas prawdziwego ataku hakerskiego. Firmy z branży cyberbezpieczeństwa jednak już wówczas donosiły o tym, że znane im są przypadki wykorzystania podatności w atakach sponsorowanych przez państwa. W tym kontekście wskazywano na działania grup przestępczych APT33 i APT34 łączonych z działaniami na rzecz Iranu.

W lipcu bieżącego roku dowództwo cyberwojsk USA wydało specjalne ostrzeżenie na temat możliwości wykorzystania podatności Outlooka przez wrogie podmioty. W październiku natomiast firma Microsoft poinformowała, że irańscy hakerzy obrali za cel konta poczty elektronicznej obsługiwane za pomocą pakietu Office365 (w którego skład wchodzi program Outlook) należące do jednego z komitetów wyborczych osoby kandydującej na urząd prezydenta USA w przyszłorocznych wyborach. Według doniesień medialnych zaatakowany został komitet obecnego prezydenta Donalda Trumpa.

Wired zwrócił uwagę, że w przypadku tej operacji nie została wykorzystana podatność "Strony domowej". Firma FireEye, która specjalizuje się w badaniu tego rodzaju ataków, podkreśliła jednak, że działania hakerów z zastosowaniem tej funkcji Outlooka wciąż są obserwowane przez jej specjalistów.

Magazyn przypomniał, że Microsoft w 2017 roku wydał aktualizację zabezpieczającą dla Outlooka, która miała neutralizować podatność. "Co zrozumiałe, to wytworzyło (w użytkownikach) przekonanie,

że firmy i sztaby wyborcze nie muszą martwić się o zagrożenie, jeśli korzystają z najnowszej wersji programu" - ocenił Wired.

Według przedstawicieli firmy TrustedSec ataki z wykorzystaniem luki "Strony domowej" to codzienność, która "przez większość czasu jest niedostrzegana w większości organizacji".

Czytaj też: Fałszywe ekrany logowania. Ostrzeżenie dla klientów banków