Producenci oprogramowania antywirusowego alarmują: ujawniono kod z nową luką systemu Windows - KHOBE. "Działanie takie naraża użytkowników i może być próbą uzyskania szybkich korzyści finansowych" - komentują sytuację specjaliści ds. bezpieczeństwa sieciowego.

Grupa osób ze środowiska akademickiego zrzeszonych w projekcie matousec.com doniosła niedawno, że odkryła nieznaną wcześniej wadę w systemie Windows - tzw. **KHOBE**, które pozwala złośliwym skryptom na całkowite ominięcie oprogramowania antywirusowego.

Wilk w owczej skórze
Zespół Matousec przeprowadził testy, w których przez oprogramowanie antywirusowe przepuszczono „zdrowy" kod, by po pozytywnej weryfikacji podmieniać go na złośliwy. Według raportu Matousec żadna ze znanych na rynku marek oprogramowania antywirusowego nie poradziła sobie z tak przeprowadzonym atakiem. Kompletna lista podatnych programów (34 pozycje) dostępna jest w artykule pod adresem http://www.matousec.com/info/articles/khobe-8.0-earthquake-for-windows-desktop-security-software.php.

Badanie przeprowadzono z wykorzystaniem 32-bitowych wersji Windows XP oraz Visty, jednak zdaniem Matousec również wersje 64-bitowe oraz Windows 7 nie są wolne od zagrożeń. Wykorzystanie luki okazało się też łatwiejsze w komputerach z procesorami wielordzeniowymi.

Ryzyko ujawnione czy podwyższone?
Choć doniesienia brzmią bardzo poważnie - największe obawy budzi w tej chwili sam sposób ujawnienia luki przez zespół Matousec. Do informacji publicznej podany został niebezpieczny fragment kodu źródłowego, który jest niczym innym, jak zaproszeniem do popełnienia cyberprzestępstwa. "Działanie takie jest nieodpowiedzialne i naraża przede wszystkim użytkowników" - komentują sprawę eksperci. Wśród innych zastrzeżeń wymieniają także próbę sprzedania specjalnego raportu na temat luki po niewiarygodnie wysokiej cenie oraz niewyjaśnioną anonimowość uczestników projektu Matousec.

Sprawę komentuje na firmowym blogu **Ralf Benzmüller** z **G Data Software**, firmy ocenianej przez europejską prasę jako producent jednego z najskuteczniejszych programów antywirusowych. Według niego wszystkie powyższe elementy sprawiają, że twórcy raportu mogli się kierować bardziej chęcią uzyskania szybkich zysków finansowych niż rzeczywistą chęcią zniwelowania zagrożenia. Ponadto, Benzmüller dodaje: „Poradziliśmy sobie z tym problemem sami. Obecnie, rozwiązanie znajduje się w fazie testów, a nasi klienci uzyskają wszelkie niezbędne zabezpieczenia wraz z następną aktualizacją oprogramowania antywirusowego."

Z wypowiedzi specjalistów cytowanych na portalu Infoworld.com wynika, że obecnie nie ma powodu do paniki. Aby doszło do ataku, cyberprzestępca musiałby najpierw uzyskać dostęp do kluczowych procesów komputera.

Someday Interactive