BŁĘDNA KONFIGURACJA NARZĘDZIA VIRUSTOTAL PROWADZI DO UJAWNIENIA WRAŻLIWYCH DANYCH

Błędna konfiguracja narzędzia VirusTotal, które pozwala stwierdzić ewentualną infekcję szkodliwym oprogramowaniem, prowadzi do niezamierzonego ujawniania wrażliwych danych, m.in. szablonów produkcyjnych i innych informacji objętych tajemnicą handlową - podała agencja Bloomberga

Agencja powołała się na analizę zajmującej się cyberbezpieczeństwem izraelskiej firmy Otorio. Spółka ta poinformowała o natrafieniu w usłudze VirusTotal na "tysiące niezabezpieczonych plików pochodzących z firm z branży farmaceutycznej, przemysłowej, motoryzacyjnej i spożywczej". Dokumenty zostały odkryte w ramach projektu badawczego obejmującego analizę złośliwego oprogramowania wykrytego przez to narzędzie.

Według Bloomberga w wyniku niewłaściwej konfiguracji program opracowany przez siostrzaną spółkę Google'a powiela pełną treść skanowanych dokumentów. Pozwala to na wgląd do nich zewnętrznym firmom zajmującym się cyberbezpieczeństwem, którym udostępnia się wyniki do dalszej analizy w celu zwiększenia jej skuteczności.

Według Otorio odkryte pliki mogłyby znaleźć zastosowanie w ataku hakerskim, jednak nie zostały wykorzystane w ramach znanych cyberoperacji.

"Na podstawie tego, co odkryliśmy, moglibyśmy zaprojektować bardzo skuteczną metodę hakowania. Odkryliśmy pliki, które pozwalały nam na stworzenie schematu działań niezbędnych do infiltracji poziomu produkcji (w jednej z firm - PAP)" - powiedział Bloombergowi szef Otorio Daniel Bren, który wcześniej pracował w izraelskim wojsku przy budowie jednostki cyberobrony.

Według Brena wśród dokumentów, do których dostęp zdobyła jego firma, znajdują się "tajemnice handlowe przedsiębiorstw", które korzystały z narzędzia VirusTotal.

Otorio poinformowało firmę Chronicle (Alphabet) o swoim odkryciu w lipcu. Według przedstawicieli izraelskiego przedsiębiorstwa, twórcy VT zgodzili się z sugestią potrzeby zwiększania świadomości na temat sposobu, w jaki działa to narzędzie i jak powinny być konfigurowane programy mające chronić bezpieczeństwo.

Bloomberg zwrócił uwagę, że warunki korzystania z Virus Total informują użytkowników o tym, iż nie powinni przesyłać na serwery narzędzia żadnych plików zawierających poufne informacje służbowe, handlowe lub dane osobowe.

Dostęp do danych gromadzonych w ramach usługi przydzielany jest specjalistom i badaczom dysponującym odpowiednie uprawnienia, jednakże, jak podkreślił w rozmowie z Bloombergiem Bren, osoby działające w złej wierze mogą łatwo nadużyć zasad platformy Virus Total i tym samym zyskać dostęp do istotnych, poufnych danych wielu podmiotów.

VirusTotal został zakupiony przez Google w 2012 roku.