

ROŚNIE AKTYWNOŚĆ RZĄDOWYCH HAKERÓW. PONAD 12 TYS. OFIAR

Ponad 12 tys. użytkowników Google zostało zaatakowanych przez hakerów będących na usługach rządów - poinformował Google Threat Analysis Group. Amerykański gigant proponuje udział w nowym autorskim programie, który ma ochronić użytkowników przed tego rodzaju działalnością.

Koncern od dawna stosuje zasadę wysyłania ostrzeżeń do użytkowników, jeśli tylko specjaliści firmy wykryją, że są lub mogą oni być ofiarami kampanii phishingowych sponsorowanych przez państwo. Według przedstawionych danych od lipca do września 2019 roku Google rozesłał ponad 12 000 alertów bezpieczeństwa do użytkowników ze 149 krajów. Dotyczyły one głównie cyberataków, które były sponsorowane przez rządy. Jest to liczba zbliżona do statystyk z roku 2018 i 2017.

„Ponad 90% tych użytkowników było atakowanych za pomocą e-maili służących do wyłudzenia informacji” – czytamy w komunikacie. – „Zazwyczaj są to próby uzyskania hasła lub innych danych umożliwiających zalogowanie, a następnie przejęcie konta”. W związku z rosnącym zagrożeniem Google zachęca „użytkowników wysokiego ryzyka” (na przykład dziennikarzy, przedstawicieli instytucji międzynarodowych, polityków) do wzięcia udziału w autorskim programie firmy Advanced Protection Program (APP), który zapewnia „najlepszą dostępną ochronę przed phishingiem i przejęciem konta”.

Firma zadeklarowała, że w przyszłości udostępnić będzie więcej szczegółów technicznych oraz konkretnych danych na temat zidentyfikowanych zagrożeń, a także sposobów przeciwdziałania. Celem Google jest pobudzenie szerszej dyskusji na temat cyberbezpieczeństwa w skali globalnej.

Google Threat Analysis Group (TAG) jest to jedna z komórek firmy, która odpowiada za przeciwdziałanie złośliwej działalności hakerskiej, wymierzonej w sieci i systemy koncernu oraz użytkowników. Jak poinformowały władze firmy na oficjalnej stronie, cyberprzestępczość jest zagrożeniem, w którego zwalczanie Google regularnie inwestuje od ponad dekady.

Threat Analysis Group obserwuje działalność ponad 270 grup cyberprzestępczych, w tym również około 50 powiązanych z rządem. Ich cele są różnorodne. Jedne specjalizują się w gromadzeniu danych wywiadowczych lub kradzieży własności intelektualnej, podczas gdy inne koncentrują się na prowadzeniu złośliwych cyberataków bądź rozpowszechnianiu dezinformacji. Władze Google podkreśliły, że firma wykorzystuje inteligentne narzędzia do ochrony zarówno swoich zasobów jak i użytkowników przed złośliwym oprogramowaniem.

Wykrywanie zagrożeń

Google na oficjalnej stronie informuje również o wykrytej ostatnio zaawansowanej działalności hakerskiej. W grudniu 2017 roku specjaliści TAG odkryli serię cyberataków, których celem było wdrożenie złośliwego oprogramowania na urządzenia z systemem Android. Pierwsza fala incydentów

miała miejsce w Korei Południowej, gdzie cyberprzestępcy w ramach Sandworm modyfikowali dostępne aplikacje, a następnie zamieszczali je w sklepie Play Store. Ostatecznie działania podjęte przez specjalistów Google sprawiły, że kampania została skutecznie zneutralizowana.

Deinformacja

TAG jest jednym z elementów wchodzących w skład szerszej struktury Google, która funkcjonuje na rzecz skoordynowania działań w celu ograniczenia rozpowszechniania dezinformacji. „Udostępniamy istotne informacje o tego typu zagrożeniach organom ścigania oraz innym firmom technologicznym” – stwierdzono w komunikacie.

W tym miejscu ponownie pojawiły się przykłady, którymi szczyci się koncern. Wśród nich wyróżniono niedawne działania TAG wymierzone przeciwko rosyjskim operacjom wpływu, skierowanym w państwa afrykańskie. Złośliwa kampania obejmowała fikcyjne serwisy informacyjne służące do rozpowszechniania wiadomości, promujących interesy Kremla w regionie. Specjaliści Google wykryli niepokojącą aktywność kont, które odpowiadały za rozpowszechnianie fake newsów w sieci.

Jak informuje koncern, głównymi celami Moskwy były takie państwa jak: Republika Środkowoafrykańska, Sudan, Madagaskar czy Republika Południowej Afryki. W celu zwiększenia zasięgu publikowanych treści posty były napisane w trzech głównych językach – angielskim, francuskim i arabskim. Google wskazuje, że reakcja ekspertów firmy była natychmiastowa. W wyniku podjętych działań zlikwidowano konta powiązane z rosyjską operacją, w tym 15 kanałów na YouTube.

Współpraca

„TAG ściśle współpracuje z innymi firmami technologicznymi w celu wymiany zdobytych danych i najlepszych praktyk” – wskazują władze firmy. Równocześnie Google zapewnił, że wszystkie informacje na temat incydentów udostępniane są organom ścigania.

Zgodnie z treścią komunikatu głównym celem koncernu jest dostarczenie większej ilości informacji na temat złośliwych kampanii wykrywanych przez TAG. Firma ma również nadzieję, że udostępnione dane będą pomocne dla podmiotów zajmujących się cyberbezpieczeństwem, co umożliwi opracowanie skutecznych mechanizmów ich powstrzymywania. Niemniej istotne jest również budowanie świadomości użytkowników na temat zagrożeń występujących w sieci.

Czytaj też: [Google przestaje targetować reklamy polityczne](#)