Cyberdefence 24

aut. Szymon Palczewski 09.10.2020

BAHAMUT, CZYLI „KRÓLOWIE" PHISHINGU I DEZINFORMACJI

Specjaliści odkryli centrum kampanii dezinformacyjnych oraz globalnych operacji hakerskich, skąd przeprowadzano cyberataki na ogromną skalę. Wszystko miało odbywać się w ramach grupy Bahamut, złożonej z „cybernajemników" pochodzących z wielu państw. Rozpowszechnianie fake newsów, zamieszczanie zainfekowanych aplikacji w Google Play oraz App Store czy serie cyberataków to jedynie część działalności, jaką prowadziła organizacja.

Analiza przeprowadzona przez specjalistów firmy BlackBerry wykazała, że grupa hakerska „Bahamut" odpowiada za szeroko zakrojone kampanie cyberataków, wymierzonych między innymi w największe koncerny oraz urzędników państwowych wielu krajów. „To jedna z najbardziej wyrafinowanych, nieuchwytnych oraz skutecznych grup znanych w środowisku" – podkreślili eksperci w raporcie „BAHAMUT: Hack-for-Hire Masters of Phishing, Fake News i Fake Apps".

Zakres działania

Obserwacja działalności hakerów pozwoliła stwierdzić, że Bahamut jest obecnie jednym z największych ugrupowań skupiających podmioty zajmujące się dezinformacją. Jej członkowie specjalizują się nie tylko w tworzeniu i zarządzaniu fikcyjnymi profilami w mediach społecznościowych, ale również kreowaniu oraz rozwijaniu całych serwisów informacyjnych, których założeniem jest rozpowszechnianie fake newsów na niebotyczną skalę.

„Wyrafinowanie i sam zakres prowadzonej działalności, który nasz zespół był w stanie połączyć z Bahamut, jest oszałamiający" – wskazał Eric Milam, wiceprezes ds. badań operacyjnych w BlackBerry. Dodał, że grupa stoi również za wieloma „niezwykle ukierunkowanymi i rozbudowanymi kampaniami phishingowymi" w celu kradzieży danych lub infekowania urządzeń ofiar złośliwym oprogramowaniem. To jednak jedynie część operacji, jakie realizowali hakerzy. Analiza kampanii prowadzonych przez grupę skłoniła ekspertów do stwierdzenia, że jej członkowie prawdopodobnie są „cybernajemnikami".

W raporcie zwrócono uwagę na szczególne zainteresowanie członków Bahamut urządzeniami mobilnymi. Hakerom z powodzeniem udało się zamieścić kilkanaście zainfekowanych aplikacji w Google Play oraz App Store. Na specjalistach BlackBerry zrobiła również wrażenie niespotykana cierpliwość hakerów podczas prowadzenia operacji.

Zdaniem Erica Milama tak wielka różnorodność działań Bahamut jednoznacznie wskazuje, że jest to bardzo zaawansowana oraz zbudowana grupa, posiadająca członków w wielu państwach. „Za dużo różnych rzeczy dzieje się w zbyt wielu różnych zakresach i w zbyt wielu różnych branżach, żeby prowadzili to z jednego kraju" – zaznaczył przedstawiciel BlackBerry.

„To niezwykła grupa, ponieważ ich bezpieczeństwo operacyjne jest na znacznie wyższym poziomie niż

pozostałych ugrupowań znanych w środowisku” – dodał Eric Milam. Próbując scharakteryzować hakerów Bahamut wskazał, że „polegają oni na złośliwym oprogramowaniu jedynie w ostateczności, są bardzo biegli w wyłudzaniu informacji oraz odznaczają się wyjątkową dbałość o szczegóły, a przede wszystkim są cierpliwi”. Podkreślił, że cyberprzestepcy potrafią obserwować swój cel przez rok lub dłużej zanim rozpoczną operację.

Czytaj też: „Cybernajemnicy” atakują Europę. Fintechy i firmy prawnicze obiektem szpiegostwa

Imperium fake newsów

„Wydaje się, że najbardziej charakterystycznym aspektem działalności Bahamut (…) jest wykorzystanie specyficznych, pieczołowicie przygotowanych witryn internetowych, aplikacji oraz profili (w social mediach – przyp. red.)” – czytamy w raporcie BlackBerry.

Jak wynika z analizy, przynajmniej w jednym przypadku grupa przejęła domenę, która pierwotnie była platformą informacyjną przeznaczoną do udostępniona treści na temat bieżących wydarzeń. Gdy weszła w posiadanie hakerów, stała się narzędziem rozpowszechniania fake newsów.

Aby wzbudzić pozory legalności, członkowie grupy zamieszczali na stronie zdjęcia znanych dziennikarzy, a także tworzyli specjalne konta w social mediach w celu wzbudzenia zaufania wśród odbiorców.

Królestwo zainfekowanych aplikacji

Specjaliści BlackBerry podczas badań odkryli również dziewięć zainfekowanych złośliwym oprogramowaniem aplikacji dostępnych w App Store oraz Google Play. Eksperci bezpośrednio przypisali je do grupy Bahamut na podstawie konfiguracji oraz innych zidentyfikowanych w sieci dowodów.

„Aplikacje były kompletne z dobrze zaprojektowanymi witrynami internetowymi, zasadami polityki prywatności i pisemnymi warunkami korzystania z usługi – często pomijanymi przez inne ugrupowania – co pomogło im ominąć zabezpieczenia wprowadzone zarówno przez Google, jak i Apple” – wskazano w raporcie.

Zbadane przez BlackBerry aplikacje były najprawdopodobniej dedykowane dla użytkowników ze Zjednoczonych Emiratów Arabskich (ZEA), o czym świadczyły ograniczenia dotyczące zakresu pobierania apki. „Co więcej, aplikacje związane z ramadanem, a także te, które odnosiły się do ruchu separatystycznego sikhów, wskazują, że grupa Bahamut miała zamiar skierować swoje działania na określone grupy religijne i polityczne” – tłumaczą eksperci.

Rzecznik Google w rozmowie z agencją Reutera przekazał, że wszystkie aplikacje wymienione w raporcie aplikacje zostały usunięte z internetowego sklepu firmy. Z kolei Apple usunął jedynie dwie apki wskazując, że na temat pozostałych nie otrzymał „wystarczających informacji, aby jednoznacznie ocenić czy są złośliwe”.

Czytaj też: „Cybernajemnicy” na usługach Teheranu. Głównym celem USA i Izrael

Kim są ofiary?

W tym miejscu warto podkreślić, że specjaliści BlackBerry nie wymienili bezpośrednio żadnych ofiar

hakerów Bahamut, jednak doniesienia pochodzące z innych źródeł sugerują, że wśród celów znajdowali się między innymi działacze na rzecz praw człowieka z Bliskiego Wschodu, przedstawiciele pakistańskiego wojska oraz biznesmeni z Zatoki Perskiej.

Co więcej, agencja Reutera wpadła na ślad poszkodowanej na skutek cyberataków organizacji**,** którą była Sikhs for Justice, czyli grupa prowadząca kampanię na rzecz niezależności Sikhów w Indiach. Jej założyciel, Gurpatwant Singh Pannun, podkreślił, że strony internetowe organizacji były wielokrotnie hakowane. Włamywano się również do skrzynki e-maili.

Według ustaleń agencji Reutera innymi ofiarami Bahamut najprawdopodobniej są podmioty i osoby ze Zjednoczonych Emiratów Arabskich, w tym między innymi: Ministerstwo Obrony, Najwyższa Rada Bezpieczeństwa Narodowego ZEA oraz dyplomata ZEA w Waszyngtonie Shaim Gargash.

Ponadto hakerzy uderzyli w usługodawcę poczty e-mail saudyjskiego rządu „Mawthouq", systemy ministerstw tego kraju oraz Saudi Center for International Strategic Partnerships.

Agencja Reutera weszła również w posiadanie informacji, które sugerują, że członkowie Bahamut mogą stać za operacjami wymierzonymi w członków rodziny królewskiej i dyrektorów biznesowych w Bahrajnie, Kuwejcie oraz Katarze.

Jak wynika z raportu BlackBerry, hakerzy często wykorzystują publicznie dostępne narzędzia oraz naśladują inne ugrupowania w celu minimalizacji ryzyka wykrycia prowadzonych operacji. Dodatkowo cyberprzestępcy zmieniają taktykę, co znacznie utrudnia ich jednoznaczną identyfikację. Sposób działania, dobór celów oraz forma prowadzenia kampanii wskazują, że Bahamut jest „grupą dobrze finansowaną, dobrze wyposażoną i dobrze zorientowaną w stanie obecnych badań nad cyberbezpieczeństwem" – stwierdzili specjaliści BlackBerry.

Czytaj też: Cybernajemnicy penetrują sektor finansowy. Alarm dla małych firm i organizacji