The Dukes – cybernetyczne ramię Moskwy?

21 września 2015

Przez ostatnie siedem lat rosyjska grupa zajmująca się cyfrowym szpiegostwem – i prawdopodobnie powiązana z rządem w Moskwie – przeprowadziła liczne ataki przeciwko rządom, think tankom i innym organizacjom. Firma F-Secure opublikowała właśnie raport na temat grupy, którą analitycy nazwali „the Dukes".

Wiadomo,że jest ona aktywna co najmniej od 2008 roku i że wyspecjalizowała się w atakowaniu dziur „zero-day". Przedstawiciele grupy korzystają zarówno z ogólnodostępnych informacji na temat takich luk, jak i samodzielnie je wyszukują. Z analiz wynika, że the Dukes dysponuje dużymi zasobami, jest świetnie zorganizowana i mocno angażuje się w podejmowane przedsięwzięcia. Jej taktyka to mieszanina nagłych ataków, kradzieży danych i wycofania się, jak i długotrwałych infiltracji podczas których kradzione są olbrzymie ilości informacji. The Dukes atakują nie tylko rządy obcych państw, ale również organizacje przestępcze działające na terenie Federacji Rosyjskiej. „Głównym celem the Dukes są rządy państw Zachodu i powiązane z nimi organizacje, polityczne think tanki czy przedsiębiorstwa otrzymujące rządowe zlecenia. Wśród ich celów są również członkowie rządów Wspólnoty Niepodległych Państw, rządy z Afryki, Azji, Bliskiego Wschodu, organizacje powiązane z czeczeńskimi terrorystami oraz Rosjanie zaangażowani w handel narkotykami i nielegalnymi substancjami" – czytamy w raporcie.

Pierwszym szkodliwym oprogramowaniem the Dukes zauważonym przez analityków z F-Secure był PinchDuke, który początkowo atakował osoby i organizacje powiązane z czeczeńskimi separatystami. Jednak już w roku 2009 grupa zaczęła atakować cele na Zachodzie, w tym NATO. The Dukes najczęściej atakują

precyzyjnie wybrane cele, ale wiadomo o co najmniej jednym ataku na szerszą skalę. Został on przeprowadzony przeciwko użytkownikom sieci Tor, a jego celem było zarażenie ich komputerów. Dotychczas różne firmy antywirusowe odkryły osiem szkodliwych kodów stworzonych przez the Dukes.

Wspomniany już PinchDuke był po raz ostatni widziany w 2010 roku. Za jego pomocą przestępcy próbowali zdobyć dane uwierzytelniające do takich serwisów jak Yahoo, Google Talk czy Mail.ru oraz dane użytkowników przechowywane w MS Outlook, Mozilla Thunderbird i Firefoksie. Kod ten został również wykorzystany do ataków na agendy rządów Gruzji, Polski, Czech, Turcji, Ugandy i amerykańskie think-tanki. Specjaliści podejrzewają, że PinchDuke był kodem eksperymentalnym, służącym nabyciu odpowiednich umiejętności i doświadczeń. Kolejny z rodziny to CosmicDuke zauważony po raz pierwszy na początku 2010 roku. Ostatnią jego aktywność zanotowano latem bieżącego roku. To kod kradnący informacje, wyposażony w funkcję keyloggera, potrafi też wykonywać zrzuty ekranowe i kraść dane ze Schowka systemu Windows. Wyszukuje pliki o określonych rozszerzeniach, kradnie nazwy użytkownika, hasła i klucze kryptograficzne.

Z kolei MiniDuke to wielowarstwowa kombinacja różnych loaderów. Pierwszym kodem, który MiniDuke instalował na zainfekowanym systemie był backdoor, który otrzymywał polecenia za pośrednictwem Twittera. MiniDuke był aktywny jeszcze wiosną bieżącego roku. Wspomnianego backdoora nie zauważono od roku. CozyDuke to kod modułowy, który na polecenie z serwera sterującego ładuje różne moduły, więc może wyglądać różnie w zależności od komputera, który padł jego ofiarą. Jest to backdoor z możliwością zapisywania naciśnięć klawiszy, wykonywania zrzutów ekranowych, kradnie też hasła, w tym hasło administratora sieci lokalnej, co prawdopodobnie umożliwia mu rozprzestrzenianie się po niej. CozyDuke może też otrzymać polecnie pobrania i zainstalowania innego kodu. Eksperci obserwowali ataki, gdy kod pobierał ogólnie dostępne

narzędzia hakerskie i czynił z nich użytek. Interesującym kodem jest OnionDuke, backdoor, który zyskał swoją nazwę, gdyż był rozpowszechniany za pomocą jednego z węzłów sieci tor. To kod modularny, potrafiący kraść dane, przeprowadzający ataki DDoS oraz generujący spam. Jest on rozpowszechniany m.in. za pośrednictwem torrentów. Najnowsze osiągnięcie the Dukes to CloudDuke odkryty w czerwcu bieżącego roku. Jedna z jego odmian rozpowszechnia się za pomocą WWW. CloudDuke to loader działający też jak backdoor. Jego głównym celem są pliki przechowywane w microsoftowej chmurze OneDrive.

O tym, że the Dukes są co najmniej powiązani z Moskwą świadczy nie tylko dobór celów, ale i rosyjskojęzyczne komentarze pozostawione w kodzie. Ponadto czas przeprowadzania różnych ataków jest zbieżny z działaniami Rosji. Na przykład w 2013 roku przed rozpoczęciem kryzysu na Ukrainie grupa rozsyłała fałszywe informacje, które rzekomo pochodziły z ukraińskich ministerstw lub z ambasad obcych państw mających swoje siedziby na Ukrainie. Celem takich fałszywych dokumentów było zarażenie konkretnych komputerów rządowych. Obecnie zaś obserwuje się spadek liczby ataków the Dukes na Ukrainę, co sugeruje, że ataki prowadzono w celu zebrania informacji wywiadowczych potrzebnych do przeprowadzenia operacji wojskowych czy dyplomatycznych przeciwko Ukrainie.

„Sądzimy, że na pracy tej grupy korzysta rząd. Czy the Dukes to zespół lub wydział wewnątrz którejś z rządowych agend, czy jest to zewnętrzny podmiot pracujący na zlecenie. czy cybergang sprzedający informacje temu, kto zapłaci najwięcej czy też to grupa ochotników-patriotów – tego nie wiemy” – mówią przedstawiciele the Dukes. Wszystko jednak wskazuje na to, że to dobrze finansowana i zorganizowana grupa, która ma jasno wytyczone cele. Trudno przypuszczać, by działała ona bez co najmniej zgody rosyjskiego rządu.

Autorstwo: Mariusz Błoński
Na podstawie: ArsTechnica.com
Źródło: KopalniaWiedzy.pl