Zatrzymano grupę cyberprzestępczą Lockbit

20 lutego 2024

Ważne wydarzenie miało miejsce w światowej walce z cyberprzestępczością. Lockbit, znana grupa przestępcza, specjalizująca się w szantażowaniu ofiar danymi, została zatrzymana w rzadkiej międzynarodowej operacji policyjnej prowadzonej przez Narodowe Biuro ds. Przestępczości (NCA) Wielkiej Brytanii oraz Federalne Biuro Śledcze (FBI) Stanów Zjednoczonych.

Informacja o zatrzymaniu grupy pojawiła się na stronie internetowej, którą dotychczas kontrolowała grupa przestępcza. „Ta strona jest teraz pod kontrolą Narodowego Biura ds. Przestępczości Wielkiej Brytanii, działającego w ścisłej współpracy z FBI i międzynarodową siłą policyjną »Operacja Cronos«" – głosi oświadczenie. Rzecznik NCA potwierdził zatrzymanie działalności grupy przestępczej, dodając, że operacja „trwa i rozwija się".

Lockbit oraz jej sojusznicy zaatakowali w ostatnich miesiącach niektóre z największych organizacji na świecie, wykorzystując metody polegające na kradzieży wrażliwych danych i żądaniu ogromnych okupów pod groźbą ujawnienia tych informacji. Partnerzy Lockbita działają jak podwykonawcy przestępczej działalności, rekrutowani przez grupę do przeprowadzania ataków za pomocą narzędzi do cyfrowego szantażu.

Ransomware, złośliwe oprogramowanie wykorzystywane przez Lockbita, szyfruje dane i domaga się okupu za ich odszyfrowanie lub odblokowanie za pomocą klucza cyfrowego, co czyni tę działalność niezwykle opłacalną dla cyberprzestępców. „Grupa Lockbit to taki Walmart wśród grup szantażujących,

prowadzą ją jak biznes – to właśnie odróżnia ich od innych" – powiedział Jon DiMaggio, główny strateg bezpieczeństwa w Analyst 1, amerykańskiej firmy zajmującej się cyberbezpieczeństwem. „To być może największa grupa szantażu danymi w dzisiejszych czasach".

Zatrzymanie działalności Lockbita stanowi istotne zwycięstwo w trwającej walce z cyberprzestępczością, podkreślając wspólne wysiłki międzynarodowych agencji policyjnych w zwalczaniu zagrożeń cyfrowych i ochronie organizacji i jednostek przed atakami internetowymi.

Incydenty związane z ransomware występują od ponad 30 lat, jednak dopiero w ostatniej dekadzie termin „ransomware" regularnie pojawia się w mediach. Ransomware to rodzaj złośliwego oprogramowania, które blokuje dostęp do systemów komputerowych lub szyfruje pliki, dopóki nie zostanie zapłacony okup. Gangi cyberprzestępcze przejęły ransomware jako szybki sposób na wzbogacenie się. Obecnie, w epoce „ransomware jako usługa", stało się to wszechobecną i bardzo dochodową taktyką. Świadczenie ransomware jako usługi oznacza, że grupy korzystają z programów partnerskich, w ramach których pobierana jest prowizja za udane żądania okupu. Mimo że jest tylko jedną z wielu działających grup, LockBit zyskuje coraz większą widoczność, z kilkoma wysokoprofilowymi ofiarami, które niedawno pojawiły się na stronie grupy.

Czym jest LockBit? Aby sprawić, żeby było to jeszcze bardziej mylące, termin LockBit odnosi się zarówno do złośliwego oprogramowania (malware), jak i do grupy, która je stworzyła. LockBit zyskał pierwszą uwagę w 2019 roku. Jest to forma oprogramowania, która została celowo zaprojektowana w celu tajnego wdrożenia wewnątrz organizacji, w celu znalezienia wartościowych danych i ich kradzieży. Ale zamiast po prostu kradzieży danych, LockBit jest formą ransomware. Po skopiowaniu danych są one szyfrowane, uniemożliwiając dostęp dla prawowitych użytkowników. Dane są następnie przetrzymywane jako okup – zapłać, albo nigdy więcej nie zobaczysz swoich

danych. Aby dodatkowo zachęcić ofiarę, jeśli okup nie zostanie zapłacony, grożą ujawnieniem skradzionych danych (często opisanych jako podwójna ekstorsja). Zagrożenie to jest wzmocnione licznikiem odliczania na blogu LockBit na dark webie.

Niewiele jest wiadomo o grupie LockBit. Na podstawie ich strony internetowej, grupa nie ma konkretnego zobowiązania politycznego. W przeciwieństwie do niektórych innych grup, również nie ograniczają liczby partnerów. O sobie mówią: „Jesteśmy zlokalizowani w Holandii, całkowicie apolityczni i zainteresowani tylko pieniędzmi. Mamy zawsze nieograniczoną liczbę partnerów, wystarczająco dużo miejsca dla wszystkich profesjonalistów. Nie ma znaczenia, w jakim kraju mieszkasz, jakim językiem mówisz, ile masz lat, w co wierzysz religii, każdy na świecie może pracować z nami w dowolnym momencie roku".

LockBit ma jednak swoje zasady dla swoich partnerów. Przykłady zakazanych celów (ofiar) obejmują infrastrukturę krytyczną instytucji, w których uszkodzenie plików mogłoby prowadzić do śmierci (np. szpitale) oraz kraje postradzieckie (takie jak Armenia, Białoruś, Estonia, Gruzja, Kazachstan, Kirgistan, Łotwa, Litwa, Mołdawia, Rosja, Tadżykistan, Turkmenistan, Ukraina i Uzbekistan). Inni dostawcy ransomware również twierdzili, że nie będą atakować instytucji takich jak szpitale – ale to nie gwarantuje bezpieczeństwa ofiary. W tym roku kanadyjski szpital padł ofiarą LockBit, co skłoniło grupę stojącą za LockBit do opublikowania przeprosin, zaoferowania darmowych narzędzi do deszyfrowania i rzekomo wydalenia partnera, który zhakował szpital.

Mimo obecności zasad zawsze istnieje potencjał, że są użytkownicy, którzy zechcą atakować zakazane organizacje. Ostatnia reguła na liście powyżej jest interesującym wyjątkiem. Według grupy te kraje są poza ich zasięgiem, ponieważ duża część członków grupy „urodziła się i dorastała w Związku Radzieckim", mimo że teraz „znajdują się w Holandii".

Kto został zhakowany przez LockBit? Wysokiej klasy ofiarami są m.in. Royal Mail i Ministerstwo Obrony Wielkiej Brytanii oraz japoński producent komponentów rowerowych Shimano. Dane skradzione z firmy lotniczej Boeing zostały ujawnione właśnie w tygodzień po tym, jak firma odmówiła zapłaty okupu LockBitowi. Chociaż jeszcze nie potwierdzono, to niedawne zdarzenie związane z ransomware, którego miał doświadczyć Industrial and Commercial Bank of China zostało zgłoszone przez LockBit. Od momentu pojawienia się na scenie cyberprzestępczości, LockBit został powiązany tylko w Stanach Zjednoczonych z niemal 2000 ofiarami.

Z listy ofiar widocznej wynika, że LockBit jest wyraźnie używany szeroko, z dużą gamą ofiar. Nie jest to seria zaplanowanych, ukierunkowanych ataków. Oprogramowanie LockBit jest używane przez różnorodne grupy przestępców w modelu usługowym.

Autorstwo: DA/DE
Na podstawie: Reuters.com
Źródło: Brytol.com