**Hakerzy biorą na celownik służbę zdrowia. SamSam Ransomware infekuje Stowarzyszenie Lekarzy w stanie Indiana.**

**Ransomware pozostaje największym zagrożeniem, z którym borykają się firmy od początku 2018 roku. Od czasu pojawienia się pierwszych odmian w 2013 roku, aż po dziś dzień, skala ataków wciąż rośnie. Ostatnie incydenty pokazały, że aktualnie na celowniku znajduje się służba zdrowia.**

Najświeższe doniesienia pochodzą ze stanu Indiana, dokładniej z South Bend. Allied Physicians Of Michiana, czyli tamtejsza służba zdrowia zgłosiła, że padła ofiarą Ransomware SamSam. W oficjalnym komunikacie prasowym możemy przeczytać, że system został zainfekowany i jakie kroki podjęto w celu ochrony danych.

„Natychmiast podjęto kroki w celu zamknięcia dostępu do sieci, aby ochronić dane osobowe i informacje o stanach zdrowotnych pacjentów”, głosi komunikat. „Wraz z personelem, specjalistą ds. ochrony danych, zewnętrznymi doradcami i innymi specjalistami, firma była w stanie przywrócić dane w bezpieczny sposób i zachować niezachwiane działanie usług świadczonych pacjentom.”

Na miejsce została wezwana grupa FBI, aby zbadać sprawę. Firma odmawia jednak odpowiedzi na pytanie, czy zapłaciła okup, aby odzyskać dostęp do swoich danych.

W komunikacie możemy przeczytać „Bezpieczeństwo danych naszych klientów jest najważniejsze” – powiedział CEO Shery Roussarie. „Dokładamy wszelkich starań, aby uprzedzić tego rodzaju cyberataki i mamy nadzieję nie doświadczyć tego rodzaju naruszeń w przyszłości.”

**Ale co to jest SamSam?**

SamSam to szczep ransomware, który przechwytuje dane za pomocą szyfrowania RSA-2048. Rozprzestrzenia się za pośrednictwem aplikacji Java, jako cel obiera serwery RDP, czyli tzw. zdalny pulpit. Używa techniki „Brute Force” do znalezienia i łamania prostych haseł w sieci. Następnie po złamaniu zabezpieczeń, za pomocą wbudowanego skryptu rozprzestrzenia się infekując każdy wrażliwy system w zasięgu.

Pierwsza wersja SamSam potrafiła rozpoznać i zaszyfrować 79 typów plików, w tym najpopularniejsze java, jar, cs, jpg, html, dane, conf, pptx, docx, pdf, xls itp. Kiedy atak zaczął być powszechnie znany, atakujący zwykle żądali od 30 do 40 bitcoinów, co odpowiadało 15 000 $ w tamtym czasie. Ta sama ilość kryptowaluty dzisiaj warta jest około 300 000$.

„SamSam od pewnego czasu jest na radarach specjalistów ds. cyberbezpieczeństwa, jak z resztą cały wzrastający trend ransomware., komentuje Mariusz Politowicz, inżynier techniczny Bitdefender z firmy Marken, „Eksperci twierdzą, że hakerzy cenią dane medyczne ze względu na ich osobistą i wrażliwą naturę, dlatego na cel obrali właśnie instytucje opieki zdrowotnej jako zyskowny cel ataków” – dodaje.

**Wcześniejsze występki**

W tym roku zaatakowany został również dostawca rozwiązań wykorzystywanych w systemach dokumentacji medycznej. SamSam spowodował wtedy awarię, która dotknęła tysiące klientów firmy w Stanach Zjednoczonych, z tego powodu część instytucji musiała wtedy odwołać wiele zaplanowanych wizyt.

Aby przybliżyć skalę ataku podamy kilka danych, które udostępnia Allscripts – sprzedawca w/w technologii. Firma obsługuje 280 000 lekarzy, 40 000 prywatnych klinik, 2 700 szpitali, 13 000 innych organizacji opieki zdrowotnej oraz łącznie posiada w swojej bazie 7 milionów pacjentów.

Inny przykład, trzy miesiące temu SamSam został użyty do zakłócenia pracy Departamentu Transportu w stanie Kolorado, zmuszając administratorów do odłączenia 2000 komputerów, aby zapobiec dalszemu rozprzestrzenianiu się wirusa.