Jak bronić się przed cyberprzestępczością w nowym wydaniu?

Statystyki są jednoznaczne. Polskie firmy i zwykli użytkownicy internetu dołączają do grona światowych ofiar zdumiewająco podstępnych ataków hakerskich. Wielu z poszkodowanych decyduje się na współpracę z cyberprzestępcami i płaci okupy… za dostęp do własnych komputerów. Sprawdź, jak radzić sobie ze zjawiskiem, w kontekście którego programy antywirusowe bywają bezradne.

Ataki hackerów większość z nas zna z filmów sensacyjnych lub serwisów informacyjnych, które donoszą o najbardziej spektakularnych, wirtualnych włamach do systemów banków i globalnych instytucji. Tymczasem w cieniu tych najgłośniejszych historii, rośnie proceder, którego celem może być każdy z nas. Ransomware nie dotyka najbogatszych, dotyka wszystkich tych, dla których dane w ich komputerze są czymś więcej, niż tylko zbiorem mało istotnych plików. Jeśli zatem twój laptop zawiera zapis kilku lat twojej pracy albo zdjęcia najbliższych, o których zawsze mówiłeś, że są cenniejsze, niż złoto, cyberprzestępcy chętnie to zweryfikują. Ransomware jest bezlitosny.

Płać, albo trać!

Nazwa „Ransomware" pochodzi od angielskiego słowa ransom, czyli okup. Ransomware jest zatem oprogramowaniem, którego celem jest wymuszenie okupu. Działanie cyberprzestępców jest w zasadzie bardzo proste – szkodliwy plik bez świadomości użytkownika instalowany jest na jego komputerze. Po zainfekowaniu dysku twardego, wszystkie znajdujące się na nim dane zostają zaszyfrowane w sposób, który absolutnie wyklucza jakikolwiek do nich wgląd, chyba, że… zapłacimy za ich odszyfrowanie!
W przeciwnym razie już nigdy nie skorzystamy z plików, a utrata dostępu do danych to dla większości firm i instytucji totalna katastrofa.

„Zwykle w tym właśnie momencie firmy lub użytkownicy prywatni trafiają do mnie." – mówi Jakub Wychowański, szef działu bezpieczeństwa danych VECTO, spółki specjalizującej się w systemach IT i ochrony danych w Polsce. „Niestety, jedynym sposobem na uniknięcie płacenia żądanego okupu jest profilaktyka, czyli wcześniejsze zabezpieczenie urządzeń i minimalizacja ryzyka zainfekowania dysków twardych szkodliwym oprogramowaniem. Warto zauważyć, że większość standardowych programów antywirusowych nie chroni naszych urządzeń przed ransomware. Klienci, którzy zgłaszają się do nas po przeprowadzonym ataku są zwykle tym zaskoczeni. Prowadzone przez nas statystyki są jednoznaczne. Skala problemu w Polsce rośnie, a przypadki zgłaszania ransomware odnotowujemy w zasadzie codziennie. Jeszcze kilka miesięcy temu było to zjawisko incydentalne." – dodaje Wychowański.

Jak dochodzi do ataku ransomware?

Najczęściej to sami użytkownicy, nieświadomie infekują swój sprzęt. Uruchamianie załączników poczty, fałszywe

reklamy, odwiedzanie niebezpiecznych stron internetowych to tylko kilka z wielu dotychczas najczęściej diagnozowanych powodów instalacji ransomware. Jednak coraz częściej, zagnieżdżenie złośliwego oprogramowania następuje niezauważalnie w trakcie korzystania z serwisów społecznościowych. „Luki w zabezpieczeniach powszechnie stosowanych aplikacji niestety ułatwiają dostęp do naszych komputerów. W zeszłym tygodniu światowy potentat w dziedzinie tworzenia oprogramowania, Adobe, wezwał użytkowników do aktualizacji wtyczki Flash, która stosowana jest przez większość przeglądarek internetowych. Adobe przyznało, że znaleziona luka umożliwia ataki typu ransomware" – mówi Wychowański.

Według opublikowanego w zeszłym roku raportu McAfee Labs Threats Report 2015, od czerwca 2014 roku poszkodowani atakami ransomware zapłacili cyberprzestępcom okupy na niebotyczną kwotę 325 milionów dolarów. Transfery tak gigantycznych kwot powinny być łatwo wykrywalne przez służby śledcze, jednak hakerzy żądają zapłaty w „bitcoin'ach" – wirtualnej krypto walucie. Identyfikacja adresatów takich transakcji jest niezwykle trudna. Wartość okupu, w przeliczeniu na złotówki wynosi zwykle od 800 złotych do nawet 40 000 złotych. „Jestem przekonany, że mnóstwo zapłaconych okupów opiewało na wielokrotność tej kwoty. Badania wskazują, że wiele firm jest gotowych zapłacić nie tylko za odszyfrowanie danych, ale i zachowanie zdarzenia w tajemnicy. Możliwość uniknięcia katastrofy wizerunkowej i utraty zaufania klientów i partnerów biznesowych dla wielu instytucji jest warta każdej ceny." – twierdzi jeden z kilkunastu specjalistów IT w firmie VECTO.

Jak się bronić przed ransomware?

Ryzyko konsekwencji przestępczej działalności hakerów można minimalizować. Jak twierdzą informatycy VECTO, najprostszym sposobem jest częste tworzenie kopii zapasowych umieszczanych w tzw. chmurze lub zewnętrznych nośnikach danych i zachowanie dużej ostrożności podczas codziennego korzystania z komputera oraz internetu. Należy unikać wchodzenia na strony zawierające niebezpieczne treści i otwierania załączników do poczty pochodzącej od nieznanych lub podejrzanych adresatów. Firmy i instytucje mogą skorzystać z kompleksowego, miesięcznego zabezpieczenia w cenie 39 PLN, które od kilkunastu tygodni ma w swojej ofercie VECTO. „Jesteśmy przygotowani na nadejście fali ataków typu ransomware, jaka w tej chwili przechodzi w USA i krajach Europy Zachodniej. Stale współpracujemy z potentatami w dziedzinie bezpieczeństwa i ochrony danych, dzięki czemu wiem jak reagować na zagrożenia ransomware. Wiele jednak zależy od świadomości niebezpieczeństw pracowników firm i instytucji, które mogą stać się obiektem potencjalnego ataku." – podsumowuje Jakub Wychowański.

Więcej informacji:
www.vecto.pl



VECTO sp. z o.o. działa od 2008 roku. Forma łączy kilkudziesięcioletnie doświadczenie kadry kierowniczej z potencjałem młodego zespołu, który rozumie realia rynku IT i wyzwania stojące przed firmami i instytucjami wobec dynamicznie zmieniającej się technologii.
Spółka dostarcza i wdraża systemy informatyczne oraz świadczy usługi outsourcingu IT dla firm. Oferuje kompleksowe rozwiązania zabezpieczania danych oraz backupu w oparciu o produkty renomowanej firmy EMC. Wszystkie prace wdrożeniowe wykonuje zespół certyfikowanych, doświadczonych inżynierów.

VECTO