Identyfikacja naruszenia bezpieczeństwa

Pomimo odważnych wysiłków w celu ochrony systemów komputerowych i danych, możesz doznać pewnego rodzaju włamania. W rzeczywistości szanse, że w pewnym momencie Twoje dane zostaną naruszone, są bliskie 100%. Jedynym prawdziwym pytaniem jest, czy włamanie nastąpi w Twoim systemie, czy w systemie kogoś innego. Ponieważ ponosisz ostateczną odpowiedzialność za utrzymanie własnych systemów komputerowych, musisz być w stanie rozpoznać oznaki potencjalnego uszkodzenia sprzętu. Jeśli hakerowi uda się przeniknąć do Twoich systemów, musisz jak najszybciej zablokować jego dostęp. Jeśli Twoje dane zostały zmanipulowane lub zniszczone, musisz przywrócić ich dokładną kopię. Jeśli systemy działają nieprawidłowo, musisz przywrócić je na właściwe tory.

Tu poznasz objawy włamania. Uzbrojeni w tę wiedzę, miejmy nadzieję, potrafisz rozpoznać, czy coś jest nie tak i wiedzieć, jakie działania naprawcze należy podjąć. Jeśli otrzymałeś już powiadomienie od zewnętrznego dostawcy, w którym przechowujesz dane, że Twoje dane zostały naruszone lub mogły zostać naruszone.

Rozpoznawanie jawnych naruszeń

Najłatwiejsze do zidentyfikowania są te, w których osoba atakująca informuje Cię, że nastąpiło włamanie, i dostarcza dowodów na to. Trzy z najczęstszych jawnych naruszeń to te związane z oprogramowaniem ransomware, zniszczeniem i deklarowanym zniszczeniem.

Oprogramowanie ransomware

Oprogramowanie wymuszające okup to złośliwe oprogramowanie, które szyfruje lub kradnie dane na urządzeniu użytkownika i żąda okupu w celu przywrócenia kontroli nad danymi. Zwykle oprogramowanie ransomware zawiera datę wygaśnięcia z ostrzeżeniem o treści „zapłać w ciągu x godzin albo dane zostaną zniszczone na zawsze!" Oczywiście, jeśli Twoje urządzenie zgłasza takie zapotrzebowanie, a ważne pliki, które powinny być dla Ciebie dostępne, nie są dostępne, ponieważ ich brakuje lub są one zaszyfrowane, możesz być pewny, że musisz podjąć działania naprawcze.

Jedna uwaga: niektóre odmiany fałszywego oprogramowania ransomware na smartfony - tak, to prawda - wyświetlają takie wiadomości, ale w rzeczywistości nie szyfrują, nie niszczą ani nie kradną danych. Przed podjęciem jakichkolwiek działań naprawczych zawsze sprawdź, czy oprogramowanie ransomware jest prawdziwe.

Wymazanie

Defacement odnosi się do włamań, w których atakujący niszczy systemy ofiary - na przykład zmieniając witrynę celu, aby wyświetlała wiadomość, że haker ją zhakował (w niemal „wirtualnym graffiti metra" - jak w sensie) lub wiadomość o wsparciu dla z jakiejś przyczyny, jak to często bywa w przypadku haktywistów. Jeśli masz osobistą witrynę internetową i jest ona zniszczona lub jeśli uruchamiasz komputer i wyświetla ona komunikat o ataku hakerskim przez <jakiegoś hakera>, możesz być dość pewny, że nastąpiło włamanie i że musisz podjąć działania naprawcze. Oczywiście naruszenie mogło mieć miejsce w witrynie hostującej Twoją witrynę, a nie na Twoim komputerze lokalnym

Roszczone zniszczenie

Hakerzy mogą zniszczyć dane lub programy, ale także awarie techniczne lub błędy ludzkie. Dlatego fakt, że dane zostały usunięte, nie oznacza, że doszło do naruszenia systemu. Jeśli jednak jakaś strona przyzna się do odpowiedzialności, prawdopodobieństwo, że problemy są wynikiem naruszenia, może gwałtownie wzrosnąć o określony plik lub zestaw plików, o których wiedziałaby tylko strona mająca

dostęp do systemu, a to jedyne pliki, które zniknęły, możesz być pewnym, że problem, z którym masz do czynienia, nie dotyczy awarii sektorów dysku twardego lub chipów dysku SSD.

Wykrywanie ukrytych naruszeń

Podczas gdy niektóre naruszenia są oczywiście widoczne jako naruszenia, większość z nich jest w rzeczywistości dość trudna do wykrycia. W rzeczywistości naruszenia są czasami tak trudne do zauważenia, że różne przedsiębiorstwa, które wydają miliony dolarów rocznie na systemy, które próbują zidentyfikować naruszenia, pozostawały niewykryte przez dłuższy czas - czasami przez lata! W poniższych sekcjach opisano niektóre objawy, które mogą wskazywać na naruszenie bezpieczeństwa komputera, tabletu lub smartfona. Należy pamiętać, że żadna z poniższych wskazówek nie istnieje w próżni, a sama obecność jakiegokolwiek indywidualnego objawu nie gwarantuje, że coś jest nie tak. Wiele przyczyn innych niż wystąpienie naruszenia może powodować nieprawidłowe działanie urządzeń i wykazywać jedną lub więcej dolegliwości opisanych w kolejnych sekcjach. Jeśli jednak urządzenie nagle wydaje się cierpieć z powodu wielu podejrzanych zachowań lub jeśli odpowiednie problemy pojawiają się tuż po kliknięciu łącza w wiadomości e-mail lub SMS-a, pobranie i uruchomienie oprogramowania dostarczonego przez źródło z potencjalnie wadliwymi procedurami bezpieczeństwa otwiera niektóre wątpliwe przywiązanie lub zrobiłeś coś innego, o którą mądrość teraz kwestionujesz, możesz podjąć działania naprawcze, zgodnie z opisem.

Rozważając prawdopodobieństwo naruszenia systemu, należy wziąć pod uwagę istotne okoliczności. Jeśli na przykład problemy zaczną się pojawiać po automatycznej aktualizacji systemu operacyjnego, prawdopodobny poziom ryzyka jest znacznie niższy, niż gdyby te same objawy zaczęły się pojawiać zaraz po kliknięciu łącza w podejrzanej wiadomości e-mail oferującej 1 000 000 USD w przypadku przetworzenia płatności wysłany przez księcia z Nigerii do kogoś w Stanach Zjednoczonych. Zachowaj odpowiednią perspektywę i nie panikuj. Jeśli coś poszło nie tak, nadal możesz podjąć działania, aby zminimalizować szkody. Twoje urządzenie wydaje się działać wolniej niż wcześniej. Złośliwe oprogramowanie działające na komputerze, tablecie lub smartfonie często wpływa na wydajność urządzenia w zauważalny sposób. Złośliwe oprogramowanie, które przesyła dane, może czasami spowalniać połączenie urządzenia z Internetem lub nawet z sieciami wewnętrznymi. Pamiętaj jednak, że aktualizacje systemu operacyjnego urządzenia lub różnych pakietów oprogramowania mogą również negatywnie wpłynąć na wydajność urządzenia, więc nie panikuj, jeśli zauważysz, że wydajność wydaje się nieco obniżona zaraz po zaktualizowaniu systemu operacyjnego lub zainstalowaniu aktualizacja oprogramowania z zaufanego źródła. Podobnie, jeśli zapełnisz pamięć w urządzeniu lub zainstalujesz wiele aplikacji intensywnie korzystających z procesora i przepustowości, wydajność prawdopodobnie spadnie nawet bez obecności złośliwego oprogramowania. Możesz zobaczyć, co działa na komputerze z systemem Windows, naciskając Ctrl + Shift + Esc i sprawdzając wyskakujące okno Menedżera zadań. Na komputerze Mac użyj Monitora aktywności, do którego można uzyskać dostęp, klikając lupę po prawej stronie paska menu u góry ekranu i rozpoczynając wpisywanie Monitor aktywności. Po wpisaniu kilku pierwszych znaków powinna wyświetlić się nazwa narzędzia, w którym to momencie możesz nacisnąć Enter, aby je uruchomić.

Menedżer zadań nie działa Jeśli spróbujesz uruchomić Menedżera zadań w systemie Windows lub Monitor aktywności na komputerze Mac (patrz poprzednia sekcja), a narzędzie nie działa, komputer może być zainfekowany złośliwym oprogramowaniem. Wiadomo, że różne szczepy złośliwego oprogramowania wpływają na działanie tych programów.

Twój Edytor rejestru nie działa

Jeśli spróbujesz uruchomić Edytor rejestru w systemie Windows (na przykład wpisując regedit w wierszu polecenia Uruchom), a program nie uruchamia się, komputer może być zainfekowany

złośliwym oprogramowaniem. Wiadomo, że różne szczepy złośliwego oprogramowania wpływają na działanie Edytora rejestru. Należy pamiętać, że podczas uruchamiania Edytora rejestru może pojawić się ostrzeżenie, że wymaga uprawnień administratora. To ostrzeżenie jest normalne i nie jest oznaką problemu. Powinien także przypominać o potencjalnie poważnych konsekwencjach wprowadzania zmian w rejestrze: nie rób żadnych, jeśli nie masz pewności, co robisz. Twoje urządzenie zaczyna cierpieć z powodu problemów z opóźnieniem Opóźnienie odnosi się do czasu potrzebnego na rozpoczęcie przesyłania danych po wydaniu instrukcji. Jeśli zauważysz opóźnienia, których wcześniej nie było - zwłaszcza jeśli wydają się one znaczące - coś może być nie tak. Oczywiście Twój dostawca Internetu lub ktoś inny może mieć problemy i wszystko może być w porządku na Twoim urządzeniu lokalnym. Jeśli jednak problemy z opóźnieniem pojawiają się tylko z jednego urządzenia lub określonego zestawu urządzeń, a nie ze wszystkich urządzeń podłączonych do tej samej sieci, i jeśli ponowne uruchomienie urządzenia, którego dotyczy problem, nie poprawi sytuacji, może to oznaczać, że Twoje urządzenie / urządzenia zostały naruszone. Jeśli urządzenie korzysta z przewodowego połączenia sieciowego, przetestuj je przy użyciu nowego kabla. Jeśli problem zniknie, prawdopodobnie przyczyną było wadliwe lub uszkodzone połączenie fizyczne. Twoje urządzenie zaczyna cierpieć z powodu problemów z komunikacją i buforowaniem. Jednym z bardzo wizualnych symptomów problemów z komunikacją i wydajnością, które można łatwo zauważyć bez dużej wiedzy technicznej, jest to, że przesyłanie strumieniowe wideo wydaje się zawieszać podczas wstępnego ładowania przyszłych ramek lub buforowania, znacznie częściej niż w przypadku przeszłość . Podczas gdy buforowanie jest irytacją, która zdarza się od czasu do czasu większości ludzi, jeśli dzieje się to regularnie na połączeniu, które wcześniej nie cierpiało regularnie na taką dolegliwość lub dzieje się to tylko z jednego lub kilku konkretnych urządzeń korzystających z połączenia, ale nie na innych, może to wskazywać na zhakowany system. Jeśli urządzenie korzysta z przewodowego połączenia sieciowego, sprawdź wszystkie fizyczne kable, które mogą powodować problemy z siecią. Zwróć uwagę, że problemy z wydajnością komunikacji mogą być również oznaką, że ktoś korzysta z twojego połączenia internetowego, co jest również rodzajem naruszenia.

Zmieniły się ustawienia Twojego urządzenia

Jeśli zauważysz, że niektóre ustawienia Twojego urządzenia uległy zmianie - i masz pewność, że to nie Ty je wprowadziłeś - może to oznaczać problem. Oczywiście niektóre programy również wprowadzają zmiany w ustawieniach (szczególnie na klasycznych komputerach, w przeciwieństwie do smartfonów), więc zmiany mogą mieć również uzasadnione źródło. Jednak większość oprogramowania nie wprowadza większych zmian bez powiadomienia. Uważaj, jeśli zauważysz dramatyczne zmiany ustawień. Twoje urządzenie wysyła lub odbiera dziwne wiadomości e-mail Jeśli Twoi znajomi lub współpracownicy zgłaszają otrzymywanie e-maili od Ciebie, które zrobiłeś.Jeśli Twoi znajomi lub współpracownicy zgłaszają, że otrzymują od Ciebie wiadomości e-mail, których do nich nie wysłałeś, prawdopodobnie coś jest nie tak - jest to szczególnie prawdziwe, jeśli wiadomości wyglądają na spam. Podobnie, jeśli otrzymujesz e-maile, które wydają się pochodzić od osób, które twierdzą, że nigdy nie wysłały odpowiednich wiadomości, może to oznaczać, że doszło do naruszenia.

Pamiętaj jednak, że wiele innych powodów (w tym inne rodzaje ataków na systemy inne niż Twoje własne urządzenia i konta) może prowadzić do tego, że spam wydaje się pochodzić od Ciebie.

Twoje urządzenie wysyła lub odbiera dziwne wiadomości tekstowe.

Jeśli Twoi znajomi lub koledzy zgłaszają otrzymywanie od Ciebie wiadomości tekstowych lub innych wiadomości typu smartfona, których im nie wysłałeś, może to oznaczać, że ktoś włamał się na Twój smartfon. Podobnie, jeśli otrzymujesz wiadomości, które wydają się pochodzić od osób, które twierdzą, że nigdy nie wysłały odpowiednich wiadomości, możliwe, że doszło do naruszenia.

Na Twoim urządzeniu jest zainstalowane nowe oprogramowanie (w tym aplikacje) - ale nie zostało ono zainstalowane. Jeśli na urządzeniu nagle pojawiają się nowe programy lub aplikacje, a ich nie zainstalowałeś, może być coś nie tak. Chociaż w przypadku niektórych urządzeń przenośnych producent lub odpowiedni usługodawca może czasami instalować określone typy aplikacji bez Twojej wiedzy, jeśli nagle pojawią się nowe aplikacje, zawsze powinieneś przyjrzeć się sprawie. Wyszukaj w Google aplikacje i zobacz, co mówią o nich wiarygodne witryny techniczne. Jeśli aplikacje nie wyświetlają się na urządzeniach innych osób, możesz mieć poważny problem na rękach. Należy jednak pamiętać, że czasami procedury instalacyjne jednego programu instalują również inne aplikacje. Na przykład dość często zdarza się, że różne programy, które są oferowane użytkownikom bezpłatnie w wersji z ograniczonymi funkcjami, instalują również inne programy, które są sprzedawane razem z nimi. Zwykle takie programy instalacyjne proszą o pozwolenie na instalację dodatkowych programów, ale taka przejrzystość nie jest wymagana przez prawo, a niektóre aplikacje nie dają użytkownikom takiego wyboru. Pamiętaj też, że jeśli pozwolisz komuś innemu komputerowi, może on coś zainstalował (legalnie lub nielegalnie).

Wydaje się, że bateria Twojego urządzenia wyczerpuje się szybciej niż wcześniej

Złośliwe oprogramowanie działające w tle zużywa energię baterii i może pomóc w rozładowaniu baterii laptopów, smartfonów i tabletów.

Wydaje się, że Twoje urządzenie nagrzewa się bardziej niż wcześniej

Złośliwe oprogramowanie działające w tle wykorzystuje cykle procesora i może spowodować, że urządzenie będzie fizycznie gorętsze niż wcześniej. Możesz usłyszeć, że wewnętrzne wentylatory chłodzące pracują głośniej lub częściej niż zwykle lub możesz poczuć, że urządzenie jest cieplejsze w dotyku.

Zawartość pliku została zmieniona

Jeśli zawartość plików uległa zmianie bez ich zmiany i bez uruchamiania oprogramowania, które mogłoby je zmienić, coś może być naprawdę nie tak. Oczywiście, jeśli pozwolisz komuś innemu używać swoich komputerów i dasz mu dostęp do plików, o których mowa, zanim obwinisz złośliwe oprogramowanie lub hakera, koniecznie zapytaj osobę, której zezwalasz używać komputera, czy wprowadziła jakieś zmiany.

Brak plików

Jeśli wydaje się, że pliki zniknęły bez ich usunięcia i bez uruchamiania jakiegokolwiek oprogramowania, które może je usunąć, coś może być naprawdę nie tak. Oczywiście awarie techniczne i błędy ludzkie również mogą powodować znikanie plików - a jeśli pozwolisz komuś innemu używać swojego komputera, może być winowajcą. Witryny internetowe wyglądają nieco inaczej niż wcześniej Jeśli ktoś zainstalował złośliwe oprogramowanie, które pośredniczy na Twoim urządzeniu - to znaczy siedzi między Twoją przeglądarką a Internetem i przekazuje komunikację między nimi (podczas czytania całej treści komunikacji i być może wstawiania różnych instrukcji sama w sobie) - może wpływać na sposób wyświetlania niektórych witryn.

Twoje ustawienia internetowe pokazują serwer proxy i nigdy go nie konfigurujesz

Jeśli ktoś skonfigurował Twoje urządzenie do używania swojego serwera jako serwera proxy, strona ta może próbować odczytać dane wysyłane do iz Twojego urządzenia i może próbować zmodyfikować zawartość Twojej sesji, a nawet próbować całkowicie ją przejąć. Niektóre legalne programy konfigurują internetowe serwery proxy - ale takie informacje o proxy powinny pojawić się podczas instalacji i

pierwszego uruchomienia oprogramowania, a nie nagle po kliknięciu wątpliwego łącza lub pobraniu programu z mniej wiarygodnego źródła.

Niektóre programy (lub aplikacje) przestają działać poprawnie

Jeśli aplikacje, o których wiesz, że działały poprawnie na Twoim urządzeniu, nagle przestają działać zgodnie z oczekiwaniami, możesz napotkać symptomy proxy lub złośliwego oprogramowania zakłócającego działanie aplikacji. Oczywiście, jeśli taki problem pojawi się natychmiast po wykonaniu aktualizacji systemu operacyjnego, aktualizacja jest znacznie bardziej prawdopodobnym źródłem problemu niż coś bardziej złowrogiego.

Programy zabezpieczające zostały wyłączone

Jeśli oprogramowanie zabezpieczające, które normalnie uruchamiasz na swoim urządzeniu, zostało nagle wyłączone, usunięte lub skonfigurowane tak, aby ignorować pewne problemy, może to oznaczać, że haker przeniknął do Twojego urządzenia i wyłączył jego zabezpieczenia, aby uniemożliwić jego lub jej wysiłki. przed zablokowaniem, a także zapewnić, że nie otrzymasz ostrzeżeń, gdy wykonuje różne dodatkowe nikczemne czynności.

Zwiększone wykorzystanie danych lub wiadomości tekstowych (SMS)

Jeśli monitorujesz wykorzystanie danych lub SMS-ów na swoim smartfonie i widzisz większe wartości wykorzystania, niż się spodziewasz, zwłaszcza jeśli wzrost ten zaczyna się zaraz po podejrzanym zdarzeniu, może to oznaczać, że złośliwe oprogramowanie przesyła dane z Twojego urządzenia do innych stron. Możesz nawet sprawdzić wykorzystanie danych na aplikację - jeśli jeden z nich wygląda tak, jakby używa zbyt dużej ilości danych w stosunku do funkcji, które zapewnia, coś może być nie tak. Jeśli zainstalowałeś aplikację z zewnętrznego sklepu z aplikacjami, możesz spróbować usunąć aplikację i zainstalować ją ponownie z bardziej zaufanego źródła. Pamiętaj jednak, że jeśli na urządzeniu znajduje się złośliwe oprogramowanie, ponowna instalacja aplikacji może nie zawsze rozwiązać problem, nawet jeśli była ona oryginalnym źródłem infekcji.

Zwiększony ruch sieciowy

Jeśli monitorujesz wykorzystanie sieci Wi-Fi lub przewodowej na swoim urządzeniu i widzisz wyższy poziom aktywności, niż się spodziewasz, zwłaszcza jeśli wzrost ten zaczyna się zaraz po podejrzanym zdarzeniu, może to oznaczać, że złośliwe oprogramowanie przesyła dane z Twojego urządzenia do innych podmiotów. W niektórych systemach możesz nawet sprawdzić wykorzystanie danych na aplikację - jeśli co najmniej jedna aplikacja wygląda tak, jakby zużywała zbyt dużo danych w stosunku do funkcji, którą zapewniają, coś może być nie tak. Jeśli zainstalowałeś aplikację z mniej niż wiarygodnego źródła, możesz spróbować usunąć aplikację i zainstalować ją ponownie z bardziej zaufanego źródła - ale jeśli na urządzeniu jest obecne złośliwe oprogramowanie, ponowne zainstalowanie aplikacji, którą przyniosło na urządzenie, może nie zawsze rozwiązać problem, nawet jeśli aplikacja była w rzeczywistości pierwotnym źródłem infekcji. Możesz sprawdzić, ile danych wykorzystuje Twój komputer - a nawet ile zużywa każdy program - instalując program monitorujący przepustowość na danym urządzeniu.

Niezwykłe otwarte porty

Komputery i inne urządzenia połączone z Internetem komunikują się za pomocą portów wirtualnych. Komunikacja dla różnych aplikacji zazwyczaj dociera do urządzenia przez różne porty. Porty są ponumerowane, a większość numerów portów powinna być zawsze zamknięta - to znaczy nie są skonfigurowane tak, aby zezwalały na komunikację. Jeśli porty, które nie są normalnie otwarte w

komputerze, nagle się otworzą i nie zainstalowałeś tylko oprogramowania, które może korzystać z takich portów, zwykle wskazuje na problem. Jeśli używasz systemu Windows - zwłaszcza jeśli trochę rozumiesz na temat sieci - możesz użyć wbudowanego polecenia netstat, aby określić, które porty są otwarte i co łączy się z twoim urządzeniem.

Twoje urządzenie zaczyna się zawieszać

Jeśli Twój komputer, tablet lub smartfon nagle zaczyna się zawieszać znacznie częściej niż w przeszłości, może być na nim uruchomione złośliwe oprogramowanie. Oczywiście, jeśli właśnie zaktualizowałeś system operacyjny, jest to prawdopodobne źródło problemu. Jeśli regularnie widzisz ekrany, takie jak niebieski ekran śmierci - lub inne ekrany wskazujące, że w komputerze wystąpił krytyczny błąd i należy go ponownie uruchomić, masz problem. Może to mieć charakter techniczny lub może wynikać z uszkodzenia spowodowanego przez złośliwe oprogramowanie lub hakera.

Twój rachunek za telefon komórkowy zawiera nieoczekiwane opłaty

Wiadomo, że przestępcy wykorzystywali zainfekowane smartfony do wykonywania drogich zagranicznych połączeń telefonicznych w imieniu strony zdalnej korzystającej z urządzenia. Podobnie, mogą używać urządzenia, które zostało naruszone, do wysyłania wiadomości SMS na numery międzynarodowe i mogą pobierać różne inne opłaty telefoniczne w inny sposób.

Nieznane programy żądają dostępu

Większość oprogramowania zabezpieczającego dla komputerów ostrzega użytkowników, gdy program po raz pierwszy próbuje uzyskać dostęp do Internetu. Jeśli otrzymujesz takie ostrzeżenia i nie rozpoznajesz programu, który szuka dostępu, lub rozpoznajesz program, ale nie możesz zrozumieć, dlaczego miałby on uzyskać dostęp do Internetu (na przykład Kalkulator Windows lub Notatnik), coś może być nie tak .

Urządzenia zewnętrzne nieoczekiwanie włączają się

Jeśli co najmniej jedno z zewnętrznych urządzeń wejściowych (w tym urządzenia takie jak kamery, skanery i mikrofony) włącza się w nieoczekiwanym momencie (na przykład gdy ich nie używasz), może to oznaczać, że złośliwe oprogramowanie lub haker jest komunikowanie się z nimi lub korzystanie z nich w inny sposób. Istnieją ataki, o których wiadomo, że przestępcy zdalnie włączają kamery i szpiegują ludzi.

Twoje urządzenie zachowuje się tak, jakby używał go ktoś inny

Złośliwi aktorzy czasami przejmują kontrolę nad komputerami i używają ich przez zdalny dostęp, prawie tak, jakby siedzieli przed klawiaturą urządzenia. Jeśli zauważysz, że Twoje urządzenie zachowuje się tak, jakby ktoś inny sprawował kontrolę - na przykład, widzisz, że wskaźnik myszy porusza się lub są wprowadzane klawisze, gdy nie używasz myszy lub klawiatury - może to oznaczać, że ktoś inny kontroluje maszyna.

Nowa wyszukiwarka przeglądarki jako domyślna

W ramach kilku technik ataków hakerzy zmieniają domyślną wyszukiwarkę używaną przez osoby przeglądające sieć. Jeśli domyślna wyszukiwarka Twojej przeglądarki zmieniła się i Ty jej nie zmieniłeś, coś może być nie tak.

Hasło Twojego urządzenia uległo zmianie

Jeśli hasło do telefonu, tabletu lub komputera uległo zmianie bez zmiany hasła, coś jest nie tak, a przyczyna jest prawdopodobnie poważna.

Pojawiają się wyskakujące okienka

Różne odmiany złośliwego oprogramowania tworzą wyskakujące okienka z prośbą o wykonanie różnych czynności. Uważaj, jeśli widzisz wyskakujące okienka. Takie złośliwe oprogramowanie jest powszechne na laptopach, ale istnieje również w przypadku niektórych smartfonów. Pamiętaj, że wyskakujące okienka, które pojawiają się, gdy nie korzystasz z internetu to duża czerwona flaga, podobnie jak wyskakujące okienka z zaleceniami dotyczącymi pobierania i instalowania „oprogramowania zabezpieczającego" lub odwiedzania witryn o wątpliwej reputacji.

Pojawiają się nowe dodatki do przeglądarki

Powinien zostać wyświetlony monit przed zainstalowaniem jakiegokolwiek dodatku do przeglądarki. Jeśli nowy dodatek zostanie zainstalowany bez Twojej wiedzy, prawdopodobnie oznacza to problem. Niektóre złośliwe oprogramowanie są dostarczane w zatrutych wersjach różnych pasków narzędzi przeglądarki.

Nowa strona główna przeglądarki

W ramach kilku technik ataków hakerzy zmieniają strony główne przeglądarek użytkowników. Jeśli strona główna Twojej przeglądarki uległa zmianie i nie zmieniłeś jej, coś może być nie tak.

Twoja poczta e-mail z urządzenia jest blokowana przez filtry spamu.

Jeśli wiadomość e-mail, którą wysyłasz z danego urządzenia, mogła bez problemu dotrzeć do zamierzonych odbiorców, ale nagle została zablokowana przez filtry spamu, może to oznaczać, że ktoś lub coś zmieniło konfigurację poczty e-mail w celu przekazywania wiadomości przez jakiś serwer, który pozwala mu czytać, blokować, a nawet modyfikować twoje wiadomości i które inne systemy bezpieczeństwa są oznaczone jako problematyczne.

Twoje urządzenie próbuje uzyskać dostęp do „złych" witryn.

Jeśli używasz komputera, tabletu lub smartfona w sieci, która blokuje dostęp do znanych problematycznych witryn i sieci (wiele firm, organizacji i instytucji rządowych korzysta z takiej technologii zarówno w swoich sieciach wewnętrznych, jak i w sieciach typu „przynieś własne urządzenie" [BYOD]) i dowiesz się, że Twoje urządzenie próbowało uzyskać dostęp do takich witryn bez Twojej wiedzy, że Twoje urządzenie próbowało uzyskać dostęp do takich witryn bez Twojej wiedzy, prawdopodobnie Twoje urządzenie zostało przejęte.

Doświadczasz nietypowych przerw w świadczeniu usług

Jeśli wydaje Ci się, że Twój smartfon nagle przerywa połączenia lub jeśli nie jest on w stanie wykonywać połączeń, gdy wydaje się, że masz dobrą siłę sygnału, lub słyszysz dziwne dźwięki podczas rozmów telefonicznych, coś może być nie tak. Należy pamiętać, że w większości przypadków objawy te dotyczą problemów technicznych niezwiązanych z naruszeniem. Jednak w niektórych przypadkach przyczyną takich dolegliwości jest naruszenie. Tak więc, jeśli zauważyłeś istotne objawy wkrótce po podjęciu działania, które teraz kwestionujesz lub żałujesz, możesz rozważyć, czy musisz podjąć działania naprawcze

Zmieniły się ustawienia języka na Twoim urządzeniu

Ludzie rzadko później zmieniają ustawienia językowe na swoich komputerach

wykonanie procedury konfiguracji początkowej, a kilka pakietów oprogramowania to robi. Tak więc, jeśli komputer nagle wyświetla menu i / lub monity w obcym języku lub nawet ma zainstalowany język, którego nigdy nie instalowałeś, coś jest nie tak.

Widzisz niewyjaśnioną aktywność na urządzeniu

Jeśli na swoim urządzeniu widzisz wiadomości e-mail w folderze Wysłane, których nie wysłałeś, prawdopodobnie ktoś włamał się na Twoje urządzenie lub konto e-mail. Podobnie, jeśli pliki, co do których masz pewność, że nigdy nie pobrałeś, pojawiają się w folderze Pobrane, ktoś inny mógł je pobrać na Twoje urządzenie.

Widzisz niewyjaśnioną aktywność online

Jeśli Twoje konto w mediach społecznościowych zawiera posty w mediach społecznościowych, co do których masz pewność, że nie stworzyłeś ani Ty, ani żadna aplikacja, na którą masz autoryzację, coś jest ewidentnie nie tak. Możliwe, że ktoś włamał się na Twoje konto, a wszystkie Twoje urządzenia są bezpieczne, lub jedno z Twoich urządzeń z dostępem do konta zostało naruszone i stało się kanałem nieautoryzowanego dostępu do Twojego konta. To samo dotyczy sytuacji, gdy zobaczysz filmy, których nigdy nie zamówiłeś. Twoje poprzednie wypożyczenia usługi strumieniowego przesyłania wideo, zakupy, które Ty kupiłeś nigdy nie pojawiały się w historii zamówień w sklepie internetowym i tak dalej.

Twoje urządzenie nagle uruchamia się ponownie

Chociaż ponowne uruchomienia są integralną częścią wielu aktualizacji systemu operacyjnego, nie powinny nastąpić nagle poza kontekstem takich aktualizacji. Jeśli Twoje urządzenie regularnie uruchamia się ponownie bez Twojej zgody, coś jest nie tak. Pytanie tylko, czy problem wynika z naruszenia bezpieczeństwa, czy z innego problemu.

Widzisz oznaki naruszenia danych i / lub wycieków

Oczywiście, jeśli wiesz, że część Twoich danych wyciekła, powinieneś spróbować ustalić źródło problemu - a proces sprawdzania oczywiście obejmuje sprawdzenie oznak problemów na wszystkich smartfonach, tabletach i komputerach.

Nastąpiło przekierowanie do niewłaściwej witryny internetowej

Jeśli masz pewność, że wpisałeś poprawny adres URL, ale nadal zostałeś przekierowany do niewłaściwej witryny, coś jest nie tak. Problem może odzwierciedlać naruszenie bezpieczeństwa w innym miejscu, ale może oznaczać, że ktoś włamał się również na Twoje urządzenie. Jeśli błędne przekierowanie występuje tylko z jednego lub większej liczby określonych urządzeń, ale nie z innych w tej samej sieci, istnieje prawdopodobieństwo, że dane urządzenia zostały naruszone. W każdym razie nigdy nie wykonuj żadnych wrażliwych zadań (takich jak logowanie do witryny internetowej) z urządzenia, które kieruje Cię nieprawidłowo.

Wygląda na to, że światło twojego dysku twardego nigdy się nie wyłącza

Jeśli lampka dysku twardego świeci się stale lub prawie stale, złośliwe oprogramowanie może coś robić z dyskiem. Oczywiście, kontrolki dysku twardego zapalają się z uzasadnionych powodów, gdy nie korzystasz aktywnie z komputera - a czasami uzasadniony powód spowoduje, że światło będzie włączone przez dłuższy czas - więc nie panikuj, jeśli to jedyny znak, że coś jest źle.

Zdarzają się inne nienormalne rzeczy

Nie można wymienić wszystkich możliwych symptomów, które złośliwe oprogramowanie może wywołać na urządzeniu. Tak więc, jeśli pamiętasz, że strony próbują włamać się do Twoich systemów i że nietypowe zachowanie Twojego urządzenia może być oznaką problemów, zwiększasz swoje szanse na zauważenie, że coś wydaje się być nie tak i na właściwe zareagowanie na naruszenie jeśli tak się dzieje, w rzeczywistości.