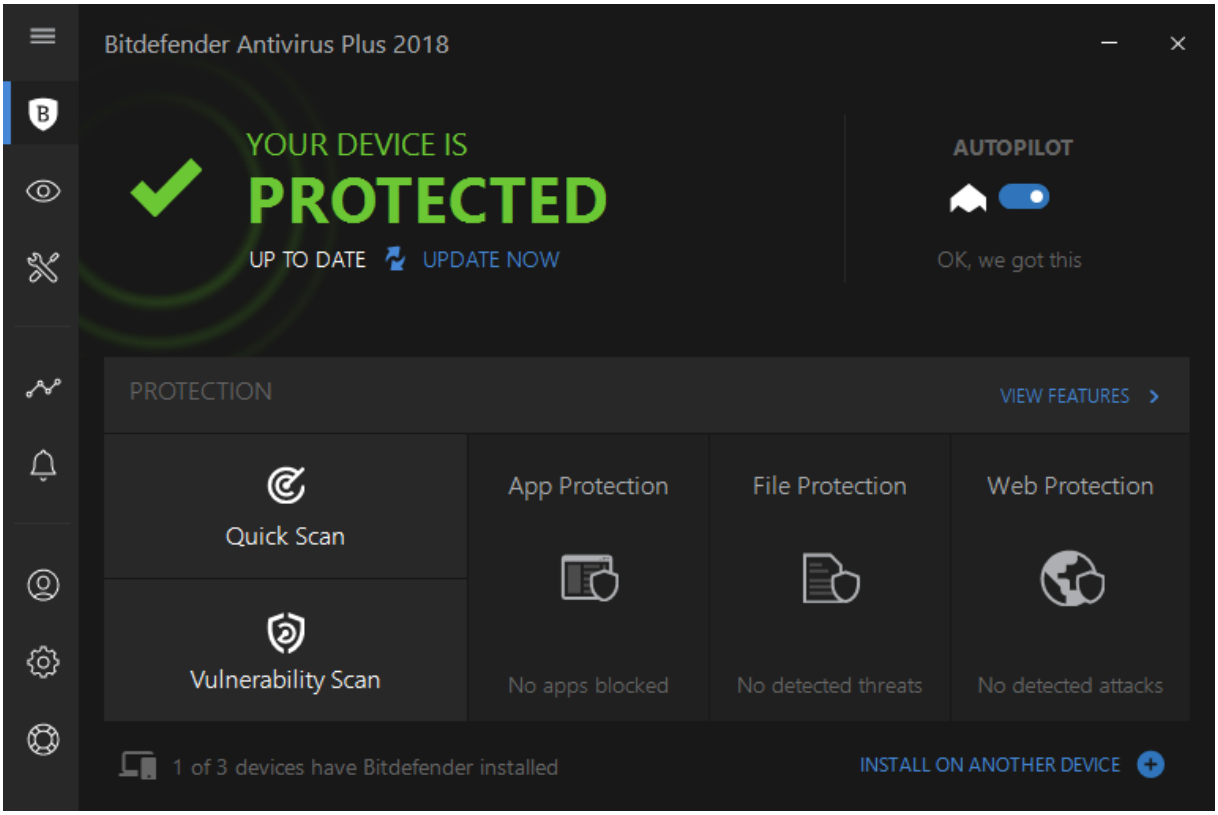
Granica dzieląca proste narzędzie antywirusowe od pełnego pakietu zabezpieczeń nie zawsze jest jasna. Weźmy na ten przykład Bitdefender Antivirus Plus. Oprócz każdej funkcji, której można oczekiwać w programie antywirusowym, zawiera menedżer haseł, zabezpieczoną przeglądarkę, bezpieczne narzędzie do usuwania, skanowanie w poszukiwaniu luk w zabezpieczeniach systemu, ochronę przed atakami ransomware i inne. Nie oferuje jednak zapór, filtrowania spamu, ani kontroli rodzicielskiej. **Jest to program antywirusowy z wieloma zaletami i pozostaje dobrym wyborem, jeśli szukasz ochrony przed złośliwym oprogramowaniem.**

Instalacja i wygląd

Podobnie jak w przypadku wielu nowoczesnych narzędzi zabezpieczających, instalacja Bitdefender wymaga konta online. Wystarczy zalogować się do Bitdefender Central, wprowadzić klucz produktu i pobrać antywirusa. Nic prostszego. Podczas procesu instalacji uruchamia się szybkie skanowanie w poszukiwaniu aktywnego oprogramowania.

Wygląd produktu nie zmienił się znacząco od poprzedniej edycji. Wciąż zawiera głównie biały tekst na ciemnoszarym tle. Menu po lewej stronie zapewnia dostęp do funkcji: ochrona, prywatność, narzędzia, aktywność, powiadomienia, konto, ustawienia i obsługa techniczna. Na panelu stanu wyświetlane jest czerwone ostrzeżenie, jeśli ustawienia konfiguracji powodują zagrożenia systemu. Włączenie systemu z powrotem w tryb Autopilota powinno rozwiązać taki problem. Jeśli pozostawisz włączony Autopilot, zawsze powinieneś zobaczyć na liście statusu „Chroniony” na zielono.

Autopilot od kilku lat jest podstawą Bitdefendera. W tym trybie program antywirusowy zajmuje się działalnością z absolutnym minimum zamieszania i wpływu na użytkowanie sprzętu. Usuwa złośliwe oprogramowanie. Aktualizuje się w razie potrzeby. Jeśli chce się z tobą komunikować, wyświetli numer w ikonie Powiadomienia.



Możesz kliknąć karty Zabezpieczenia i prywatność, aby wyświetlić szczegóły funkcji. W zakładce Funkcje ochrony zobaczysz, że zapora i ochrona antyspamowa wymagają uaktualnienia. W obszarze Funkcje prywatności, szyfrowanie plików, ochrona kamery internetowej i doradca rodzicielski także zobaczysz ukatualnienia. Strona Narzędzia jest ponadto wypełniona w całości funkcjami, które są obecne tylko w najnowocześniejszym zestawie Bitdefender.

Fantastyczne wyniki badań laboratoryjnych

Każde z niezależnych laboratoriów testujących antywirusy ma własne podejście do testowania i oceniania produktów antywirusowych. Im więcej laboratoriów, które wykorzystują produkt do testów, tym dokładniejszy obraz można uzyskać, patrząc na wszystkie ich wyniki. Podążamy za pięcioma laboratoriami, a wszystkie pięć z nich testowało Bitdefender.

SE Labs próbuje naśladować rzeczywiste sytuacje w jak najwierniejszym zakresie testowania, przechwytując prawdziwe złośliwe witryny i używając systemu odtwarzania, aby trafić do każdego produktu dokładnie tym samym atakiem. Laboratorium oferuje certyfikację na pięciu poziomach: AAA, AA, A, B i C. Bitdefender otrzymał najwyższą certyfikację, AAA, a także kilka innych.

Z wielu testów przeprowadzanych regularnie przez AV-Comparatives śledzimy wyniki czterech. Laboratorium certyfikuje produkt na poziomie standardowym pod warunkiem, że osiąga ocenę przechodzącą. Te, które wychodzą lepiej lub znacznie lepiej, mogą uzyskać certyfikat na poziomie zaawansowanym. Z czterech testów Bitdefender zdobył cztery oceny Advanced +.

Większość testów przedstawia wynik liczbowy lub poziom oceny. Testy przeprowadzone przez MRG-Effitas tak nie robią. Produkt albo wychodzi z testu obronną ręką, albo ponosi porażkę. Bitdefender zdał test bankowy w zakresie złośliwego oprogramowania. W ogólnym testowaniu złośliwego oprogramowania uzyskał certyfikat poziomu 2, co oznacza, że chociaż nie zapobiega całkowicie atakom na złośliwe oprogramowanie, to jednak naprawił wszystkie skutki ataków w ciągu 24 godzin.

Wyniki badań laboratoryjnych

Testerzy w AV-Test Institute wprowadzając produkt antywirusowy do testów, oceniają go w trzech obszarach: Ochrona, wydajność i użyteczność. Ta ostatnia kategoria oznacza otrzymywanie fałszywych alarmów (dobre programy lub witryny uznane za złe) w stopniu minimalnym. W każdej kategorii do uzyskania jest sześć punktów, co daje łączną liczbę 18. Bitdefender osiągnął prawie najwyższy wynik, ale 5,5 punktów za użyteczność przyniosło końcowy wynik na poziomie 17,5.

Virus Bulletin regularnie publikuje wyniki z testu RAP (Reactive And Proactive). Wynik Bitdefendera jest znacznie powyżej obecnej średniej.

Aby uzyskać ten łączny wynik, używamy formuły, która porównuje wyniki każdego laboratorium w skali od 0 do 10, a następnie je łączy. Łączny wynik Bitdefender wynosi 9,8. Żaden inny produkt testowany przez wszystkie laboratoria nie uzyskał wyższego wyniku!

Testy ochrony przed malware

Dzięki tak dokładnym raportom z laboratoriów, moje własne testy nie są tak istotne. Nadal je prowadzę, aby zrozumieć, jak działa każdy produkt.

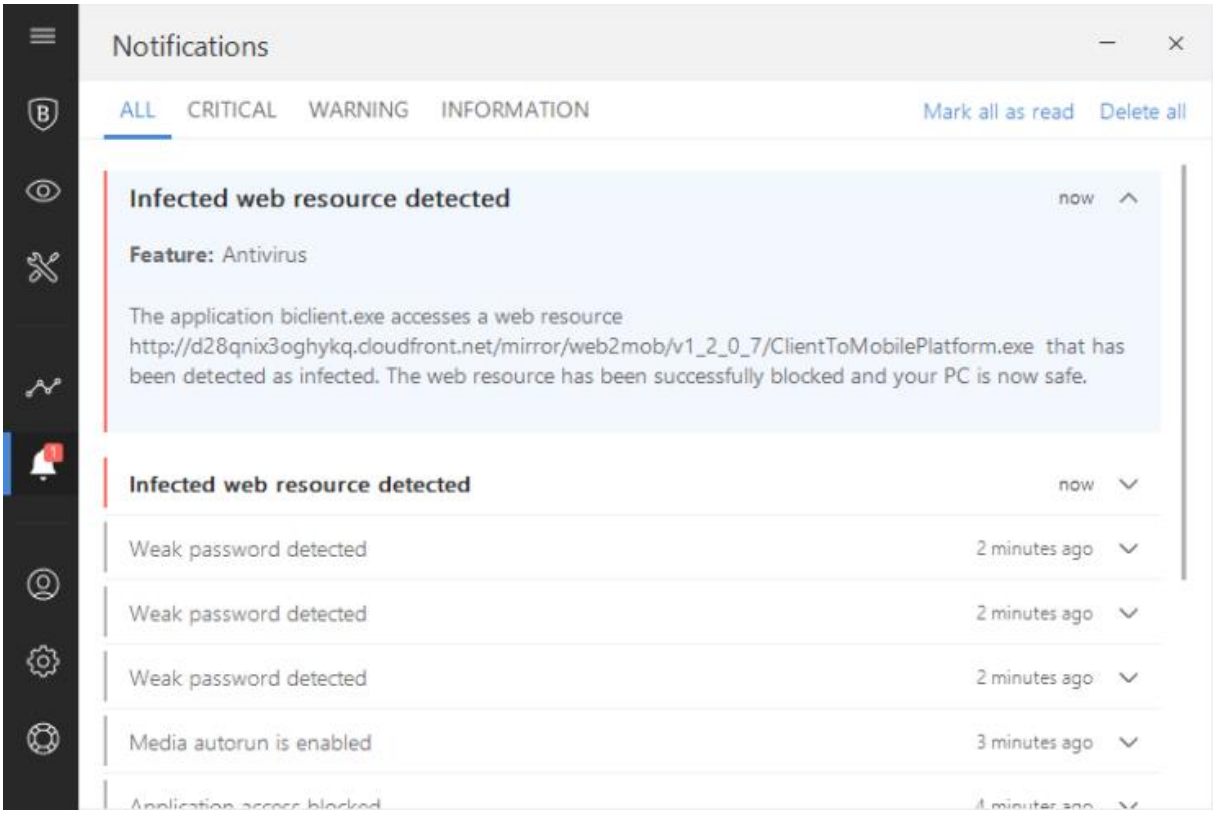
Test ochrony przed złośliwym oprogramowaniem rozpoczyna się po otwarciu folderu zawierającego bieżący zestaw próbek. Bitdefender natychmiast zaczął przeglądać próbki, sprawdzając, czy nie są rozpoznawalne, ale jego zachowanie nie było wcale oczywiste. Działając w trybie Autopilot, po cichu eliminuje znane zagrożenia. Jedyną oznaką jego aktywności była stale malejąca liczba plików zgłoszonych przez Eksploratora Windows.

Kiedy numery przestały się kłócić, sprawdziłem, ile próbek pozostało. Bitdefender wyeliminował 54 procent z nich.

Aby kontynuować test, uruchomiłem każdą z pozostałych próbek. Funkcja Bezpieczne pliki (więcej o tym poniżej) zablokowała kilka plików, ale nie aktywnie identyfikowała ich jako złośliwego oprogramowania, dlatego nie liczyło się to się jako skuteczna detekcja. Kilka innych przeszło, a niektóre, które wykryto, nadal były umieszczane w systemie testowym plików zawierających złośliwe oprogramowanie. Jego całkowity wskaźnik wykrywalności to 75 procent i ocena 7.1 punktu. Zauważyłem, że wszystkie pominięte próbki trafiły do kategorii o niższym ryzyku.

Wyniki ochrony przed złośliwym oprogramowaniem

Ręcznie analizuję wszystkie próbki w mojej kolekcji, aby móc dokładnie określić, jak każdy antywirus blokuje instalację. Ta analiza jest dość długim procesem i w rezultacie używam tego samego zestawu próbek przez wiele miesięcy. Z drugiej strony, mój test ochrony przed złośliwymi adresami URL, zawsze korzysta z najnowszego złośliwego oprogramowania. W tym teście Bitdefender wypada znacznie lepiej.



Zaczynamy od kanału najnowszych odkryć dotyczących niebezpiecznych adresów URL z MRG-Effitas. Uruchamiając każdą z kolei, biorę pod uwagę, jak działa antywirus. Daję równe prawo do blokowania wszystkich dostępu do adresu URL i usunięcia szkodliwego oprogramowania podczas pobierania. I dalej, dopóki nie mam danych dla 100 prawidłowych adresów URL zawierających złośliwe oprogramowanie.

Bitdefender zablokował 80 procent próbek na poziomie adresu URL, w wielu przypadkach identyfikując zagrożenie w witrynie na podstawie nazwy. W trakcie pobierania wyrzucił kolejne 11 procent, a całkowita stopa ochrony wynosiła 91 procent, co jest dobrym rezultatem.

Niesamowita ochrona przed phishingiem

Ochrona przed szkodliwym adresem URL Bitdefender odbywa się na poziomie sieci, bez potrzeby instalowania wtyczki przeglądarki. W moich wcześniejszych testach zauważyłem, że blokuje połączenia internetowe za pomocą próbek złośliwego oprogramowania. Mimo, że ta funkcja nie sprawdziła się w dostępie do adresów URL zawierających złośliwe oprogramowanie, to wypadła lepiej przeciwko witrynom wyłudzania informacji - fałszywym witrynom, które próbują kraść dane.

W tym teście przeszukuję internet, szukając w szczególności tych najnowszych oszustw, by zostały przeanalizowane. Strony wyłudzające informacje są ulotne; Jak tylko któraś zostanie zamknięta, to oszust założy nową. Najlepsze narzędzia antywirusowe analizują strony w czasie rzeczywistym, nie tylko polegając na czarnych listach.

Wyniki o zabezpieczeniach przed wyłudzaniem informacji

Fałszywe triki i trendy zmieniają się nieustannie, więc zamiast raportować wskaźnik wykrywania w tym teście, porównuję wskaźnik wykrycia produktu z szybkością wykrywacza phishingu Norton, a także z ochroną przed phishingiem wbudowanym w Chrome, Firefox i Internet Explorer. Niewiele produktów pokonało Norton, a wiele nie potrafiło poradzić sobie lepiej niż ochrona wbudowana w przeglądarce.

Poprzednio Bitdefender uzyskał najlepszy wynik w tym teście, pokonując wskaźnik wykrywania Nortona o 5 procent. Tym razem przewyższył Norton, z szybkością wykrywania w pełni o 12 procent wyższą. Jest to w części ze względu na całkowity spadek, jaki ostatnio obserwowałem w wykrywaniu oszustw firmy Norton. Ale to wciąż imponujące. Oczywiście, Bitdefender pomyślnie pokonał wszystkie trzy przeglądarki.

Wyniki wyszukiwania Markup

Nawet nie musisz odwiedzać strony, aby uzyskać ochronę dzięki analizie TrafficLight firmy Bitdefender. TrafficLight oznacza wyniki wyszukiwania jako bezpieczne lub niebezpieczne, korzystając z oczekujących zielonych i czerwonych ikon. Ale to nie wszystko.

Jeśli napotkasz czerwoną ikonę ostrzeżenia, możesz ją kliknąć, aby uzyskać szczegółowe informacje. Phishing i malware są oczywiście na samej górze listy. Wśród innych typów oszustw oznaczonych przez TrafficLight są witryny piractwa, oszustwa związane z zatrudnianiem i witryny z fałszywymi przekierowaniami.

Wiele opcji skanowania

Bitdefender oferuje szybkie skanowanie złośliwego oprogramowania na swojej stronie głównej. Na stronie z funkcjami ochrony można zamiast tego wybrać pełne skanowanie systemu. Szybkie skanowanie mojego standardowego, czystego testowego systemu zakończyło się w niecałą minutą, ale pełne skanowanie trwało 1 godzinę i 15 minut, przewyższając obecnie średnią 45 minut. Pełne skanowanie zostało zakończone w 38 minut, co sugeruje, że Bitdefender używa pierwszego skanowania, aby zoptymalizować kolejne skanowania.

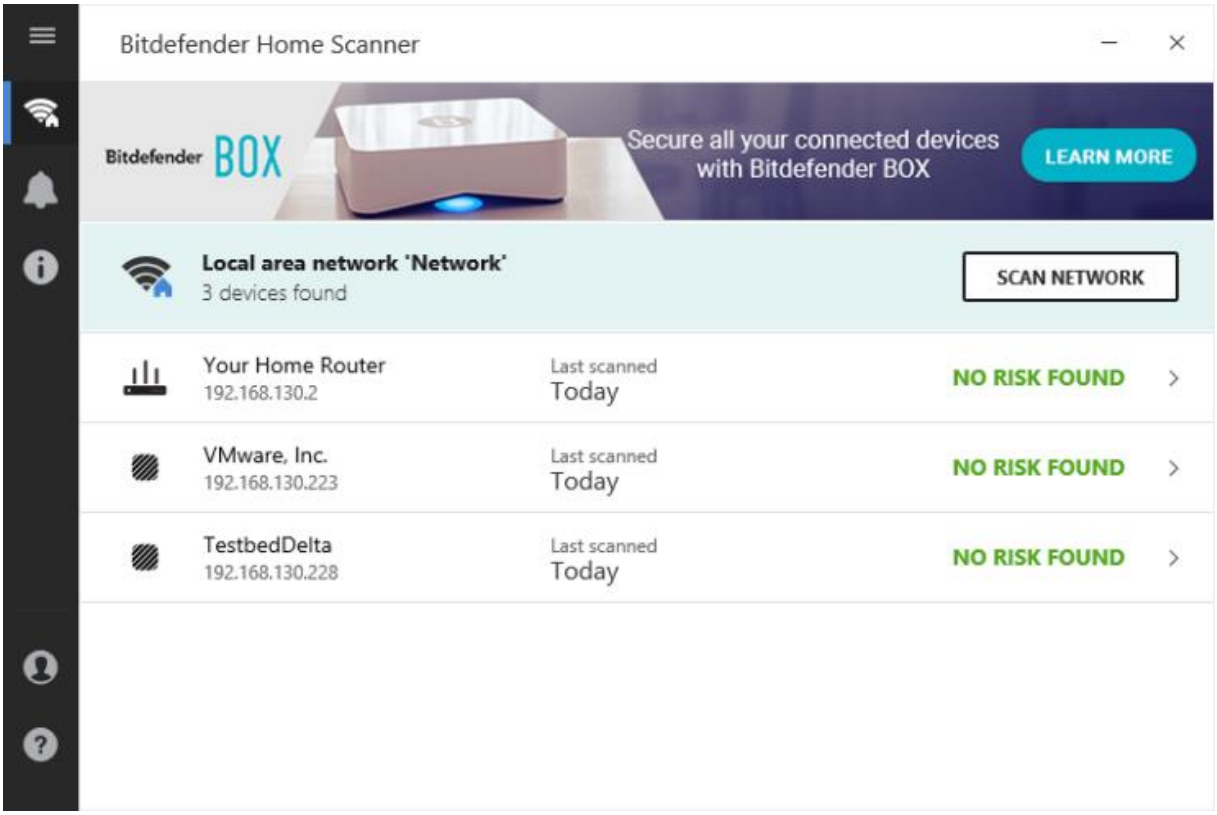
Jeśli uruchomisz złośliwe oprogramowanie, które jest odporne na zwykłe skanowanie, nie powodując całkowitego wyłączenia systemu, tryb ratunkowy Bitdefender może cię uratować. Nie trzeba pobierać obrazu ISO, nagrać dysku ratunkowego ani wykonywać innych rzeczy. Wystarczy wybrać tryb ratunkowy i pozwolić, aby Bitdefender uruchomił się ponownie w alternatywnym systemie operacyjnym, w którym szkodliwe oprogramowanie z systemem Windows jest bezbronne wobec oporu przed skanerem antywirusowym.

Klikając Zarządzaj skanami, możesz tworzyć własne skanowanie niestandardowe lub ustawić harmonogram skanowania. Można zaplanować skanowanie do uruchomienia przy starcie systemu lub w określonym przez użytkownika odstępie dni, tygodni lub miesięcy.

Bitdefender skanuje również system w poszukiwaniu luk w zabezpieczeniach. Obejmuje to brak poprawek zabezpieczeń ważnych aplikacji i komponentów systemu, podobnie jak w McAfee AntiVirus Plus i Avast. Jednak podobnie jak Kaspersky, Bitdefender wykracza poza to, sprawdzając system w zakresie problemów z konfiguracją zabezpieczeń. W moim systemie testowym zgłoszono nieaktualną instalację Firefoksa i kilka słabych haseł.

Doradca Wi-Fi i skaner domowy

Bitdefender zawiera doradcę Ochrony Wi-Fi, który sprawdza lokalną sieć bezprzewodową w przypadku problemów z bezpieczeństwem. Ponieważ moje systemy testowania maszyn wirtualnych nie mają Wi-Fi, nie widziałem tej funkcji w akcji. Zgodnie z dokumentacją po prostu wywołuje ostrzeżenie, gdy połączysz się z niebezpiecznym punktem dostępu Wi-Fi.



Początkowo miałem wrażenie, że to instalacja automatycznego skanera antywirusowego Bitdefender Home Scanner. Jak się okazuje, instalacja ta nastąpiła tylko dlatego, że moje konto Bitdefender Central zawiera już skaner domowy. Gorąco polecam skorzystać z tego bezpłatnego narzędzia. W skrócie: wymienia wszystkie urządzenia w sieci, w tym komputery, urządzenia przenośne i urządzenia Internetu Rzeczy. Oznacza, że są one potencjalnie podatne na ataki. I oferuje porady dotyczące radzenia sobie z tymi lukami.

Wbudowana ochrona przed Ransomware

Uderzenie ransomware może zepsuć Ci cały dzień - lub nawet całą firmę. Istnieje wiele podejść do ochrony przed ransomware, od śledzenia zachowania specyficznego dla ransomware po to, aby zapobiec nieautoryzowanemu modyfikowaniu ważnych plików. Funkcja Bezpieczne pliki Bitdefender okazała się skuteczna w testowaniu.

Domyślnie funkcja chroni pliki w folderze Dokumenty, Zdjęcia, Wideo i Pulpit, ale można dodać inne foldery zawierające ważne dokumenty. Bezpieczne pliki zezwalają na dostęp za pośrednictwem znanych, zaufanych programów, ale jeśli nieznany proces próbuje modyfikować lub tworzyć pliki w chronionym miejscu, Bitdefender blokuje go i wyświetla powiadomienie. Jeśli nieznany plik jest niezbyt znanym edytorem tekstowym, który został zainstalowany samodzielnie, można powiedzieć, że plik jest na tyle bezpieczny, aby dodać go do zaufanej listy. Jeśli jednak nie zrobiłeś nic, aby wywołać takie powiadomienie, zdecydowanie pozwól, aby Bitdefender blokował dostęp.

Aby przetestować tę funkcję, zacząłem używać niezwykle prostego programu do szyfrowania plików, który sam kodowałem. Jak obiecano, Bitdefender zablokował dostęp. Zablokował także mój ręczny kodowany edytor niewielkich rozmiarów. W celach testowych wyłączyłem ochronę w czasie rzeczywistym, a także wyłączyłem system ochrony przed zagrożeniami związanymi z zachowaniem.

Po izolacji systemu testowego, aby zapobiec jakiejkolwiek ewakuacji ransomware, uruchomiłem pół

tuzina próbek. W każdym przypadku Bitdefender wykrył i zablokował atak. Kilka z nich zademonstrowało swoje żądania okupu, twierdząc, że zaszyfrowały moje pliki, ale było to kłamstwo.

Próbowałem również uruchomić symulator KnowBe4's RanSim. Bezpieczne pliki blokowały wielokrotnie dostęp, ale ta aktywność zakłóciła symulację w stopniu wystarczającym do awarii procesów roboczych programu. W rzeczywistej sytuacji nie narzekam na ochronę antywirusową, która spowodowała awarię procesów ataku. Ogólnie rzecz biorąc, bezpieczne pliki okazały się bardzo skuteczne.

Portfel do ochrony haseł

Zarządzanie hasłami jest cechą bardziej powszechnie spotykaną w pakietach zabezpieczeń niż w autonomicznych produktach antywirusowych. Funkcja Portfel w Bitdefender zawiera hasła, dane osobowe i dane karty kredytowej do użytku na stronach internetowych, a także zapisuje hasła do aplikacji i sieci Wi-Fi.

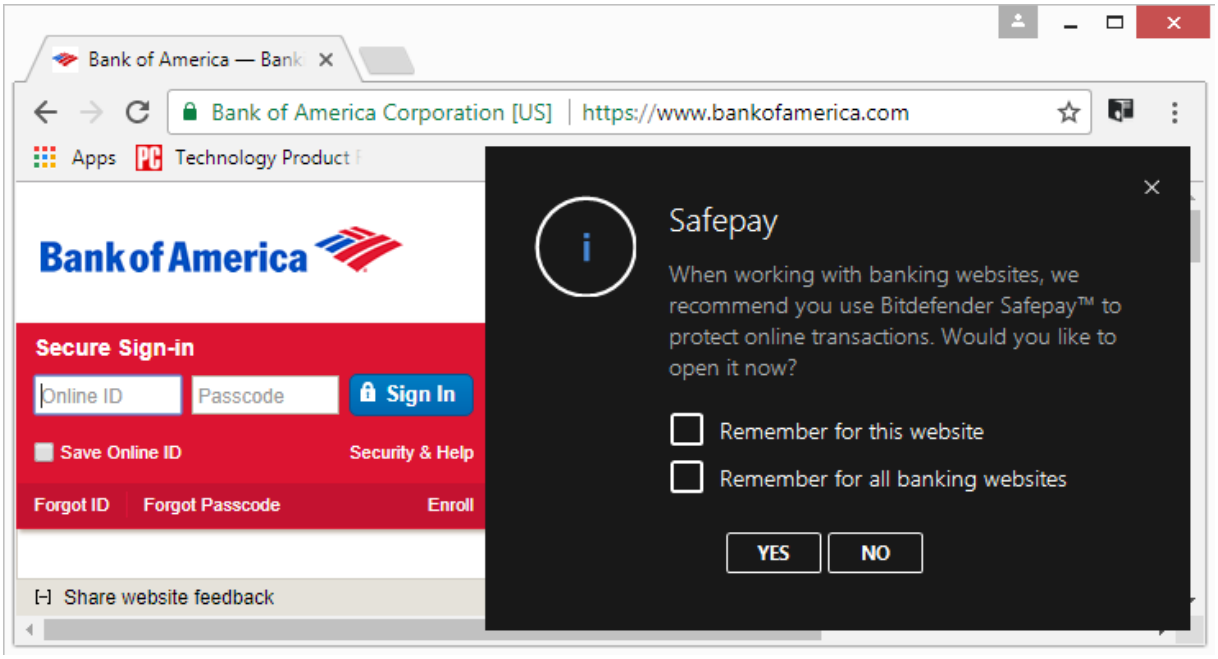
Portfel zmienił się bardzo niewiele od poprzedniej edycji Bitdefendera, poza faceliftem interfejsu użytkownika. Nadal wymaga silnego hasła głównego, oddzielonego od hasła Bitdefender Central. Nadal pozwala na tworzenie wielu portfeli, być może oddzielnych dla haseł domowych i służbowych. Automatycznie rejestruje poświadczenia logowania podczas ich wpisywania i powtarza je w razie potrzeby.

Podczas rejestrowania nowego konta, można użyć generatora haseł Portfela, który domyślnie tworzy 15-znakowe hasła z liter i cyfr.

Zabezpieczenie transakcji finansowych

Program Safepay firmy Bitdefender automatycznie uruchamia się, gdy wykryje, że masz zamiar połączyć się z witryną bankową lub inną wrażliwą witryną, oferując bezpieczne połączenie. Możesz zawsze używać Safepay w danej witrynie lub w każdej witrynie banku.

Safepay jest pulpitem własnym, z wbudowaną grafiką. Procesy uruchomione na pulpicie programu Safepay nie mają połączenia ze zwykłym komputerem stacjonarnym. Przeglądarka Safepay obsługuje Portfel, oczywiście, w razie potrzeby można zainstalować program Flash, ale żadne inne rozszerzenia nie są obsługiwane.



Oddzielenie procesu przeglądarki Safepay powinno chronić przed keyloggerem lub innymi programami szpiegującymi. Idąc dalej, klawiatura wirtualna służy do pokonania nawet najsilniejszych keyloggerów. Uniemożliwia to również programom przechwytywanie zrzutów ekranu w celu kradzieży poufnych informacji.

Niszczarka Pików dla bezpiecznego usuwania

Prawdopodobnie wiesz, że usunięcie pliku w systemie Windows po prostu wysyła go do Kosza. Nawet jeśli opróżnisz lub pomijasz kosz, usunięte dane pliku pozostają na dysku, dopóki nie zostaną nadpisane przez nowe informacje. Oprogramowanie może często odzyskać pliki, które uważasz za bezpieczne. W przypadku prawdziwego, trwałego wymazywania plików potrzebny jest program rozdrabniający.

Niszczarka plików Bitdefender zastępuje dane o plikach trzykrotnie przed usunięciem, co zdecydowanie wystarczy. Możesz kliknąć prawym przyciskiem myszy plik lub folder i wybrać Niszczarkę Plików Bitdefender. Możesz otworzyć niszczarkę i przeglądać, aby wybrać pliki do trwałego usunięcia. Nowość w tym wydaniu i najbardziej mile widziana, możesz po prostu przeciągnąć i upuścić pliki w oknie niszczarki.

Ta funkcja jest często powiązana z szyfrowaniem plików. Aby zapewnić najwyższy poziom bezpieczeństwa, najpierw szyfrujesz poufne pliki, a następnie rozdrabniasz niezabezpieczone oryginały. Bitdefender oferuje szyfrowanie, ale nie na poziomie antywirusowym.

Bitdefender Antivirus to świetny wybór

Przede wszystkim Bitdefender Antivirus Plus oferuje doskonałą ochronę przed złośliwym oprogramowaniem, czego dowodem są doskonałe wyniki z wielu niezależnych laboratoriów testowych. Moje własne testy wskazują, że jest bardzo skuteczny wobec zagrożeń internetowych, w tym witryn zawierających złośliwe oprogramowanie i stron phishingowych. Poza tym wykorzystuje wiele funkcji, które można by uznać za pakiet. **Bitdefender Antivirus Plus to doskonały wybór!**

Informację można dowolnie wykorzystać podając markę Bitdefender jako źródło.
Marken Systemy Antywirusowe – oficjalny przedstawiciel marki Bitdefender w Polsce.

Źródło: https://www.pcmag.com/article2/0,2817,2460688,00.asp
Autor: Neil J. Rubenking