THE INDEPENDENT ANTIVIRUS TESTS

Test ochrony bankowości internetowej

Nazwa produktu: Arcabit Internet Security
Wersja: 2019.02.14
Data testu: luty 2019

Rodzaj testu	Ustawienia domyślne	Ustawienia zmodyfikowane i/lub tryb bankowy
Przechwytywanie schowka. Test sprawdza, czy złośliwe oprogramowanie może przechwytywać zawartość schowka systemowego i wysyłać informacje do serwera kontrolowanego przez hackera.	✓ POZYTYWNY	✓ POZYTYWNY
Podmiana schowka. Test sprawdza, czy złośliwe oprogramowanie może zmieniać zawartość schowka systemowego np. skopiowany numer konta bankowego na inny.	✓ POZYTYWNY	✓ POZYTYWNY
Rejestrowanie klawiatury. Test sprawdza, czy złośliwe oprogramowanie może rejestrować naciśnięcia klawiszy na klawiaturze podczas logowania do konta bankowego i wysyłać informacje na konto Gmail osoby atakującej.	✓ POZYTYWNY	✓ POZYTYWNY
Wykonywanie zrzutów ekranu. Test sprawdza, czy złośliwe oprogramowanie może wykonywać zrzuty ekranu podczas korzystania z bankowości internetowej.	✓ POZYTYWNY	✓ POZYTYWNY
Przeszukiwanie pamięci RAM. Test sprawdza, czy złośliwe oprogramowanie może wyodrębnić poufne informacje z pamięci RAM, np. numery kart kredytowych, hasła, loginy lub numery kont bankowych.	✓ POZYTYWNY	✓ POZYTYWNY
Wstrzykiwanie bibliotek DLL. Test sprawdza, czy możliwe jest wstrzykiwanie złośliwych plików DLL do procesów tzw. „bezpiecznej przeglądarki" lub „środowiska wirtualnego" lub procesów antywirusa. Używane metody: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✗ NEGATYWNY	✓ POZYTYWNY (Włączony moduł Safe Browser)
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest wstawienie kodu HTML i kodu JavaScript do stron internetowych.	✗ NEGATYWNY	✗ NEGATYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest przechwycenie poufnych informacji ze stron internetowych zabezpieczonych certyfikatem SSL.	✗ NEGATYWNY	✗ NEGATYWNY
Ukryty pulpit. Test sprawdza, czy złośliwe oprogramowanie może nawiązać zdalne połączenie z serwerem hackera podczas aktywnej sesji bankowej.	✓ POZYTYWNY	✓ POZYTYWNY
Modyfikowanie pliku HOSTS. Test sprawdza, czy złośliwe oprogramowanie może manipulować zawartością pliku HOSTS systemu Windows.	✗ NEGATYWNY	✓ POZYTYWNY (Włączony moduł Safe Browser)
Wykrywanie trzynastu trojanów bankowych znalezionych in-the-wild w lutym 2019 roku.	POZYTYWNY: 13 / 13	

ZDANYCH TESTÓW: 9 / 11

Włączenie niektórych funkcji lub trybu bankowego pozwala uzyskać lepszy wynik.

Opis unikalnych składników ochrony bankowej, aby umożliwić lepsze zrozumienie, w jaki sposób technologia chroni użytkowników podczas aktywnej sesji bankowej.

Niezawodna przeglądarka Arcabit Safe Browser zapewnia wysoki poziom bezpieczeństwa w trakcie korzystania z zasobów Internetu, a zwłaszcza w trakcie operacji bankowych, płatniczych oraz wymagających podawania wrażliwych danych. Safe Browser ściśle współpracuje z pozostałymi modułami pakietu Arcabit i stale kontroluje poziom bezpieczeństwa systemu, nie dopuszczając do sytuacji, w których newralgiczne dane mogłyby trafić w niepowołane ręce. Producent zastosował ochronę w oparciu o „białe listy" procesów, co oznacza, że jeszcze przed włączeniem bezpiecznej przeglądarki sprawdzane są uruchomione procesy. Niektóre z nich mogą być szkodliwe i działać w ukryciu, oszukując ochronę antywirusową. Arcabit wyprzedza autorów złośliwego oprogramowania i wyświetla procesy, które nie są zdefiniowane przez producenta jako bezpieczne. Decyzja, które z nich powinny być zamknięte, a które nie, jest uwarunkowana preferencjami użytkownika. Sposób korzystania z Arcabit Safe Browser jest następujący: wszystkie procesy, które znajdują się na wyświetlonej liście uruchomionych procesów, powinny zostać zamknięte. Tak na wszelki wypadek, aby niepotrzebne nie narażać się na ryzyko utraty pieniędzy czy przechwycenia poufnych informacji uwierzytelniających w systemie on-line.

Rekomendacja AWARD BEST++

Test ochrony bankowości internetowej

Nazwa produktu: Avast Premier
Wersja: 19.2
Data testu: luty 2019

Rodzaj testu	Ustawienia domyślne	Ustawienia zmodyfikowane i/lub tryb bankowy
Przechwytywanie schowka. Test sprawdza, czy złośliwe oprogramowanie może przechwytywać zawartość schowka systemowego i wysyłać informacje do serwera kontrolowanego przez hackera.	✓ POZYTYWNY	✓ POZYTYWNY
Podmiana schowka. Test sprawdza, czy złośliwe oprogramowanie może zmieniać zawartość schowka systemowego np. skopiowany numer konta bankowego na inny.	✓ POZYTYWNY	✓ POZYTYWNY
Rejestrowanie klawiatury. Test sprawdza, czy złośliwe oprogramowanie może rejestrować naciśnięcia klawiszy na klawiaturze podczas logowania do konta bankowego i wysyłać informacje na konto Gmail osoby atakującej.	✓ POZYTYWNY	✓ POZYTYWNY
Wykonywanie zrzutów ekranu. Test sprawdza, czy złośliwe oprogramowanie może wykonywać zrzuty ekranu podczas korzystania z bankowości internetowej.	✓ POZYTYWNY	✓ POZYTYWNY
Przeszukiwanie pamięci RAM. Test sprawdza, czy złośliwe oprogramowanie może wyodrębnić poufne informacje z pamięci RAM, np. numery kart kredytowych, hasła, loginy lub numery kont bankowych.	✓ POZYTYWNY	✓ POZYTYWNY
Wstrzykiwanie bibliotek DLL. Test sprawdza, czy możliwe jest wstrzykiwanie złośliwych plików DLL do procesów tzw. „bezpiecznej przeglądarki" lub „środowiska wirtualnego" lub procesów antywirusa. Używane metody: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest wstawienie kodu HTML i kodu JavaScript do stron internetowych.	✗ NEGATYWNY	✗ NEGATYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest przechwycenie poufnych informacji ze stron internetowych zabezpieczonych certyfikatem SSL.	✗ NEGATYWNY	✗ NEGATYWNY
Ukryty pulpit. Test sprawdza, czy złośliwe oprogramowanie może nawiązać zdalne połączenie z serwerem hackera podczas aktywnej sesji bankowej.	✓ POZYTYWNY	✓ POZYTYWNY
Modyfikowanie pliku HOSTS. Test sprawdza, czy złośliwe oprogramowanie może manipulować zawartością pliku HOSTS systemu Windows.	✓ POZYTYWNY	✓ POZYTYWNY
Wykrywanie trzynastu trojanów bankowych znalezionych in-the-wild w lutym 2019 roku.	POZYTYWNY: 13 / 13	

Opis unikalnych składników ochrony bankowej, aby umożliwić lepsze zrozumienie, w jaki sposób technologia chroni użytkowników podczas aktywnej sesji bankowej.

Avast w trybie bankowym uniemożliwia hakerom podejrzenie wpisywanych informacji. Tym samym chroni przed wyciekiem haseł, numerów kart kredytowych i innych danych. Tryb bankowy jest dodatkowym zabezpieczeniem dołączonym do przeglądarki Avast Secure Browser. Tworzy odizolowaną sesję pulpitu podczas wykonywania bankowości online lub innych czynności, które wymagają odseparowania przeglądarki od systemu. Technologia opracowana przez firmę Avast to w rzeczywistości odizolowany obszar (nowy pulpit) od systemu operacyjnego, który sprawia, że złośliwe oprogramowanie, takie jak keylogger czy spyware nie może rejestrować wpisywanych znaków na klawiaturze ani nie przekazuje osobistych informacji osobie niepowołanej. Dodatkowo tryb bankowy zapewnia prywatność, gdy w grę wchodzą jakiekolwiek informacje o płatnościach lub poufne dane. Trybu można używać dla bankowości internetowej, zakupów online, zarządzania kryptowalutami lub testowania nieznanego oprogramowania, bądź potencjalnie zainfekowanych faktur. Otworzona przeglądarka w odizolowanym trybie graficznym tworzy bezpieczną przestrzeń, która jest poza zasięgiem nawet antywirusa. Sprawia to, że złośliwe oprogramowanie nie może przedostać się z systemu do bezpiecznej strefy, ani odwrotnie.

ZDANYCH TESTÓW: **9 / 11**

Włączenie niektórych funkcji lub trybu bankowego nie miało wpływu na lepszy wynik.

Rekomendacja AWARD BEST++

THE INDEPENDENT ANTIVIRUS TESTS

Avira

Test ochrony bankowości internetowej

Nazwa produktu: Avira Antivirus Pro
Wersja: 15.0
Data testu: luty 2019

Rodzaj testu	Ustawienia domyślne	Ustawienia zmodyfikowane i/lub tryb bankowy
Przechwytywanie schowka. Test sprawdza, czy złośliwe oprogramowanie może przechwytywać zawartość schowka systemowego i wysyłać informacje do serwera kontrolowanego przez hackera.	✓ POZYTYWNY	✓ POZYTYWNY
Podmiana schowka. Test sprawdza, czy złośliwe oprogramowanie może zmieniać zawartość schowka systemowego np. skopiowany numer konta bankowego na inny.	✗ NEGATYWNY	✗ NEGATYWNY
Rejestrowanie klawiatury. Test sprawdza, czy złośliwe oprogramowanie może rejestrować naciśnięcia klawiszy na klawiaturze podczas logowania do konta bankowego i wysyłać informacje na konto Gmail osoby atakującej.	✓ POZYTYWNY	✓ POZYTYWNY
Wykonywanie zrzutów ekranu. Test sprawdza, czy złośliwe oprogramowanie może wykonywać zrzuty ekranu podczas korzystania z bankowości internetowej.	✗ NEGATYWNY	✗ NEGATYWNY
Przeszukiwanie pamięci RAM. Test sprawdza, czy złośliwe oprogramowanie może wyodrębnić poufne informacje z pamięci RAM, np. numery kart kredytowych, hasła, loginy lub numery kont bankowych.	✗ NEGATYWNY	✗ NEGATYWNY
Wstrzykiwanie bibliotek DLL. Test sprawdza, czy możliwe jest wstrzykiwanie złośliwych plików DLL do procesów tzw. „bezpiecznej przeglądarki" lub „środowiska wirtualnego" lub procesów antywirusa. Używane metody: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest wstawienie kodu HTML i kodu JavaScript do stron internetowych.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest przechwycenie poufnych informacji ze stron internetowych zabezpieczonych certyfikatem SSL.	✓ POZYTYWNY	✓ POZYTYWNY
Ukryty pulpit. Test sprawdza, czy złośliwe oprogramowanie może nawiązać zdalne połączenie z serwerem hackera podczas aktywnej sesji bankowej.	✓ POZYTYWNY	✓ POZYTYWNY
Modyfikowanie pliku HOSTS. Test sprawdza, czy złośliwe oprogramowanie może manipulować zawartością pliku HOSTS systemu Windows.	✓ POZYTYWNY	✓ POZYTYWNY
Wykrywanie trzynastu trojanów bankowych znalezionych in-the-wild w lutym 2019 roku.	POZYTYWNY: 13 / 13	

Opis unikalnych składników ochrony bankowej, aby umożliwić lepsze zrozumienie, w jaki sposób technologia chroni użytkowników podczas aktywnej sesji bankowej.

Pakiet bezpieczeństwa Avira Antivirus Pro w bankowości internetowej blokuje ataki phishingowe, zabezpieczając przed kradzieżą poufnych danych z kart debetowych i poświadczeń bankowych. Zabezpiecza system przed trojanami bankowymi, złośliwymi hostami i witrynami rozprzestrzeniającymi szkodliwe oprogramowanie. Blokuje nieautoryzowane podejrzane procesy, które wykonują operacje na rejestrze systemowym. Antywirus potrafi wykrywać i blokować skrypty śledzące, reklamy oraz skrypty kopiące kryptowalutę. Do ochrony systemu operacyjnego wykorzystuje technologię w chmurze, która dostarcza metadanych o stronach phishingowych. W chmurze Avira Protection Cloud weryfikowane są nie tylko adresy URL, ale też pliki, które są sprawdzane na podstawie baz sygnatur wirusów, ochrony heurystycznej i dogłębnej analizy. Dzięki temu możliwe jest szybsze reagowanie na pojawiające się nowe przestępcze kampanie internetowe. To bardzo dobra metoda weryfikowania bezpieczeństwa plików o zerowej reputacji. Z technologii firmy Avira korzystają zewnętrzni dostawcy technologii antywirusowych, co świadczy o dojrzałych i stabilnych rozwiązaniach tego producenta.

ZDANYCH TESTÓW: **8 / 11**

Włączenie niektórych funkcji lub trybu bankowego nie miało wpływu na lepszy wynik.

Recommendacja AWARD GOOD+

THE INDEPENDENT ANTIVIRUS TESTS

Bitdefender

Test ochrony bankowości internetowej

Nazwa produktu: Bitdefender Total Security
Wersja: 23.0
Data testu: luty 2019

Rodzaj testu	Ustawienia domyślne	Ustawienia zmodyfikowane i/lub tryb bankowy
Przechwytywanie schowka. Test sprawdza, czy złośliwe oprogramowanie może przechwytywać zawartość schowka systemowego i wysyłać informacje do serwera kontrolowanego przez hackera.	✗ NEGATYWNY	✓ POZYTYWNY (Bitdefender Safepay)
Podmiana schowka. Test sprawdza, czy złośliwe oprogramowanie może zmieniać zawartość schowka systemowego np. skopiowany numer konta bankowego na inny.	✗ NEGATYWNY	✓ POZYTYWNY (Bitdefender Safepay)
Rejestrowanie klawiatury. Test sprawdza, czy złośliwe oprogramowanie może rejestrować naciśnięcia klawiszy na klawiaturze podczas logowania do konta bankowego i wysyłać informacje na konto Gmail osoby atakującej.	✓ POZYTYWNY	✓ POZYTYWNY
Wykonywanie zrzutów ekranu. Test sprawdza, czy złośliwe oprogramowanie może wykonywać zrzuty ekranu podczas korzystania z bankowości internetowej.	✗ NEGATYWNY	✓ POZYTYWNY (Bitdefender Safepay)
Przeszukiwanie pamięci RAM. Test sprawdza, czy złośliwe oprogramowanie może wyodrębnić poufne informacje z pamięci RAM, np. numery kart kredytowych, hasła, loginy lub numery kont bankowych.	✗ NEGATYWNY	✗ NEGATYWNY
Wstrzykiwanie bibliotek DLL. Test sprawdza, czy możliwe jest wstrzykiwanie złośliwych plików DLL do procesów tzw. „bezpiecznej przeglądarki" lub „środowiska wirtualnego" lub procesów antywirusa. Używane metody: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest wstawienie kodu HTML i kodu JavaScript do stron internetowych.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest przechwycenie poufnych informacji ze stron internetowych zabezpieczonych certyfikatem SSL.	✓ POZYTYWNY	✓ POZYTYWNY
Ukryty pulpit. Test sprawdza, czy złośliwe oprogramowanie może nawiązać zdalne połączenie z serwerem hackera podczas aktywnej sesji bankowej.	✓ POZYTYWNY	✓ POZYTYWNY
Modyfikowanie pliku HOSTS. Test sprawdza, czy złośliwe oprogramowanie może manipulować zawartością pliku HOSTS systemu Windows.	✗ NEGATYWNY	✓ POZYTYWNY (Bitdefender Safepay)
Wykrywanie trzynastu trojanów bankowych znalezionych in-the-wild w lutym 2019 roku.	POZYTYWNY: 13 / 13	

Opis unikalnych składników ochrony bankowej, aby umożliwić lepsze zrozumienie, w jaki sposób technologia chroni użytkowników podczas aktywnej sesji bankowej.

Jednym z najważniejszych modułów do ochrony sesji online jest technologa, która w pełni wykorzystuje opracowane mechanizmy w chmurze. Bitdefender Safepay występuje w wersji z pakietami bezpieczeństwa tej firmy oraz jako oddzielne oprogramowanie. Chroni przed oszustwami, phishingiem, wirusami i szkodliwym oprogramowaniem, m.in keyloggerami i screenloggerami, które zostały zaprojektowane w celu przechwytywania naciśnięć klawiszy i robienia zrzutów ekranu. Użytkownik może przełączać się pomiędzy wirtualnym środowiskiem Bitdefender Safepay, a swoim pulpitem. W trakcie tych czynności może korzystać z komputera tak jak do tej pory, bez zbędnego obciążenia zasobów systemowych. Jeżeli sesja Safepay jest aktywna, nie pozwoli to zewnętrznym aplikacjom modyfikować środowiska Bitdefender Safepay. W ten sposób przełączając się do bezpiecznej przeglądarki komputer będzie chroniony przed zagrożeniami internetowymi, oszustwami, niezaufanym witrynami, witrynami ze spamem oraz stronami ze złośliwym oprogramowaniem.

ZDANYCH TESTÓW: **10 / 11**

Włączenie niektórych funkcji lub trybu bankowego pozwala uzyskać lepszy wynik.

Rekomendacja AV-LAB AWARD BEST++

THE INDEPENDENT ANTIVIRUS TESTS

Test ochrony bankowości internetowej

Nazwa produktu: BullGuard Premium Protection
Wersja: 19.0
Data testu: luty 2019

Rodzaj testu	Ustawienia domyślne	Ustawienia zmodyfikowane i/lub tryb bankowy
Przechwytywanie schowka. Test sprawdza, czy złośliwe oprogramowanie może przechwytywać zawartość schowka systemowego i wysyłać informacje do serwera kontrolowanego przez hackera.	✓ POZYTYWNY	✓ POZYTYWNY
Podmiana schowka. Test sprawdza, czy złośliwe oprogramowanie może zmieniać zawartość schowka systemowego np. skopiowany numer konta bankowego na inny.	✗ NEGATYWNY	✗ NEGATYWNY
Rejestrowanie klawiatury. Test sprawdza, czy złośliwe oprogramowanie może rejestrować naciśnięcia klawiszy na klawiaturze podczas logowania do konta bankowego i wysyłać informacje na konto Gmail osoby atakującej.	✓ POZYTYWNY	✓ POZYTYWNY
Wykonywanie zrzutów ekranu. Test sprawdza, czy złośliwe oprogramowanie może wykonywać zrzuty ekranu podczas korzystania z bankowości internetowej.	✗ NEGATYWNY	✗ NEGATYWNY
Przeszukiwanie pamięci RAM. Test sprawdza, czy złośliwe oprogramowanie może wyodrębnić poufne informacje z pamięci RAM, np. numery kart kredytowych, hasła, loginy lub numery kont bankowych.	✗ NEGATYWNY	✗ NEGATYWNY
Wstrzykiwanie bibliotek DLL. Test sprawdza, czy możliwe jest wstrzykiwanie złośliwych plików DLL do procesów tzw. „bezpiecznej przeglądarki" lub „środowiska wirtualnego" lub procesów antywirusa. Używane metody: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest wstawienie kodu HTML i kodu JavaScript do stron internetowych.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest przechwycenie poufnych informacji ze stron internetowych zabezpieczonych certyfikatem SSL.	✓ POZYTYWNY	✓ POZYTYWNY
Ukryty pulpit. Test sprawdza, czy złośliwe oprogramowanie może nawiązać zdalne połączenie z serwerem hackera podczas aktywnej sesji bankowej.	✓ POZYTYWNY	✓ POZYTYWNY
Modyfikowanie pliku HOSTS. Test sprawdza, czy złośliwe oprogramowanie może manipulować zawartością pliku HOSTS systemu Windows.	✗ NEGATYWNY	✗ NEGATYWNY
Wykrywanie trzynastu trojanów bankowych znalezionych in-the-wild w lutym 2019 roku.	POZYTYWNY: 13 / 13	

Opis unikalnych składników ochrony bankowej, aby umożliwić lepsze zrozumienie, w jaki sposób technologia chroni użytkowników podczas aktywnej sesji bankowej.

BullGuard łączy w sobie wiele modułów bezpieczeństwa. Posiada zaprę sieciową wykrywającą ataki, skanuje sieć domową i blokuje złośliwe hosty, dzięki czemu dobrze sprawdził się w ochronie przed atakami man-in-the-middle. Dla bankowości internetowej producent przygotował ochronę przez phishingiem oraz stronami rozprzestrzeniającymi złośliwe oprogramowanie. Rozwiązanie posiada funkcję ochrony przed potencjalnie niechcianymi aplikacjami (PUP), która wykrywa i usuwa oprogramowanie modyfikujące ustawienia przeglądarki internetowej, jak np. zmienię strony startowej. Z kolei technologia monitorowania zasobów śledzi aktywność użytkownika w systemie i sprawdza, jakie działania są wykonywane przez każdy program. Zastosowano tu inteligentną ochronę potrójnej warstwy — najpierw rozpoznawana jest reputacja strony i pobieranego programu. Później wykonywane jest skanowanie kodu pod kątem anomalii związanych ze złośliwym oprogramowaniem. Na końcu każde wykryte złośliwe oprogramowanie jest blokowane, poddawane kwarantannie i neutralizowane.

ZDANYCH TESTÓW: **7 / 11**

Włączenie niektórych funkcji lub trybu bankowego nie miało wpływu na lepszy wynik.

Recommendacja AV LAB AWARD GOOD+

THE INDEPENDENT ANTIVIRUS TESTS

ZoneAlarm By Check Point

Test ochrony bankowości internetowej

Nazwa produktu: Check Point ZoneAlarm Extreme Security
Wersja: 15.4
Data testu: luty 2019

Rodzaj testu	Ustawienia domyślne	Ustawienia zmodyfikowane i/lub tryb bankowy
Przechwytywanie schowka. Test sprawdza, czy złośliwe oprogramowanie może przechwytywać zawartość schowka systemowego i wysyłać informacje do serwera kontrolowanego przez hackera.	✓ POZYTYWNY	✓ POZYTYWNY
Podmiana schowka. Test sprawdza, czy złośliwe oprogramowanie może zmieniać zawartość schowka systemowego np. skopiowany numer konta bankowego na inny.	✓ POZYTYWNY	✓ POZYTYWNY
Rejestrowanie klawiatury. Test sprawdza, czy złośliwe oprogramowanie może rejestrować naciśnięcia klawiszy na klawiaturze podczas logowania do konta bankowego i wysyłać informacje na konto Gmail osoby atakującej.	✗ NEGATYWNY	✓ POZYTYWNY (Włączony Anti-Keylogger)
Wykonywanie zrzutów ekranu. Test sprawdza, czy złośliwe oprogramowanie może wykonywać zrzuty ekranu podczas korzystania z bankowości internetowej.	✓ POZYTYWNY	✓ POZYTYWNY
Przeszukiwanie pamięci RAM. Test sprawdza, czy złośliwe oprogramowanie może wyodrębnić poufne informacje z pamięci RAM, np. numery kart kredytowych, hasła, loginy lub numery kont bankowych.	✓ POZYTYWNY	✓ POZYTYWNY
Wstrzykiwanie bibliotek DLL. Test sprawdza, czy możliwe jest wstrzykiwanie złośliwych plików DLL do procesów tzw. „bezpiecznej przeglądarki" lub „środowiska wirtualnego" lub procesów antywirusa. Używane metody: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest wstawienie kodu HTML i kodu JavaScript do stron internetowych.	✗ NEGATYWNY	✓ POZYTYWNY (Włączony moduł ARP protection)
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest przechwycenie poufnych informacji ze stron internetowych zabezpieczonych certyfikatem SSL.	✗ NEGATYWNY	✓ POZYTYWNY (Włączony moduł ARP protection)
Ukryty pulpit. Test sprawdza, czy złośliwe oprogramowanie może nawiązać zdalne połączenie z serwerem hackera podczas aktywnej sesji bankowej.	✓ POZYTYWNY	✓ POZYTYWNY
Modyfikowanie pliku HOSTS. Test sprawdza, czy złośliwe oprogramowanie może manipulować zawartością pliku HOSTS systemu Windows.	✓ POZYTYWNY	✓ POZYTYWNY
Wykrywanie trzynastu trojanów bankowych znalezionych in-the-wild w lutym 2019 roku.	POZYTYWNY: 13 / 13	

ZDANYCH TESTÓW: **11 / 11**

Włączenie niektórych funkcji lub trybu bankowego pozwala uzyskać lepszy wynik.

Rekomendacja AV LAB AWARD BEST+++

Opis unikalnych składników ochrony bankowej, aby umożliwić lepsze zrozumienie, w jaki sposób technologia chroni użytkowników podczas aktywnej sesji bankowej.

ZoneAlarm Extreme Security jest odpowiedzią firmy Check Point specjalizującej się w dostarczaniu zabezpieczeń sieciowych na ewoluujące zagrożenia i ataki. W tym produkcie dostępna jest technologia Threat Emulation. Check Point ZoneAlarm Extreme Security czerpie z doświadczenia pracowników Check Point, którzy dostarczają usługi dla dużego biznesu. Autorzy szkodliwego oprogramowania mogą tworzyć takie próbki, które z łatwością omijają tradycyjne produkty sygnaturowe. Detekcja zagrożeń na podstawie definicji wirusów to stara technika wykrywania znanych ataków. Obecnie służy bardziej do wspierania niż do stanowienia rdzenia ochrony. Z kolei emulacja zagrożeń zabezpiecza przed nowymi szkodliwymi programami szyfrującymi. Taką właśnie technologię wykorzystuje Check Point ZoneAlarm Extreme Security. Produkt charakteryzują jeszcze dwie rzeczy. To autorski firewall, który zabezpiecza m.in. przed modyfikacją plik HOSTS. Chroni przed internetowymi atakami, a także pozwala na konfigurację restrykcji dla kierunków dostępu aplikacji do sieci. Drugim znakiem szczególnym jest ochrona w przeglądarce dzięki bazie zagrożeń pochodzącej z systemu ThreatCloud. Jest to ogromna zorganizowana sieć do walki z cyberprzestępczością, która dostarcza dane o zagrożeniach i trendy ataków na podstawie globalnej sieci czujników zagrożeń.

THE INDEPENDENT ANTIVIRUS TESTS

COMODO
Creating Trust Online®

Test ochrony bankowości internetowej

Nazwa produktu: Comodo Internet Security
Wersja: 11.0
Data testu: luty 2019

Rodzaj testu	Ustawienia domyślne	Ustawienia zmodyfikowane i/lub tryb bankowy
Przechwytywanie schowka. Test sprawdza, czy złośliwe oprogramowanie może przechwytywać zawartość schowka systemowego i wysyłać informacje do serwera kontrolowanego przez hackera.	✓ POZYTYWNY	✓ POZYTYWNY
Podmiana schowka. Test sprawdza, czy złośliwe oprogramowanie może zmieniać zawartość schowka systemowego np. skopiowany numer konta bankowego na inny.	✓ POZYTYWNY	✓ POZYTYWNY
Rejestrowanie klawiatury. Test sprawdza, czy złośliwe oprogramowanie może rejestrować naciśnięcia klawiszy na klawiaturze podczas logowania do konta bankowego i wysyłać informacje na konto Gmail osoby atakującej.	✓ POZYTYWNY	✓ POZYTYWNY
Wykonywanie zrzutów ekranu. Test sprawdza, czy złośliwe oprogramowanie może wykonywać zrzuty ekranu podczas korzystania z bankowości internetowej.	✓ POZYTYWNY	✓ POZYTYWNY
Przeszukiwanie pamięci RAM. Test sprawdza, czy złośliwe oprogramowanie może wyodrębnić poufne informacje z pamięci RAM, np. numery kart kredytowych, hasła, loginy lub numery kont bankowych.	✓ POZYTYWNY	✓ POZYTYWNY
Wstrzykiwanie bibliotek DLL. Test sprawdza, czy możliwe jest wstrzykiwanie złośliwych plików DLL do procesów tzw. „bezpiecznej przeglądarki" lub „środowiska wirtualnego" lub procesów antywirusa. Używane metody: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest wstawienie kodu HTML i kodu JavaScript do stron internetowych.	✗ NEGATYWNY	✓ POZYTYWNY (Włączony anti-ARP spoofing)
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest przechwycenie poufnych informacji ze stron internetowych zabezpieczonych certyfikatem SSL.	✗ NEGATYWNY	✓ POZYTYWNY (Włączony anti-ARP spoofing)
Ukryty pulpit. Test sprawdza, czy złośliwe oprogramowanie może nawiązać zdalne połączenie z serwerem hackera podczas aktywnej sesji bankowej.	✓ POZYTYWNY	✓ POZYTYWNY
Modyfikowanie pliku HOSTS. Test sprawdza, czy złośliwe oprogramowanie może manipulować zawartością pliku HOSTS systemu Windows.	✓ POZYTYWNY	✓ POZYTYWNY
Wykrywanie trzynastu trojanów bankowych znalezionych in-the-wild w lutym 2019 roku.	POZYTYWNY: 13 / 13	

ZDANYCH TESTÓW: 11 / 11

Włączenie niektórych funkcji lub trybu bankowego pozwala uzyskać lepszy wynik.

Opis unikalnych składników ochrony bankowej, aby umożliwić lepsze zrozumienie, w jaki sposób technologia chroni użytkowników podczas aktywnej sesji bankowej.

Comodo Internet Security posiada moduł bezpiecznych zakupów. Ta funkcjonalność pozwala włączyć wirtualne środowisko i bez obaw o bezpieczeństwo uruchamiać np. podejrzane załączniki i sprawdzać ich szkodliwość. Bezpieczne Zakupy (ang. Secure Shopping) zawiera ochronę przed keyloggerami, trojanami, robakami, screenloggerami, a także izoluje procesy uniemożliwiając wstrzykiwanie złośliwego kodu do przeglądarki w środowisku wirtualnym. Trzeba mocno zaakcentować (chociaż są to archiwalne informacje), że kilka lat temu agencja CIA poddała testom większość znanych aplikacji antywirusowych, lecz tylko jedna szczególnie zaszła za skórę hakerom zatrudnionym przez amerykańskie biuro. Pakiet firmy Comodo zyskał określenie „trudnego do złamania" antywirusa. Do najbardziej znaczących modułów zaliczamy wyspecjalizowany firewall do skanowania ruchu internetowego, który chroni przed atakami ARP spoofing. HIPS monitoruje aktywność systemu i aplikacji pozwalając upewnić się, czy potencjalnie niebezpieczny plik realizuje pewne czynności, które mogą być zarezerwowane dla szkodliwego oprogramowania. Domyślnie aktywny moduł Viruscope to behawioralny składnik do analizy i monitorowania procesów pod kątem wprowadzanych potencjalnych złośliwych zmian. Automatyczna piaskownica realizuje ochronę przed zagrożeniami 0-day, których silnik antywirusowy nie zdoła wykryć za pomocą sygnatur lub skanowania plików w chmurze. Comodo Internet Security to potężne narzędzie do ochrony systemu przed malware 0-day i atakami hakerów.

Rekomendacja AV LAB AWARD BEST+++

Test ochrony bankowości internetowej

Nazwa produktu: Dr.Web Space Security
Wersja: 12.0
Data testu: luty 2019

Rodzaj testu	Ustawienia domyślne	Ustawienia zmodyfikowane i/lub tryb bankowy
Przechwytywanie schowka. Test sprawdza, czy złośliwe oprogramowanie może przechwytywać zawartość schowka systemowego i wysyłać informacje do serwera kontrolowanego przez hackera.	✓ POZYTYWNY	✓ POZYTYWNY
Podmiana schowka. Test sprawdza, czy złośliwe oprogramowanie może zmieniać zawartość schowka systemowego np. skopiowany numer konta bankowego na inny.	✗ NEGATYWNY	✗ NEGATYWNY
Rejestrowanie klawiatury. Test sprawdza, czy złośliwe oprogramowanie może rejestrować naciśnięcia klawiszy na klawiaturze podczas logowania do konta bankowego i wysyłać informacje na konto Gmail osoby atakującej.	✓ POZYTYWNY	✓ POZYTYWNY
Wykonywanie zrzutów ekranu. Test sprawdza, czy złośliwe oprogramowanie może wykonywać zrzuty ekranu podczas korzystania z bankowości internetowej.	✗ NEGATYWNY	✗ NEGATYWNY
Przeszukiwanie pamięci RAM. Test sprawdza, czy złośliwe oprogramowanie może wyodrębnić poufne informacje z pamięci RAM, np. numery kart kredytowych, hasła, loginy lub numery kont bankowych.	✗ NEGATYWNY	✗ NEGATYWNY
Wstrzykiwanie bibliotek DLL. Test sprawdza, czy możliwe jest wstrzykiwanie złośliwych plików DLL do procesów tzw. „bezpiecznej przeglądarki" lub „środowiska wirtualnego" lub procesów antywirusa. Używane metody: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest wstawienie kodu HTML i kodu JavaScript do stron internetowych.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest przechwycenie poufnych informacji ze stron internetowych zabezpieczonych certyfikatem SSL.	✓ POZYTYWNY	✓ POZYTYWNY
Ukryty pulpit. Test sprawdza, czy złośliwe oprogramowanie może nawiązać zdalne połączenie z serwerem hackera podczas aktywnej sesji bankowej.	✓ POZYTYWNY	✓ POZYTYWNY
Modyfikowanie pliku HOSTS. Test sprawdza, czy złośliwe oprogramowanie może manipulować zawartością pliku HOSTS systemu Windows.	✓ POZYTYWNY	✓ POZYTYWNY
Wykrywanie trzynastu trojanów bankowych znalezionych in-the-wild w lutym 2019 roku.	POZYTYWNY: 13 / 13	

ZDANYCH TESTÓW: **8 / 11**

Włączenie niektórych funkcji lub trybu bankowego nie miało wpływu na lepszy wynik.

Opis unikalnych składników ochrony bankowej, aby umożliwić lepsze zrozumienie, w jaki sposób technologia chroni użytkowników podczas aktywnej sesji bankowej.

Rozwiązanie Dr.Web Space Security zostało wyposażone w rozszerzony zakres ochrony procesów, usług, sterowników, rejestru, połączeń sieciowych i protokołu WMI, z którego korzysta wiele typów szkodliwego oprogramowania. Zadaniem ochrony jest monitorowanie i kontrolowanie wszystkich zagrożeń, które próbują zrobić cokolwiek podejrzanego za pomocą zaufanych procesów systemowych. Heurystyczne algorytmy pokrywają ataki szkodliwych skryptów i blików binarnych. W przeglądarce znajdujemy ochronę, która realizowana jest za pośrednictwem chmury. Jest to moduł łączący komputer użytkownika z informacjami o zagrożeniach w chmurze, który skanuje pliki konfiguracyjne zainstalowanych wtyczek i analizuje je pod kątem bezpieczeństwa. Ochrona prewencyjna w pakiecie Dr.Web polega na analizowaniu zachowania uruchomionych aplikacji i wszystkich procesów systemowych. Komponenty chronią przed najnowszymi szkodliwymi programami, które zostały zaprojektowane, by ukrywać się przed antywirusem.

Recommendacja AWARD GOOD+

THE INDEPENDENT ANTIVIRUS TESTS

EMSISOFT

Test ochrony bankowości internetowej

Nazwa produktu: Emsisoft Anti-Malware Home
Wersja: 2019.1.1
Data testu: luty 2019

Rodzaj testu	Ustawienia domyślne	Ustawienia zmodyfikowane i/lub tryb bankowy
Przechwytywanie schowka. Test sprawdza, czy złośliwe oprogramowanie może przechwytywać zawartość schowka systemowego i wysyłać informacje do serwera kontrolowanego przez hackera.	✓ POZYTYWNY	✓ POZYTYWNY
Podmiana schowka. Test sprawdza, czy złośliwe oprogramowanie może zmieniać zawartość schowka systemowego np. skopiowany numer konta bankowego na inny.	✓ POZYTYWNY	✓ POZYTYWNY
Rejestrowanie klawiatury. Test sprawdza, czy złośliwe oprogramowanie może rejestrować naciśnięcia klawiszy na klawiaturze podczas logowania do konta bankowego i wysyłać informacje na konto Gmail osoby atakującej.	✓ POZYTYWNY	✓ POZYTYWNY
Wykonywanie zrzutów ekranu. Test sprawdza, czy złośliwe oprogramowanie może wykonywać zrzuty ekranu podczas korzystania z bankowości internetowej.	✓ POZYTYWNY	✓ POZYTYWNY
Przeszukiwanie pamięci RAM. Test sprawdza, czy złośliwe oprogramowanie może wyodrębnić poufne informacje z pamięci RAM, np. numery kart kredytowych, hasła, loginy lub numery kont bankowych.	✓ POZYTYWNY	✓ POZYTYWNY
Wstrzykiwanie bibliotek DLL. Test sprawdza, czy możliwe jest wstrzykiwanie złośliwych plików DLL do procesów tzw. „bezpiecznej przeglądarki" lub „środowiska wirtualnego" lub procesów antywirusa. Używane metody: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest wstawienie kodu HTML i kodu JavaScript do stron internetowych.	✗ NEGATYWNY	✗ NEGATYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest przechwycenie poufnych informacji ze stron internetowych zabezpieczonych certyfikatem SSL.	✗ NEGATYWNY	✗ NEGATYWNY
Ukryty pulpit. Test sprawdza, czy złośliwe oprogramowanie może nawiązać zdalne połączenie z serwerem hackera podczas aktywnej sesji bankowej.	✓ POZYTYWNY	✓ POZYTYWNY
Modyfikowanie pliku HOSTS. Test sprawdza, czy złośliwe oprogramowanie może manipulować zawartością pliku HOSTS systemu Windows.	✓ POZYTYWNY	✓ POZYTYWNY
Wykrywanie trzynastu trojanów bankowych znalezionych in-the-wild w lutym 2019 roku.	POZYTYWNY: 13 / 13	

ZDANYCH TESTÓW: **9 / 11**

Włączenie niektórych funkcji lub trybu bankowego nie miało wpływu na lepszy wynik.

Opis unikalnych składników ochrony bankowej, aby umożliwić lepsze zrozumienie, w jaki sposób technologia chroni użytkowników podczas aktywnej sesji bankowej.

Cechą charakterystyczną Emsisoft Anti-Malware Home jest monitor zachowawczy, który obserwuje wszystkie aktywne programy w czasie rzeczywistym pod kątem niebezpiecznych wskaźników. Umożliwia wykrywanie nowych trojanów, ransomware, spyware, backdoorów i innych niebezpiecznych zagrożeń zero-day. Technologia bazuje na metodzie proaktywnej, czyli nie potrzebuje do działania aktualizacji sygnatur. Producent od lat rozwija własne technologie przy udziale społeczności i jest w tym dobry. Niedawno producent opracował nowe rozszerzenie Emsisoft Browser Security dla przeglądarek, które stawia na pierwszym miejscu prywatność — nie loguje żadnych szczegółów dotyczących aktywności przeglądania stron. Istotnym elementem ochrony jest technologia File Guard, która sprawdza wszystkie pobierane lub uruchamiane pliki, porównując je ze z wielomilionową bazą sygnatur. Używając zaawansowanego silnika, skanuje pliki bez nadmiernego obciążania zasobów systemu. Ustawienia domyślne Emsisoft zapewniają równowagę pomiędzy wydajnością a bezpieczeństwem i są wystarczające dla większości użytkowników. Emsisoft już 16 rok z rzędu potwierdza, że tylko najlepsi, dostosowując się do bardzo szybko zmieniających się trendów, mogą utrzymać się na rynku.

Rekomendacja AV LAB AWARD BEST++

THE INDEPENDENT ANTIVIRUS TESTS

Test ochrony bankowości internetowej

Nazwa produktu: Eset Internet Security
Wersja: 12.0.31.0
Data testu: luty 2019

Rodzaj testu	Ustawienia domyślne	Ustawienia zmodyfikowane i/lub tryb bankowy
Przechwytywanie schowka. Test sprawdza, czy złośliwe oprogramowanie może przechwytywać zawartość schowka systemowego i wysyłać informacje do serwera kontrolowanego przez hackera.	✗ NEGATYWNY	✓ POZYTYWNY (Włączony firewall w trybie interaktywnym)
Podmiana schowka. Test sprawdza, czy złośliwe oprogramowanie może zmieniać zawartość schowka systemowego np. skopiowany numer konta bankowego na inny.	✗ NEGATYWNY	✗ NEGATYWNY
Rejestrowanie klawiatury. Test sprawdza, czy złośliwe oprogramowanie może rejestrować naciśnięcia klawiszy na klawiaturze podczas logowania do konta bankowego i wysyłać informacje na konto Gmail osoby atakującej.	✗ NEGATYWNY	✓ POZYTYWNY (Włączona ochrona bankowości internetowej)
Wykonywanie zrzutów ekranu. Test sprawdza, czy złośliwe oprogramowanie może wykonywać zrzuty ekranu podczas korzystania z bankowości internetowej.	✗ NEGATYWNY	✗ NEGATYWNY
Przeszukiwanie pamięci RAM. Test sprawdza, czy złośliwe oprogramowanie może wyodrębnić poufne informacje z pamięci RAM, np. numery kart kredytowych, hasła, loginy lub numery kont bankowych.	✗ NEGATYWNY	✓ POZYTYWNY (Włączona ochrona bankowości internetowej)
Wstrzykiwanie bibliotek DLL. Test sprawdza, czy możliwe jest wstrzykiwanie złośliwych plików DLL do procesów tzw. „bezpiecznej przeglądarki" lub „środowiska wirtualnego" lub procesów antywirusa. Używane metody: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest wstawienie kodu HTML i kodu JavaScript do stron internetowych.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest przechwycenie poufnych informacji ze stron internetowych zabezpieczonych certyfikatem SSL.	✓ POZYTYWNY	✓ POZYTYWNY
Ukryty pulpit. Test sprawdza, czy złośliwe oprogramowanie może nawiązać zdalne połączenie z serwerem hackera podczas aktywnej sesji bankowej.	✓ POZYTYWNY	✓ POZYTYWNY
Modyfikowanie pliku HOSTS. Test sprawdza, czy złośliwe oprogramowanie może manipulować zawartością pliku HOSTS systemu Windows.	✗ NEGATYWNY	✓ POZYTYWNY (HIPS w trybie inteligentnym)
Wykrywanie trzynastu trojanów bankowych znalezionych in-the-wild w lutym 2019 roku.	POZYTYWNY: 13 / 13	

Opis unikalnych składników ochrony bankowej, aby umożliwić lepsze zrozumienie, w jaki sposób technologia chroni użytkowników podczas aktywnej sesji bankowej.

ESET trzyma wysoki poziom ochrony dzięki chmurze Live Grid oraz bardzo dobrej detekcji programów potencjalnie niepożądanych. Posiada funkcję blokującą zagrożenia, które próbują aktywować się i atakować użytkownika zaraz po włączeniu komputera, zanim jeszcze uruchomi się system operacyjny — to tak zwany skaner UEFI. Największe wrażenie robi dobrze skonfigurowany moduł firewall, który wykrywa złośliwą komunikację wykorzystywaną przez sieci botnet. Nie bez znaczenia są odpierane ataki „ARP spoofing" pozwalające atakującemu przechwytywać dane przesyłane w obrębie segmentu sieci lokalnej, a także ataki sieciowe „DNS cache poisoning" polegające na przesłaniu przez atakującego fałszywej informacji do serwera DNS kojarzącego nazwę domeny z adresem IP. Na straży danych czuwa dwukierunkowy firewall zawierający system wykrywania intruzów (IDS, ang. Intrusive Detection System), który wykrywa ataki zatruwające tablice ARP, ataki modyfikujące wpisy DNS, fałszywe zapytania PING, ataki wykorzystujące luki na protokoły SMB, RPC, RDP i ataki skanujące porty. Przydatną funkcją jest ochrona bankowości internetowej zabezpieczająca systemowe WinAPI przed przechwytywaniem klawiszy, czyli w trakcie wprowadzania numerów konta bankowego lub logowania się do bankowości internetowej użytkownik jest chroniony przed manipulowaniem wprowadzanych danych na poziomie interfejsu przeglądarki.

ZDANYCH TESTÓW: **9 / 11**

Włączenie niektórych funkcji lub trybu bankowego pozwala uzyskać lepszy wynik.

Rekomendacja AWARD BEST++

THE INDEPENDENT ANTIVIRUS TESTS

Test ochrony bankowości internetowej

Nazwa produktu: F-Secure SAFE
Wersja: 17.5
Data testu: luty 2019

Rodzaj testu	Ustawienia domyślne	Ustawienia zmodyfikowane i/lub tryb bankowy
Przechwytywanie schowka. Test sprawdza, czy złośliwe oprogramowanie może przechwytywać zawartość schowka systemowego i wysyłać informacje do serwera kontrolowanego przez hackera.	✓ POZYTYWNY	✓ POZYTYWNY
Podmiana schowka. Test sprawdza, czy złośliwe oprogramowanie może zmieniać zawartość schowka systemowego np. skopiowany numer konta bankowego na inny.	✓ POZYTYWNY	✓ POZYTYWNY
Rejestrowanie klawiatury. Test sprawdza, czy złośliwe oprogramowanie może rejestrować naciśnięcia klawiszy na klawiaturze podczas logowania do konta bankowego i wysyłać informacje na konto Gmail osoby atakującej.	✓ POZYTYWNY	✓ POZYTYWNY
Wykonywanie zrzutów ekranu. Test sprawdza, czy złośliwe oprogramowanie może wykonywać zrzuty ekranu podczas korzystania z bankowości internetowej.	✓ POZYTYWNY	✓ POZYTYWNY
Przeszukiwanie pamięci RAM. Test sprawdza, czy złośliwe oprogramowanie może wyodrębnić poufne informacje z pamięci RAM, np. numery kart kredytowych, hasła, loginy lub numery kont bankowych.	✓ POZYTYWNY	✓ POZYTYWNY
Wstrzykiwanie bibliotek DLL. Test sprawdza, czy możliwe jest wstrzykiwanie złośliwych plików DLL do procesów tzw. „bezpiecznej przeglądarki" lub „środowiska wirtualnego" lub procesów antywirusa. Używane metody: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest wstawienie kodu HTML i kodu JavaScript do stron internetowych.	✗ NEGATYWNY	✗ NEGATYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest przechwycenie poufnych informacji ze stron internetowych zabezpieczonych certyfikatem SSL.	✗ NEGATYWNY	✗ NEGATYWNY
Ukryty pulpit. Test sprawdza, czy złośliwe oprogramowanie może nawiązać zdalne połączenie z serwerem hackera podczas aktywnej sesji bankowej.	✓ POZYTYWNY	✓ POZYTYWNY
Modyfikowanie pliku HOSTS. Test sprawdza, czy złośliwe oprogramowanie może manipulować zawartością pliku HOSTS systemu Windows.	✗ NEGATYWNY	✗ NEGATYWNY
Wykrywanie trzynastu trojanów bankowych znalezionych in-the-wild w lutym 2019 roku.	POZYTYWNY: 13 / 13	

ZDANYCH TESTÓW: **8 / 11**

Włączenie niektórych funkcji lub trybu bankowego nie miało wpływu na lepszy wynik.

Recommendacja AV LAB AWARD GOOD+

Opis unikalnych składników ochrony bankowej, aby umożliwić lepsze zrozumienie, w jaki sposób technologia chroni użytkowników podczas aktywnej sesji bankowej.

Mocną stroną pakietu F-Secure jest zawarta w silniku antywirusowym technologia DeepGuard. To rodzaj zabezpieczenia behawioralnego, które monitoruje pliki pod kątem podejrzanego zachowania. W przypadku wykrycia ryzyka niebezpieczny program jest automatycznie blokowany. DeepGuard weryfikuje bezpieczeństwo aplikacji na podstawie informacji z zaufanej usługi zewnętrznej. Kiedy nie można zweryfikować bezpieczeństwa aplikacji funkcja DeepGuard zaczyna monitorować działanie procesu. DeepGuard jest w stanie wykrywać nowe konie trojańskie, robaki, luki w oprogramowaniu i inne szkodliwe aplikacje, które próbują wprowadzać zmiany na komputerze, a także uniemożliwia podejrzanym programom dostępu do Internetu. Potencjalne szkodliwe zmiany w systemie, które są wykrywane przez technologię DeepGuard, obejmują: zmiany ustawień systemu (rejestru systemu Windows), próby wyłączenia ważnych programów systemowych (na przykład programów zabezpieczających) oraz próby edytowania ważnych plików systemowych. Technologia nie tylko chroni przed wymuszeniami ransomware, ale także blokuje aplikacje, które mogłyby podmienić, zmienić nazwę lub usunąć istotne pliki. W zakresie trybu bankowego wszystkie połączenia internetowe są zatrzymywane na czas działania ochrony. Przebiega to automatycznie, ale użytkownik ma nad tym kontrolę (uniemożliwia to komunikowanie się szkodliwemu oprogramowaniu z zewnętrznymi hostami).

THE INDEPENDENT ANTIVIRUS TESTS

Test ochrony bankowości internetowej

Nazwa produktu: G Data Total Protection
Wersja: 25.5.1.21
Data testu: luty 2019

Rodzaj testu	Ustawienia domyślne	Ustawienia zmodyfikowane i/lub tryb bankowy
Przechwytywanie schowka. Test sprawdza, czy złośliwe oprogramowanie może przechwytywać zawartość schowka systemowego i wysyłać informacje do serwera kontrolowanego przez hackera.	✗ NEGATYWNY	✓ POZYTYWNY (Firewall w trybie interaktywnym)
Podmiana schowka. Test sprawdza, czy złośliwe oprogramowanie może zmieniać zawartość schowka systemowego np. skopiowany numer konta bankowego na inny.	✓ POZYTYWNY	✓ POZYTYWNY
Rejestrowanie klawiatury. Test sprawdza, czy złośliwe oprogramowanie może rejestrować naciśnięcia klawiszy na klawiaturze podczas logowania do konta bankowego i wysyłać informacje na konto Gmail osoby atakującej.	✓ POZYTYWNY	✓ POZYTYWNY
Wykonywanie zrzutów ekranu. Test sprawdza, czy złośliwe oprogramowanie może wykonywać zrzuty ekranu podczas korzystania z bankowości internetowej.	✓ POZYTYWNY	✓ POZYTYWNY
Przeszukiwanie pamięci RAM. Test sprawdza, czy złośliwe oprogramowanie może wyodrębnić poufne informacje z pamięci RAM, np. numery kart kredytowych, hasła, loginy lub numery kont bankowych.	✗ NEGATYWNY	✗ NEGATYWNY
Wstrzykiwanie bibliotek DLL. Test sprawdza, czy możliwe jest wstrzykiwanie złośliwych plików DLL do procesów tzw. „bezpiecznej przeglądarki" lub „środowiska wirtualnego" lub procesów antywirusa. Używane metody: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest wstawienie kodu HTML i kodu JavaScript do stron internetowych.	✗ NEGATYWNY	✗ NEGATYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest przechwycenie poufnych informacji ze stron internetowych zabezpieczonych certyfikatem SSL.	✗ NEGATYWNY	✗ NEGATYWNY
Ukryty pulpit. Test sprawdza, czy złośliwe oprogramowanie może nawiązać zdalne połączenie z serwerem hackera podczas aktywnej sesji bankowej.	✓ POZYTYWNY	✓ POZYTYWNY
Modyfikowanie pliku HOSTS. Test sprawdza, czy złośliwe oprogramowanie może manipulować zawartością pliku HOSTS systemu Windows.	✗ NEGATYWNY	✗ NEGATYWNY
Wykrywanie trzynastu trojanów bankowych znalezionych in-the-wild w lutym 2019 roku.	POZYTYWNY: 13 / 13	

ZDANYCH TESTÓW: 7 / 11

Włączenie niektórych funkcji lub trybu bankowego pozwala uzyskać lepszy wynik.

Opis unikalnych składników ochrony bankowej, aby umożliwić lepsze zrozumienie, w jaki sposób technologia chroni użytkowników podczas aktywnej sesji bankowej.

G Data Total Protection to bardzo, bardzo rozbudowany pakiet chroniący przed atakami i zagrożeniami internetowymi. W samym centrum zabezpieczeń użytkownik znajdzie informacje podsumowujące dane z pozostałych modułów. Dla bezpieczeństwa najważniejszymi komponentami jest zapora sieciowa oraz ochrona antywirusowa obejmująca większość protokołów, w tym nowa technologia DeepRay. Bazując na wieloletnim doświadczeniu eksperci opracowali nowe metody wykrywania złośliwego kodu. Oprogramowanie może stwierdzić, które z kombinacji czynników są potencjalnie szkodliwe, np.: obecność instrukcji skoku w nagłówkach PE, stosunek ilości wykonywanego kodu do wielkości pliku, specyficzne metody kompresji pliku czy liczba importowanych funkcji systemowych. W tym aspekcie kompleksowość ochrony polega na pokryciu wszystkich protokołów, przez które użytkownik komunikuje się z Internetem. DeepRay stosuje uczenie maszynowe do wykrywania złośliwego kodu, niezależnie od ręcznie przeprowadzanych analiz przez specjalistów w tej dziedzinie. Pracownicy G Data opracowali samouczący się system oparty na maszynowym uczeniu, który wykrywa dobrze zakamuflowane złośliwe oprogramowanie. A więc DeepRay to technologia, w której zawarto metodę supervised learning, czyli oprogramowanie antywirusowe „nauczono" analizowania złośliwego kodu i kalkulowania ryzyka przy uwzględnieniu ponad 100 czynników. W kwestii zabezpieczeń G Data dostarcza wysokiej klasy oprogramowanie, które usatysfakcjonuje nawet geeków komputerowych.

Recommendacja AV-LAB AWARD GOOD+

Test ochrony bankowości internetowej

Nazwa produktu: Kaspersky Internet Security
Wersja: 19.0.0.1088
Data testu: luty 2019

Rodzaj testu	Ustawienia domyślne	Ustawienia zmodyfikowane i/lub tryb bankowy
Przechwytywanie schowka. Test sprawdza, czy złośliwe oprogramowanie może przechwytywać zawartość schowka systemowego i wysyłać informacje do serwera kontrolowanego przez hackera.	✗ NEGATYWNY	✓ POZYTYWNY (Włączony moduł Bezpieczne Pieniądze)
Podmiana schowka. Test sprawdza, czy złośliwe oprogramowanie może zmieniać zawartość schowka systemowego np. skopiowany numer konta bankowego na inny.	✗ NEGATYWNY	✓ POZYTYWNY (Włączony moduł Bezpieczne Pieniądze)
Rejestrowanie klawiatury. Test sprawdza, czy złośliwe oprogramowanie może rejestrować naciśnięcia klawiszy na klawiaturze podczas logowania do konta bankowego i wysyłać informacje na konto Gmail osoby atakującej.	✗ NEGATYWNY	✓ POZYTYWNY (Włączony moduł Bezpieczne Pieniądze)
Wykonywanie zrzutów ekranu. Test sprawdza, czy złośliwe oprogramowanie może wykonywać zrzuty ekranu podczas korzystania z bankowości internetowej.	✗ NEGATYWNY	✓ POZYTYWNY (Włączony moduł Bezpieczne Pieniądze)
Przeszukiwanie pamięci RAM. Test sprawdza, czy złośliwe oprogramowanie może wyodrębnić poufne informacje z pamięci RAM, np. numery kart kredytowych, hasła, loginy lub numery kont bankowych.	✗ NEGATYWNY	✓ POZYTYWNY (Włączony moduł Bezpieczne Pieniądze)
Wstrzykiwanie bibliotek DLL. Test sprawdza, czy możliwe jest wstrzykiwanie złośliwych plików DLL do procesów tzw. „bezpiecznej przeglądarki" lub „środowiska wirtualnego" lub procesów antywirusa. Używane metody: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest wstawienie kodu HTML i kodu JavaScript do stron internetowych.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest przechwycenie poufnych informacji ze stron internetowych zabezpieczonych certyfikatem SSL.	✓ POZYTYWNY	✓ POZYTYWNY
Ukryty pulpit. Test sprawdza, czy złośliwe oprogramowanie może nawiązać zdalne połączenie z serwerem hackera podczas aktywnej sesji bankowej.	✓ POZYTYWNY	✓ POZYTYWNY
Modyfikowanie pliku HOSTS. Test sprawdza, czy złośliwe oprogramowanie może manipulować zawartością pliku HOSTS systemu Windows.	✓ POZYTYWNY	✓ POZYTYWNY
Wykrywanie trzynastu trojanów bankowych znalezionych in-the-wild w lutym 2019 roku.	POZYTYWNY: 13 / 13	

Opis unikalnych składników ochrony bankowej, aby umożliwić lepsze zrozumienie, w jaki sposób technologia chroni użytkowników podczas aktywnej sesji bankowej.

Cechami wyróżniającymi produkt jest ochrona otwieranych i modyfikowanych plików, ochrona komunikatorów skanująca wiadomości w poszukiwaniu szkodliwych odnośników, a także ochrona poczty. Skanowanie stron internetowych pod kątem phishingu i złośliwych zasobów, w tym niebezpiecznych skryptów to kolejna wartość, na którą zwracamy uwagę. Bardzo ważnym modułem jest Bezpieczne Pieniądze. Ten moduł sugeruje otwieranie bezpiecznej przeglądarki odpornej na wstrzykiwanie złośliwych bibliotek DLL czy choćby odczytywanie poufnych informacji z pamięci RAM wprowadzonych do przeglądarki. Atakujący albo szkodliwe oprogramowanie nie może uzyskać uzyskania loginu i hasła lub zastąpienia zawartości (kwota, konto bankowe itp.) transakcji bankowych poprzez wyświetlanie na ekranie użytkownika fałszywych okien imitujących prawdziwą stronę internetową. Nie jest też w stanie robić zrzutów ekranu, ani rejestrować klawiatury i kliknięć myszy. Blokowane są również wszelkie próby wykonywania zrzutów ekranu, łącznie ze zrzutami całego obszaru pulpitu wykonywanymi przy użyciu funkcji API takich jak GDI, DirectX lub OpenGL. Kaspersky to niezwykle solidne oprogramowanie. Nie dość, że nie sprawia problemów z komputerami to chroni urządzenia na najwyższym poziomie. Posiada zaporę filtrującą aktywność sieciową. Ochronę kamery internetowej zapobiegającą śledzeni i moduł blokowania ataków sieciowych.

ZDANYCH TESTÓW: 11 / 11

Włączenie niektórych funkcji lub trybu bankowego pozwala uzyskać lepszy wynik.

Rekomendacja

THE INDEPENDENT ANTIVIRUS TESTS

Test ochrony bankowości internetowej

Nazwa produktu: mks_vir Internet Security
Wersja: 2019.02.14
Data testu: luty 2019

Rodzaj testu	Ustawienia domyślne	Ustawienia zmodyfikowane i/lub tryb bankowy
Przechwytywanie schowka. Test sprawdza, czy złośliwe oprogramowanie może przechwytywać zawartość schowka systemowego i wysyłać informacje do serwera kontrolowanego przez hackera.	✓ POZYTYWNY	✓ POZYTYWNY
Podmiana schowka. Test sprawdza, czy złośliwe oprogramowanie może zmieniać zawartość schowka systemowego np. skopiowany numer konta bankowego na inny.	✓ POZYTYWNY	✓ POZYTYWNY
Rejestrowanie klawiatury. Test sprawdza, czy złośliwe oprogramowanie może rejestrować naciśnięcia klawiszy na klawiaturze podczas logowania do konta bankowego i wysyłać informacje na konto Gmail osoby atakującej.	✓ POZYTYWNY	✓ POZYTYWNY
Wykonywanie zrzutów ekranu. Test sprawdza, czy złośliwe oprogramowanie może wykonywać zrzuty ekranu podczas korzystania z bankowości internetowej.	✓ POZYTYWNY	✓ POZYTYWNY
Przeszukiwanie pamięci RAM. Test sprawdza, czy złośliwe oprogramowanie może wyodrębnić poufne informacje z pamięci RAM, np. numery kart kredytowych, hasła, loginy lub numery kont bankowych.	✓ POZYTYWNY	✓ POZYTYWNY
Wstrzykiwanie bibliotek DLL. Test sprawdza, czy możliwe jest wstrzykiwanie złośliwych plików DLL do procesów tzw. „bezpiecznej przeglądarki" lub „środowiska wirtualnego" lub procesów antywirusa. Używane metody: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✗ NEGATYWNY	✓ POZYTYWNY (Włączony moduł Safe Browser)
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest wstawienie kodu HTML i kodu JavaScript do stron internetowych.	✗ NEGATYWNY	✗ NEGATYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest przechwycenie poufnych informacji ze stron internetowych zabezpieczonych certyfikatem SSL.	✗ NEGATYWNY	✗ NEGATYWNY
Ukryty pulpit. Test sprawdza, czy złośliwe oprogramowanie może nawiązać zdalne połączenie z serwerem hackera podczas aktywnej sesji bankowej.	✓ POZYTYWNY	✓ POZYTYWNY
Modyfikowanie pliku HOSTS. Test sprawdza, czy złośliwe oprogramowanie może manipulować zawartością pliku HOSTS systemu Windows.	✗ NEGATYWNY	✓ POZYTYWNY (Włączony moduł Safe Browser)
Wykrywanie trzynastu trojanów bankowych znalezionych in-the-wild w lutym 2019 roku.	POZYTYWNY: 13 / 13	

ZDANYCH TESTÓW: 9 / 11

Włączenie niektórych funkcji lub trybu bankowego pozwala uzyskać lepszy wynik.

Opis unikalnych składników ochrony bankowej, aby umożliwić lepsze zrozumienie, w jaki sposób technologia chroni użytkowników podczas aktywnej sesji bankowej.

Niezawodna przeglądarka mks_vir Safe Browser zapewnia wysoki poziom bezpieczeństwa w trakcie korzystania z zasobów Internetu, a zwłaszcza w trakcie operacji bankowych, płatniczych oraz wymagających podawania wrażliwych danych. Safe Browser ściśle współpracuje z pozostałymi modułami pakietu mks_vir i stale kontroluje poziom bezpieczeństwa systemu, nie dopuszczając do sytuacji, w których newralgiczne dane mogłyby trafić w niepowołane ręce. Producent zastosował ochronę w oparciu o „białe listy" procesów, co oznacza, że jeszcze przed włączeniem bezpiecznej przeglądarki sprawdzane są uruchomione procesy. Niektóre z nich mogą być szkodliwe i działać w ukryciu, oszukując ochronę antywirusową. Mks_vir wyprzedza autorów złośliwego oprogramowania i wyświetla procesy, które nie są zdefiniowane przez producenta jako bezpieczne. Decyzja, które z nich powinny być zamknięte, a które nie, jest uwarunkowana preferencjami użytkownika. Sposób korzystania z mks_vir Safe Browser jest następujący: wszystkie procesy, które znajdują się na wyświetlonej liście uruchomionych procesów, powinny zostać zamknięte. Tak na wszelki wypadek, aby niepotrzebne nie narażać się na ryzyko utraty pieniędzy czy przechwycenia poufnych informacji uwierzytelniających w systemie on-line.

Rekomendacja AV-LAB AWARD BEST++

THE INDEPENDENT ANTIVIRUS TESTS

Test ochrony bankowości internetowej

Nazwa produktu: Norton Security
Wersja: 22.5
Data testu: luty 2019

Rodzaj testu	Ustawienia domyślne	Ustawienia zmodyfikowane i/lub tryb bankowy
Przechwytywanie schowka. Test sprawdza, czy złośliwe oprogramowanie może przechwytywać zawartość schowka systemowego i wysyłać informacje do serwera kontrolowanego przez hackera.	✓ POZYTYWNY	✓ POZYTYWNY
Podmiana schowka. Test sprawdza, czy złośliwe oprogramowanie może zmieniać zawartość schowka systemowego np. skopiowany numer konta bankowego na inny.	✓ POZYTYWNY	✓ POZYTYWNY
Rejestrowanie klawiatury. Test sprawdza, czy złośliwe oprogramowanie może rejestrować naciśnięcia klawiszy na klawiaturze podczas logowania do konta bankowego i wysyłać informacje na konto Gmail osoby atakującej.	✓ POZYTYWNY	✓ POZYTYWNY
Wykonywanie zrzutów ekranu. Test sprawdza, czy złośliwe oprogramowanie może wykonywać zrzuty ekranu podczas korzystania z bankowości internetowej.	✓ POZYTYWNY	✓ POZYTYWNY
Przeszukiwanie pamięci RAM. Test sprawdza, czy złośliwe oprogramowanie może wyodrębnić poufne informacje z pamięci RAM, np. numery kart kredytowych, hasła, loginy lub numery kont bankowych.	✓ POZYTYWNY	✓ POZYTYWNY
Wstrzykiwanie bibliotek DLL. Test sprawdza, czy możliwe jest wstrzykiwanie złośliwych plików DLL do procesów tzw. „bezpiecznej przeglądarki" lub „środowiska wirtualnego" lub procesów antywirusa. Używane metody: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest wstawienie kodu HTML i kodu JavaScript do stron internetowych.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest przechwycenie poufnych informacji ze stron internetowych zabezpieczonych certyfikatem SSL.	✓ POZYTYWNY	✓ POZYTYWNY
Ukryty pulpit. Test sprawdza, czy złośliwe oprogramowanie może nawiązać zdalne połączenie z serwerem hackera podczas aktywnej sesji bankowej.	✓ POZYTYWNY	✓ POZYTYWNY
Modyfikowanie pliku HOSTS. Test sprawdza, czy złośliwe oprogramowanie może manipulować zawartością pliku HOSTS systemu Windows.	✓ POZYTYWNY	✓ POZYTYWNY
Wykrywanie trzynastu trojanów bankowych znalezionych in-the-wild w lutym 2019 roku.	POZYTYWNY: 13 / 13	

Opis unikalnych składników ochrony bankowej, aby umożliwić lepsze zrozumienie, w jaki sposób technologia chroni użytkowników podczas aktywnej sesji bankowej.

Norton Security to bardzo rozbudowany pakiet wykorzystujący wykrywanie heurystyczne i proaktywne, zapewniające skuteczną ochronę poprzez wykrywanie podejrzanego działania aplikacji, jak i podczas pobierania mało popularnych plików. W rozwiązaniu dobrze sprawdza się ochrona przed nieznanymi zagrożeniami, która bazuje na reputacji plików. Norton wykrywając destrukcyjny kod gwarantuje bezpieczeństwo na wyższym poziomie, chroniąc przed nieznanymi jeszcze zagrożeniami, dla których nie zostały wydane sygnatury. Zapora internetowa to bardzo użyteczny moduł. Blokuje ataki hakerów i nieautoryzowany ruch poprzez monitorowanie komunikacji odbywającej się pomiędzy komputerami w sieci. Informuje o połączeniach pochodzących z innych urządzeń, jak również połączeniach wykonywanych przez aplikacje znajdujące się w systemie użytkownika. Dodatkowym atutem jest fakt, że zamyka nieaktywne porty, chroniąc przed skanowaniem portów. Firewall monitoruje ruch sieciowy, zarówno przychodzący, jak również wychodzący i porównuje przekazywane informacje z bazami sygnatur ataków. Sygnatury te zawierają informacje pozwalające wykryć atak wykorzystujący luki w oprogramowaniu lub systemie operacyjnym. W momencie, kiedy takie dane zostaną wykryte przez moduł, automatycznie przerywane jest połączenie z hostem, a otrzymany pakiet zostaje odrzucony.

ZDANYCH TESTÓW: **11 / 11**

Włączenie niektórych funkcji lub trybu bankowego nie miało wpływu na lepszy wynik.

Rekomendacja AV LAB AWARD BEST+++

THE INDEPENDENT ANTIVIRUS TESTS

Test ochrony bankowości internetowej

Nazwa produktu: Panda Dome Advanced
Wersja: 18.07.00
Data testu: luty 2019

Rodzaj testu	Ustawienia domyślne	Ustawienia zmodyfikowane i/lub tryb bankowy
Przechwytywanie schowka. Test sprawdza, czy złośliwe oprogramowanie może przechwytywać zawartość schowka systemowego i wysyłać informacje do serwera kontrolowanego przez hackera.	✗ NEGATYWNY	✓ POZYTYWNY (Włączony moduł Kontrola Aplikacji)
Podmiana schowka. Test sprawdza, czy złośliwe oprogramowanie może zmieniać zawartość schowka systemowego np. skopiowany numer konta bankowego na inny.	✗ NEGATYWNY	✓ POZYTYWNY (Włączony moduł Kontrola Aplikacji)
Rejestrowanie klawiatury. Test sprawdza, czy złośliwe oprogramowanie może rejestrować naciśnięcia klawiszy na klawiaturze podczas logowania do konta bankowego i wysyłać informacje na konto Gmail osoby atakującej.	✗ NEGATYWNY	✓ POZYTYWNY (Włączony moduł Kontrola Aplikacji)
Wykonywanie zrzutów ekranu. Test sprawdza, czy złośliwe oprogramowanie może wykonywać zrzuty ekranu podczas korzystania z bankowości internetowej.	✗ NEGATYWNY	✓ POZYTYWNY (Włączony moduł Kontrola Aplikacji)
Przeszukiwanie pamięci RAM. Test sprawdza, czy złośliwe oprogramowanie może wyodrębnić poufne informacje z pamięci RAM, np. numery kart kredytowych, hasła, loginy lub numery kont bankowych.	✗ NEGATYWNY	✓ POZYTYWNY (Włączony moduł Kontrola Aplikacji)
Wstrzykiwanie bibliotek DLL. Test sprawdza, czy możliwe jest wstrzykiwanie złośliwych plików DLL do procesów tzw. „bezpiecznej przeglądarki" lub „środowiska wirtualnego" lub procesów antywirusa. Używane metody: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest wstawienie kodu HTML i kodu JavaScript do stron internetowych.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest przechwycenie poufnych informacji ze stron internetowych zabezpieczonych certyfikatem SSL.	✓ POZYTYWNY	✓ POZYTYWNY
Ukryty pulpit. Test sprawdza, czy złośliwe oprogramowanie może nawiązać zdalne połączenie z serwerem hackera podczas aktywnej sesji bankowej.	✓ POZYTYWNY	✓ POZYTYWNY
Modyfikowanie pliku HOSTS. Test sprawdza, czy złośliwe oprogramowanie może manipulować zawartością pliku HOSTS systemu Windows.	✗ NEGATYWNY	✓ POZYTYWNY (Włączony moduł Kontrola Aplikacji)
Wykrywanie trzynastu trojanów bankowych znalezionych in-the-wild w lutym 2019 roku.	POZYTYWNY: 13 / 13	

Opis unikalnych składników ochrony bankowej, aby umożliwić lepsze zrozumienie, w jaki sposób technologia chroni użytkowników podczas aktywnej sesji bankowej.

W oprogramowaniu Panda Dome znajduje się bardzo istotny moduł do blokowania zagrożeń w oparciu o zachowanie i analizę heurystyczną, a także wykrywanie potencjalnie niepożądanych aplikacji. Na plus zaliczamy monitorowanie adresów URL, do których uzyskuje dostęp uruchomiony proces. To bardzo ważne w kontekście bezplikowej infekcji oraz wszystkich innych złośliwych plików korzystających z wiersza poleceń. Jako że detekcja nieznanych zagrożeń realizowana jest w chmurze, antywirus Panda Dome może o 30 sekund opóźnić uruchamianie programów, co do których nie może od razu uzyskać informacji o statusie bezpieczeństwa. Bardzo ważnym składnikiem ochrony jest zapora sieciowa, która zabezpiecza urządzenie przed większością znanych ataków. Jednak w kontekście nowych trojanów bankowych najważniejszym modułem (domyślnie wyłączony) jest kontrola aplikacji, która tworzy bezpieczne i zamknięte środowisko. Zatem jest to idealna dodatkowa warstwa ochrony przed zagrożeniami 0-day. Kontrola aplikacji pozwala nie tylko skonfigurować te programy, które można uruchamiać na komputerze, ale także ustawić akcje do wykonania, jeżeli nieznany program spróbuje się uruchomić. W ten sposób komponent może bezpośrednio zablokować wykonanie programu lub poprosić o potwierdzenie użytkownika przed przystąpieniem do uruchomienia nieznanego programu.

ZDANYCH TESTÓW: **11 / 11**

Włączenie niektórych funkcji lub trybu bankowego pozwala uzyskać lepszy wynik.

Rekomendacja

AWARD BEST+++

THE INDEPENDENT ANTIVIRUS TESTS

Quick Heal
Security Simplified

Test ochrony bankowości internetowej

Nazwa produktu: Quick Heal Total Security
Wersja: 18.00
Data testu: luty 2019

Rodzaj testu	Ustawienia domyślne	Ustawienia zmodyfikowane i/lub tryb bankowy
Przechwytywanie schowka. Test sprawdza, czy złośliwe oprogramowanie może przechwytywać zawartość schowka systemowego i wysyłać informacje do serwera kontrolowanego przez hackera.	✗ NEGATYWNY	✓ POZYTYWNY
Podmiana schowka. Test sprawdza, czy złośliwe oprogramowanie może zmieniać zawartość schowka systemowego np. skopiowany numer konta bankowego na inny.	✗ NEGATYWNY	✓ POZYTYWNY
Rejestrowanie klawiatury. Test sprawdza, czy złośliwe oprogramowanie może rejestrować naciśnięcia klawiszy na klawiaturze podczas logowania do konta bankowego i wysyłać informacje na konto Gmail osoby atakującej.	✗ NEGATYWNY	✓ POZYTYWNY
Wykonywanie zrzutów ekranu. Test sprawdza, czy złośliwe oprogramowanie może wykonywać zrzuty ekranu podczas korzystania z bankowości internetowej.	✗ NEGATYWNY	✓ POZYTYWNY
Przeszukiwanie pamięci RAM. Test sprawdza, czy złośliwe oprogramowanie może wyodrębnić poufne informacje z pamięci RAM, np. numery kart kredytowych, hasła, loginy lub numery kont bankowych.	✗ NEGATYWNY	✗ NEGATYWNY
Wstrzykiwanie bibliotek DLL. Test sprawdza, czy możliwe jest wstrzykiwanie złośliwych plików DLL do procesów tzw. „bezpiecznej przeglądarki" lub „środowiska wirtualnego" lub procesów antywirusa. Używane metody: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest wstawienie kodu HTML i kodu JavaScript do stron internetowych.	✗ NEGATYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest przechwycenie poufnych informacji ze stron internetowych zabezpieczonych certyfikatem SSL.	✗ NEGATYWNY	✓ POZYTYWNY
Ukryty pulpit. Test sprawdza, czy złośliwe oprogramowanie może nawiązać zdalne połączenie z serwerem hackera podczas aktywnej sesji bankowej.	✓ POZYTYWNY	✓ POZYTYWNY
Modyfikowanie pliku HOSTS. Test sprawdza, czy złośliwe oprogramowanie może manipulować zawartością pliku HOSTS systemu Windows.	✗ NEGATYWNY	✗ NEGATYWNY
Wykrywanie trzynastu trojanów bankowych znalezionych in-the-wild w lutym 2019 roku.	POZYTYWNY: 13 / 13	

Opis unikalnych składników ochrony bankowej, aby umożliwić lepsze zrozumienie, w jaki sposób technologia chroni użytkowników podczas aktywnej sesji bankowej.

Co bardzo istotne, bezpieczna bankowość w pakiecie Quick Heal nie ogranicza się tylko do modułu wirtualnego pulpitu. Znajdujemy tu ochronę m.in. przed podmianą adresów DNS. Przejmując kontrolę nad adresami DNS osoba nieuprawniona mogła odszyfrowywać komunikację SSL. Korzystanie z Bezpiecznej Bankowości w oprogramowaniu Quick Heal zapobiega takim atakom. Istotnym elementem ochrony jest wbudowany moduł IPS/IDS. W zaawansowanych atakach, gdzie wykorzystuje się bardziej wyszukane metody niż socjotechnikę (są to głównie ataki na niezabezpieczone i niezaktualizowane protokoły np. SMB), to właśnie IPS/IDS odgrywają bardzo ważną rolę w zabezpieczeniu. Dwukierunkowy firewall zawierający system wykrywania intruzów może wykryć ataki zatruwające tablice ARP, fałszywe zapytania PING, ataki modyfikujące wpisy DNS, ataki na luki na protokoły SMB, RPC, RDP i ataki skanujące porty. Osłania to sieć domową przed złośliwym oprogramowaniem i zatrzymuje malware zanim zainstaluje się w systemie. Zabezpiecza przed pobraniem niebezpiecznego pliku m.in. przez CMD.exe lub PowerShell.exe (są to procesy systemowe bardzo często wykorzystywane w kodzie szkodliwego oprogramowania).

ZDANYCH TESTÓW: **9 / 11**

Włączenie niektórych funkcji lub trybu bankowego nie miało wpływu na lepszy wynik.

Rekomendacja AV LAB AWARD BEST++

Test ochrony bankowości internetowej

Nazwa produktu: Sophos Intercept X
Wersja: 2.0.12
Data testu: luty 2019

Rodzaj testu	Ustawienia domyślne	Ustawienia zmodyfikowane i/lub tryb bankowy
Przechwytywanie schowka. Test sprawdza, czy złośliwe oprogramowanie może przechwytywać zawartość schowka systemowego i wysyłać informacje do serwera kontrolowanego przez hackera.	✓ POZYTYWNY	✓ POZYTYWNY
Podmiana schowka. Test sprawdza, czy złośliwe oprogramowanie może zmieniać zawartość schowka systemowego np. skopiowany numer konta bankowego na inny.	✓ POZYTYWNY	✓ POZYTYWNY
Rejestrowanie klawiatury. Test sprawdza, czy złośliwe oprogramowanie może rejestrować naciśnięcia klawiszy na klawiaturze podczas logowania do konta bankowego i wysyłać informacje na konto Gmail osoby atakującej.	✓ POZYTYWNY	✓ POZYTYWNY
Wykonywanie zrzutów ekranu. Test sprawdza, czy złośliwe oprogramowanie może wykonywać zrzuty ekranu podczas korzystania z bankowości internetowej.	✓ POZYTYWNY	✓ POZYTYWNY
Przeszukiwanie pamięci RAM. Test sprawdza, czy złośliwe oprogramowanie może wyodrębnić poufne informacje z pamięci RAM, np. numery kart kredytowych, hasła, loginy lub numery kont bankowych.	✓ POZYTYWNY	✓ POZYTYWNY
Wstrzykiwanie bibliotek DLL. Test sprawdza, czy możliwe jest wstrzykiwanie złośliwych plików DLL do procesów tzw. „bezpiecznej przeglądarki" lub „środowiska wirtualnego" lub procesów antywirusa. Używane metody: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest wstawienie kodu HTML i kodu JavaScript do stron internetowych.	✗ NEGATYWNY	✓ POZYTYWNY (Blokowanie połączeń przychodzących)
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest przechwycenie poufnych informacji ze stron internetowych zabezpieczonych certyfikatem SSL.	✗ NEGATYWNY	✓ POZYTYWNY (Blokowanie połączeń przychodzących)
Ukryty pulpit. Test sprawdza, czy złośliwe oprogramowanie może nawiązać zdalne połączenie z serwerem hackera podczas aktywnej sesji bankowej.	✓ POZYTYWNY	✓ POZYTYWNY
Modyfikowanie pliku HOSTS. Test sprawdza, czy złośliwe oprogramowanie może manipulować zawartością pliku HOSTS systemu Windows.	✓ POZYTYWNY	✓ POZYTYWNY
Wykrywanie trzynastu trojanów bankowych znalezionych in-the-wild w lutym 2019 roku.	POZYTYWNY: 13 / 13	

ZDANYCH TESTÓW: 11 / 11

Włączenie niektórych funkcji lub trybu bankowego pozwala uzyskać lepszy wynik.

Opis unikalnych składników ochrony bankowej, aby umożliwić lepsze zrozumienie, w jaki sposób technologia chroni użytkowników podczas aktywnej sesji bankowej.

Podobnie jak w rozwiązaniu dla klientów indywidualnych Sophos Intercept X wykorzystuje maszynowe uczenie do wykrywania nieznanych zagrożeń. Ponadto dostępność dodatkowych modułów i konfiguracji jest znacznie większa, dlatego nie bez znaczenia rozwiązanie firmy Sophos spełnia wymagania stawiane przez duże banki, korporacje i instytucje rządowe. Niezwykle dużą rolę w zabezpieczeniu stacji roboczych przed nowymi zagrożeniami 0-day odgrywa ostrzeganie przed plikami o niskiej reputacji, przy czym nie ma znaczenie rozszerzenie pobieranego pliku. Wyspecjalizowany trojan bankowy napisany pod konkretną instytucję z pewnością spowoduje zaalarmowanie administratora. Wszystkie zagrożenia są automatycznie usuwane, a informacja o wykrytej podejrzanej aktywności jest wysyłana ze stacji roboczych do Sophos Central. Ustawienia polityk bezpieczeństwa przygotowane przez producenta mogą być zmienione na bardziej agresywne. Nie należy wyłączać już domyślnie aktywowanych funkcjonalności, ponieważ może to wpłynąć na pogorszenie skuteczność. Sophos Intercept X oferuje kompleksową ochronę przed zagrożeniami bankowymi, jednakże ustawienia polityki dla komputerów, z których korzystają pracownicy podczas bankowości online, powinny zwrócić szczególną uwagę administratora.

Rekomendacja

THE INDEPENDENT ANTIVIRUS TESTS

SOPHOS HOME

Test ochrony bankowości internetowej

Nazwa produktu: Sophos Home Premium
Wersja: 2.0.12
Data testu: luty 2019

Rodzaj testu	Ustawienia domyślne	Ustawienia zmodyfikowane i/lub tryb bankowy
Przechwytywanie schowka. Test sprawdza, czy złośliwe oprogramowanie może przechwytywać zawartość schowka systemowego i wysyłać informacje do serwera kontrolowanego przez hackera.	✓ POZYTYWNY	✓ POZYTYWNY
Podmiana schowka. Test sprawdza, czy złośliwe oprogramowanie może zmieniać zawartość schowka systemowego np. skopiowany numer konta bankowego na inny.	✓ POZYTYWNY	✓ POZYTYWNY
Rejestrowanie klawiatury. Test sprawdza, czy złośliwe oprogramowanie może rejestrować naciśnięcia klawiszy na klawiaturze podczas logowania do konta bankowego i wysyłać informacje na konto Gmail osoby atakującej.	✓ POZYTYWNY	✓ POZYTYWNY
Wykonywanie zrzutów ekranu. Test sprawdza, czy złośliwe oprogramowanie może wykonywać zrzuty ekranu podczas korzystania z bankowości internetowej.	✓ POZYTYWNY	✓ POZYTYWNY
Przeszukiwanie pamięci RAM. Test sprawdza, czy złośliwe oprogramowanie może wyodrębnić poufne informacje z pamięci RAM, np. numery kart kredytowych, hasła, loginy lub numery kont bankowych.	✓ POZYTYWNY	✓ POZYTYWNY
Wstrzykiwanie bibliotek DLL. Test sprawdza, czy możliwe jest wstrzykiwanie złośliwych plików DLL do procesów tzw. „bezpiecznej przeglądarki" lub „środowiska wirtualnego" lub procesów antywirusa. Używane metody: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest wstawienie kodu HTML i kodu JavaScript do stron internetowych.	✗ NEGATYWNY	✗ NEGATYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest przechwycenie poufnych informacji ze stron internetowych zabezpieczonych certyfikatem SSL.	✗ NEGATYWNY	✗ NEGATYWNY
Ukryty pulpit. Test sprawdza, czy złośliwe oprogramowanie może nawiązać zdalne połączenie z serwerem hackera podczas aktywnej sesji bankowej.	✓ POZYTYWNY	✓ POZYTYWNY
Modyfikowanie pliku HOSTS. Test sprawdza, czy złośliwe oprogramowanie może manipulować zawartością pliku HOSTS systemu Windows.	✓ POZYTYWNY	✓ POZYTYWNY
Wykrywanie trzynastu trojanów bankowych znalezionych in-the-wild w lutym 2019 roku.	POZYTYWNY: 13 / 13	

Opis unikalnych składników ochrony bankowej, aby umożliwić lepsze zrozumienie, w jaki sposób technologia chroni użytkowników podczas aktywnej sesji bankowej.

Sophos Home Premium wykorzystuje uczenie maszynowe w technologii Deep Learning do wykrywania zagrożeń, czyli te same rozwiązania, z których korzystają największe światowe przedsiębiorstwa chroniące swoje interesy za pośrednictwem rozwiązań Sophos. Oprogramowanie używa sztucznej inteligencji, która może wykrywać i blokować zarówno znane, jak i nowe złośliwe oprogramowanie. Sophos Home Premium oferuje ochronę w czasie rzeczywistym — powstrzymuje cyberprzestępców przed wykorzystywaniem luk w zaufanych aplikacjach i systemach operacyjnych lub kradzieżą danych uwierzytelniających. W kwestii ochrony bankowości internetowej rozwiązanie brytyjskiej firmy chroni dane bankowe i karty kredytowe przed przechwyceniem przez osoby trzecie. Sophos Home szyfruje naciśnięcia klawiszy w celu zapewnienia dodatkowej warstwy bezpieczeństwa. Dzisiaj zdecydowana większość transakcji bankowych odbywa się w Internecie. Sophos nakłada dodatkowe zabezpieczenia na przeglądarkę. Oprócz szyfrowania klawiszy mamy stale aktywną ochronę przed exploitami, detekcję programów łączących się z zewnętrznymi hostami i ostrzeganie przed nieuprawnionym wstrzykiwaniem kodu do przeglądarki. Wszystkie te technologie działają automatycznie i domyślnie są włączone.

ZDANYCH TESTÓW: **9 / 11**

Włączenie niektórych funkcji lub trybu bankowego nie miało wpływu na lepszy wynik.

Rekomendacja AV-LAB AWARD BEST++

THE INDEPENDENT ANTIVIRUS TESTS

Test ochrony bankowości internetowej

Nazwa produktu: SpyShelter Firewall
Wersja: 11.4
Data testu: luty 2019

Rodzaj testu	Ustawienia domyślne	Ustawienia zmodyfikowane i/lub tryb bankowy
Przechwytywanie schowka. Test sprawdza, czy złośliwe oprogramowanie może przechwytywać zawartość schowka systemowego i wysyłać informacje do serwera kontrolowanego przez hackera.	✓ POZYTYWNY	✓ POZYTYWNY
Podmiana schowka. Test sprawdza, czy złośliwe oprogramowanie może zmieniać zawartość schowka systemowego np. skopiowany numer konta bankowego na inny.	✓ POZYTYWNY	✓ POZYTYWNY
Rejestrowanie klawiatury. Test sprawdza, czy złośliwe oprogramowanie może rejestrować naciśnięcia klawiszy na klawiaturze podczas logowania do konta bankowego i wysyłać informacje na konto Gmail osoby atakującej.	✓ POZYTYWNY	✓ POZYTYWNY
Wykonywanie zrzutów ekranu. Test sprawdza, czy złośliwe oprogramowanie może wykonywać zrzuty ekranu podczas korzystania z bankowości internetowej.	✓ POZYTYWNY	✓ POZYTYWNY
Przeszukiwanie pamięci RAM. Test sprawdza, czy złośliwe oprogramowanie może wyodrębnić poufne informacje z pamięci RAM, np. numery kart kredytowych, hasła, loginy lub numery kont bankowych.	✓ POZYTYWNY	✓ POZYTYWNY
Wstrzykiwanie bibliotek DLL. Test sprawdza, czy możliwe jest wstrzykiwanie złośliwych plików DLL do procesów tzw. „bezpiecznej przeglądarki" lub „środowiska wirtualnego" lub procesów antywirusa. Używane metody: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest wstawienie kodu HTML i kodu JavaScript do stron internetowych.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest przechwycenie poufnych informacji ze stron internetowych zabezpieczonych certyfikatem SSL.	✓ POZYTYWNY	✓ POZYTYWNY
Ukryty pulpit. Test sprawdza, czy złośliwe oprogramowanie może nawiązać zdalne połączenie z serwerem hackera podczas aktywnej sesji bankowej.	✓ POZYTYWNY	✓ POZYTYWNY
Modyfikowanie pliku HOSTS. Test sprawdza, czy złośliwe oprogramowanie może manipulować zawartością pliku HOSTS systemu Windows.	✓ POZYTYWNY	✓ POZYTYWNY
Wykrywanie trzynastu trojanów bankowych znalezionych in-the-wild w lutym 2019 roku.	POZYTYWNY: 13 / 13	

ZDANYCH TESTÓW: 11 / 11

Włączenie niektórych funkcji lub trybu bankowego nie miało wpływu na lepszy wynik.

Opis unikalnych składników ochrony bankowej, aby umożliwić lepsze zrozumienie, w jaki sposób technologia chroni użytkowników podczas aktywnej sesji bankowej.

Oprogramowanie stanowi zapobiegawcze podejście do bezpieczeństwa i wykorzystuje zaawansowane techniki wykrywania i blokowania prób naruszenia danych. Działania defensywne mogą obejmować ostrzeganie użytkownika za pomocą komunikatów jak i skanera w chmurze. SpyShelter nie blokuje szkodników z wykorzystaniem opracowanych szczepionek lub heurystycznych metod. Rozwiązanie monitoruje wszystkie procesy i usługi systemowe, które tworzą bezpieczną przestrzeń roboczą zwaną systemem operacyjnym. SpyShelter Firewall gwarantuje ochronę systemu i danych przed całym spektrum malware: od robaków, spyware, po keyloggery i ransomware. Jednak nie zabezpiecza aktywów użytkownika w taki sam sposób, jak robią to inne, wyspecjalizowane rozwiązania wykrywające anomalie w oparciu o heurystykę. Podstawową różnicą pomiędzy nimi jest sposób wykrywania nieprawidłowości, czyli odstępstw od normalnego działania procesów, systemu operacyjnego i zainstalowanych programów. Dla oprogramowania SpyShelter Firewall zagrożenie takie jak keylogger, spyware czy ransomware nie jest wirusem w tradycyjnym tego słowa znaczeniu, a ciągiem nierozłącznych zdarzeń (akcji), o których działaniu powiadamia użytkownika. SpyShelter Firewall nie usuwa automatycznie złośliwego oprogramowania, może rozpoznawać pliki za pomocą zintegrowanego skanera antywirusowego w chmurze Jotti (lub innego — posiada możliwość konfiguracji zewnętrznego skanera plików). HIPS to tylko jedna warstwa obrony, która wchodzi w skład rozwiązania SpyShelter Firewall.

Rekomendacja

Test ochrony bankowości internetowej

Nazwa produktu: Trend Micro Maximum Security
Wersja: 15.0.1212
Data testu: luty 2019

Rodzaj testu	Ustawienia domyślne	Ustawienia zmodyfikowane i/lub tryb bankowy
Przechwytywanie schowka. Test sprawdza, czy złośliwe oprogramowanie może przechwytywać zawartość schowka systemowego i wysyłać informacje do serwera kontrolowanego przez hackera.	✗ NEGATYWNY	✓ POZYTYWNY (Poziom ochrony Hypersensitive Protection Level)
Podmiana schowka. Test sprawdza, czy złośliwe oprogramowanie może zmieniać zawartość schowka systemowego np. skopiowany numer konta bankowego na inny.	✗ NEGATYWNY	✓ POZYTYWNY (Poziom ochrony Hypersensitive Protection Level)
Rejestrowanie klawiatury. Test sprawdza, czy złośliwe oprogramowanie może rejestrować naciśnięcia klawiszy na klawiaturze podczas logowania do konta bankowego i wysyłać informacje na konto Gmail osoby atakującej.	✓ POZYTYWNY	✓ POZYTYWNY
Wykonywanie zrzutów ekranu. Test sprawdza, czy złośliwe oprogramowanie może wykonywać zrzuty ekranu podczas korzystania z bankowości internetowej.	✗ NEGATYWNY	✓ POZYTYWNY (Poziom ochrony Hypersensitive Protection Level)
Przeszukiwanie pamięci RAM. Test sprawdza, czy złośliwe oprogramowanie może wyodrębnić poufne informacje z pamięci RAM, np. numery kart kredytowych, hasła, loginy lub numery kont bankowych.	✗ NEGATYWNY	✓ POZYTYWNY (Poziom ochrony Hypersensitive Protection Level)
Wstrzykiwanie bibliotek DLL. Test sprawdza, czy możliwe jest wstrzykiwanie złośliwych plików DLL do procesów tzw. „bezpiecznej przeglądarki" lub „środowiska wirtualnego" lub procesów antywirusa. Używane metody: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest wstawienie kodu HTML i kodu JavaScript do stron internetowych.	✗ NEGATYWNY	✗ NEGATYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest przechwycenie poufnych informacji ze stron internetowych zabezpieczonych certyfikatem SSL.	✗ NEGATYWNY	✗ NEGATYWNY
Ukryty pulpit. Test sprawdza, czy złośliwe oprogramowanie może nawiązać zdalne połączenie z serwerem hackera podczas aktywnej sesji bankowej.	✓ POZYTYWNY	✓ POZYTYWNY
Modyfikowanie pliku HOSTS. Test sprawdza, czy złośliwe oprogramowanie może manipulować zawartością pliku HOSTS systemu Windows.	✓ POZYTYWNY	✓ POZYTYWNY
Wykrywanie trzynastu trojanów bankowych znalezionych in-the-wild w lutym 2019 roku.	POZYTYWNY: 13 / 13	

ZDANYCH TESTÓW: **9 / 11**

Włączenie niektórych funkcji lub trybu bankowego pozwala uzyskać lepszy wynik.

Opis unikalnych składników ochrony bankowej, aby umożliwić lepsze zrozumienie, w jaki sposób technologia chroni użytkowników podczas aktywnej sesji bankowej.

Trend Micro wykorzystuje własne technologie lokalne do ochrony przed malware. Moduł antywirusowy analizuje informacje na temat każdego pliku, który można otworzyć, zapisać lub pobrać. Jeśli plik zawiera w sobie złośliwy kod to antywirus za pomocą sygnatur lub analizy heurystycznej będzie próbował plik naprawić lub usunąć. W przypadku identyfikacji zagrożenia jako spyware, Trend Micro automatycznie je usuwa. Ochrona antywirusowa jest wspierana przez skanowanie w chmurze. Trend Micro Smart Protection Network, aby pomóc w rozwoju ochrony przed nowymi zagrożeniami, automatycznie koreluje informacje dotyczące zagrożeń bezpieczeństwa, znajdujące się na milionach komputerów na całym świecie. Im więcej osób uczestniczy w tym projekcie, tym bardziej efektywna jest sieć. Smart Protection Network gromadzi ponad 6 terabajtów danych zagrożeń każdego dnia. Dane te reprezentują coraz bardziej rozszerzające się wektory zagrożeń, w tym adresy URL, IP, domeny, pliki, ruch sieciowy, serwery C&C. W bankowości internetowej Trend Micro umożliwia bezpieczny dostęp do witryn bankowych lub sklepów za pomocą domyślnej przeglądarki, dzięki funkcji Pay Gurd. Po zainstalowaniu automatycznie tworzy ikonę skrótu na pulpicie, która wywołuje domyślną przeglądarkę i zapewnia bezpieczeństwo potrzebne do internetowych przelewów.

Rekomendacja

Test ochrony bankowości internetowej

Nazwa produktu: Webroot SecureAnywhere Antivirus
Wersja: 9.0.24.49
Data testu: luty 2019

Rodzaj testu	Ustawienia domyślne	Ustawienia zmodyfikowane i/lub tryb bankowy
Przechwytywanie schowka. Test sprawdza, czy złośliwe oprogramowanie może przechwytywać zawartość schowka systemowego i wysyłać informacje do serwera kontrolowanego przez hackera.	✗ NEGATYWNY	✓ POZYTYWNY (Włączenie heurystyki w trybie Whitelist Mode)
Podmiana schowka. Test sprawdza, czy złośliwe oprogramowanie może zmieniać zawartość schowka systemowego np. skopiowany numer konta bankowego na inny.	✗ NEGATYWNY	✓ POZYTYWNY (Włączenie heurystyki w trybie Whitelist Mode)
Rejestrowanie klawiatury. Test sprawdza, czy złośliwe oprogramowanie może rejestrować naciśnięcia klawiszy na klawiaturze podczas logowania do konta bankowego i wysyłać informacje na konto Gmail osoby atakującej.	✗ NEGATYWNY	✓ POZYTYWNY (Włączenie heurystyki w trybie Whitelist Mode)
Wykonywanie zrzutów ekranu. Test sprawdza, czy złośliwe oprogramowanie może wykonywać zrzuty ekranu podczas korzystania z bankowości internetowej.	✗ NEGATYWNY	✓ POZYTYWNY (Włączenie heurystyki w trybie Whitelist Mode)
Przeszukiwanie pamięci RAM. Test sprawdza, czy złośliwe oprogramowanie może wyodrębnić poufne informacje z pamięci RAM, np. numery kart kredytowych, hasła, loginy lub numery kont bankowych.	✗ NEGATYWNY	✓ POZYTYWNY (Włączenie heurystyki w trybie Whitelist Mode)
Wstrzykiwanie bibliotek DLL. Test sprawdza, czy możliwe jest wstrzykiwanie złośliwych plików DLL do procesów tzw. „bezpiecznej przeglądarki" lub „środowiska wirtualnego" lub procesów antywirusa. Używane metody: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ POZYTYWNY	✓ POZYTYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest wstawienie kodu HTML i kodu JavaScript do stron internetowych.	✗ NEGATYWNY	✗ NEGATYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest przechwycenie poufnych informacji ze stron internetowych zabezpieczonych certyfikatem SSL.	✗ NEGATYWNY	✗ NEGATYWNY
Ukryty pulpit. Test sprawdza, czy złośliwe oprogramowanie może nawiązać zdalne połączenie z serwerem hackera podczas aktywnej sesji bankowej.	✓ POZYTYWNY	✓ POZYTYWNY
Modyfikowanie pliku HOSTS. Test sprawdza, czy złośliwe oprogramowanie może manipulować zawartością pliku HOSTS systemu Windows.	✓ POZYTYWNY	✓ POZYTYWNY
Wykrywanie trzynastu trojanów bankowych znalezionych in-the-wild w lutym 2019 roku.	POZYTYWNY: 13 / 13	

ZDANYCH TESTÓW: **9 / 11**

Włączenie niektórych funkcji lub trybu bankowego pozwala uzyskać lepszy wynik.

Opis unikalnych składników ochrony bankowej, aby umożliwić lepsze zrozumienie, w jaki sposób technologia chroni użytkowników podczas aktywnej sesji bankowej.

Produkty Webroot w pełni wykorzystują potencjał chmury obliczeniowej. Agent antywirusowy nie pobiera sygnatur na dysk lokalny. Waga programu po instalacji to około 4MB. Skanowanie plików odbywa się na serwerach producenta, dzięki czemu udało się osiągnąć dobrą wydajność. W kwestii ochrony bankowości internetowej Webroot posiada wszystko to, czego można spodziewać się po nowoczesnym oprogramowaniu do zwalczania internetowej przestępczości. Webroot wskazuje na kilkanaście rodzajów ataków, przed którymi chroni: kradzieżą plików cookie i danymi internetowymi, atakami man-in-the-middle, keyloggerami, wyodrębnianiem schowka systemowego, atakami man-in-the-browser, robieniem zrzutów ekranów przez złośliwe oprogramowanie i blokowaniem podejrzanych procesów, które mogą uzyskiwać dostęp do przeglądarki. Podejrzane aplikacje są monitorowane na czas działania i w razie potrzeby blokowane. Kontrolowane procesy ciągle mają dostęp do Internetu, więc skradzionych danych z komputera nie da się odzyskać. Zastosowane ustawienia domyślne są skonfigurowane pod nietechnicznego użytkownika, w związku z tym nie są najlepsze.

Rekomendacja AV LAB AWARD BEST++

THE INDEPENDENT ANTIVIRUS TESTS

Test ochrony bankowości internetowej

Nazwa produktu: Windows Defender
Data testu: luty 2019

Rodzaj testu	Ustawienia domyślne (Chrome i włączona zapora sieciowa)	Ustawienia zmodyfikowane (EDGE i Windows Defender SmartScreen)
Przechwytywanie schowka. Test sprawdza, czy złośliwe oprogramowanie może przechwytywać zawartość schowka systemowego i wysyłać informacje do serwera kontrolowanego przez hackera.	✓ POZYTYWNY	✓ POZYTYWNY
Podmiana schowka. Test sprawdza, czy złośliwe oprogramowanie może zmieniać zawartość schowka systemowego np. skopiowany numer konta bankowego na inny.	✗ NEGATYWNY	✗ NEGATYWNY
Rejestrowanie klawiatury. Test sprawdza, czy złośliwe oprogramowanie może rejestrować naciśnięcia klawiszy na klawiaturze podczas logowania do konta bankowego i wysyłać informacje na konto Gmail osoby atakującej.	✗ NEGATYWNY	✗ NEGATYWNY
Wykonywanie zrzutów ekranu. Test sprawdza, czy złośliwe oprogramowanie może wykonywać zrzuty ekranu podczas korzystania z bankowości internetowej.	✗ NEGATYWNY	✗ NEGATYWNY
Przeszukiwanie pamięci RAM. Test sprawdza, czy złośliwe oprogramowanie może wyodrębnić poufne informacje z pamięci RAM, np. numery kart kredytowych, hasła, loginy lub numery kont bankowych.	✗ NEGATYWNY	✗ NEGATYWNY
Wstrzykiwanie bibliotek DLL. Test sprawdza, czy możliwe jest wstrzykiwanie złośliwych plików DLL do procesów tzw. „bezpiecznej przeglądarki" lub „środowiska wirtualnego" lub procesów antywirusa. Używane metody: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✗ NEGATYWNY	✗ NEGATYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest wstawienie kodu HTML i kodu JavaScript do stron internetowych.	✗ NEGATYWNY	✗ NEGATYWNY
Atak Man-In-The-Middle. Test sprawdza, czy możliwe jest przechwycenie poufnych informacji ze stron internetowych zabezpieczonych certyfikatem SSL.	✗ NEGATYWNY	✗ NEGATYWNY
Ukryty pulpit. Test sprawdza, czy złośliwe oprogramowanie może nawiązać zdalne połączenie z serwerem hackera podczas aktywnej sesji bankowej.	✓ POZYTYWNY	✓ POZYTYWNY
Modyfikowanie pliku HOSTS. Test sprawdza, czy złośliwe oprogramowanie może manipulować zawartością pliku HOSTS systemu Windows.	✗ NEGATYWNY	✗ NEGATYWNY
Wykrywanie trzynastu trojanów bankowych znalezionych in-the-wild w lutym 2019 roku.	POZYTYWNY: 13 / 13	

Opis unikalnych składników ochrony bankowej, aby umożliwić lepsze zrozumienie, w jaki sposób technologia chroni użytkowników podczas aktywnej sesji bankowej.

Oprogramowanie Windows Defender jako integralna część systemów Windows zabezpiecza przed szkodliwym oprogramowaniem oraz przed exploitami i ransomware. Współpracuje z systemową funkcją SmartScreen, która analizuje pobierane pliki z sieci i aplikacje ze sklepu Microsoft pod kątem źródła pochodzenia, sum kontrolnych i wzorców czarnych list plików. Wszystkie te informacje są dostarczane do Windows Defender pod postacią sygnatur. Jak przystało na oprogramowanie antywirusowe Windows Defender działa w czasie rzeczywistym, chroniąc przed spyware, trojanami, fałszywymi instalatorami czy chociażby potencjalnie niepożądanymi aplikacjami. SmartScreen, chociaż skutecznie zabezpiecza przed podejrzanymi plikami i ostrzega, jeśli plik nie ma podpisu cyfrowego, to jednak może generować fałszywe alarmy i blokować legalne instalatory. Antywirusowi brakuje podstawowych mechanizmów ochrony na poziomie zapory sieciowej oraz bardziej zaawansowanych technik analizowania nowego złośliwego kodu, w tym skryptów w systemie Windows.

ZDANYCH TESTÓW: **2 / 11**

Włączenie niektórych funkcji lub trybu bankowego nie miało wpływu na lepszy wynik.

Recommendacja AV LAB ONLY TESTED