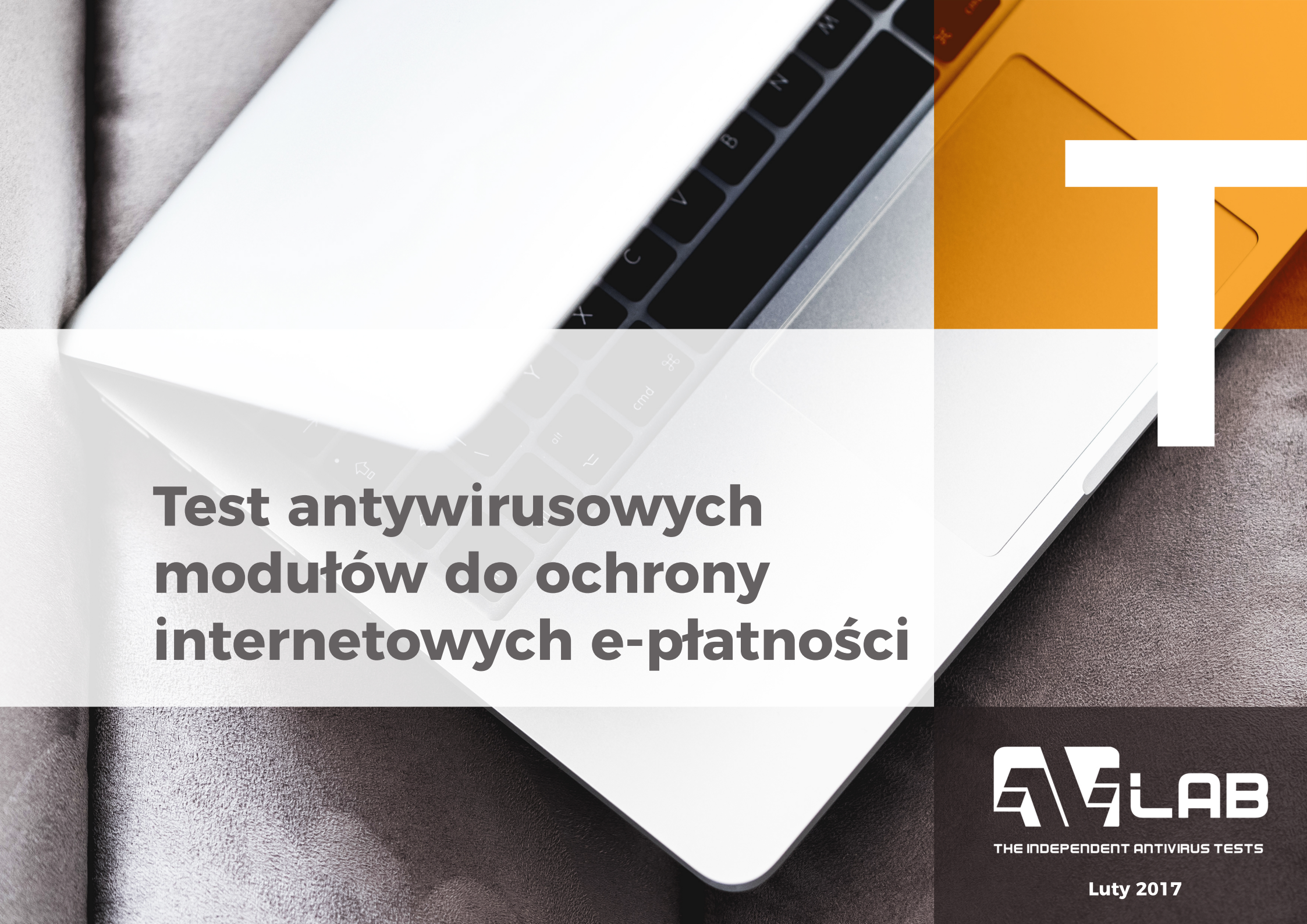


Test antywirusowych modułów do ochrony internetowych e-płatności

AV-TEST LAB

THE INDEPENDENT ANTIVIRUS TESTS

Luty 2017

_KONSPEKT

Po przeczytaniu tego raportu dowiesz się, czy tzw. "bezpieczne przeglądarki" chronią przed m.in.:

a. przechwytywaniem i modyfikowaniem danych ze schowka systemowego

b. przechwytywaniem naciskanych klawiszy na klawiaturze

c. wstrzykiwaniem złośliwych bibliotek DLL do procesów

d. wydobywaniem z pamięci RAM poufnych informacji (haseł, loginów, numerów kart płatniczych)

e. przechwytywaniem danych logowania ze stron HTTPS

Na przełomie stycznia i lutego 2017 roku, eksperci z AVLab, którzy zajmują się testami kompleksowych rozwiązań do ochrony urządzeń i stacji roboczych oraz edukowaniem użytkowników w dziedzinie internetowego bezpieczeństwa, poddali testom kilka antywirusowych produktów, które posiadają tak zwane moduły do zabezpieczenia internetowych e-płatności. Większość z nich jest bezpośrednio zintegrowana z przetestowanymi aplikacjami, jedyny wyjątek stanowi firma Bitdefender, która za darmo udostępnia swój produkt o nazwie „Bitdefender Safepay" – aplikacja ta może działać jako niezależne oprogramowanie wraz z konkurencyjnymi programami antywirusowymi od firm trzecich.

Test został przeprowadzony w celu sprawdzenia skuteczności ochrony, które mają zapewniać tak zwane „bezpieczne przeglądarki" przed atakami hackerów oraz kradzieżą danych w momencie wykonywania e-przelewów i przeglądania stron internetowych, których to bezpieczeństwo potwierdzone jest certyfikatami SSL.

Test został podzielony na dwie części:

1. W pierwszym etapie eksperci sprawdzili ochronę z wyłączonymi modułami antywirusowymi, aby udowodnić, że użytkownik podczas wykonywania finansowych e-transakcji powinien korzystać ze wszystkich funkcji ochrony, jakie są dostępne w testowanych rozwiązaniach antywirusowych.

2. W drugim etapie (i na ustawieniach domyślnych) – z włączonymi wszystkimi funkcjami ochrony, poddano testom tak zwane „bezpieczne przeglądarki" w celu porównania skuteczności z wyłączonymi i włączonymi składnikami ochrony popularnych programów antywirusowych.

POPRZEDNIE PUBLIKACJE

Test ochrony przed zagrożeniami ransomware

Test bepłatnych skanerów antywirusowych

_KONSPEKT CD.

Z pośród przetestowanych rozwiązań firm: Arcabit, Avast, Bitdefender, Comodo, Eset, F-Secure, G Data, Kaspersky i Qihoo, tylko producenci: Arcabit, Comodo oraz Kaspersky Lab dostarczają rozwiązania do ochrony użytkowników i ich pieniędzy w wystarczającym stopniu, aby uzyskać rekomendację od AVLab.

Eksperci z AVLab do testu wykorzystali systemowy interpreter poleceń Windows PowerShell oraz złośliwe skrypty napisane w języku Python, aby sprawdzić, czy znane i popularne w naszym kraju antywirusowe rozwiązania w należytym stopniu chronią użytkownika, podczas gdy ten korzysta z internetowej bankowości, e-zakupów lub odwiedza serwisy internetowe przy wykorzystaniu tak zwanych „bezpiecznych przeglądarek" lub „wirtualnych środowisk", które mają gwarantować skuteczną ochronę przed m.in.: keyloggerami, przechwytywaniem danych ze schowka systemowego, wydobywaniem poufnych informacji z pamięci RAM, modyfikowaniem pliku HOSTS, czy chociażby atakami man-in-the-middle.

Eksperci przed testem zapoznali się z publicznie dostępnymi informacjami na temat testowanych rozwiązań i opracowali metodologię, która była sprawiedliwa dla każdego oprogramowania – nie faworyzowała, ani nie umniejszała możliwości ochrony któregokolwiek z nich.

_TESTOWANE PROGRAMY

NAZWA PROGRAMU	WERSJA
QIHOO 360 Total Security 9	*9.0.0.1085*
ARCABIT Internet Security	*2017.01.23*
AVAST Free Antivirus	*12.03.2280*
AVAST Premier	*12.03.2280*
BITDEFENDER Safepay	*2.0.0.744*
BITDEFENDER Total Security 2017	*21.0.22.1050*
COMODO Internet Security Premium 10	*10.0.0.6092*
ESET Smart Security Premium 10	*10.0.386.2*
F-SECURE Safe	*2.76.211.0*
G DATA Total Security	*25.3.0.1*
KASPERSKY Total Security 2017	*17.00.611*

_METODOLOGIA

Aby zastosować się do zasady „równości”, eksperci z AVLab zdecydowali się przetestować na ustawieniach domyślnych i w identycznym środowisku testowym tzw. „przeglądarki do internetowej bankowości”, które są zintegrowane z programami antywirusowymi. Wyjątek stanowi rozwiązanie Bitdefender Safepay, które może bez przeszkód współpracować z aplikacjami firm trzecich do ochrony komputerów (Bitdefender Safepay jest także zintegrowany z pakietami bezpieczeństwa firmy Bitdefender).

Dzięki zachowaniu powyższej zasady, każde rozwiązanie zostało sprawdzone w takich samych warunkach i przy wykorzystaniu tego samego algorytmu postępowania.

Eksperci z AVLab do testu wykorzystali skrypty napisane w języku programowania Python, systemowy interpreter poleceń Windows PowerShell oraz ogólnodostępne narzędzia dla systemu Linux. Wszystkie „szkodliwe” skrypty, które sprawdzały ochronę testowanych rozwiązań nie były wykrywalne przez antywirusowe sygnatury, dlatego czytelnik może traktować „próbki” wykorzystane w teście jako całkowicie niewykrywalne dla programów antywirusowych.

B

Badania były przeprowadzane z wykorzystaniem złośliwego oprogramowania działającego w Windows przy aktywnej ochronie tzw. "bezpiecznych przeglądarek", które służą do wykonywania internetowych przelewów.

Sposób postępowania:

1. Instalacja testowanego rozwiązania na przygotowanym wcześniej obrazie systemu Windows 10 x64.

2. Sekwencyjne uruchamianie procedur sprawdzających: Test 1, Test 2, Test 3, ... , Test 14.

_OBJAŚNIENIA

Test 1: W trakcie przenoszenia skopiowanych danych ze schowka systemowego do „bezpiecznej przeglądarki" lub do „wirtualnego środowiska", sprawdzono, czy możliwe jest przechwycenie zawartości schowka systemowego.

Test 2: W trakcie przenoszenia skopiowanych danych z „bezpiecznej przeglądarki" lub „wirtualnego środowiska" do systemu Windows, sprawdzono, czy możliwe jest przechwycenie zawartości schowka systemowego.

Test 3: W trakcie kopiowania danych ze schowka systemowego w obrębie kart „bezpiecznej przeglądarki" lub „wirtualnego środowiska", sprawdzono, czy możliwe jest przechwycenie zawartości schowka systemowego przez wirusa uruchomionego w systemie operacyjnym Windows.

Test 4: W trakcie kopiowania danych ze schowka systemowego z Windows, sprawdzono, czy możliwa jest podmiana numeru konta bankowego skopiowanego np. z komunikatora internetowego, e-maila, faktury PDF lub ze strony internetowej do „bezpiecznej przeglądarki" lub „wirtualnego środowiska".

Eksperci z AVLab wykorzystując zagrożenia do testów nie współpracują z żadnym producentem oprogramowania zabezpieczającego. Dzięki temu nie zachodzi podejrzenie, że testowany program wykrywa próbki zagrożeń, które są dostarczane przez jego dewelopera.

Technikę podmiany numeru konta bankowego zastosowali twórcy złośliwego oprogramowania m.in. w kampanii wymierzonej w polskich użytkowników, która została wykryta przez CERT Polska: http://bit.ly/2ijLtfP

_OBJAŚNIENIA CD.

Test 5: W trakcie logowania się do witryny Banku sprawdzono, czy złośliwe oprogramowanie może rejestrować wciskane klawisze na klawiaturze.

Test 6: W trakcie logowania się do witryny Banku, sprawdzono, czy możliwe jest wykonywanie zrzutów ekranu przez złośliwe oprogramowanie.

Test 7: W trakcie przeglądania stron HTTPS, sprawdzono, czy możliwe jest wydobywanie z pamięci RAM poufnych informacji, np. numerów kart kredytowych, haseł, loginów, numerów kont bankowych.

Test 8: W trakcie przeglądania stron HTTPS, sprawdzono, czy możliwe jest wstrzykiwanie złośliwych bibliotek DLL do procesów „bezpiecznej przeglądarki" lub „wirtualnego środowiska".

Test 9: W trakcie przeglądania stron WWW, sprawdzono, czy możliwe jest wstrzykiwanie kodu HTML i JavaScript do witryn internetowych (HTTP).

Test 10: W trakcie przeglądania stron WWW (HTTP), sprawdzono, czy możliwe jest manipulowanie kodem źródłowym wyświetlanej strony.

Test 11: W trakcie przeglądania stron HTTPS, sprawdzono, czy możliwe jest przekierowywanie użytkownika na inne adresy IP.

Test 12: W trakcie przeglądania stron HTTPS, sprawdzono, czy możliwe jest przechwytywanie poufnych informacji ze stron, których bezpieczeństwo potwierdzone jest certyfikatem SSL.

Test 13: W trakcie korzystania z tzw. „bezpiecznych przeglądarek" lub „wirtualnych środowisk", sprawdzono, czy możliwe jest ustanowienie zdalnego połączenia podczas aktywnej sesji z bezpieczną stroną Banku.

Test 14: W trakcie korzystania z tzw. „bezpiecznych przeglądarek" lub „wirtualnych środowisk", sprawdzono, czy możliwe jest manipulowanie zawartością pliku HOSTS.

WSZYSTKIE MODUŁY OCHRONY SĄ WYŁĄCZONE

FAIL – PASS

	Qihoo	Arcabit	Avast (Free)	Avast (Premier)	Bitdefender (Safepay)	Bitdefender	Comodo	Eset	F-Secure	G Data	Kaspersky
Nazwa modułu	Shopping Protection	Safe Browser	SafeZone Browser	SafeZone Browser	Safepay (bez antywirusa)	Safepay (Total Sec.)	Bezpieczne Zakupy	Ochrona bankowości	Ochrona bankowości	BankGuard	Bezpieczne pieniądze
Test 1	FAIL	PASS	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL
Test 2	FAIL	PASS	FAIL	FAIL	FAIL	FAIL	PASS	FAIL	FAIL	FAIL	FAIL
Test 3	FAIL	PASS	FAIL	FAIL	FAIL	FAIL	PASS	FAIL	FAIL	FAIL	FAIL
Test 4	FAIL	PASS	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL
Test 5	FAIL	PASS	FAIL	FAIL	PASS	PASS	PASS	FAIL	FAIL	FAIL	FAIL
Test 6	FAIL	PASS	FAIL	FAIL	PASS	PASS	PASS	FAIL	FAIL	FAIL	FAIL
Test 7	FAIL	PASS	FAIL	FAIL	FAIL	FAIL	PASS	FAIL	FAIL	FAIL	FAIL
Test 8	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
Test 9	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL
Test 10	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL
Test 11	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL
Test 12	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	PASS
Test 13	FAIL	PASS	FAIL	FAIL	FAIL	FAIL	PASS	FAIL	FAIL	FAIL	FAIL
Test 14	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL

DOMYŚLNE USTAWIENIA OCHRONY ANTYWIRUSOWEJ

FAIL – PASS

	Qihoo	Arcabit	Avast (Free)	Avast (Premier)	Bitdefender (Safepay)	Bitdefender	Comodo	Eset	F-Secure	G Data	Kaspersky
Nazwa modułu	Shopping Protection	Safe Browser	SafeZone Browser	SafeZone Browser	Safepay (bez antywirusa)	Safepay (Total Sec.)	Bezpieczne Zakupy	Ochrona bankowości	Ochrona bankowości	BankGuard	Bezpieczne pieniądze
Test 1	FAIL	PASS	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	PASS
Test 2	FAIL	PASS	FAIL	FAIL	FAIL	FAIL	PASS	FAIL	FAIL	FAIL	PASS
Test 3	FAIL	PASS	FAIL	FAIL	FAIL	FAIL	PASS	FAIL	FAIL	FAIL	PASS
Test 4	FAIL	PASS	FAIL	FAIL	FAIL	FAIL	PASS	FAIL	FAIL	FAIL	FAIL
Test 5	FAIL	PASS	FAIL	FAIL	PASS	PASS	PASS	PASS	FAIL	PASS	PASS
Test 6	FAIL	PASS	FAIL	FAIL	PASS	PASS	PASS	FAIL	FAIL	FAIL	PASS
Test 7	FAIL	PASS	FAIL	FAIL	FAIL	FAIL	PASS	FAIL	FAIL	FAIL	PASS
Test 8	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
Test 9	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	PASS	FAIL	FAIL	FAIL
Test 10	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	PASS	FAIL	FAIL	FAIL
Test 11	FAIL	PASS	FAIL	FAIL	FAIL	FAIL	FAIL	PASS	FAIL	FAIL	FAIL
Test 12	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	PASS	FAIL	FAIL	PASS
Test 13	FAIL	PASS	FAIL	FAIL	FAIL	PASS	PASS	FAIL	FAIL	FAIL	FAIL
Test 14	PASS	PASS	FAIL	FAIL	FAIL	FAIL	PASS	FAIL	FAIL	FAIL	PASS

_INTERPRETACJA WYNIKÓW

Podczas wykonywania transakcji internetowych, użytkownik jest szczególnie narażony na przechwytywanie newralgicznych informacji przez nieuprawnione osoby trzecie, a także przez złośliwe oprogramowanie. Sprawdzone przez ekspertów z AVLab rozwiązania, w zasadzie nie chronią przed atakami man-in-the-middle. Nieznaczne odstępstwo od tej reguły stanowi oprogramowanie Arcabit Internet Security, Kaspersky Total Security oraz przede wszystkim nowy ESET Smart Security 10, gdzie w przypadku testów sprawdzających odporność na zatruwanie tablic ARP, firewall słowackiego producenta robił to, co powinien – czyli zapobiegał wysyłaniu i odbieraniu danych pomiędzy testowym komputerem o niewłaściwym adresie MAC a routerem. W tym przypadku, wektor ataku wymaga umieszczenia atakującego lub pewnych złośliwych narzędzi pomiędzy ofiarą a docelowym zasobem, takim jak strona internetowa Banku lub cały komputer. Ataki te mogą być bardzo skuteczne i dość trudne do wykrycia, zwłaszcza dla użytkowników, którzy nie są świadomi niebezpieczeństw.

Większość z przetestowanych rozwiązań do ochrony internetowych e-płatności nie zabezpiecza w należyty sposób transakcji przed możliwymi atakami hackerów w miejscach publicznych i przed złośliwym oprogramowaniem, które jest niewykrywalne przez skanowanie sygnaturami.

Przeważająca część z przetestowanych rozwiązań do ochrony internetowych płatności nie zabezpiecza w należyty sposób e-transakcji przed możliwymi atakami hackerów w miejscach publicznych i przed złośliwym oprogramowaniem, które jest niewykrywalne przez skanowanie sygnaturami i ochronę behawioralną.

_INTERPRETACJA WYNIKÓW CD.

Okazuje się, że tzw. analiza heurystyczna oraz behawioralna, które sprawdzają działanie podejrzanego programu podczas jego uruchomienia w bezpiecznym środowisku za pomocą emulatora procesora (analiza heurystyczna statyczna i dynamiczna) i monitorują wywoływane systemowe funkcje API oraz sprawdzają ich sumy kontrolne (analiza behawioralna) nie gwarantują najlepszej ochrony. I chociaż żaden z testowanych programów nie uzyskał maksymalnego wyniku, to rekomendacje za dobrą lub przyzwoitą ochronę w poszczególnych etapach testu należą się dla:

Arcabit Internet Security za pionierskie podejście do ochrony newralgicznych informacji przesyłanych droga internetową. Producent z Polski zastosował odmienne mechanizmy zabezpieczające dla swojej przeglądarki Safe Browser, które nie pozwalają na uruchomienie niedozwolonych procesów podczas aktywnej aplikacji Safe Browser.

Comodo Internet Security za bezpieczne środowisko uruchomieniowe, które w należyty sposób zabezpiecza e-transakcje - chociaż użytkownik nie może zapominać o podatności swojego przenośnego urządzenia na ataki man-in-the-middle i powinien korzystać z sieci VPN oraz przestrzegać zasady bezpiecznego korzystania z komputera w miejscach publicznych.

ESET Smart Security za skuteczną ochronę przed zatruwaniem tablic ARP. Oprogramowanie słowackiego producenta jako jedyne skutecznie chroniło newralgiczne dane użytkownika w testach sprawdzających odporność na ataki man-in-the-middle, za co producentowi ESET należy się uznanie ekspertów AVLab.

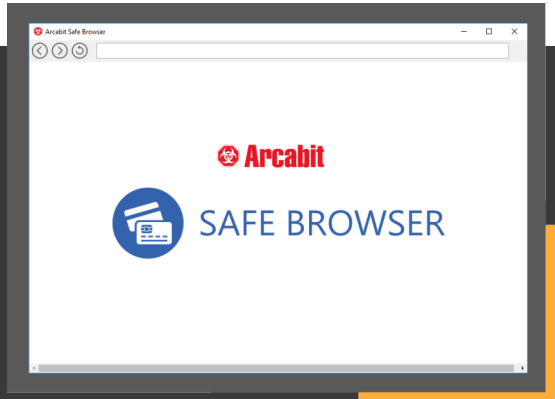
Kaspersky Total Security za kompleksowość ochrony, która już na ustawieniach domyślnych gwarantuje wysoki poziom zabezpieczeń przed większością symulowanych ataków i zagrożeń, które mogą realnie zagrozić użytkownikom.

WIĘCEJ BEZPIECZEŃSTWA

Po więcej informacji w zakresie prywatności, bezpieczeństwa i zabezpieczenia urządzeń odsyłamy do opracowanego przez ekspertów AVLab edukacyjnego materiału.

_SPECJALNE REKOMENDACJE DLA:

ARCABIT



Arcabit, producent z wieloletnią tradycją tworzenia oprogramowania antywirusowego i ochronnego oraz dostawca skutecznej bariery dla wszelkich współczesnych cyberzagrożeń, zastosował w rozwiązaniu Arcabit Safe Browser kilka mechanizmów ochronnych:

- "Biała lista" procesów, które są dopuszczone do działania wraz z aktywnym oknem Arcabit Safe Browser. Ta metoda ochrony jest bardzo skuteczna, ponieważ jeszcze przed włączeniem samej przeglądarki sprawdzane są uruchomione procesy. Niektóre z nich mogą być szkodliwe i działać w ukryciu oszukując ochronę antywirusową, dlatego Arcabit po raz kolejny przechytrza twórców złośliwego oprogramowania i informuje użytkownika o działających procesach, które nie są bezpieczne. Decyzja, które z nich powinny zostać zamknięte, a które nie, uwarunkowana jest preferencjami użytkownika. W tym kontekście metoda działania Arcabit Safe Browser jest następująca: wszystkie procesy, które znajdują się na liście aktualnie uruchomionych procesów powinny zostać zamknięte – tak na wszelki wypadek, aby niepotrzebne nie narażać użytkownika na ryzyko utraty pieniędzy lub przechwycenia poufnych informacji.

- Analiza połączeń sieciowych mająca na celu wykrycie ewentualnych przekierowań ruchu. Jeśli Arcabit Safe Browser wykryje podejrzane zachowanie, użytkownik zostanie o tym poinformowany jeszcze przed uruchomieniem przeglądarki.

- Ochrona procesu przeglądarki nie pozwala na naruszenie ich integralności np. poprzez tzw. "wstrzykiwanie" szkodliwych bibliotek.

- Aktywny Filtr WWW sprawdza w czasie rzeczywistym, czy odwiedzane strony nie są sklasyfikowane jako szkodliwe (wykradające dane).

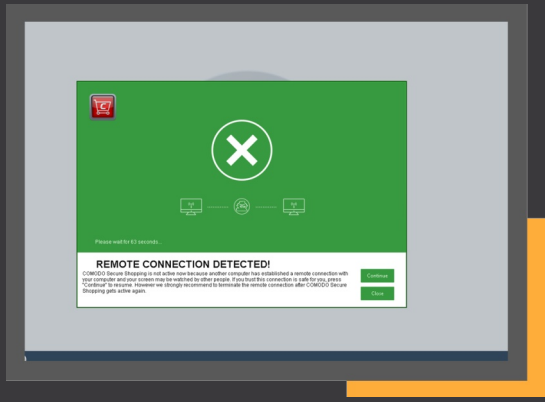
_SPECJALNE REKOMENDACJE DLA:

COMODO

Producent Comodo wraz z przekazaniem w ręce użytkowników nowej wersji sztandarowego rozwiązania Comodo Internet Security 10 wyposażonego w moduł Bezpieczne Zakupy, chroni poufne dane swoich klientów m.in. przed keyloggerami oraz atakami, które wykorzystują tak zwaną technikę „memory scraping". Tym samym, newralgiczne operacje, w których zachodzi potrzeba ochrony poufnych danych lub ukrycia tożsamości, jest dostępna bezpłatnie dla każdego użytkownika, który nie musi posiadać specjalistycznej wiedzy z zakresu działania technologii komputerowych.

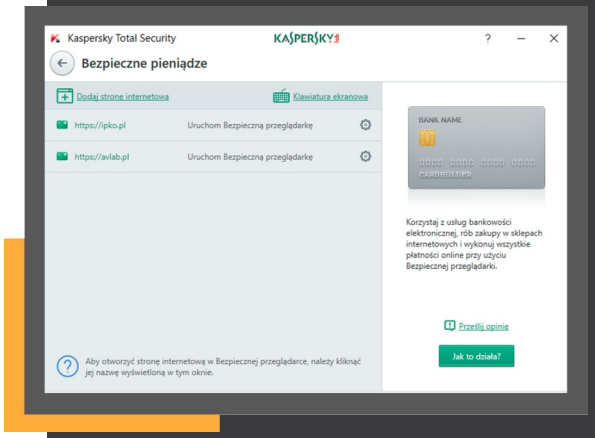
Comodo, podczas aktywnej sesji bezpiecznego środowiska, do zwiększenia ochrony przed atakami ma-in-the-middle pozwala uruchomić dowolnie wskazaną aplikację już w odizolowanym środowisku zupełnie odseparowanym od systemu, dzięki czemu użytkownik ma możliwość ustanowienia połączenia VPN i bezpiecznego połączenia się z dowolnymi stronami WWW w miejscach publicznych.

W ramach systematycznie rozwijanego od kilku lat wyizolowanego środowiska, operacje płatności za zakupy kartą, logowania się do internetowych banków i bezpiecznego łączenia się z systemami on-line są w odpowiedni sposób chronione przed złośliwym oprogramowaniem. Integralny z warstwą antywirusową wirtualny pulpit zabezpiecza urządzenie przed nawiązywaniem zdalnej sesji hackera z komputerem – i co najważniejsze – nawet wtedy, kiedy zaawansowane szkodliwe oprogramowanie zdoła ominąć wszystkie warstwy zabezpieczeń Comodo.



_SPECJALNE REKOMENDACJE DLA:

KASPERSKY



Działanie modułu Bezpieczne pieniądze funkcjonującego w produktach Kaspersky Lab opiera się na trzech fundamentach: zaufana strona WWW, zaufane połączenie oraz zaufane środowisko.

Po sprawdzeniu autentyczności strony, na której ma być realizowana transakcja finansowa online przeglądarka przełącza się w tryb bezpieczny, który chroni przed wniknięciem podejrzanego kodu oraz zapewnia dodatkową ochronę podczas wszelkich operacji online. Jeżeli adres URL nie zostanie znaleziony w bazie, strona zostanie sprawdzona przez moduł heurystyczny, którego zadaniem jest wyszukiwanie oszustw phishingowych. Gwarantuje to, że użytkownik otwiera prawdziwą stronę systemu bankowego lub płatności online, a nie tę stworzoną przez oszustów.

Kolejnym krokiem jest sprawdzenie autentyczności serwera, z którym użytkownik łączy się podczas korzystania z bankowości elektronicznej. W przypadku braku możliwości zweryfikowania danej strony, zapytanie kierowane jest do chmury Kaspersky Security Network.

Po uruchomieniu przeglądarki w trybie Bezpieczne pieniądze, blokowane są próby wprowadzenia szkodliwego kodu za pośrednictwem przeglądarki, odczytu pamięci, wyświetlania fałszywych okien. 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.

_PRZYZNANE REKOMENDACJE

BEST+++ minimum 11 zaliczonych testów
BEST++ minimum 7 zaliczonych testów
GOOD+ minimum 3 zaliczone testy
ONLY TESTED mniej niż 3 zaliczone testy

Na końcowe wyniki wpływ miały rezultaty osiągnięte tylko przy włączonej ochronie antywirusowej (tabelka druga)

ARCABIT Internet Security
(11 zaliczonych testów)

COMODO Internet Security 10
(9 zaliczonych testów)

KASPERSKY Total Security 2017
(9 zaliczonych testów)

ESET Smart Security 10
(6 zaliczonych testów)

BITDEFENDER Safe
(3 zaliczone testy)

BITDEFENDER Total Security 2017
(3 zaliczone testy)

G DATA Internet Security
(2 zaliczone testy)

QIHOO 360 Total Security 9
(2 zaliczone testy)

AVAST Free Antivirus
(tylko 1 zaliczony test)

AVAST Internet Security
(tylko jeden zaliczony test)

F-SECURE Safe
(tylko jeden zaliczony test)

_INFORMACJE O AVLAB

Kontakt w sprawie testów dla producentów:
kontakt@avlab.pl

Przyznane certyfikaty do pobrania w wysokiej rozdzielczości:
https://avlab.pl/dla-prasy

AVLab skupia w jednym miejscu miłośników rozwiązań zabezpieczających. Nasze działania obejmują testowanie programów i dzielenie się wynikami z naszych analiz ze wszystkimi użytkownikami Internetu. Nie jesteśmy kontrolowani i/lub powiązani w jakikolwiek sposób z żadnym producentem lub dystrybutorem oprogramowania zabezpieczającego.

Testy AVLab są niezależne i odbywają się w warunkach zbliżonych do rzeczywistości. Nie należy kierować się naszymi wynikami, jako ostateczną decyzją w wyborze aplikacji bezpieczeństwa. W celu dokonania ostatecznego wyboru, sugerujemy zapoznać się także z testami innych niezależnych laboratoriów, które korzystają z różnych metod i technik testowania oprogramowania. Ponadto, decyzje w wyborze zależą od osobistych preferencji, dostępności niezbędnych funkcji, skuteczności, wykrywalności, wpływu na wydajność systemu, wyglądu interfejsu, ceny, łatwości użytkowania, kompatybilności, języka, wsparcia technicznego i wielu innych cech.

AVLAB
THE INDEPENDENT ANTIVIRUS TESTS

www.avlab.pl