AV-TEST CYBERSECURITY FOUNDATION

Analiza modułów do ochrony bankowości i płatności internetowych

amtso
The cybersecurity industry's testing standard community
MEMBER

Test trybu bankowego w nowoczesnych rozwiązaniach antywirusowych

Grudzień 2023

Na skróty

I Dlaczego tak ważna jest ochrona płatności online?

II Metodologia

III Wyniki

IV Wnioski z testu

Dlaczego tak ważna jest ochrona płatności online?

Dedykowana ochrona dla internetowych płatności online ma na celu zabezpieczyć finanse, dane osobowe i chronić przed cyberprzestępczością. Dzięki niej podnosisz na wyższy poziom ochronę usług bankowych i transakcji online. Masz większą pewność, że Twoje pieniądze i dane są bezpieczne. Używając rekomendowanych przez AVLab zabezpieczeń znacząco minimalizujesz ryzyko cyberataku.

Większość nowoczesnych programów antywirusowych dla systemów macOS i Windows w zakresie podstawowym zabezpiecza bankowość i płatności internetowe przed zagrożeniami. Do takich technologii zaliczamy na przykład: anty-phishing, anty-malware, anty-keylogger, anty-screenlogger, blokowanie połączeń niezaufanych aplikacji i skryptów, wykrywanie zmian systemowych serwerów DNS oraz inne. Jednak niektórzy producenci oferują dla użytkownika znacznie więcej – tak zwany wyspecjalizowany moduł, który został zaprogramowany do protekcji systemu podczas wykonywania płatności internetowych lub innych ważnych i poufnych operacji na plikach i danych.

Głównym celem naszego badania było przetestowanie modułów do odpierania ataków na bankowość internetową, niezależnie od znanego i początkowego protokołu inicjacji cyberataku. Do przeprowadzenia analizy wykorzystaliśmy prawdziwe złośliwe oprogramowanie w symulowanym scenariuszu. Głównym celem testerów było wykraść informacje z urządzenia zabezpieczonego przez oprogramowanie antywirusowe w momencie korzystania z dedykowanego trybu ochrony bankowości lub płatności internetowych.

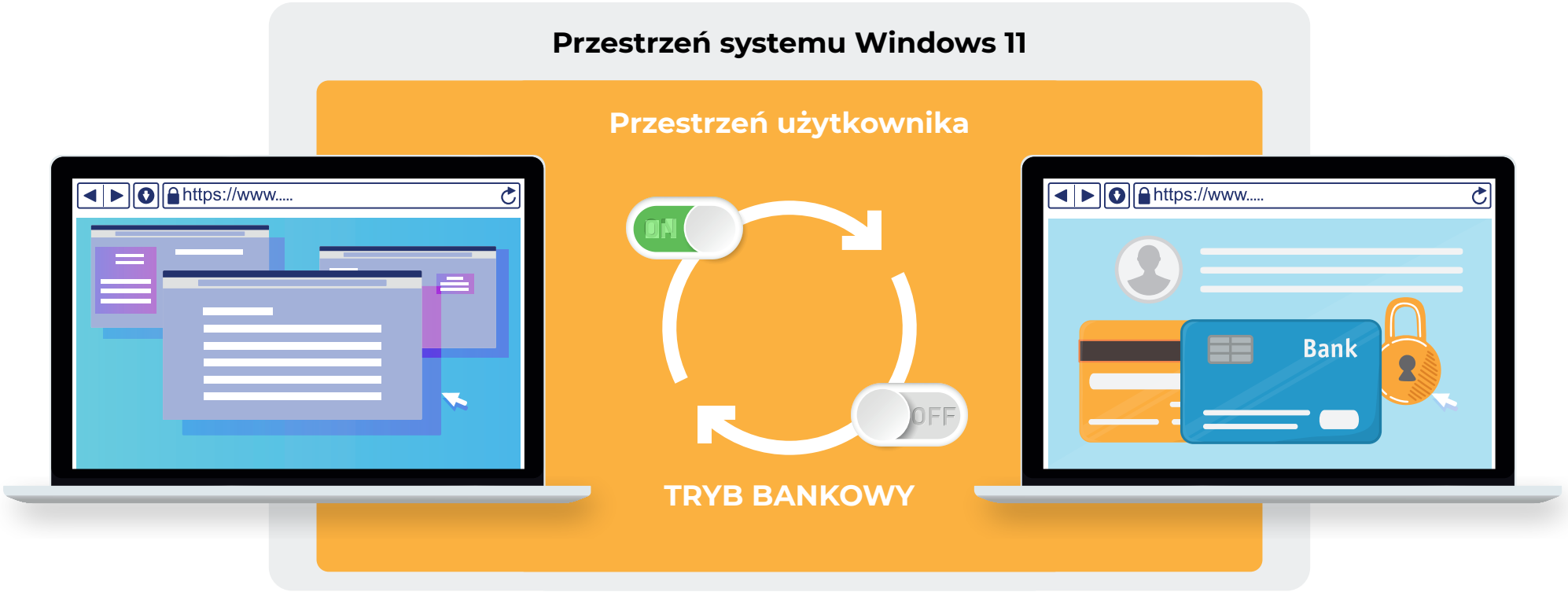
W tej edycji posłużyliśmy się komunikatorem Telegram, aby przesłać ofierze zagrożenie pod postacią zaufanej aplikacji od „znajomego kontaktu” – powiedzmy, że przesyłaliśmy wersję beta nowej gry, którą zaprogramował wasz kumpel. Do podobnego ataku może dojść z wykorzystaniem dowolnego komunikatora.

Dostarczenie malware do systemu poprzez komunikator to w pewnym sensie ominięcie podstawowej warstwy ochrony. Daje to atakującemu minimalnie większą szansę, ale też lepiej odzwierciedla styczność malware z technologiami obronnymi.

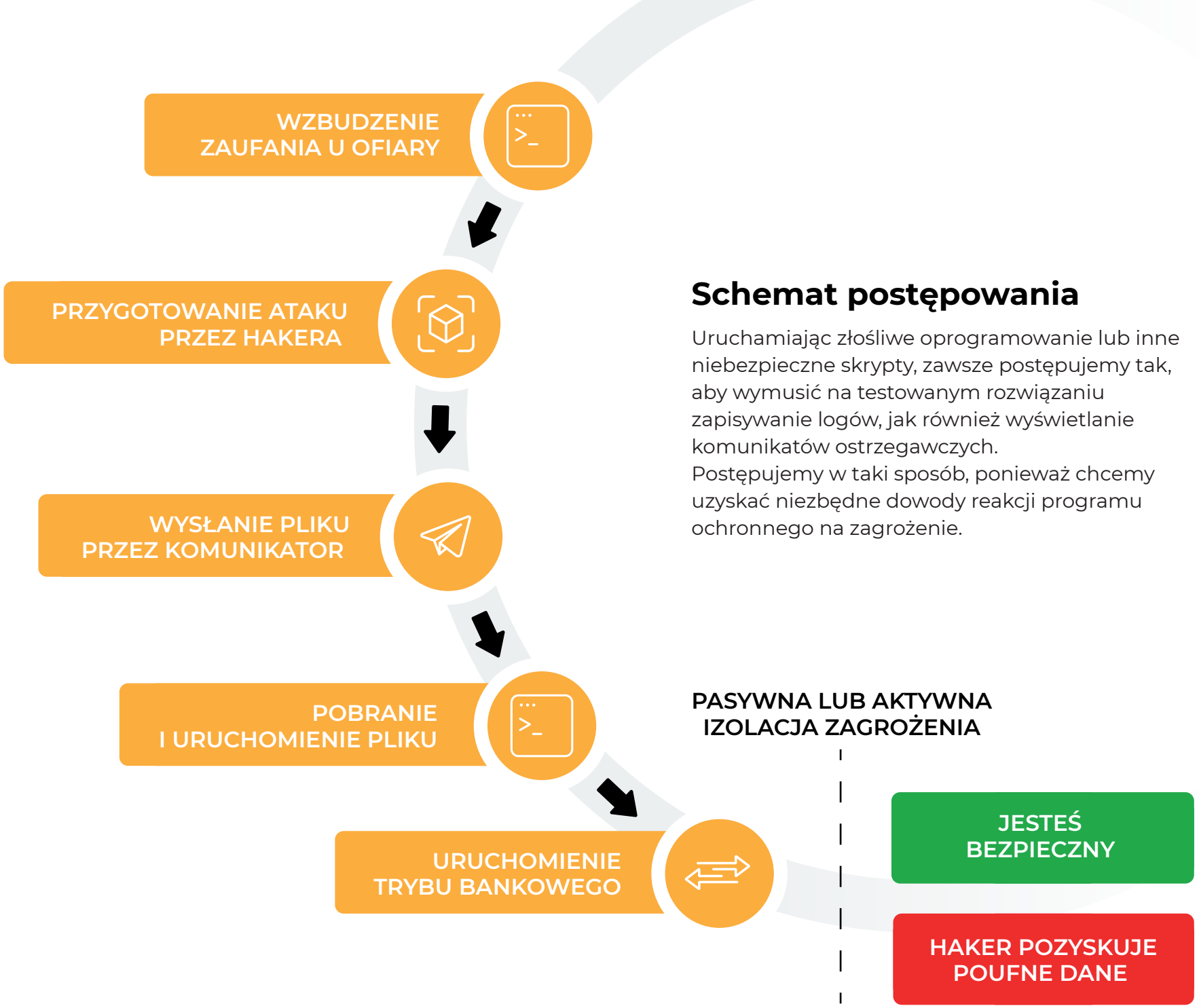
W tym scenariuszu zagrożenie-plik w pierwszej fazie omija swoją identyfikację w przeglądarce. Producenci dobrze opanowali tę technikę, dlatego tym razem nie chcieliśmy korzystać z przeglądarki jako wektora inicjacji ataku.

II Metodologia

Metodologia została opracowana zgodnie ze standardami Anti-Malware Testing Standard Organization. Daje to czytelnikowi gwarancję, że każdego producenta potraktowaliśmy tak samo, dając mu czas na przeanalizowanie dostarczonych logów oraz odniesienie się do wyników.



Złośliwe oprogramowanie pobieraliśmy do systemu przez komunikator Telegram – niezbyt popularny protokół w rozprzestrzenianiu zagrożeń. Zadaniem testowanych rozwiązań z uruchomionym trybem bankowości w tle było wykrycie i zatrzymanie ataku na dowolnym etapie: przed uruchomieniem, po uruchomieniu lub po nawiązaniu połączenia z serwerem hakera.



Schemat postępowania

Uruchamiając złośliwe oprogramowanie lub inne niebezpieczne skrypty, zawsze postępujemy tak, aby wymusić na testowanym rozwiązaniu zapisywanie logów, jak również wyświetlanie komunikatów ostrzegawczych.
Postępujemy w taki sposób, ponieważ chcemy uzyskać niezbędne dowody reakcji programu ochronnego na zagrożenie.

Czym się posługiwaliśmy?

Wykorzystaliśmy język programowania Python oraz ChatGPT, aby przygotować nieskomplikowane, złośliwe pliki EXE, które następnie używaliśmy w symulowanych cyberatakach, dostarczając przygotowane programy komunikatorem Telegram.

W tym scenariuszu nie było potrzeby, aby na urządzeniu ofiary znajdowało się środowisko Python, ponieważ złośliwe oprogramowanie zostało wcześniej skompilowane do jednego pliku wykonywalnego EXE przy użyciu narzędzia PyInstaller. Dodatkowo niektóre pliki podpisaliśmy własnym certyfikatem SSL wygenerowanym przez Microsoft SignTool, więc nie pochodziło ono od żadnego zaufanego wydawcy (brak CA, ang. Certification Authority).

Postępowaliśmy według poniższego scenariusza

01

Próba wprowadzenia malware do systemu i aktywacja w systemie.

02

Aktywacja modułu odpowiedzialnego za ochronę płatności internetowych. W zależności od testowanego rozwiązania ochrona może być uruchamiana automatycznie – po wejściu na stronę internetową banku lub manualnie przez użytkownika.

03

Zaobserwowanie reakcji programu ochronnego oraz tego, co udało się przechwycić atakującemu. Powtórzenie kroku dla wszystkich scenariuszy testowych.

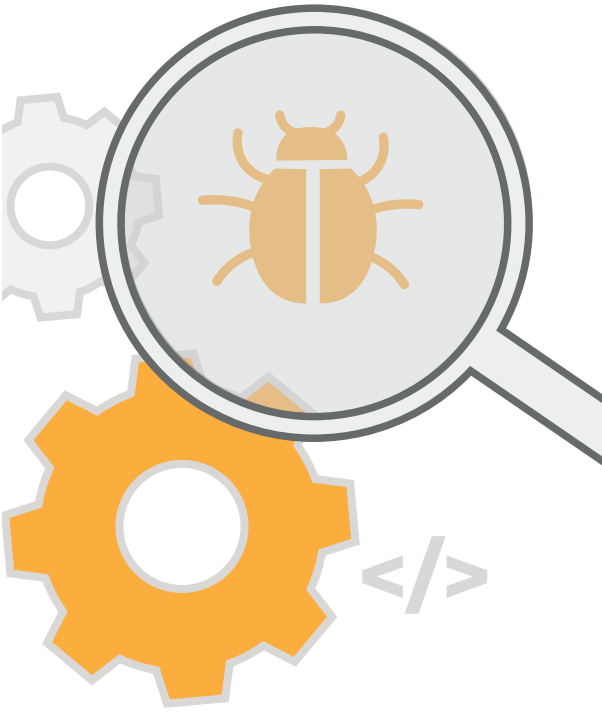
04

Zapisanie wniosków i indywidualna ocena produktu.

Programy, które testowaliśmy i ich ustawienia

Pakiety bezpieczeństwa były zainstalowane na ustawieniach domyślnych. Jeżeli np. ochrona przed keyloggerami była domyślnie wyłączona, to aktywowaliśmy tę funkcję. Zatem, kiedy złośliwe oprogramowanie nie było wykrywane na ustawieniach domyślnych, to od razu eksperymentowaliśmy z innymi ustawieniami (jeżeli były dostępne).

	Produkt	Specjalny Moduł do Ochrony Bankowości
Avast	AVAST Free Antivirus	Avast Secure Browser & Bank Mode
Bitdefender	BITEDEFENDER Total Security	Bitdefender Safepay
F-Secure	F-SECURE Total	Secure Browsing & Banking Protection
	MICROSOFT Defender	Application Guard
	MICROSOFT Defender	Windows Sandbox
mks_vir	MKS Internet Security	Safe Browser
Quick Heal Security Simplified	QUICK HEAL Total Security	Safe Browser + Safe Banking
xcitium The Power of Zero. Unleashed.	XCITIUM (Comodo) Internet Security Pro	Secure Shopping



Sposób dostarczenia malware – dlaczego komunikator?

Dostarczenie szkodliwego pliku do systemu ofiary to ważny aspekt testowania. Zwykle szkodliwe oprogramowanie jest pobierane do systemu albo poprzez e-mail albo przeglądarkę. Chcieliśmy uniknąć jednoznacznej sytuacji, kiedy plik trafia do systemu znanymi wektorami, ponieważ producenci całkiem nieźle opanowali techniki blokowania plików 0-day.

Tym razem wykorzystaliśmy komunikator Telegram z jego własnym algorytmem przesyłania i szyfrowania plików.
Przesyłane pliki przez komunikator są zapisywane bezpośrednio na dysku – Telegram nie tworzy czegoś w rodzaju linków do pliku, jak ma to miejsce w komunikatorze Discord.

Warto tutaj odnotować, że kiedy wysyłasz załącznik przez Discord, to do niego zostanie utworzone hiperłącze w domenie: **https://cdn.discordapp.com/attachments/**

Link do pliku z Discord ma następującą strukturę i jest pobierany z zaufanej domeny, co nie oznacza, że jest bezpieczny:

```
cdn.discordapp.com/attachments/[id]/[id]/file.exe
```

Różnica pomiędzy Telegram a Discord jest subtelna. Telegram wykorzystuje autorski protokół przesyłania i szyfrowania danych. Omija to znany i popularny wektor dostarczania pliku do systemu przez przeglądarkę. Z kolei link z komunikatora Discord jest otwierany w domyślnej przeglądarce, dlatego mechanizmy obronne antywirusów są w stanie zidentyfikować zagrożenie już na wczesnym etapie.

Wyniki

Scenariusze ataków

01

Przechwytywanie schowka systemowego
Test sprawdza, czy złośliwe oprogramowanie napisane w języku Python może przechwytywać zawartość schowka systemowego i wysyłać informacje na konto Telegram kontrolowane przez hakera.

02

Podmiana schowka systemowego
Test sprawdza, czy złośliwe oprogramowanie może zmieniać zawartość schowka systemowego np. skopiowany numer konta bankowego na inny podczas otwartej strony bankowej w bezpiecznym środowisku. Numer konta był pobierany ze zdalnej lokalizacji w serwisie pastebin.com.

03

Rejestrowanie klawiatury
Test sprawdza, czy złośliwe oprogramowanie może rejestrować naciśnięcia klawiszy na klawiaturze podczas korzystania z tzw. bezpiecznej przeglądarki lub trybu bankowego i czy może wysyłać poufne informacje na konto komunikatora kontrolowane przez atakującego.

04

Przechwytywanie zrzutów ekranu
Test sprawdza, czy złośliwe oprogramowanie napisane w języku Python może wykonywać zrzuty ekranu podczas korzystania z bankowości internetowej oraz wysyłać je do hakera.

05 *

Zdalne sterowanie komputerem
Test sprawdza, czy hacker w ataku socjotechnicznym za pomocą legalnego oprogramowania może kontrolować komputer użytkownika podczas aktywnego trybu płatności internetowych. W ataku wykorzystaliśmy legalne oprogramowanie Team Viewer. *

06

Przeszukiwanie dysku i kradzież plików
Test sprawdza, czy złośliwe oprogramowanie może skanować dysk użytkownika pod kątem wybranych rozszerzeń plików i wysłać je na konto Telegram kontrolowane przez atakującego.

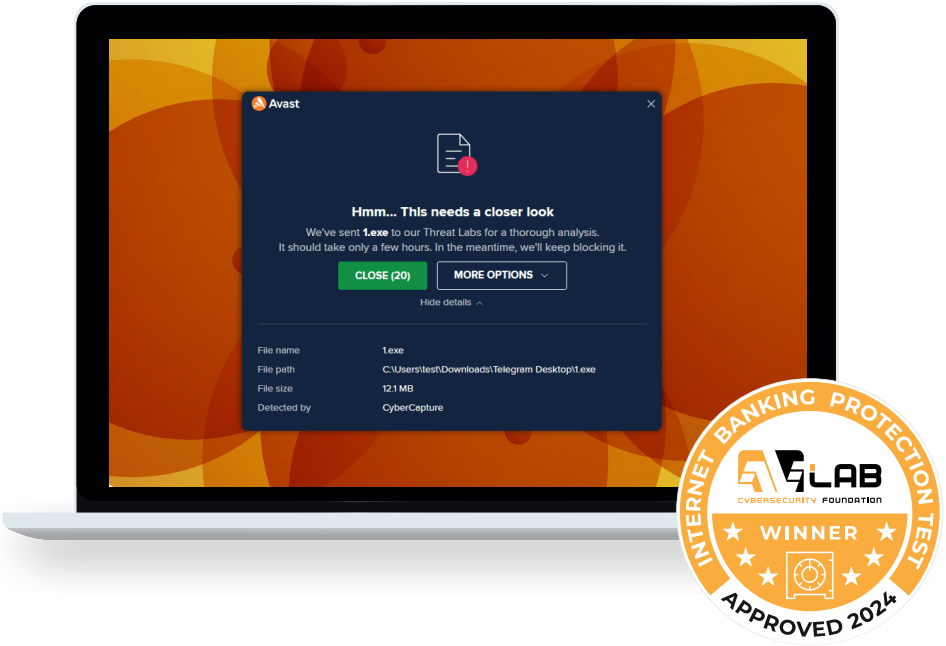
* Jest to specyficzny scenariusz, ponieważ legalne oprogramowanie nie zawsze będzie blokowane i to od decyzji użytkownika będzie zależeć kontynuowanie jego działania. Niektórzy producenci stosują pewne mechanizmy białych list programów lub specjalnie odseparowanej sesji od pulpitu użytkownika, aby w trybie bankowym nic nie zostało ujawnione.

AVAST Free Antivirus

Specjalny moduł do ochrony bankowości:

Avast Secure Browser & Bank Mode
Ustawienia programu: domyślne

PRZECHWYTYWANIE SCHOWKA	✓
PODMIANA SCHOWKA	✓
REJESTROWANIE KLAWIATURY	✓
PRZECHWYTYWANIE ZRZUTÓW EKRANU	✓
WYKRYWANIE ZDALNEGO STEROWANIA	✓
WYKRYWANIE KRADZIEŻY DANYCH Z DYSKU	✓



Specjalny tryb bankowy tworzy wirtualny pulpit dla użytkownika, który współdzieli z systemem operacyjnym podstawowe sterowniki niezbędne do obsługi podłączonych urządzeń: klawiatura, mysz, monitor, dyski, sieć itp. W tym trybie odseparowane środowisko od głównego Windows zabezpiecza sesję użytkownika przed dostaniem się szkodliwego oprogramowania do sesji trybu bankowego. Natomiast na zewnątrz trybu bankowego o bezpieczeństwo użytkownika odpowiada technologia CyberCapture, która na czas analizy nieznanego, złośliwego oprogramowania 0-day, blokuje dostęp do tego pliku i nie dopuszcza do jego uruchomienia do momentu ręcznej analizy przez zespół ekspertów z Avast Threat Labs.

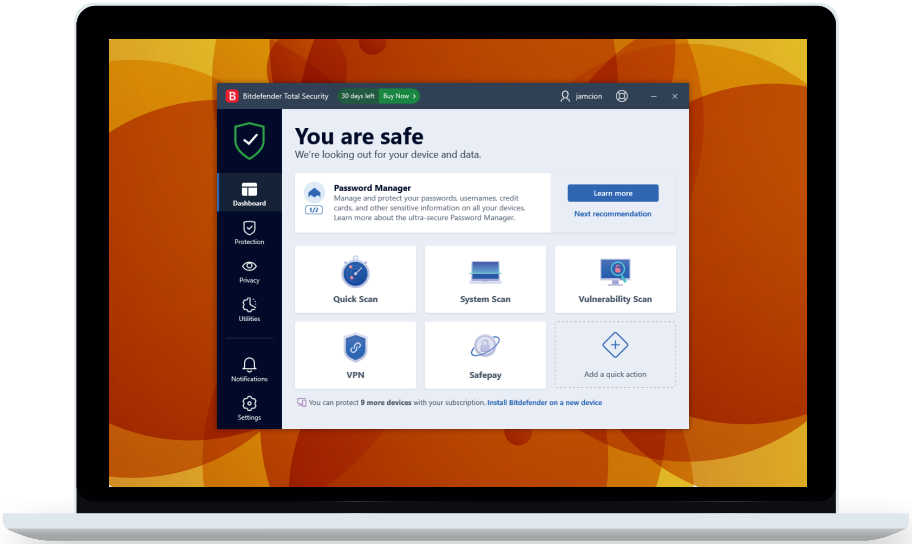
Bitdefender

BITEDEFENDER Total Security

Specjalny moduł do ochrony bankowości:

Bitdefender Safepay
Ustawienia programu: domyślne

PRZECHWYTYWANIE SCHOWKA	✗
PODMIANA SCHOWKA	✗
REJESTROWANIE KLAWIATURY	✓
PRZECHWYTYWANIE ZRZUTÓW EKRANU	✓
WYKRYWANIE ZDALNEGO STEROWANIA	✗
WYKRYWANIE KRADZIEŻY DANYCH Z DYSKU	✗



Uruchomiony Bitdefender Safepay chroni w czasie rzeczywistym przed oszustwami, phishingiem, szkodliwym oprogramowaniem, które zostało zaprojektowane w celu przechwytywania naciśnięć klawiszy i zbierania zrzutów ekranu. Użytkownik może przełączać się pomiędzy wirtualnym środowiskiem Bitdefender Safepay, a swoim pulpitem. W trakcie tych czynności możliwe jest korzystanie z komputera, tak jak do tej pory, bez zbędnego obciążenia zasobów systemowych. Teoretycznie, jeżeli sesja Safepay jest aktywna, nie pozwala to nieznanym aplikacjom korzystać z wirtualnego środowiska Safepay. Niestety testowe przypadki udowodniły, że jest to możliwe.

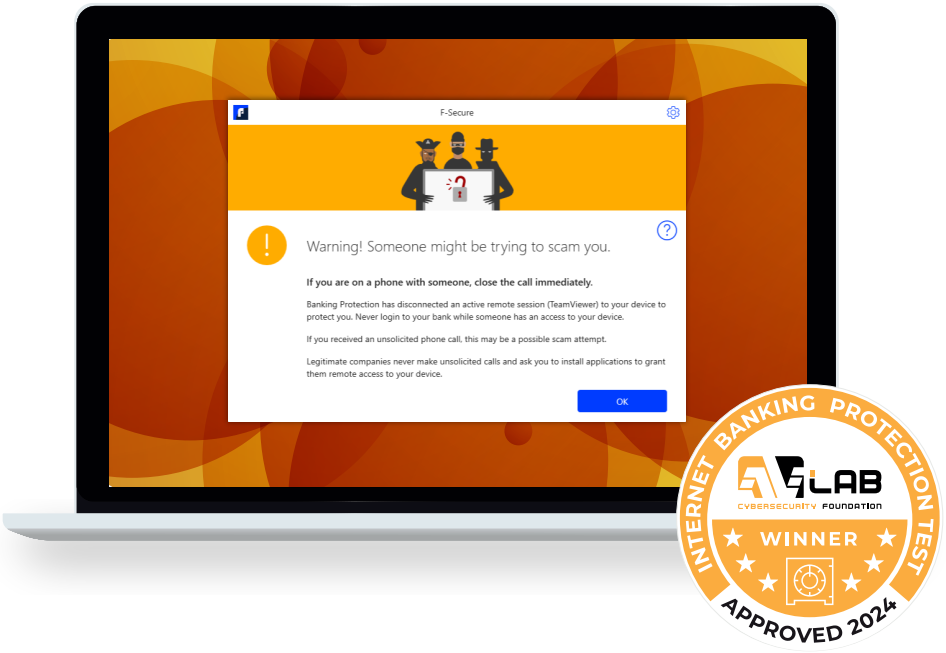
F-Secure

F-SECURE Total

Specjalny moduł do ochrony bankowości:

Secure Browsing & Banking Protection
Ustawienia programu: domyślne

PRZECHWYTYWANIE SCHOWKA	✓
PODMIANA SCHOWKA	✓
REJESTROWANIE KLAWIATURY	✓
PRZECHWYTYWANIE ZRZUTÓW EKRANU	✓
WYKRYWANIE ZDALNEGO STEROWANIA	✓
WYKRYWANIE KRADZIEŻY DANYCH Z DYSKU	✓



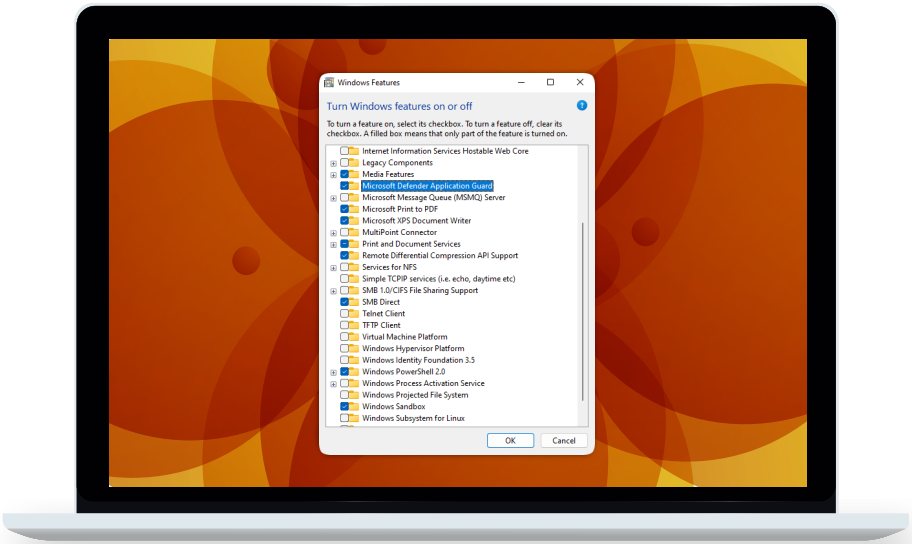
Podczas aktywnego trybu bankowego połączenia internetowe są zatrzymywane na czas działania ochrony, co zapobiega nawiązywaniu połączeń przez niezaufane aplikacje inne niż przeglądarka. Nieznane oprogramowanie (w tym posiadające podpis cyfrowy) nie może łączyć się z serwerem hakera. I na przykład, gdy plik jest uruchamiany po raz pierwszy, to F-Secure weryfikuje jego bezpieczeństwo w usłudze reputacji plików Security Cloud. Jeśli nie można zweryfikować bezpieczeństwa pliku 0-day, technologia DeepGuard zaczyna monitorować jego zachowanie i automatycznie blokuje. Dodatkowo Remote Access Blocker zapobiega przed oszustwami na tzw. konsultantów telefonicznych, którzy żądają od ofiary podania ID oraz hasła do zdalnego połączenia, aby przejąć kontrolę nad komputerem i sesją bankową.

MICROSOFT Defender

Specjalny moduł do ochrony bankowości:

Application Guard
Ustawienia programu: domyślne

PRZECHWYTYWANIE SCHOWKA	✓
PODMIANA SCHOWKA	✓
REJESTROWANIE KLAWIATURY	✗
PRZECHWYTYWANIE ZRZUTÓW EKRANU	✗
WYKRYWANIE ZDALNEGO STEROWANIA	✗
WYKRYWANIE KRADZIEŻY DANYCH Z DYSKU	✗



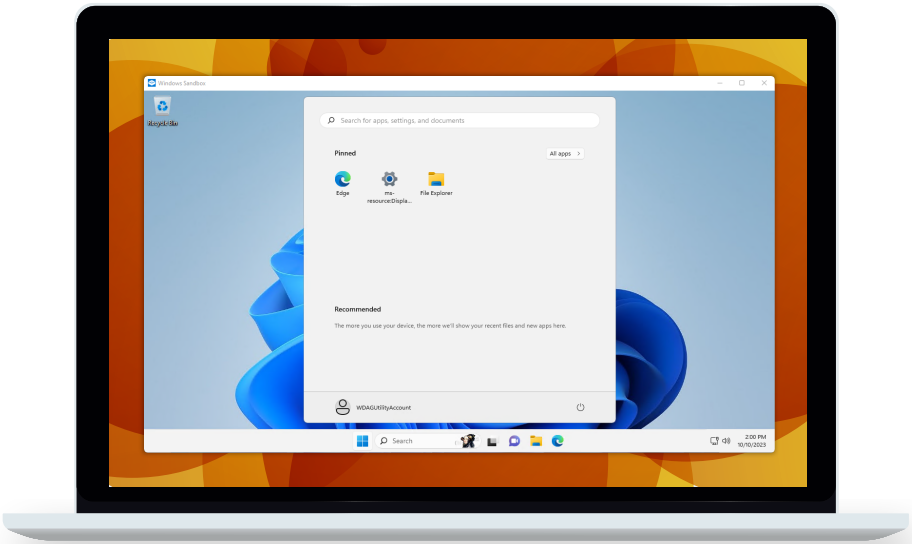
Microsoft w pierwszej kolejności umożliwia izolowanie procesów przeglądarki Edge dzięki technologii Application Guard, która odpowiada za otwieranie niezaufanych plików w izolowanym kontenerze od systemu operacyjnego, ale nie działa to w drugą stronę. Nasze testy wykazały, że niezaufane oprogramowanie może uzyskać dostęp do danych wprowadzanych do obszaru izolowanej karty Edge.

MICROSOFT Defender

Specjalny moduł do ochrony bankowości:

Windows Sandbox
Ustawienia programu: domyślne

PRZECHWYTYWANIE SCHOWKA	✓
PODMIANA SCHOWKA	✓
REJESTROWANIE KLAWIATURY	✗
PRZECHWYTYWANIE ZRZUTÓW EKRANU	✗
WYKRYWANIE ZDALNEGO STEROWANIA	✗
WYKRYWANIE KRADZIEŻY DANYCH Z DYSKU	✗



Windows Sandbox to izolowana przestrzeń w systemie Windows, wykorzystująca technologię wirtualizacji, która pozwala na bezpieczne uruchamianie aplikacji. Działa niezależnie od głównego systemu operacyjnego, co oznacza, że stan środowiska w piaskownicy jest resetowany po zakończeniu każdej sesji. Narzędzie jest przydatne do testowania nieznanych aplikacji lub przeglądania niezaufanych stron internetowych. Windows Sandbox teoretycznie nie jest przeznaczony do wykonywania transakcji finansowych w Internecie. Na podstawie wyników z testu nieznane oprogramowanie uruchomione na głównym systemie może w pewnych scenariuszach uzyskać dostęp do izolowanej przestrzeni.

MKS_VIR Internet Security

Specjalny moduł do ochrony bankowości:

Safe Browser
Ustawienia programu: domyślne

PRZECHWYTYWANIE SCHOWKA	✓
PODMIANA SCHOWKA	✓
REJESTROWANIE KLAWIATURY	✓
PRZECHWYTYWANIE ZRZUTÓW EKRANU	✓
WYKRYWANIE ZDALNEGO STEROWANIA	✓
WYKRYWANIE KRADZIEŻY DANYCH Z DYSKU	✓

Przeglądarka mks_vir Safe Browser zapewnia wysoki poziom bezpieczeństwa podczas wykonywania operacji bankowych, płatniczych i przekazywania wrażliwych danych. Ściśle współpracuje z pozostałymi modułami pakietu antywirusowego: stale monitoruje poziom bezpieczeństwa systemu i zabezpiecza przed nieautoryzowanym dostępem do kluczowych danych. Po każdorazowym uruchomieniu producent zastosował „białe listy" procesów, dzięki którym w specjalnym oknie mks_vir wyświetlane są wszystkie podejrzane, aktywne procesy, jeszcze przed uruchomieniem przeglądarki. Użytkownik może zdecydować, które z nich zamknąć, aby dostosować środowisko pracy do indywidualnych preferencji.

Quick Heal

Security Simplified

QUICK HEAL Total Security

Specjalny moduł do ochrony bankowości:

Safe Browser + Safe Banking
Ustawienia programu: domyślne

PRZECHWYTYWANIE SCHOWKA	✓
PODMIANA SCHOWKA	✓
REJESTROWANIE KLAWIATURY	✓
PRZECHWYTYWANIE ZRZUTÓW EKRANU	✓
WYKRYWANIE ZDALNEGO STEROWANIA	✓
WYKRYWANIE KRADZIEŻY DANYCH Z DYSKU	✓

Quick Heal zabezpiecza sesję bankowości na kilka sposobów. Umożliwia uruchomienie przeglądarki w piaskownicy, która ma na celu skutecznie zabezpieczać urządzenie przed potencjalnymi zagrożeniami. Dodatkowo dostępny jest moduł Safe Banking, który poprzez wirtualne środowisko izoluje system hosta od gościa, zapewniając kompleksową i wyspecjalizowaną ochronę. Cały mechanizm zabezpiecza urządzenie z Windows przed podmianą adresów DNS. Pracuje w czasie rzeczywistym, analizując bezpieczeństwo odwiedzanych stron internetowych i blokuje podejrzane połączenia.

xcitium

The Power of Zero. Unleashed.

XCITIUM (Comodo) Internet Security Pro

Specjalny moduł do ochrony bankowości:

Secure Shopping
Ustawienia programu: domyślne

PRZECHWYTYWANIE SCHOWKA	✓
PODMIANA SCHOWKA	✓
REJESTROWANIE KLAWIATURY	✓
PRZECHWYTYWANIE ZRZUTÓW EKRANU	✓
WYKRYWANIE ZDALNEGO STEROWANIA	✓
WYKRYWANIE KRADZIEŻY DANYCH Z DYSKU	✓

Technologia Secure Shopping zabezpiecza urządzenie przed keyloggerami, trojanami, screenloggerami, a także izoluje procesy, uniemożliwiając im wstrzykiwania złośliwego kodu do przeglądarki w środowisku wirtualnym. Tak zwany sandbox realizuje ochronę sesji online na kilka sposobów: automatycznie zapewnia protekcję przed zagrożeniami 0-day, których silnik antywirusowy nie zdoła wykryć za pomocą sygnatur i skanowania plików w chmurze. Po drugie ostrzega, jeżeli aktywne jest zdalne połączenie z komputerem. Po trzecie wykrywa fałszywe certyfikaty SSL, aby powstrzymać ataki typu man-in-the-middle. Wreszcie po czwarte uniemożliwia hakerom i złośliwemu oprogramowaniu wykonywanie zrzutów ekranu z sesji użytkownika. Moduł Secure Shopping bez większych obaw o bezpieczeństwo można wykorzystać do uruchamiania podejrzanych plików.

Produkt	Specjalny Moduł do Ochrony Bankowości	Przechwytywanie Schowka	Podmiana Schowka	Rejestrowanie Klawiatury	Wykonywanie Zrzutów Ekranu	Wykrywanie Zdalnego Sterowania	Kradzież Danych z Dysku
AVAST Free Antivirus	Avast Secure Browser & Bank Mode	✓	✓	✓	✓	✓	✓
BITEDEFENDER Total Security	Bitdefender Safepay	✗	✗	✓	✓	✗	✗
F-SECURE Total	Secure Browsing & Banking Protection	✓	✓	✓	✓	✓	✓
MICROSOFT Defender	Application Guard	✓	✓	✗	✗	✗	✗
MICROSOFT Defender	Windows Sandbox	✓	✓	✗	✗	✗	✗
MKS Internet Security	Safe Browser	✓	✓	✓	✓	✓	✓
QUICK HEAL Total Security	Safe Browser + Safe Banking	✓	✓	✓	✓	✓	✓
XCITIUM (Comodo) Internet Security Pro	Secure Shopping	✓	✓	✓	✓	✓	✓

IV Wnioski z testu

Część rozwiązań do bezpiecznej bankowości jest dostępna jako niezależne oprogramowanie np. Avast Secure Browser. Pamiętaj, że nigdy nie będzie to kompleksowe zabezpieczenie i na pewno nie będzie bardziej skuteczne przeciwko zagrożeniom niż pełnoprawny pakiet ochronny.

Zagrożenia użyte w teście stanowiły tak zwane potencjalnie niebezpieczne oprogramowanie 0-day, które w dniu testowania było nieznane dla producentów. Jest to dobra sytuacja, ponieważ właśnie w taki sposób możliwe jest przetestowanie rozwiązania przed czymś zupełnie nowym.

W scenariuszu nr 5 użyliśmy oprogramowania do zdalnych połączeń, konferencji, zarządzania komputerem, które jest całkowicie legalne i traktowane jako bezpieczne, dlatego przez niektórych producentów może być dopuszczone do działania. Niemniej uważamy, że „tryb bankowy" powinien być szczególnie wrażliwym obszarem, do którego nic lub prawnie nic nie powinno mieć dostępu.

Ochronę tego obszaru, także w kontekście oprogramowania do zdalnego zarządzania, najlepiej realizuje Avast, F-Secure, mks_vir, Quick Heal i Comodo, ponieważ obierają model podobny do architektury Zero-Trust. Biorąc pod uwagę wyniki, jest to najbardziej rozsądne podejście do zabezpieczania sesji bankowej, która jest szczególnie ważna dla użytkowników końcowych. Taka ochrona zapewnia minimalne uprawnienia, niezbędne do zrealizowania przelewu i opiera się na nowoczesnym podejściu do proaktywnego bezpieczeństwa w czasie rzeczywistym.

W żadnym ze scenariuszy nie wyłączaliśmy ochrony antywirusowej, ponieważ po dezaktywacji składników, bezpieczeństwo użytkownika zostałoby wystawione na ryzyko ataku. Niezależne moduły trybu bankowego bez udziału ochrony w czasie rzeczywistym mogą nie wystarczyć przeciwko atakom na pieniądze użytkownika.

AVLab
CYBERSECURITY FOUNDATION

Fundacja AVLab dla Cyberbezpieczeństwa jako niezależna organizacja stoi na straży ochrony prywatności i bezpieczeństwa w Internecie. Budujemy świadomość użytkowników z zakresu ochrony cyfrowej. Wydajemy opinie, techniczne analizy oraz testy rozwiązań informatycznych w sferze cyberbezpieczeństwa. Naszym najmocniejszym atutem są wnikliwe i szczegółowe recenzje, przygotowywanie raportów związanych z prywatnością i ochroną urządzeń końcowych, a w szczególności testy bezpieczeństwa, dzięki którym jesteśmy rozpoznawalni na całym świecie, jako jedno z najpopularniejszych laboratoriów testujących.

Jesteśmy stowarzyszeni w grupie roboczej non-profit AMTSO (Anti-Malware Testing Standards Organization). W ramach pełnionych funkcji w międzynarodowych środowisku ekspertów pracujemy nad poprawą transparentności, obiektywności oraz jakości przeprowadzanych testów oprogramowania ochronnego.

Aby poznać szczegóły techniczne producenci mogą kierować swoje zapytania na adres: kontakt@avlab.pl

amtso
The cybersecurity industry's testing standard community
MEMBER