AVLAB

CYBERSECURITY FOUNDATION

Analysis of modules for protection of online banking and payments

INTERNET BANKING PROTECTION TEST

AVLAB CYBERSECURITY FOUNDATION

WINNER

APPROVED 2024

amtso

The cybersecurity industry's testing standard community

MEMBER

Test of a banking mode in modern antivirus solutions

December 2023

Na skróty

I

Why online payments protection is so important?

Dedicated protection for online payments is designed to secure your finances, personal data, and protect you against cybercrime. Thanks to it, you take the protection of banking services and online transactions to a higher level. You have a greater guarantee that your money and data are safe. By using security solutions recommended by AVLab, you significantly minimize the risk of a cyberattack.

Most modern antivirus applications for macOS and Windows provide basic protection for online banking and payments against advanced threats. Such technologies include, for example: anti-phishing, anti-malware, anti-keylogger, anti-screenlogger, blocking connections of untrusted applications and scripts, detecting system changes in DNS servers, and other functionalities. However, some developers offer a user much more – the so-called specialized module that is intended to protect an operating system when making online payments or other important and confidential operations on files and data.

The main objective of our test was to test modules to protect against attacks on online banking, regardless of the known and original protocol for initiating a cyberattack. To perform the analysis, we used real malware in a simulated scenario. The goal of testers was to steal information from the device protected by antivirus software at the time of using a dedicated online banking and payments protection mode.

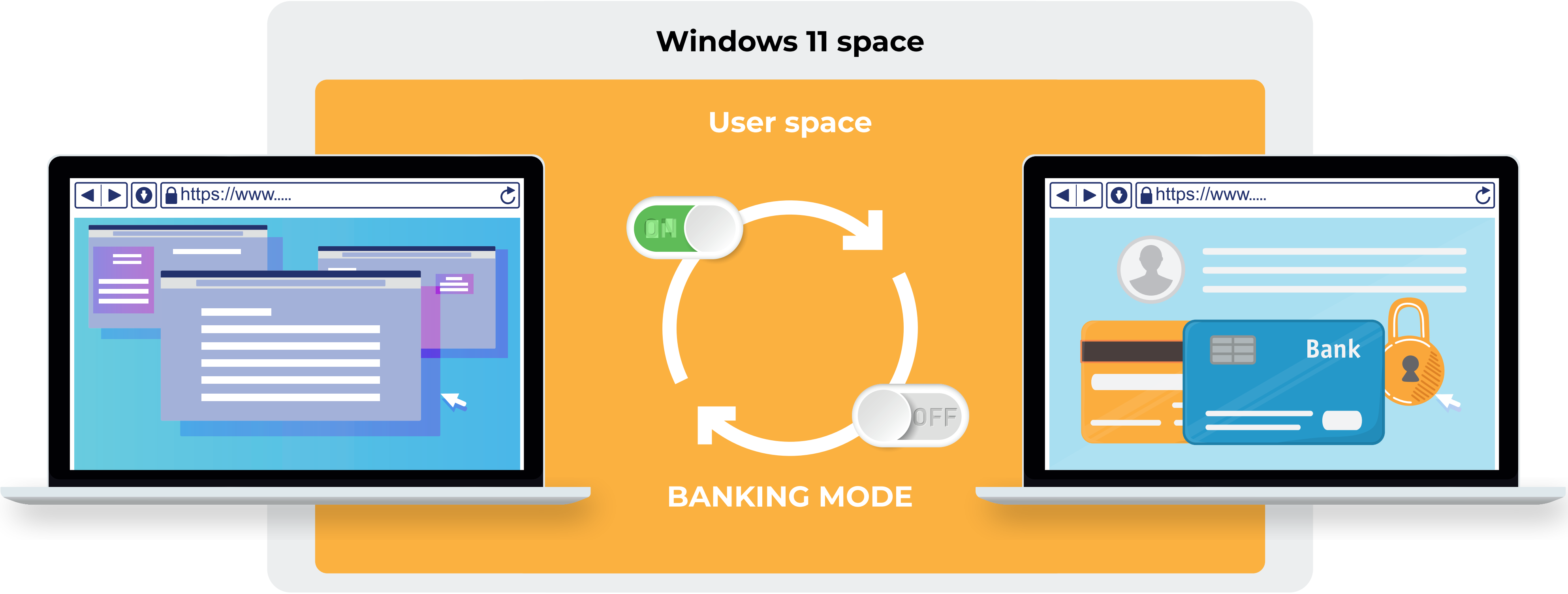
In this edition, we used Telegram to send the victim a threat in the form of a trusted application from a "familiar contact" – let us say we were uploading a beta version of a new game that our buddy programmed. A similar attack can occur using any messenger.
Delivering malware to the system via messenger is, at some point, bypassing the basic layer of protection.
This gives the attacker a slightly greater advantage, but also better shows the contact between malware and security technology.

In this scenario, a file threat in the first phase bypasses its identification in a browser.
Developers have mastered this technique well, therefore, this time we did not want to use a browser as an attack initiation vector.

II

Methodology

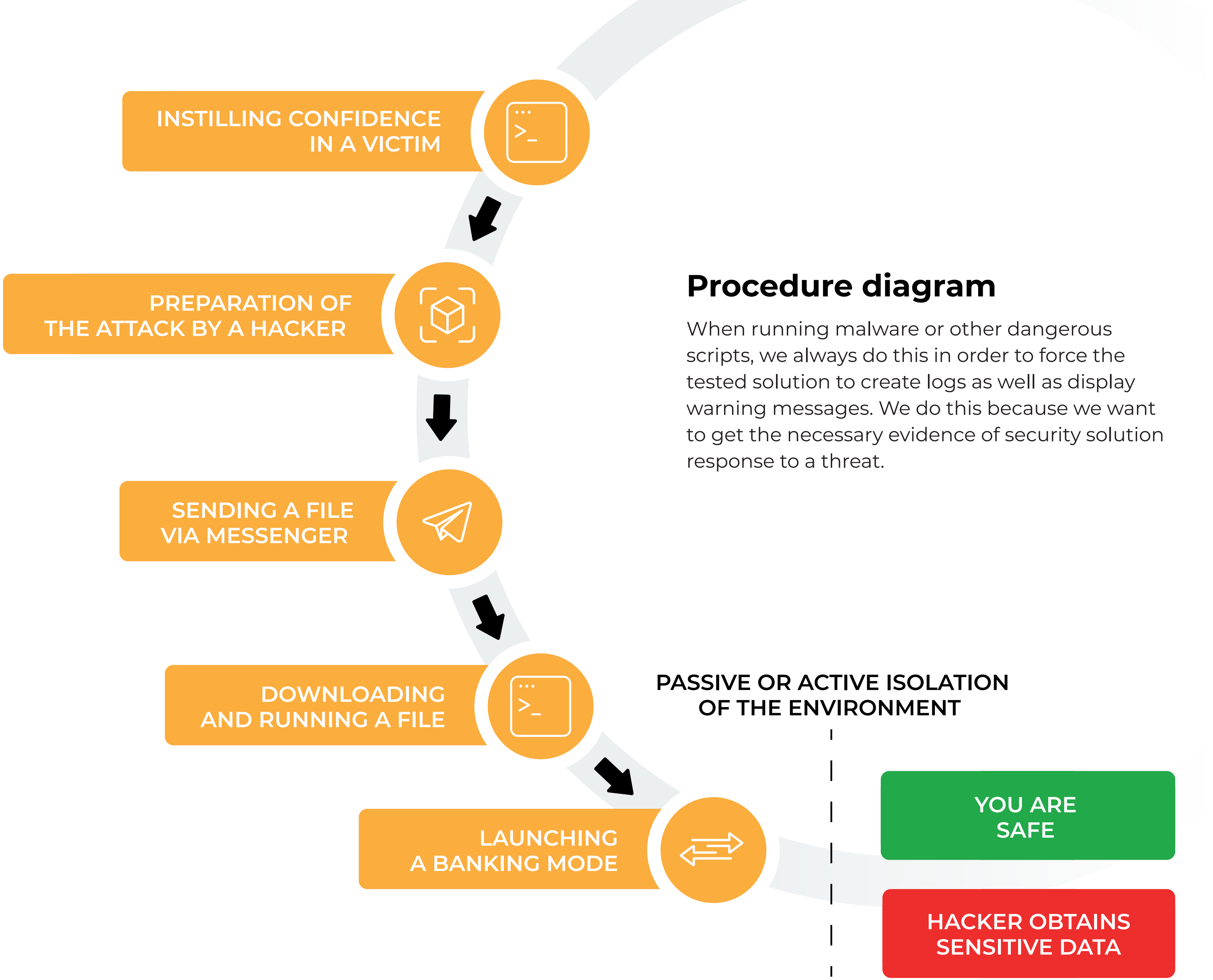
The methodology was developed in accordance with the Anti-Malware Testing Standard Organization. This gives the reader a guarantee that we have treated each developer in the same way, giving them time to analyze the provided logs, and refer to the results.



We downloaded malware to the system via the Telegram messenger – a not very popular protocol for spreading threats. The task for the tested solutions with the banking mode running in the background was to detect and stop an attack at any stage: before launching, after starting, or after establishing a connection to the server owned by a hacker.

Procedure diagram

When running malware or other dangerous scripts, we always do this in order to force the tested solution to create logs as well as display warning messages. We do this because we want to get the necessary evidence of security solution response to a threat.



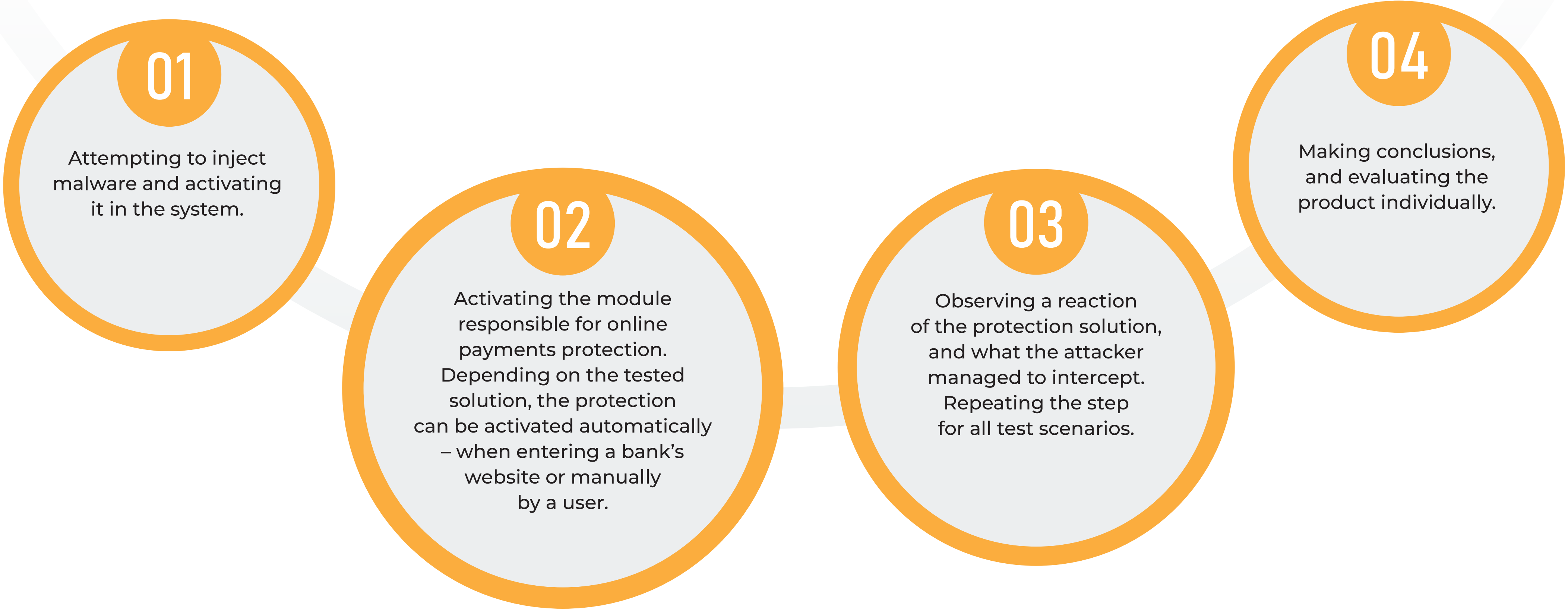
INSTILLING CONFIDENCE IN A VICTIM
PREPARATION OF THE ATTACK BY A HACKER
SENDING A FILE VIA MESSENGER
DOWNLOADING AND RUNNING A FILE
LAUNCHING A BANKING MODE
PASSIVE OR ACTIVE ISOLATION OF THE ENVIRONMENT
YOU ARE SAFE
HACKER OBTAINS SENSITIVE DATA

What did we use?

We used the Python programming language and the ChatGPT tool to prepare malicious EXE files which we then used in simulated cyberattacks. The prepared applications were delivered to the system via the Telegram messenger.

In this scenario, there was no need for the Python environment to be present on the victim device, as the malware had previously been compiled into a single EXE file using the PyInstaller tool. In addition, we signed some files with our own SSL certificate generated by Microsoft SignTool, so it did not come from any trusted publisher (no CA Root, Certification Authority).

We followed the scenario below



01

Attempting to inject malware and activating it in the system.

02

Activating the module responsible for online payments protection. Depending on the tested solution, the protection can be activated automatically – when entering a bank's website or manually by a user.

03

Observing a reaction of the protection solution, and what the attacker managed to intercept. Repeating the step for all test scenarios.

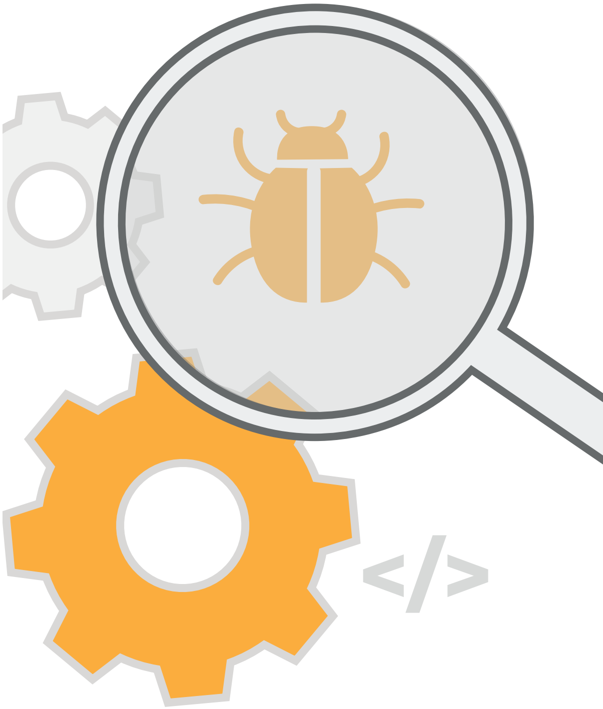
04

Making conclusions, and evaluating the product individually.

Software we tested and settings

Security suites were installed on the default settings. If, for example, keylogger protection was disabled by default, we activated this feature. Therefore, when malware was not detected on the default settings, we immediately experimented with other settings (if available).

	Product	Special Module for Banking Protection
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



Malware Injection Method - Why Messenger?

Delivering a malicious file to the victim's system is an important aspect of testing. Usually, malware is downloaded to the system either via email or a browser. We wanted to avoid an unambiguous situation where a file enters the system via known vectors because developers have mastered techniques of blocking 0-day files to a good extent.

This time, we used the Telegram messenger with its own file transfer and encryption algorithm.
Uploaded files in messenger are saved directly on a drive – Telegram does not create some kind of links to a file, as is the case in Discord.

It is worth noting here that when you send an attachment via Discord, a hyperlink to it is created in the domain: https://cdn.discordapp.com/attachments/

A link to a file from Discord has the following structure and comes from a trusted domain which does not mean that it is safe:

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

The difference between Telegram and Discord is subtle.
Telegram uses a proprietary protocol for transferring and encrypting data. This bypasses the well-known and popular vector of delivering a file to the system via a browser.
On the other hand, the link from the Discord messenger is opened in a default browser which is why antivirus protection mechanisms are able to identify the threat at an early stage.

III

Results

Description of attacks

01

Hijacking system clipboard
The test verifies whether malware written in Python can capture the contents of the system clipboard and send that information to the Telegram account controlled by a hacker.

02

Swapping system clipboard
The test verifies whether the malware can modify the contents of the system clipboard, e.g. copied bank account number to a different one while opening a bank website in a secure environment.
The account number was retrieved from a remote location on pastebin.com.

03

Logging keystrokes
The test verifies whether the malware can register keystrokes on a keyboard when using the so-called secure browser or banking mode, and send sensitive information to a messenger account controlled by an attacker.

04

Capturing screenshots
The test verifies whether the malware written in Python can take screenshots while using online banking and send them to a hacker.

05 *

Remote control of computer
The test verifies whether a hacker using a social engineering attack and legitimate software can control a user's computer while online payments mode is active.
We used legitimate Team Viewer software in the attack. *

06

Searching drive and file theft
The test verifies whether the malware can scan the user's drive for selected file extensions and send them to the attacker's Telegram account.

* This is a specific scenario because legitimate software will not always be blocked, and it will depend on the user’s decision whether or not to continue its operation. Some developers use certain mechanisms of application whitelisting or a special session separated from the user's desktop so that nothing is revealed when the banking mode is active.

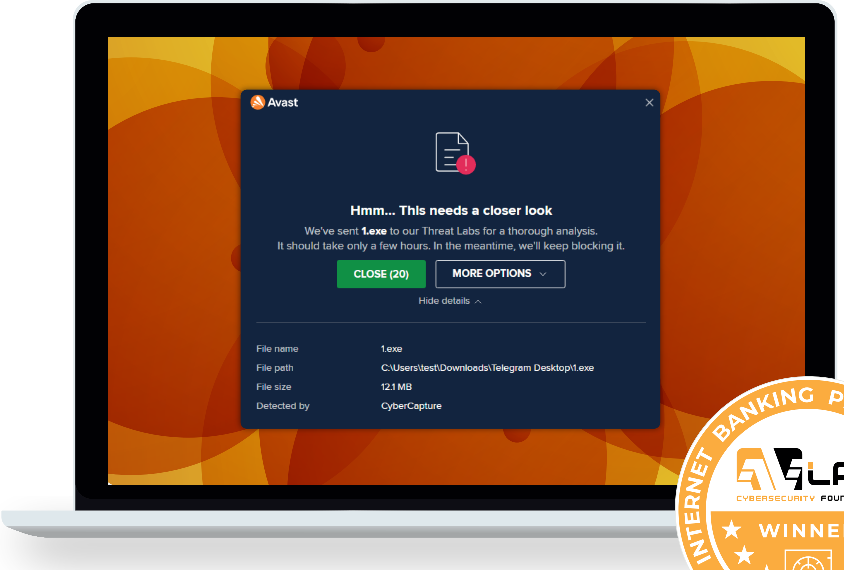
Avast

AVAST Free Antivirus

Special Module for Banking Protection

Avast Secure Browser & Bank Mode
Application Settings: default

HIJACKING CLIPBOARD	✓
SWAPPING CLIPBOARD	✓
LOGGING KEYSTROKES	✓
CAPTURING SCREENSHOTS	✓
DETECTING REMOTE CONNECTION	✓
DETECTING DATA THEFT FROM DRIVE	✓



Hmm... This needs a closer look

We've sent **1.exe** to our Threat Labs for a thorough analysis.
It should take only a few hours. In the meantime, we'll keep blocking it.

File name 1.exe
File path C:\Users\test\Downloads\Telegram Desktop\1.exe
File size 12.1 MB
Detected by CyberCapture

BANKING PROTECTION INTERNET TEST
AVLAB CYBERSECURITY FOUNDATION
WINNER
APPROVED 2024

Special Banking Mode creates for a user a virtual desktop which shares with an operating system the basic drivers necessary to operate the connected devices: keyboard, mouse, monitor, drives, network, etc. In this mode, the environment separated from the Windows system prevents malware from breaking into the user's session in banking mode. While apart from banking mode, CyberCapture technology is responsible for user security, blocking access to unknown malware of 0-day file and preventing it from being run until it is manually analyzed by a team of experts from Avast Threat Labs.

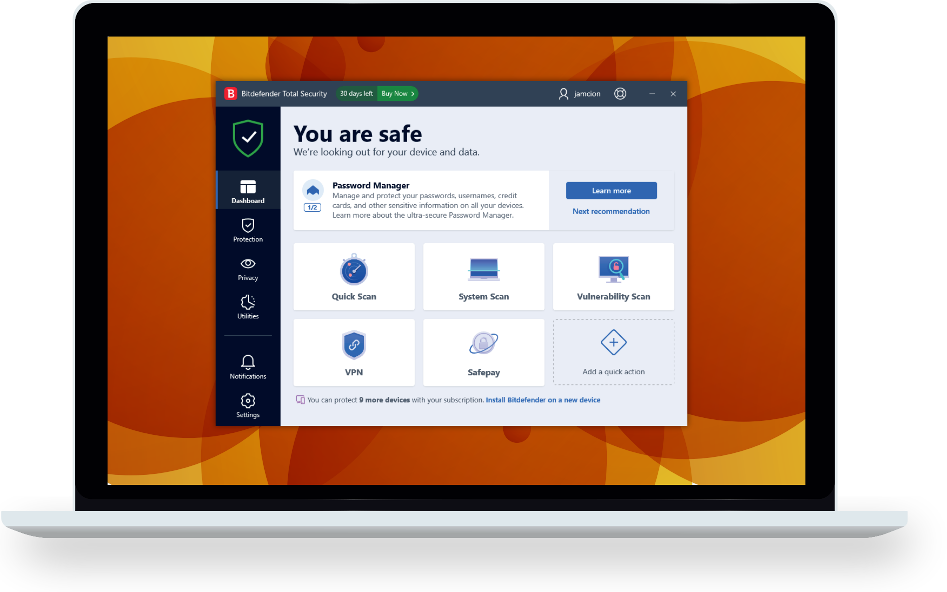
Bitdefender

BITEDEFENDER Total Security

Special Module for Banking Protection

Bitdefender Safepay
Application Settings: default

HIJACKING CLIPBOARD	✗
SWAPPING CLIPBOARD	✗
LOGGING KEYSTROKES	✓
CAPTURING SCREENSHOTS	✓
DETECTING REMOTE CONNECTION	✗
DETECTING DATA THEFT FROM DRIVE	✗



You are safe

We're looking out for your device and data.

Password Manager
Manage and protect your passwords, usernames, credit cards, and other sensitive information on all your devices. Learn more about the ultra-secure Password Manager.

You can protect **9 more devices** with your subscription. Install Bitdefender on a new device

When launched, Bitdefender Safepay provides real-time protection against fraud, phishing, malware that is designed to prevent logging keystrokes and capturing screenshots. A user can switch between a virtual, secure environment called Bitdefender Safepay and a desktop. During these activities, it is possible to use the computer as usual, without unnecessarily taking up system resources. Theoretically, if the Safepay session is active, it does not allow unknown applications to use the Safepay virtual environment. Unfortunately, test cases have proven that we have succeeded.

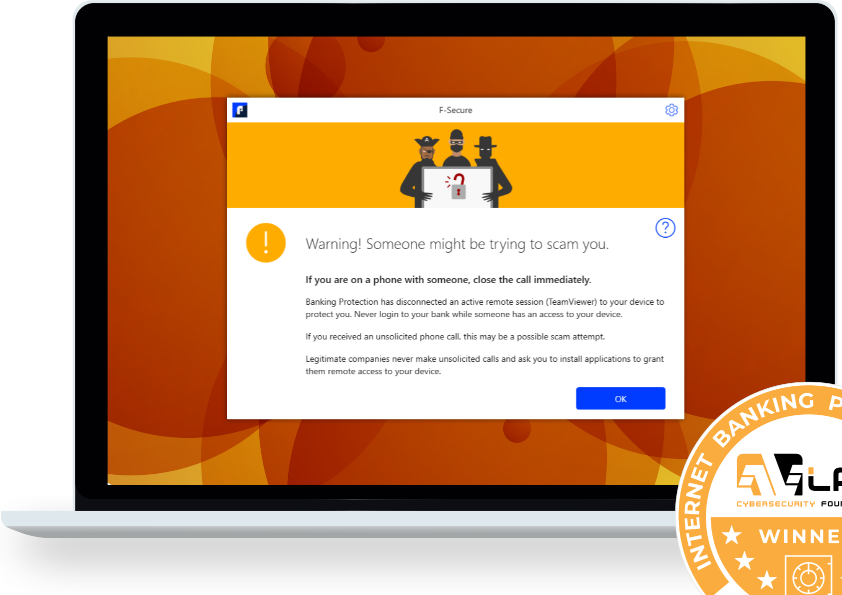
F-Secure®

F-SECURE Total

Special Module for Banking Protection

Secure Browsing & Banking Protection
Application Settings: default

HIJACKING CLIPBOARD	✓
SWAPPING CLIPBOARD	✓
LOGGING KEYSTROKES	✓
CAPTURING SCREENSHOTS	✓
DETECTING REMOTE CONNECTION	✓
DETECTING DATA THEFT FROM DRIVE	✓



Warning! Someone might be trying to scam you.

If you are on a phone with someone, close the call immediately.

Banking Protection has disconnected an active remote session (TeamViewer) to your device to protect you. Never login to your bank while someone has an access to your device.

If you received an unsolicited phone call, this may be a possible scam attempt.

Legitimate companies never make unsolicited calls and ask you to install applications to grant them remote access to your device.

INTERNET BANKING PROTECTION TEST
AVLAB CYBERSECURITY FOUNDATION
WINNER
APPROVED 2024

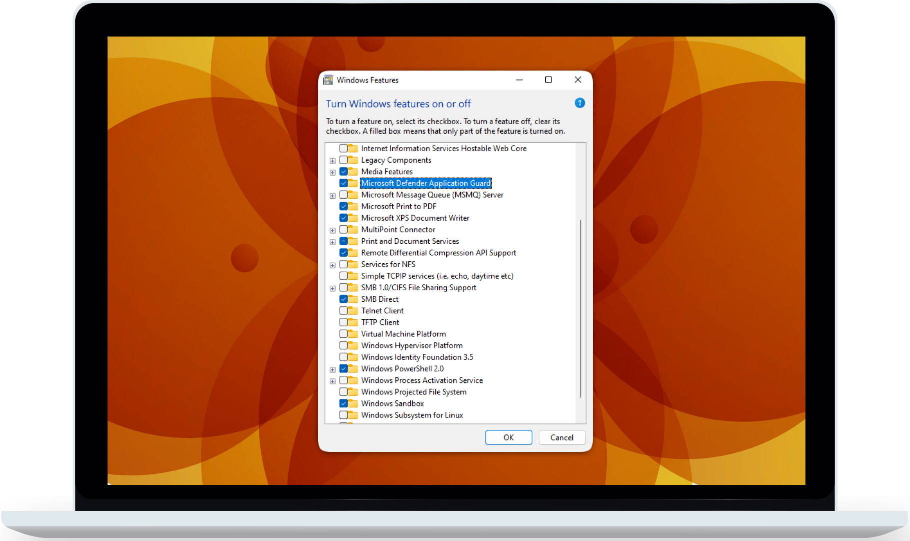
During active banking mode, Internet connections are stopped for the duration of protection which prevents untrusted applications other than the browser from making connections. Unknown software (including those with a digital signature) cannot connect to the hacker server. For example, when a file is started for the first time, F-Secure verifies its security in the Security Cloud file reputation service. If the security of the 0-day file cannot be verified, DeepGuard technology begins to monitor its behavior and automatically blocks it. In addition, Remote Access Blocker prevents fraud on so-called telephone consultants who request the victim to provide an ID and password for a remote connection to take control of the computer and the banking session.

MICROSOFT Defender

Special Module for Banking Protection

Application Guard
Application Settings: default

HIJACKING CLIPBOARD	✓
SWAPPING CLIPBOARD	✓
LOGGING KEYSTROKES	✗
CAPTURING SCREENSHOTS	✗
DETECTING REMOTE CONNECTION	✗
DETECTING DATA THEFT FROM DRIVE	✗



Windows Features

Turn Windows features on or off

To turn a feature on, select its checkbox. To turn a feature off, clear its checkbox. A filled box means that only part of the feature is turned on.

- □ Internet Information Services Hostable Web Core
- □ Legacy Components
- ☑ Media Features
- ☑ Microsoft Defender Application Guard
- □ Microsoft Message Queue (MSMQ) Server
- ☑ Microsoft Print to PDF
- ☑ Microsoft XPS Document Writer
- □ MultiPoint Connector
- ■ Print and Document Services
- ☑ Remote Differential Compression API Support
- □ Services for NFS
- □ Simple TCPIP services (i.e. echo, daytime etc)
- □ SMB 1.0/CIFS File Sharing Support
- ☑ SMB Direct
- □ Telnet Client
- □ TFTP Client
- □ Virtual Machine Platform
- □ Windows Hypervisor Platform
- □ Windows Identity Foundation 3.5
- ☑ Windows PowerShell 2.0
- □ Windows Process Activation Service
- □ Windows Projected File System
- ☑ Windows Sandbox
- □ Windows Subsystem for Linux

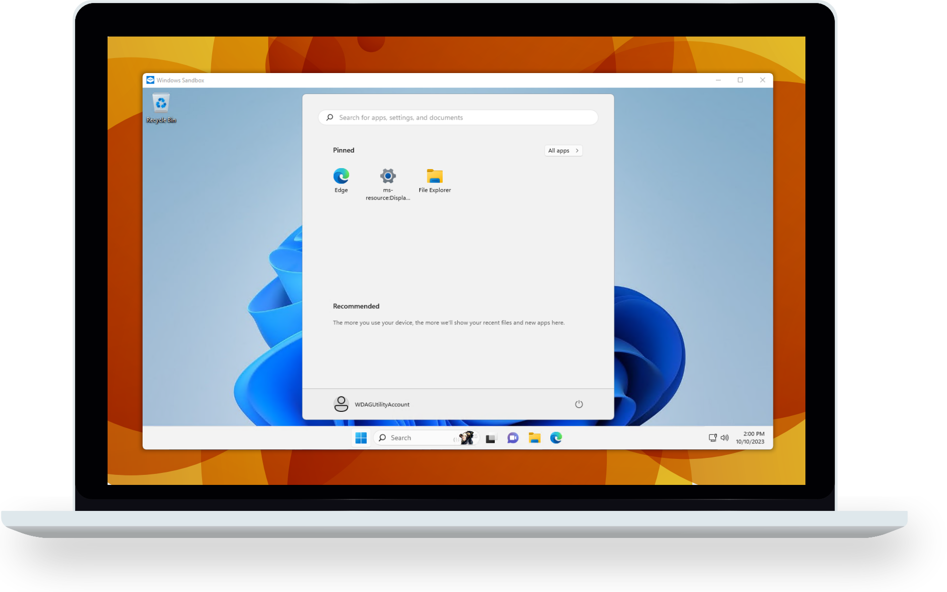
Microsoft first allows to isolate processes of the Edge browser using the Application Guard technology that is responsible for opening untrusted files in a container isolated from the operating system, but it does not work the other way around. Our tests have shown that untrusted software can access data entered into the isolated Edge area.

MICROSOFT Defender

Special Module for Banking Protection

Windows Sandbox
Application Settings: default

HIJACKING CLIPBOARD	✓
SWAPPING CLIPBOARD	✓
LOGGING KEYSTROKES	✗
CAPTURING SCREENSHOTS	✗
DETECTING REMOTE CONNECTION	✗
DETECTING DATA THEFT FROM DRIVE	✗



The more you use your device, the more we'll show your recent files and new apps here.

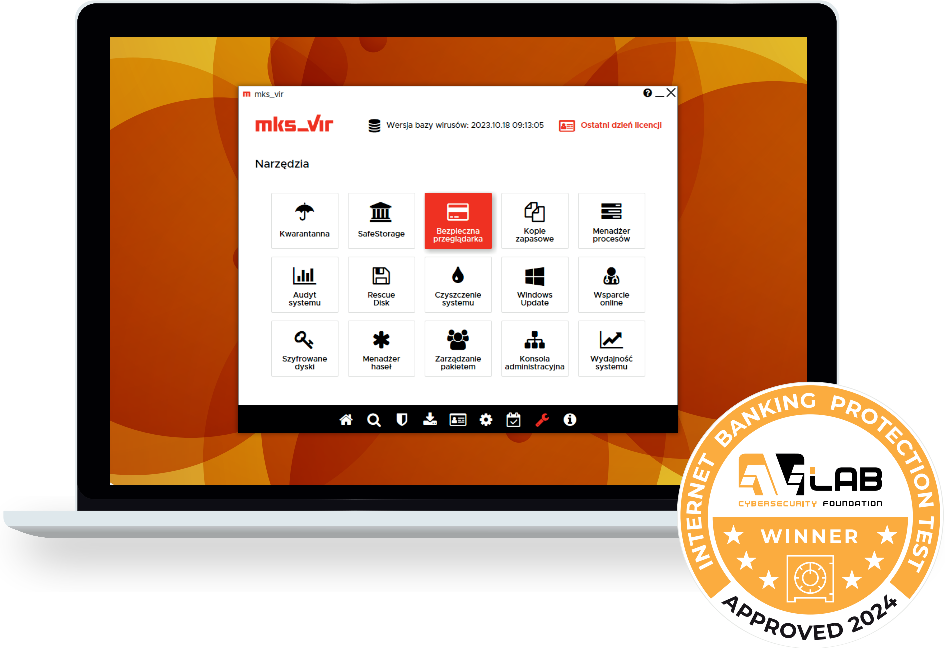
Windows Sandbox is an isolated space in Windows that uses virtualization technology which allows applications to run securely. It operates independently of the hosting system which means that the state of the sandbox environment is reset after the end of each session. The tool is useful for testing unknown applications or browsing untrusted websites. Theoretically, Windows Sandbox is not designed to perform online payments on the Internet. Based on the test results, unknown software running on the hosted system can access the isolated space in certain scenarios.

MKS_VIR Internet Security

Special Module for Banking Protection

Safe Browser
Application Settings: default

HIJACKING CLIPBOARD	✓
SWAPPING CLIPBOARD	✓
LOGGING KEYSTROKES	✓
CAPTURING SCREENSHOTS	✓
DETECTING REMOTE CONNECTION	✓
DETECTING DATA THEFT FROM DRIVE	✓



Wersja bazy wirusów: 2023.10.18 09:13:05

BANKING PROTECTION TEST
INTERNET
AVLAB CYBERSECURITY FOUNDATION
WINNER
APPROVED 2024

Mks_vir Safe Browser provides an extremely high level of security when performing banking and payment operations, and processing sensitive data. The browser works closely with the rest of mks_vir suite modules, constantly monitoring the security level of the system and preventing from unauthorized access to key data. The developer has used process “whitelists", thanks to which all suspicious active processes are displayed in a special mks_vir window even before launching a browser. A user can decide which of them to close in order to adapt the work environment to individual preferences.

Quick Heal®

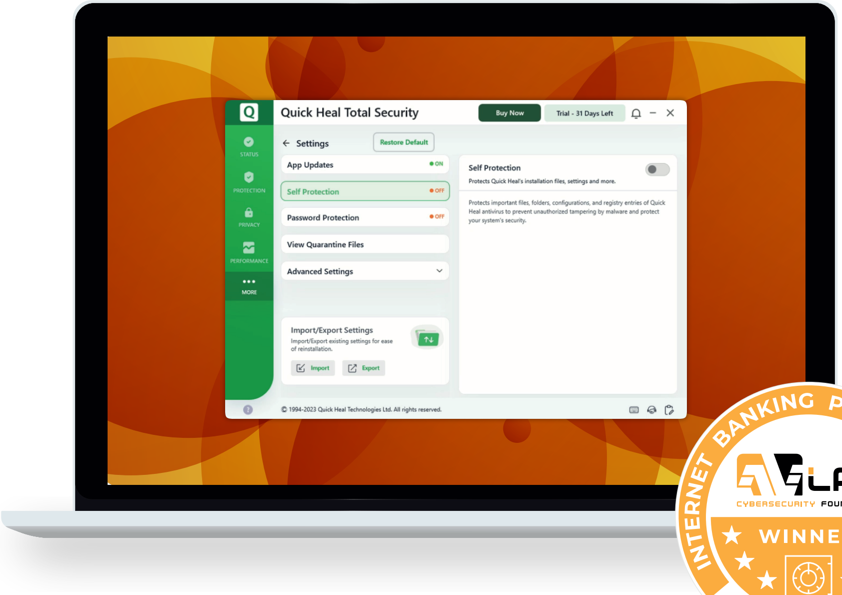
Security Simplified

QUICK HEAL Total Security

Special Module for Banking Protection

Safe Browser + Safe Banking
Application Settings: default

HIJACKING CLIPBOARD	✓
SWAPPING CLIPBOARD	✓
LOGGING KEYSTROKES	✓
CAPTURING SCREENSHOTS	✓
DETECTING REMOTE CONNECTION	✓
DETECTING DATA THEFT FROM DRIVE	✓



Quick Heal Total Security

Settings

App Updates ● ON

Self Protection ● OFF

Password Protection ● OFF

View Quarantine Files

Advanced Settings

Import/Export Settings

Import/Export existing settings for ease of reinstallation.

Self Protection

Protects Quick Heal's installation files, settings and more.

Protects important files, folders, configurations, and registry entries of Quick Heal antivirus to prevent unauthorized tampering by malware and protect your system's security.

© 1994-2023 Quick Heal Technologies Ltd. All rights reserved.

INTERNET BANKING PROTECTION TEST
AVLAB
CYBERSECURITY FOUNDATION
WINNER
APPROVED 2024

Quick Heal secures your banking session in several ways. It allows to run a browser in the sandbox which is designed to effectively protect a device from potential threats. In addition, the available Safe Banking module isolates the host system from the guest using a virtual environment, providing comprehensive and specialized protection. The whole mechanism protects the device with Windows from swapping DNS addresses. It works in real time, analyzing the security of visited websites and blocks suspicious Internet connections.

xcitium

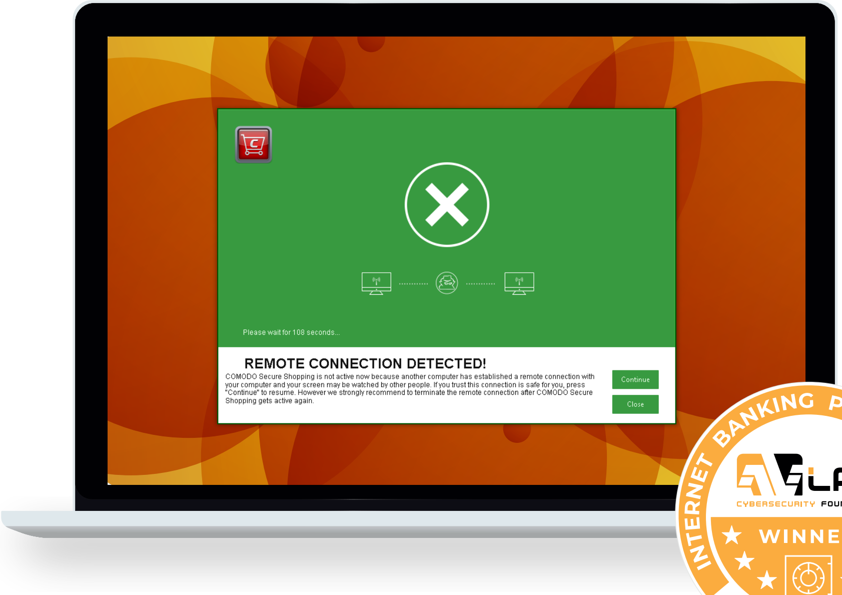
The Power of Zero. Unleashed.

XCITIUM (Comodo) Internet Security Pro

Special Module for Banking Protection

Secure Shopping
Application Settings: default

HIJACKING CLIPBOARD	✓
SWAPPING CLIPBOARD	✓
LOGGING KEYSTROKES	✓
CAPTURING SCREENSHOTS	✓
DETECTING REMOTE CONNECTION	✓
DETECTING DATA THEFT FROM DRIVE	✓



Please wait for 108 seconds...

REMOTE CONNECTION DETECTED!

COMODO Secure Shopping is not active now because another computer has established a remote connection with your computer and your screen may be watched by other people. If you trust this connection is safe for you, press "Continue" to resume. However we strongly recommend to terminate the remote connection after COMODO Secure Shopping gets active again.

INTERNET BANKING PROTECTION TEST
AVLAB CYBERSECURITY FOUNDATION
WINNER
APPROVED 2024

Secure Shopping technology protects your device against keyloggers, trojans, screenloggers, and also isolates processes, preventing them from injecting malicious code into a browser in a virtual environment. The so-called sandbox performs online session protection in several ways: it automatically provides protection against 0-day threats that the antivirus engine cannot detect using signatures and file scanning in the cloud. Secondly, it prompts if a remote connection to the computer is active. Thirdly, it detects fake SSL certificates to stop man-in-the-middle attacks. Finally, fourthly, it prevents hackers and malware from taking screenshots of a user's session. The Secure Shopping module can be used to run suspicious files without any major security concerns.

Product	Special Module for Banking Protection	Hijacking Clipboard	Swapping Clipboard	Logging keystrokes	Capturing screenshots	Detecting Remote Connection	Detecting Data Theft from Drive
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_VIR Internet Security	Safe Browser	✓	✓	✓	✓	✓	✓
QUICK HEAL Total Security	Safe Browser + Safe Banking	✓	✓	✓	✓	✓	✓
XCITIUM (Comodo) Internet Security Pro	Secure Shopping	✓	✓	✓	✓	✓	✓

IV

Conclusions from the test

Some solutions for banking protection are available as stand-alone tools, such as Avast Secure Browser. Keep in mind that this is not a full-fledged antivirus software, and will certainly not be effective against threats.

Threats (with the exception of 5th scenario) used in the test were so-called 0-day malware which were unknown to developers on the day of testing. This is a good situation because it makes possible to test the solution against something completely new.

Analyzing 5th scenario, one may have a different opinion. Namely, software for remote desktop, conferences, system management, is completely legal and treated as safe, so it can be allowed to operate. Nevertheless, we believe that the banking mode should be a particularly sensitive area to which nothing or almost nothing should have access.

This area, also in the context of remote management software, is best protected by F-Secure and mks_vir, as they have a model similar to the Zero-Trust architecture. Based on the results, this seems to be the most reasonable approach to securing a banking session which is especially important for end users. Such protection provides the minimum permissions necessary to complete funds transfer, and is based on a modern approach to proactive security in real time.

We did not disable antivirus protection in any of the scenarios. Certainly, with the exclusion of certain components, the user's security would be significantly reduced. Independent modules of the so-called secure browsers or banking mode may not be sufficient against threats selected for the test, as well as during a real attack on the user's money.

AVLAB
CYBERSECURITY FOUNDATION

The AVLab Cybersecurity Foundation is an independent organization dedicated to protecting privacy and security on the Internet. We are part of the CTF (Cyber Transparency Forum) and provide independent assessments of cybersecurity vendors' systems. We are a member of AMTSO (Anti-Malware Testing Standards Organization), which works to improve the transparency, objectivity and quality of testing.

We build awareness of users in the field of digital protection. We issue opinions, technical analyzes and tests of IT solutions in the field of cybersecurity. Our strongest assets include thorough and detailed reviews, preparation of reports related to privacy and endpoint protection, and in particular, security tests that make us recognizable all over the world as one of the most trusted and popular testing laboratories.

To learn more about other opportunities for cooperation,
please refer to our full offer and contact us.: kontakt@avlab.pl

amtso
The cybersecurity industry's
testing standard community

MEMBER

www.avlab.pl