Keywords: accreditation; assessment; testing; test plan; avlab; banking, payment protection; secure browser;

September 20, 2023
Version 1.0

Analysis of Online Payment Protection Modules in Windows 11

01 October – 31 October 2023

Sponsored and authored by:
AVLab Cybersecurity Foundation

AMTSO Standard Compliance Statement:
This Test Plan Template provides the structure for constructing a Test Plan that is compliant with the AMTSO Testing Protocol Standards. This document is an informative reference to the AMTSO Testing Protocol Standard for the Testing of Anti-Malware Solutions (the "Standard"), and specifically to the requirements within such Standard for Test Plan construction and presentation. Wherever conflicts might exist between this Template and the Live Standards Version 1.3, the Testing Protocol Standards will provide the prevailing rule.

The cybersecurity industry's
testing standard community

Table of concept

Analysis Of Online Payment Protection Modules In Windows 11 - Test Plan 2023

1. Introduction

Most modern protection software for macOS and Windows systems offer basic security for online banking and internet payments against advanced threats. Protection components include: anti-phishing, anti-malware, anti-keylogger, anti-screenlogger, blocking connections of untrusted applications and scripts, DNS-spoofing prevention, and other features. However, some solutions offer a user much more – a specialized module that has been designed to secure data and the system when making online payments, or other important and confidential operations on files and data, particularly sensitive and extremely important for a user.

The main objective of our test was to check the functionality of modules to protect against attacks on online banking, regardless of the known and baseline protocol of initiation of a cyberattack. The threat-file in the first phase of delivery to the system bypasses identification through scanning in a browser because developers have fully mastered this technique. Delivering malware to the system via messenger is sort of bypassing the first layer of protection which gives an attacker a slightly better chance, but also better captures the comparison of malware versus technology, and better reflects the usefulness of this type of protection.

Why is dedicated online money protection important?

Dedicated online money protection is essential to secure finances, personal information, and protect against cybercrime. Thanks to special security modules, you elevate protection of banking services and online transactions to the next level giving greater certainty that your money and data are safe.

2. Scope and Participations

Sample calendar of testing for October 2023

Product Vendor	***Product and Module Name***	***Version Selected or Process Used***
Bitdefender	*Bitdefender Total Security* *+ Bitdefender Safepay*	*Test will use the Latest Version available by Test Commencement Date*
Eset	*Eset Smart Security Premium* *+ Payment & Banking Protection*	*Test will use the Latest Version available by Test Commencement Date*
F-Secure	*F-Secure Total* *+ Secure Browsing & Banking Protection*	*Test will use the Latest Version available by Test Commencement Date*
GenDigital	*Avast Free Antivirus* *+ Avast Secure Browser & Bank Mode*	*Test will use the Latest Version available by Test Commencement Date*
Kaspersky	*Kaspersky Plus* *+ Safe Money*	*Test will use the Latest Version available by Test Commencement Date*
Microsoft	*Microsoft Defender +* *Windows Sandbox*	*Test will use the Latest Version available by Test Commencement Date*
Microsoft	*Microsoft Defender +* *Application Guard*	*Test will use the Latest Version available by Test Commencement Date*

mks_vir	*Mks_vir Internet Security* *+ Safe Browser*	*Test will use the Latest Version available by Test Commencement Date*
Quick Heal	*Quick Heal Total Security* *+ Safe Banking*	*Test will use the Latest Version available by Test Commencement Date*
Xcitium (Comodo)	*Xcitium Internet Security* *+ Secure Shopping*	*Test will use the Latest Version available by Test Commencement Date*

Security suites were installed on default settings, unless the table states otherwise.

In the event that malware has not been detected on default settings, we immediately experimented with other settings which was noted in the description. If, for example, keylogger protection was disabled by default, we activated the feature before starting the test.

If security software did not have a special bank mode, we included the solution in the test at the express request of the developer.

3. Methodology and Strategy

We used real malware to compare such modules. It was not a simulation of attacks, but a true mapping of an attacker, aimed at stealing information from a device that was protected by antivirus software when using a dedicated mode to protect online banking or internet payments (this is variously named by developers of these solutions).

In this edition, we used Telegram messenger to send the victim a threat in the form of a trusted application from a "familiar contact" – let's say we have sent an alpha version of a new game that our friend had just programmed. A similar attack can occur using any messenger. Some of the attack details may vary.

Scheme of procedure

author of attack -> creates a malicious file -> sends a file via messenger -> you download and run the "game" -> you start bank mode -> result of protection

What have we used?

We have used the Python programming language and ChatGPT to prepare simple malicious applications which then we used in simulated cyberattacks.

In this scenario, there was no need for the victim's device to have the Python environment because the malware had been previously compiled into a single EXE executable 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 issuer (no CA – Certification Authority).

Why we use a messenger?

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

This time we used the Telegram messenger with its own algorithm for transferring and encrypting files. The files sent via messenger are saved directly to the internal storage – Telegram does not create some kind of links to a file, as is the case in the Discord messenger. It is worth noting here that once you send an attachment via Discord, for instance, a file to a friend, a hyperlink will be created in the following domain:

https://cdn.discordapp.com/attachments/

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

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

The difference between Telegram and Discord is subtle. Telegram uses an authorial protocol for transmitting and encrypting data which bypasses the well-known and popular vector of file delivery to the system by a browser. On the other hand, the link from the Discord messenger is opened in a default browser, so that protection mechanisms of antiviruses are able to identify a threat at an early stage.

4. Participation

At the special request, any developer of endpoint security software with so-called special modules for baking & payment protection for Windows 11 can participate in the test. We usually test software on default settings or those suggested by a developer which will be publicly announced. We provide the possibility of carrying out classified tests if a developer wants to include a product in the test on the revised configuration or wants to test a new feature and get the conclusions from technical analysis.

Developers that are included in the test can access the test information under the same conditions as regular test participants. The difference is that we will not have all the necessary logs that a software developer may require because it requires consultation beforehand. In such cases, we rely our own logs. We require a developer to declare at least one day before the end of the test whether he wants to receive basic telemetry data from the test.

Opt-Out Policy:

Developers that are included in the test may opt out of the test throughout its duration with a reason but no later than 1 day before the end of the test.

If we do not receive a request to opt out of the test by that date, it is considered that a developer has not opposed and is interested in potential cooperation to improve security of the entire community. We want to make the opt-out publicly available.

Conflict of Interest Disclosure:

In a contentious situation, e.g. in the case of failing to block a malware sample, after providing the logs, a developer may refer to the results by expressing his opinion and presenting appropriate counterarguments.

Possible errors may occur either on the side of the Tester who will be obliged to fix them in the future, or on the side of a developer who should update the software.

In such disputable situations, after agreement of both parties, the Tester may remove the questionable part of samples from the test, or will not publish the results for the software, or will publish the results under an anonymous software name.

Funding:

The form of continuous participation in the test requires a predetermined fee in exchange for providing detailed telemetry data and consulting errors in order to improve the developer's software. We do not charge for participation in the test, and we do not charge a developer any fees if the software will be included in the tests once. The difference is that a developer who does not want to pay for the test will not receive an additional service in the form of providing technical information from the test. In addition, the fee for the tests is equivalent to the right to use marketing materials: logos, certificates, reports, and other materials related to the test.

It may happen that the detected bug during the processing of a malware sample by the antivirus engine will contribute to the release of an update for the protection software which is intended to minimize the risk associated with a potential error in the Developer's software. The Developer's cooperation with the Test is an investment in security and an improvement of protection software.

5. Environment

Physical Configuration:

Tests are carried out using virtual machines based on Windows 11 Pro. Each machine has allocated 8 GB of RAM, 60GB of NVMe drive, and 2 to 4 cores of the physical processor. In the Windows 11 environment, Sysmon is installed with the driver altitude set to 244999 for capturing Windows events.

Distribution of Test Data:

The collected telemetry data from the test is used to resolve contentious cases and fix errors related to security software. We usually upload all logs and malware samples used in the test, if a developer requires it. If not, we limit ourselves only to samples and logs that relate to contentious cases.

6. Schedule

Start Date Range: 01 October – 31 October 2023

We start the test on the 1st day of the month and finish on the last day. Next, we contact a developer to provide logs, discuss the results, implement changes to the default configuration and changes to our testing system, and consult the essential changes necessary to improve the functioning of the software.

We require that after receiving the results a developer provides us with feedback and necessary comments within 2 weeks from the date of sending the telemetry data. After all disputes have been resolved, we proceed to the publication of the results.

Risks and Risk Management:

A developer who keeps threat statistics, makes them publicly available, creates educational or statistical materials based on them, should (but does not have to) exclude telemetry data from our technical backend by recognizing the IP address of the server or as otherwise acceptable to both parties.

7. Control Procedures

The Test Plan may include instructions for potential Participants to provide Specific Data regarding the Product(s) to be included in the test. These elements are included in the Control Procedures section.

Connectivity Validation:

Confirmation of communication of the tested software with the developer's cloud is carried out by the Tester using publicly available malicious URLs or using a set of tools from AMTSO. A developer may indicate any other method confirming the proper communication of the software with its infrastructure.

Logging:

Developers may require specific logs or enable features to obtain more detailed telemetry data from testing. In such cases, a developer should contact the Tester to propose an additional configuration.

Updates:

Tested software is configured to download an update of signature database every hour. Once a day, an automatic update of all tested products is carried out, and during this time software can additionally update its files to a newer version.

8. Scoring Process

Software with a score of 100% blocked threats is certified.

9. Dispute Process

In case of dispute over a malware sample, a developer within 14 days of providing the basic telemetry data should respond to the submitted test information. It is worth a developer to verify a checksum of a threat in its infrastructure and look at logs from the testing application installed in the Tester's infrastructure – this is proof of the result.

The submission of more detailed telemetry data by the Tester is not mandatory. Both parties should be interested in clarifying the inaccuracies, however, the Tester may charge a fee for additional consultation and detailed logs.

10. Attestations

I understand and agree that I am submitting this Test Plan, and the following Attestations, on behalf of the entity listed below, and I represent and warrant that I have authority to bind such entity to these Attestations. All references to “I” or “me” or similar language refer to such entity. I represent and warrant that the following Attestations are true, to the best of my knowledge and belief, and each of the following commitments will be upheld to the best of my ability.

1. I will provide public notification on the AMTSO website covering my obligation for notification of a Public Test, regardless of whether a potential Participant is in actual receipt of such notification prior to the Commencement Date of a Test. (Section 1, Section 4, Section 6)

2. All products included in this Test will be analyzed fairly and equally. (Section 2, Section 3, Section 5)

3. I will disclose any anticipated or known imbalance or inequity in the Test design to all Participants in the Test. (Section 2, Section 3)

4. Although I may charge for participation in a Test, I will not charge any additional fees for a vendor to be a test subject under the Standards. (Section 4)

5. I will disclose any material conflicts of interest or other information that could materially impact the reliability of the Test. (Section 4)

6. I will disclose how the Test was funded. (Section 4)

I hereby affirm, to the best of my knowledge and belief that this Test Plan complies with the AMTSO Testing Standards, as of the date hereof.

Signature: /s/ Adrian Ścibor

Name: Adrian Ścibor

Test Lab: AVLab Cybersecurity Foundation

AMTSO Test ID: [AMTSO-LS1-TP089]