THE INDEPENDENT ANTIVIRUS TESTS

Arcabit

Test of software for online banking protection

Product name: Arcabit Internet Security
Version: 2019.02.14
Testing date: february 2019

Type of test	Default Settings	Custom Settings or/and Banking Mode ON
Clipboard Hijacking Attack. The test verifies whether it's possible for malware to capture clipboard content and send it to a C&C server.	✓ PASSED	✓ PASSED
Clipboard Swapping Attack. The test verifies whether it's possible for malware to change clipboard content copied from messenger, email, PDF invoice or website.	✓ PASSED	✓ PASSED
Keylogger Attack. The test verifies whether it's possible for malware to register keystrokes on a keyboard while logging into bank account and send them to attacker's Gmail account.	✓ PASSED	✓ PASSED
Screenshot Attack. The test verifies whether it's possible for malware to take a screenshot.	✓ PASSED	✓ PASSED
RAM Scraping Attack. The test verifies whether it's possible for malware to extract confidential information from RAM, e.g. credit card numbers, passwords, logins, or bank account numbers.	✓ PASSED	✓ PASSED
DLL Injecting Attack. The test verifies whether it's possible to inject malicious DLLs into "safe browser", "virtual environment", or web browser processes while visiting HTTP pages. Used methods: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✗ FAILED	✓ PASSED (Enabled Safe Browser)
MITM Code Injecting Attack. The test verifies whether it's possible to inject HTML and JavaScript code into websites.	✗ FAILED	✗ FAILED
MITM Password Sniffing Attack. The test verifies whether it's possible to capture confidential information from websites which are secured by SSL certificate.	✗ FAILED	✗ FAILED
Hidden Desktop Sniffing Attack. The test verifies whether it's possible for malware to establish remote connection during active session with secured login page of the bank.	✓ PASSED	✓ PASSED
HOSTS Modifying Attack. The test verifies whether it's possible for malware to manipulate the contents of Windows HOSTS file.	✗ FAILED	✓ PASSED (Enabled Safe Browser)
Detecting thirteen banking trojans in-the-wild in February 2019.	POSITIVE: 13 / 13	

Description of unique banking protection components to allow better understanding how your technology protects users when banking session is active.

A reliable Arcabit Safe Browser provides a high level of security when using Internet resources, especially during banking and payment sessions, and operations requiring sensitive data exchange. The Safe Browser works closely with other modules of Arcabit suite and constantly monitors a system security level, preventing situations when sensitive data could fall into unauthorized hands. The developer has applied protection based on the "white lists" of processes which means that running processes are checked before launching the safe browser. Some of them may be harmful and work silently, deceiving an antivirus protection. Arcabit stays ahead of the malware authors and displays processes which aren't defined as safe by the developer. The decision which of them should be closed and which not depends on the user preferences. The use of Arcabit Safe Browser is as follows: all processes that are on the list of running processes should be closed. Just in case to avoid unnecessary risk of losing money or capturing confidential credentials in the online system.

PASSED TESTS: 9 / 11

Enabling certain features or banking mode allowed to obtain a better result.

Recommendation AWARD BEST++

THE INDEPENDENT ANTIVIRUS TESTS

Test of software for online banking protection

Product name: Avast Premier
Version: 19.2
Testing date: february 2019

Type of test	Default Settings	Custom Settings or/and Banking Mode ON
Clipboard Hijacking Attack. The test verifies whether it's possible for malware to capture clipboard content and send it to a C&C server.	✓ PASSED	✓ PASSED
Clipboard Swapping Attack. The test verifies whether it's possible for malware to change clipboard content copied from messenger, email, PDF invoice or website.	✓ PASSED	✓ PASSED
Keylogger Attack. The test verifies whether it's possible for malware to register keystrokes on a keyboard while logging into bank account and send them to attacker's Gmail account.	✓ PASSED	✓ PASSED
Screenshot Attack. The test verifies whether it's possible for malware to take a screenshot.	✓ PASSED	✓ PASSED
RAM Scraping Attack. The test verifies whether it's possible for malware to extract confidential information from RAM, e.g. credit card numbers, passwords, logins, or bank account numbers.	✓ PASSED	✓ PASSED
DLL Injecting Attack. The test verifies whether it's possible to inject malicious DLLs into "safe browser", "virtual environment", or web browser processes while visiting HTTP pages. Used methods: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ PASSED	✓ PASSED
MITM Code Injecting Attack. The test verifies whether it's possible to inject HTML and JavaScript code into websites.	✗ FAILED	✗ FAILED
MITM Password Sniffing Attack. The test verifies whether it's possible to capture confidential information from websites which are secured by SSL certificate.	✗ FAILED	✗ FAILED
Hidden Desktop Sniffing Attack. The test verifies whether it's possible for malware to establish remote connection during active session with secured login page of the bank.	✓ PASSED	✓ PASSED
HOSTS Modifying Attack. The test verifies whether it's possible for malware to manipulate the contents of Windows HOSTS file.	✓ PASSED	✓ PASSED
Detecting thirteen banking trojans in-the-wild in February 2019.	POSITIVE: 13 / 13	

Description of unique banking protection components to allow better understanding how your technology protects users when banking session is active.

Avast in a banking mode prevents hackers from capturing entered information. Thereby preventing a password, credit card numbers and other data leaking. The banking mode is an additional protection attached to the Avast Secure Browser. It creates a separated desktop session when carrying out banking and other operations that require a browser to be isolated from the system. The technology developed by Avast is in fact an isolated area (a new desktop) in the operating system, which ensures that malicious software, such as keylogger and spyware, can't capture keystrokes and send personal information to an unauthorized person. In addition, the banking mode provides privacy when it comes to any payment information or confidential data. This mode can be used for online banking, shopping, cryptocurrency management, or testing unknown software, or potentially infected invoices. A browser that is opened in the separated graphical mode creates a secured area which is beyond of reach even for an antivirus. This means that malicious software can't be moved from the system to safe zone and vice versa.

PASSED TESTS: 9 / 11

Enabling certain features or banking mode had no impact on the final result.

Recommendation AWARD BEST++

THE INDEPENDENT ANTIVIRUS TESTS

Test of software for online banking protection

Product name: Avira Antivirus Pro
Version: 15.0
Testing date: february 2019

Type of test	Default Settings	Custom Settings or/and Banking Mode ON
Clipboard Hijacking Attack. The test verifies whether it's possible for malware to capture clipboard content and send it to a C&C server.	✓ PASSED	✓ PASSED
Clipboard Swapping Attack. The test verifies whether it's possible for malware to change clipboard content copied from messenger, email, PDF invoice or website.	✗ FAILED	✗ FAILED
Keylogger Attack. The test verifies whether it's possible for malware to register keystrokes on a keyboard while logging into bank account and send them to attacker's Gmail account.	✓ PASSED	✓ PASSED
Screenshot Attack. The test verifies whether it's possible for malware to take a screenshot.	✗ FAILED	✗ FAILED
RAM Scraping Attack. The test verifies whether it's possible for malware to extract confidential information from RAM, e.g. credit card numbers, passwords, logins, or bank account numbers.	✗ FAILED	✗ FAILED
DLL Injecting Attack. The test verifies whether it's possible to inject malicious DLLs into "safe browser", "virtual environment", or web browser processes while visiting HTTP pages. Used methods: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ PASSED	✓ PASSED
MITM Code Injecting Attack. The test verifies whether it's possible to inject HTML and JavaScript code into websites.	✓ PASSED	✓ PASSED
MITM Password Sniffing Attack. The test verifies whether it's possible to capture confidential information from websites which are secured by SSL certificate.	✓ PASSED	✓ PASSED
Hidden Desktop Sniffing Attack. The test verifies whether it's possible for malware to establish remote connection during active session with secured login page of the bank.	✓ PASSED	✓ PASSED
HOSTS Modifying Attack. The test verifies whether it's possible for malware to manipulate the contents of Windows HOSTS file.	✓ PASSED	✓ PASSED
Detecting thirteen banking trojans in-the-wild in February 2019.	POSITIVE: 13 / 13	

Description of unique banking protection components to allow better understanding how your technology protects users when banking session is active.

Avira Antivirus Pro security suite blocks phishing attacks in online banking, protecting from theft of confidential data from credit cards and bank credentials. It protects an operating system against banking Trojans, malicious hosts, and websites spreading malware. It blocks unauthorized and suspicious processes that perform operations in a system registry. Antivirus is able to detect and block tracking scripts, ads, and scripts mining cryptocurrencies. In order to protect an operating system, It uses technology in the cloud which provides a metadata about a phishing website. Avira Protection Cloud verifies not only URLs, but also files that are checked based on virus signature databases, a heuristic protection, and an in-depth analysis. This way, it is possible to respond faster to emerging new cybercrime Internet campaigns. This is very good method of verifying files security with a zero reputation. The Avira technology is used by external providers of antivirus technologies which proves mature and stable solutions of this developer.

PASSED TESTS: **8 / 11**

Enabling certain features or banking mode had no impact on the final result.

Recommendation AWARD GOOD+

THE INDEPENDENT ANTIVIRUS TESTS

Bitdefender

Test of software for online banking protection

Product name: Bitdefender Total Security
Version: 23.0
Testing date: february 2019

Type of test	Default Settings	Custom Settings or/and Banking Mode ON
Clipboard Hijacking Attack. The test verifies whether it's possible for malware to capture clipboard content and send it to a C&C server.	✗ FAILED	✓ PASSED (Bitdefender Safepay)
Clipboard Swapping Attack. The test verifies whether it's possible for malware to change clipboard content copied from messenger, email, PDF invoice or website.	✗ FAILED	✓ PASSED (Bitdefender Safepay)
Keylogger Attack. The test verifies whether it's possible for malware to register keystrokes on a keyboard while logging into bank account and send them to attacker's Gmail account.	✓ PASSED	✓ PASSED
Screenshot Attack. The test verifies whether it's possible for malware to take a screenshot.	✗ FAILED	✓ PASSED (Bitdefender Safepay)
RAM Scraping Attack. The test verifies whether it's possible for malware to extract confidential information from RAM, e.g. credit card numbers, passwords, logins, or bank account numbers.	✗ FAILED	✗ FAILED
DLL Injecting Attack. The test verifies whether it's possible to inject malicious DLLs into "safe browser", "virtual environment", or web browser processes while visiting HTTP pages. Used methods: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ PASSED	✓ PASSED
MITM Code Injecting Attack. The test verifies whether it's possible to inject HTML and JavaScript code into websites.	✓ PASSED	✓ PASSED
MITM Password Sniffing Attack. The test verifies whether it's possible to capture confidential information from websites which are secured by SSL certificate.	✓ PASSED	✓ PASSED
Hidden Desktop Sniffing Attack. The test verifies whether it's possible for malware to establish remote connection during active session with secured login page of the bank.	✓ PASSED	✓ PASSED
HOSTS Modifying Attack. The test verifies whether it's possible for malware to manipulate the contents of Windows HOSTS file.	✗ FAILED	✓ PASSED (Bitdefender Safepay)
Detecting thirteen banking trojans in-the-wild in February 2019.	POSITIVE: 13 / 13	

Description of unique banking protection components to allow better understanding how your technology protects users when banking session is active.

One of the most important protection modules for online sessions is a technology which makes full use of developed mechanisms in the cloud. Bitdefender Safepay is available in security suites and as standalone software. It protects against scams, phishing, viruses, and malicious software, including keyloggers and screenloggers that are designed to capture keystrokes and take screenshots. A user can switch between the Bitdefender Safepay virtual environment and his desktop. If the Safepay session is active, it will not allow external applications to modify the Bitdefender Safepay environment. This way, by switching to the secure browser, a computer will be protected against online threats, scams, untrusted, spam, and malware websites.

PASSED TESTS: **10 / 11**

Enabling certain features or banking mode allowed to obtain a better result.

Recommendation AWARD BEST++

THE INDEPENDENT ANTIVIRUS TESTS

Test of software for online banking protection

Product name: BullGuard Premium Protection
Version: 19.0
Testing date: february 2019

Type of test	Default Settings	Custom Settings or/and Banking Mode ON
Clipboard Hijacking Attack. The test verifies whether it's possible for malware to capture clipboard content and send it to a C&C server.	✓ PASSED	✓ PASSED
Clipboard Swapping Attack. The test verifies whether it's possible for malware to change clipboard content copied from messenger, email, PDF invoice or website.	✗ FAILED	✗ FAILED
Keylogger Attack. The test verifies whether it's possible for malware to register keystrokes on a keyboard while logging into bank account and send them to attacker's Gmail account.	✓ PASSED	✓ PASSED
Screenshot Attack. The test verifies whether it's possible for malware to take a screenshot.	✗ FAILED	✗ FAILED
RAM Scraping Attack. The test verifies whether it's possible for malware to extract confidential information from RAM, e.g. credit card numbers, passwords, logins, or bank account numbers.	✗ FAILED	✗ FAILED
DLL Injecting Attack. The test verifies whether it's possible to inject malicious DLLs into "safe browser", "virtual environment", or web browser processes while visiting HTTP pages. Used methods: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ PASSED	✓ PASSED
MITM Code Injecting Attack. The test verifies whether it's possible to inject HTML and JavaScript code into websites.	✓ PASSED	✓ PASSED
MITM Password Sniffing Attack. The test verifies whether it's possible to capture confidential information from websites which are secured by SSL certificate.	✓ PASSED	✓ PASSED
Hidden Desktop Sniffing Attack. The test verifies whether it's possible for malware to establish remote connection during active session with secured login page of the bank.	✓ PASSED	✓ PASSED
HOSTS Modifying Attack. The test verifies whether it's possible for malware to manipulate the contents of Windows HOSTS file.	✗ FAILED	✗ FAILED
Detecting thirteen banking trojans in-the-wild in February 2019.	POSITIVE: 13 / 13	

Description of unique banking protection components to allow better understanding how your technology protects users when banking session is active.

BullGuard combines many security modules. It has a network firewall that detects attacks, scans a home network, and blocks malicious hosts, making it well suited for protecting against man-in-the-middle attacks. When it comes to the online banking, the developer has prepared a protection against phishing and websites that spreads malicious software. The solution has a feature of protection against potentially unwanted applications (PUP) which detects and removes software that modifies Internet browser settings, such as changing a home page. In contrast, a resource monitoring technology tracks user activity in the system and checks what kind of actions are performed by each application. A triple layer of intelligent protection was applied here – first, it recognized website reputation and downloaded application. Then, it scans a code in order to discover anomalies related to malicious software. Finally, it blocks, quarantines, and neutralizes any detected malware.

PASSED TESTS: 7 / 11

Enabling certain features or banking mode had no impact on the final result.

Recommendation AWARD GOOD+

THE INDEPENDENT ANTIVIRUS TESTS

ZoneAlarm By Check Point

Test of software for online banking protection

Product name: Check Point ZoneAlarm Extreme Security
Version: 15.4
Testing date: february 2019

Type of test	Default Settings	Custom Settings or/and Banking Mode ON
Clipboard Hijacking Attack. The test verifies whether it's possible for malware to capture clipboard content and send it to a C&C server.	✓ PASSED	✓ PASSED
Clipboard Swapping Attack. The test verifies whether it's possible for malware to change clipboard content copied from messenger, email, PDF invoice or website.	✓ PASSED	✓ PASSED
Keylogger Attack. The test verifies whether it's possible for malware to register keystrokes on a keyboard while logging into bank account and send them to attacker's Gmail account.	✗ FAILED	✓ PASSED (Enabled Anti-Keylogger)
Screenshot Attack. The test verifies whether it's possible for malware to take a screenshot.	✓ PASSED	✓ PASSED
RAM Scraping Attack. The test verifies whether it's possible for malware to extract confidential information from RAM, e.g. credit card numbers, passwords, logins, or bank account numbers.	✓ PASSED	✓ PASSED
DLL Injecting Attack. The test verifies whether it's possible to inject malicious DLLs into "safe browser", "virtual environment", or web browser processes while visiting HTTP pages. Used methods: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ PASSED	✓ PASSED
MITM Code Injecting Attack. The test verifies whether it's possible to inject HTML and JavaScript code into websites.	✗ FAILED	✓ PASSED (Enabled ARP protection)
MITM Password Sniffing Attack. The test verifies whether it's possible to capture confidential information from websites which are secured by SSL certificate.	✗ FAILED	✓ PASSED (Enabled ARP protection)
Hidden Desktop Sniffing Attack. The test verifies whether it's possible for malware to establish remote connection during active session with secured login page of the bank.	✓ PASSED	✓ PASSED
HOSTS Modifying Attack. The test verifies whether it's possible for malware to manipulate the contents of Windows HOSTS file.	✓ PASSED	✓ PASSED
Detecting thirteen banking trojans in-the-wild in February 2019.	POSITIVE: 13 / 13	

Description of unique banking protection components to allow better understanding how your technology protects users when banking session is active.

ZoneAlarm Extreme Security is a response from Check Point company that specializes in providing network security to evolving threats and attacks. A Threat Emulation technology is available in this product. Check Point ZoneAlarm Extreme Security benefits from Check Point employees experience who provide services for large business. Malware authors can create samples that can easily bypass security of traditional signature products. A threat detection based on virus definitions is an old technique for detecting known attacks. Currently, it serves better as support than being a protection core. In contrast, the threats emulation protects against new encryption malware. This is technology used by Check Point Zone Alarm Extreme Security. The product is characterized by two more things. A unique firewall that protects, among others, against modifying HOSTS files. It protects against Internet attacks, and also allows a configuration of restrictions for directions of application access to the network. The second unique thing is a protection in the browser thanks to a threat database from the ThreatCloud system. It is a huge organized network for fighting with a cybercrime which provides data about threats and attack trends based on a global network of threat sensors.

PASSED TESTS: 11 / 11

Enabling certain features or banking mode allowed to obtain a better result.

Recommendation AWARD BEST+++

THE INDEPENDENT ANTIVIRUS TESTS

COMODO
Creating Trust Online®

Test of software for online banking protection

Product name: Comodo Internet Security
Version: 11.0
Testing date: february 2019

Type of test	Default Settings	Custom Settings or/and Banking Mode ON
Clipboard Hijacking Attack. The test verifies whether it's possible for malware to capture clipboard content and send it to a C&C server.	✓ PASSED	✓ PASSED
Clipboard Swapping Attack. The test verifies whether it's possible for malware to change clipboard content copied from messenger, email, PDF invoice or website.	✓ PASSED	✓ PASSED
Keylogger Attack. The test verifies whether it's possible for malware to register keystrokes on a keyboard while logging into bank account and send them to attacker's Gmail account.	✓ PASSED	✓ PASSED
Screenshot Attack. The test verifies whether it's possible for malware to take a screenshot.	✓ PASSED	✓ PASSED
RAM Scraping Attack. The test verifies whether it's possible for malware to extract confidential information from RAM, e.g. credit card numbers, passwords, logins, or bank account numbers.	✓ PASSED	✓ PASSED
DLL Injecting Attack. The test verifies whether it's possible to inject malicious DLLs into "safe browser", "virtual environment", or web browser processes while visiting HTTP pages. Used methods: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ PASSED	✓ PASSED
MITM Code Injecting Attack. The test verifies whether it's possible to inject HTML and JavaScript code into websites.	✗ FAILED	✓ PASSED (Enabled anti-ARP spoofing)
MITM Password Sniffing Attack. The test verifies whether it's possible to capture confidential information from websites which are secured by SSL certificate.	✗ FAILED	✓ PASSED (Enabled anti-ARP spoofing)
Hidden Desktop Sniffing Attack. The test verifies whether it's possible for malware to establish remote connection during active session with secured login page of the bank.	✓ PASSED	✓ PASSED
HOSTS Modifying Attack. The test verifies whether it's possible for malware to manipulate the contents of Windows HOSTS file.	✓ PASSED	✓ PASSED
Detecting thirteen banking trojans in-the-wild in February 2019.	POSITIVE: 13 / 13	

PASSED TESTS: 11 / 11

Enabling certain features or banking mode allowed to obtain a better result.

Description of unique banking protection components to allow better understanding how your technology protects users when banking session is active.

Comodo Internet Security has a secure shopping module. This functionality allows to enable a virtual environment, and without fear for the security, run, for example, suspicious attachments and check their threat level. The Secure Shopping contains protection against keyloggers, trojans, worms, screenloggers, and also isolates processes preventing a malicious code injection into a browser in the virtual environment. It's important to emphasize (although it's archival information) that a few years ago the CIA tested the majority of well-known antivirus applications, but only one of them particularly got under hackers skin who worked for the agency. The Comodo suite has gained a term of "hard to hack" antivirus. The most significant modules include a specialized firewall for scanning Internet traffic which protects against ARP spoofing attacks. HIPS monitors the system and application activity to ensure that potentially dangerous file performs certain actions that can be reserved for malicious software. The Viruscope module, active by default, is a behavioral component for analyzing and monitoring processes for potential malicious modifications. Automatic sandbox implements protection against 0-day threats that can't be detected by antivirus engine through signatures or scanning files in the cloud. Comodo Internet Security is a powerful tool to protect the system against 0-day malware and hacker attacks.

Recommendation AV LAB AWARD BEST+++

THE INDEPENDENT ANTIVIRUS TESTS

Dr.WEB® Anti-virus

Test of software for online banking protection

Product name: Dr.Web Space Security
Version: 12.0
Testing date: february 2019

Type of test	Default Settings	Custom Settings or/and Banking Mode ON
Clipboard Hijacking Attack. The test verifies whether it's possible for malware to capture clipboard content and send it to a C&C server.	✓ PASSED	✓ PASSED
Clipboard Swapping Attack. The test verifies whether it's possible for malware to change clipboard content copied from messenger, email, PDF invoice or website.	✗ FAILED	✗ FAILED
Keylogger Attack. The test verifies whether it's possible for malware to register keystrokes on a keyboard while logging into bank account and send them to attacker's Gmail account.	✓ PASSED	✓ PASSED
Screenshot Attack. The test verifies whether it's possible for malware to take a screenshot.	✗ FAILED	✗ FAILED
RAM Scraping Attack. The test verifies whether it's possible for malware to extract confidential information from RAM, e.g. credit card numbers, passwords, logins, or bank account numbers.	✗ FAILED	✗ FAILED
DLL Injecting Attack. The test verifies whether it's possible to inject malicious DLLs into "safe browser", "virtual environment", or web browser processes while visiting HTTP pages. Used methods: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ PASSED	✓ PASSED
MITM Code Injecting Attack. The test verifies whether it's possible to inject HTML and JavaScript code into websites.	✓ PASSED	✓ PASSED
MITM Password Sniffing Attack. The test verifies whether it's possible to capture confidential information from websites which are secured by SSL certificate.	✓ PASSED	✓ PASSED
Hidden Desktop Sniffing Attack. The test verifies whether it's possible for malware to establish remote connection during active session with secured login page of the bank.	✓ PASSED	✓ PASSED
HOSTS Modifying Attack. The test verifies whether it's possible for malware to manipulate the contents of Windows HOSTS file.	✓ PASSED	✓ PASSED
Detecting thirteen banking trojans in-the-wild in February 2019.	POSITIVE: 13 / 13	

PASSED TESTS: 8 / 11

Enabling certain features or banking mode had no impact on the final result.

Description of unique banking protection components to allow better understanding how your technology protects users when banking session is active.

Dr.Web Space Security solution is equipped with an extended protection scope of processes, services, driver, registry, network connections, and WMI protocol which is used by many types of malware. The protection task is to monitor and control all threats that try to do anything suspicious using trusted system processes. Heuristic algorithms detect attacks of malicious scripts and binary files. In the browser can be found protection which is carried through the cloud. It's a module that connects a user computer with information about threats in the cloud which scans installed plugins configurations files and analyzes them for security. The preventive protection in the Dr.Web suite is based on analyzing the behavior of running applications and system processes. The components protect against the latest malicious software which has been designed to hide from antivirus.

Recommendation AWARD GOOD+

THE INDEPENDENT ANTIVIRUS TESTS

EMSISOFT

Test of software for online banking protection

Product name: Emsisoft Anti-Malware Home
Version: 2019.1.1
Testing date: february 2019

Type of test	Default Settings	Custom Settings or/and Banking Mode ON
Clipboard Hijacking Attack. The test verifies whether it's possible for malware to capture clipboard content and send it to a C&C server.	✓ PASSED	✓ PASSED
Clipboard Swapping Attack. The test verifies whether it's possible for malware to change clipboard content copied from messenger, email, PDF invoice or website.	✓ PASSED	✓ PASSED
Keylogger Attack. The test verifies whether it's possible for malware to register keystrokes on a keyboard while logging into bank account and send them to attacker's Gmail account.	✓ PASSED	✓ PASSED
Screenshot Attack. The test verifies whether it's possible for malware to take a screenshot.	✓ PASSED	✓ PASSED
RAM Scraping Attack. The test verifies whether it's possible for malware to extract confidential information from RAM, e.g. credit card numbers, passwords, logins, or bank account numbers.	✓ PASSED	✓ PASSED
DLL Injecting Attack. The test verifies whether it's possible to inject malicious DLLs into "safe browser", "virtual environment", or web browser processes while visiting HTTP pages. Used methods: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ PASSED	✓ PASSED
MITM Code Injecting Attack. The test verifies whether it's possible to inject HTML and JavaScript code into websites.	✗ FAILED	✗ FAILED
MITM Password Sniffing Attack. The test verifies whether it's possible to capture confidential information from websites which are secured by SSL certificate.	✗ FAILED	✗ FAILED
Hidden Desktop Sniffing Attack. The test verifies whether it's possible for malware to establish remote connection during active session with secured login page of the bank.	✓ PASSED	✓ PASSED
HOSTS Modifying Attack. The test verifies whether it's possible for malware to manipulate the contents of Windows HOSTS file.	✓ PASSED	✓ PASSED
Detecting thirteen banking trojans in-the-wild in February 2019.	POSITIVE: 13 / 13	

Description of unique banking protection components to allow better understanding how your technology protects users when banking session is active.

A characteristic feature of Emsisoft Anti-Malware Home is behavior blocker that monitors all active applications in real time for dangerous indicators. It allows detecting new trojans, ransomware, spyware, backdoors, and other dangerous 0-day threats. The technology is based on a proactive method, so it doesn't need updated signatures. For years the developer has been developing its own technologies with the participation of the community and he is good at it. Recently, the developer has released a new plugin for browsers, Emsisoft Browser Security that puts privacy first – it doesn't log any details about browsing activity. The File Guard technology is an important element of protection which checks all downloaded or run files, crosschecking them with a multimillion signature database. It scans file without an excessive use of system resources. The default settings of Emsisoft provide a balance between performance and security and are sufficient for most users. For 16th year in a row Emsisoft confirms that only the best can stay on the market, adjusting to rapidly changing trends.

PASSED TESTS: 9 / 11

Enabling certain features or banking mode had no impact on the final result.

Recommendation AWARD BEST++

THE INDEPENDENT ANTIVIRUS TESTS

Test of software for online banking protection

Product name: Eset Internet Security
Version: 12.0.31.0
Testing date: february 2019

Type of test	Default Settings	Custom Settings or/and Banking Mode ON
Clipboard Hijacking Attack. The test verifies whether it's possible for malware to capture clipboard content and send it to a C&C server.	✗ FAILED	✓ PASSED (Firewall Interactive Mode)
Clipboard Swapping Attack. The test verifies whether it's possible for malware to change clipboard content copied from messenger, email, PDF invoice or website.	✗ FAILED	✗ FAILED
Keylogger Attack. The test verifies whether it's possible for malware to register keystrokes on a keyboard while logging into bank account and send them to attacker's Gmail account.	✗ FAILED	✓ PASSED (Enabled Banking & Payment)
Screenshot Attack. The test verifies whether it's possible for malware to take a screenshot.	✗ FAILED	✗ FAILED
RAM Scraping Attack. The test verifies whether it's possible for malware to extract confidential information from RAM, e.g. credit card numbers, passwords, logins, or bank account numbers.	✗ FAILED	✓ PASSED (Enabled Banking & Payment)
DLL Injecting Attack. The test verifies whether it's possible to inject malicious DLLs into "safe browser", "virtual environment", or web browser processes while visiting HTTP pages. Used methods: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ PASSED	✓ PASSED
MITM Code Injecting Attack. The test verifies whether it's possible to inject HTML and JavaScript code into websites.	✓ PASSED	✓ PASSED
MITM Password Sniffing Attack. The test verifies whether it's possible to capture confidential information from websites which are secured by SSL certificate.	✓ PASSED	✓ PASSED
Hidden Desktop Sniffing Attack. The test verifies whether it's possible for malware to establish remote connection during active session with secured login page of the bank.	✓ PASSED	✓ PASSED
HOSTS Modifying Attack. The test verifies whether it's possible for malware to manipulate the contents of Windows HOSTS file.	✗ FAILED	✓ PASSED (HIPS Inteligence Mode)
Detecting thirteen banking trojans in-the-wild in February 2019.	POSITIVE: 13 / 13	

Description of unique banking protection components to allow better understanding how your technology protects users when banking session is active.

ESET maintains a high level of protection through Live Grid cloud and very good detection of potentially unwanted programs. Its features block threats that try to activate and attack a user right after turning on a computer before booting the operating system – this is so-called UEFI scanner. A well-configured firewall module which detects malicious communication used by botnet networks makes the most impression. Not without significance it blocks "ARP spoofing" attacks that allow hacker to capture data sent within a local area network, as well as "DNS cache poisoning" network attacks in which an attacker sends false information to a DNS server that associates a domain name with an IP. The two-way firewall containing Intrusive Detection System guards data and detects attacks poisoning ARP tables and modifying DNS entries, fake PING queries, attacks that exploit SMB, RPC, RDP protocols and scan ports. Online banking protection is an useful feature that secures WinAPI of the system against key interception, so the user is protected against manipulation of data entry at the browser level when typing bank account numbers or logging into online bank account.

PASSED TESTS: **9 / 11**

Enabling certain features or banking mode allowed to obtain a better result.

Recommendation AWARD BEST++

THE INDEPENDENT ANTIVIRUS TESTS

Test of software for online banking protection

Product name: F-Secure SAFE
Version: 17.5
Testing date: february 2019

Type of test	Default Settings	Custom Settings or/and Banking Mode ON
Clipboard Hijacking Attack. The test verifies whether it's possible for malware to capture clipboard content and send it to a C&C server.	✓ PASSED	✓ PASSED
Clipboard Swapping Attack. The test verifies whether it's possible for malware to change clipboard content copied from messenger, email, PDF invoice or website.	✓ PASSED	✓ PASSED
Keylogger Attack. The test verifies whether it's possible for malware to register keystrokes on a keyboard while logging into bank account and send them to attacker's Gmail account.	✓ PASSED	✓ PASSED
Screenshot Attack. The test verifies whether it's possible for malware to take a screenshot.	✓ PASSED	✓ PASSED
RAM Scraping Attack. The test verifies whether it's possible for malware to extract confidential information from RAM, e.g. credit card numbers, passwords, logins, or bank account numbers.	✓ PASSED	✓ PASSED
DLL Injecting Attack. The test verifies whether it's possible to inject malicious DLLs into "safe browser", "virtual environment", or web browser processes while visiting HTTP pages. Used methods: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ PASSED	✓ PASSED
MITM Code Injecting Attack. The test verifies whether it's possible to inject HTML and JavaScript code into websites.	✗ FAILED	✗ FAILED
MITM Password Sniffing Attack. The test verifies whether it's possible to capture confidential information from websites which are secured by SSL certificate.	✗ FAILED	✗ FAILED
Hidden Desktop Sniffing Attack. The test verifies whether it's possible for malware to establish remote connection during active session with secured login page of the bank.	✓ PASSED	✓ PASSED
HOSTS Modifying Attack. The test verifies whether it's possible for malware to manipulate the contents of Windows HOSTS file.	✗ FAILED	✗ FAILED
Detecting thirteen banking trojans in-the-wild in February 2019.	POSITIVE: 13 / 13	

PASSED TESTS: 8 / 11

Enabling certain features or banking mode had no impact on the final result.

Description of unique banking protection components to allow better understanding how your technology protects users when banking session is active.

The strength of the F-Secure suite is the DeepGuard technology embedded in the antivirus engine. This is a type of behavioral security that monitors files for suspicious behavior. If a risk is detected, a dangerous applications is automatically blocked. The DeepGuard verifies application security based on information from a trusted external service. When the application security can't be verified, the DeepGuard begins to monitor the functioning of the process. DeepGuard is able to detect new trojans, worms, software vulnerabilities, and other malicious applications that try to make changes to the computer, and also prevents the suspicious applications access to the Internet. Potential harmful changes in the system that are detected by DeepGuard technology include: changes in the system settings (Windows system registry), attempts to disable important system applications (for example security software), and attempts to edit important system files. The technology not only protects against ransomware, but also blocks applications that could replace, rename, or delete important files. In the banking mode, it stops all Internet connections when protection is active. It runs automatically, but a user has control over it (this prevents the malware from communicating with external hosts).

Recommendation AWARD GOOD+

THE INDEPENDENT ANTIVIRUS TESTS

Test of software for online banking protection

Product name: G Data Total Protection
Version: 25.5.1.21
Testing date: february 2019

Type of test	Default Settings	Custom Settings or/and Banking Mode ON
Clipboard Hijacking Attack. The test verifies whether it's possible for malware to capture clipboard content and send it to a C&C server.	✘ FAILED	✓ PASSED (Firewall Interactive Mode)
Clipboard Swapping Attack. The test verifies whether it's possible for malware to change clipboard content copied from messenger, email, PDF invoice or website.	✓ PASSED	✓ PASSED
Keylogger Attack. The test verifies whether it's possible for malware to register keystrokes on a keyboard while logging into bank account and send them to attacker's Gmail account.	✓ PASSED	✓ PASSED
Screenshot Attack. The test verifies whether it's possible for malware to take a screenshot.	✓ PASSED	✓ PASSED
RAM Scraping Attack. The test verifies whether it's possible for malware to extract confidential information from RAM, e.g. credit card numbers, passwords, logins, or bank account numbers.	✘ FAILED	✘ FAILED
DLL Injecting Attack. The test verifies whether it's possible to inject malicious DLLs into "safe browser", "virtual environment", or web browser processes while visiting HTTP pages. Used methods: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ PASSED	✓ PASSED
MITM Code Injecting Attack. The test verifies whether it's possible to inject HTML and JavaScript code into websites.	✘ FAILED	✘ FAILED
MITM Password Sniffing Attack. The test verifies whether it's possible to capture confidential information from websites which are secured by SSL certificate.	✘ FAILED	✘ FAILED
Hidden Desktop Sniffing Attack. The test verifies whether it's possible for malware to establish remote connection during active session with secured login page of the bank.	✓ PASSED	✓ PASSED
HOSTS Modifying Attack. The test verifies whether it's possible for malware to manipulate the contents of Windows HOSTS file.	✘ FAILED	✘ FAILED
Detecting thirteen banking trojans in-the-wild in February 2019.	POSITIVE: 13 / 13	

PASSED TESTS: 7 / 11

Enabling certain features or banking mode allowed to obtain a better result.

Description of unique banking protection components to allow better understanding how your technology protects users when banking session is active.

G Data Total Protection is a very well developed security suite that protects against online attacks and threats. At the security center, a user will find information summarizing data from other modules. For security purposes the most important components are a firewall and antivirus protection, covering most protocols, including the new DeepRay technology. Based on many years of experience , experts have developed new methods of detecting malicious code. The software can determine which of a combination of factors are potentially harmful, for example, presence of jump instructions in PE headers, the ratio between executed code and file size, specific file compression methods or number of imported system functions. In this aspect, the complexity of protection consist in covering all protocols through which user communicated with the Internet. DeepRay uses machine learning to detect malicious code, regardless of the manual analyses carried out by specialists in the field. G Data employees have developed a self-learning system based on machine learning that detects well-disguised malicious software. So DeepRay is a technology in which the supervised learning method is included which means that antivirus software "was taught" to analyze malicious code and calculate risk taking into account over 100 factors. On safety features, G Data provides high-quality software that will satisfy even computer geeks.

Recommendation AWARD GOOD+

Test of software for online banking protection

Product name: Kaspersky Internet Security
Version: 19.0.0.1088
Testing date: february 2019

Type of test	Default Settings	Custom Settings or/and Banking Mode ON
Clipboard Hijacking Attack. The test verifies whether it's possible for malware to capture clipboard content and send it to a C&C server.	✗ FAILED	✓ PASSED (Enabled Safe Money)
Clipboard Swapping Attack. The test verifies whether it's possible for malware to change clipboard content copied from messenger, email, PDF invoice or website.	✗ FAILED	✓ PASSED (Enabled Safe Money)
Keylogger Attack. The test verifies whether it's possible for malware to register keystrokes on a keyboard while logging into bank account and send them to attacker's Gmail account.	✗ FAILED	✓ PASSED (Enabled Safe Money)
Screenshot Attack. The test verifies whether it's possible for malware to take a screenshot.	✗ FAILED	✓ PASSED (Enabled Safe Money)
RAM Scraping Attack. The test verifies whether it's possible for malware to extract confidential information from RAM, e.g. credit card numbers, passwords, logins, or bank account numbers.	✗ FAILED	✓ PASSED (Enabled Safe Money)
DLL Injecting Attack. The test verifies whether it's possible to inject malicious DLLs into "safe browser", "virtual environment", or web browser processes while visiting HTTP pages. Used methods: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ PASSED	✓ PASSED
MITM Code Injecting Attack. The test verifies whether it's possible to inject HTML and JavaScript code into websites.	✓ PASSED	✓ PASSED
MITM Password Sniffing Attack. The test verifies whether it's possible to capture confidential information from websites which are secured by SSL certificate.	✓ PASSED	✓ PASSED
Hidden Desktop Sniffing Attack. The test verifies whether it's possible for malware to establish remote connection during active session with secured login page of the bank.	✓ PASSED	✓ PASSED
HOSTS Modifying Attack. The test verifies whether it's possible for malware to manipulate the contents of Windows HOSTS file.	✓ PASSED	✓ PASSED
Detecting thirteen banking trojans in-the-wild in February 2019.	POSITIVE: 13 / 13	

Description of unique banking protection components to allow better understanding how your technology protects users when banking session is active.

Protection of opened and modified files, communications protection that scans messages for malicious links, and email protection are distinguishing features of this product. Website scanning for phishing and malicious resources, including dangerous scripts is another value that draw our attention. The Safe Money is a very important module. It suggests opening a secure browser resistant to injecting malicious DDLs, or even reading confidential information from RAM inserted into a browser. An attacker or malicious software can't obtain a login and a password or replace the content (amount, bank account, etc.) of banking transactions by displaying on the screen of the user fake windows imitating a real website. He is also unable to take screenshots, register keystrokes, and mouse clicks. Any attempts to take screenshots are also blocked, including screenshots of the entire desktop using API functions such as GDI, DirectX, or OpenGL. Kaspersky is extremely robust software. Not only, it doesn't cause problems with computers, but it protects devices at the highest level. It has a firewall that filters network activity, a webcam protection that prevents tracking, and network attacks blocking module.

PASSED TESTS: **11 / 11**

Enabling certain features or banking mode allowed to obtain a better result.

Recommendation AWARD BEST+++

THE INDEPENDENT ANTIVIRUS TESTS

mks_vir

Test of software for online banking protection

Product name: mks_vir Internet Security
Version: 2019.02.14
Testing date: february 2019

Type of test	Default Settings	Custom Settings or/and Banking Mode ON
Clipboard Hijacking Attack. The test verifies whether it's possible for malware to capture clipboard content and send it to a C&C server.	✓ PASSED	✓ PASSED
Clipboard Swapping Attack. The test verifies whether it's possible for malware to change clipboard content copied from messenger, email, PDF invoice or website.	✓ PASSED	✓ PASSED
Keylogger Attack. The test verifies whether it's possible for malware to register keystrokes on a keyboard while logging into bank account and send them to attacker's Gmail account.	✓ PASSED	✓ PASSED
Screenshot Attack. The test verifies whether it's possible for malware to take a screenshot.	✓ PASSED	✓ PASSED
RAM Scraping Attack. The test verifies whether it's possible for malware to extract confidential information from RAM, e.g. credit card numbers, passwords, logins, or bank account numbers.	✓ PASSED	✓ PASSED
DLL Injecting Attack. The test verifies whether it's possible to inject malicious DLLs into "safe browser", "virtual environment", or web browser processes while visiting HTTP pages. Used methods: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✗ FAILED	✓ PASSED (Enabled Safe Browser)
MITM Code Injecting Attack. The test verifies whether it's possible to inject HTML and JavaScript code into websites.	✗ FAILED	✗ FAILED
MITM Password Sniffing Attack. The test verifies whether it's possible to capture confidential information from websites which are secured by SSL certificate.	✗ FAILED	✗ FAILED
Hidden Desktop Sniffing Attack. The test verifies whether it's possible for malware to establish remote connection during active session with secured login page of the bank.	✓ PASSED	✓ PASSED
HOSTS Modifying Attack. The test verifies whether it's possible for malware to manipulate the contents of Windows HOSTS file.	✗ FAILED	✓ PASSED (Enabled Safe Browser)
Detecting thirteen banking trojans in-the-wild in February 2019.	POSITIVE: 13 / 13	

Description of unique banking protection components to allow better understanding how your technology protects users when banking session is active.

A reliable mks_vir Safe Browser provides a high level of security when using Internet resources, especially during banking and payment sessions, and operations requiring sensitive data exchange. The Safe Browser works closely with other modules of mks_vir suite and constantly monitors a system security level, preventing situations when sensitive data could fall into unauthorized hands. The developer has applied protection based on the "white lists" of processes which means that running processes are checked before launching the safe browser. Some of them may be harmful and work silently, deceiving an antivirus protection. Mks_vir stays ahead of the malware authors and displays processes which aren't defined as safe by the developer. The decision which of them should be closed and which not depends on the user preferences. The use of mks_vir Safe Browser is as follows: all processes that are on the list of running processes should be closed. Just in case to avoid unnecessary risk of losing money or capturing confidential credentials in the online system.

PASSED TESTS: 9 / 11

Enabling certain features or banking mode allowed to obtain a better result.

Recommendation

AV LAB AWARD BEST++

THE INDEPENDENT ANTIVIRUS TESTS

Test of software for online banking protection

Product name: Norton Security
Version: 22.5
Testing date: february 2019

Type of test	Default Settings	Custom Settings or/and Banking Mode ON
Clipboard Hijacking Attack. The test verifies whether it's possible for malware to capture clipboard content and send it to a C&C server.	✓ PASSED	✓ PASSED
Clipboard Swapping Attack. The test verifies whether it's possible for malware to change clipboard content copied from messenger, email, PDF invoice or website.	✓ PASSED	✓ PASSED
Keylogger Attack. The test verifies whether it's possible for malware to register keystrokes on a keyboard while logging into bank account and send them to attacker's Gmail account.	✓ PASSED	✓ PASSED
Screenshot Attack. The test verifies whether it's possible for malware to take a screenshot.	✓ PASSED	✓ PASSED
RAM Scraping Attack. The test verifies whether it's possible for malware to extract confidential information from RAM, e.g. credit card numbers, passwords, logins, or bank account numbers.	✓ PASSED	✓ PASSED
DLL Injecting Attack. The test verifies whether it's possible to inject malicious DLLs into "safe browser", "virtual environment", or web browser processes while visiting HTTP pages. Used methods: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ PASSED	✓ PASSED
MITM Code Injecting Attack. The test verifies whether it's possible to inject HTML and JavaScript code into websites.	✓ PASSED	✓ PASSED
MITM Password Sniffing Attack. The test verifies whether it's possible to capture confidential information from websites which are secured by SSL certificate.	✓ PASSED	✓ PASSED
Hidden Desktop Sniffing Attack. The test verifies whether it's possible for malware to establish remote connection during active session with secured login page of the bank.	✓ PASSED	✓ PASSED
HOSTS Modifying Attack. The test verifies whether it's possible for malware to manipulate the contents of Windows HOSTS file.	✓ PASSED	✓ PASSED
Detecting thirteen banking trojans in-the-wild in February 2019.	POSITIVE: 13 / 13	

PASSED TESTS: 11 / 11

Enabling certain features or banking mode had no impact on the final result.

Description of unique banking protection components to allow better understanding how your technology protects users when banking session is active.

Norton Security is a very complex suite that uses a heuristic and proactive detection, providing an effective protection by detecting a suspicious application activity and also when downloading unknown files. The solution works well with a protection against unknown threats which is based on the files reputation. Norton guarantees a security at a higher level by detecting a destructive code and a protection against unknown threats for which no signatures have been released. A firewall is a very useful module. It blocks hacker attacks and unauthorized traffic by monitoring communications between networked computers. It informs about connections from other devices as well as connections made by applications located in the system. An additional advantage is the fact that it closes inactive ports, protecting against scanning them. The firewall monitors a network traffic both incoming and outgoing, and compares information communicated with the signatures database of the attacks. These signatures contain information allowing to detect an attack that exploits software or operating system vulnerabilities. When such data are detected by the module, the connection with a host is interrupted and a received packet is rejected.

Recommendation AWARD BEST+++

THE INDEPENDENT ANTIVIRUS TESTS

Test of software for online banking protection

Product name: Panda Dome Advanced
Version: 18.07.00
Testing date: february 2019

Type of test	Default Settings	Custom Settings or/and Banking Mode ON
Clipboard Hijacking Attack. The test verifies whether it's possible for malware to capture clipboard content and send it to a C&C server.	✗ FAILED	✓ PASSED (Enabled Application Control)
Clipboard Swapping Attack. The test verifies whether it's possible for malware to change clipboard content copied from messenger, email, PDF invoice or website.	✗ FAILED	✓ PASSED (Enabled Application Control)
Keylogger Attack. The test verifies whether it's possible for malware to register keystrokes on a keyboard while logging into bank account and send them to attacker's Gmail account.	✗ FAILED	✓ PASSED (Enabled Application Control)
Screenshot Attack. The test verifies whether it's possible for malware to take a screenshot.	✗ FAILED	✓ PASSED (Enabled Application Control)
RAM Scraping Attack. The test verifies whether it's possible for malware to extract confidential information from RAM, e.g. credit card numbers, passwords, logins, or bank account numbers.	✗ FAILED	✓ PASSED (Enabled Application Control)
DLL Injecting Attack. The test verifies whether it's possible to inject malicious DLLs into "safe browser", "virtual environment", or web browser processes while visiting HTTP pages. Used methods: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ PASSED	✓ PASSED
MITM Code Injecting Attack. The test verifies whether it's possible to inject HTML and JavaScript code into websites.	✓ PASSED	✓ PASSED
MITM Password Sniffing Attack. The test verifies whether it's possible to capture confidential information from websites which are secured by SSL certificate.	✓ PASSED	✓ PASSED
Hidden Desktop Sniffing Attack. The test verifies whether it's possible for malware to establish remote connection during active session with secured login page of the bank.	✓ PASSED	✓ PASSED
HOSTS Modifying Attack. The test verifies whether it's possible for malware to manipulate the contents of Windows HOSTS file.	✗ FAILED	✓ PASSED (Enabled Application Control)
Detecting thirteen banking trojans in-the-wild in February 2019.	POSITIVE: 13 / 13	
	PASSED TESTS: 11 / 11	
	Enabling certain features or banking mode allowed to obtain a better result.	

Description of unique banking protection components to allow better understanding how your technology protects users when banking session is active.

The Panda Dome software has a very important module that blocks threats on the basis of behavior and heuristic analysis, as well as the detection of potentially unwanted applications. On the plus side we include URL addresses monitoring to which running process gets access. This is very important in the context of fileless infection and all other malicious files that use a command line. As a detection of unknown threats is carried out in the cloud, the Panda Dome antivirus can delay launching applications for 30 seconds which security status can't be obtained immediately. A very important protection component is a firewall that protects a device against the majority of known attacks. However, in the context of new banking trojans, an application control is the most important module (disabled by default) which creates a secure and closed environment. Thus, it's an ideal additional layer of protection against 0-day threats. The application control allows not only to configure those programs which can be run on a computer, but also set up actions to be performed, if an unknown application attempts to launch. In this way, the component can directly block an application execution or ask for confirmation before running an unknown program.

Recommendation AWARD BEST+++

THE INDEPENDENT ANTIVIRUS TESTS

Quick Heal
Security Simplified

Test of software for online banking protection

Product name: Quick Heal Total Security
Version: 18.00
Testing date: february 2019

Type of test	Default Settings	Custom Settings or/and Banking Mode ON
Clipboard Hijacking Attack. The test verifies whether it's possible for malware to capture clipboard content and send it to a C&C server.	✗ FAILED	✓ PASSED
Clipboard Swapping Attack. The test verifies whether it's possible for malware to change clipboard content copied from messenger, email, PDF invoice or website.	✗ FAILED	✓ PASSED
Keylogger Attack. The test verifies whether it's possible for malware to register keystrokes on a keyboard while logging into bank account and send them to attacker's Gmail account.	✗ FAILED	✓ PASSED
Screenshot Attack. The test verifies whether it's possible for malware to take a screenshot.	✗ FAILED	✓ PASSED
RAM Scraping Attack. The test verifies whether it's possible for malware to extract confidential information from RAM, e.g. credit card numbers, passwords, logins, or bank account numbers.	✗ FAILED	✗ FAILED
DLL Injecting Attack. The test verifies whether it's possible to inject malicious DLLs into "safe browser", "virtual environment", or web browser processes while visiting HTTP pages. Used methods: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ PASSED	✓ PASSED
MITM Code Injecting Attack. The test verifies whether it's possible to inject HTML and JavaScript code into websites.	✗ FAILED	✓ PASSED
MITM Password Sniffing Attack. The test verifies whether it's possible to capture confidential information from websites which are secured by SSL certificate.	✗ FAILED	✓ PASSED
Hidden Desktop Sniffing Attack. The test verifies whether it's possible for malware to establish remote connection during active session with secured login page of the bank.	✓ PASSED	✓ PASSED
HOSTS Modifying Attack. The test verifies whether it's possible for malware to manipulate the contents of Windows HOSTS file.	✗ FAILED	✗ FAILED
Detecting thirteen banking trojans in-the-wild in February 2019.	POSITIVE: 13 / 13	

Description of unique banking protection components to allow better understanding how your technology protects users when banking session is active.

What is very important, secure banking in Quick Heal isn't limited to the virtual desktop module. Among others, a protection against replacing DNS addresses can be found here. By taking a control of DNS addresses, an unauthorized person can decrypt SSL communication. Using Safe Banking in Quick Heal prevents such attacks. An important element of protection is embedded IPS/IDS module. In advanced attacks where more sophisticated methods than social engineering are used (these are mainly attacks on unprotected and outdated protocols, for example, SMB), IPS/IDS plays a very important role in security. A two-way firewall containing an intruder detection system can detect attacks: poisoning ARP tables, fake PING queries, modifying DNS entries, SMB, RPC, RDP protocols, and port scanning. It protects a home network against malicious software and stops malware before it installs on the system. It protects against downloading a dangerous file via CMD.exe or PowerShell.exe (these are system processes very often used in the malware code.)

PASSED TESTS: 9 / 11

Enabling certain features or banking mode had no impact on the final result.

Recommendation AWARD BEST++

THE INDEPENDENT ANTIVIRUS TESTS

SOPHOS HOME

Test of software for online banking protection

Product name: Sophos Home Premium
Version: 2.0.12
Testing date: february 2019

Type of test	Default Settings	Custom Settings or/and Banking Mode ON
Clipboard Hijacking Attack. The test verifies whether it's possible for malware to capture clipboard content and send it to a C&C server.	✓ PASSED	✓ PASSED
Clipboard Swapping Attack. The test verifies whether it's possible for malware to change clipboard content copied from messenger, email, PDF invoice or website.	✓ PASSED	✓ PASSED
Keylogger Attack. The test verifies whether it's possible for malware to register keystrokes on a keyboard while logging into bank account and send them to attacker's Gmail account.	✓ PASSED	✓ PASSED
Screenshot Attack. The test verifies whether it's possible for malware to take a screenshot.	✓ PASSED	✓ PASSED
RAM Scraping Attack. The test verifies whether it's possible for malware to extract confidential information from RAM, e.g. credit card numbers, passwords, logins, or bank account numbers.	✓ PASSED	✓ PASSED
DLL Injecting Attack. The test verifies whether it's possible to inject malicious DLLs into "safe browser", "virtual environment", or web browser processes while visiting HTTP pages. Used methods: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ PASSED	✓ PASSED
MITM Code Injecting Attack. The test verifies whether it's possible to inject HTML and JavaScript code into websites.	✗ FAILED	✗ FAILED
MITM Password Sniffing Attack. The test verifies whether it's possible to capture confidential information from websites which are secured by SSL certificate.	✗ FAILED	✗ FAILED
Hidden Desktop Sniffing Attack. The test verifies whether it's possible for malware to establish remote connection during active session with secured login page of the bank.	✓ PASSED	✓ PASSED
HOSTS Modifying Attack. The test verifies whether it's possible for malware to manipulate the contents of Windows HOSTS file.	✓ PASSED	✓ PASSED
Detecting thirteen banking trojans in-the-wild in February 2019.	POSITIVE: 13 / 13	

PASSED TESTS: 9 / 11

Enabling certain features or banking mode had no impact on the final result.

Description of unique banking protection components to allow better understanding how your technology protects users when banking session is active.

Sophos Home Premium uses a machine learning in the Deep Learning technology for detecting threats, so the same solutions used by the largest global companies protecting their interest through Sophos solutions. The software uses an artificial intelligence that can detect and block both known and new malicious software. Sophos Home Premium offers a real-time protection – preventing cybercriminals from exploiting vulnerabilities in trusted applications and operating systems or security credentials theft. Concerning online banking protection, the solution of the British company protects bank details and credit cards against interception by third parties. Sophos Home encrypts keystrokes in order to provide an additional layer of security. Nowadays, the vast majority of banking transactions take place on the Internet. Sophos additionally secures a browser. Besides a keystroke encryption, we've got constantly active protection against exploits, a detection of applications that access external hosts, and warnings against unauthorized code infection to a browser. All of these technologies work automatically and are enabled by default.

Recommendation AWARD BEST++

THE INDEPENDENT ANTIVIRUS TESTS

Test of software for online banking protection

Product name: Sophos Intercept X
Version: 2.0.12
Testing date: february 2019

Type of test	Default Settings	Custom Settings or/and Banking Mode ON
Clipboard Hijacking Attack. The test verifies whether it's possible for malware to capture clipboard content and send it to a C&C server.	✓ PASSED	✓ PASSED
Clipboard Swapping Attack. The test verifies whether it's possible for malware to change clipboard content copied from messenger, email, PDF invoice or website.	✓ PASSED	✓ PASSED
Keylogger Attack. The test verifies whether it's possible for malware to register keystrokes on a keyboard while logging into bank account and send them to attacker's Gmail account.	✓ PASSED	✓ PASSED
Screenshot Attack. The test verifies whether it's possible for malware to take a screenshot.	✓ PASSED	✓ PASSED
RAM Scraping Attack. The test verifies whether it's possible for malware to extract confidential information from RAM, e.g. credit card numbers, passwords, logins, or bank account numbers.	✓ PASSED	✓ PASSED
DLL Injecting Attack. The test verifies whether it's possible to inject malicious DLLs into "safe browser", "virtual environment", or web browser processes while visiting HTTP pages. Used methods: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ PASSED	✓ PASSED
MITM Code Injecting Attack. The test verifies whether it's possible to inject HTML and JavaScript code into websites.	✗ FAILED	✓ PASSED (Block Inbound Connections in Private Network)
MITM Password Sniffing Attack. The test verifies whether it's possible to capture confidential information from websites which are secured by SSL certificate.	✗ FAILED	✓ PASSED (Block Inbound Connections in Private Network)
Hidden Desktop Sniffing Attack. The test verifies whether it's possible for malware to establish remote connection during active session with secured login page of the bank.	✓ PASSED	✓ PASSED
HOSTS Modifying Attack. The test verifies whether it's possible for malware to manipulate the contents of Windows HOSTS file.	✓ PASSED	✓ PASSED
Detecting thirteen banking trojans in-the-wild in February 2019.	POSITIVE: 13 / 13	

PASSED TESTS: 11 / 11

Enabling certain features or banking mode allowed to obtain a better result.

Description of unique banking protection components to allow better understanding how your technology protects users when banking session is active.

As in the solution for individual customers, Sophos Intercept X uses machine learning to detect unknown threats. Moreover, the availability of additional modules and configurations is much greater, so the Sophos solution meets the requirements set by large banks, corporations and government institutions, not without significance. Warning about files with low reputation plays an extremely important role in protecting workstations against new 0-day threats, while an extension of the downloaded file doesn't matter. A banking trojan developed for a specific institution will certainly alert the administrator. All threats are automatically removed and information about detected suspicious activity is sent from workstations to the Sophos Central. Security policy settings prepared by the developer can be changed to more aggressive. Already activated by default functionality should not be disabled, because it can affect effectiveness. Sophos Intercept X offers comprehensive protection against banking threats, however policy settings for computer used by employees during online banking should pay particular attention to the administrator.

Recommendation AWARD BEST+++

THE INDEPENDENT ANTIVIRUS TESTS

Test of software for online banking protection

Product name: SpyShelter Firewall
Version: 11.4
Testing date: february 2019

Type of test	Default Settings	Custom Settings or/and Banking Mode ON
Clipboard Hijacking Attack. The test verifies whether it's possible for malware to capture clipboard content and send it to a C&C server.	✓ PASSED	✓ PASSED
Clipboard Swapping Attack. The test verifies whether it's possible for malware to change clipboard content copied from messenger, email, PDF invoice or website.	✓ PASSED	✓ PASSED
Keylogger Attack. The test verifies whether it's possible for malware to register keystrokes on a keyboard while logging into bank account and send them to attacker's Gmail account.	✓ PASSED	✓ PASSED
Screenshot Attack. The test verifies whether it's possible for malware to take a screenshot.	✓ PASSED	✓ PASSED
RAM Scraping Attack. The test verifies whether it's possible for malware to extract confidential information from RAM, e.g. credit card numbers, passwords, logins, or bank account numbers.	✓ PASSED	✓ PASSED
DLL Injecting Attack. The test verifies whether it's possible to inject malicious DLLs into "safe browser", "virtual environment", or web browser processes while visiting HTTP pages. Used methods: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ PASSED	✓ PASSED
MITM Code Injecting Attack. The test verifies whether it's possible to inject HTML and JavaScript code into websites.	✓ PASSED	✓ PASSED
MITM Password Sniffing Attack. The test verifies whether it's possible to capture confidential information from websites which are secured by SSL certificate.	✓ PASSED	✓ PASSED
Hidden Desktop Sniffing Attack. The test verifies whether it's possible for malware to establish remote connection during active session with secured login page of the bank.	✓ PASSED	✓ PASSED
HOSTS Modifying Attack. The test verifies whether it's possible for malware to manipulate the contents of Windows HOSTS file.	✓ PASSED	✓ PASSED
Detecting thirteen banking trojans in-the-wild in February 2019.	POSITIVE: 13 / 13	

PASSED TESTS: 11 / 11

Enabling certain features or banking mode had no impact on the final result.

Description of unique banking protection components to allow better understanding how your technology protects users when banking session is active.

The software provides a preventive approach to the security and uses advanced techniques to detect and block data breach attempts. Defensive actions may include alerting a user with messages and a scanner in the cloud. SpyShelter doesn't block malware with the use of developed vaccines or heuristic methods. The solution monitors all system processes and services that create a secured workspace called the operating system. The SpyShelter Firewall guarantees an operating system and data protection against the entire spectrum of malware: worms, spyware, keyloggers, and ransomware. However, it doesn't secure user assets in the same way as other specialized solutions which detect anomalies on the basis of heuristics. The main difference between them is the method of detecting abnormalities, i.e. deviations from the normal functioning of processes, operating system, and installed applications. For the SpyShelter Firewall, threats such as keyloggers, spyware, or ransomware, aren't viruses in the traditional sense of the word, but a sequence of inseparable events (actions) which notifies a user about. The SpyShelter Firewall doesn't automatically remove malicious software, it can recognize files using the integrated antivirus scanner in the Jotti cloud (or other – it has the ability to configure an external file scanner). HIPS is just one defense layer that is part of the SpyShelter Firewall solution.

Recommendation AWARD BEST+++

THE INDEPENDENT ANTIVIRUS TESTS

Test of software for online banking protection

Product name: Trend Micro Maximum Security
Version: 15.0.1212
Testing date: february 2019

Type of test	Default Settings	Custom Settings or/and Banking Mode ON
Clipboard Hijacking Attack. The test verifies whether it's possible for malware to capture clipboard content and send it to a C&C server.	✘ FAILED	✓ PASSED (Hypersensitive Protection Level)
Clipboard Swapping Attack. The test verifies whether it's possible for malware to change clipboard content copied from messenger, email, PDF invoice or website.	✘ FAILED	✓ PASSED (Hypersensitive Protection Level)
Keylogger Attack. The test verifies whether it's possible for malware to register keystrokes on a keyboard while logging into bank account and send them to attacker's Gmail account.	✓ PASSED	✓ PASSED
Screenshot Attack. The test verifies whether it's possible for malware to take a screenshot.	✘ FAILED	✓ PASSED (Hypersensitive Protection Level)
RAM Scraping Attack. The test verifies whether it's possible for malware to extract confidential information from RAM, e.g. credit card numbers, passwords, logins, or bank account numbers.	✘ FAILED	✓ PASSED (Hypersensitive Protection Level)
DLL Injecting Attack. The test verifies whether it's possible to inject malicious DLLs into "safe browser", "virtual environment", or web browser processes while visiting HTTP pages. Used methods: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ PASSED	✓ PASSED
MITM Code Injecting Attack. The test verifies whether it's possible to inject HTML and JavaScript code into websites.	✘ FAILED	✘ FAILED
MITM Password Sniffing Attack. The test verifies whether it's possible to capture confidential information from websites which are secured by SSL certificate.	✘ FAILED	✘ FAILED
Hidden Desktop Sniffing Attack. The test verifies whether it's possible for malware to establish remote connection during active session with secured login page of the bank.	✓ PASSED	✓ PASSED
HOSTS Modifying Attack. The test verifies whether it's possible for malware to manipulate the contents of Windows HOSTS file.	✓ PASSED	✓ PASSED
Detecting thirteen banking trojans in-the-wild in February 2019.	POSITIVE: 13 / 13	

Description of unique banking protection components to allow better understanding how your technology protects users when banking session is active.

TrendMicro uses its own local technologies to protect against malware. The antivirus module analyzes information about each file that can be opened, saved, and downloaded. If a file contains a malicious code, the antivirus will try to fix or delete a file using signatures or a heuristic analysis. In the event that a threat is identified as spyware, TrendMicro automatically removes it. The antivirus protection is supported by scanning in the cloud. The TrendMicro Smart Protection Network automatically correlates information on security threats on millions of computers around the World to help to develop a protection against new threats. The more users participate in this project, the more effective the network is. The Smart Protection Network collects over 6 terabytes of data on a daily basis. These data represent increasingly expanding threat vectors, including URLs, IP addresses, domains, files, network traffic, and C&C servers. In online banking, TrendMicro allows secure access to banking websites or online stores using a default browser through Pay Guard feature. Once installed, it automatically creates a shortcut icon on the desktop that launch the default browser and provides the security necessary for online transfers.

PASSED TESTS: 9 / 11

Enabling certain features or banking mode allowed to obtain a better result.

Recommendation AWARD BEST++

THE INDEPENDENT ANTIVIRUS TESTS

WEBROOT® Smarter Cybersecurity™

Test of software for online banking protection

Product name: Webroot SecureAnywhere Antivirus
Version: 9.0.24.49
Testing date: february 2019

Type of test	Default Settings	Custom Settings or/and Banking Mode ON
Clipboard Hijacking Attack. The test verifies whether it's possible for malware to capture clipboard content and send it to a C&C server.	✗ FAILED	✓ PASSED (Enabled Heuristic Whitelist Mode)
Clipboard Swapping Attack. The test verifies whether it's possible for malware to change clipboard content copied from messenger, email, PDF invoice or website.	✗ FAILED	✓ PASSED (Enabled Heuristic Whitelist Mode)
Keylogger Attack. The test verifies whether it's possible for malware to register keystrokes on a keyboard while logging into bank account and send them to attacker's Gmail account.	✗ FAILED	✓ PASSED (Enabled Heuristic Whitelist Mode)
Screenshot Attack. The test verifies whether it's possible for malware to take a screenshot.	✗ FAILED	✓ PASSED (Enabled Heuristic Whitelist Mode)
RAM Scraping Attack. The test verifies whether it's possible for malware to extract confidential information from RAM, e.g. credit card numbers, passwords, logins, or bank account numbers.	✗ FAILED	✓ PASSED (Enabled Heuristic Whitelist Mode)
DLL Injecting Attack. The test verifies whether it's possible to inject malicious DLLs into "safe browser", "virtual environment", or web browser processes while visiting HTTP pages. Used methods: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✓ PASSED	✓ PASSED
MITM Code Injecting Attack. The test verifies whether it's possible to inject HTML and JavaScript code into websites.	✗ FAILED	✗ FAILED
MITM Password Sniffing Attack. The test verifies whether it's possible to capture confidential information from websites which are secured by SSL certificate.	✗ FAILED	✗ FAILED
Hidden Desktop Sniffing Attack. The test verifies whether it's possible for malware to establish remote connection during active session with secured login page of the bank.	✓ PASSED	✓ PASSED
HOSTS Modifying Attack. The test verifies whether it's possible for malware to manipulate the contents of Windows HOSTS file.	✓ PASSED	✓ PASSED
Detecting thirteen banking trojans in-the-wild in February 2019.	POSITIVE: 13 / 13	

Description of unique banking protection components to allow better understanding how your technology protects users when banking session is active.

Webroot products make the most of the potential of the cloud computing. The antivirus agent doesn't download signatures to a local disk. Its size after installation is about 4MB. Files are scanned on the developer servers to achieve a better performance. Converning the protection of online banking, Webroot has everything that can be expected from modern software to combat Internet crime. Webroot points to several types of attacks against which it protects: cookie files and Internet data theft, man-in-the-middle attacks, keyloggers, system clipboard isolation, man-in-the-browser attacks, taking screenshots by malware, and blocking suspicious processes that may access a browser. Suspicious applications are monitored during operation and blocked if necessary. A controlled process still have access to the Internet, so a stolen computer data can't be recovered. The default settings are configured for non-technical users, therefore they aren't the best.

PASSED TESTS: 9 / 11

Enabling certain features or banking mode allowed to obtain a better result.

Recommendation AV LAB AWARD BEST++

THE INDEPENDENT ANTIVIRUS TESTS

Test of software for online banking protection

Product name: Windows Defender
Testing date: february 2019

Type of test	Default Settings Chrome and Firewall ON	Custom Settings EDGE and Windows Defender SmartScreen ON
Clipboard Hijacking Attack. The test verifies whether it's possible for malware to capture clipboard content and send it to a C&C server.	✓ PASSED	✓ PASSED
Clipboard Swapping Attack. The test verifies whether it's possible for malware to change clipboard content copied from messenger, email, PDF invoice or website.	✗ FAILED	✗ FAILED
Keylogger Attack. The test verifies whether it's possible for malware to register keystrokes on a keyboard while logging into bank account and send them to attacker's Gmail account.	✗ FAILED	✗ FAILED
Screenshot Attack. The test verifies whether it's possible for malware to take a screenshot.	✗ FAILED	✗ FAILED
RAM Scraping Attack. The test verifies whether it's possible for malware to extract confidential information from RAM, e.g. credit card numbers, passwords, logins, or bank account numbers.	✗ FAILED	✗ FAILED
DLL Injecting Attack. The test verifies whether it's possible to inject malicious DLLs into "safe browser", "virtual environment", or web browser processes while visiting HTTP pages. Used methods: CreateRemoteThread, QueueUserAPC, RtlCreateUserThread, SetThreadContext.	✗ FAILED	✗ FAILED
MITM Code Injecting Attack. The test verifies whether it's possible to inject HTML and JavaScript code into websites.	✗ FAILED	✗ FAILED
MITM Password Sniffing Attack. The test verifies whether it's possible to capture confidential information from websites which are secured by SSL certificate.	✗ FAILED	✗ FAILED
Hidden Desktop Sniffing Attack. The test verifies whether it's possible for malware to establish remote connection during active session with secured login page of the bank.	✓ PASSED	✓ PASSED
HOSTS Modifying Attack. The test verifies whether it's possible for malware to manipulate the contents of Windows HOSTS file.	✗ FAILED	✗ FAILED
Detecting thirteen banking trojans in-the-wild in February 2019.	POSITIVE: 13 / 13	

Description of unique banking protection components to allow better understanding how your technology protects users when banking session is active.

Windows Defender as an integral part of the Windows systems protects against malware, exploits, and ransomware. It works with the system SmartScreen feature which analyzes downloaded files from the network and applications from the Microsoft Store for source files, checksums, and file blacklist patterns. All this information are delivered to Windows Defender in the form of signatures. As befits antivirus software, Windows Defender has a real-time protection against, spyware, trojans, fake installers, or even potentially unwanted applications. Although, the SmartScreen effectively protects against suspicious files and warns if the file doesn't have a digital signature, but it can generate false positives and block legitimate installers. The antivirus lacks basic protection mechanisms at the firewall level and more advanced techniques for analyzing a new malicious code, including scripts in the Windows system.

PASSED TESTS: 2 / 11

Enabling certain features or banking mode had no impact on the final result.

Recommendation AV LAB ONLY TESTED