Executive Summary
On Zemana Antilogger

CYBER SECURITY &
PRIVACY FOUNDATION

Software: Zemana Antilogger for Windows.

Lab Setup:

Oracle Virtualbox v4.3.6 r91406

Operating System:

Machine 1: Windows 7 32-Bit.

Processor:

Intel(R) Core(TM)i5-4200U CPU @1.60GHz 2.30GHz

RAM:

512MB

Test Criteria:

This test is specifically done for Indian Environment as it is unique as 50% of the machine are pre infected machines. Though there are awards like Virus Bulletin 100, VB 100 concentrates on a product detecting 100% of all the viruses "In The Wild" (ITW). Many of the samples which are present in India do not make to ITW List. All the products of VB 100% award are checked for only detecting the virus, most of the products fail in Indian Environment because the machine is pre infected or the anti-virus is not able to clean them. We decided to test the products with the test criteria which is unique to the Indian Environment.

We have set up the test in various levels.

Known Keylogger: Keylogger that is widely spread and is detect by a majority of antiviruses are anti keyloggers.

Unknown Keylogger: Keylogger sample that was developed exclusively for this test, hence unknown to any antivirus vendor.

Test for Webcam Hijacking: In this test, the machine is infected with malwares. These malwares hijack the webcam and the mic of the infected machine.

Test for MITB Attacks: In this test a malware is infected into the machine that is specifically specified to perform Man-in-the-Browser (MITB) attack.

Test for Clipboard Capture: In this test the machine is infected with a malware that is specifically designed to capture the clipboard contents.

Test for Screenshot capture: In this test the machine is infected with a malware that is specifically designed to capture the screenshots of the machine in which it is running.

Infecting the machine before installing the Antilogger: In this test the machines were infected with known malware before the antilogger is installed. The reason for this test is that most of Indian computers are already infect with some sort of malware before an antivirus is installed and the this test hopes to test if the antilogger is able to remove all previous infections after it is installed.

Infecting the machine after installing the Antilogger: In this test the computers are not infected with any keyloggers or malwares before the antilogger is installed. After the antilogger is installed, the machine is scanned for keyloggers and malwares.

Installation:

General Installation with all the Terms and Agreement to be agreed.

Configuration:

General pre-built Configuration that comes by default in Zemana Antilogger.

Product: Zemana Antilogger.

Test Results:

Test 1: Detection of Known Keylogger.

- ☑ Machine Infected before Zemana Antilogger was installed.
- ☑ Machine infected after Zemana Antilogger was installed.

Test 2: Detection of Unknown Keylogger.

- ☒ Machine Infected before Zemana Antilogger was installed.
- ☒ Machine infected after Zemana Antilogger was installed.

Test 3: Detection of Malware that performs MITB Attacks.

- ☒ Machine Infected before Zemana Antilogger was installed.
- ☑ Machine infected after Zemana Antilogger was installed.

Test 4: Detecting of malware that performs "Clipboard Capture" attacks.

- ☒ Was found unsuccessful in detecting the malware.

Test 5: Detecting of malware that captures webcam.

- ☒ Was found successful in detecting the malware and alerting the user.

Test 6: Detecting of malware that captures screenshot.

- ☒ Was found unsuccessful in detecting the malware.

Product: Zemana Antilogger Free.

Test 1: Detection of Known Keylogger.

- ☑ Machine Infected before Zemana Antilogger Free was installed.
- ☑ Machine infected after Zemana Antilogger Free was installed.

Test 2: Detection of Unknown Keylogger.

- ☑ Machine Infected before Zemana Antilogger was installed.
- ☑ Machine infected after Zemana Antilogger was installed.

Test 3: Detection of Malware that performs MITB Attacks.

- ☒ Was found unsuccessful in detecting the malware.

Conclusion:

In conclusion we observed that Zemana Antilogger was able to stop malicious software from being installed but failed to detect when the malware was actually intercepting passwords from protected pages. After doing much analysis with both Zemana Antilogger and the Zemana Antilogger Free Protection we found that both these tools are potentially good tools but we would say that the Zemana Antilogger needs some more bug fixes and sophistication. And we even recommend the inclusion of key scrambler into the Zemana Antilogger which was found to be present in the Free version, but not in the paid version.

The overall rating that we would give "Zemana Antilogger" is

"7/10"

The overall rating that we would give "Zemana Antilogger Free Protection" is

"9/10"