Report on
Zemana Antilogger

CYBER SECURITY &
PRIVACY FOUNDATION

Software Product: Zemana Antilogger.

Description of the Product:

Zemana AntiLogger is a powerful, efficient, and lightweight app that blocks hackers. It detects any attempts to modify your computer's settings, record your activities, hook to your PC's sensitive processes, or inject malicious code in your system.

Financial Malware Protection

The vast majority of banking and financial transactions take place on SSL-protected secure sites whose URLs begin with https. SSL data encryption reliably secures your data during online shopping and financial transactions, but hackers have found a vulnerable spot.

Sophisticated banker trojans and SSL sniffers are designed to steal your data directly from your PC, while you are entering it and before it gets encrypted, for transfer over the internet. This is an attack method used by the infamous ZeuS. The AntiLogger is one of the the very few products on the market that is able to close this dangerous vulnerability by intercepting and shutting down suspicious processes.

Cloud Powered Early Response System

Zemana's IntelliGuard is a smart early warning and response system that makes the AntiLogger easier to use and more reliable than ever before. Through IntelliGuard, your AntiLogger references in real time the latest community intelligence base of threats; and threats detected on your computer are scanned against over 40 malicious files databases and known bad files are blocked automatically. With IntelliGuard you will not receive prompts about legitimate programs you are installing on your computer.

Keystroke Logging Protection

Keystroke monitoring malware is the most common method of criminals to steal your login credentials. It is also very efficient if someone wishes to spy on you.
Zemana AntiLogger will prompt you when someone or something is trying to obtain access to your keyboard, regardless as to whether it is a known or new piece of spyware, banker trojan, financial malware or custom designed spy tool.

Screen Capture Protection

Screen input through virtual keyboards or image recognition is increasingly used as an extra security measure. Yet, if you have screen grabbing malware on your computer, the criminals will be able to see what is shown on your screen and where you point and click with the mouse. As part of the AntiLogger's all-round protection, your clipboard is safe from intruders.

Clipboard Remote Access Protection

How often do you copy and paste sensitive material? We all know we shouldn't, yet most of us do it. When you copy something, it remains stored in your computer's clipboard, where it can be made away with. As part of the AntiLogger's all-round protection, your clipboard is safe from intruders.

Webcam and Microphone Hijacking Protection

Yes, it is possible that your webcam and microphone can be turned on remotely, and if a pro is doing this, the status LED on your webcam will remain off. Your webcam can be turned into a surveillance camera; and while the hackers won't be able to drain your bank account or hijack your email, this is very intrusive and unpleasant. What if this were your child's computer?
Zemana AntiLogger constantly monitors all processes accessing your computer and will prompt you when an illegal application is trying to switch it on.

System Intrusion Protection

Malware relies on invading your system's sensitive areas, like its registry and physical memory (RAM), so it can inject its malicious code and seize control of your PC.
The AntiLogger's System Defense module secures the very heart of your PC in a future-proof way: it detects malicious attempts based purely upon their behavior, regardless of whether or not the malware attacking you has been identified, isolated, analyzed and your signature database updated.

Lab Setup:

Oracle Virtualbox v4.3.6 r91406

Operating System:

Machine: 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.

Report (Installation and configuration)

Installation:

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

Configuration:

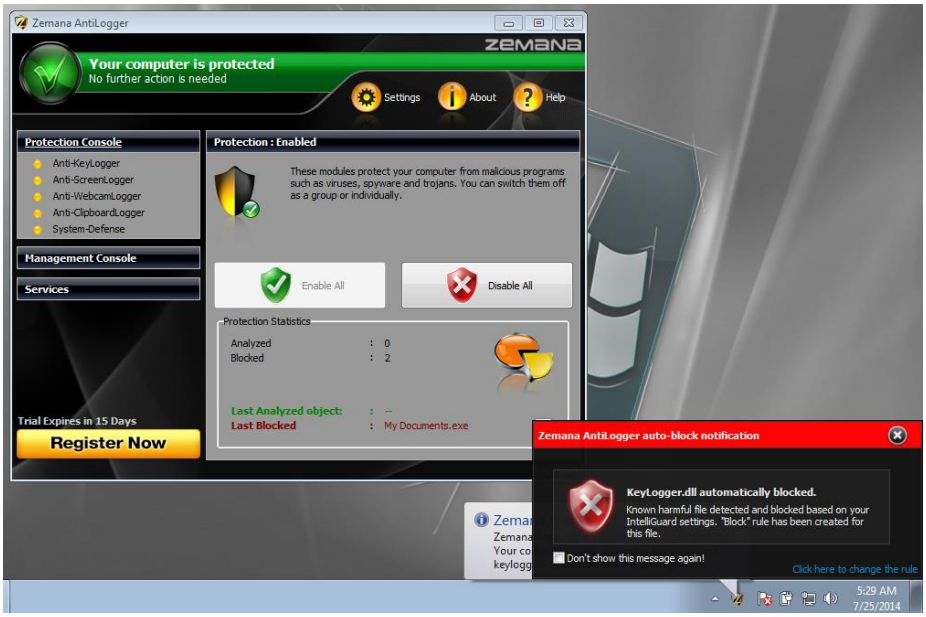
Pre-built configuration of the Zemana Antilogger.

Test Details

Infecting the machine before installing Zemana Antilogger:

Test 1: Detection of Known Keylogger.

Result: Detected the Known Keylogger Successfully and blocked it from recording the keystrokes further.

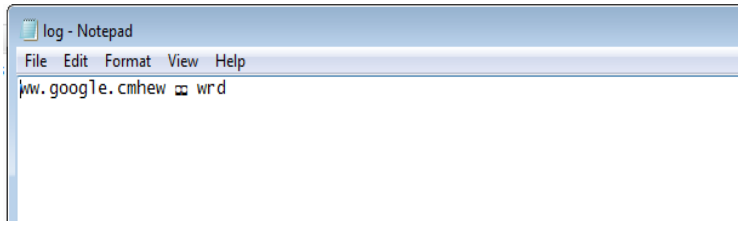


Description:

In this test we infected the machine with known keylogger and then we installed Zemana Antilogger to test if the Antilogger could detect the known keylogger. It was discovered that the Zemana Antilogger was able to successfully detect the keylogger and block it.

Test 2: Detection of Unknown Keylogger.

Result: Did not detect the Unknown Keylogger, and the keylogger was able to record the keystrokes successfully.



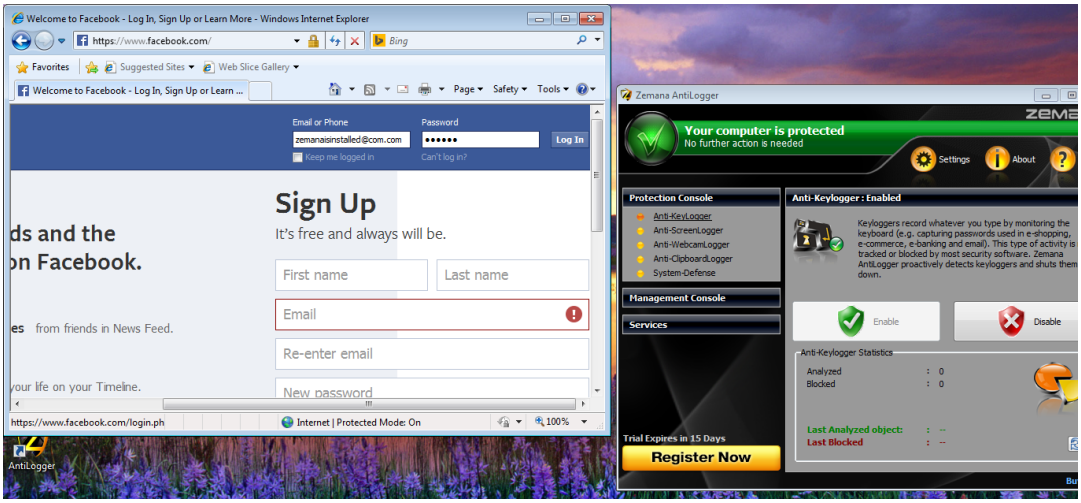
Description:

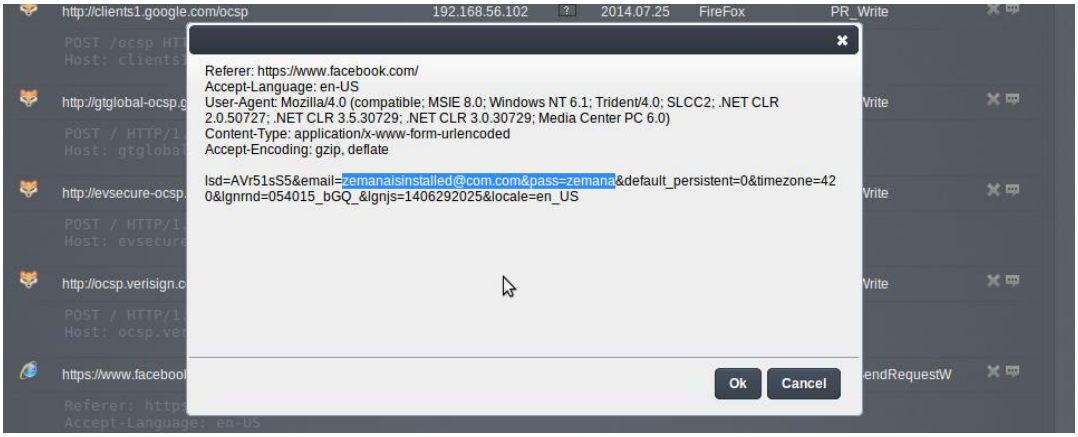
In this test we infected the machine with unknown keylogger and then we installed Zemana Antilogger to test if the Antilogger could detect the known keylogger. It was discovered that the Zemana Antilogger was unsuccessful in detecting the unknown keylogger and the keylogger was still able to capture the keystrokes successfully.

Test 3: Detection of Malwares that perform MITB Attacks.

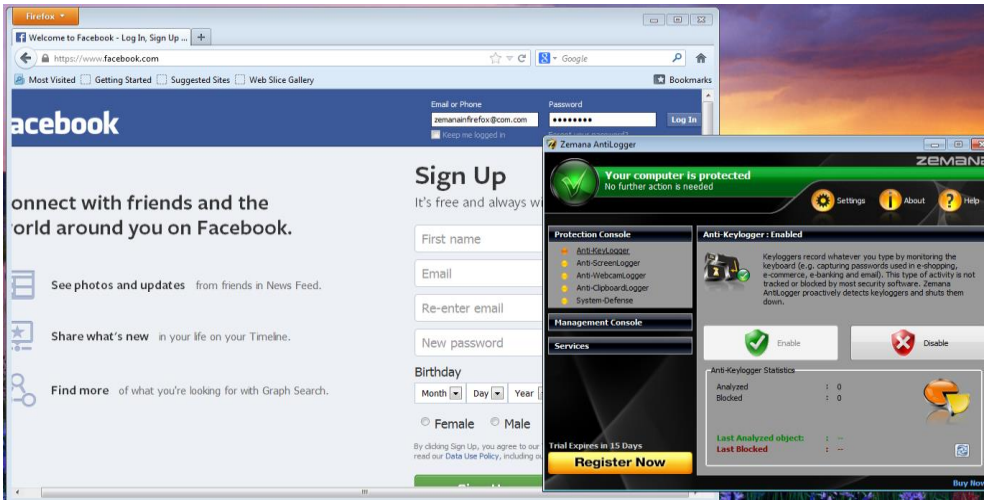
Result: Zemana was not able to detect that a malware was doing MITB attacks on the browsers. The malware was successfully able to intercept the passwords.

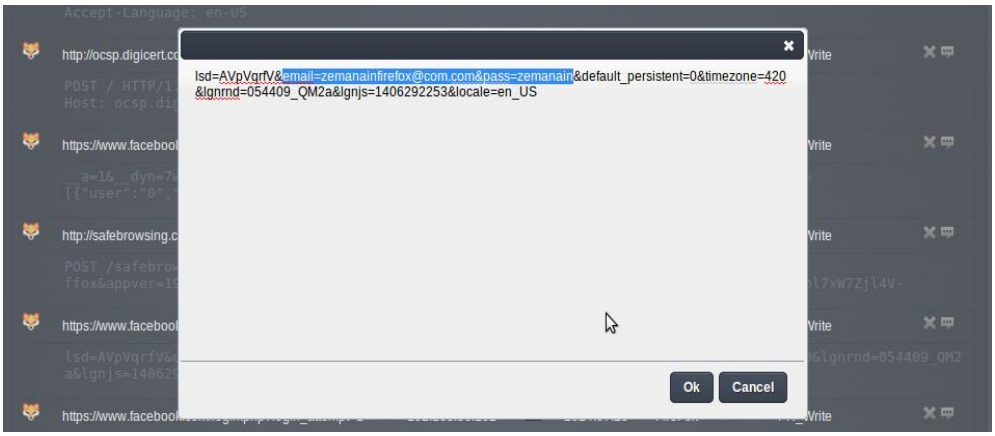
- Internet Explorer:





- Firefox:





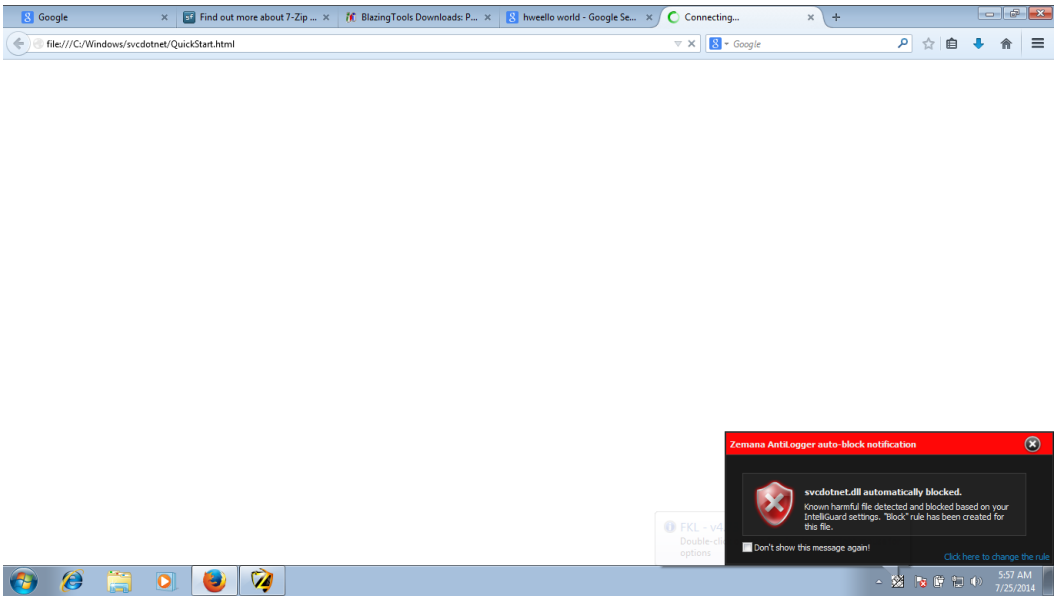
Description:

In this attack we infected a malware into the machine that was able to perform the Man-in-the-Browser (MITB) attack. We tried testing if Zemana Antilogger could detect this malware. But it was unsuccessful in detecting the malware and the malware was successful in intercepting the passwords.

Infecting the machine after installing Zemana Antilogger:

Test 1: Detection of Known Keylogger.

Result: Detected the Known Keylogger and removed it.

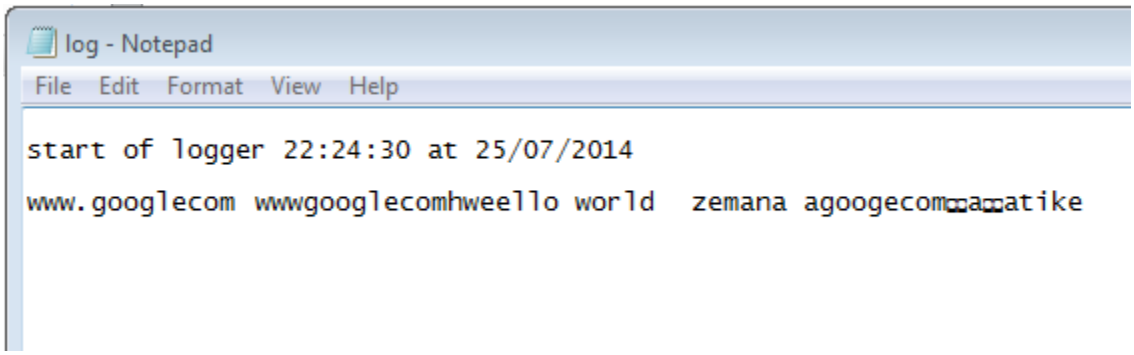


Description:

In this test we infected the known keylogger into a machine with Zemana Antilogger already installed. And we found that Zemana Antilogger was able to detect the keylogger and block it successfully.

Test 2: Detection of Unknown Keylogger.

Result: Zemana Antilogger was not able to detect the unknown Keylogger.



Description:

In this test we infected an unknown keylogger into a machine with Zemana Antilogger already installed. And we found that Zemana Antilogger unsuccessful in detecting the keylogger and the keylogger was able to successfully log the keystrokes.

Test 3: Detection of Malwares that do MITB Attacks.

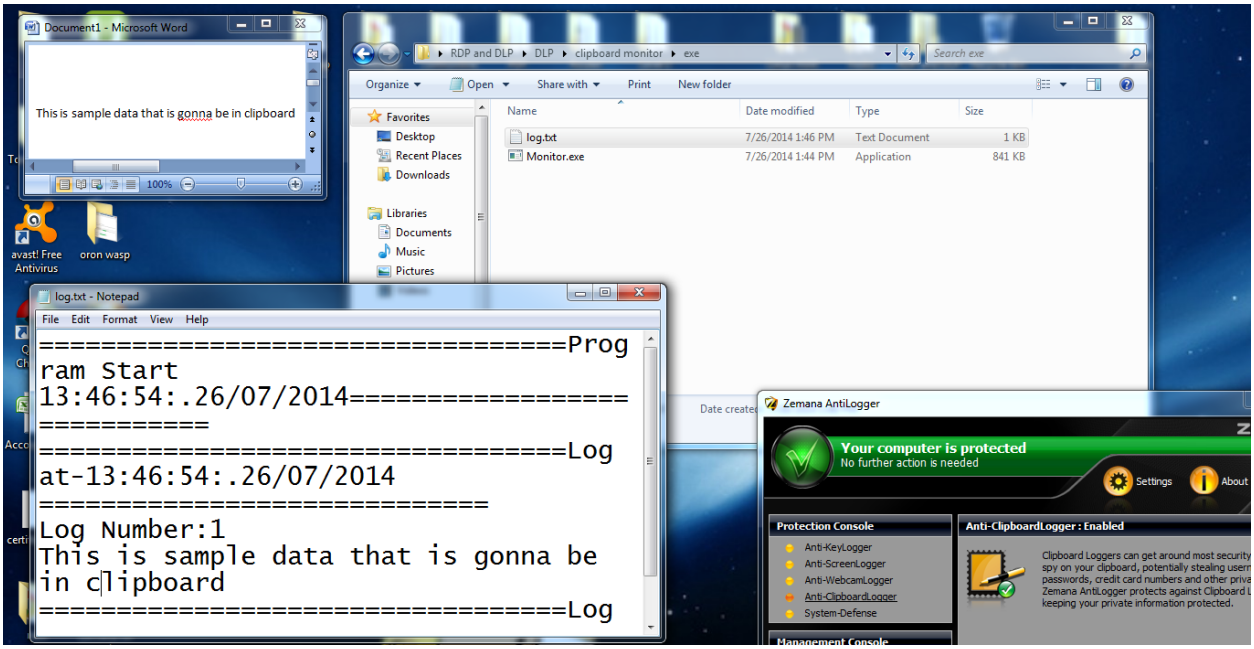
Result: Zemana was successful in blocking the malware from installing itself.

Description:

In this test we installed Zemana before we installed the malware that performs Man-in-the-Browser (MITB) attack and we observed that Zemana was indeed successful in block the malware from installing itself.

Detecting of malware that performs "Clipboard Capture" attacks.

Result: Zemana Antilogger was not able to detect that a malware was capturing the clipboard of the computer.

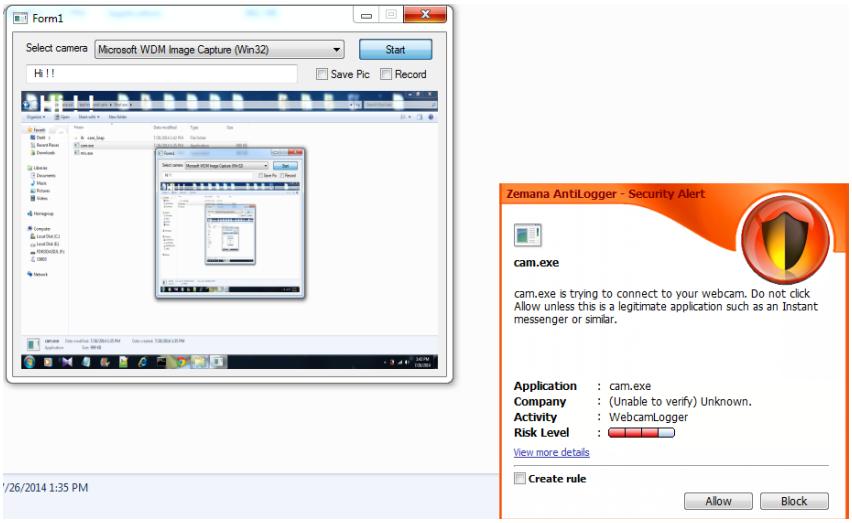


Description:

We infected the machine with a malware that was specified to perform "clipboard capture" attack. We tested the Zemana Antilogger if it protects against malwares that perform "clip board" capture attacks, and found that it was unsuccessful in detecting the malware.

Detection of malware that captures webcam.

Result: Zemana was able to successfully detect that a program is trying to access the webcam and showed a warning to the user.

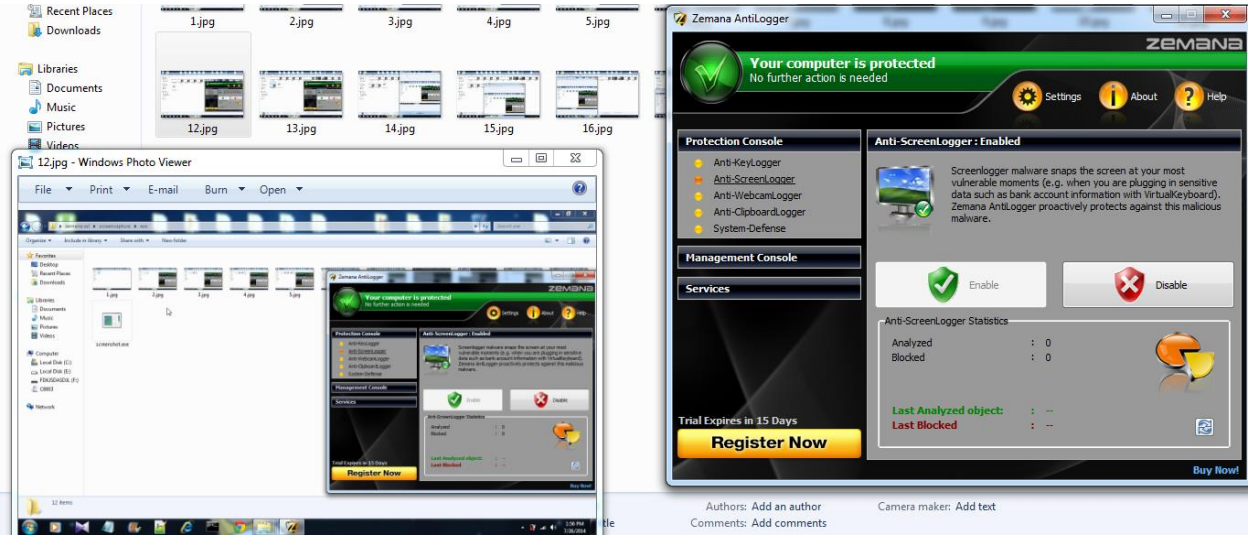


Description:

We infected the machine with a malware that was specified to capture images using webcam. We tested the Zemana Antilogger if it protects against such malwares, and found that it was successful in detecting the malware and showed a warning notification to the user.

Detection of malware that captures screenshots.

Result: Zemana was unsuccessful in detecting a program that was taking the screenshots of the machine.



Description:

We infected the machine with a malware that was specified to capture the screenshots of the machine. We tested the Zemana Antilogger if it protects against malwares that capture screenshots of the machine, and found that it was unsuccessful in detecting the malware.

Product: Zemana Antilogger Free

We even were able to test the free version of Zemana Antilogger and found the following results.

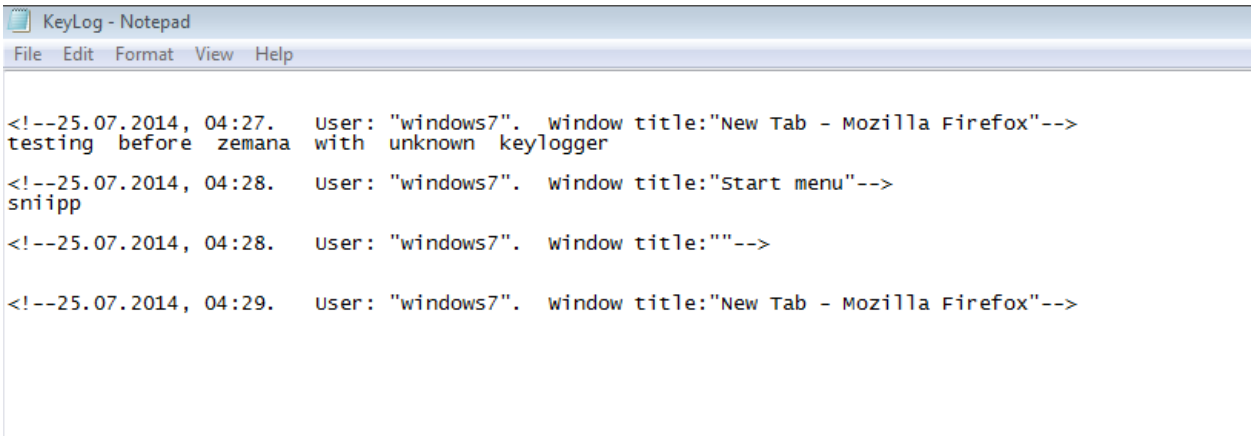
Key Feature of Zemana Antilogger Free Protection:

- Keylogger attacks from identity thieves and criminals
- Protects every application on your computer, and not just your web browser
- Stops keyloggers by scrambling every key that you type instantly, quietly, effective, in the background
- Even if the keyloggers capture your keystrokes, all they'll see are highly encrypted random characters
- No confusing options to set. The Free version scrambles every keystroke, and protects everything that you type.

Infecting the machine before installing the Antilogger

Test 1: Detection of Known Keylogger.

Result: Successfully didn't allow the keylogger to log the keystrokes.

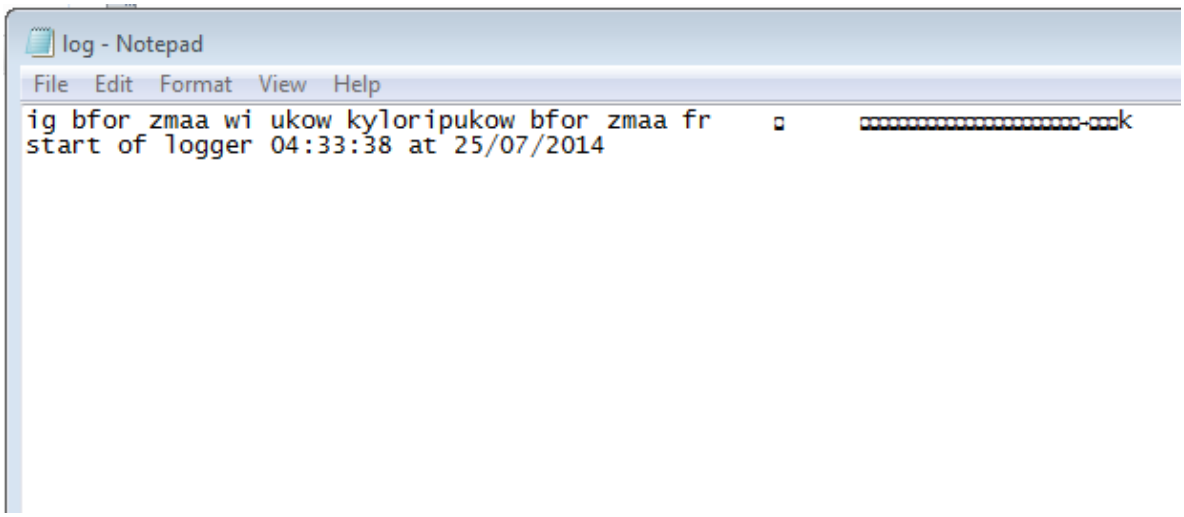


Description:

The above image is of the log file of the Keylogger, at time 4:27 when Zemana Free Antlogger was not installed we were able to see that the Keylogger was able to log the Keystrokes successfully. Later at time 4:29 when Zemana Free Antilogger was installed we were able to see that the Keylogger was not able to log any keystrokes.

Test 2: Detection of Unknown Keylogger.

Result: Successfully didn't allow the keylogger to log the keystrokes.

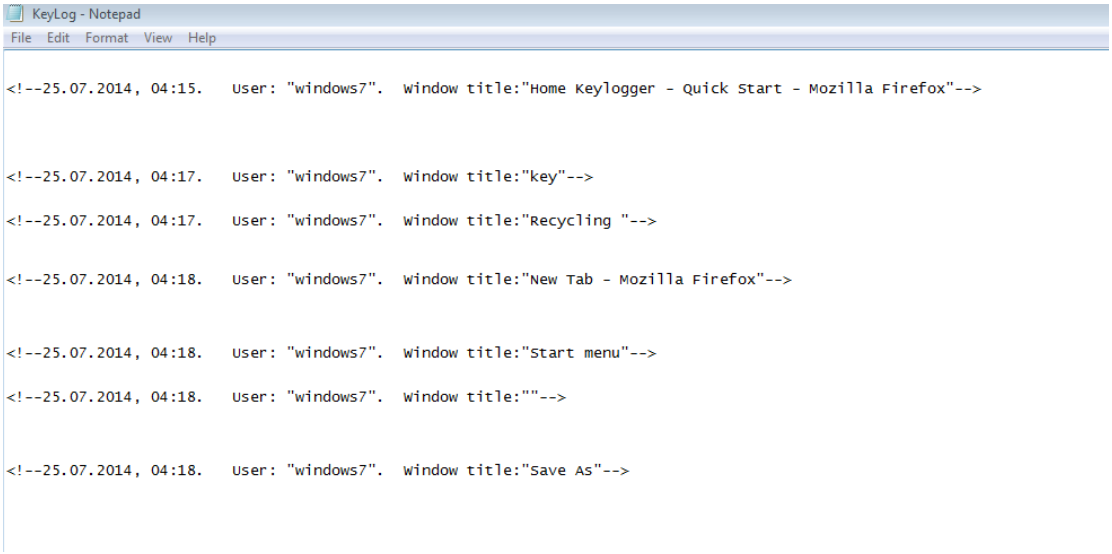


Description:

In the above image we see that the keylogger was successfully logging the keystrokes before Zemana Free Antilogger was installed. After the installation of the Zemana Free Antilogger, we found that the unknown keylogger was not able to log the keystrokes.

Infecting the machine after installing the Antilogger.

Test 1: Detection of Known Keylogger.

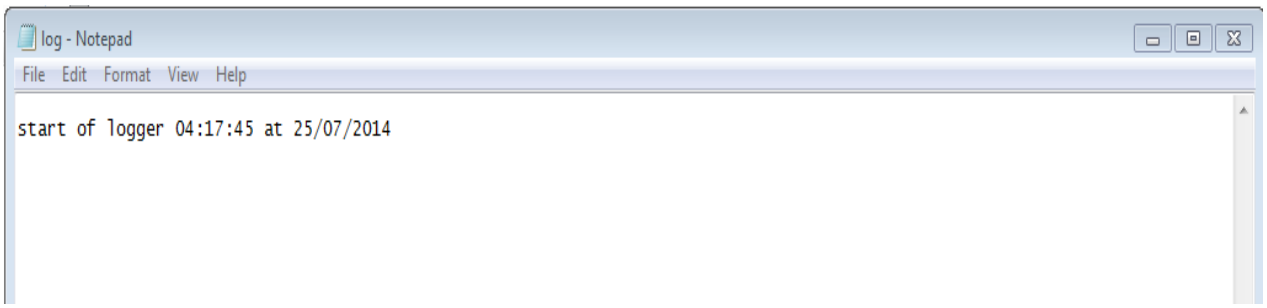


Description:

In the above image we see that a keylogger being infected into a system in which Zemana Free Antilogger is already installed. And we see that Zemana Free Antilogger did not allow the keylogger to log the keystrokes.

Test 2: Detection of the Unknown Keylogger.

Result: We discovered that the Zemana Free Antilogger did not allow the Unknown Keylogger to record the keystrokes.



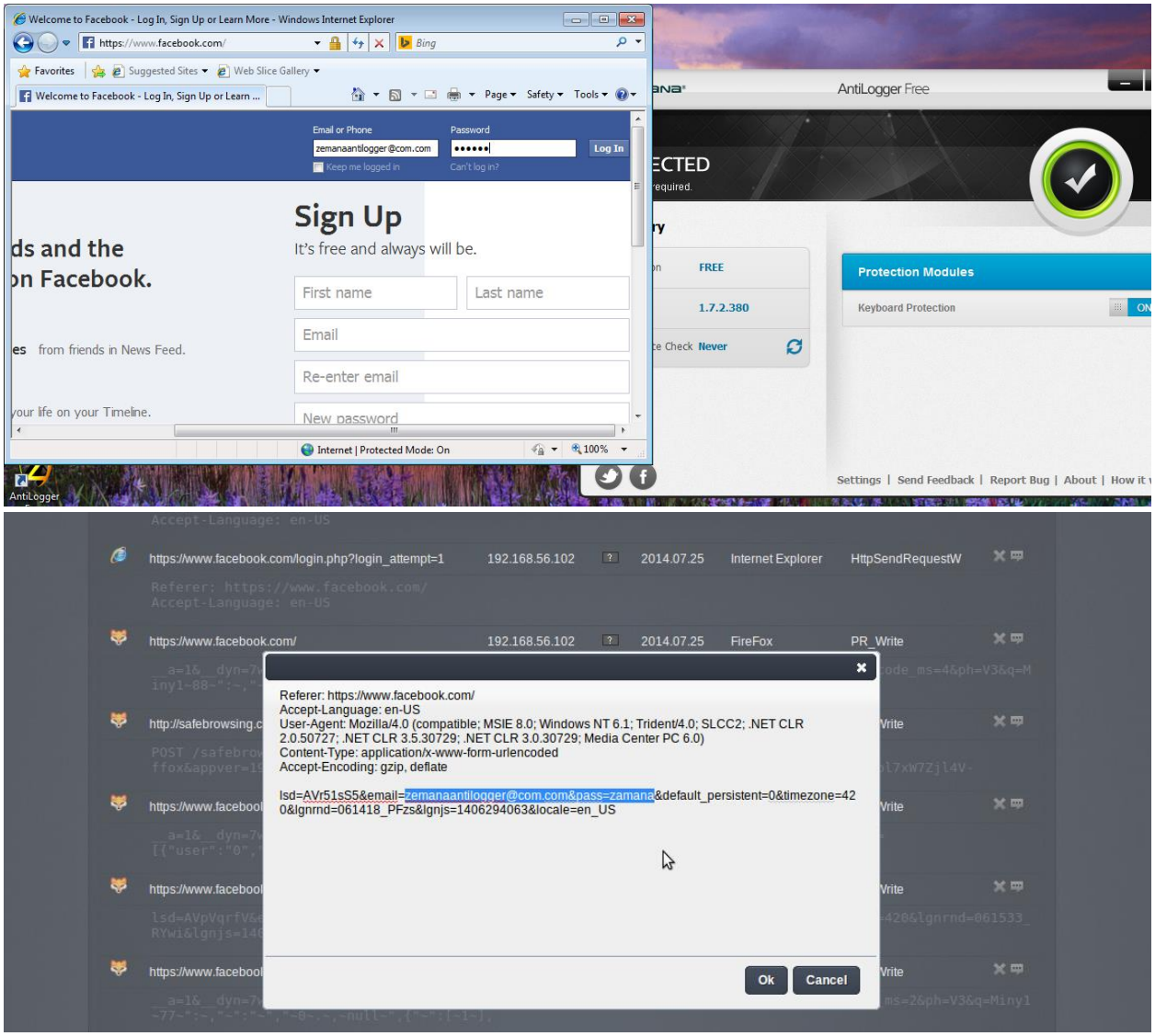
Description: We discovered that when the unknown keylogger was installed on a machine which already had Zemana Free Antilogger was installed, we found that the Zemana Free Antilogger did not allow the keylogger to log the keystrokes.

Test 3: Protection against MITB Malware.

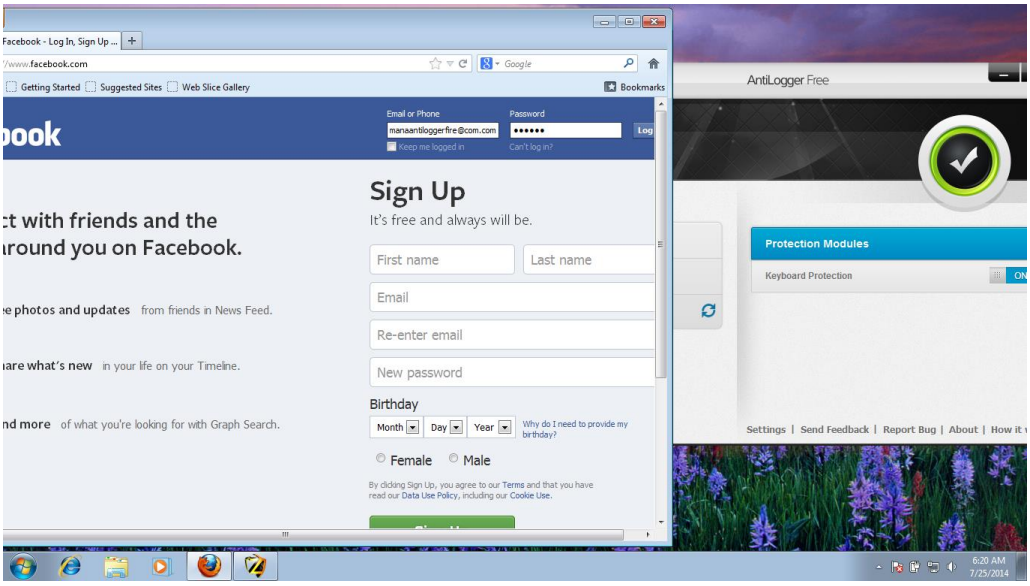
Result: As seen in the screenshots we found that it was not able to protect against MITB attacks.

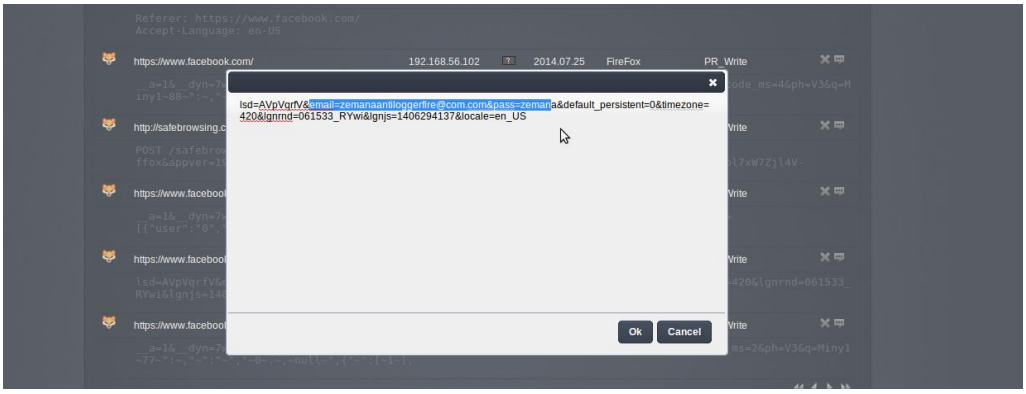
Test site: https://www.facebook.com

Internet Explorer:



Firefox:





Description:

In this attack we infected a malware into the machine that was able to perform the Man-in-the-Browser (MITB) attack. We tried testing if Zemana Free Antilogger could protect against this malware. But it was unsuccessful and the malware was successful in intercepting the passwords.

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"