



We Keep You Safe!

ZEMANA®



Zero-Hour Behavior Triggered Data Theft Prevention

Now Available as Your Competitive Edge

Financial Malware

The notorious Zeus is just one example of modern-day financial malware. It impacted an estimated 3.6 million computers in the U.S. alone and over 13 million worldwide. Damages are estimated at over \$500 million. To date, it is designed to change its shape every couple of hours, effectively bypassing fingerprint based protection. After 5 years of hide-and-seek with the security industry, Zeus remains a major threat today.

Research alarms that even up-to-date anti-virus programs are only 23% effective at blocking Zeus. Zeus' source code is now available on the back market for just a couple hundred dollars.

In 2010 a new form of financial malware was discovered: Carberp. It takes full control of infected machines, detects and removes competing infections, such as Zeus, and has the ability to completely disable anti-virus products. Carberp is seen as one of the more advanced forms of financial malware and experts expect its infections in the West to increase significantly in coming years.

Recent news report that Shylock, a financial malware popular with its ability to remain undetected by anti-virus products, is making a comeback.

The question seems to be not if, but when the next big one is coming. And will it be just one or a number of them...?

Traditional Security Solutions are Essential, But Not Enough

Malware is now more aggressive than ever, the reason being clear and simple: designing malware is now a business. A very lucrative business. As the world is sharing more and more over the internet and security is improving, criminals are becoming more creative, more professional and more savvy in getting what they want. Estimates vary, but over 60,000 new pieces of malware every day seems to be the commonly accepted figure.

While traditional security solutions are essential, zero-day, advanced and custom designed malware is able to slip through. Hardly surprising, these are the most malicious types of malware, causing billions of dollars in losses each year.

An Intelligent Protection

Zemana AntiLogger is made to protect against the new kind of threats: forms of malware that are developed as a money-making tool. Viruses, worms, key-loggers and screen-grabbers, (SSL) banker trojans, rootkits and executables that are developed to collect passwords, credit cards, social security numbers, or outright drain bank accounts. Oversimplifying it, these forms of malware always rely on stealing information

and/or gaining access to the browser as the first step in their process.

Zemana AntiLogger employs an innovative approach in closing important loopholes present in the vast majority of traditional security solutions. The technology does not rely on the standard

Detection-Analysis-Updates process and adds a protection layer which is independent from the fingerprint database. By analyzing how computer processes behave, the AntiLogger is able to effectively address vulnerabilities exploited by new forms of malware, such as Zeus and SpyEye. It is able to detect






sophisticated and highly targeted attacks that are designed to bypass traditional security solutions.

After a couple of years on the market as a standalone product, and with proven functionality, reliability and stability, Zemana AntiLogger is now available as semi-branded or fully rebranded product, and as ready and simple to implement Software Development Kit (SDK).

The product offers a line of defense that is conceptually different from traditional security solutions and is designed to work alongside them. It has been proven effective by numerous tests and reviews.

Modern-day cyber criminals know the loopholes in traditional security solutions and are able to circumvent them

Protection Features

-  Intercepts attempts to record and steal user information in real time: at the moment of the attempt. Its behavior-based technology is equally efficient against known and zero-day malware.
-  Monitors in real time the system's sensitive processes, installation, registry and file changes, spotting and stopping all suspicious behavior. No need to scan. Runs virtually invisible to the user.
-  Virtually no false positives and possibilities to automate product response through intelligent analysis and the power of the cloud.
-  Bulletproof Self-defense: resilient against targeted attacks to be bypassed, tampered with or disabled.
-  Small in size, runs efficiently, needs little system resources, supports silent updates, user friendly and compatible.

Protection Modules

The technology features a number of separate modules in order to ensure coverage of all points where user information may be stolen from, namely:

- Keystroke Capture Protection Module
- Screen Capture Protection Module
- Webcam Hijack Protection Module
- Clipboard Capture Protection Module
- SSL Logger Protection Module
- System Defense Module



How it Works

Zemana AntiLogger is able to intercept over 60 types of attacks used by information stealing malware. It guards against attempts to log the keyboard, screen, clipboard, webcam, microphone and the system's sensitive elements (featuring a HIPS). Our unique SSL logger protection technology is efficient against advanced financial malware, such as Zeus. The product works at kernel level, protecting the system as a whole and is thus application independent.

The AntiLogger employs an innovative, proactive and signature independent approach. By monitoring the system's processes in real time and using sophisticated behavioral analysis, Zemana AntiLogger is able to isolate malicious processes based purely on their activity. In this way it closes the time gap when new forms of malware can spread uncontrollably. Zemana AntiLogger is also efficient against niche, targeted attacks which may go undetected by the traditional signature based apps.

No False Positives

False positives are traditionally associated with behavior-based malware detection methods, heavily impacting user interaction and experience. They also lead to compromised overall effectiveness due to limited reliability of the users' decision to run or block suspicious files.

Zemana's IntelliGuard is a smart early warning and response system that improves the product's reliability and enhances user experience. By harnessing the power of the cloud, the technology ensures that a single false positive will appear only once, or in the worst case scenario a couple of times, while real threats are blacklisted instantly.

The system allows for tailor-making of the level of automation in allow/block decisions and fine-tuning user interaction to suit your needs. It can trigger auto-response based on the statistical data about allow/block decisions taken within the user community, known threats can be automatically blocked, and all this with or without user prompts, and with or without option for the user to override the decision.

Independent Product Performance Audit

By: Software Security Consultants, LLC
 Product: Zemana AntiLogger
 Methodology: Attempts to defeat the Product using all possible attack vectors ("like an attacker")

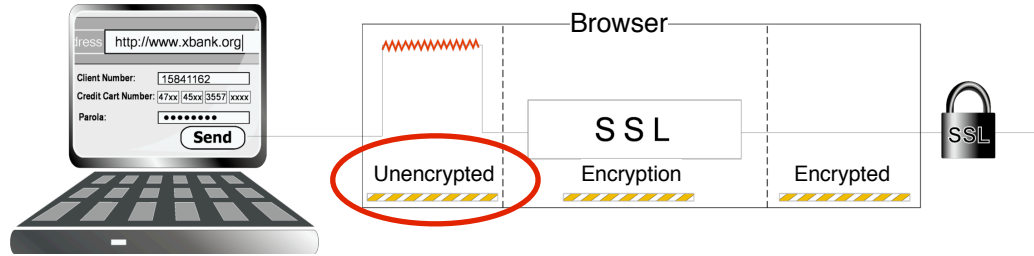
Screen Capture Protection	Custom Exploit Code
Webcam Capture Protection	Custom Rules
Clipboard Capture Protection	Malicious Shutdown of processes
SSL Logging Protection	Interception of firmware updates
Sound Recording Protection	Interaction of System Calls and Hooking with Operating System
ZWLST Bypass	Reverse Engineering of Binaries
System Defense	Certificate Validation
Supervisory Bypasses	Man-In-The Middle Attacks (MITM)
Hooking of internal APIs	Architectural Risk Analysis and Threat Modeling
Source Code and Design Document Review	Device Driver Analysis - AntiLog32.sys – Virtual Drive Mappings

Outcome: Passed | Date: February 2012

Copyright Software Security Consultants LLC
www.softwaresecurityconsultants.com

SSL Vulnerabilities

Secure Sockets Layer (SSL) has become the gold standard in data protection, used widely to secure financial transactions and sensitive data. While the 128 bit data encryption safeguards information during its transmission over the internet, severe vulnerabilities exist at user level. Advanced modern-day malware is able to capture sensitive information directly from the user's system, before encryption takes place.



Man-in-the-Middle or Man-in-the-Browser Attacks

This particular SSL vulnerability is used in, among others, the most advanced Man-In-The-Middle and SSL Sniffer attacks. This seemingly narrow and isolated weak spot allows financial malware a wide range of opportunities. Some forms of malware insert additional fields (such as PIN, full credit card number, etc.) during user login in order to gain access to the information, while more advanced forms are able to divert bank transfers executed by users to third party bank accounts, change the amount of the transfer and then even change the remaining balance the user will see after the transaction so they remain undetected. This is exactly the vulnerability used by advanced financial malware, like Zeus and SpyEye.

Zemana's unique SSL Logger Protection Module is able to detect such attempts at system process level, effectively intercepting and stopping malicious actions.

Encryption and Browser Lockdown v/s Process Management

Protection against data stealing malware has been traditionally associated with various forms of encryption or browser lockdown methods. Our approach is conceptually different. Compared to the Browser Lockdown approach and the vast majority of encryption solutions, the AntiLogger is system based and application (including browser) independent. It also adds a number of additional protection layers, covering all locations that may be used to steal users' data or invade their privacy.

By relying on malware action for detection, as opposed to merely making the information illegible, the AntiLogger is more resilient against targeted attacks, which may be able to break the encryption algorithms or gain access to data before encryption takes place. The MRG Effitas Online Banking Security Test proves this, showing that arguably the most widely spread keystroke encryption software fails to stop the simulator from gaining access to the account credentials.

Online Banking Security Test

Test by: MRG Effitas Ltd

Simulator: Zero-day financial malware mimicking the methods used by Zeus

Methodology: Attempt to capture PayPal® account credentials (SSL environment)

AVG Internet Security	✗
Kaspersky Internet Security	✗
MacAfee Internet Security	✗
Norton 360	✗
Zone Alarm Internet Security	✗
Acronis Internet Security Suite	✗
Agnium Outpost Security Suite	✗
BitDefender Internet Security	✗
Bluepoint Security	✗
BullGuard Internet Security	✗
ESET Smart Security	✗
F-Secure Internet Security	✗
G-Data Internet Security	✗
Norman Security Suite	✗
Panda Internet Security	✗
Symantec Endpoint Protection	✗
Trend Micro Internet Security	✗
Webroot Internet Security Essentials	✗
PrevX (Currently part of Webroot)	✓
Key Scrambler by QFX Software	✗
Zemana AntiLogger	✓

Copyright MRG Effitas Ltd.

Contact Zemana Today

sales@zemana.com

US Toll Free +1.866.293.2016

www.zemana.com

References and Further Materials

Full MRG Effitas Online Banking Security Test report can be downloaded [here](#)
 BBC Click feature and test on Man-in-the-Middle attacks can be viewed [here](#)

