

BANKING SECURITY MAGAZINE

VOL.1 NO.1 ISSUE 1/2011(4)

Mobile & Internet Banking

A phishing Primer

Malicious codes Zeust



**How Blackberry
is being choked**

Mob and Webbanking

Modern phone frauds

Dear Readers,

I have got the honour to announce our following project called Online Banking Security Magazine. It is the new vision how we could provide the information in terms of IT security systems in banks and other financial institutions. We are hoping that it will meet your all expectations.

It is specially dedicated to people from IT and financial departments to improve their knowledge and give them the easy access to the interesting and up to date stuff. I am deeply convinced that you will find many useful things that you desire to have.

The monthly access to the portal and its content (regular issues, six special editions in the year, archival issues, white papers and other publications) costs you 15\$.

I had a pleasure to collaborate with many experts in this field, who create things with passion and full commitment to the case. Moreover they believe that information belongs to the masses. Everyone has got the right to know what it is going on and through the publications they are able to start off to share knowledge and make it more available to the society.

I would like to recommend you especially the articles written by David Harley and HongSun Kim. The first explains what „phishing” really is, how works and what kind of damages provides. The second one focuses on how malicious codes especially Zeus - what it does and how proactive fraud management will keep you safe from those malware attacks.

Furthermore in this issue you will find a huge arrange of other essential articles like “The Security of Over the wire banking”, “How Blackbery is being choked by the government” or “Attacks, Securing & Impacts on Mobile & Internet Banking”. It is worth reading them!

I hope that our work will be appreciated and reading will be associated only with the pleasure.

Regards
Anna Nowak

BANKING SECURITY MAGAZINE

Managing:

Grzegorz Tabaka
grzegorz.tabaka@software.com.pl

Anna Nowak
anna.nowak@software.com.pl

Senior Consultant/Publisher:

Paweł Marciniak
Editor in Chief:
Katarzyna Chauca Grzesik
k.chauca@software.com.pl

Art Director:

Marcin Ziółkowski
Graphics & Design Studio
www.gdstudio.pl

DTP: Marcin Ziółkowski
Graphics & Design Studio, www.gdstudio.pl

Production Director:
Andrzej Kuca
andrzej.kuca@software.com.pl

Marketing Director:
Grzegorz Tabaka
grzegorz.tabaka@software.com.pl
Anna Nowak
anna.nowak@software.com.pl

Publisher: Software Press Sp. z o.o. SK
02-682 Warszawa, ul. Bokserska 1
Phone: 1 917 338 3631
www.hakin9.org/en

Whilst every effort has been made to ensure the high quality of the magazine, the editors make no warranty, express or implied, concerning the results of content usage.

All trade marks presented in the magazine were used only for informative purposes.

All rights to trade marks presented in the magazine are reserved by the companies which own them.

To create graphs and diagrams we used program by Mathematical formulas created by Design Science MathType™

DISCLAIMER!

The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

Content issue 01/2011

■ **A CLOSE LOOK AT THE MOST EVOLVED SECURITY THREAT TO THE ONLINE BANKING: AND ITS COUNTERMEASURE**

■ **THE REAL COST OF POOR SECURITY MANAGEMENT**

■ **THE COMPLEAT ANGLER – A PHISHING PRIMER**

■ **„MONEY OVER THE BITS N BYTES”**

■ **HOW BLACKBERRY IS BEING CHOKED BY THE GOVERMENT AND HOW VARIOUS OTHER MOBILE AS WELL**

AS PC CHAT CLIENTS LIKE SKYPE, GTALK – COULD BE BOTH DANGEROUS AND HELPFUL AT TIMES.

■ **ARE THE CON ARTISTS BACK? A PRELIMINARY ANALYSIS OF MODERN PHONE FRAUDS.**

■ **ATTACKS, SECURING & IMPACTS ON MOBILE & INTERNET BANKING.**

and much more



A Close Look at The Most Evolved Security Threat to the Online Banking:

And Its Countermeasure

Malicious codes are constantly trying to intercept online banking account information and various types of personal information for criminal purposes, and Zeus is a one-of-the-kind example of malicious codes.

In this article, we will take a closer look at the infamous Zeus, what it does and how proactive fraud management will keep you safe from those malware attacks.

A Look at Zeus

Zeus is committing financial crimes of an astronomical scale throughout the world, and the steadily updated versions of Zeus are being used for cybercrimes. Zeus Kit is a typical BotNet generating Kit, which was probably first developed in 2007 in Russia. The Bot created by the Zeus Kit is called ZBot or Zeus bot, and it has become the most notorious criminal software in the world since the online banking crimes committed by using Zeus in northern Europe in late 2009.

Zeus consists of following two components: Zeus Builder and Zeus Admin.

– Zeus Builder

Zeus Builder is the tool creates Zeus bot. For each click of the Bot generation button, it creates different malicious codes with changed binary codes to avoid the conventional security solution. You can find the functions of Zeus bots that created by Zeus builder in Table. 1 and Pic.1

Table 1. File name and functions

Files	Major function
sdra64.exe	Executing Zeus bot
local.ds	Saves stolen information from victims
user.ds	Sets target website lists

– Zeus Admin

Zeus admin is a web dashboard page of Zeus C&C(Command and Control) server. It manages Zeus-infected PCs and monitors the status of botnets including collected information from victims. (See Pic. 2)

Zeus bot delivers many malicious functions including:

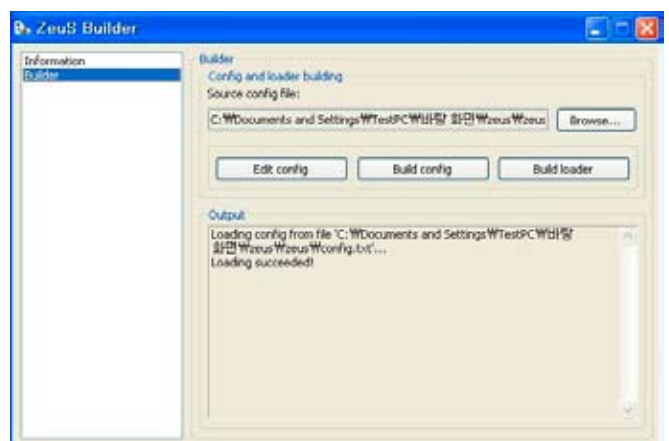
- **Collecting system configuration data:** It collects system configuration data including Zeus Bot information, version of OS and language, location and time zone, IP address and the name of running process from infected PCs, and send them to C&C server.
- **Collecting transaction and personal information:** When victims access to any URLs in the list in user.ds file,

Zeus steals every inputted data to C&C server. This is the main function of Zeus which brings lots of financial damage to victims who use online banking. Zeus uses two methods to steal the information, API hooking and screen capture. API hooking is to steal the data from web browser to server and later one is for those who use virtual keyboard.

- **Web Injection:** As the banks strengthen the security against keylogging and network-sniffing attacks, Zeus uses HTML injection to avoid it. For example, you can see how simply they can modify the webpage to steal the social security numbers(or any information the attacker want to know) in Pic.3 and 4. Of course, the snatched information goes to attacker's C&C server.
- **Additional functions:** Zeus also can deliver other malicious orders from attacker through C&C server including reboot and/or shutdown of PC, deletion of system file, accepting/denial of access to specific URL, download and running of specific file, search and transmission of file/folder in infected PC, updating Zeus configuration file, modifying the file name of Zeus bot.

How It spread and its increasing menace

To infect the PC, attackers send phishing or spam emails to the targets of their attacks. Zeus mainly spreads via these spam mails. Secondly, Zeus also can be injected into any websites and hence, users can be infected by visiting and clicking links in the malicious



Pic. 1. UI of Zeus Builder

web page. Last but not least, the shortened URLs (which lead the users to malicious website) through SNS, such as Twitter and Facebook is emerging method to spread it.

We should also be aware that ZeuS is targeting various browsers and it also works in the mobile environment. Not just the Internet Explorer but the Firefox is also the target of ZeuS attacks. ZeuS remote-controls the victim's PCs and instructs the infected PCs to transmit money, steal accounts information, launch HTML attacks, or forge or modify transactions. Furthermore, they are recently expanding their arena of crimes to include the mobile environment. Recently major media delivered that Blackberry OS faces fresh threats from the Trojan ZeuS. Prior to this, a Symbian OS was also attacked in October 2010. As financial transactions on smart phones increase, it is quite probable that ZeuS attacks will expand their arena to the smart phone field. This is something that definitely calls for our attention.

Why is ZeuS called the most malicious of the existing malwares? Many experts point out that it is the most optimized, yet the most generalized hacking tool since the developers of Zeus have implemented all the latest complex hacking technologies which enable them to attack exactly the way they wish. At the same time, ZeuS offers a user interface that anybody can use very easily. What is even more terrifying is that a Bot created by using the ZeuS Kit not only can set up various types of targets to be attacked but it can change binary code of the bot with a single click of the Bot generation button to avoid the conventional security solution and successfully carries out the attacks programmed by the makers of malicious codes.

Moreover, the price of ZeuS Kit is on the rise because it is constantly being updated, and it can be purchased easily through the black market. The latest version of ZeuS Kit is 1.3.4.x at the time

of this writing, and it is known to be sold and bought in the underground world at the price of 3,000 ~ 4,000 dollars. At additional payment, modules are available that have various expansion functions. It also offers regular technical support and updates just like a normal software.

Security Service Providers Agonize Over Lack of Counter-measures

As explained earlier, ZeuS is composed of neat packages capable of processing, modifying and producing spywares as intended by malicious hackers. It is relatively simple to obtain a ZeuS online. It is even possible to breed a new modified ZeuS-Bot at every click of the ZeuS package builder. For these reasons, ZeuS is very popular among malicious hackers. For lack of appropriate countermeasures against the exponentially breeding ZeuS variants, globally famous anti-virus vendors are updating their engines by analyzing ZeuS variants that are steadily being collected. Anti-virus vendors are also tracking down the ZeuS C&C servers to block connections to the criminal servers. Despite the all-out efforts to prevent cyber crimes, however, only 40.2% of hacking attempts are being detected according to the statistics of a certain website (<http://zeus-tracker.abuse.ch>).

Especially, like mentioned earlier, the traditional Anti-virus vendors are highly limited in protecting against ZeuS that is stealing information from the browser before encryption. It is more desirable to secure entire of banking transaction for fundamental protection, rather than relying on the old-fashioned detection & destroy methodology offered by many anti-virus vendors.

New concept in Online Banking Security

Rather than relying on conventional methods offered by traditional Anti-virus vendors, experts cite a critical need for security providers specializing exclusively in online banking to assume the lead role in the war against ZeuS. One such company effectively combating ZeuS is Seoul based, AhnLab through its AhnLab Online Security (AOS) solution.

AOS is a security solution that protects the entire transaction processes with a thorough understanding of all the trends in hacking. The biggest advantage of AOS as a security solution is that it harmoniously combines a variety of advanced security technologies. AOS consists of a dedicated security browser, an Anti-keylogger, and a network invasion blocker. Getting at the root of ZeuS's principal behaviors, AOS blocks variants of ZeuS that have not yet been collected as well as new born variants.



Fig. 2. UI of Zeus Admin



Fig. 3. The example of HTML injection by Zeus



Fig. 4. The result of HTML injection by Zeus

First, AOS Firewall blocks the actions of all detectable ZeuS. Then, AOS Secure Browser and AOS Anti-keylogger defend the system against the capture of the web page log-in information, HTML injection, and screen capture. The AOS is outstanding not only in its performance but it is also supported by an excellent infrastructure. The AhnLab Security E-response Center (ASEC), a global organization dedicated to countermeasures against malicious codes, is full speed ahead in analyzing ZeuS and other malwares. In addition, the Security Operation Center (SOC) run by AhnLab is providing fast countermeasures by collecting information on real time attacks and/or threats so that clients do not receive any damages from malware attacks.

For individual users: Top 5 Questions Consumers Should Ask

In the age of online banking, consumers should play every bit as close attention to a bank's online security as its savings and CD interest rates. Before choosing a certain bank, be sure to visit its

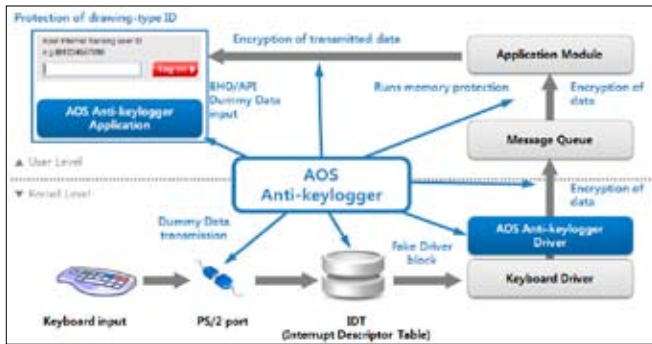


Figure 1. AOS Anti-key logger protects every stage of the transaction carried out during keyboard input (PS/2 illustrated)

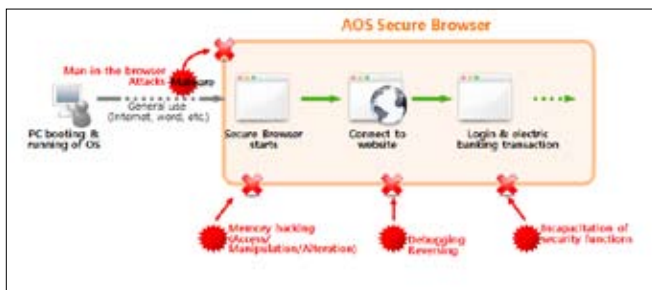


Figure 2. AOS Secure Browser wards off hacking and MITB applying the anti-hacking browser service

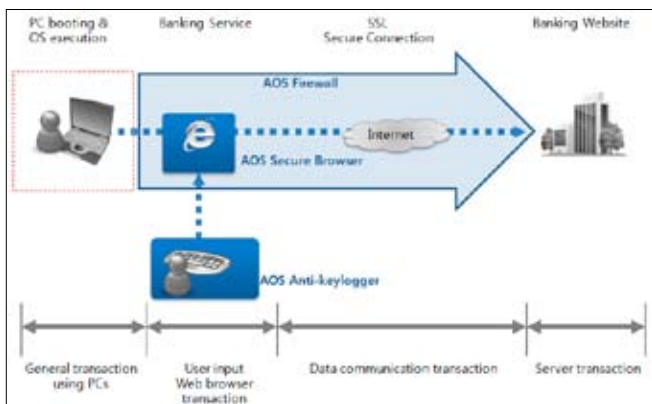


Figure 3. AOS secures a safe and reliable electronic financial transaction environment

internet website and talk to a representative about the protections a bank has in place. Although every major bank offers some degree of security, the level of protection widely varies. Here are the Top 5 Questions consumers need to be asking their banks:

- 1) What security does the bank have in place to protect online banking users?
- 2) What specifically is the bank doing to protect against complex malicious threats like Zeus?
- 3) Has the bank been victim to any online thefts recently? What was done to correct the security breaches?
- 4) Is the bank's solution to protect online banking easy to use?
- 5) Does the bank have up-to-date online banking protection?

Conclusion

Trust and safety are the topmost items on the priority list for providers of financial services who manage client assets. Damages inflicted by Zeus have a devastating influence on banks and other financial service providers both in terms of reputation and financial liability. In the era of Zeus, financial service providers need to seriously consider installing an online transaction security solution such

as AOS (AhnLab Online Security), and consumers to ensure they choose banks that are well protected.



**HONGSUN KIM
CHIEF EXECUTIVE OFFICER,
AHLAB, INC.**

Hongsun Kim is CEO of AhnLab, leading provider of integrated security solutions since August, 2008. With his over 20 years of experience in IT networking and security expertise, is responsible for building AhnLab's presence, driving business and providing future direction to the company.

Prior to joining AhnLab, as the Founder & CEO, he spent 9 years in SecureSoft, where he held management roles in overall business and product management. He joined AhnLab in 2007 as the CTO & Vice President as AhnLab acquires network security business from SecureSoft. Since joining AhnLab, he helped to define AhnLab's strategy for security and other security-related technologies.

He also serves as the member of Ministry of Knowledge Economy IT industry Policy Advisory Committee, IT industry advisor of National Informatization Council and National Economic Advisory Council.

Hongsun Kim holds a Ph.D. in computer science from Purdue University in United States and Master of Science from Graduate School of Engineering, Seoul University in Korea.

Career path

- Chief Executive Officer, AhnLab, Inc. (2008.08~Present)
- CTO & Vice President, AhnLab, Inc. (2007.1~2008.7)
- The management counselor at Unipoint (2005~2006)
- Founder & CEO, SecureSoft (1996~2004)
- Vice President, Business Development at TSI (1994~1996)
- Researcher at Texas State University (1990)
- Senior researcher, Computer Business Unit at Samsung Electronics (1990~1994)

Activities

- 2010. 03 - Presence The member of National Economic Advisory Council
- 2010. 03 - Presence The member of MKE(Ministry of Knowledge Economy) IT industry Policy Advisory Committee
- 2010. 01 - Presence IT industry advisor of National Informatization Council
- Vice president of KISIA(The Knowledge Information Security Industry Association) / Vice president of Korea Information Processing Society / Vice president of Korea Software Property-right Council
- Co-founder & chairman of KISIA (The Knowledge Information Security Industry Association) / vice-chairman of Korea Internet Corporations Association / the member of board of directors of Korea Venture Business Association
- Adjunct professor of Korea Univ., Hanyang Univ., and Kangwon Univ.

Educations

- 1990 Earned Ph.D. in computer science from Purdue University
- 1985 Earned Master of Science from Graduate School of Engineering, Seoul Univ.
- 1983 Earned Bachelor of Science from Department of Electrical Engineering Seoul National Univ.

Awards

- 2010 The Best Science and technology Award from Ministry of Education, Science and Technology
- 2009 Received presidential citation
- 2009 Grand Prize for Korea Internet Award
- 2003 Outstanding Electrical and Computer Engineer Award from Purdue Univ.
- 1999 Received Industrial Service Medal, Cultural Awards from Jung-Jinki Culture Foundation