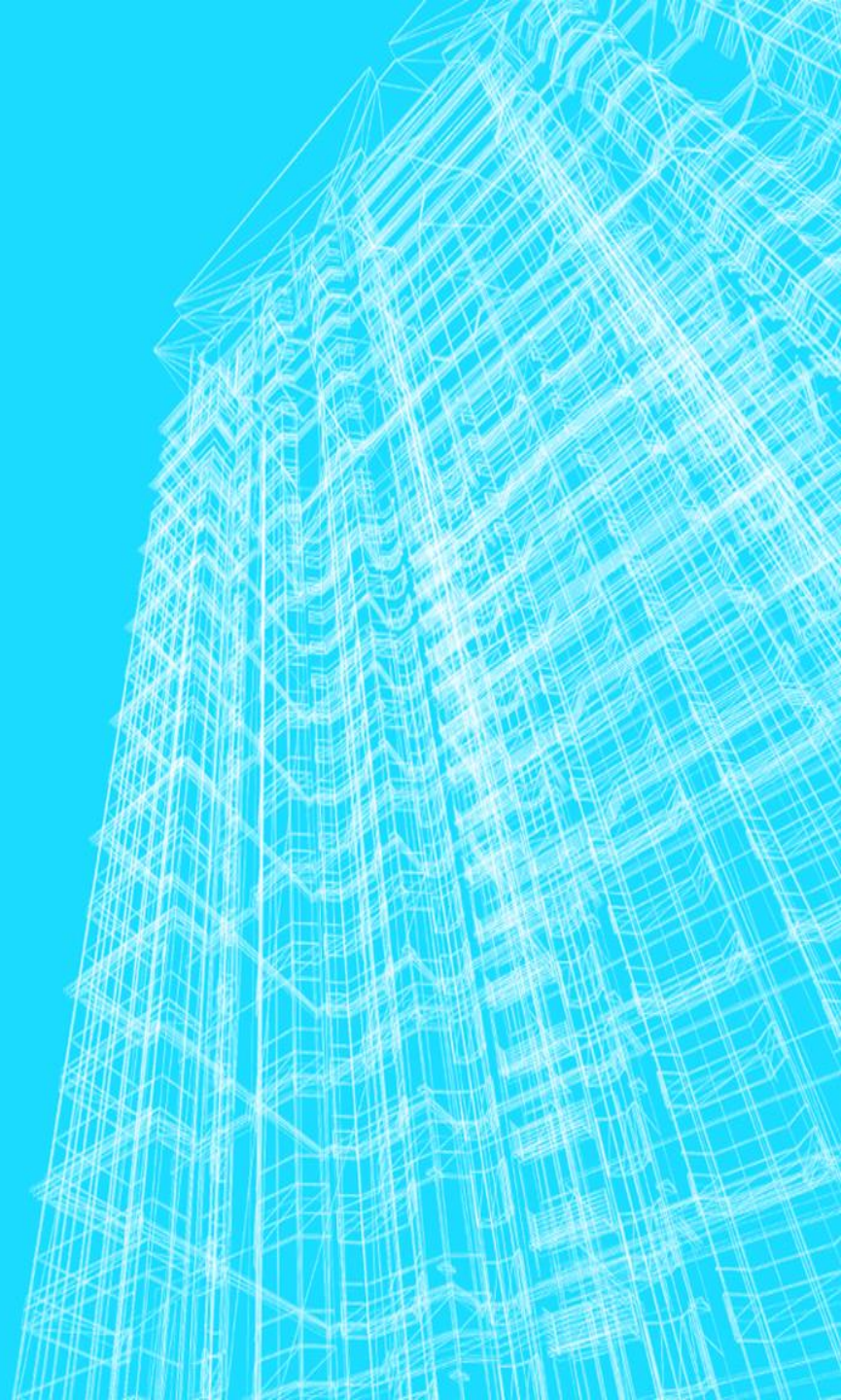
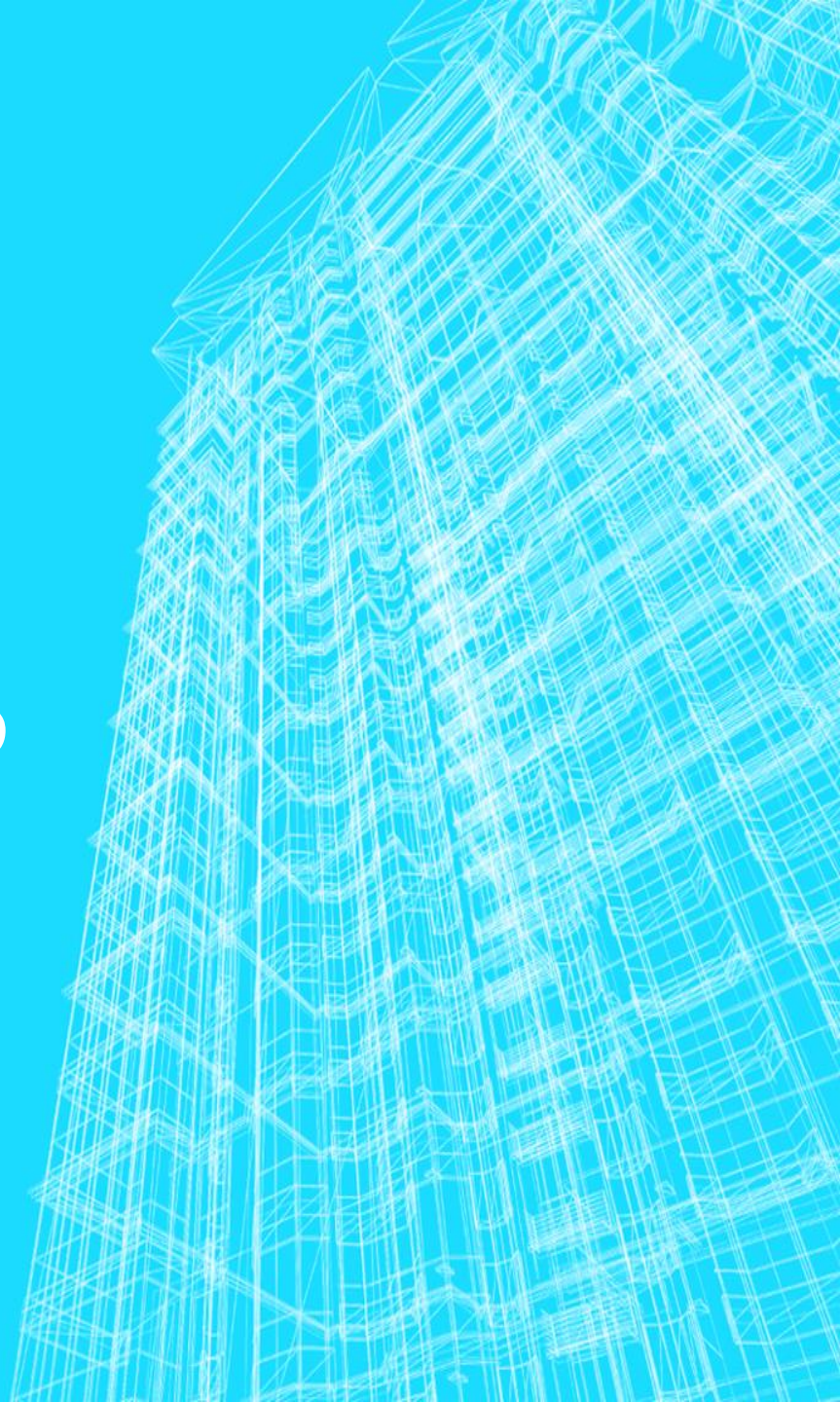
ZEUS'S FORENSIC ANALYSIS

Trojan Horse that cost USD 70 Million

Syndicate:
Capt Salman Akram
NC Muhammad Umar Farooq



GETTING TO KNOW SOME BASIC TERMS



FORENSIC ANALYSIS

- Forensic science (often shortened to forensics) is the application of a broad spectrum of sciences to answer questions of interest to a legal system. This may be in relation to a **crime** or a civil action

MALWARE

- Software that is intended to damage or disable computers and computer systems.

TROJAN HORSE

- A **Trojan horse**, or **Trojan**, is a non-self-replicating type of malware which appears to perform a desirable function but instead drops a malicious payload, often including a backdoor allowing unauthorized access to the target's computer.
- Trojan horses may steal information, or harm their host computer systems.
- Trojan horses employ a form of "social engineering," presenting themselves as harmless, useful gifts, in order to persuade victims to install them on their computers.

POPULARITY

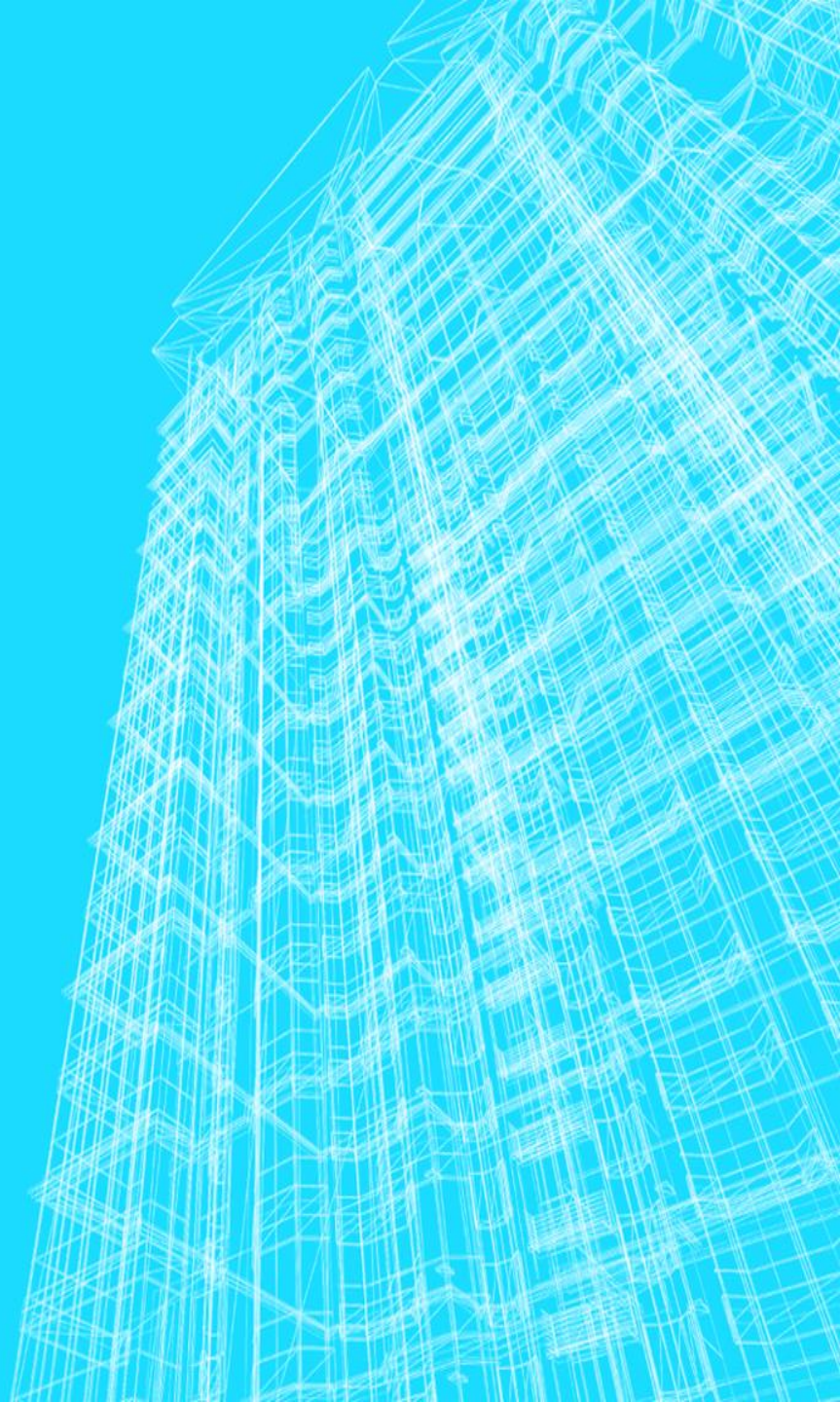
- According to BitDefender, "Trojan-type malware is on the rise, accounting for 83-percent of the global malware detected in the world.“
- One of the most popularly known Trojan is “Zeus”.

BOTNET

- A **botnet** is a collection of internet-connected programs communicating with other similar programs in order to perform tasks.

ZEUS IN GENERAL

Made way to FBI wanted list



INTRODUCTION

- The Zbot, is a Trojan horse used to infect computers and steal confidential information.
- It tricks people into downloading its malware by sending emails posing as real websites or organizations, such as MySpace, Facebook.
- From there, it prompts people to visit a website to enter in confidential information, where the malware installs and infects the computer.
- **Zeus** steals banking information by Man-in-the-browser, keystroke logging and Form Grabbing.

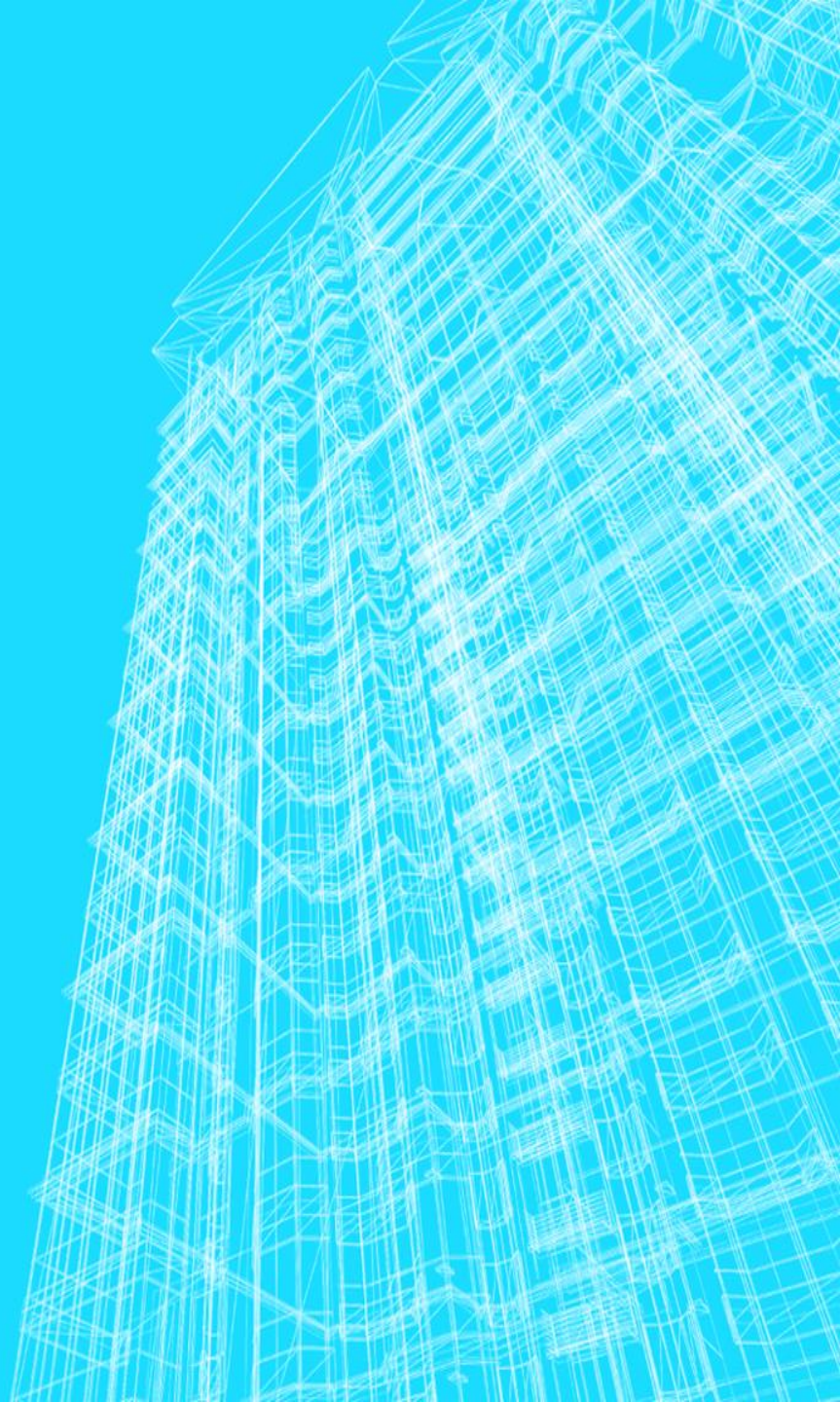
ORIGIN

- The Zeus bot originated in a Russian-speaking country
- The bot's help files and major code are written in Russian.
- The total amount of variants exceeds 40,000 including sophisticated peer to peer versions.

VICTIMS

- Bank of America, NASA, Monster.com, ABC, Oracle, Play.com, Cisco,Amazon, and *BusinessWeek*.

FUNCTION



FUNCTION

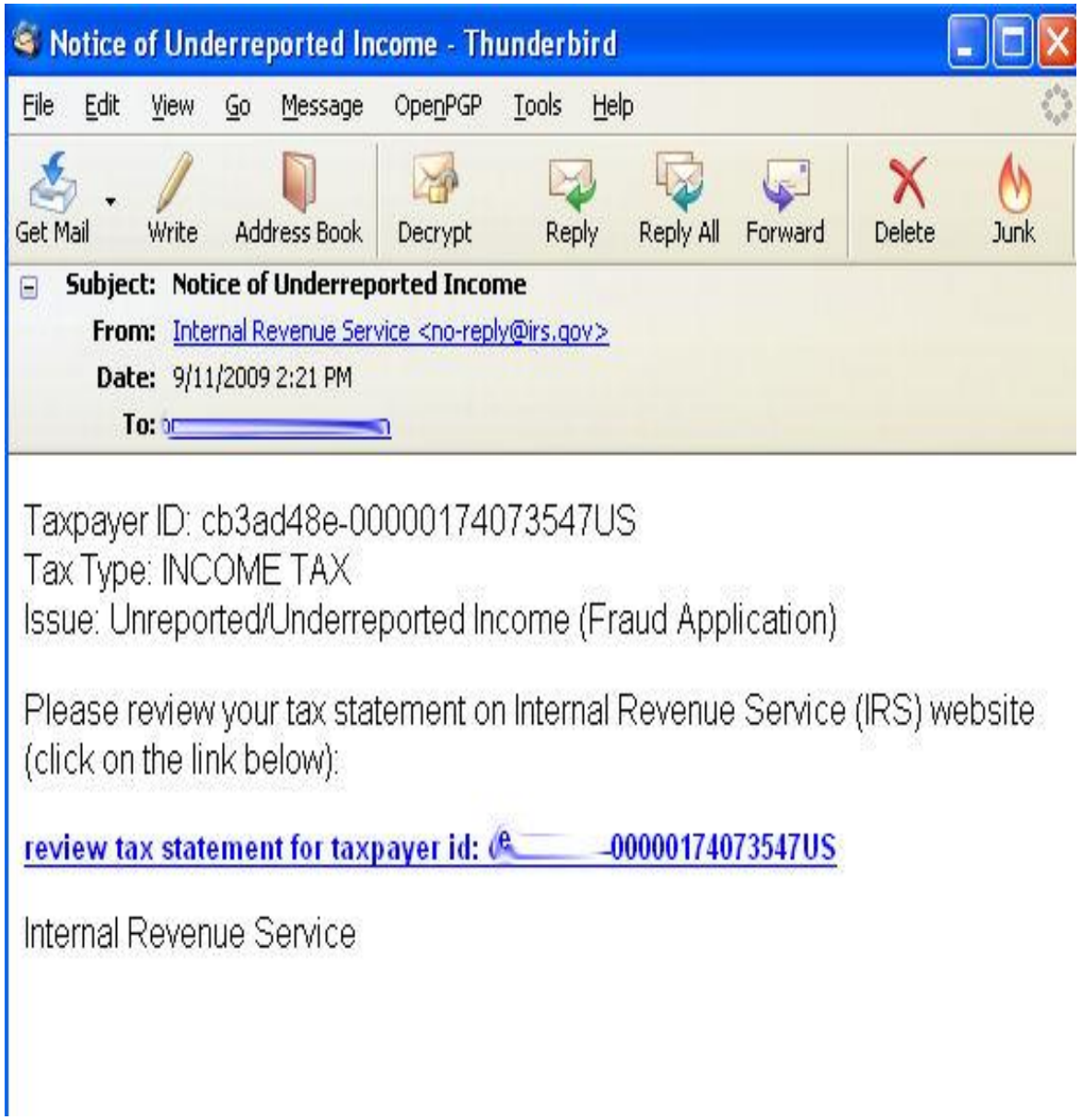
- The Zeus bot is used to gather banking information, personal online information and personal computer information.
- For example, the bot can gather passwords stored by Internet Explorer, which allows hackers to use the information to access personal accounts, such as online banking accounts.
- It can also collect personal information entered in websites.

TARGET

- The Zeus bot targets Windows operating systems, ranging from Windows NT to Windows Vista.
- According to a 2009 Symnatec.com graph, it primarily attacks computers located in the United States, most of Europe, India, Japan, China and Australia.
- In the United States, the bot primarily attacks computer in major cities, such as New York City, Los Angeles and Houston.
- In Europe, more clusters are gathered around northern mainland Europe.

DISTRIBUTION

- According to Symnatec.com, hackers can create this Trojan with a Trojan-building toolkit that can costs upwards of $700.
- These kits are available in marketplaces and secret forums that distribute content to Internet-based criminals.
- The hackers then spread the Trojan through spam campaigns by sending phishing emails to email accounts.

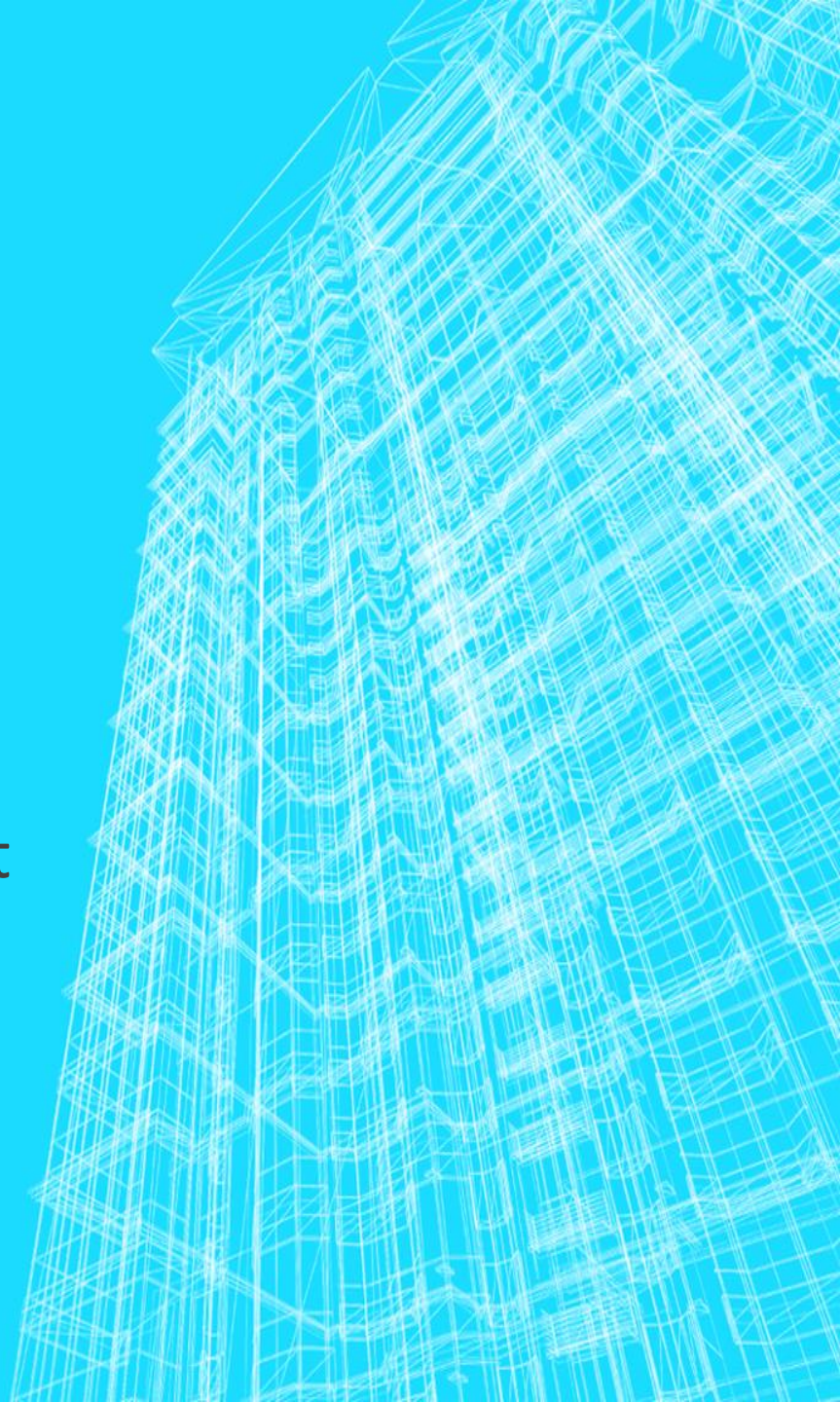

Notice of Underreported Income - Thunderbird
File Edit View Go Message OpenPGP Tools Help
Get Mail Write Address Book Decrypt Reply Reply All Forward Delete Junk
Subject: Notice of Underreported Income
From: Internal Revenue Service <no-reply@irs.gov>
Date: 9/11/2009 2:21 PM
To:
Taxpayer ID: cb3ad48e-00000174073547US
Tax Type: INCOME TAX
Issue: Unreported/Underreported Income (Fraud Application)
Please review your tax statement on Internal Revenue Service (IRS) website (click on the link below):
review tax statement for taxpayer id: -00000174073547US
Internal Revenue Service

PREVENTING

- To avoid getting the Zeus bot, you should not open any links in emails that ask you to enter your personal information, such as their password.
- Also avoid clicking on any email or instant messenger links containing an .exe file, which can contain malicious code.
- Links leading to .pdf, .swf or .ppt files can also contain malware.
- Anti-virus programs can also prevent these bots from installing.

ZEUS FOR EXPERTS

Largest BOTNET on the internet



ALIASES

- Zeus (other)
- Wsnpoem (Symantec)
- Citadel (other)

ALERT LEVEL

Severe

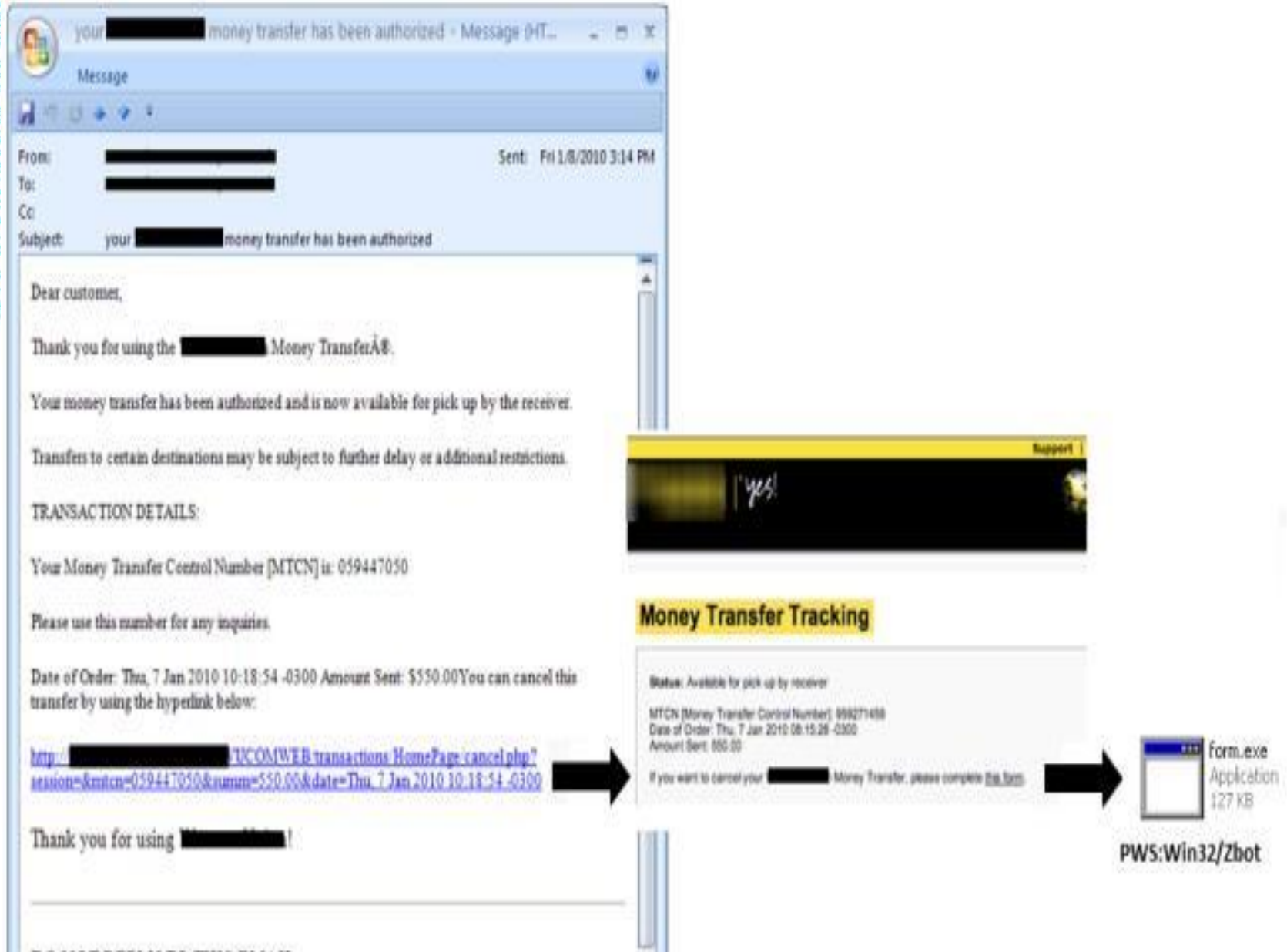
SYMPTOMS

- The presence of the following files:
  - *<system folder>\ntos.exe*
  - *<system folder>\sdra64.exe*
  - *<system folder>\twex.exe*
  - *<system folder>\wsnpoem\audio.dll*
  - *<system folder>\wsnpoem\video.dll*
  - *<system folder>\twain_32\user.ds*
  - *<system folder>\lowsec\local.ds*
  - *<system folder>\lowsec\user.ds*
- The following programs may stop running for no obvious reason:
  - Outpost Firewall - *outpost.exe ;* Zone Alarm Firewall - *zlclient.exe*

TYPICAL SPAM EMAIL

- Subject: *<Courier name> Failure Delivery Notification Message*
  Attachment: *SN_122010.zip*
- Subject: *<Social network site> Password Reset Confirmation*
  Attachment: *<Social network site>_Password_e9081.zip*
- Subject: *<Software company> Software Critical Upgrade Notification ID: RA4NFDKPJBD*
  Attachment: *<Software company>Systems-Software_CriticalUpdate_Dec_2011-6PGCF713B.zip*
- Subject: *Important Account Information from <Company name> TRACK-ID: 70341011278*
  Attachment: *<Company name>-Account-Status-Notification-Dec-2011.exe*
- Subject: *Your credit balance is over its limits.*
  Attachment: *balancechecker.zip*

PHISHING


your [redacted] money transfer has been authorized - Message (HT...
Message
From: [redacted]
Sent: Fri 1/8/2010 3:14 PM
To: [redacted]
Cc:
Subject: your [redacted] money transfer has been authorized
Dear customer,
Thank you for using the [redacted] Money TransferÂ®.
Your money transfer has been authorized and is now available for pick up by the receiver.
Transfers to certain destinations may be subject to further delay or additional restrictions.
TRANSACTION DETAILS:
Your Money Transfer Control Number [MTCN] is: 059447050
Please use this number for any inquiries.
Date of Order: Thu, 7 Jan 2010 10:18:54 -0300 Amount Sent: $550.00You can cancel this transfer by using the hyperlink below:
http:// [redacted] /ICOM/WEB/transactions/HomePage/cancel.php?session=&mtcn=059447050&sumne=550.00&date=Thu, 7 Jan 2010 10:18:54 -0300
Thank you for using [redacted]!
Support
yes!
Money Transfer Tracking
Status: Available for pick up by receiver
MTCN [Money Transfer Control Number]: 059271458
Date of Order: Thu, 7 Jan 2010 08:15:28 -0300
Amount Sent: 850.00
If you want to cancel your [redacted] Money Transfer, please complete the form
form.exe
Application
127 KB
PWS:Win32/Zbot

REMOTE DESKTOP SERVICE

- If your computer is using Remote Desktop Service (RDS), and connected to other computers, Zbot may attempt to install itself on your computer through this channel.
- If your computer is running a Remote Desktop Service, Zbot may attempt to run a process for every connected RDS session and create a copy of itself in the startup folder:
- *%RDSUserProfilePath%\Start Menu\Programs\Startup\<random letters>.exe* where *%RDSUserProfilePath%* is generated by enumerating each user in this registry key using the user's unique security identifier (SID) .
- In subkey:
  HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ProfileList
  Sets value: *ProfileImagePath*

AN EXAMPLE WITH RDS

- If the administrator account SID is: S-1-5-21-1844237615-2111687655-839522115-500
- Then profile path will be: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-1844237615-2111687655-839522115-500
- If ProfileImagePath is: %SystemDrive%\Documents and Settings\Administrator
- Then the full drop file will be: C:\Documents and Settings\Administrator\Programs\Startup\<random letters>.exe
- This means that, as the affected computer is remotely connected to other computers, they risk being infected as well.

INSTALLATION

- Earlier versions of PWS:Win32/Zbot have been observed dropping copies of itself as any of the following files:
  - *<system folder>**ntos.exe*
  - *<system folder>**sdra64.exe*
  - *<system folder>**twex.exe*
- It also drops the following files, containing encrypted data used by the trojan, to the folder "*<system folder>**wsnpoem*\":
  - *audio.dll*
  - *video.dll*
- It also creates either of the following encrypted log files, in which it may store the stolen data:
  - *<system folder>**twain_32**user.ds*
  - *<system folder>**lowsec**user.ds*

INSTALLATION

- Zbot modifies the registry to ensure that its copy is executed at each Windows start:
- In subkey:
  HKLM\Software\Microsoft\WindowsNT\Currentversion\Winlogon
  Sets value: "*userinit*"
  With data: *"<system folder>\userinit.exe,<system folder>\<malware file>“*
- *Some versions also copy at*
- *%APPDATA%\<random letters>\<random letters>.exe*

EXAMPLE INSTALLATION

- In subkey:
  HKCU\Software\Microsoft\Windows\Currentversion\Run
  Sets value: *"{GUID of Windows volume}"*
  With data: "*%APPDATA%*\<*random letters*>\<*random letters*>.*exe*"

- Specifically
  - In subkey: *HKCU\Software\Microsoft\Windows\Currentversion\Run*
    Sets value: *{449829B8-9322-5694-4C31-974E87EDDDA5}*
    With data: "*C:\Documents and Settings\Administrator\Application data\ecymy\huojq.exe*"
  - Newer variants may make the following modification for the same purpose:
  - In subkey: *HKCU\Software\Microsoft\Windows\Currentversion\Run*
    Sets value: <random letters>
    With data: "*%APPDATA%*\<*random letters*>\<*random letters*>.*exe*"

INJECTIONS

- Zbot injects code into the address space of all running processes, matching the privilege of the currently logged on user.
- Otherwise, the trojan will inject its code into all user-level processes (such as "*explorer.exe*", "*iexplore.exe*" and so on).
- This behavior is intended to hide the trojan behavior from security applications.
- It also hooks the following Windows system APIs to aid in the capture of sensitive data, for example, online banking and shopping, email credentials and network information:
- *NSPR.DLL , NTDLL.DLL, KERNEL32.DLL, WININET.DLL, WS2_32.DLL, GDI32.DLL, USER32.DLL, CRYPT32.DLL, SSLEAY32.DLL, SECUR32.DLL*

DISABLE FIREWALL

- Zbot makes the following changes to the registry in order to disable the Windows Firewall
- In subkey:
  HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile
  Modifies value: "*EnableFirewall*"
  With data: "*0*"

LOWERS BROWSER SECURITY

- Disables phishing filtering:
- In subkey: *HKCU\Software\Microsoft\Internet Explorer\PhishingFilter*
  Sets value: "*Enabled*"
  With data: "*0*"
  Sets value: "*EnabledV8*"
  With data: "*0*"
- Prevents the removal of expired Internet Explorer browser cookies:
- In subkey: *HKCU\Software\Microsoft\Internet Explorer\Privacy*
  Sets value: "*CleanCookies*"
  With data: "*0”*

LOWERS ZONE SECURITY

- Lowers Internet Explorer Internet zone security settings:

  (all values set to “0”)

- In subkey: *HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0*
  Set value: "*1609*” With data: "*0*"

- In subkey: *HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1*
  Sets value: "*1406*"

- In subkey: *HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2*
  Sets value: "*1609*"

- In subkey: *HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3*
  Sets value: "*1406*"

- In subkey: *HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4*
  Sets value: "*1406*"

REMOTE ACCESS

- Zbot allows varying degrees of remote access and control, depending on the information in the configuration data in each particular variant. The trojan could perform, but is not limited to, any of the following actions:
- *Reboot/shut down your computer, Uninstall Zbot, Update Zbot and its configuration file, Search and remove files and directories, Log you off your computer, Run a program, Steal or delete Internet Explorer cookies, Steal or delete certificates, Block or unblock URLs, Change the Internet Explorer homepage, Steal your FTP credentials, Steal your email login credentials, Steal your Flash Player credentials.*

CONFIGURATION FILE

- Zbot download a configuration file from a remote server that determines how the trojan will behave.
- The trojan may generate up to 1020 pseudo-randomly named domains, and attempt connections with the generated list to download a configuration file. The generated domain names are based on the system date and time and have one of the following suffixes:
- *Biz, com, info, net, org, ru*
- *E.g. rvowslrmvnfkblkfyttpfemwx.com*

DATA IN CONFIG FILE

- The configuration file contains data used by the malware such as the following:
- Locations form which to download updates for Zbot
- Locations from which to download additional data files
- The version of the malware
- Online financial institutions to target
- HTML and JavaScript code for performing its data stealing payload

INFORMATION STOLEN

The trojan steals the following sensitive information from the affected computer:

- Digital certificates
- Internet Explorer and Firefox cookies
- Cached passwords
- Logged keystrokes
- Images of screen and window captures
- Passwords and other details (such as credit card numbers), as you enter them in to targeted websites

TARGET SITES AND SOFTWARES

The following are some of the target websites found in the configuration file of Zbot:

amazon.com
flickr.com
myspace.com
youtube.com
microsoft.com
facebook.com
feedback.ebay.com/ws/eBayISAPI.dll?ViewFeedback&
us.hsbc.com

The trojan collects FTP credentials (IP, port, user name, and passwords) from the following FTP software:

FlashFXP
Total Commander
ws_ftp
FileZilla
FAR/FAR2
winscp
FTP Commander
CoreFTP
SmartFTP

WINDOWS LIVE CREDENTIALS

- It also steals windows live and mail credentials. If the infected computer is running on Windows XP or below, Win32/Zbot uses COM libraries "*msoeacct.dll*" and "*wab32.dll*" to capture the following details:
- Windows mail account name, Email address, Server, User name, Password.
- The DLL files are searched in the directory defined in the registry key below:
- *HKLM\SOFTWARE\Microsoft\WAB\DLLPath*
- Otherwise, if running on Windows Vista and above, the trojan captures the credentials by parsing the Windows mail folder, specified in this registry subkey:
- *HKCU\SOFTWARE\Microsoft\Windows Mail\Store Root*

ZEUS PREVENTION AND RECOVERY

Source code of 11 Million bytes

PREVENTION

- Enable a firewall on your computer
- Get the latest computer updates for all your installed software
- Use up-to-date antivirus software
- Limit user privileges on the computer
- Use caution when opening attachments and accepting file transfers
- Use caution when clicking on links to webpages
- Avoid downloading pirated software
- Protect yourself against social engineering attacks
- Use strong passwords

RECOVERY

- Restoring your system registry (export from regedit.exe)
- Configuring Security Zone settings for Internet Explorer
- Enabling the Phishing Filter in Internet Explorer 7, 8 and 9
- Changing or choosing the default search provider

OR

RUN Microsoft Fix it
http://support.microsoft.com/mats/windows_security_diagnostic

THANKS FOR YOUR TIME

Questions .. ?