**TABLE OF CONTENTS**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION</td>
<td>3</td>
</tr>
<tr>
<td>I THINK I’VE SEEN THIS BEFORE...</td>
<td>4</td>
</tr>
<tr>
<td>WHY ZEUS? PARTNYORKA CONNECTIONS</td>
<td>6</td>
</tr>
<tr>
<td>PUTTING THE PIECES TOGETHER</td>
<td>7</td>
</tr>
<tr>
<td>CONCLUSION</td>
<td>8</td>
</tr>
<tr>
<td>SOURCES</td>
<td>9</td>
</tr>
</tbody>
</table>
INTRODUCTION

In August 2009, Trend Micro’s Threat Research Team started noticing a sudden spike in the activities of a new malware dubbed “BREDOLAB,” which was, apparently, related to the Zeus malware family.

The sudden rise in prominence could not have been random so we decided to follow the malware and trace its place of origin and objective. This document is a product of the research we conducted.

This document explores BREDOLAB’s inner workings, the economics behind the threat, and recommendations to mitigate its effects on home users and corporations.

Figure 1. BREDOLAB malware’s growth
BREDOLAB is a simple downloading platform programmed by cybercriminals to facilitate virus infections and their timely updates. When we began analyzing BREDOLAB, we immediately noted that upon infection, the first thing the malware did was execute a “call home” routine. The Web communication was encrypted so we could not read its contents. Subsequent connections followed albeit with significant differences, which made us think they were not directly related. The differences were substantial so we focused on understanding the first batch of Web connections.

We conducted an in-depth analysis and arrived at a very clear conclusion—that the initial Web connections were downloading a series of executable files. These were then run on victims’ machines. We were able to decrypt each of the malicious programs and keep a record to see what kinds of software BREDOLAB installed on infected PCs.

BREDOLAB has a particular noticeable trait—all the Web connections it made pointed to the same server, which was usually located in Russia. The host’s name was hard-coded into the BREDOLAB executable, indicating a weak point in the bad guys’ network infrastructure. So if the malicious server is taken down, none of the infected PCs would be able to continue downloading updates to the malware.

After monitoring this particular server for a few weeks, we noticed that it was eventually taken down. However, the BREDOLAB group owners was able to successfully move the server name to a different IP address, enabling it to very quickly become active from a different location. It is likely that this routine has been taking place for some time now.

Other BREDOLAB samples we have seen point to other servers, which may hold different malicious programs. The Russian server we monitored, for instance, uploaded the following binaries into infected systems:

1. **Rogue antivirus program called Antivirus Pro 2010.** This program’s graphical user interface (GUI) looks very professional, just like that of a real antivirus program. Once installed, it asks the victim to pay for an “unlicensed” copy of the software in order to clean nonexistent viruses from the machine.

![Figure 2. Unlicensed Antivirus Pro 2010 GUI](image-url)
Rogue antivirus applications always claim to have found viruses in an infected machine even though they never actually scan anything since they are not real. The name of a rogue antivirus program, in fact, changes every few weeks or months. This is a well-known scam.

2. **Zeus bot.** The second component that is always present in such an infection is the bot agent of a botnet dubbed “Zeus.” The Zeus botnet connects to a command and control (C&C) server through encrypted Web connections and gets further instructions for its information-stealing functionality. This includes monitoring and stealing banking credentials and other login data.

In our experience while monitoring the BredOlAB download server, we found that the executable files were always very similar. Though they might vary slightly every now and then, their general contents were pretty consistent.

While working with BredOlAB, we discovered that it had a strong similarity with Pushdo in the way it downloads and executes files. Pushdo is a downloader that also connects back home through a Web connection and downloads a series of executable files in one single encrypted chunk. This chunk is then split into smaller pieces that the Pushdo downloader runs by either direct execution or injecting the code into a Microsoft OS component—a technique shared by BredOlAB. Both Pushdo and BredOlAB decide between these two options by looking at a field that tells the downloader how the execution should take place.

Pushdo and BredOlAB both exhibit unusual behaviors, which led us to believe that they are probably products of the same programmer or development team. During our investigation of Pushdo, we found out that its authors were Russian and that their product primarily catered to the Russian spam market.

While searching some underground Russian sources, we were able to obtain the source code of the BredOlAB C&C backend server that served the encrypted executable files. As we suspected, all the comments were in Russian, which matched our expectations at this point.

**Установка**

```
1. Создать на хосте базу данных
4. Отредактировать файл main.php, основное внимание обратить на разд "Настройки путей" и "Подключение к СУБД", остальные настройки мож
5. Загрузить пакет с приложением по указанной в инструкции ссылке
6. Установить права доступа "777" (чтение/изменение/запись) на директори
   - /install/
   - /logs/
   - /logs/error.log
   - /templates_c/
```

**Figure 3. Read Me file of the BredOlAB C&C software installation**
WHY ZEUS? PARTNYORKA CONNECTIONS

So what is the exact relationship between BREDOLAB and the two programs it downloads? We started digging a bit more into the possible business relationships that exist among Russian underground organizations.

Things in the Russian underground are organized by affiliate program or partnyorka. Affiliate programs in both the commercial world and in the underground provide a means for Web vendors to create a network of business partners that help them out by redirecting traffic to their own servers. For instance, Some online pharmacy outfits in Russia that sell low-cost generic medicines made in lower-paying factories exclusively go to market online. One example of such a shady organization online-rx.biz has an affiliate program that earns affiliates 25% of each sale made. They even estimate that each customer’s average order is worth 130–160 euros so they only need to sell an average of 31 orders to make their first 1,150 euros.

Fake antivirus vendors have similar affiliate programs. The only difference is they do not sell anything, they just scam people. These vendors pay botnet owners sales commissions from the money scam victims dole out.

Following this logic, this particular BREDOLAB group seems to have partnered with a rogue antivirus company and uploads its software to every infected PC. This way, the group makes money every time a victim falls for the trick and pays for the “premium version” of a fake antivirus software.

The fact that different BREDOLAB versions download software from different servers just proves that its developers are selling their software (probably both client and server programs) as an additional source of income.

 Affiliate programs or partnyorka in both the commercial world and in the underground provide a means for Web vendors to create a network of business partners that help them out by redirecting traffic to their own servers.
PUTTING THE PIECES TOGETHER

When it comes to malware, especially those that originate from Russia, the impression is that it is all about business and making money. Bredolab is no exception. Keeping in mind the Russian underground economy and all of its affiliate programs, there seems to be at least two distinct groups of actors in this picture, namely:

1. **Vendors.** These refer to the creators of the scam. What they do may be borderline illegal or plainly criminal but they do not expose themselves much. They provide marketing tools and sales commissions to the second group.

2. **Enablers.** These try to expand the vendors’ businesses by exposing themselves in exchange for huge commissions.

In certain cases, there may be a third group of people—developers. These make the software sold in the underground market and facilitate the enablers.

Bredolab is a good example that shows how a criminal ecosystem works. Developed and maintained by a group of developers then sold to enablers, Bredolab furthers a vendor’s business by distributing fake antivirus software. Apart from that, this legitimate-looking malware also infects victims’ systems with a botnet agent to continue subverting users’ Internet connection for other nefarious ends. We can thus surmise that the same group behind our Bredolab samples is also establishing a Zeus botnet with a very concrete agenda—monetizing stolen data. This same group aims to get money from both techniques—fake antivirus pay-per-install and credential-stealing.

The same Russian group that developed Bredolab is quite likely behind a similar malware—pushdo. While Bredolab focuses more on its fake antivirus affiliation, Pushdo builds a spamming platform for criminal groups’ enablers. Both activities—spamming and forceful installation—known in the underground as “loads,” are complementary and work well toward the vendors’ objective of enriching their affiliates while making a lot of money in the process.

Although the Bredolab samples we analyzed came from spam campaigns, their enablers mainly infected victims via the Web. They infiltrated victims’ PCs by redirecting their browsers to malicious websites. This was usually done by either putting a malicious link in a legitimate page (e.g., posting malicious links in forums and guest books or hacking legitimate pages) or creating a page containing malicious links and making it score very high in search engines so that it appears as a top search result, a technique known as “blackhat search engine optimization (SEO).”
CONCLUSION

In order to avoid being hit by these shady organizations, users should ensure that they always have the latest versions of their antivirus software of choice running on their PCs. If possible, it is also worth considering using security software that makes you a part of a community-based network such as the Trend Micro Smart Protection Network™. Smart Protection Network combines unique Internet-based technologies with lightweight clients. By checking URLs, emails, and files against continuously updated and correlated threat databases in the cloud, customers always have immediate access to the latest protection wherever they connect—from home, within the company network, or on the go. This approach is particularly effective in dealing with malware that propagate via the Web such as BREDOLAB and PUSHDO.

Users who think they may have been affected by malware such as BREDOLAB and PUSHDO may also try using a free antivirus tools such as HouseCall, Trend Micro’s highly popular and capable on-demand scanner for identifying and removing viruses, Trojans, worms, unwanted browser plugins, and other malware.
You Scratch My Back...
BREDOLAB’s Sudden Rise in Prominence

SOURCES