Hesperbot – A New, Advanced Banking Trojan in the Wild

By Robert Lipovsky

Archived: 2026-04-06 15:34:26 UTC

Malware

A new and effective banking trojan has been discovered targeting online banking users in Turkey, the Czech Republic, Portugal and the United Kingdom. It uses very credible-looking phishing-like campaigns, related to trustworthy organizations, to lure victims into running the malware.

04 Sep 2013 • , 5 min. read

A new and effective banking trojan has been discovered targeting online banking users in Turkey, the Czech Republic, Portugal and the United Kingdom. It uses very credible-looking phishing-like campaigns, related to trustworthy organizations, to lure victims into running the malware.

For technical analysis of the Win32/Spy.Hesperbot binaries see our three blog posts: Hesperbot - A New Advanced Banking Trojan in the Wild, Hesperbot Technical Analysis Part 1/2 and Hesperbot Technical Analysis Part 2/2. You can download the comprehensive whitepaper here.

The Story

In the middle of August we discovered a malware-spreading campaign in the Czech Republic. Our interest was first kindled by the site that the malware was hosted on – a domain that passed itself off as belonging to the Czech Postal Service – but more interesting findings followed.

Analysis of the threat revealed that we were dealing with a banking trojan, with similar functionality and identical goals to the infamous Zeus and SpyEye, but significant implementation differences indicated that this is a new malware family, not a variant of a previously known trojan.

Despite being a “new kid on the block”, it appears that **Win32/Spy.Hesperbot** is a very potent banking trojan which features common functionalities, such as keystroke logging, creation of screenshots and video capture, and setting up a remote proxy, but also includes some more advanced tricks, such as creating a hidden VNC server on the infected system. And of course the banking trojan feature list wouldn’t be complete without network traffic interception and HTML injection capabilities. Win32/Spy.Hesperbot does all this in quite a sophisticated manner.

When comparing the Czech sample to known malware in our collection, we discovered that we had already been detecting earlier variants generically as Win32/Agent.UXO for some time and that online banking users in the Czech Republic weren’t the only ones targeted by this malware. Banking institutions in Turkey and Portugal were also being targeted.

The aim of the attackers is to obtain login credentials giving access to the victim’s bank account and to get them to install a mobile component of the malware on their Symbian, Blackberry or Android phone. Keep reading for

details on the malware spreading campaigns, their targets and for technical details on the trojan.

The Campaigns Timeline

The Czech malware-spreading campaign started on August 8, 2013. The perpetrators have registered the domain **www.ceskaposta.net**, which is very close to the real website of the Czech Postal Service, www.ceskaposta.cz.

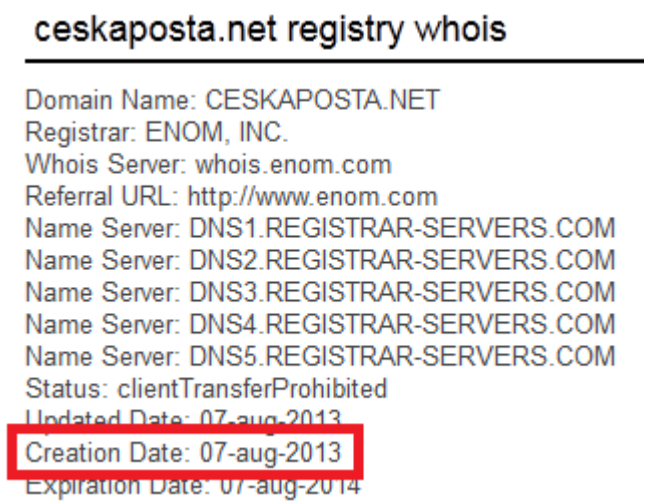

Figure 1 - Registration date of ceskaposta.net

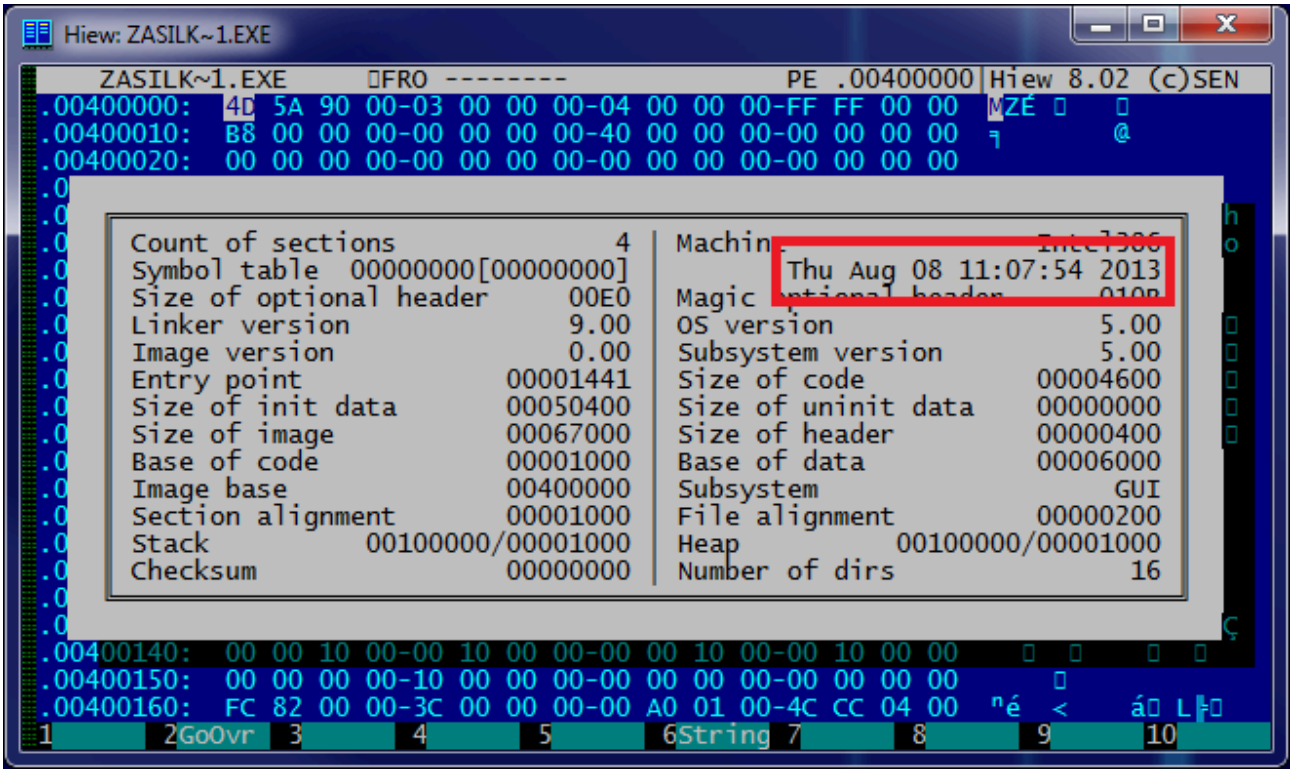

Figure 2 - Compilation timestamp of malware used in the Czech campaign

The domain was registered on August 7, 2013 and the first malware Hesperbot binaries (detected as **Win32/Agent.UXO** at first) distributed in the Czech Republic were compiled on the morning of August 8, 2013

and picked up by our LiveGrid® system moments later.

It's probably not surprising that the attackers tried to lure potential victims into opening the malware by sending emails which looked as parcel tracking information from the Postal Service. Similar techniques have been used many times before (e.g. here and here). The filename used was zasilka.pdf.exe: "zasilka" means *mail* in Czech. The link in the email showed the legitimate www.ceskaposta.cz domain while pointing to www.ceskaposta.net, which many victims hadn't noticed. Interestingly enough, the fake domain actually redirected to the real website when opened directly.

It should be noted that the Czech Postal Service responded very quickly by issuing a warning about the scam on their website.

Figure 3 - Warning about the fraudulent e-mails issued by the Czech Postal Service

While the Czech campaign was the one that caught our attention, the country most affected by this banking trojan is **Turkey** and Hesperbot detections in Turkey are dated even earlier than August 8.

Recent peaks in botnet activity were observed in Turkey in July 2013, but we have also found older samples that go back at least as far back as April 2013. During the analysis of the samples we found that they were sending debugging information to the C&C – an indicator that these variants were in the early stages of development. Additional research revealed that Turkey has been facing Hesperbot infections for some time now.

The campaigns used in Turkey are of a similar nature to the Czech campaign. The phish-like e-mail that was sent to potential victims purported to be an invoice (the file name is *fatura* in Turkish) from TTNET (the largest ISP in Turkey). A malicious file with a double extension – .PDF.EXE – was used here too. An analysis of this campaign has been published on the website of the Turkish National Information Security Program.

Only later in our research did we find that the malware operators have shifted their sights towards **Portugal**. Similarly to the Turkish campaign, the malicious files were disguised as an invoice from a local service provider with a very large market share, Portugal Telecom.

A variant designated to target computer users in the **United Kingdom** has also been found in the wild, but we cannot provide further details about its spreading campaign at the time of writing.

In the course of our research, we also stumbled upon an additional component used by Win32/Spy.Hesperbot. This malware, detected by ESET as Win32/Spy.Agent.OEC, harvests e-mail addresses from the infected system and sends them to a remote server. It is possible that these collected addresses were also targeted by the malware-spreading campaigns.

Targeted Banks and Victims

The configuration files used by the malware's HTTP interception and injection module specify which online banking websites are to be targeted by each botnet.

Czech Republic

```
https://ib24.csob.cz* csob_pers
https://bb24.csob.cz* csob_corp
https://www.servis24.cz/ebanking-s24/ib/base/usr/aut/login* servis24
https://www.business24.cz/ebanking-b24/ib/base/usr/aut/login* business24
https://www.mojebanka.cz/InternetBanking/* mojebanka_pers
https://www.mojebanka.cz/BusinessBanking/* mojebanka_corp
https://cz.unicreditbanking.net/disp?link=login.* unicreditbanking
https://mcsign.ba-ca.com/mcatweb/* ba-ca.com
https://www1.netbanka.cz/ZIBAIBS32/ControllerServlet* netbanka
https://uctrader.unicreditgroup.eu* unicreditgroup
https://klient4.rb.cz/ebts/version_02/eng/* klient4.rb
https://klient1.rb.cz/ebts/version_02/eng/* klient1.rb
https://ibs.rb.cz/IB/* ibs.rb
```

Figure 4 - Czech banks targeted by Hesperbot

Turkey

```
https://isube.kuveytturk.com.tr/
https://intbank.finansbank.com.tr/FWF/
https://internetsubesi.akbank.com/WebApplication.UI/entrypoint.aspx
https://esube.teb.com.tr/bireysel/*.do
https://kurumsalinternetsubesi.akbank.com/WebApplication.UI/entrypoint.aspx
https://internetbankaciligi.vakifbank.com.tr/*.aspx
https://websubem.vakifbank.com.tr/*.aspx
https://isube.garanti.com.tr/isube/
https://acikdeniz.denizbank.com/*.aspx
https://acikdeniz.denizbank.com/CustomLogin/Retail.aspx
https://internetsube.yapikredi.com.tr/*
https://ticari.yapikredi.com.tr/*
```

Figure 5 - Turkish banks targeted by Hesperbot

Portugal

```
https://ind.millenniumbcp.pt/*aspx*
https://caixaebanking.cgd.pt/*
https://www.bpinet.pt/*
https://caixadirectaonline.cgd.pt/*
https://www.particulares.santandertotta.pt*
```

Figure 6 - Portuguese banks targeted by Hesperbot

In the case of the Turkish and Portuguese botnets, the configuration files also included web-injects, i.e. pieces of HTML code that the trojan would insert into the banks' web-pages when viewed on the infected PC. This was not present in the Czech configuration file that we found, so most probably only simple form-grabbing and keylogging functionality was used in that instance.

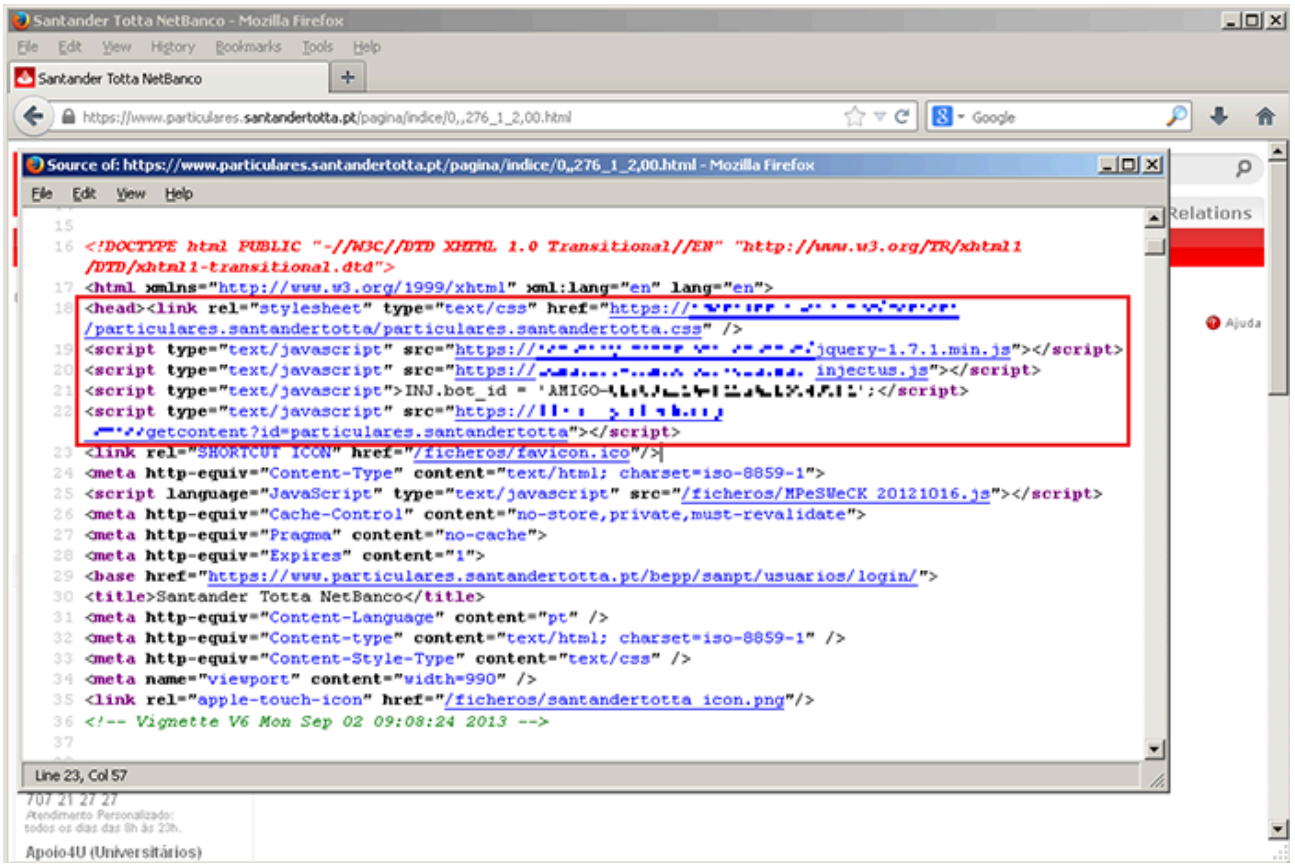

Figure 7 - Malicious scripts injected into Portuguese bank website. Notice that the URL address is legitimate, including the HTTPS protocol.

According to our ESET LiveGrid® telemetry, as well as our hands-on research into the malware operation, we estimate that the number of people that may have fallen victim to the Hesperbot banking trojan is in the scale of **tens in the Czech Republic and Portugal** (respectively) and in the scale of **several hundred in Turkey**. Detection statistics per country are shown in the figure below. It has also come to our attention that victims in the Czech Republic have lost significant amounts of money as a result of infection by this malware. It's quite possible that there are similarly unfortunate victims in Turkey and Portugal as well.

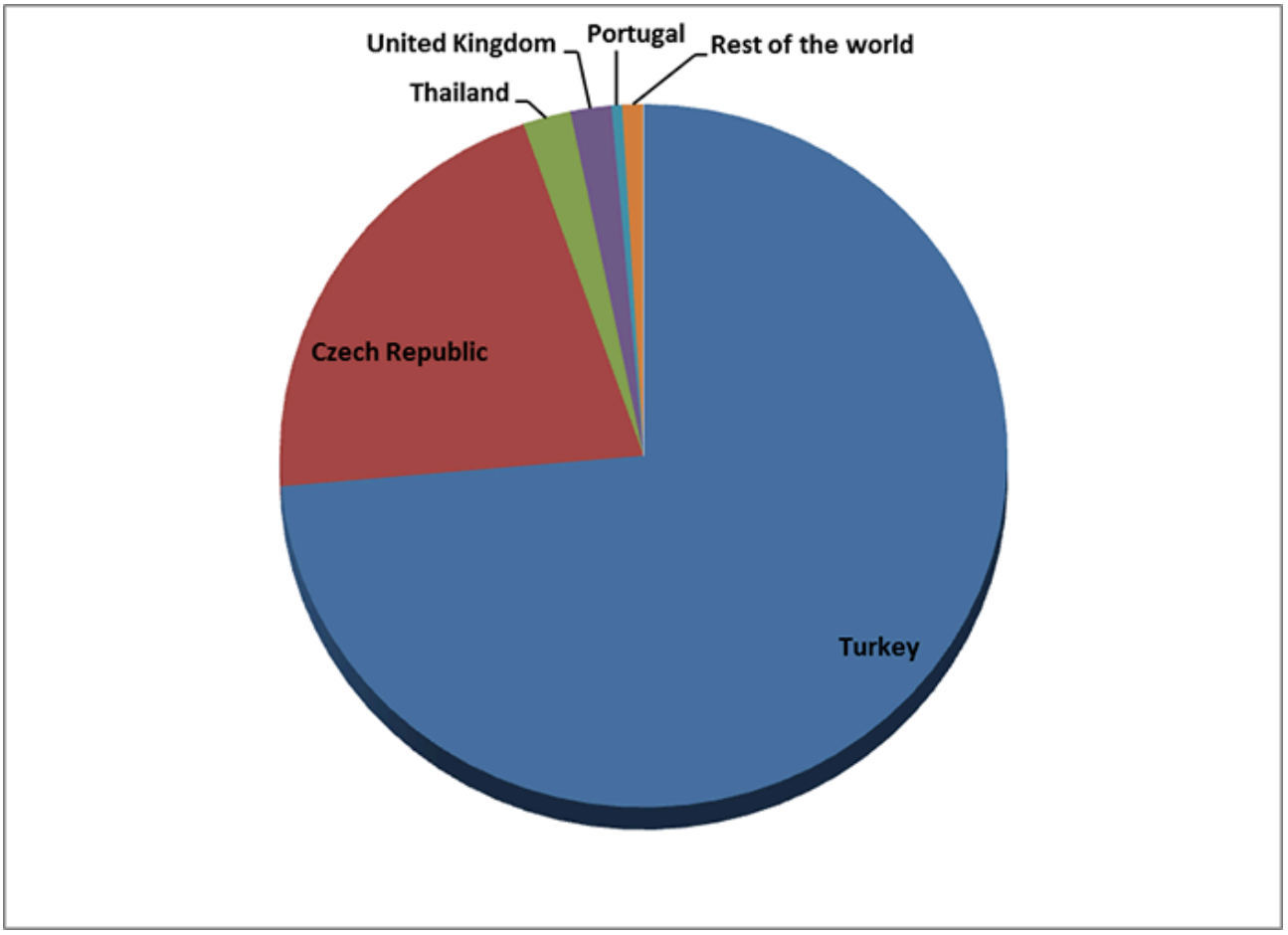

Figure 8 - Detection statistics of Win32/Spy.Hesperbot according to ESET LiveGrid

Our thorough technical analysis of the Win32/Spy.Hesperbot binaries can be found here and here. Refer to the comprehensive whitepaper for full details.

Source: https://www.welivesecurity.com/2013/09/04/hesperbot-a-new-advanced-banking-trojan-in-the-wild/