

Analysis of a Banker Trojan

INFIGO-TD-2008-02

2008-12-10

©INFIGO IS. All rights reserved.

This document contains information protected by copyright. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of INFIGO IS.

Infigo IS d.o.o.
Horvatovac 20
10000 Zagreb

tel. +385 1 4662 700
fax. +385 1 4662 701
info@infigo.hr
www.infigo.hr



TABLE OF CONTENTS

<u>1. SUMMARY</u>	4
<u>2. TECHNICAL ANALYSIS</u>	5
2.1. INFECTION VECTORS	5
2.2. DATA THEFT COMPONENTS	6
2.3. SUBMISSION OF HARVESTED INFORMATION TO ATTACKER	7
<u>3. PROTECTION RECOMMENDATIONS</u>	9

1. SUMMARY

The rise of criminal activity on the Internet has been evident quite some time. In the last couple of years, the criminals have started targeting Internet banking users. The increasing number of targeted malware calls for additional caution.

Croatian banks have historically been neglected by various Trojan horses, probably due to two main reasons: a perception of a smaller return of invested to the attackers and relatively high levels of protection implemented in Internet banking services typically found in Croatia.

INFIGO IS's security research team regularly tracks and analyses malicious activities on the Internet. For the first time, a Trojan horse belonging to the Banker family that amongst foreign banks also attacks Croatian banks has been identified. The two biggest Croatian banks, "Zagrebacka banka" and "Privredna banka" are targeted by the Trojan. These banks are especially attractive to attackers due to their large number of clients.

The analyzed Trojan horse targets end users (client machines) and is limited to stealing data from forms rendered in web browsers. It should be noted that Internet banking applications that use two factor authentication (smart cards, tokens) are not vulnerable due to dynamically generated passwords specific for every user session and/or transaction.

However, there are certain services offered by targeted banks that do not use two factor authentication. Such services can be exploited by the analyzed Trojan horse in order to read account credentials of the victim user and possibly conduct unauthorized transactions.

The rest of the paper contains a technical analysis of the Trojan horse as well as a section with recommendations for protection and identification of infected systems.

While some capabilities of the analyzed Trojan horse are not fully functional (i.e. logging of pressed keys in the Mozilla Firefox web browser), it can be expected that the attackers will fix identified bugs and add new features in the future.

Users are recommended to follow and apply security recommendations given in chapter 3.

2. TECHNICAL ANALYSIS

2.1. INFECTION VECTORS

The Trojan horse does not have the ability to automatically spread. It instead uses other attack vectors to infect new computers. The attack vectors used by the analyzed Banker Trojan horse are listed below:

- Compromised web servers redirect visitors to a dedicated (compromised) server hosting the Trojan horse. The web page on the server hosting the Trojan horse uses an Internet Explorer vulnerability.

By exploiting the MS06-014 vulnerability (*Microsoft Data Access Components*), the Trojan horse can be automatically installed on vulnerable machines.

- If the exploit fails, the user is prompted to download and install the Trojan horse through various social engineering techniques.

At the time of the analysis script the exploit for the vulnerability in Internet Explorer was available at [http://buskirava.awardspace.com/\[REMOVED\].htm](http://buskirava.awardspace.com/[REMOVED].htm).

If the exploit runs successfully, it will retrieve a file from the above server and store it on the victim's computer in the temporary directory as `bl4ck.exe`. The file is executed automatically by the exploit.

The Trojan horse now infects the victim's computer and tries to hide itself using the following steps:

- The original file is copied into the system directory (`C:\WINDOWS\System32`) as `mshelp.exe`.
- After it has been successfully copied, the original process (`bl4ck.exe`) starts a new process by executing the `mshelp.exe` file and exits.
- The Trojan horse then checks the location it was started from and the file name of the executable; it continues only if the previous two steps have been fulfilled.
- In order to ensure it will get started after a system reboot, the Trojan horse creates the following *Registry* keys with the content of `mshelp.exe`:
 - "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run" containing "Generic Host Process for WinXP Services",
 - "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices" containing "Generic Host Process for WinXP Services".
- After installation, the Trojan horse fetches a configuration file from the following URL address [http://buskirava.awardspace.com/\[REMOVED\].txt](http://buskirava.awardspace.com/[REMOVED].txt). The configuration file is saved as `C:\WINDOWS\System32\descript.lnk`. This is not a real LNK file but a plain text file.
- Depending on the parameters in the configuration file, the Trojan horse further fetches additional files from the following web sites:
 - `bisyeton.netfirms.com`,
 - `festashka.awardspace.com`,
 - `bsakurmeh.awardspace.com`.

2.2. DATA THEFT COMPONENTS

In order to steal user information, the Trojan horse first initializes a data structure with addresses of all web pages that will be monitored for activity. Among other foreign banks, there are several web sites in the Croatian domain space (the .hr domain) that the Trojan steals data from:

- pbz.hr,
- zaba.hr,
- open.hr,
- kaptol.hr.

The addresses listed above also include all the subdomains that the user of the infected computer visits. When any such web site is visited, the Trojan horse will steal data ignoring the URL prefix (eg. the Trojan will steal data from both www.pbz.hr and net.pbz.hr).

The following picture shows the Trojan horse code executed in the OllyDbg debugger. References to Croatian domain addresses are visible in the screenshot.

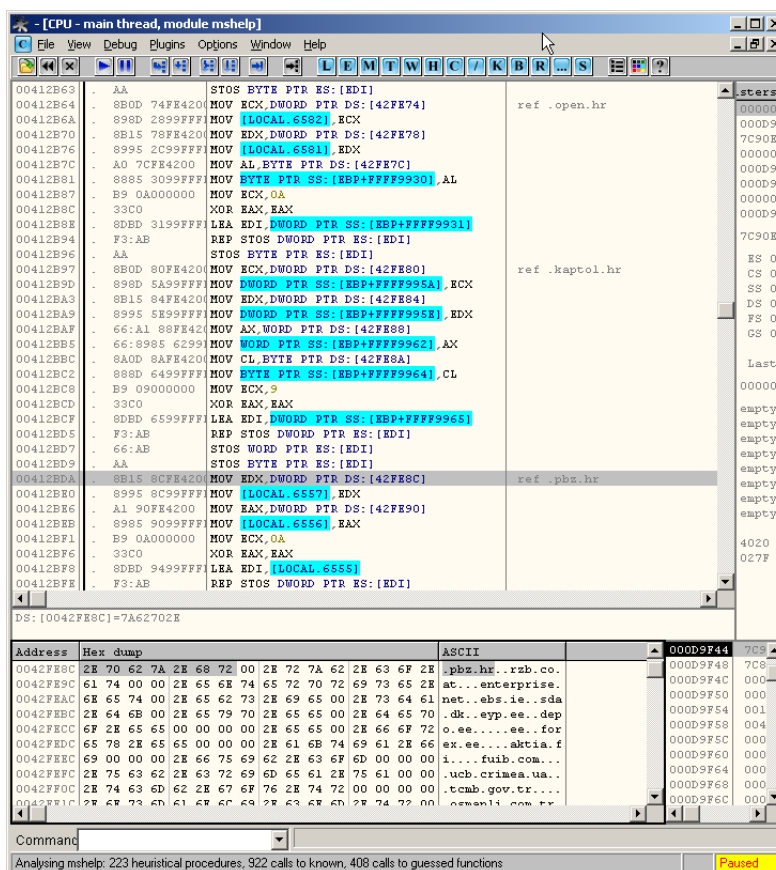


Figure 1: References to addresses from the Croatian domain space (.hr)

The Trojan horse can steal data from the Internet Explorer and Mozilla Firefox web browsers, however, a thorough analysis of program code revealed that the data stealing component from the Mozilla Firefox web browser is not fully implemented and that it does not work in the obtained sample.

Once executed, the Trojan horse tries to identify active web browser windows by using the EnumWindows() function. This function allows identification of currently open windows on the system. If the Internet Explorer browser's window is identified, the Trojan horse fetches the content of the address bar and compares it to the list of addresses in the previously described structure.

The URL addresses that the Trojan horse steals information from are grouped in two categories; simple and advanced data stealing lists. Depending on the list, the Trojan horse will execute appropriate code:

- The URL addresses in the simple list contain pages that will be monitored for all user activity. The Trojan horse will steal data from all forms identified on the web page. In other words, the Trojan horse cannot distinguish authentication data from other types of data (i.e. search field data) which means that the attacker needs to further analyze captured data. All identified Croatian web pages belong to this group.
- The advanced list contains pages that the attacker is familiar with and knows from which fields on the web page data needs to be stolen (i.e. username and password fields).

To steal the data the Trojan horse uses the `GetAsyncKeyState()` function. This function allows the Trojan horse to detect mouse and keyboard activity. All user interaction is monitored and logged in textual format as shown in the following table:

```
{Current Window: PBZ 365 - Microsoft Internet Explorer}  
user_name{LBUTTON}PIN{LBUTTON}{LBUTTON}
```

2.3. SUBMISSION OF HARVESTED INFORMATION TO ATTACKER

The Trojan horse will submit harvested data to the attacker's web site, once one of the following conditions is satisfied:

- 300 seconds elapsed since the Trojan horse started logging user activity,
- The user has pressed the {ESC} key,
- More than 9000 bytes of data have been logged.

The stolen data is sent to the following URL address on the attacker's web site, [http://buskirava.awardspace.com/_\[REMOVED\].php](http://buskirava.awardspace.com/_[REMOVED].php). An example of an HTTP POST request that sends stolen data to the previously mentioned URL is shown below:

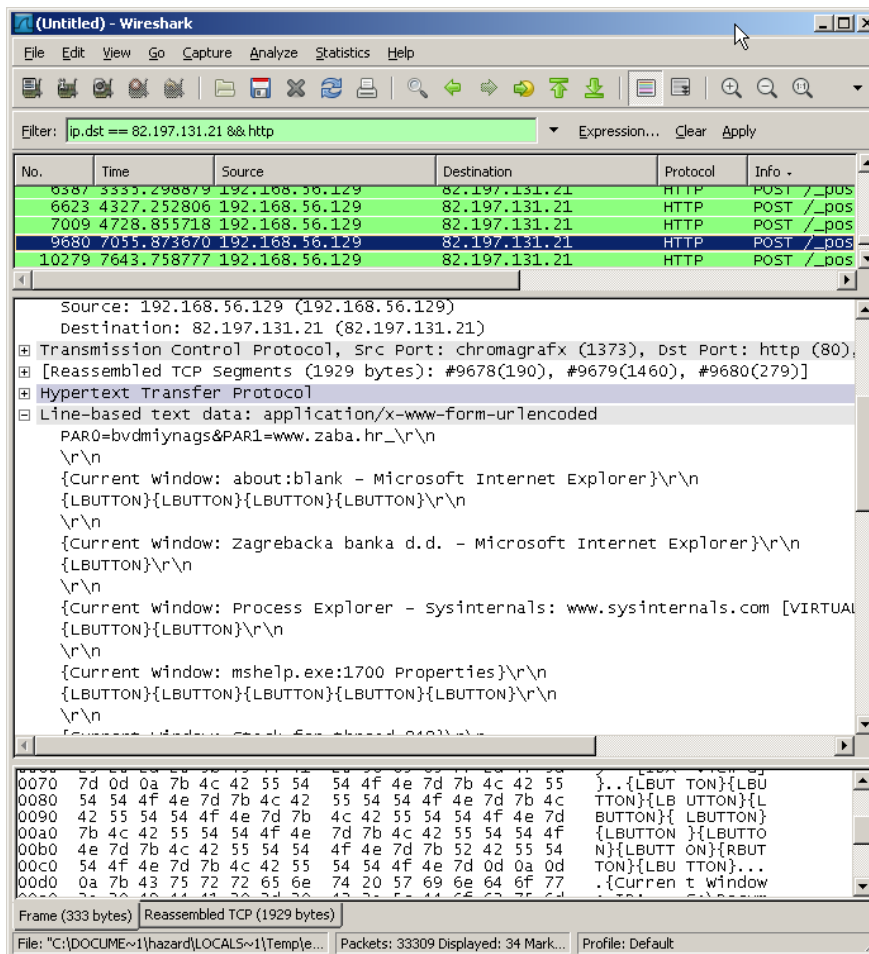
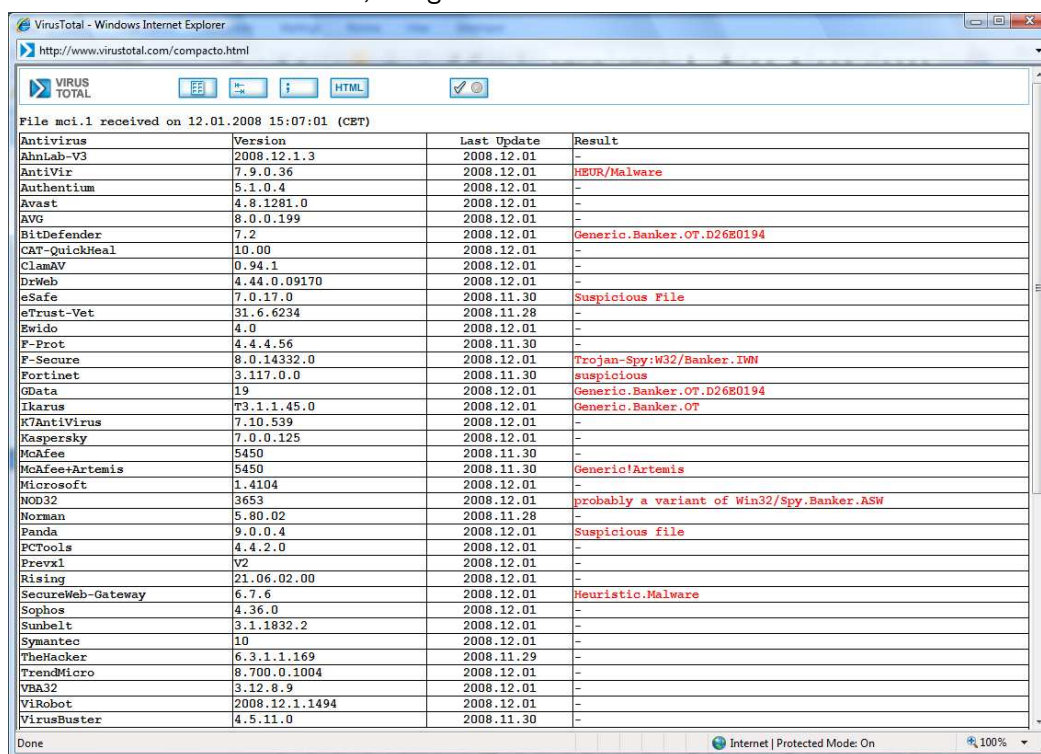


Figure 2: Network data of an HTTP POST request sending stolen data

3. PROTECTION RECOMMENDATIONS

As with most Trojan horses, there is not a single solution for protection. Instead, a layered approach should be considered. INFIGO IS recommends that users follow the steps listed below:

- Security updates for operating systems and applications should be regularly installed. The security updates have to be installed on all computers in order to prevent attackers from exploiting known security vulnerabilities. In this case, the analyzed Trojan horse used an old vulnerability in the Internet Explorer web browser. Special attention should be given to applications that cannot be updated through the Windows Update service.
- An Anti-Virus program should be installed and regularly updated on all machines. Although Anti-Virus programs cannot provide full protection from malware, they provide an additional layer of security. In the case of the analyzed Trojan horse, during a preliminary analysis it has been established that only a small number of Anti-Virus products successfully detected it. The following picture shows results of Anti-Virus detection made on 1.12.2008, using the VirusTotal service:



Antivirus	Version	Last Update	Result
AhnLab-V3	2008.12.1.3	2008.12.01	-
AntiVir	7.9.0.36	2008.12.01	HEUR/Malware
Authentium	5.1.0.4	2008.12.01	-
Avast	4.8.1281.0	2008.12.01	-
AVG	8.0.0.199	2008.12.01	-
BitDefender	7.2	2008.12.01	Generic.Banker.OT.D26E0194
CAT-QuickHeal	10.00	2008.12.01	-
ClamAV	0.94.1	2008.12.01	-
DrWeb	4.44.0.09170	2008.12.01	-
eSafe	7.0.17.0	2008.11.30	Suspicious File
eTrust-Vet	31.6.6234	2008.11.28	-
Ewido	4.0	2008.12.01	-
F-Prot	4.4.4.56	2008.11.30	-
F-Secure	8.0.14332.0	2008.12.01	Trojan-Spy:W32/Banker.IWN
Fortinet	3.117.0.0	2008.11.30	suspicious
GData	19	2008.12.01	Generic.Banker.OT.D26E0194
Ikarus	T3.1.1.45.0	2008.12.01	Generic.Banker.OT
K7AntiVirus	7.10.539	2008.12.01	-
Kaspersky	7.0.0.125	2008.12.01	-
McAfee	5450	2008.11.30	-
McAfee+Artemis	5450	2008.11.30	Generic!Artemis
Microsoft	1.4104	2008.12.01	-
NOD32	3653	2008.12.01	probably a variant of Win32/Spy.Banker.ASW
Norman	5.80.02	2008.11.28	-
Panda	9.0.0.4	2008.12.01	Suspicious file
ECTools	4.4.2.0	2008.12.01	-
Prevx1	V2	2008.12.01	-
Rising	21.06.02.00	2008.12.01	-
SecureWeb-Gateway	6.7.6	2008.12.01	Heuristic.Malware
Sophos	4.36.0	2008.12.01	-
Sunbelt	3.1.1832.2	2008.12.01	-
Symantec	10	2008.12.01	-
TheHacker	6.3.1.1.169	2008.11.29	-
TrendMicro	8.700.0.1004	2008.12.01	-
VBA32	3.12.8.9	2008.12.01	-
ViRobot	2008.12.1.1494	2008.12.01	-
VirusBuster	4.5.11.0	2008.11.30	-

Figure 3: VirusTotal results for the analyzed Trojan horse

- Install and use a personal firewall to minimize exposure on the Internet.

Banks and web site owners should perform the following proactive steps to protect their customers:

- As the main attack vector today are compromised web servers, regularly penetration testing of web servers should be conducted in order to confirm and maintain a high level of security.
- Clients should be continuously educated (security awareness).
- Security teams in banks should regularly monitor security sources and act preventively in cases of information disclosure about malware that can have impact on their clients.