

Testing Rapport UPG vs. 7 malware

September 1, 2008

David Matoušek

Roman Říha

Matousec – Transparent security

<http://www.matousec.com/>

research@matousec.com

Summary: Rapport prevented all known attacks against eBay performed by the tested malware.

Introduction

Our task was to test Rapport against seven dangerous malware that attack financial institutions. The audit's scope included analyzing the malware' attacks against financial institutions' websites and finding out whether Rapport thwarts all attempts to steal credentials or defraud the user. The malware to be tested were NetHell (Trojan.Win32.Delf.dgw), SilentBanker (Trojan.Win32.Silentbanker), two variants of Wsnpoem (Trojan-Spy.Win32.Zbot.nm and Trojan-Spy.Win32.Zbot.dqu – the first one is the original standalone variant while the other one is known to be bundled with the notorious "Antivirus XP 2008" fake anti-virus software, and both are delivered through the fake "PayPal invoice" spam), Papras (Trojan-PSW.Win32.Papras.ea), MBR Torpig (Trojan.Sinowal.fd), Torpig (Trojan.PSW.Sinowal.G) and CoreFlood (Trojan-Downloader.Win32.Zlob.pmd). The malware' binaries as well as the decryption routines for their encrypted communication were provided with the task assignment. Each malware uses a technique to steal the credentials. These techniques were divided into three categories.

The tests were performed on a clean machine with Windows XP Service Pack 2 with Internet Explorer 6 installed.

Each test was performed in the following steps:

1. The machine was infected by the malware and rebooted.
2. A user login on ebay.com was performed. The username was "sample_user_123", the password was "qwer1234". The other malware' influences such as displaying the pages that are not genuine were noted.
3. The stolen data was retrieved and analyzed. Additional analysis of the malware behavior was performed.
4. Rapport was installed and the machine was rebooted.
5. A new user "sample_user_3211" was signed in ebay.com when the full Rapport protection was installed. The password for this account was "rewq4321".
6. The stolen data was retrieved and analyzed again.

The analysis of the stolen data included decryption (if needed) and check whether it contains the credentials.

Malicious Browser Add-ons

Malware in this category: NetHell, SilentBanker

Internet Explorer add-on technology allows adding software components (add-ons) into the browser. These add-ons are divided into a few categories such as Browser Helper Objects (BHO), ActiveX Control and so on. Each add-on can control everything that goes on within the browser. Add-ons are usually used to add features (for example: extra toolbars, animated mouse pointers, stock tickers, and pop-up ad blockers) to the browser. Many add-ons come from the Internet. Most add-ons from the Internet require that the user gives permission before they are downloaded to the computer. Some, however, might be installed without the user's knowledge. Some add-ons are installed with Microsoft Windows. Although this technology was created to add useful features to the browser, it is widely used by attackers to perform malicious activity such as stealing sensitive information, injecting transactions into authenticated sessions, and changing information the user sees. This attack is called man-in-the-browser.

Code Hooking

Malware in this category: SilentBanker, Wsnpoem, Papras, MBR-Torpig, Torpig

Using this technique the malware hooks specific browser functions and injects its own code into these functions. Once done, the malware operates inside the browser's process and whenever the browser calls a hooked function, the malware code runs and has a full access to all the information inside the browser. Function hooking is a well know technique. Any application can access the browser's memory and look for functions. When the function is found, it is possible to override it with a different code. The malware can then cut the begging of the function and place its own code instead. The malware can also make sure that the code which was cut off will run once the malware code completes its execution. Function hooking might sound complicated but is actually very easy to do. There are many code samples and even freeware and commercial tools that make it very simple to hook various functions inside the browser or one of its components (such as WinInet).

Direct/External DOM Access

Malware in this category: CoreFlood

Add-ons are not the only way to communicate with the browser. The same API that add-ons can use to control the browser is also available to any program on the user's desktop. A malware can very easily retrieve a reference to the browser and use this reference to access the browser's Document Object Model (DOM). From this moment on the malware can use the same API as the add-on. While add-ons can be switched on and off by the user, programs that access the browser are out of the user's control and are thus the most dangerous form of man-in-the-browser.

NetHell

Known attacks: Credentials theft

Tested against: Rapport Dawsonite Build 0417.2

This malware uses a Browser Helper Object to inject its malicious library into Internet Explorer. This code steals the credentials via intercepting the keystrokes and analyzing the data to be sent. The stolen data are encrypted and saved to "C:\WINDOWS\system32\alog.txt". This file is periodically checked and if it has a nonzero size the contents are sent out and the file is deleted.

The encrypted data	The decrypted data
<pre> ufzz~}4!!}gi`g` klow macly}!kLowG]oAG jbb1]gi`g`+<8 {3fzz~+o+<H+<Hyyy klow macS0{k g 3EKWBAIIKJ4}oc~bkq{k k q?<=0u fzz~}4!!}gi`g` klow macly}!kLowG]oAG jbb1]gi`g`+<8 {3fzz~+o+<H+<Hyyy klow macS0~o}}3EKWBAIIKJ4}yk ?<=:EKW]\KOJ4}yk ?<=:0ufzz~}4!!}gi`g` klow macly}!kLowG]oAG jbb1maq~o z`k g 3<+<8}gzk g 3>+<8[]`g`!j]B3?S0Yk bmac. za. kLowchmg]oAGmacco`j3]g g`Yk bmac 0 fg 30b k3hob k ob x30cg 30 fcg 30 gzk g 3>0maq~o z`k g 3<0[]g`!j]B3?0 {3fzz~+o+<H+<Hyyy klow mac ~30~o?30~o<30~o=30g?3#?0~o1kZw~k3#?0 zC 02030>?+=j1LWobGf>H 000000yA}{x>Dz+<LY}C=H00v0+<LC>?4=J0G00L0MKG_10+=LZM>?+=JyL:T[6 z+<L 00001yMw j 0000000c pV007 `oia?F_603a9gLeov0M+=L^j+=Jz >0{k g 3}oc~bkq{k k q?<=0~o}}30yk ?<=:0eimz30 </pre>	<pre> [https://signin.ebay.com/ws/eBayISAPI.dll?signin%26ru=http%3A%2F %2Fwww.ebay.com] userId=KEYLOGGED:sample_user_123 KEYSREAD:sample_user_123 [https://signin.ebay.com/ws/eBayISAPI.dll?signin%26ru=http%3A%2F %2Fwww.ebay.com] pass=KEYLOGGED:qwer1234 KEYSREAD:qwer1234 [https://signin.ebay.com/ws/eBayISAPI.dll?co_partnerid=2%26sitei d=0%26usingSSL=1] welcome to ebay MFISAPICcommand=signinwelcome bhid= lse=false lsv= mid= hmid= siteid=0 co_partnerId=2 UsingSSL=1 ru=http%3A%2F%2Fwww.ebay.com pp= pa1= pa2= pa3= i1=-1 pageType=-1 rtmData=A01%3DgBYALIH0FAAAAAAAw0Suv0Jt%26wDM3FjAxAX%3BM01%3DAIAAB ACEIQGA%3BTC01%3DwB4ZU8T%26GBAAAGwCyBdBAAAAAAAMguJXAA9SnAgo1HQ8A Do7iBkAxAC%3BPS%3DT_0 userId=sample_user_123 pass=qwer1234 kgct= </pre>

Before the installation of Rapport, the credentials from ebay.com were stolen. After the installation, NetHell was not able to steal any credentials from ebay.com.

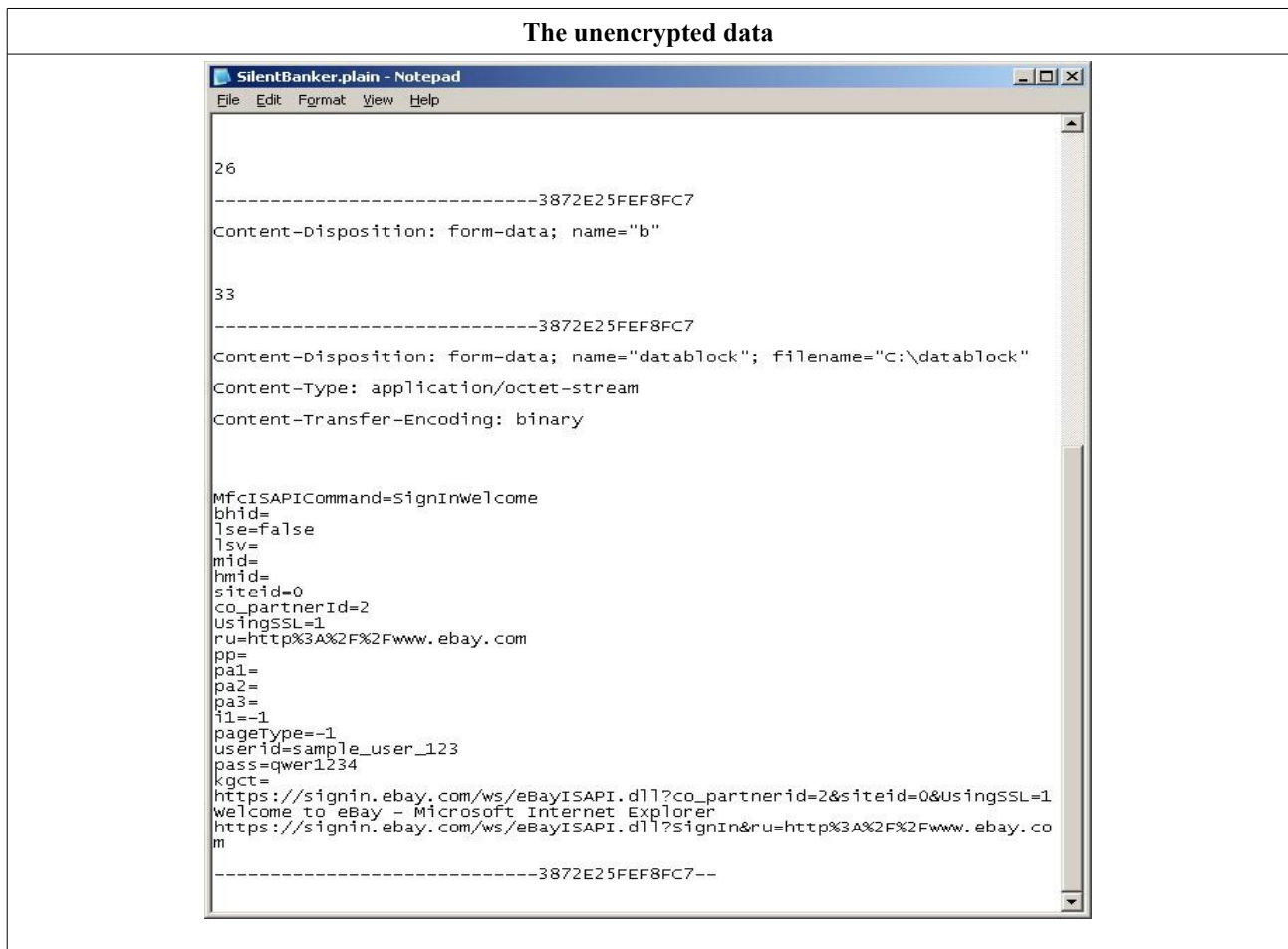
Result: Rapport prevented all known NetHell's attacks against eBay.

SilentBanker

Known attacks: Credentials theft

Tested against: Rapport Dawsonite Build 0417.2

SilentBanker creates a new dynamic library in the system directory and installs it as a Browser Helper Object. This library hooks some functions including the `HttpSendRequest*` functions. The credentials transmitted via this functions are stolen and sent out. The stolen data are sent out in an unencrypted form.



Before the installation of Rapport, the credentials from ebay.com were stolen. After the installation, SilentBanker was not able to steal any credentials from ebay.com.

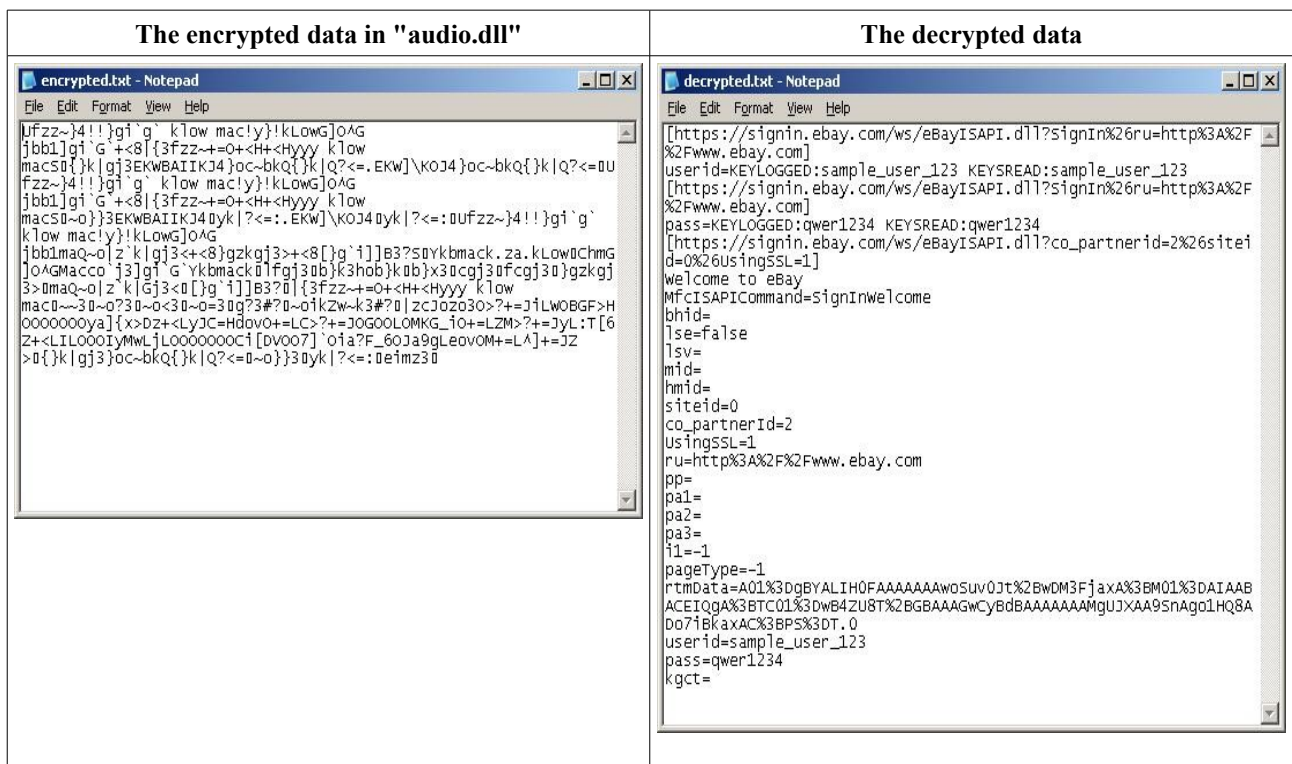
Result: Rapport prevented all known SilentBanker's attacks against eBay.

Wsnpoem

Known attacks: Credentials theft

Tested against: Rapport Dawsonite Build 0407.0 (the first variant), Rapport Dawsonite Build 0417.2 (the second variant)

This malware injects malicious code into many processes including "winlogon.exe", Windows Explorer, Internet Explorer and so on. User mode hooks are installed within Internet Explorer to steal the data sent via HttpSendRequest*. The data is encrypted and saved to "C:\WINDOWS\system32\wsnpoem\audio.dll".



Before the installation of Rapport, the credentials from ebay.com were stolen. After the installation, Wsnpoem was not able to steal any credentials from ebay.com.

Result: Rapport prevented all known Wsnpoem's attacks against eBay.

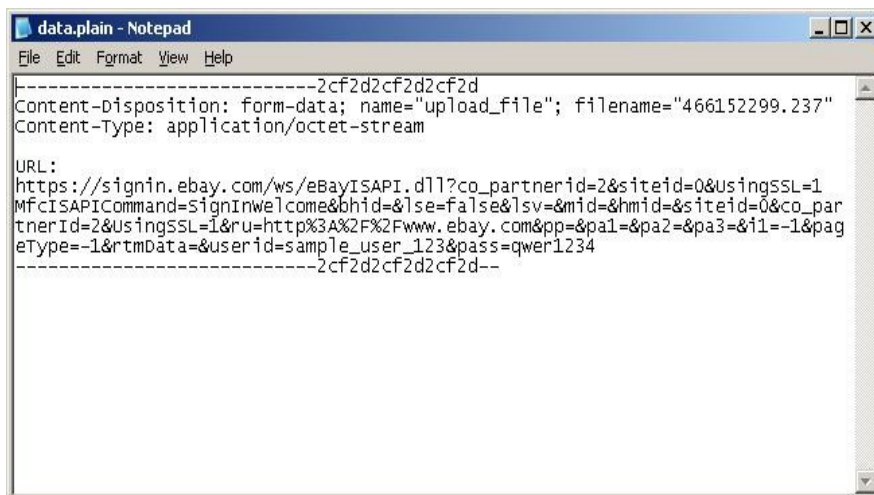
Papras

Known attacks: Credentials theft

Tested against: Rapport Dawsonite Build 0407.0

Papras creates a new binary file in "C:\Windows\" and executes it. Then it loads a driver and installs some SSDT hooks to hide its presence in the system. After that, it injects some malicious code into many processes including Internet Explorer and hooks some functions including HttpSendRequestA. The data to be send via this function is parsed and sent to the hidden process using WM_COPYDATA message. This process uses HttpSendRequestA function to send the data out. However, the sending of the data failed very often because its mothership was not very stable. Therefore we decided not to analyze the traffic. We developed a utility that hooks the HttpSendRequestA function in the hidden process and saves the data to be sent in a log file. This data was used as a proof of the stolen credentials.

The unencrypted data



```
-----2cf2d2cf2d2cf2d
Content-Disposition: form-data; name="upload_file"; filename="466152299.237"
Content-Type: application/octet-stream

URL:
https://signin.ebay.com/ws/eBayISAPI.dll?co_partnerid=2&siteid=0&usingSSL=1
MfcISAPICommand=SignInwelcome&bhid=&lse=false&lsv=&mid=&hmid=&siteid=0&co_par
tnerId=2&usingSSL=1&ru=http%3A%2F%2Fwww.ebay.com&pp=&pa1=&pa2=&pa3=&i1=-1&pag
eType=-1&rtmData=&userid=sample_user_123&pass=qwer1234
-----2cf2d2cf2d2cf2d--
```

Before the installation of Rapport, the credentials from ebay.com were stolen. After the installation, Papras was not able to steal any credentials from ebay.com.

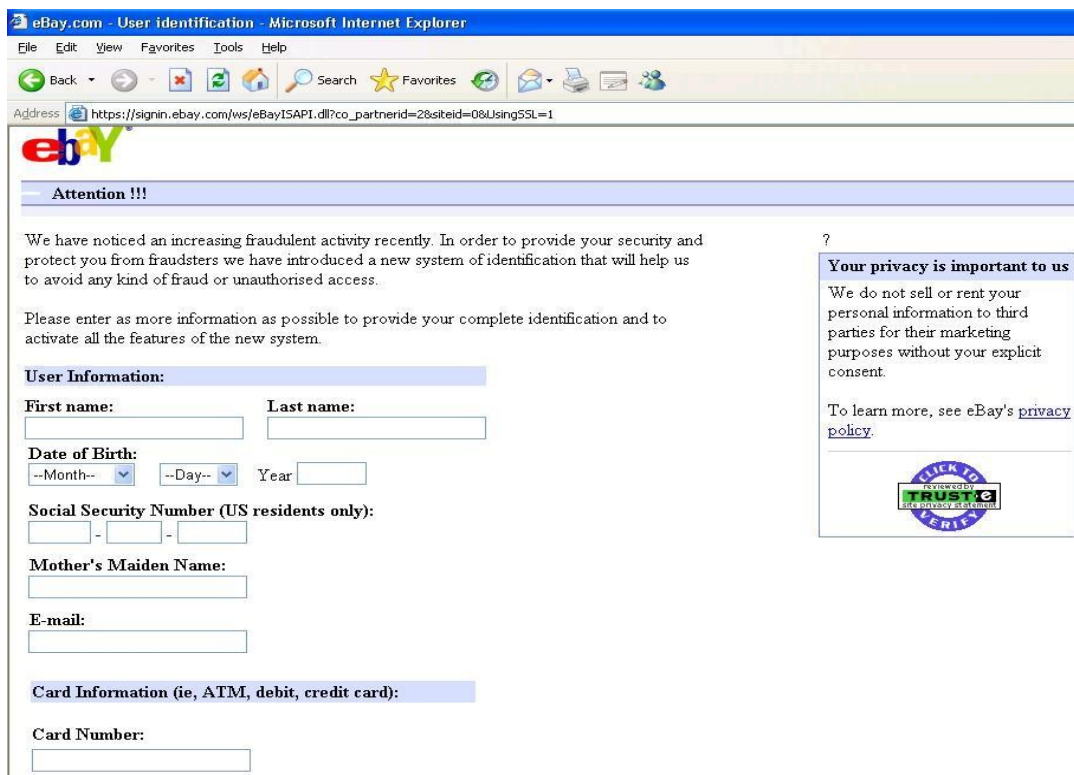
Result: Rapport prevented all known Papras' attacks against eBay.

MBR Torpig

Known attacks: Credentials theft, Displaying phishing pages

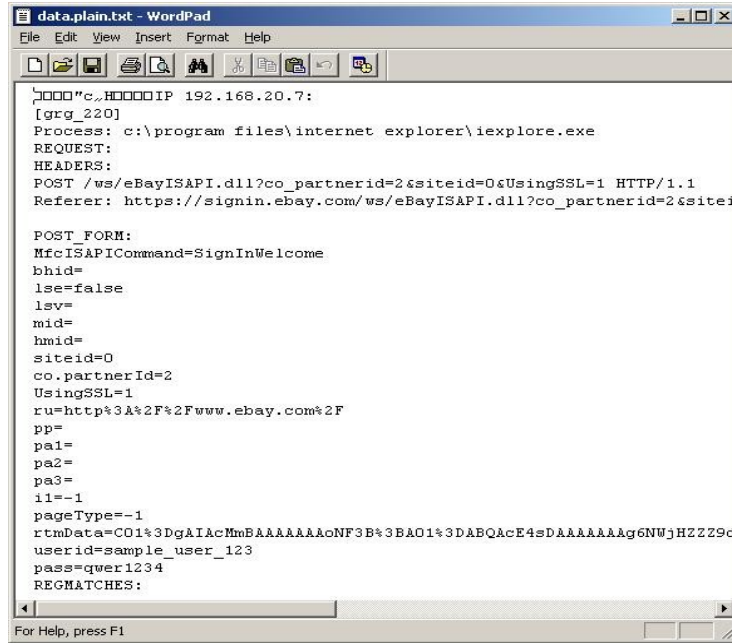
Tested against: Rapport Dawsonite Build 0407.0

This malware installs itself into the master boot record to be executed whenever the computer starts. The Torpig's code runs inside the process "services.exe" and from within this process it saves the stolen data in "C:\Windows\Temp\" directory. The data is stolen via inline hooks placed into Internet Explorer. Whenever a user tries to login on ebay.com or paypal.com, the malware shows a phishing page that asks for the user's private data. Here is an example of such phishing page:



We used slightly different approach to test this malware. On the testing machine was installed MBR Torpig and then Rapport. Rapport was turned off and Torpig was tested as usual (login on eBay with username "sample_user_123" and password "qwer1234"). After this, Rapport was turned on and we performed the test again (login on eBay with username "sample_user_3211" and password "rewq4321"). To analyze the stolen data we used the data stored in "C:\Windows\Temp" directory.

The unencrypted data



```
data.plain.txt - WordPad
File Edit View Insert Format Help
Process: c:\program files\internet explorer\iexplore.exe
REQUEST:
HEADERS:
POST /ws/eBayISAPI.dll?co_partnerid=2&siteid=0&UsingSSL=1 HTTP/1.1
Referer: https://signin.ebay.com/ws/eBayISAPI.dll?co_partnerid=2&siteid=0

POST FORM:
MfcISAPICommand=SignInWelcome
bhid=
lse=false
lsv=
mid=
hmid=
siteid=0
co.partnerId=2
UsingSSL=1
ru=http%3A%2F%2Fwww.ebay.com%2F
pp=
pa1=
pa2=
pa3=
il=-1
pageType=-1
rtmData=CO1%3DgAIacMmBAAAAAAAAAoNF3B%3BA01%3DABQAcE4sDAAAAAAAAAg6NUjHZZZ9d
userid=sample_user_123
pass=qwer1234
REGMATCHES:
```

Before the installation of Rapport, the credentials from ebay.com were stolen and the phishing page appeared. After the installation, Torpig was not able to steal any credentials from ebay.com and no phishing page appeared.

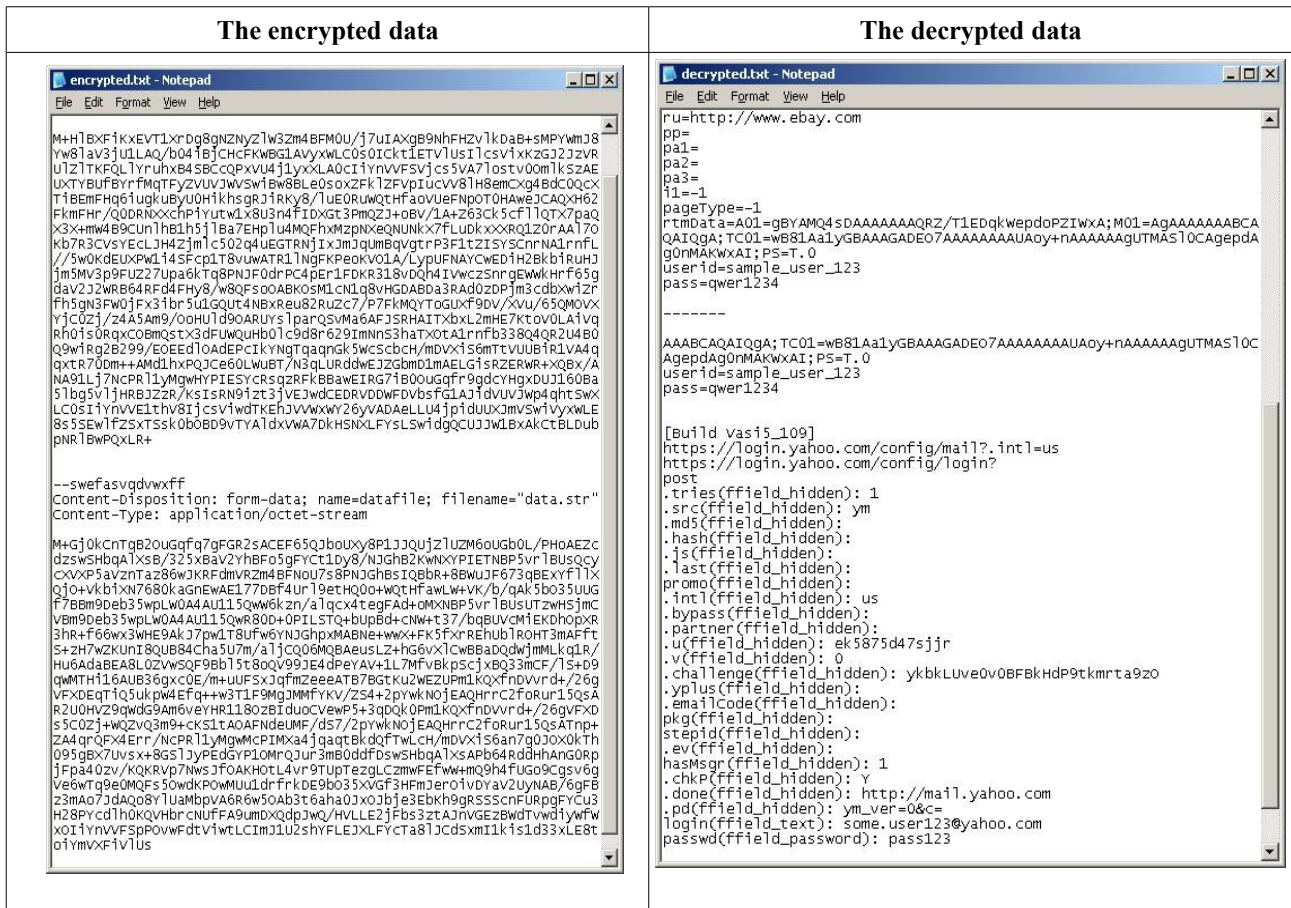
Result: Rapport prevented all known MBR Torpig's attacks against eBay.

Torpig

Known attacks: Credentials theft

Tested against: Rapport Dawsonite Build 0407.0

This malware creates new dynamic libraries in "C:\Program Files\Common Files\Microsoft Shared\Web Folders" and injects one of them into almost all running processes. This library hooks many functions including Crypt* and HttpSendRequest* functions. Then the malware runs a new instance of "svchost.exe", which saves the stolen credentials into a file in "C:\Windows\Temp". The stolen credentials are sent out by the "svchost.exe" via the HttpSendRequestA API in an encrypted form.



Before the installation of Rapport, the credentials from ebay.com were stolen. After the installation, Torpig was not able to steal any credentials from ebay.com.

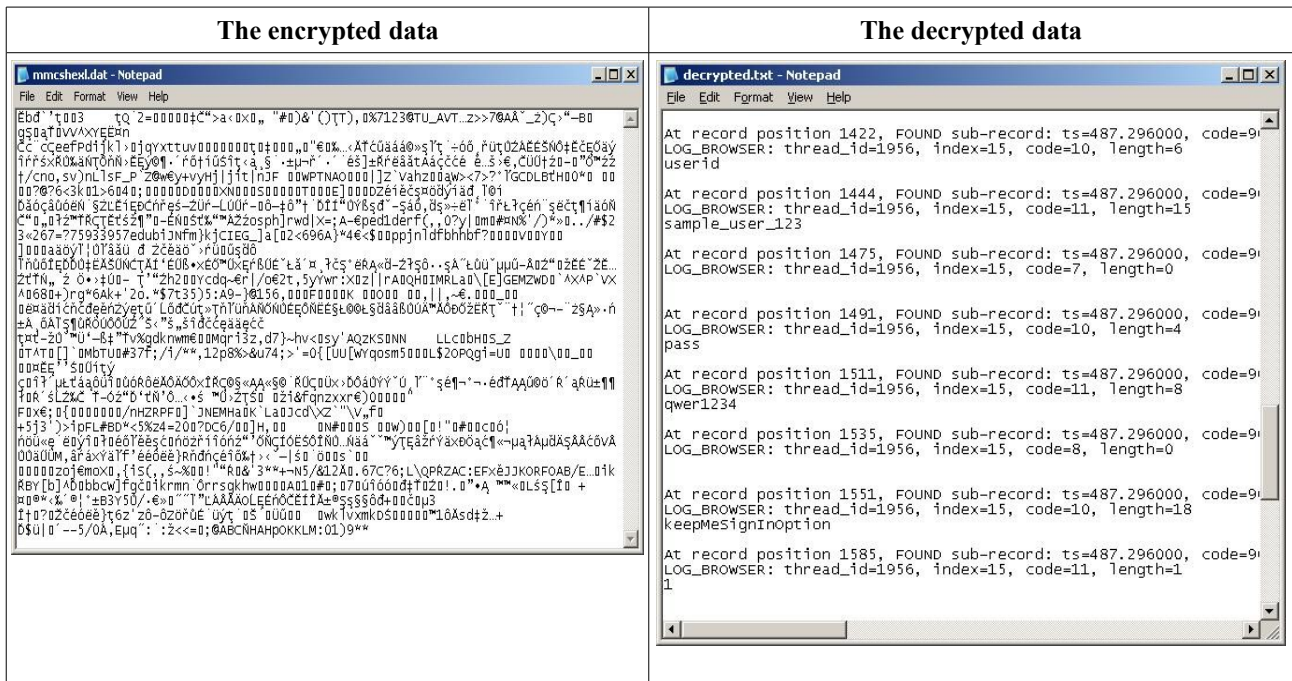
Result: Rapport prevented all known Torpig's attacks against eBay.

CoreFlood

Known attacks: Credentials theft

Tested against: Rapport Dawsonite Build 0417.2

This malware creates some files in system directory "C:\WINDOWS\system32" including ".dat" files and one ".dil" file. The ".dil" file is loaded into Internet Explorer and Windows Explorer as an Icon Overlay Handler (IOH). When a user enters credentials on a login page and then clicks on a button, the malware saves the credentials in memory and within a while it encodes them and saves them into one of the ".dat" files.



Before the installation of Rapport, the credentials from ebay.com were stolen. After the installation, CoreFlood was not able to steal any credentials from ebay.com.

Result: Rapport prevented all known CoreFlood's attacks against eBay.

Summary

Rapport prevented all known attacks against eBay. The credentials under the Rapport's protection were successfully transmitted to the target without a danger of a theft. In case of MBR Torpig, Rapport prevented not only the data theft but also prevented its phishing attempts. Other malware did not display phishing pages.

Malware	Testing result	
	Credentials theft	Phishing
NetHell	PREVENTED	N/A
SilentBanker	PREVENTED	N/A
Wsnpoem	PREVENTED	N/A
Papras	PREVENTED	N/A
MBR Torpig	PREVENTED	PREVENTED
Torpig	PREVENTED	N/A
CoreFlood	PREVENTED	N/A

About Matousec – Transparent security

Matousec – Transparent security is a group of talented individuals with unique skills and knowhow on the field of computer security, especially in topics related to the security and the protection of Windows desktops, Internet security, security software design, reverse engineering and malware prevention, detection and analyses.

Since establishment of our group, we have focused on analyses, testing and design of security related software that runs on Windows NT platforms (Windows 2000, XP, 2003 and Vista). We also have experiences with malware analyses, development of penetration tools and vulnerability research. We have provided various researches and consultations to the leading vendors of personal firewall software. We have also been involved in the design and development of various security related software.