



**Final Dispatch: Postcard Scams 2007**  
**infectionvectors.com**  
**March 2007**

**Overview**

Postcard schemes have been a common sight in the inboxes of Internet mail users for years. A greeting like the following is often employed:

<p>You have just received a virtual postcard from a family member! You can pick up your postcard at the following web address:</p>
--

Although the test above came from a very real message, we (as both recipient and researcher) will not necessarily ever know who actually sent the message that is referenced above. Nor will we know with any certainty who coded the file that is downloaded as a result of complying with the mailed request and is referred to as “malware” later in this text. We can assume that the message was not initiated by a family member, however, that is not necessarily true. We will certainly never understand the intentions of the person constructing the message, although as researchers we make a number of “educated guesses.” This report examines some of the things we do know about postcard scams and relates them to the larger world of email fraud, which includes phishing.

**The Edge**

The “postcard” scam involves a simple premise: tell someone a friend or family member has sent them a digital postcard from a well-known web site and wait for the target to download and execute it. The postcard itself is real (as much as anything on the Internet is) and true enough – there is a greeting on the Internet awaiting our retrieval. Although the location/URL of this postcard is not completely visible (a practice that is not unusual for emailed greetings), it is provided in a format that is far from the most obfuscated that someone with web coding experience could have produced.

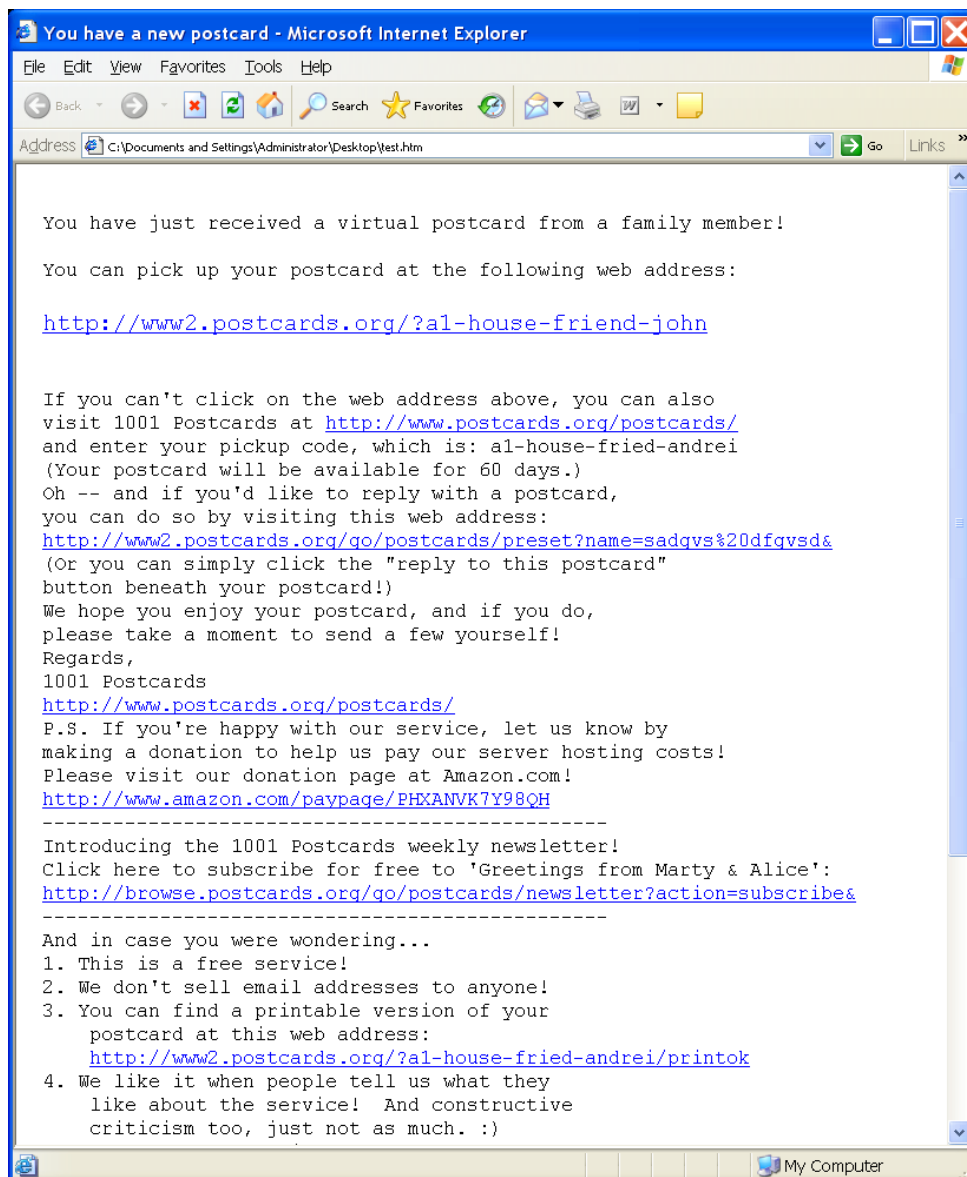
Of course, the postcard is actually a piece of malware – usually an IRC-bot. The act of downloading the “greeting” from a central server is what makes most of these distinct from other “postcard”-related schemes involving attaching an executable to the email (which was seen with Luder/Tibs in December of 2006<sup>1</sup>). Forcing the recipient to download the postcard means the emails themselves will travel without the burden of having an easily spotted IRC-bot attached to them, but does not help with users that have updated antivirus software running on their local machines. The size of most of these bots is also somewhat prohibitive for use as an attachment. The Luder worm referenced above

is about 16KB<sup>2</sup>, the IRC-bot studied here (representative of all the samples seen at infectionvectors.com is 675KB).

The premise may seem tired to those working in malware defense – this type of compromise is rare for the savvier web users of 2007 – but infections from this type of scheme are the single greatest source of inquiry to infectionvectors.com’s support practice. The promise of a greeting from a family member is an enticing ploy, and one that clearly snares a great number of Internet users.

## Predetermined

The letter itself can be viewed as a “claim ticket” of sorts for a package that is awaiting pick-up. In the case analyzed below, a server in the United States (Connecticut) serves as the post office that one must visit.



The bulk of the text is like one would receive from the actual 1001 Postcards site, down to the request for donations (which links to the real Amazon.com donation site). In this way, much of the story told by the email is true; in fact, none of the visible text can be labeled explicitly false on its face (although, the presence of two distinct postcard pickup codes is a tip-off that the email is a forgery – given that the reader believes the intent of the sender was to make the recipient believe the message was crafted by 1000 Postcards). If one was to check the real postcard site for the various greetings that have supposedly been created (“a1-house-friend-john” or “a1-house-fried-andrei”), they would find the codes to be incorrect. There were no actual electronic postcards waiting for someone who typed the code in manually at the time of message receipt.

If, however, one clicks the link in the email message, they are not taken to the true “1001 Postcards” site, but to roxydoll12.com:

```
<a href="http://roxydoll12.com/postcard/postcard.exe" target="_self">
```

From here, the “postcard” is downloaded – all that is remaining is for the user to open the package. The line above was extracted from the HTML/JavaScript used to code the email message itself. Most of this content would be invisible to the casual reader.

A second site (<http://67.15.207.206/%7Efelix/postcard.exe>) was provided by the email, towards the bottom of the message. It is the disguised target of the “preset?name...” link. The “%7” is, of course, the “~” symbol, common for user home pages of large ISPs. The address, 67.15.207.206 is registered to Everyones Internet of Houston, Texas (USA). The interesting correlation to the rest of the email is that in the header, the email server is listed as:

```
X-AntiAbuse: Primary Hostname - cpanel.ev1servers.net  
X-AntiAbuse: Original Domain - -----  
X-AntiAbuse: Originator/Caller UID/GID - [500 501] / [47 12]  
X-AntiAbuse: Sender Address Domain - cpanel.ev1servers.net
```

The Return-Path pointed to 209.85.35.10, also an Everyones Internet (ev1servers.net) owned IP address (Ontario). There is no suspected involvement, of course, between the scammer and Everyones Internet (all of the information above could certainly have been forged – the ease with which decoys can be added to such schemes further impedes our search for the truth). Moreover, as will be discussed later, deceitfully invoking the names of legitimate businesses such as Everyones Internet and 1001 Postcards may have lasting effects on the respective groups’ reputations.

The “~Efelix” link returned a 404 (unavailable) when researched. It simply points to either a slip in the scrubbing of the document before distribution, or the number of distractions a coder will implement to throw researchers off the course. The visible text of the message also showed a “sender-ip” of “172.211.194.127,” which is registered to AOL (UK) and is believed to be simply a red herring.

More clues inside the HTML of the message include the possible use of Outblaze mail services to develop the scam:

```
<form action="/scripts/mail/Outblaze.mail" method="post"
      name="inBoxMessages"></form>
```

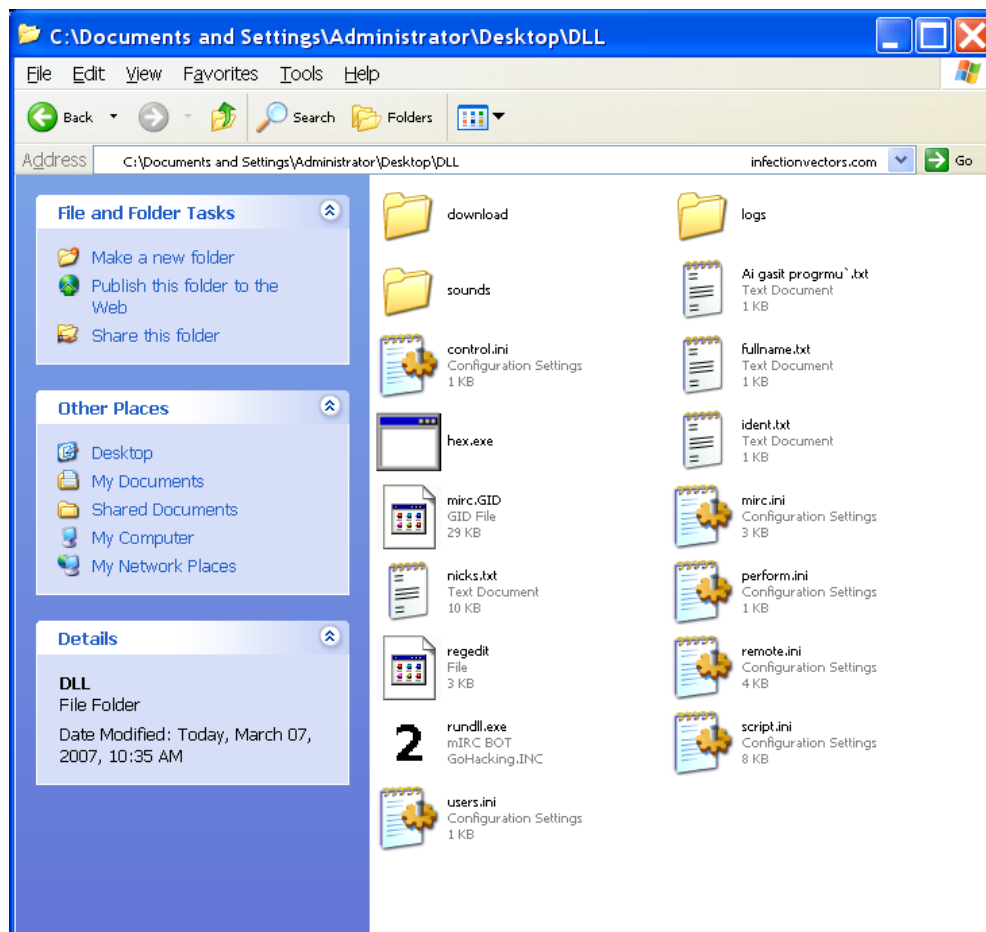
And possibly the directory structure of the machine that was used to craft the message:

```
<link type="text/css" rel="stylesheet"
      href="shit/hack/read.mail_files/getCSS.css">
```

None of these items can be conclusively linked to this iteration of the scam (i.e.: they could be forged or remnants of someone else's distribution of a similar scam) or even the person that sent these emails (for the same reasons). They again go to show some of the difficulty involved in tracking down such criminals on the Internet.

### Sendings<sup>3</sup>

The downloaded file is a single executable (postcard.exe), which is a self-extracting RAR archive. The content of the "package" includes a single directory, which in turn houses three directories and thirteen files.



The contents can be seen in the image above. It includes the three empty folders:

`\dll\download`

`\dll\logs`

`\dll\sounds`

And various files:

`ai gasit progrmu'.txt`

`control.ini`

`fullname.txt`

`hex.exe`

`ident.txt`

`mircl.GID`

`nicks.txt`

`perform.ini`

`regedit`

`remote.ini`

`rundll.exe`

`script.ini`

`users.ini`

The mIRC and IRC control files will not be discussed, as they have offer nothing unique to the IRC-bot discourse and have been analyzed as part of previous reports.

The entire “\dll” directory is unpacked to: “c:\windows\system32\drivers\nVIDIA\” via SFX script, which silently places the malware on the victim’s machine once he or she opens the “postcard.” Immediately upon installation, the script also executes the file, “rundll.exe<sup>4</sup>.” This file, identified with the “2” icon and a blatantly correct description of “mIRC BOT” to the casual viewer calls the other files, as needed, including “hex.exe.”

0018031A	00598F1A	0	About mIRC
00180336	00598F36	0	MS Shell Dlg
001803CE	00598FCE	0	romanian hacker
00180426	00599026	0	2003-2004 GoHacking.INC.
00180478	00599078	0	Licensed to:
001804B0	005990B0	0	Fuck the license

Although the strings analysis referenced a date of 2003-2004, this piece of code appears to be more recent than that.<sup>5</sup> The file itself is a customized copy of mIRC, the popular IRC client. It draws from the accompanying configuration files to ensure that the compromised machine connects to a command and control server to await instructions from its master. It is common to assume that the master is the creator of the bot, however, with the known sale of malware on the Internet<sup>w</sup> there is certainly no guarantee of that.

At this point, all we can safely assume about this application is that the creator of the code intended it to be used to take control of a machine via IRC channels. The sender of the email and the person responsible for posting the linked content (the postcard.exe file) are likely connected (if not the same person). There is no limit to what could be done with a PC compromised with this software as the mIRC-bot could easily be instructed to download and execute any piece of code the controller wished.

More clues from the package include the use of WindowHide, more specifically the Window v1.2 application, used to make Windows visible and invisible to the desktop viewer. The application itself is not considered malware, however, one can surmise that a

malware coder may include this file to make the mIRC bot window invisible. By analyzing the configuration script of the bot, this is confirmed. That may be more than ample evidence to an analyst that the intentions of the “postcard” sender were not good – as only malicious actions need to be kept hidden from the target.

## Limits

Just as with phishing scams, where every financial institution in the world is (or will be) a target, the e-postcard companies of the world can all expect to be used in schemes like that described above.

```
<title>I sent you an eCard from AmericanGreetings. Happy Valentine's
Day !</title>
[content removed for brevity]
<a href="http://86228.americangreetings.net/uk/viewcard.html">
http://www.americangreetings.com/customer/emailus.pd?source=ag999</a><b
r>
```

A server that appears to be in Spain (given the IP address) disguised as the “Your Postcard” site (which actually was for sale, without postcard content up at the time of this writing):

```
<a href="http://213.221.110.73/~oheimann/postcard.exe">here</a> to
receive your animated postcard! </strong><br><br>
<strong>=====</strong><br>
Thank you for using <span class="style1">www.yourpostcard.com</span> 's
services !!!<br>
```

Although the effect of phishing on branding has been discussed, the use of postcard sites, which do generate revenue for their owners, has not. The owners of the respective trade and service marks likely feel affected, no matter the result of the brand infringement. That is, even if the sender of the “postcards” has very benevolent intentions or none of the recipients actually downloads and executes the IRC-bot, the companies behind the forged email feel harmed.

The affect of widespread phishing efforts on branding has only increased since discussed in an infectionvectors.com report on email crime<sup>6</sup> in 2005. Organizations such as the Brandprotect<sup>7</sup> have made email-borne fraud that infringes on corporate brands a primary focus. There is little doubt that phishing needs to be a concern of every corporation – whether they actually do business themselves via email or not.

As is the case with many con artists, the phisher is dependant on the legitimate company – that the corporation built a good relationship with its customers. This capital is of course exploited, and eventually eroded by the criminal, destroying the assets of their illicit enterprise and being forced to expand the net to include trademarks of more and more businesses, of all sizes. That parasitic relationship is the reason that every organization can consider themselves potential targets of the phishers.

## Notes

1. Luder circulated around New Year's Eve with special greetings to all recipients. Check it out on the F-Secure Malware Information Pages: [http://www.f-secure.com/v-descs/luder\\_a.shtml](http://www.f-secure.com/v-descs/luder_a.shtml).

2. Known as Nuwar at McAfee, the size is included with their write-up at: [http://vil.nai.com/vil/content/v\\_140835.htm](http://vil.nai.com/vil/content/v_140835.htm).

3. By inserting "envois" into the "Original text" box on the Google text translation page ([http://translate.google.com/translate\\_t](http://translate.google.com/translate_t)), and selecting "French to English" from the pull-down prior to clicking "Translate," one gets "sendings." "Dispatches" is often seen in other texts as the translation; however, the use of Google's answer seemed more appropriate to the author.

4. This file would likely be the only one considered true "malware" by the bulk of researchers as the others are text/configuration files or tools that have legitimate purposes (HideWindow.exe). For research/cataloging purposes, the MD5 sum for this IRC-bot is: AB9A199958394051099922B000ABAFB3.

5. A search for the MD5 sum revealed this piece of code has been catalogued before (2006) by Castle Cops: [http://www.castlecops.com/t173953-MD5\\_ab9a199958394051099922b000abafb3\\_rundll\\_exe.html](http://www.castlecops.com/t173953-MD5_ab9a199958394051099922b000abafb3_rundll_exe.html).

6. See the email crime rundown, "Mail Call, Part 4" at: [http://www.infectionvectors.com/library/mail\\_call\\_pt4\\_iv.pdf](http://www.infectionvectors.com/library/mail_call_pt4_iv.pdf)

7. The company is part of the Branddimensions group (<http://www.branddimensions.com/>): For information on phishing and brand protection: [www.bdbrandprotect.com](http://www.bdbrandprotect.com). For a fact sheet on phishing: [http://www.brandprotect.com/solutions\\_3.html](http://www.brandprotect.com/solutions_3.html). For a FAQ on phishing: [http://www.brandprotect.com/resources/bd-protect\\_phishing\\_FAQ\\_1-3.pdf](http://www.brandprotect.com/resources/bd-protect_phishing_FAQ_1-3.pdf) For excellent whitepapers/industry reports available to the public on their site (which are well worth reading for anyone interested in the real business effects of phishing: <http://www.brandprotect.com/whitepapers.html>. Significantly, BD-BrandProtect uses the term "attack" to describe phishing events and combats the problem with dedicated honeypots, analysts, and incident response teams.

## Additional References

John P. Mello Jr. "Security Firms Bust Malware-For-Sale Racketeers." TechNewsWorld 20 April 2006. <http://www.technewsworld.com/story/EOEWqNIsZpOBNv/Security-Firms-Bust-Malware-for-Sale-Racketeers.xhtml>.

infectionvectors.com "Weaponized: Virulence and Malware" September 2006. <http://www.infectionvectors.com/vectors/weaponized.htm>.

## Appendix: Additional Information for the Curious

### More clues about the coder's development environment

From the "regedit" file included with postcard.exe:

```
[HKEY_CURRENT_CONFIG\Software\Microsoft\Windows
NT\CurrentVersion\Windows] run = "D:\neterminate\BoT\DLL\rundll32.exe"
[HKEY_CURRENT_CONFIG\Software\Microsoft\Windows\CurrentVersion\Windows]
run = "D:\neterminate\BoT\DLL\rundll32.exe"
```

Possibly another look into the directory structure the developer was working under for this bot.

### MD5 of the rundll.exe file

```
rundll.exe
AB9A199958394051099922B000ABAFB3
```

### JavaScript from the email footer

```
<script language="javascript" type="text/javascript"> <!--
imgblocked="" ;
if (imgblocked=="yes") document.write('<tr><td class="f"
style="background:#fff"><hr>HTML graphics in this message have been
blocked. [
```