



**Mail Call: Criminal Email Businesses**  
**gordon@infectionvectors.com**  
**May 2005**

## **Overview**

The general distrust over email warnings is well founded; mass mailings went from nuisance to international crime effort in an instant. Today email-borne fraud and malware distribution is one of the most common occurrences on the Internet, one that threatens ecommerce and every home web surfer with the ever-profitable business of compromising computers and stealing personal data. This paper examines the nature of email-based crime and a few specific examples of existing threats.

## **The Inbox**

The reason any untargeted scam makes it to one's Inbox can generically be summarized in one word: money. To make money the scammer may be angling for personal information or a direct transfer of funds, but in the end the vast majority of crime is committed for something that will be liquidated. Without at doubt there are crimes committed for reasons of vandalism, simply to compromise machines for the "sport" of it, and pure curiosity. However, the rise of phishing scams is virtually all a result of con artists attempting to raise revenue in their medium of choice.

There are no particular targets of phishing attempts, just as with most spam. Even the sender may never know exactly where their messages get to or who reads them. It is a completely anonymous crime in many ways, which is ironic, given that identity theft is often the goal of the criminal. What would seem like a very personal transgression is actually one of the most disconnected actions at its heart. This type of false front is the essence of the scam.

A good phishing attempt is not at all what it appears, like any good con effort. If fraud signals its true nature, it is a failed attempt. It is a message where every piece of information that can be forged probably is forged.

Received: from [193.140.151.6] (helo=altay.adm.deu.edu.tr) by mx.mailix.net with esmtp (Exim 4.24-VA) id 1DNEYv-0000hc-Tp for email@infectionvectors; Sun, 17 Apr 2005 11:32:06 -0700

Received: from altay.adm.deu.edu.tr (localhost.adm.deu.edu.tr [127.0.0.1]) by altay.adm.deu.edu.tr (8.13.1/8.12.11) with ESMTP id j3HIWTXm045024 for <email@infectionvectors>; Sun, 17 Apr 2005 21:32:29 +0300 (EEST) (envelope-from nobody@altay.adm.deu.edu.tr)

Date: Sun, 17 Apr 2005 21:32:29 +0300 (EEST)  
Message-Id: <200504171832.j3HIWTU8045021@altay.adm.deu.edu.tr>  
To: email@infectionvectors  
Subject: Fraud Detected On Your Account  
From: Service Team<service@BankofAmerica.com>

In the case above, the only pieces of information that can be trusted are that it was destined for the recipient, a fact only evidenced by the fact that it appeared in the correct Inbox, and that the last hop identifies the correct mail relay (simply a function of SMTP, many spammers will forge additional "Received:" lines to fool scanners). This does not even consider the content of the message, which is a fraud in every sense except that the sender really does want the recipient's personal information.

The problems of unsigned (digital signatures), unencrypted email and the inherent insecurity of SMTP have become apparent to many Internet users. Even otherwise non-technical users are likely to have an inherent distrust of email messages, whether because of personal experience with phishing and mass mail worms or because of warnings from financial institutions, television news, and their ISPs. The exercise of deciphering what is reliable and what is not in an email message is not one undertaken by the average user however. The search for what is true and what is false when it comes to the Inbox has been replaced by a wholesale rejection of email-based requests.<sup>1</sup>

### **Brand Loyalty**

Mass mailers have been eroding the general trust in email for years. ILOVEYOU<sup>2</sup> and Melissa<sup>3</sup> have left a legacy of SMTP-mobile malware. When Beagle spoofs<sup>4</sup> "support@yourdomain.com," and the word gets out on the worm (admittedly slow in coming for many viruses), the average user base is less inclined to trust anything from support, admin, or anything else @yourdomain.com. Even within private organizations, the use of email to make requests and pass important information is spoiled.

Damage to brand names and companies has occurred within the spam arena already. One of well known instance of this problem is the Rolex story<sup>5</sup>. Beginning in late 2004, an explosion of spam touting cheap Rolex-like watches flooded the Internet from discount shops. The impact on the branding of Rolex when associated with such a product/producer could be tremendous, certainly more than they could expect to recoup if the company ever successfully sued the spammers.

Similarly, phishing hurts brand names across the board. Victims of fraud may associate the brand with poor security, blaming the company (also a victim in the attack) for the actions of a criminal. The consumer may also hold the company responsible for the loss, something that has proven to be a common problem. The majority of users now believe that the company that is used as the bait in phishing attempts has responsibility for the results of the scam.<sup>6</sup>

The impact of phishing may well be to severely Internet-based business as a whole, not just the email notifications, which have all but been taken away from online companies as

a means of interacting with customers. As phishing scams become more elaborate and users become more skeptical of all web-based forms (the necessary complementary medium of most phishing today), the future of e-commerce could be in jeopardy.

### **No Stamp Required**

The criminal element's use of email is not limited to trolling for personal credit information. Well before most users knew anything about phishing they knew about mass mail worms, or at least the idea that unsolicited attachments could be dangerous. As mentioned above, the ILOVEYOU and Melissa worms made some of the largest virus headlines and allowed for significant coverage of email security issues. These worms, however, did not seek to steal passwords or bank account data.

The professional virus writer has made great strides in the few years since those mail-based threats. SoBig and Beagle have paved the way for any number of exploits based on mass mailings. To date, the Beagle worm, beyond installing a backdoor to compromised machines, has successfully installed the following types of applications:

- Keystroke Loggers
- Password Stealer
- Email/Spam Relay
- Bank Account Information Grabber
- Security Software/Update Killer

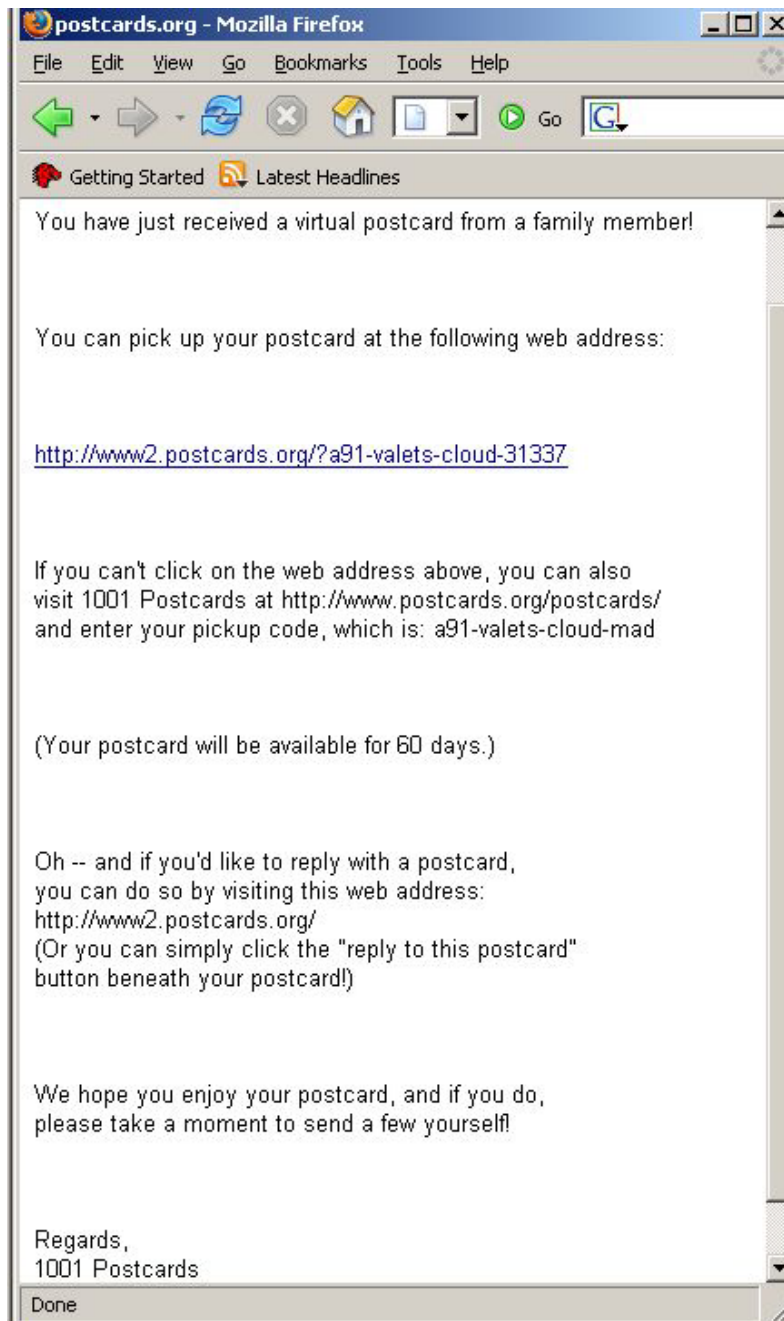
The MyDoom family, which now includes hybrid mailer/bot Mytob<sup>7</sup>, and Netsky provided some of the broadest virus coverage ever in 2004 when their exponential growth (and "war" that included Beagle) lead to exceptionally high numbers of reports and infections worldwide. When worms such as these infect machines, leaving an open backdoor for the authors, there is virtually no end to what the compromised boxes can be used for – from selling like a commodity to others simply in need of anonymous clients to using as spam engines and nets for bank account data. On a smaller scale, non-self-propagating Trojans are sent to thousands of users' mailboxes everyday. These range from applications that simply seek to steal software keys to IRC-directed remote control programs.

Mass mail continues to be a simple (from a coder's perspective) and effective means of reaching a high number of users. As such, even as anti-virus analysts predict the demise of the mass mailer worm, there will be plenty of choices for users to make when it comes to malicious attachments in the future.

The following examples review the tactics and intentions of a few criminally-minded mass mail efforts.

## The Postcard<sup>8</sup>

One of the simplest efforts to entice a user into downloading a Trojan is the “postcard” routine seen in 2005. The premise is to send out a short notice stating that the recipient has been sent a virtual post card from a friend, family member, etc. and that they need to download the card to view it on their local machine. Most samples that have been received are well written, in that they do not contain any obvious spelling or grammatical errors that often tip users to a phishing attempt.



The letter shows the following last hop data (an address and domain registered to Ontario, Canada), which is not appended with additional “received from” lines as many spammers use to obfuscate the source:

```
Received: from [69.28.228.90] (helo=wubrothers.ca)
```

For the curious, there was no actual postcard available if one went to the address shown and used the “pickup code.” This looks very much like a legitimate notification from any of the free web greeting card services. There is an advertisement for sending reply postcards, alternate instructions for viewing, and its simple message is without spelling errors.

Of course, the notification is a scam, and in the HTML source one can see the true destination of retrieval request:

```
<p align="left"><font size="2" face="Arial">You can pick up your postcard at
```

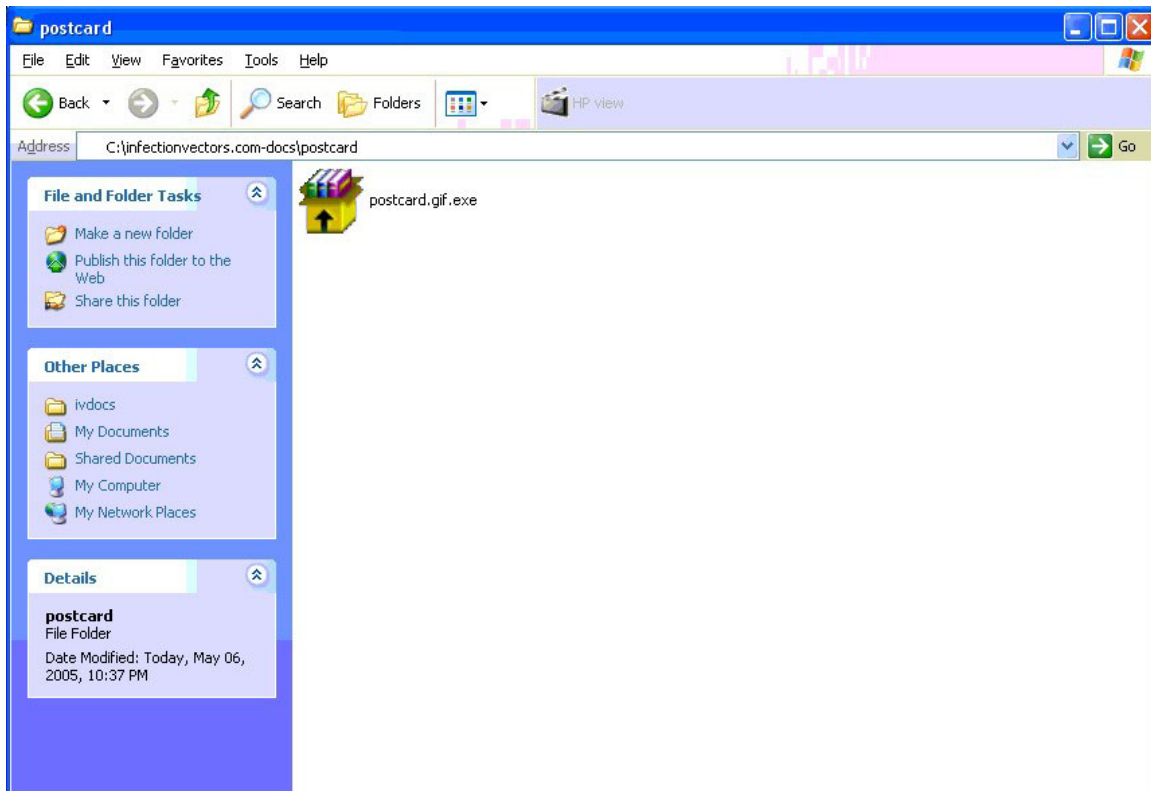
```
the following web address:</font></p>
```

```
<p align="left"><font color="#FFFFFF" size="2" face="Arial">.</font></p>
```

```
<p align="left"><font size="2" face="Arial"><A href="http://www.fumatoru.go.ro/postcard.gif.exe" target=_blank>http://www2.postcards.org/?a91-valets-cloud-31337</A></font></p>
```

```
<p align="left"><font color="#FFFFFF" size="2" face="Arial">.</font></p>
```

This site, fumatoru.go.ro, is as the TLD implies, registered to a group in Bucharest, Romania and was hosted at 81.196.20.134. The file that is downloaded, “postcard.gif.exe,” is 915KB, rather large for most malicious code, although the size will be soon explained by the contents of the “postcard.” This size would have been prohibitive in the days when dial-up connections dominated the home Internet market, but is quite tolerable for a user of broadband. In addition, a dial-up user expecting a personal greeting from a family member may be more than willing to wait the required time for the file. In any case, the UPX-packed file that is downloaded appears to be a WinRAR archive, based on its icon:



There is no mechanism to automatically launch the executable, the user must initiate that. In cases where a user has the extensions of known files hidden, that may be a foregone conclusion. Even with the general awareness about double-clicking unknown executables, it is likely that a user that has gone this far will open the file. When that occurs, the “postcard” installs a number of files onto the device, which will certainly carry a greeting, albeit not the type the user hoped for.

The coder of this particular sample did not ensure that the application would install correctly on every platform, and in fact, will not properly place itself in the Windows %System% directory. In cases initially discovered when attempting to launch the file on a standalone Windows 9x machine (also used in addition to the XP device seen in the screenshot above), the program drops a copy of itself into:

```
C:\Program Files%\systemroot%\system32\
```

As one can see, the install routine interprets the “%systemroot%” literally. When this copy of the application is run (a slightly smaller copy that no longer has the %systemroot% installation routine, 847,743 bytes unpacked vice 982,140) the load is functionally correct. The installation created a directory in the root of the C: drive (or local install root) named “Recycler.” Within this directory is a file named “svchost.exe” that is also called by a Registry hook to start the application each time Windows loads:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]  
"GNP Generic Host Process"="C:\\RECYCLER\\svchost.exe"
```

Also in this directory are nine INI files and three additional directories named, “download,” “sounds,” and “logs.” If the suspense is still gripping the reader, the svchost.exe file is mIRC, and the customizations direct the client to an IRC channel where it awaits commands, likely from one or more of the four handles it notifies upon startup (which appear to correspond to the 8 “users” in the users.ini). There are 18 servers listed in the servers.ini file and 13,132 NICKS in the nicks.txt file. From the mirc.ini configuration, we get a few clues as to how this is laid out. Most of the initial information is generated by random selection when the mIRC script begins, such as user (taken from nicks.txt) and the NICK (random, as established in script):

```
[mirc]
user=cream}{
nick=Vy3sIo1bX
anick=Vr0tBq8tA
email=M
host=Helsinki.FI.EU.Undernet.orgSERVER:Helsinki.FI.EU.Undernet.org:6667
GROUP:Underet
[files]
servers=servers.ini
finger=finger.txt
urls=urls.ini
addrbk=addrbk.ini
trayicon=mirc.ico
```

The icon used, “mirc.ico” is blank, it will display no obvious clue to the machine’s operator. Startup controls are defined by the script.ini file, now well-known to mIRC users as generally malicious, which assures that notification and proper connections to the server/channel are established. The last line of the script helps identify the compromised machine in the IRC channel:

```
n124=alias ver return :_:_: _R_unning _o_n :_:_: ( _1_W_indows: $os
_):_:_: ( _0_S_crew-_B_oT _v_3.1.3.3.7 _b_y _M_AD @_ ):_:_: ( _1_O_ntime:
$uptime(server,1) _):_:_:
```

This type of malware is far from new, mIRC script exploits, specifically, the “script.ini” transfers via auto-DCC-Get have floated around for a number of years. The delivery however, is now reaching a new level – taking the form of email scams designed to hook non-IRC users and their computers. To many reading a report such as this, the use email may not appear significant, as worms and phishers have been dealing in it for years. However, when considered in the same fashion as Beagle or MyDoom, it is important: no matter how many warnings are issued, when malware is delivered in the exceptional volume afforded by spamming tactics, there will be profitable infections.

### **Important Message**

When it comes to creating an anonymous spam network, one of the most flagrant social engineering attempts belongs to a Beagle/Mitglieder-like application named Lohav<sup>9</sup> (by Sophos). The email that accompanies this Trojan makes the following claim:

Dear user user@infectionvectors

Your account has been used to send a large amount of spam messages during the recent week.

Most likely your computer had been infected by a recent virus and now runs a trojaned proxy server.

We recommend that you run in attach free trojan and spyware remover software to keep your computer safe.

Archive password: 333666

Best regards,  
Support team

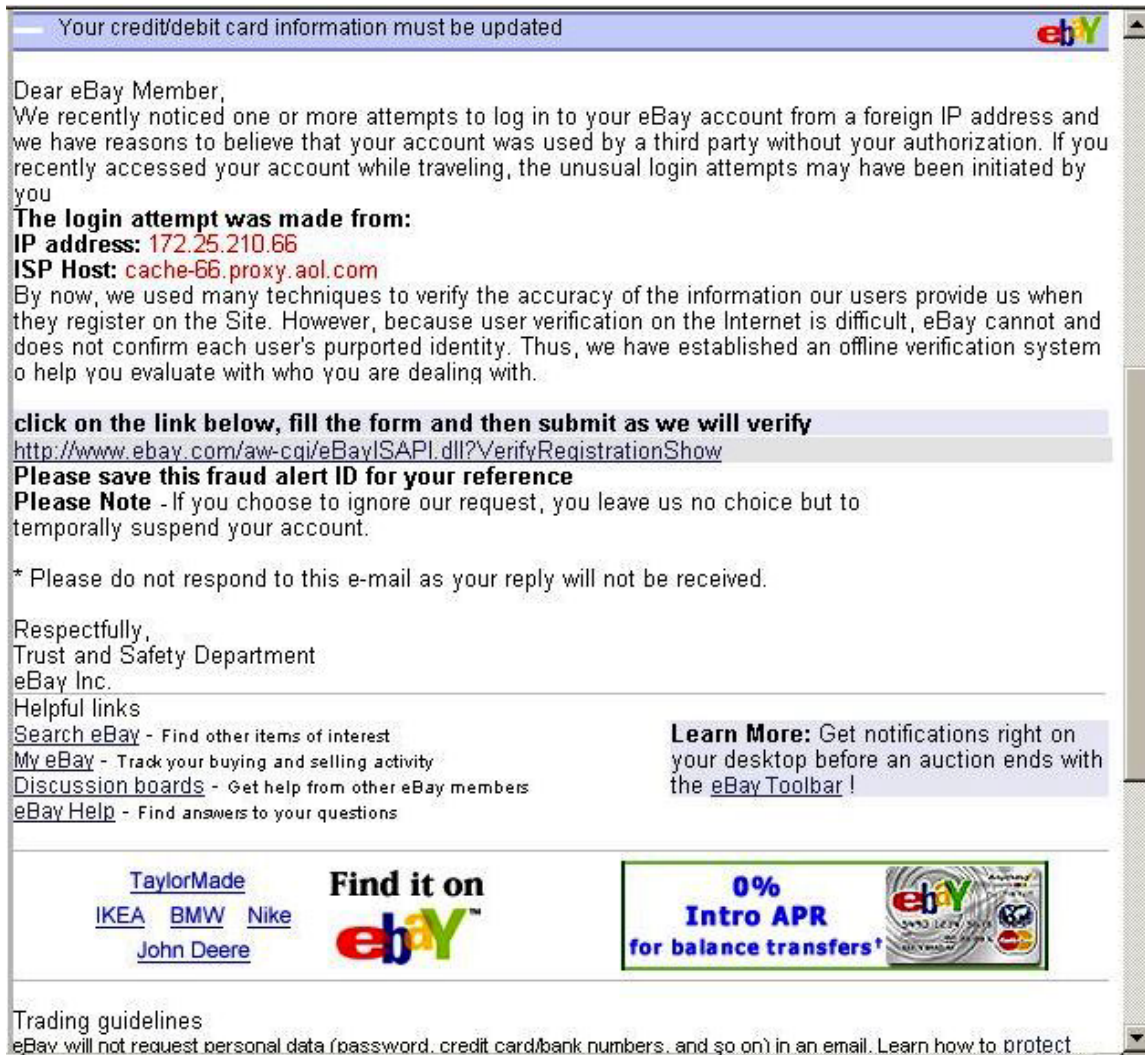
As one may have already guessed, the “spyware remover” is actually a spam relay that registers the infected computer with the authors and attempts to download additional malicious code. Moreover, the Trojan disables a great deal of security-enhancing software and blocks access to applications like Regedit, just in case the user had ideas of removing the malware manually.

The FSG-protected Lohav establishes itself as “spykiller.exe” in some email messages (as was analyzed for this report the attachment name was “setup.exe” although it dropped a copy of the Trojan as “spykiller” on the test machine in C:\spykiller.exe\ as it is coded to do as well as dropping a copy as “winhost.exe” in the %System% folder). The password is required to install the application (which comes complete with a GUI install for the user’s peace of mind), as the contents of the package are encrypted. This protection ensures that anti-virus software does not immediately grab the program, as the malicious parts are hidden from the prying eyes of the security applications.

Lohav and its Beagle cousins are efforts to build the very infrastructure that sends out more threats like themselves, less dangerous spam, and worms. They immediately register the machine with the controller and place additional damaging software on the affected computer, software that often waits to steal additional information/keystrokes from the operator. Traditional phishing and Nigerian 419 scams almost seem tame by comparison.

### **Very Important Message**

The most common scare tactic employed by phishers is the need to “update account information.” Threats such as “suspension of your credit card” are passed around by the millions. Unfortunately for the criminals, the more elaborate they attempt to make the requests, the more skeptical many users become. This is especially true in cases where grammar and spelling problems stand out to the reader. Consider the recent sample below:



Clearly designed for non-technical readers (as the IP address given is from RFC 1918 private ranges which are not routable on the Internet), the email<sup>10</sup> has no shortage of logos and “official” tags.

Of course, the code underneath the colorful exterior reveals the true destination of the “user verification.”

```
<p><a href=3D"http://verify-your-account-com.keymachine.de/signin.ebay/signin.ebay.com/acounts/memb/avncenter/dll187443/BayISAPI.dll/sign_in.htm">  
<font size=3D"2">http://www.ebay.com/aw-cgi/eBayISAPI.dll?VerifyRegistrationShow</font></a></td>
```

The phishing page looks real enough, as it is lifted almost entirely from the actual ebay site. The requests it makes go from a simple login through very detailed personal information, which eventually deposits the user on the real ebay site. These types of scams are typical of phishing exploits and can be replicated with minimal investment on the criminal’s part. In fact, it is common for single sites to host numerous scams at any

given time, allowing the criminal to deliver millions of varied email warnings and reap the rewards in very little time, provided the email infrastructure noted above is in place.

The creation of a spamming network is an integral piece of the criminal puzzle, without that anonymous and widespread platform, seeding both additional malware and phishing attempts is much more difficult. Email itself is a ubiquitous tool, making it a good target for criminals as well. To that end, it is no surprise that email-based scams have received so much attention, nor that the attention will not cease until there is a solid means of authenticating email or users give up on the tool altogether.

More information on email scams and malware defense is available at the source of this report: <http://www.infectionvectors.com>. In addition, there is information specific to phishing and related email issues at <http://www.infectionvectors.com/vectorspaces.htm>.

## References

1. Users have begun to replace critical email investigation with wholesale dumping of unsolicited email requests:  
“Caught in a phishing trap” Matt Hines CNET News.com 17 November 2004 ZDNet  
[http://news.zdnet.com/2100-1009\\_22-5453203.html](http://news.zdnet.com/2100-1009_22-5453203.html)
2. ILOVEYOU information: CERT Advisory on the Love Letter Worm  
<http://www.cert.org/advisories/CA-2000-04.html>
3. Information on the macro known as Melissa:  
<http://service1.symantec.com/sarc/sarc.nsf/html/W97M.Melissa.W.html>
4. Beagle information can be found at infectionvector.com:  
<http://www.infectionvectors.com/malagents/beagle.htm>
5. “‘Rolex’ spam taps into bling-bling culture” Will Sturgeon Silicon.com 25 October 2004 ZDNet  
[http://news.zdnet.com/2100-9588\\_22-5425119.html](http://news.zdnet.com/2100-9588_22-5425119.html)  
“Spam – your brand, your problem?” Silicon.com 25 October 2004  
<http://comment.silicon.com/0,39024711,39125278,00.htm>
6. Users are holding companies accountable, as found by MailFrontier:  
MailFrontier Press Release, 10 November 2004  
[http://www.mailfrontier.com/press/press\\_finance.html](http://www.mailfrontier.com/press/press_finance.html)
7. MyDoom/Mytob information available at infectionvectors.com  
<http://www.infectionvectors.com/malagents/mydoom.htm>  
<http://www.infectionvectors.com/malagents/mytob.htm>
8. Nod and apology to Jacques Derrida.
9. Lohav Information  
<http://www.sophos.com/virusinfo/analyses/trojlohavq.html>
10. ebay scam also catalogued by APWG:  
[http://www.antiphishing.org/phishing\\_archive/04-18-05\\_eBay/04-18-05\\_eBay.html](http://www.antiphishing.org/phishing_archive/04-18-05_eBay/04-18-05_eBay.html)

## Additional Information

Lohav connects to the following to register the infected computer (do not follow links):

00005EFF	00405EFF	<a href="http://paromy.ru/_old_img/in.php">http://paromy.ru/_old_img/in.php</a>
00005F20	00405F20	<a href="http://www.ladywears.com/in.php">http://www.ladywears.com/in.php</a>
00005F40	00405F40	<a href="http://nine-one-one.ca/img/in.php">http://nine-one-one.ca/img/in.php</a>
00005F62	00405F62	<a href="http://68.24.54.122/in.php">http://68.24.54.122/in.php</a>
00005F7D	00405F7D	<a href="http://64.12.212.12/in.php">http://64.12.212.12/in.php</a>
00005F98	00405F98	<a href="http://www.evocreations.com/img/in.php">http://www.evocreations.com/img/in.php</a>
00005FBF	00405FBF	<a href="http://sexyforum.ru/in.php">http://sexyforum.ru/in.php</a>
00005FDA	00405FDA	<a href="http://janda.com/in.php">http://janda.com/in.php</a>
00005FF2	00405FF2	<a href="http://www.cardgoods.com/img/ini.php">http://www.cardgoods.com/img/ini.php</a>

And downloads additional code from:

00006037	00406037	<a href="http://www.cardgoods.com/img/1.exe">http://www.cardgoods.com/img/1.exe</a>
----------	----------	---

## Processes Killed by Lohav

OUTPOST.EXE	NETMON.EXE	RESCUE.EXE
SAVSCAN.EXE	NETSCANPRO.EXE	RESCUE32.EXE
navapsvc.exe	NETSPYHUNTER-1.2.EXE	RRGUARD.EXE
NPROTECT.EXE	NETSTAT.EXE	RSHELL.EXE
ccApp.exe	NISSERV.EXE	RTVSCN95.EXE
ccEvtMgr.exe	NISUM.EXE	RULAUNCH.EXE
SymWSC.exe	CFIAUDIT.EXE	SAFEWEB.EXE
NavShExt.dll	LUCOMSERVER.EXE	SBSERV.EXE
NMAIN.EXE	AGENTSVR.EXE	SD.EXE
NORTON_INTERNET_SECU_3.0_407.EXE	ANTI-TROJAN.EXE	SETUP_FLOWPROTECTOR_US.EXE
NPF40_TW_98_NT_ME_2K.EXE	ANTI-TROJAN.EXE	SETUPVAMEVAL.EXE
NPFMESSENGER.EXE	ANTIVIRUS.EXE	SFC.EXE
NPROTECT.EXE	ANTS.EXE	SGSSF32.EXE
NSCHED32.EXE	APIMONITOR.EXE	SH.EXE
NTVDM.EXE	APLICA32.EXE	SHELLSPYINSTALL.EXE
NVARCH16.EXE	APVXDWIN.EXE	SHN.EXE
KERIO-WRP-421-EN-WIN.EXE	ATCON.EXE	SMC.EXE
KILLPROCESSSETUP161.EXE	ATGUARD.EXE	SOFI.EXE
LDPRO.EXE	ATRO55EN.EXE	SPF.EXE
LOCALNET.EXE	ATWATCH.EXE	SPHINX.EXE
LOCKDOWN.EXE	AVCONSOL.EXE	SPYXX.EXE
LOCKDOWN2000.EXE	AVGSERV9.EXE	SS3EDIT.EXE
LSETUP.EXE	AVSYNMGR.EXE	ST2.EXE
CLEANPC.EXE	BD_PROFESSIONAL.EXE	SUPFTRL.EXE
AVprotect9x.exe	BIDDEF.EXE	LUALL.EXE
CMGRDIAN.EXE	BIDSERVER.EXE	SUPPORTER5.EXE
CMON016.EXE	BIPCP.EXE	SYMPROXYSVC.EXE
CPF9X206.EXE	BIPCPEVALSETUP.EXE	SYSEDIT.EXE
CPFNT206.EXE	BISP.EXE	TASKMON.EXE
CV.EXE	BLACKD.EXE	TAUMON.EXE
CWNB181.EXE	BLACKICE.EXE	TAUSCAN.EXE
CWNTDWMO.EXE	BOOTWARN.EXE	TC.EXE
ICSSUPPNT.EXE	NWINST4.EXE	TCA.EXE

DEFWATCH.EXE	NWTOOL16.EXE	TCM.EXE
DEPUTY.EXE	OSTRONET.EXE	TDS2-98.EXE
DPF.EXE	OUTPOSTINSTALL.EXE	TDS2-NT.EXE
DPFSETUP.EXE	OUTPOSTPROINSTALL.EXE	TDS-3.EXE
DRWATSON.EXE	PADMIN.EXE	TFAK5.EXE
ENT.EXE	PANIXK.EXE	TGBOB.EXE
ESCANH95.EXE	PAVPROXY.EXE	TITANIN.EXE
AVXQUAR.EXE	DRWEBUPW.EXE	TITANINXP.EXE
ESCANHNT.EXE	PCC2002S902.EXE	TRACERT.EXE
ESCANV95.EXE	PCC2K_76_1436.EXE	TRJSCAN.EXE
AVPUPD.EXE	PCC10MON.EXE	TRJSETUP.EXE
EXANTIVIRUS-CNET.EXE	PCDSETUP.EXE	TROJANTRAP3.EXE
FAST.EXE	PCFWALLICON.EXE	UNDOBOOT.EXE
FIREWALL.EXE	PCFWALLICON.EXE	VBCMSERV.EXE
FLOWPROTECTOR.EXE	PCIP10117_0.EXE	VBCONS.EXE
FP-WIN_TRIAL.EXE	PDSETUP.EXE	VBUST.EXE
FRW.EXE	PERISCOPE.EXE	VBWIN9X.EXE
FSAV.EXE	PERSFW.EXE	VBWINNTW.EXE
AUTODOWN.EXE	PF2.EXE	VCSETUP.EXE
FSAV530STBYB.EXE	AVLTMAIN.EXE	VFSETUP.EXE
FSAV530WTBYB.EXE	PFWADMIN.EXE	VIRUSMDPERSONALFIREWALL.EXE
FSAV95.EXE	PINGSCAN.EXE	VNLAN300.EXE
GBMENU.EXE	PLATIN.EXE	VNPC3000.EXE
GBPOLL.EXE	POPProxy.EXE	VPC42.EXE
GUARD.EXE	POPCAN.EXE	VPFW30S.EXE
GUARDDOG.EXE	PORTDETECTIVE.EXE	VPTRAY.EXE
HACKTRACERSETUP.EXE	PPINUPDT.EXE	VSCENU6.02D30.EXE
HTLOG.EXE	PPTBC.EXE	VSECOMR.EXE
HWPE.EXE	PPVSTOP.EXE	VSHWIN32.EXE
IAMAPP.EXE	PROCEXPLOREVR1.0.EXE	VS1SETUP.EXE
IAMAPP.EXE	PROPORT.EXE	VSMAN.EXE
IAMSERV.EXE	PROTECTX.EXE	VSMON.EXE
ICLOAD95.EXE	PSPF.EXE	VSSTAT.EXE
ICLOADNT.EXE	WGFE95.EXE	VSWIN9XE.EXE
ICMON.EXE	WHOSWATCHINGME.EXE	VSWINNTSE.EXE
ICSUPP95.EXE	AVWUPD32.EXE	VSWINPERSE.EXE
ICSUPPNT.EXE	NUPGRADE.EXE	W32DSM89.EXE
IFW2000.EXE	WHOSWATCHINGME.EXE	W9X.EXE
IPARMOR.EXE	WINRECON.EXE	WATCHDOG.EXE
IRIS.EXE	WNT.EXE	WEBSCANX.EXE
JAMMER.EXE	WRADMIN.EXE	CFIAUDIT.EXE
ATUPDATER.EXE	WRCTRL.EXE	CFINET.EXE
AUPDATE.EXE	WSBGATE.EXE	ICSUPP95.EXE
KAVLITE40ENG.EXE	WYVERNWORKSFIREWALL.EXE	MCUPDATE.EXE
KAVPERS40ENG.EXE	XPF202EN.EXE	CFINET32.EXE
KERIO-PF-213-EN-WIN.EXE	ZAPRO.EXE	CLEAN.EXE
KERIO-WRL-421-EN-WIN.EXE	ZAPSETUP3001.EXE	CLEANER.EXE
BORG2.EXE	ZATUTOR.EXE	LUINIT.EXE
BS120.EXE	CFINET32.EXE	MCAGENT.EXE
CDP.EXE	CLEAN.EXE	MCUPDATE.EXE
CFGWIZ.EXE	CLEANER.EXE	MFW2EN.EXE
CFIADMIN.EXE	CLEANER3.EXE	MFWENG3.02D30.EXE
CFIAUDIT.EXE	CLEANPC.EXE	MGUI.EXE
AUTOUPDATE.EXE	CMGRDIAN.EXE	MINILOG.EXE
CFINET.EXE	CMON016.EXE	MOOLIVE.EXE
NAVAPW32.EXE	CPD.EXE	MRFLUX.EXE
NAVDX.EXE	CFGWIZ.EXE	MSCONFIG.EXE

NAVSTUB.EXE  
NAVW32.EXE  
NC2000.EXE  
NCINST4.EXE  
AUTOTRACE.EXE  
NDD32.EXE  
NEOMONITOR.EXE  
NETARMOR.EXE  
NETINFO.EXE

CFIADMIN.EXE  
PURGE.EXE  
PVIEW95.EXE  
QCONSOLE.EXE  
QSERVER.EXE  
RAV8WIN32ENG.EXE  
REGEDT32.EXE  
REGEDIT.EXE  
UPDATE.EXE

MSINFO32.EXE  
MSSMMC32.EXE  
MU0311AD.EXE  
NAV80TRY.EXE  
ZAUINST.EXE  
ZONALM2601.EXE  
ZONEALARM.EXE

Copyright © 2005 infectionvectors.com All rights reserved.