Lessons from Virus Developers:
The Beagle Worm History Part 2: April 25 Through August 31, 2004
Jason Gordon gordon@infectionvectors.com

Introduction

The first part of this report ("History of the Beagle Worm Through April 24, 2004") focused on the tremendous evolution shown by the Beagle worm over its first three months of life in the wild.[1] Specifically how the author appeared to take great care in testing and optimizing worm variants before releasing them. Since that time there have been more variants of the code and new uses of the boxes they infected. Beagle's lessons have extended to all computer users, not just security professionals. All machine are equally valuable in Beagle's attack, in which it simply requires an army of infected machines from which to launch the next wave of its messages. Although from this tremendous list of machines the author could single out high-profile targets to control, they are more likely all just part of the same "spam net;" all with equal positions and fulfilling the same purpose: conquer more machines, harvest more target addresses, and remove barriers that interfere with relaying additional copies of the worm.

The effects of the Beagle worm have already been felt in the security community. The innovations it has included so far (and those to come) will continue to shape policy and products. One notable addition to virus scanners, especially those used on gateway devices, is password-cracking technology[2]. Whether through OCR[3] (grabbing the password delivered in non-text/image files) or brute force cracking attempts, the need to open ciphered ZIP files has been proven to be a requirement by Beagle.

Since January 2004 the Beagle worm has compromised thousands of machines, turning them into slaves capable of relaying mail, redirecting general Internet traffic, and virtually anything the worm author could conceive of doing with them. The previous report ended the last week of April 2004, just in the midst of Beagle.X. At that time it was not known how good of a stopping point that would be in documenting the Beagle history, it was the last variant for over two months.

The Return of the Worm

Beagle.Y

Discovered July 4, 2004, Beagle.Y represented the return of the familiar worm to the virus scene[4]. The lay-off between worms (.X was released in late April) did not result in any immediate innovations. Beagle.Y looked very much like .X, continuing to carry its own SMTP engine, opening a backdoor for remote control (this time TCP 1234), and attempting to stop a long list of security products. In addition, it also uses UPX compression and appends copies of itself with random data, making checksums of the worm variable.

One change in the worm (seen first in X but not explored in the first History paper) is the use of mutex[5] spawning in addition to process killing to combat rival worms such as Netsky. By creating a mutex that is equivalent to those created by other worms, Beagle is able to prevent the respective viruses from running (and subsequently killing Beagle processes). The wide range of file types concocted by Beagle (possible extension/types include VBS, CPL, HTA, EXE, and ZIP) requires that the worm craft a corresponding infection routine. In each case, however, the virus drops a file (copy of the worm) into the Windows system directory and executes it. Beagle.X also employed a trick used early on, displaying a fake error message to hide the routines taking place in the background:

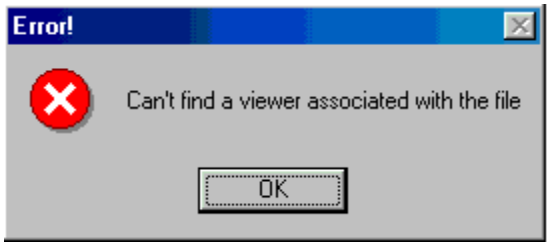

Figure 1: Beagle.Y Error Box

A user seeing this box and dismissing it by clicking "OK" would likely think that all is well and not that an application is running behind the scenes.

Since late April 2004, the Beagle variants adhered to a simple infection and propagation routine, as compared to earlier versions. Email attachments and file share replication (by copying itself to directories with "shar" in the name) were the only mechanisms used to spread from one box to another. The messages generated were not nearly as long or complicated as previous bodies (in terms of crafting the message with various pieces of the destination address, etc.).

As was the case with .X and carries though later versions of the worm, Beagle.Y deletes associated Registry values, exits memory, and ends its process after Janaury 25, 2005.

In what may prove to be a defining point in the worm's history, this version of the worm carried a copy of its source code with it, dropping the file on infected machines (attached with a name of "sources.zip" no less). As of the date of this report, there have been no confirmed variants built with the code left by Y. The source was written in pure assembly, an indication (in addition to the features of the worm) that the author is a very skilled programmer.

The inclusion of the source code in this single version of the worm grabbed headlines, even though the number of infections was kept relatively low. It is curious that the only version thus far to include the source code would also not attempt to kill active antivirus processes. Speculation in the media for the presence of the source code mirrored that of MyDoom.C:[6] it was likely dropped on machines to make possession of the code a weaker piece of evidence should the author get caught. The explanation for the removal of the "kill" routine then could be that the author believed it was important for this version to be

discovered by as many people as possible, getting the fact that the source code was dropped by the worm into the headlines.

Beagle.Z

The next day, July 5, Beagle.Z was released. In addition to the random checksum values, Beagle.Z was delivered using PeX compression, providing another small wrinkle for AV companies to handle. Otherwise, the worm is functionally similar to X and Y. This version also removed the ability to kill security applications and set a very short termination date of July 6, 2004.

Beagle.AA

One week later, July 12, 2004, the 27th unique variant was discovered and catalogued. The only noticeable differences in Beagle.AA include its compression (it is packed with FSG) and changes to the Registry key values/filenames.

Beagle.AB

July 15, 2004, witnessed the next version, one that changed a few of the identifying marks of the last few variants. The backdoor port changed to TCP 1080, it is again packed with UPX, and reasserts the "alerting" functionality of previous Beagle worms. AB attempts to connect to a long list of domains in an effort to alert the author to new infections.

Because of the widespread seeding of this variant, as well as AA, reports of infections flooded antivirus vendors and gained media attention. Much of this involved comparing the damage to MyDoom[7], the previously reigning king of mass mailers in 2004. It is at this point that Beagle should be considered in a different league of virus from the casual writers' worms. The Beagle author has repeatedly demonstrated the ability to compromise huge numbers of boxes, seemingly at will, and cemented that ability with the releases in early July 2004. There is little luck involved with the worm at this point; the author appears to calculate each change in the code (see the development discussion in Part 1), select changes that entice users to continue opening the attachments, and plant the worm on a myriad of machines to ensure high infection rates.

Beagle.AC

Discovered July 17, 2004, AC was packed with PeX, but delivered few changes to the worm over superficial adjustments to Registry values, etc.

Beagle.AG

Beagle.AG was released July 19, 2004. Although again packed with PeX, this worm extends the "suicide" date to May 5, 2006. AG included the use of password-protected ZIP files (again carrying the password as an image file), a trick used with great success in

earlier variants. AG found a great deal of success in its own right, hammering networks everywhere with unwanted email[8].

Beagle.AH

After another 3-day break, the next version of Beagle appeared on July 22, 2004. The port used for backdoor control changed to TCP 1234, it employs UPX compression, and brings back the "Error" box shown above.

On the same date, a new version of the Mitglieder Trojan (Mitglieder.M) was also discovered. The Trojan connects to another long list of web servers and attempts to download and execute an application. The first part of this report presented the Beagle/Mitglieder relationship, which is still seen in the identification and naming processes of AV vendors[9]. Additional information on Mitglieder is presented below.

Beagle.AO

Beagle.AO was released on August 9, 2004, and much like its recent predecessors, it instantly became a major threat to Internet users (Symantec's Category 3, Trend's Medium Threat, Panda's assignment of a 3 (out of 4) Threat Level, Medium from McAfee, High from CA), again likely due to high seeding levels. AO is equipped a few new tricks, notably the use of a modified exterior shell to entice opening of the attachment. The email has no subject, a spoofed From: field, and a message body of "price" or "new price."

The worm arrives as a modified version of the Mitglieder Trojan, packaged as a ZIP file with one of the following names:

```
08_price.zip
new_price.zip
new__price.zip
newprice.zip
price.zip
price_08.zip
price_new.zip
price2.zip
```

The ZIP archive contains a folder (named "price") and an HTML file (also named "price" and containing approximately 30 lines of JavaScript). When the HTML file is executed the script launches the EXE inside the "price" directory, which is the Trojan that downloads additional code from numerous possible websites to the infected host. The download looks for a file called "2.jpg" and saves it as an EXE ("~.exe"), bypassing any attempts to prevent a workstation from downloading executable files. This code is the Beagle mass mailing/file share propagation code and is subsequently executed by the Trojan. A visual representation of this process is shown below:

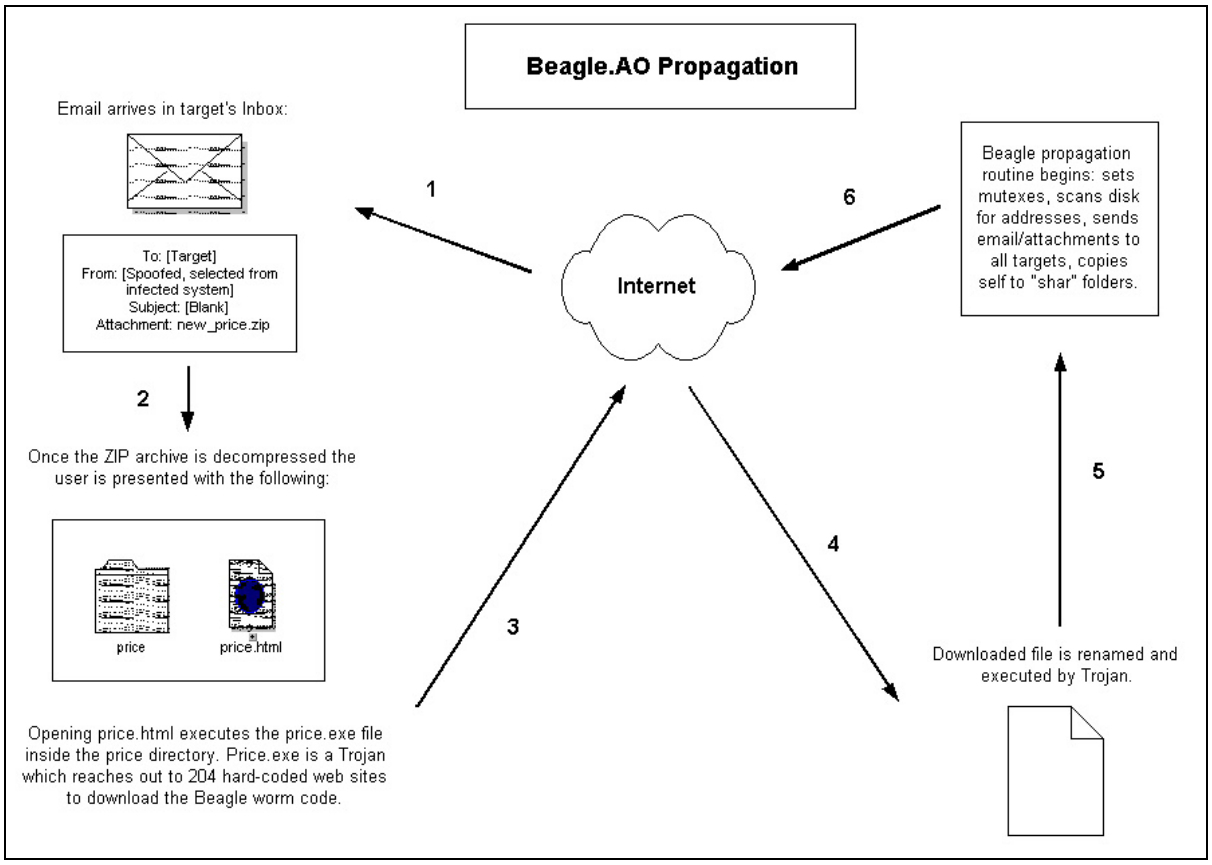

Figure 2: Beagle.AO Propagation

The Trojan dropper copies “windirect.exe” to the local box and establishes itself with the value: “win_upd.exe=%system%\WINdirect.exe”, placed in:

```
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

of both the LocalMachine and CurrentUser hives. The worm code (once executed by the Trojan) crafts the following value: “erthgdr=%system%windll.exe” in:

```
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

Beagle.AO sets a Registry key:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ru1n
```

Which is reminiscent of the “ru1n” key set by older versions (Beagle.T being the last) as possibly a simple marker of a compromise.

The author has once again found a new use for the ZIP archive medium as it relates to distributing viruses. In the case of AO, Beagle packages the malicious EXE (the Trojan that downloads the worm) inside of a directory that is placed inside of the ZIP attached to the mass mail message. If a user opened the archive with Windows XP’s built-in ZIP viewer, the directory would be visible, as would the HTML file. To anyone who has

saved a web page with Windows, the presence of "price.html" next to a similarly named directory would appear familiar, the result of saving a web page named "price." This innocuous HTML file, however, executes within the "Local Machine" context of the machine; a much more dangerous means of viewing the file than if the user had surfed to the page or clicked a link in an email (assuming the Internet Explorer has at least minimal restrictions over what type of content can run from a web host) [10]. This combination of tricks to have a user launch a Trojan on their machine is well crafted; something the Beagle author has proven to be quite skilled at during 2004.

Below is what a user would see opening the attached ZIP file with Windows XP:

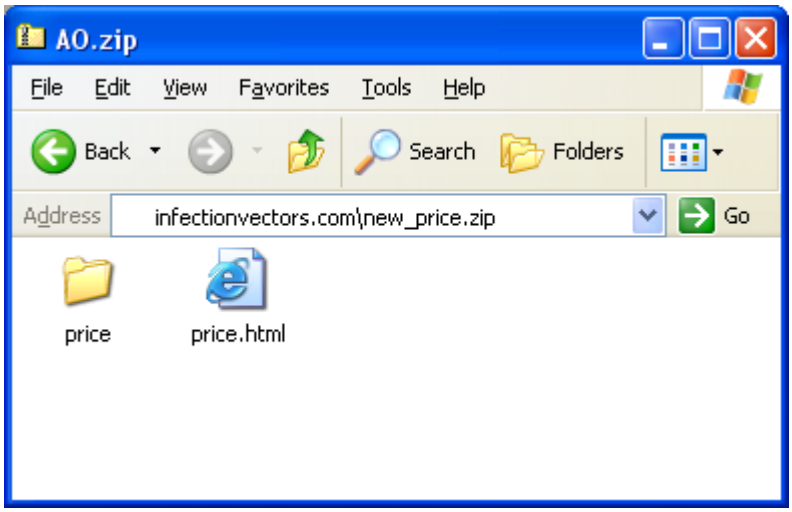

Figure 3: Beagle.AO Attachment (Windows Explorer View)

The use of an external ZIP utility, however, produces very different results. Although many users would be equally likely to open the HTML document accompanying it, the EXE is plainly visible with such programs as WinZip, as seen below:

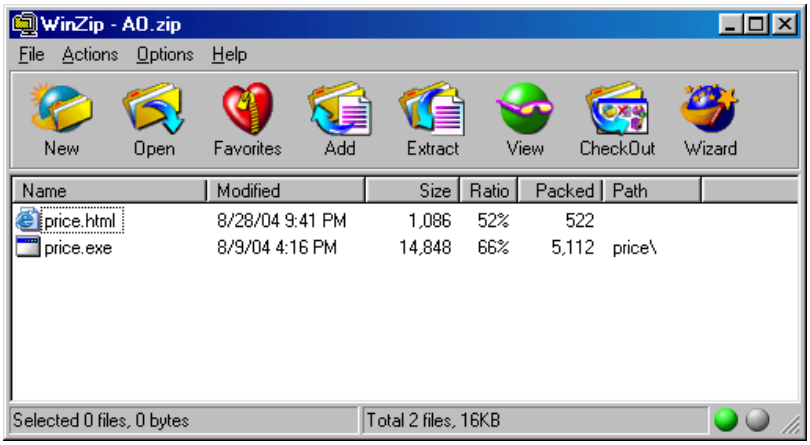

Figure 4: Beagle.AO Attachment (External ZIP Viewer/WinZip)

When the folder hiding the "price.exe" file is stripped from view, the attachment looks a little more ominous.

In a move reminiscent of spyware tricks, Beagle.AO's script executed code by calling on a CLSID (a URL scheme that allows a code to reference COM objects), which is a popular way to add unwanted Browser Helper Objects (BHO), toolbars, etc. to unsuspecting users' computers. Detection of the worm prior to specific signature release caught the script file as spyware in certain cases.

The worm opens TCP and UDP 80, an open port for virtually every system connected to the Internet for backdoor purposes. In addition, this variant kills security processes, increasing the likelihood that a compromise and future compromises will be successful. Another move that hides the worm functions is injecting the Beagle propagation routine into the explorer.exe process via the "_dll.exe" program.

Beagle.AP

August 17, 2004 brought Beagle.AP, a version of the worm that combined many of the familiar pieces of previous variants with a slightly modified look. Once executed, the worm performs the same obfuscation functions of its cousins, presenting the user with the crafted error message: "Can't find a viewer associated with this file."

From there, the worm works behind the scenes to contact an author-owned site/PHP script. The attachment is more direct than AO, consisting of a CPL, HTA, EXE, COM, SCR, VBS, or ZIP file containing the worm proper. The interesting collection of names that the author used for the files in this iteration include: "You_will_answer_to_me," "Nervous_illnesses," "Details," "Joke," "Half_Live," "Loves_money," "You_are_dismissed," and "Information."

Beagle.AQ

The last day of August 2004 brought AQ to the Internet. This version merged many of the features of AO and AP. Some antivirus vendors catalogued two separate instances of Beagle on August 31, both with very similar attributes.

The worm continues to deliver only the Trojan to the user's mailbox, waiting for them to open the attachment before downloading the worm itself. The worm adds the same Registry key to the startup locations (erthgdr = %SYSTEM%\windll.exe), kick starts the same set of Netsky mutexes, and deletes the Netsky Registry values.
The ever-changing nature of the worm (using a Trojan, attaching directly, etc.) continues to add to the confusing naming of Beagle. This version in particular goes by a number of different names, not just different letters after Beagle/Bagle, but being referred to as a Mitglieder variant, or just Glieder[11]. It carries the Trojan and HTML trigger inside of a ZIP file the same way AO does, including hiding the EXE within a folder in the ZIP.

Although successful pieces of previous versions are integrated into AQ, it is the development of new tactics for which the Beagle author is known. AQ prompts the infected machine to retrieve and updated version of the code every 6 hours, from a long

list of possible servers. This list is initially approximately 130, but, of course, could grow or change altogether within the 6-hour window in which a machine updates. This further complicates the process of removing or disabling compromised host servers, making the task virtually impossible. The Beagle author has had no difficulty cycling through a seemingly endless supply of servers under his/her control.

Another new function added to the Beagle worm allows it to stop services running on Windows XP/2000/2003 machines[12]. The initial targets for this routine appear to be IPSec and the Internet Connection Firewall/Internet Connection Sharing services, good choices for a worm designed to allow unfettered access to relay ports.

Of special note with Beagle.AQ is the fact that none of the 131 servers coded into the worm actually were available with the file ("b.jpg" which is saved as "_re_file.exe"), a possible indicator that the author is once again simply testing new methods prior to releasing the "production" versions of the code.

Beagle.AQ Email:

```
To: [Target]
From: [Spoofed]                          inside foto.zip:
Subject: foto                                  foto\foto1.exe
Attachment: foto.zip                           foto.html
```

Figure 5: Sample Beagle.AQ Email

Gliding

As was introduced in part one of the history report, the Beagle worm continues to keep ties with a Trojan labeled "Mitglieder." Based on the number of unique variants found with Beagle releases, it is likely that the Beagle author also wrote Mitglieder; at a minimum, the author is customizing the Trojan for use with the mass mailer. This component is separate from the Beagle worm itself; the worm is the self-propagating element of Beagle responsible for the mass mailing and file share copying. The Trojan remains an important part of the Beagle family, used to retrieve the actual worm from various sites and execute the code on compromised machines. Notable variants such as AO employed the Trojan to pull fresh copies of Beagle from the Internet (although it certainly could be used for downloading any code).

Mitglieder was also discovered independently from new versions of Beagle in a number of cases since the worm's release in January, indicating its widespread use beyond just downloading fresh copies of the mass mailer. After the release of AP in mid-August 2004, two newly crafted versions of Mitglieder were also discovered. This continued the trend of distributing new variants of the Trojan after revisions of the Beagle worm, possibly using those infected boxes as the launching point for Mitglieder.

Releases for Mitglieder followed a more controlled pattern than Beagle, and had new versions in June, when new Beagle variants were absent, the table below shows the release dates and any special notes for each variant of Mitglieder.

Variant	Release	Additional Info.
Mitglieder.A	January 8, 2004	LDPinch download
Mitglieder.B	January 20, 2004	
Mitglieder.C	January 20, 2004	discovered with Beagle.A
Mitglieder.D	March 13, 2004	TCP 25555
Mitglieder.E	March 13, 2004	TCP 20742
Mitglieder.F	April 5, 2004	hard coded DNS
Mitglieder.G	April 5, 2004	
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	August 20, 2004	added full process kill list
Mitglieder.O	August 20, 2004	

Figure 6: Mitglieder Releases

With Beagle.AO, a modified version of Mitglieder was the attachment, "price," that came with the modest emails. It established automatic start-up for itself much like the worm, by adding an entry to the Registry's "Run" key. In addition, it dropped "_dll.exe" and injected the file into a running process. This process then becomes the initiator of the propagation routine. Mitglieder then reaches out to the Internet to grab the Beagle worm code and execute it on the local machine. This small, very extensible Trojan is simple for the author to modify to evade SMTP virus scanners and client anti-virus software. The Trojan does the bulk of the set-up work: infecting a running process, disabling the security software, opening ports for remote updates, and downloading the Beagle code.

The code was also known to download a separate companion, known as Harbag[13], which harvested email addresses, uploaded them to a server, and then deleted itself from a compromised machine. Previous versions of Beagle or Mitglieder did not show this propensity, they allowed the scope of the worm's propagation to determine how many users would be targeted. This action (first seen as this report is concluding in August of 2004) would allow for a new generation of attacks. The new attacks would allow the author to seed a variant by using just a few machines (or possibly a single box), letting it blast the worm out to millions of addresses that were collected and compiled by the last version.

Other companion pieces of code associated with Beagle include password stealers/keyloggers Tarno and LDPinch, both of which appeared with new versions in the summer of 2004.

Infection Paths

Beagle stays true to a core set of proven infection vectors, namely simple email messages and file sharing. The reliance on user intervention requires that copies of the worm are enticing enough to open. As seen in the variants since January 2004, the author has had success with very direct EXE attachments as well as the more artistic creations in AO.

The names used for file share copies of the worm have remained constant for nearly the entire life of the worm, making it the most recognizable piece of many new variants:

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

Figure 7: Names Used by Beagle for Copies Delivered Via Filsharing

Message bodies have veered away from the long texts included with mass mailers like Lovgate and some earlier Beagle worms, favoring the believable, short, look of its later messages. Examples of this approach:

Beagle.AG

```
From: [selected from addresses harvested from infected machine]
Subject: Re:
Message: >The snake
Attachment: New_MP3_Player.com
```

Beagle.Z

```
From: [selected from addresses harvested from infected machine]
Subject: Re: Thanks :)
Message: Check attached file.
Attachment: Updates.vbs
```

Figure 8: Sample Beagle.AG and .Z Email Messages

The results of over 6 months of learning and development have undoubtedly paid off. The latest versions of Beagle were the most successful, in terms of reported sightings. AO's success was documented above. Beagle.X remained as a Threat Level Medium (on a scale of Low, Medium, High) on Trend Micro's site over two months after its release. Symantec categorized most of the early variants at Level 2 (on a scale of 1 to 5, 5 being the greatest threat). Beagle.AB and AG both remained at a rating of 3 into August of 2004. Named AG and AH on Panda Software's site (includes a very similar variant not catalogued by Symantec) Beagle.AG captured their highest rating, a Threat Level of 4. It also was given a High on CA's Threat assessment in their Virus Information Center.

The continued use of spoofed "From" fields has helped the worm convince people to open the attachments as well. Beagle's contribution to email security was explored in the previous report. Since its widespread use of spoofed sender addresses that came from those it harvested from the infected machine, Beagle variants have been at the forefront of making automatically generated warning messages worthless annoyances. Beagle, more than any other mass mailer proves why one can't trust information received from a worm.

Sowing the Seeds

It is the investment in early advances and testing that has paid off for the Beagle author(s). Many companies practice this type of software development, under headings such as CMM/CMMI and other process improvement strategies. This idea is an extension of that presented in "History Through April 24, 2004," and is examined with regards to the newer variants in this section.

The success of these variants is due in large part to the adherence to successful methods of fooling people to open Beagle's attachments, still the critical component in compromising a host. Another factor in the widespread distribution of the later versions is the use of a pre-built machine base, a collection of machines previously compromised by the worm[14]. From these machines, the Beagle author could seed the next wave of attacks, distributing the new variant from thousands of machines simultaneously (effectively "spamming" the worm out to the world)[15]. This seeding of a new variant is based on spamming methods: control a large set of anonymous mail relays (the infected boxes), upload the message to be sent, and distribute it from all around the world.

Each version of Beagle extended the author's network of hosts and helped improve on the tactics used by the next "update." In many ways, the tremendous number of compromised machines has reduced the need for technological innovation. A virus author can still rest assured that a good percentage of users will open any attachment sent their way, meaning that given a large enough set of targets, a simple mass mailer will compromise more than enough hosts from which to launch additional attacks. In the case of the Beagle worm, many of the improvements from January through April of 2004 allowed the author to build a large base of zombies. This base (and the undoubtedly extensive list of addresses lifted from each device) propelled new versions (including many that relied on few if any of the technical developments of early variants) to great success.

Beyond the network of compromised machines, the authors continued to develop technical and cosmetic pieces of the worm, both important to the overall success of the attack. Technical improvements came in the way of delivery mechanisms such as the web download of the worm instead of simply attaching the entire file. By dropping only a script file or small Trojan with the original email, the Beagle developers kept the transmission size of the mass mail small. The Trojan could disable security and antivirus applications and then download a fresh copy of the worm, allowing the authors to improve upon the code (or change it enough to dodge virus signatures written for it)

while the outbreak was occurring. Multiple versions of the worm could be located on different servers around the world.

Technical improvements were guided by testing new facets of the worm. It is possible that the download functionality of attaching just the Trojan was part of AO's routine. The long list of addresses used for download contained many invalid domain names and hosts that did not have the requested file present. AO also set a very quick termination date for worm propagation, but left the Trojan. This leaves open the possibility that the author simply wanted to experiment with the update capabilities of a program built for downloading software instead of the update (-upd) functions used in previous variants. Although the propagation routine was dumped one day after release, the download function runs every 10 hours.

In addition, the public face of the worm (the email message/attachments) was overhauled on numerous occasions, from the straightforward EXE attached to early variants through the script files and password protected ZIP files of the summer. Beagle.Y and AB presented themselves as "information," providing very innocuous subject lines and message bodies, indicating something like, "Check attached file for details." Beagle.AG took the same style and changed all the tags, giving the attachment names such as "Garry" or "Cool_MP3" and including message bodies like "The snake" and "Lovely animals." The effect of such changes was to nullify "word of mouth" and casually read virus warnings. With the multitude of possible attachment formats and names, message bodies, and subject lines, it is impossible for a general user to positively identify a Beagle message. Users who may be ready for "ILOVEYOU" showing up in their Inbox are far less prepared for the ever changing and subtle messages generated by Beagle.

Beagle.AO took the worm to a new level, giving most users something they had never seen in terms of viruses, a packed directory (hiding the Trojan from sight) and HTML file. The general user would not think twice about opening an HTML file, as they are familiar with the fact that web pages are constructed with the language[16].

This report continues to make references to professional development processes, such as CMMI, the same way the first part of the "History" report did. The additional three months of evidence for the author's ability to overtake machine after machine help point out the difficulty in slowing the spread of worms such as Beagle. Beagle's reach is much larger than its mass mailing cousins, of which there have been many in 2004 (including variants of Lovgate as well as new entries such as Neveg and Amus). Most mass mailers have found little success at grabbing headlines and compromising PCs, something Beagle is capable of doing at any time.

Old Grudges…

Since Beagle.M the code has included attempts to terminate and prevent Netsky infections on victim machines (in fact, later copies of Beagle include process termination functions for 23 Netsky variants). In addition, later Beagle versions create the Netsky mutexes for 7 variants. This is likely not done out of the goodness of the author's heart,

but rather for self preservation, many versions of Netsky kill Beagle processes. After the long-running war between the two worms in the spring of 2004, there is probably some lingering animosity.

A curious omission from the list of Netsky targets is the Netsky.AB variant. No version of Beagle as of August 30, 2004 included it in the list of mutexes or Registry entries deleted. This worm used the value "BagleAV" in the Windows Registry to ensure startup with the OS. At the time that the late summer versions of Beagle were released, Netsky.AB had been out for months.

The Netsky author confessed to being the writer of Sasser as well (in the code for Netsky.AC and then later after arrest), explaining why Sasser variants (namely Sasser.E) also targeted Beagle and Mitglieder Registry keys values.

It is theorized that the Beagle authors kept the virus away from the spotlight for a few months because of the highly publicized arrest of the alleged Netsky author, one of many arrests in 2004 of suspected virus coders[17]. The MyDoom variants also stopped for the month of June (but as noted above, Mitglieder did not, which is significant if one believes the Trojan was written by the Beagle author). MyDoom came back in July with three new variants; versions that were also quite successful.

In what is likely just interesting yet coincidental timing, many later versions of Beagle are set to cease propagation functions on May 5, 2005, almost precisely one year after the alleged Netsky author was arrested.

… And New

In the summer of 2004, after the "Netsky arrest," other worms took it upon themselves to pick up on the anti-Beagle battle and included routines that dumped the worm from host machines. One of note, Fremmy, packaged itself much like the worm it was intending to remove. It contained a very simple set of possible "From:" field combinations and attachments (also sent as a ZIP archive with a SCR, CPL, EXE, BAT, or PIF inside)

In early July the Atak[18] worm (specifically its Atak.B released July 15, 2004) added routines to kill versions of Beagle and some other successful worms. Within the code of Atak is the following message:

```
"Developed by Melhacker(TM) for personal research only."
4tt4(k 4g4!n$t N3tSky, B34gl3, MyD00m, L0vG4t3, N4ch!, Bl4st3r
```

Figure 9: Message Found in Atak.B Code

The "attack against" these worms takes the same form as the Netsky/Beagle war: a mass mailer. On August 16, 2004, Atak.C was released included a function to delete files associated with AO, just days after AO's distribution. Atak.C kept its list of Netsky values to delete as well-a list that looks just like the list included in Beagle, with the same omission of Netsky AB and AC.

What Else Have We Learned?

This could also be known as, "Why a second part of the report?" The first part of this story fleshed out a list of many lessons worms like Beagle have for security professionals. The need to remain aware of new virus tactics and infection vectors, training end users regularly, and examining trends in virus development all still belong on this list. Each of these is only strengthened by what has been witnessed over the summer of 2004.

In addition, the second part of the Beagle worm's history also intends to point out how strong a virus can become when developed in a professional manner, with a specific goal in mind. The Beagle author has built an army of machines whose size is currently unknown, except to say it is undoubtedly large. This army could easily be turned to any activity, likely with the strength of numbers to accomplish any DoS attack, spamming enterprise, or distributed processing/password crack. The use of the term "spam net" in the introduction is meant to invoke ideas of "mix net" and "bot net." The Beagle author has virtually guaranteed the success of any additional variant by crafting a giant, anonymous network of drones.

The lesson is greater than "the Internet is not safe;" the real lesson from the Beagle author is that the Internet will never be safe as long as the world trusts the existing infrastructure. Problems battling Beagle rival those with spam, as the technology used is virtually the same. Trust in SMTP (by home and corporate users alike) prevents warnings about mass mailers from stopping Beagle infections. When a message arrives with a friend's name in the "From" field, the recipient is likely to open it without much thought. Even after Beagle, MyDoom, SoBig, MiMail, and a long list of mail-borne viruses, this is true. Knowing that a browser protects web pages when viewed on the Internet but not when opened on the local machine is a concept that is difficult to understand and put into practice for most users.

The Internet boom has left a sea of unprotected machines available to worm writers. In many ways it will be impossible to protect these machines without changes to the underlying technologies of the Internet as a whole, such as providing built-in assurance to SMTP. The high-visibility targets of big corporations and military installations are still important to nefarious coders around the globe, however, the first step to hitting those will be compromising a group of boxes from which to launch the attack. The Beagle worm has shown security professionals how easy it is for a talented programmer to seize thousands of the broadband-connected, high-powered, and available machines that are connected to the Internet all the time. At this point, the motives have been simply to harvest email accounts and turn these machines into mail relays. There should be no confusion, however, that this has already cost Internet users a great deal in terms of spam filtering, virus mitigation, traffic congestion, and the associated preventative measures.

The Beagle author continues to take what is given, by using his/her coding skills to hone one of the most successful worms in Internet history. Although the innovations of the worm are astounding, there is no reliance on technical magic, no need to speed a release

in hopes of catching machines without the latest patches, no attempts to conjure something out of nothing. Beagle takes only what is publicly available and makes it formidable, a demonstration that should inspire security administrators to do the same for their networks.

Under the Radar

A final note about the worm at this stage of its life relates to its author. Beagle's author has remained anonymous, even with a very successful virus in the wild and an active search for his/her whereabouts. The high-profile arrests of many virus writers in 2004 may have deterred the author for a few months and been the cause for the inclusion of the source code in Beagle.Z. Although the success of the worm has been great, it has not lead to the same bounty that exists for the SoBig and MyDoom (Microsoft's $250,000US bounty) authors. The bounty may well have been responsible for the arrest of Beagle's archrival, the Netsky author. It is possible that Microsoft has not placed Beagle on the "most wanted" list since so many variants completely dodge MSN, Hotmail, and Microsoft addresses and there has never been a denial of service routine included with Beagle (unlike MyDoom.B and Doomjuice).

In a move that may be similar to the red herrings thrown out by the Netsky author, Beagle.Y included the following lines of text in the code:

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

This is significant to the history of the worm for a few reasons. The first of which is that it is the first time the apparent author has referred to the virus in the code, seemingly selecting "Bagle" as his or her preference for the worm. Second, it is the first message that has any substance (as opposed to the picture of the butterfly and captions used in M and S, see "History Through April 24, 2004" for these) that is not pointed at the Netsky author. Third, the location provided ("Germany") is the location that the Netsky arrest was made (although the date in Beagle.Y's message was approximately 10 days prior to that arrest). This is the probable red herring referred to above, as the Netsky author repeatedly used the location of Russia in messages left in that worm. The date provided in Y is approximately 9 weeks prior to the discovery of the message/worm.

The message itself is not composed of many identifying strings, save the second line, which appears to be from a song lyric. It is generically the life of every worm: to remain viable the worm must overtake a new host and spread again. Beagle's warning is certainly not empty, it continues to spread to new hosts everyday. The author is undoubtedly improving the worm for additional releases, building on the success of the first six months of development. The need for a third part of the history is not certain, but likely.

Notes

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.
2. For specific ways Beagle is changing gateway scanners see the following report that notes how scanners are incorporating password cracking in their routines. Dragos Onac from BitDefender wrote a great article covering this trend for Virus Bulletin in May of 2004:
http://www.virusbtn.com/magazine/archives/200405/protect.xml
3. Optical Character Recognition
4. Additional links to specific variants are in the Reference section. Beagle.Y's analysis:
http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.y@mm.html.
5. Mutex – ensures that only one copy of program is running at a time. Mutual exclusivity protects a virus from itself, that is, if a box was to be infected multiple times, the machine user would likely notice the performance toll. Furthermore, a machine infected by the same worm multiple times would become unstable, at best it would be slowed down greatly, thereby interfering with viral propagation.
6. If thousands of people have the source code, then just having it doesn't mean they wrote it. A report to read for more information on Beagle's source code drop:
http://www.computerworld.com/securitytopics/security/virus/story/0,10801,94367,00.html?f=x74
Additionally a good report of the assembler code left by Beagle is found at:
http://news.zdnet.co.uk/internet/security/0,39020375,39159596,00.htm
And the analysis for leaving a copy of the code on infected machines:
http://www.sophos.com/virusinfo/articles/doomevidence.html.
7. Being compared to MyDoom is pretty significant, considering the level of attention MyDoom received in January and February of 2004.
http://software.silicon.com/malware/0,3800003100,39122319,00.htm
8. Email from AG pummeled corporate and ISP networks for days during its peak:
http://www.eweek.com/article2/0,1759,1624970,00.asp.
9. For example, Mitglieder.M is known as bagle.aj!proxy at McAfee's site:
http://vil.nai.com/vil/content/v_127029.htm
10. Microsoft's Internet Explorer allows a user to set different security policies based on the location of the content (i.e.: the Web, Intranet, local host, etc.). The "Local Machine" zone operates with complete trust of the OS; no restrictions are placed on content that is run from the local box. This effectively means that surfing to an exploit on the web is much safer than opening the same page if its location is the local hard disk, as is the case with HTML pages delivered to a POP3 mailbox. XP's SP2 allows users to "lock down" the Local zone as well. Information on the use of zones and the upgrades with SP2:
http://msdn.microsoft.com/library/default.asp?url=/workshop/security/szone/overview/overview.asp
11. AQ called Glieder at http://www.f-secure.com/v-descs/gliederh.shtml
12. Stopping a process or a service is nothing revolutionary, however the inclusion of the new routine in the Beagle variants is significant as it targeted the firewall heralded by Microsoft as critical to one's security with their release of XP SP2.
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_BAGLE.AL&VSect=T
13. Harbag also skips the same set of email addresses (those with any of the strings listed below) as Beagle. CA catalogued each version of this code separately, a good reference can be found at:
http://www3.ca.com/securityadvisor/virusinfo/virus.aspx?id=40044.
14. Seeding the worm was actually discussed by a few analysts after Beagle.A:
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci945285,00.html
15. Alert for Beagle.X seeding: http://www.eweek.com/article2/0,1759,1563819,00.asp
AB seeding: http://www.nwfusion.com/news/2004/0716newbagle.html
And additional information on the seeding of Beagle variants through July:
http://www.itnews.com.au/storycontent.asp?ID=9&Art_ID=20647
16. Beagle as a whole has been difficult for most users to positively identify. This may be the most skillful use of coding/social engineering seen in a family of worms. A report mentioning the problem for users is found at:
http://www.securitypark.co.uk/article.asp?articleid=22738&CategoryID=1

17. http://www.informationweek.com/story/showArticle.jhtml?articleID=22103914
18. Atak has seen three variants thusfar, the latter two take shots at Beagle:
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_ATAK.B&VSect=T

Additional Information for the Curious

Cross Reference of Netsky Mutexes/Registry Values

As mentioned in the paper, the war against Netsky continues through the summer of 2004. Beagle accounts for all but the last two variants of Netsky, as seen below. The latest versions of Beagle carry the following set of mutexes to create and startup Registry values to delete:

Netsky Mutexes:

MuXxXxTENYKSDesignedAsTheFollowerOfSkynet-D	Netsky.AA
'D'r'o'p'p'e'd'S'k'y'N'e't'	Netsky.P (Trend named)
-oOaxX|-+S+-+k+-+y+-+N+-+e+-+t+-|XxKOo-	Netsky.Q
[SkyNet.cz]SystemsMutex	Netsky.D
AdmSkynetJklS003	Netsky.B
____--->>>>U<<<<--____	Netsky.X
_-oO]xX|-S-k-y-N-e-t-|Xx[Oo-_	Netsky.P (Symantec named)

Netsky Registry Hooks:

Service	Netsky.A, .B
ICQ Net	Netsky.C, .E, .K
ICQNet	Netsky.D
Zone Labs Client Ex	Netsky.F
Special Firewall Service	Netsky.G
Antivirus	Netsky.H
Tiny AV	Netsky.I
My AV	Netsky.J
HtProtect	Netsky.L
9XHtProtect	Netsky.M
NetDy	Netsky.N, .W
MsInfo	Netsky.O
Norton Antivirus AV	Netsky.P
SysMonXP	Netsky.Q
PandaAVEngine	Netsky.R
EasyAV	Netsky.S, .T, .U
KasperskyAVEng	Netsky.V
FirewallSvr	Netsky.X, .Y
Jammer2nd	Netsky.Z
SkynetsRevenge	Netsky.AA

Found in:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Interestingly, two versions of Netsky (released just a few weeks prior to alleged author's arrest) are not terminated or prevented by any version of Beagle.

Netksy Registry Values Untouched:	
Netsky.AB	BagleAV
Netsky.AC	wserver

Netsky Mutexes Not Mimicked:	
Netsky.AB	S-k-y-n-e-t--A-n-t-i-v-i-r-u-s-T-e-a-m
Netsky.AC	SkyNet-Sasser

Addresses Skipped by the Worm

In the tradition of the earliest copies of Beagle, the later variants also pass over sending themselves to certain addresses. Any harvested address with the following strings are bypassed:

@avp.
@foo
@iana
@messagelab
@microsoft
abuse
admin
anyone@
bsd
bugs@
cafee
certific
contract@
feste
free-av
f-secur
gold-certs@
google
help@
icrosoft
info@
kasp
linux
listserv
local
news
nobody@

noone@
noreply
ntivi
panda
pgp
postmaster@
rating@
root@
samples
sopho
spam
support
unix
update
winrar
winzip

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

Tangents on Beagle.Y Message

"In an nameless time" is the name of a song by the band Rage. It is a song written as 3 parts. It appeared on the 1995 album Black in Mind." The three parts of this song are "The Mysterium, "The Expedition," and "Finding Out."

Beagle Function Development

This was introduced in "History Through April 24, 2004" and is updated for this report:

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

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

References

The details of each Beagle strain were compiled from independent evaluation of code samples and reports found at the AV vendor sites listed below.

Virus identification and reverse engineering produces varied results; exact names will not be consistent with the paper (for internal consistency, the Symantec nomenclature was used for the Beagle variants through .M), however, the following sites will provide a wealth of background on all the variants discussed here.

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/

Sophos
http://www.sophos.com/

Kaspersky Labs
http://www.kaspersky.com/

Specific References for more Beagle Information

Beagle.Z Analysis
http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.z@mm.html

Beagle.AO Analysis
http://www.symantec.com/avcenter/venc/data/w32.beagle.ao@mm.html

"Beagle Worm Variant Slips Through Defenses" (AO)
http://www.eweek.com/article2/0,1759,1633740,00.asp

Beagle.AQ (AV Panda)
http://www.pandasoftware.com/virus_info/encyclopedia/overview.aspx?lst=det&idvirus=51651

AQ Disables XP Firewall
http://www.sophos.com/virusinfo/articles/bagledla.html

Beagle.AQ (F-Secure AL)
http://www.f-secure.com/v-descs/bagle_al.shtml

Beagle.AQ (Trend AL)
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_BAGLE.AL

Beagle.AG (McAfee AI)
http://vil.nai.com/vil/content/v_126798.htm

Beagle.AQ (CA AJ)
http://www3.ca.com/securityadvisor/virusinfo/virus.aspx?id=40057

Additional Reading

CERT Advisory on E-mail Worms
http://www.cert.org/advisories/CA-2004-02.html

Beagle 2 Mars Exploration Site
http://www.beagle2.com/