



Cotton, China, and Bagles: The Beagle Worm's Second Anniversary¹
infectionvectors.com
January 2006

Overview

The average professional career in the US National Football League (NFL) has been charted at less than five years.² That doesn't sound like a whole lot, but the NFL is a tough game, and there is a very small window of opportunity, even for someone with the talent to be a professional athlete. There are debilitating injuries every week, a small number of roster spots relative to the number of applicants, and a hundred other factors from luck to the choice of position and even agent. So, even a short career is pretty good, and certainly something to be proud of. In the world of computer viruses, there is an even smaller window of opportunity in which to make a career – with anti-virus signatures from many different companies, vulnerability patches, user awareness, and aggressive law enforcement agencies.

The Beagle worm, with a professional ethic to rival many legitimate software outfits, has defied the odds and remains in business after two full years. And to be sure, these aren't two years spent on the bench, staying off the field to avoid injury. The Beagle worm and its related malware have been infecting machines, harvesting personal data, and making revenue (if not a healthy profit) for its authors. This report continues the previous research and analyzes the releases since May of 2005.³ Specifically, this portion of the paper focuses on release trends with the worm.

Mail Carriers

Beagle has accounted for untold millions of email messages over the last two years. The previous chapters in this report described what appears to be dedication to producing a quality product on the part of the Beagle author(s). The idea that a malware enterprise could be so well managed (even that malware creators would be part of an "enterprise") may have been a questionable concept prior to the for-profit worms seen in recent years. Beagle and its professional life have ended any mystery as to whether malware authors can be an organized, focused group.⁴

So dedicated is the Beagle team (which may be only one member strong), that numerous concepts in IT management can be extracted from the worm's story. Researching the first year's worth of releases showed a complex product which was managed under an umbrella of best practices in software development.⁵ During the second year, it was apparent that the strategy went beyond just making a good worm; there are other factors, such as release management itself, at play.

Release Management, an ITIL discipline⁶, involves keeping both a physical and logical store of all software within the organization. Admittedly, many of the terms and concepts related to release management are not going to fit precisely with a malware enterprise as the concepts were created with a different vision of “organization” in mind. However, there is a definite correlation between the business goals, software products, version control requirements, and customer base between a malware enterprise and any other “legitimate” organization.

Release management is called out in a number of best practice guides. Microsoft published a guide to implementing release management and called out five goals for any program:

- Plan releases in line with requirements resulting from approved changes.
- Build effective release packages for the deployment of one or many changes into production.
- Test release mechanisms to ensure minimum disruption to the production environment.
- Review preparation for the release to ensure maximum successful deployments.
- Deploy the release in line with structured implementation guidelines.⁷

The Beagle family has produced results in each of these areas. Although the “approval” for changes (item #1) is probably not a traditional control board, there would seem to be a good deal of testing and decision making going on with each release. Change management itself (item #2) was discussed at length in the prior reports. Successful command of the bot-net has required and resulted in careful release patterns (items #3 and 4). Hopefully (at least for curious researchers such as the author if this paper), it will be discovered one day exactly how structured the Beagle creator’s “implementation guidelines” (item #5) really are.

Such dedication to seemingly mundane topics (certainly for many coders) yields a more efficient distribution system to the author, likely resulting in additional profitability. The Beagle components are probably (if the author is captured one day these questions may be answered) now produced with lower implementation costs and development times than the early iterations. Widespread distributions are issued with less risk than counterparts that are not crafted within the same testing structure.

The Family Portrait

At the second anniversary of Beagle, it is easy to see a very well-defined group of offspring that has been produced over the years. Although some of the variants are placed in different groups by antivirus vendors, the functional groups are still somewhat distinct:

Beagle worm – the mass mailer continues to be the workhorse of the enterprise, removing some barriers to propagation (such as the Netsky worm, some local security settings,

etc.), establishing the slave bot networks (registering clients, installing backdoors, etc.), and distributing new software.

Mitglieder/Beagooz – the earliest complementary product is used to build spam relays on compromised machines. In some cases it also halts security software, steals email addresses, and downloads new versions of itself.

Tooso – Written specifically to weaken security on the target system, Tooso erodes a machine's protection by stopping software processes, deleting security-related Registry keys, attempting to disrupt update services, and even deleting protective software from the local hard disks.

Lodear – The relative newcomer to the family, Lodear is designed to retrieve and install new family members from the Internet.

Monikey – A close cousin of the family, Monikey is a new attempt at mail and file sharing propagation using the familiar Beagle components.

LDPinch – Dating back to the earlier days of Beagle, LDPinch was designed to snatch passwords from infected boxes.

Tarno – Another password stealing application, Tarno has seen new versions as late as December of 2005.

Formglieder – The first anniversary of Beagle was marked by the release of this group of applications, used to lift banking/financial account information.

What is the benefit of having the products broken down into component families? For software coders, the advantage is clear: the ability to focus work only in areas of the application that need attention. Consider that the greatest technical enemy of the Beagle worm is the antivirus signature file⁸, something that has been building a profile of Beagle in all its forms for two years. If the worm author was required to make the whole family evade antivirus scanners each time it was released, the work would require more development time and would be much less profitable. Instead, the coder can focus changes on the component(s) that kill security software altogether, then use that product to retrieve other pieces (possibly ones that have not even been changed since their previous release). This is discussed further with respect to Tooso (used to open the door for other applications) below.

Software engineers are apt to see the advantages of a modular architecture as well. Not only has it worked for bot technology such as Agobot/SDBot, but also for many mainstream management applications. Such modularity breeds an agile overall product, allows for customized releases (feeding the release management goals noted above), and reduces R&D time for the whole package.

Even when evading scanners is not the primary concern, there are other benefits to distributing the product in multiple pieces. Testing and development is easier when the strategy is broken down into separate parts. Furthermore, the controller can deploy only the pieces necessary for a new onslaught. During 2005, virus researchers were inundated by waves of Beagle components, sometimes coming at rather regular intervals. Each wave consisted of varying combinations of the family members.

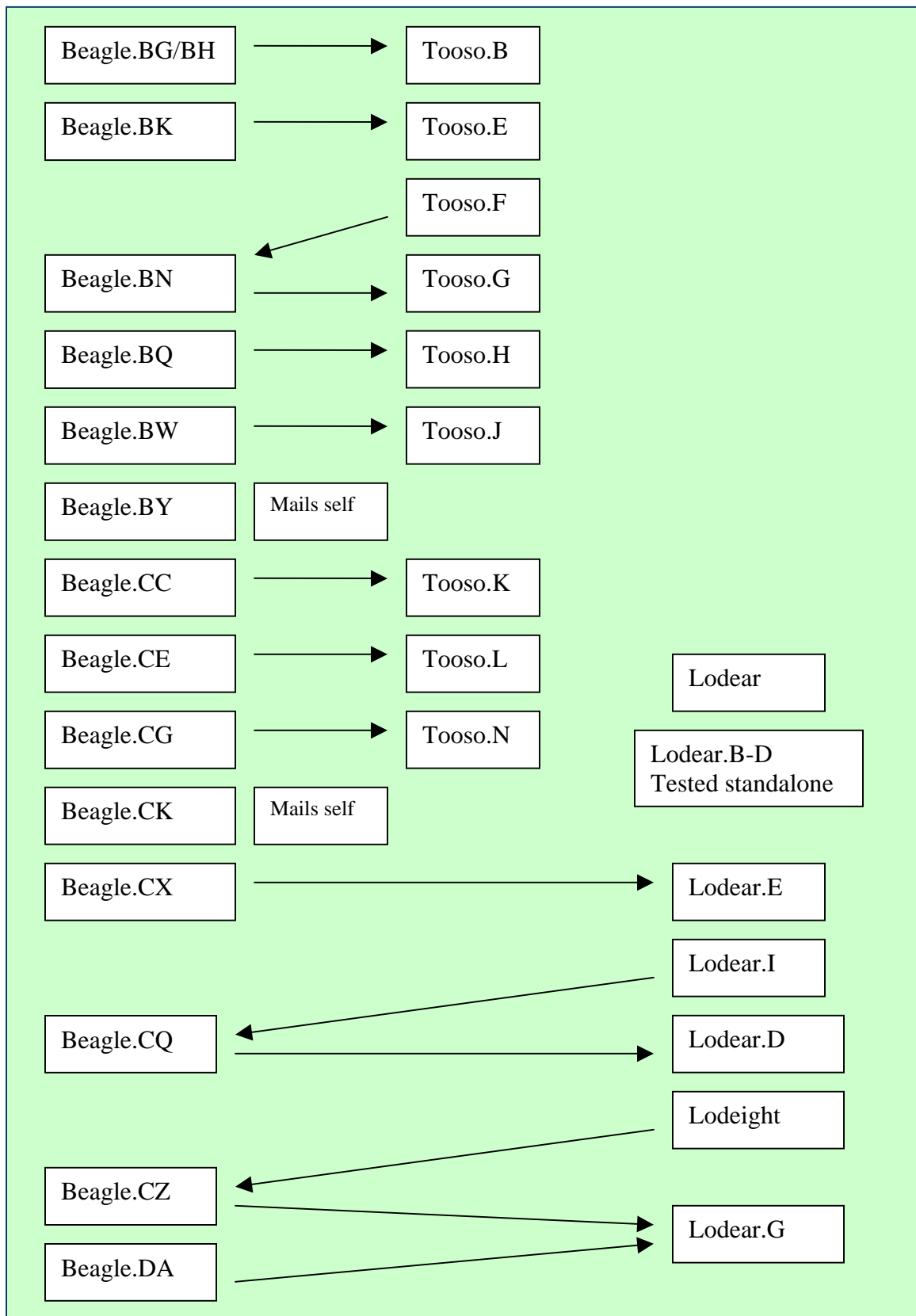
Slipstream

How are the various pieces of malware introduced into circulation? The original Beagle worm (at least the latest incarnation of the worm) is still used extensively to distribute the wares of its authors. The mass-mailing worm is employed to deliver software, such as Tooso or Lodear once the respective tools have been tested. For example, we'll examine the release of "Lodear" software.

Initially discovered in the wild during the first week of November, Lodear is not seen riding upon Beagle messages until much later. The Lodear group closely resembles the Beagle and Mitglieder code, but serves a different function to the latter group of Trojans: downloading remote files to compromised boxes. As noted above, Mitglieder established itself as the spam-relay in the family. Beagle and Tooso have been used to weaken security settings. Lodear is designed to make the distribution system stronger. After its first release, there were at least four additional iterations, used through November and early December 2005. On December 15, 2005, the release of Beagle.CX⁹ marked the Lodear entry into the Beagle fray – the Trojan was mass mailed by CX and put into greater distribution.

Trojan distribution is very difficult to monitor and document, as any previous (or new) copy of any malware can be renamed and downloaded by any other piece of software that retrieves files from the Internet. In general, that strategy would be rejected, as anti-virus signatures for a particular piece of code would make re-release prohibitive for a malware writer. However, as can be seen below, that is not always the case.

The graphic below shows the entry of the Lodear family along with some of the Tooso releases since the last portion of this report was released. Note that the Beagle worm variant and a right-traveling line indicate that a Trojan was mass-mailed by that version of the worm; left-traveling lines indicate the worm is retrieved by particular Trojans.



Distribution calculus was described in earlier portions of this work; nonetheless, it is clear that the author of the malware has a great deal of control over how versions are introduced. He/she can stay ahead of anti-virus signatures, keep respective pieces of software in large or small release groups, and continuously change the appearance of a Beagle release (one time it may mail itself, sometimes a new version of the worm, sometimes a particular Trojan, etc.).

Tooso to Tango

The fall of 2005 saw a familiar onslaught of variants, designed to keep ahead of antivirus signatures and get the worm onto as many new machines as possible. Building the zombie army was the task of variants associated with the Tooso line. Specifically, Tooso.O appeared in mid-September 2005¹⁰. This iteration used attachment names with "price" in them and the filename "winshost.exe" when it copied itself to the Windows system directory (used by previous versions of the worm). It deletes outright the following in an attempt to prevent security-related software from ever starting:

```
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\McAfee
.InstantUpdate.Monitor"
HKLM\SOFTWARE\Agnitum
HKLM\SOFTWARE\KasperskyLab
HKLM\SOFTWARE\McAfee
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\APVXDWIN"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\avg7_cc"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\avg7_emc"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ccApp"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\KAV50"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\McAfee Guardian"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\NAV CfgWiz"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SSC_UserPrompt"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Symantec NetDriver
Monitor"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Zone Labs Client"
HKLM\SOFTWARE\Panda Software
HKLM\SOFTWARE\Symantec
HKLM\SOFTWARE\Zone Labs
```

Tooso then renames files associated with antivirus, firewall, and IDS software and stops services associated with security functions. Finally, it checks with the hard-coded list of over 150 websites to download additional code.

Tooso is an important piece of the puzzle for the Beagle enterprise. It arrives with no SMTP engine of its own (as do the other Trojan components), destroys local security functions, and then acquires additional code (often the mass mailing worm). Antivirus applications are then powerless to stop what may well be an unchanged, older version of Beagle. Tooso is another effort to keep functionality separated between malware families; allowing the coders to focus on making changes to subsets of the software instead of the entire package.

Review of Releases

Beagle.BQ, released on May 10, 2005¹¹, came with a copy of Tooso which it mass mailed with each infection. This version of Beagle is equipped with the Netsky mutex routine, a list of Registry values to delete, and a function which retrieves and executes a file from the Internet (the site used for the download was not found up during research period). This is representative of the strategy throughout the spring and summer of 2005 when variants such as Beagle.BW came equipped with new versions of Tooso and an expanded list of Registry keys to remove (see Appendix).

Beagle.BY was a nod to the "classic" mass mailer: a worm that mailed copies of only itself to targets harvested from the local machine. Another nod to the original scheme was the use of the string "test" (used in the very first version back in January 2004). This time, if a particular file is retrieved from the Internet and executed, the following Registry entry is made:

```
HKCU\Software\Timeout\"test.exe"
```

It was near this time that the Lodear line of code was being developed for release, initially as standalone software. Lodear was mailed to targets without the use of a worm (a method seen before with Mitglieder, the target list was very well an amalgamation of addresses lifted from previous Trojan infections). By its fifth public iteration, however, Lodear found itself a part of the complex distribution network of other Beagle-related code. Early versions of Lodear used autostart values such as "auto_hloader_key" in the Registry. This somewhat descriptive value is replaced by "anti_troj" as the code moved to its broad-release versions. This is a minor clue to the testing procedures used by Beagle's controller: prior to widespread release, there was much less concern over the malware's public face.

Lodear, as mentioned earlier, is used to retrieve and execute new components. Often, the Trojan will delete any existing files in the download directory created by its brethren before adding new software to a compromised machine (a rudimentary download management function). Lodear.E utilized a list of 52 web servers from which it selected download points for additional code. This code can be swapped at any time by the controller and could include not only a new copy of Beagle, but virtually any type of product desired.

A quick look at two Lodear variants will provide anyone interested with a solid overview of the malware, especially with regard to the Beagle business plan. The early versions of the code used the rather truthful filenames when adding itself to the Windows Registry (strings extraction from Lodear.B):

```
0000203D    0040463D    auto__hloader__key
00002050    00404650    \hloader_exe.exe
00002061    00404661    \hloader_dll.dll
00002072    00404672    explorer.exe
00002084    00404684    SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

The self-start routine covers all bases with three separate Registry keys:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
    auto_hloader_key      "C:\WINDOWS\SYSTEM\hloader_exe.exe"
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
    auto_hloader_key      "C:\WINDOWS\SYSTEM\hloader_exe.exe"
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run
    auto_hloader_key      "C:\WINDOWS\SYSTEM\hloader_exe.exe"
```

And like some previous versions of the Beagle worm, this Trojan injects itself into the Explorer process via a separate DLL, kicked off by the "autoloaded" EXE:

```
C:\WINDOWS\SYSTEM\hloader_exe.exe
C:\WINDOWS\SYSTEM\hloader_dll.dll
```

The "production run" of the software (which was added to the Beagle distribution network) added such things as a deceptive name for the executable:

```
C:\WINDOWS\SYSTEM\anti_troj.exe
```

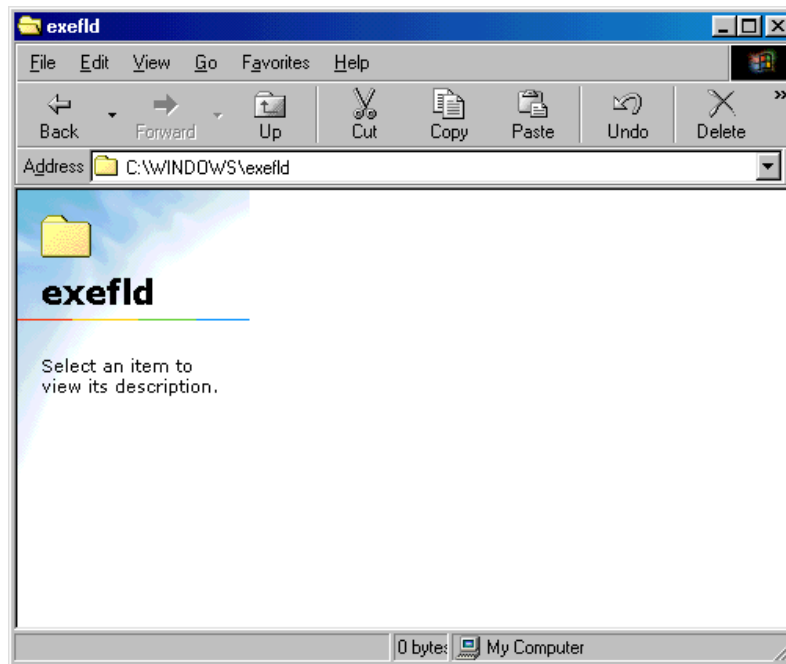
And, more telling of the overall strategy, added a marker to the infected system, indicating that it had been compromised (note the FirstRRRun key which has no associated value that affects the installation/execution):

```
HKEY_CURRENT_USER\Software\FirstRRRun
HKEY_CURRENT_USER\Software\FirstRRRun      FirstRRRun
    dword:00000001
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
    anti_troj      "C:\WINDOWS\SYSTEM\anti_troj.exe"
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
    anti_troj      "C:\WINDOWS\SYSTEM\anti_troj.exe"
HKEY_USERS\.DEFAULT\Software\FirstRRRun
HKEY_USERS\.DEFAULT\Software\FirstRRRun      FirstRRRun
    dword:00000001
HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run
    anti_troj      "C:\WINDOWS\SYSTEM\anti_troj.exe"
```

The later versions of Lodear added a download repository to the infected system, as well as the Trojan:

```
C:\WINDOWS\exefld      1KB
C:\WINDOWS\SYSTEM\anti_troj.exe      11KB
```





After Lodear was established as a means of efficiently moving new code in and out of the Beagle network, additional worm variants continued to be spread. In the last week of December, Beagle.CY¹² turned to sending out “Happy New Year”-titled messages with nefarious attachments. A torrent of Beagle-related code was released with subject lines such as:

Happy New Year
New Year's
New Year's Day.¹³

These messages came with copies of Lodear, wrapped into ZIP archives with the original trick of using image files to deliver the password to users.

In the Middle

Beginning in November of 2005, analysts began seeing a new version of an old scam: “postcard” notifications alerting recipients that there was a greeting waiting for them to download. Dubbed Monikey by researchers, the scam began incorporating revisions of Beagle-related code like LDPinch. Other ties to Beagle include the use of the Netsky mutexes, incorporation of Vipgsm code (another password stealer attributed to the Beagle authors by Kaspersky analysts¹⁴), and the familiar list of filenames used when spreading via network shares:

ACDSee 9.exe
Adobe Photoshop 9 full.exe
Ahead Nero 7.exe
Kaspersky Antivirus 5.0.exe

KAV 5.0.exe
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

Working with new distribution mechanisms is nothing new for the Beagle author. Recall the changes in propagation methods in 2004 when Beagle.Q began using mail client exploits and web delivery.

Another possible shift in delivery comes by way of a worm named Reattle¹⁵. In August of 2005, this mass mailer dropped new versions of Beagle (BY) and used the filename "beagle.exe" when it installed this copy of Beagle (similar to "bbeagle.exe" used in January 2004). Clues such as this don't prove much except that the author of Reattle had access to the Beagle source, but it is at least an interesting branch in the worm's history.

See What Sticks

No matter the combination of threats, the Beagle roll-outs have had a familiar look: a blast of variants over a short time period. This tactic was used during the "war" with Netsky in 2004 and then lost some steam as after Sven Jaschen was arrested.

There was at least one strain of new Beagle code (from at least one of the functional branches) in each month of 2005. In addition, there were sharp spikes in the overall number of iterations in the wild. These occurred as noted below:

- At the beginning of March, there were at least four worm variants and four new Trojans released over two days.
- At the very end of May, three new strains of code were found on the same day.
- On June 26, two additional variants were released.
- August fifth saw a pair of iterations, followed by seven on August 12.
- Eight independent versions of code were released on September 12.
- An additional six incarnations were found on November 23rd.¹⁶

This type of "shotgun" strategy has been used in the past by other malware creators, but it is especially useful for "professional" outfits¹⁷. If one is to establish a profit center prior to having servers taken down by security professionals or clients wiped out by anti-virus signatures, it is necessary to outpace the researchers with either remarkable anti-disassembly tricks or an overwhelming amount of work for analysts. Most coders will

find that the skill of professional analysts makes the former choice difficult to actualize, so they must rely on many minor adjustments in their code over a short amount of time.

A quick attack with multiple weapons is a trick also honed by phishing artists. In a phishing effort, a very close cousin to the work done by Beagle's author, the con requires that a large volume of messages be sent out in a short time period. The scammer can rely upon a small, but consistent, number of people opening and believing the email they are sent. This subset of individuals is then led to a temporary server, probably hosting a number of different scams, where personal information is lifted. Beagle makes use of the same basic plan, but steals personal information through passive means rather than blatantly asking a user to provide it. By simply waiting for a user to enter financial data, Beagle's minions can reap much more data from each compromise – in turn, ramping up the potential profitability of each successful attack.

Moreover, it is very possible that Beagle-infected machines have been used to distribute phishing attempts, as the anonymous mail relays established by Mitglieder are perfect for delivering spam/scams all over the globe.

Management Potential

The control of such a large cadre of software and the zombie network it has built is no small task. Although there is likely no formal set of process management practices sitting on the desk of the Beagle author, there is a rather dedicated professional sitting behind it. As mentioned in the prior works in this series, without law enforcement intervention, there are no limits to the scope of such committed attackers.

There is little point echoing the sentiment that it is unfortunate such a gifted software designer is using their talents for malicious ends. However, there may still be merit in analyzing the Beagle business model for best practice corollaries in the "legitimate" business world.

Appendix: Additional Information for the Curious**Tooso.O Service Kill List**

Ahnlab task Scheduler	KLBLMain	PAVFNSVR
alerter	McAfee Firewall	Pavkre
AlertManger	McAfeeFramework	PavProt
AVExch32Service	McShield	PavPrSrv
avg7alrt	McTaskManager	PAVSRV
avg7updsvc	mcupdmgr.exe	PCCPFW
AvgCore	MCVSRte	PersFW
AvgFsh	MonSvcNT	PREVSRV
AvgServ	navapsvc	PSIMSVc
avpcc	navapsvc	ravmon8
AVPCC	navapsvc	SAVFMSE
AVUPDService	navapsvc	SAVScan
Avxlni	Network Associates Log Service	SAVScan
awhost32	NISSERV	SAVScan
backweb client - 4476822	NISUM	SBSService
BackWeb Client - 7681197	NOD32ControlCenter	schscnt
backweb client-4476822	NOD32Service	SharedAccess
BlackICE	Norman NJeeves	sharedaccess
CAISafe	Norman ZANDA	SmcService
ccEvtMgr	Norton Antivirus Server	SNDSrv
ccEvtMgr	NPFMntor	SPBBCSvc
ccPwdSvc	NProtectService	SweepNet
ccSetMgr	NSCTOP	SWEEPSRV.SYS
ccSetMgr.exe	nvcoas	Symantec AntiVirus Client
DefWatch	NVCScheduler	Symantec Core LC
dvpapi	nwclntc	Symantec Core LC
dpinit	nwclntd	Symantec Core LC
fsbwsys	nwclnte	Tmntsrv
FSDFW	nwclntf	V3MonNT
fsdfwd	nwclntg	V3MonSvc
F-Secure Gatekeeper Handler Starter	nwclnth	VexiraAntivirus
F-Secure Gatekeeper Handler Starter	NWService	VisNetic AntiVirus Plug-in
FSMA	Outbreak Manager	vsmon
FSMA	Outpost Firewall	vsmon
KAVMonitorService	OutpostFirewall	wuauerv
KAVMonitorService	PASSRV	XCOMM
kavsvc		

Registry Values Dumped by Beagle.BW

```

HKCU\Software\Microsoft\Windows\CurrentVersion\Ruln\9XHtProtect
HKCU\Software\Microsoft\Windows\CurrentVersion\Ruln\Antivirus
HKCU\Software\Microsoft\Windows\CurrentVersion\Ruln\EasyAV
HKCU\Software\Microsoft\Windows\CurrentVersion\Ruln\FirewallSvr
HKCU\Software\Microsoft\Windows\CurrentVersion\Ruln\HtProtect
HKCU\Software\Microsoft\Windows\CurrentVersion\Ruln\ICQ Net
HKCU\Software\Microsoft\Windows\CurrentVersion\Ruln\ICQNet
HKCU\Software\Microsoft\Windows\CurrentVersion\Ruln\Jammer2nd
HKCU\Software\Microsoft\Windows\CurrentVersion\Ruln\KasperskyAVEng
HKCU\Software\Microsoft\Windows\CurrentVersion\Ruln\MsInfo
HKCU\Software\Microsoft\Windows\CurrentVersion\Ruln\My AV
HKCU\Software\Microsoft\Windows\CurrentVersion\Ruln\NetDy
HKCU\Software\Microsoft\Windows\CurrentVersion\Ruln\Norton Antivirus AV
HKCU\Software\Microsoft\Windows\CurrentVersion\Ruln\PandaAVEngine
HKCU\Software\Microsoft\Windows\CurrentVersion\Ruln\service
HKCU\Software\Microsoft\Windows\CurrentVersion\Ruln\SkynetsRevenge
HKCU\Software\Microsoft\Windows\CurrentVersion\Ruln\Special Firewall
Service
HKCU\Software\Microsoft\Windows\CurrentVersion\Ruln\SysMonXP
HKCU\Software\Microsoft\Windows\CurrentVersion\Ruln\Tiny AV
HKCU\Software\Microsoft\Windows\CurrentVersion\Ruln\Zone Labs Client Ex
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Ruln\9XHtProtect
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Ruln\Antivirus
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Ruln\EasyAV
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Ruln\FirewallSvr
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Ruln\HtProtect
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Ruln\ICQ Net
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Ruln\ICQNet
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Ruln\Jammer2nd
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Ruln\KasperskyAVEng
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Ruln\MsInfo
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Ruln\My AV
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Ruln\NetDy
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Ruln\Norton Antivirus AV
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Ruln\PandaAVEngine
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Ruln\service
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Ruln\SkynetsRevenge
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Ruln\Special Firewall
Service
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Ruln\SysMonXP
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Ruln\Tiny AV
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Ruln\Zone Labs Client Ex

```

Monikey Mutexes

The familiar set of mutexes, established to keep infected machines free of Netsky:

```

MuXxXxTENYKSDesignedAsTheFollowerOfSkynet-D
'D'r'o'p'p'e'd'S'k'y'N'e't'
_-oOaxX|-+S+-+k+-+y+-+N+-+e+-+t+-|XxKOo-_
[ SkyNet.cz ] SystemsMutex
AdmSkynetJk1s003
_____---->>>U<<<<--_____-
_-oO]xX|-S-k-y-N-e-t-|Xx[Oo-_

```

References

1. The traditional gift for a second anniversary is cotton, with the modern equivalent being china. Researched for this attempt at humor at:

Modern/Traditional Gift Table <http://www.findgift.com/Anniversary-Table/>

And, for the most part, I use the Symantec “Beagle” over “Bagle” since it is consistent with the rest of the paper. I like the use of “anniversary” over “birthday” (which may seem more intuitively correct) because of the marriage of so many different types of applications in the Beagle network.

2. NFL Players Association, “About Us” Page at official site:

<http://nflpa.org/AboutUs/main.asp?faq=How+long+do+most+NFL+careers+last&subPage=InfoForNFLHopefuls&x=7&y=6>

3. The four previous parts of this work were combined into “The Complete Year of the Beagle.” It is available at:

http://www.infectionvectors.com/library/complete_year_of_the_beagle.pdf.

4. More information on the professionalism of malware can be found at infectionvectors.com in the form of the following reports:

One's Complement: On Professional Malware

http://www.infectionvectors.com/library/one's_complement_iv.pdf

Mytob Infantry: Balancing the Malware Equation

http://www.infectionvectors.com/library/mytob_infantry_iv.pdf

5. This point is made in each of the first three sections, available at the link in note #3.

6. Release management is a key concept for numerous best practice and process management structures. ITIL (Information Technology Infrastructure Library) is one such program. More information is available: <http://www.itil.co.uk/>.

7. “Microsoft Solutions for Management: Release Management.” Updated 27 March 2004. <http://www.microsoft.com/technet/itsolutions/cits/mo/smf/smfrelmg.msp>

8. Until there is an overhaul of SMTP, this will be the case. The greatest non-technical (and probably strongest natural enemy) threat will continue to be user awareness and education.

9. Beagle.CX at Symantec:

<http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.cx@mm.html>

10. Tooso.O at Symantec:

<http://www.symantec.com/avcenter/venc/data/trojan.tooso.o.html>

11. Beagle.BQ at Symantec:

<http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.bq@mm.html>

12. Beagle.CY at Symantec:

<http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.cy@mm.html>

13. "Businesses brace themselves against Bagle barrage." 23 December 2005.

<http://www.sophos.com/pressoffice/news/articles/2005/12/baglebrace.html>

14. Yury Mashevsky, Analyst's Diary: "Monikey or: the continuing evolution of Bagle." August 17, 2005.

<http://www.viruslist.com/en/weblog?weblogid=168848252>

15. Reagle information at Trend Micro:

<http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FREATLE%2EF&VSect=T>

16. Pulled from the discovery dates accompanying various write-ups and analyst blogs provided by F-Secure. <http://www.f-secure.com/weblog/archives/archive-082005.html>

September information was bolstered by:

John Leyden, "Bagle blitz unleashed." The Register, reprinted in SecurityFocus, 21 September 2005.

<http://www.securityfocus.com/news/11325>

17. The "antivirus outrun" tactic was used in 2005 by Mytob with great success. The steady flow of new iterations of the worm code allowed the authors to build a solid army of zombie machines.

Additional Release Citations

Details of each Beagle iteration mentioned was researched through independent analysis (often identified by using Symantec's antivirus products) and verification through the various antivirus vendor sites. Below are links to each version mentioned (not otherwise cited), for those seeking greater detail about particular iterations:

Beagle.BG

<http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.bg@mm.html>

Beagle.BK

<http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.bk@mm.html>

Beagle.BN

<http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.bn@mm.html>

Beagle.BT

<http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.bt@mm.html>

Beagle.BW

<http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.bt@mm.html>

Beagle.BY

<http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.by@mm.html>

Beagle.CC

<http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.cc@mm.html>

Beagle.CD

<http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.cd@mm.html>

Beagle.CE

<http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.ce@mm.html>

Beagle.CG

<http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.cg@mm.html>

Beagle.CK

<http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.ck@mm.html>

Beagle.CL

<http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.cl@mm.html>

Beagle.CQ

<http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.cq@mm.html>

Beagle.CZ

<http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.cz@mm.html>

Beagle.DA

<http://securityresponse.symantec.com/avcenter/venc/data/w32.beagle.da@mm.html>

Beagle.DB

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

Tooso

Tooso.F

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

Tooso.G

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

Lodear

Lodear.I

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

Lodeight

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

Reatle

<http://securityresponse.symantec.com/avcenter/venc/data/w32.reatle.e@mm.html>

<http://securityresponse.symantec.com/avcenter/venc/data/w32.reatle.i@mm.html>

Monikey

<http://www.viruslist.com/en/viruses/encyclopedia?virusid=90403>

<http://securityresponse.symantec.com/avcenter/venc/data/w32.monikey@mm.html>

Vipgsm

http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_DROPPER.JP

Monikey/Vipgsm

<http://www.pandasoftware.com/virus%5Finfo/encyclopedia/overview.aspx?lst=det&idvirus=100867>

<http://www.pandasoftware.com/virus%5Finfo/encyclopedia/overview.aspx?lst=det&idvirus=85147>