



# Malware Outbreak Trend Report: Bagle/Beagle

March 6, 2007

## Outbreak Description

The Bagle worm – also known as Beagle – continues to burst across the Internet in 2007. The mass-emailing worm is well known in the anti-virus community since it has been around for over three years, but despite its age the Bagle malware continues to bypass many AV engines and infect email users. The massive-variant email-borne malware has released nearly 30,000 distinct variants since the beginning of 2007.

## Detection Highlights

### Massive Multi-variant Outbreak

Distinct variants since January 9, 2007	~ 30,000
Average distinct variants per day	625
Max distinct variants in a single day	1034

The server-side polymorphic technique of writing and releasing large numbers of variants, each variant distributed via just a few email messages, is used by the malware writers to enable them to continue to defeat traditional AV solutions that are based on signatures or heuristic rules. These common anti-virus techniques depend on prior knowledge of malware to devise tools to block future outbreaks. Since server-side polymorphs like Bagle distribute each variant in a small number of emails and then switch to new variants, by the time traditional AV vendors can develop a signature or heuristic appropriate for one variant its lifecycle has ended and new variants are being propagated. Overwhelmed with a constant barrage of new variants, traditional AV solutions have difficulty keeping up. In the first two months of 2007, an average of 625 new distinct variants were introduced per day, reaching as high as 1000 on peak days.

Server-side polymorphic malware has recently gained popularity due to its success in exploiting the first hours of an outbreak, when traditional AV solutions are most vulnerable. With today's malware releasing such massive numbers of variants in a succession of short bursts, malware writers have made every hour of an outbreak as vulnerable as the first. In the past, traditional AV writers were concerned with the zero-hour of each new outbreak. Today's server-side polymorphs have magnified the damage they can do by using massive variants to make every hour of an outbreak a zero-hour.

What is most remarkable about Bagle is its longevity; the first Bagle variants were detected in January 2004. Despite over three years of awareness, many leading anti-virus vendors have yet to develop a signature or heuristic that can block the myriad of new variants as quickly as they emerge.

NOTE: According to Commtouch's terminology, two variants are distinct if they differ in their MD5 checksum, either by the checksum of the entire executable file or of a portion of it. This means that during the outbreak there could be several such distinct variants for which a single signature or heuristic rule would fit for other anti-virus engines. Nonetheless, also from a code-variation standpoint, the vast amount of such distinct variants groups them into multiple distinct variants that no single signature or heuristic rule can fit.



## Detection Statistics

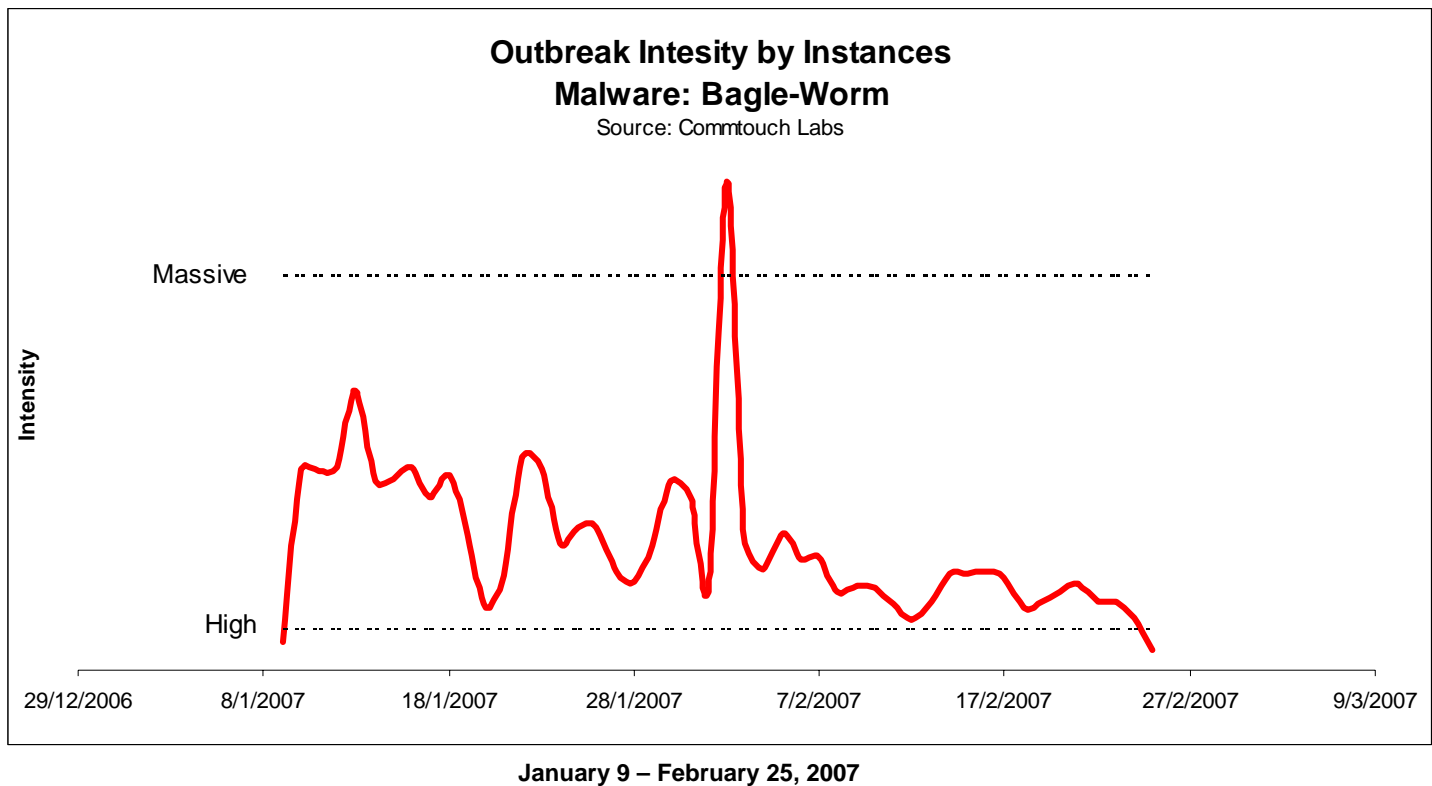
**Data source:** Data for this report were provided by Commtouch Virus Outbreak Detection (VOD) Research Labs, which analyzes email messages proactively for messaging threats.

**Report period:** 09 January 2007 – 25 February 2007

### Intensity by Instances: Multiple Massive Waves

The following graph illustrates the changes in distribution intensity of the Bagle-Worm outbreak throughout the report period. Intensity is measured by the number of separate email messages containing the malware that were monitored by Commtouch. The data lead to the following key conclusions:

- Bagle-Worm is high to massive in volume.
- Bagle-Worm is released in multiple, successive waves.
- Waves range greatly in intensity.
- Bagle-Worm is still in progress three years after its inception.

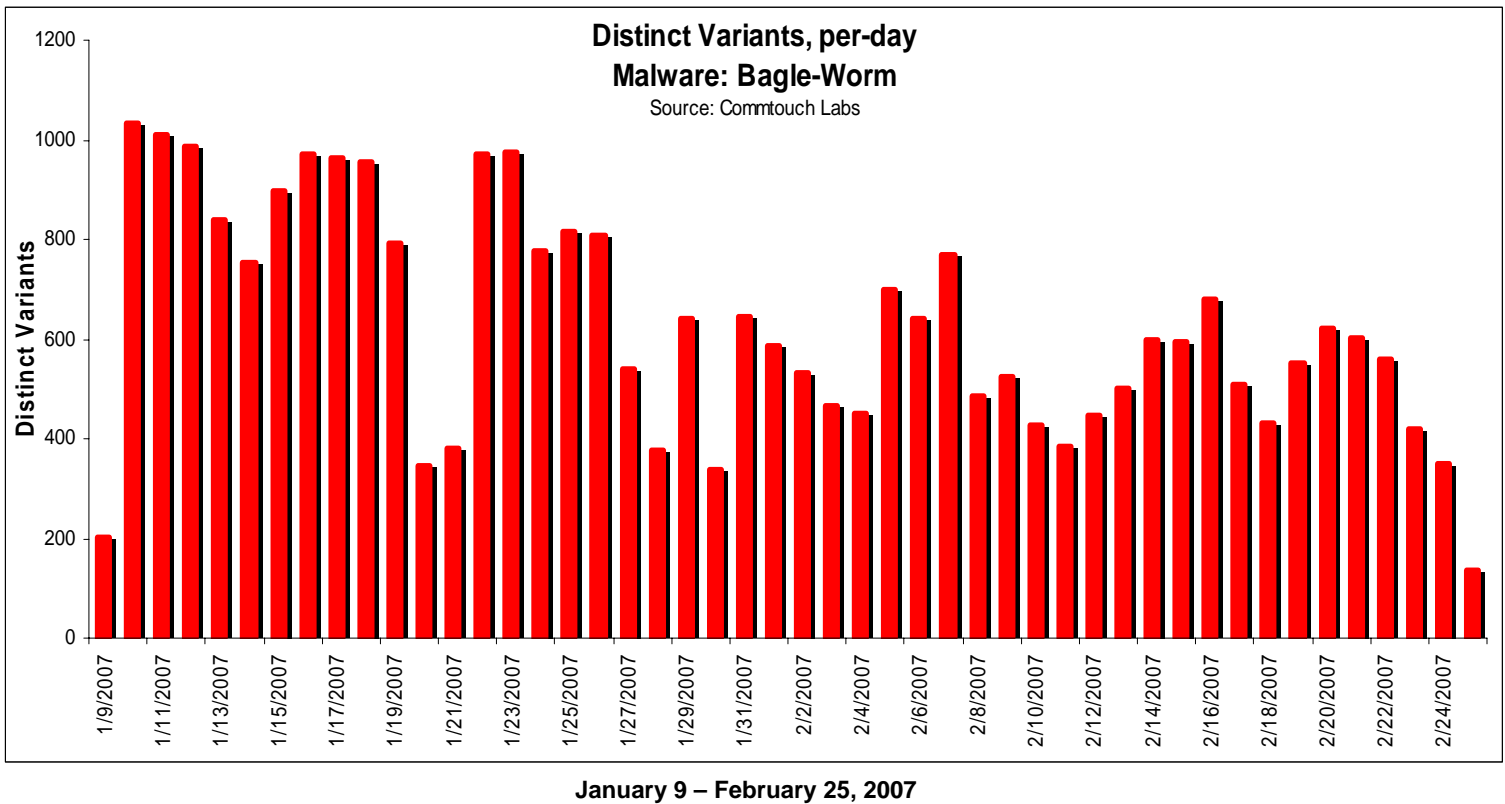




## Distinct Variants: Server-Side Polymorphic Malware

The following graph illustrates the volume of distinct variants monitored by Commtouch each day of the report period. The data lead to the following key conclusions:

- Bagle-Worm is distributed via a massive number of distinct variants each day.
- Even if some signatures protect against a number of variants, the sheer quantity of variants is overwhelming.
- By blasting Internet users with hundreds of different malware variants each day, the originators of Bagle-Worm virtually ensure that many traditional signature and heuristic-based anti-virus scanners will not be able to catch all of them.





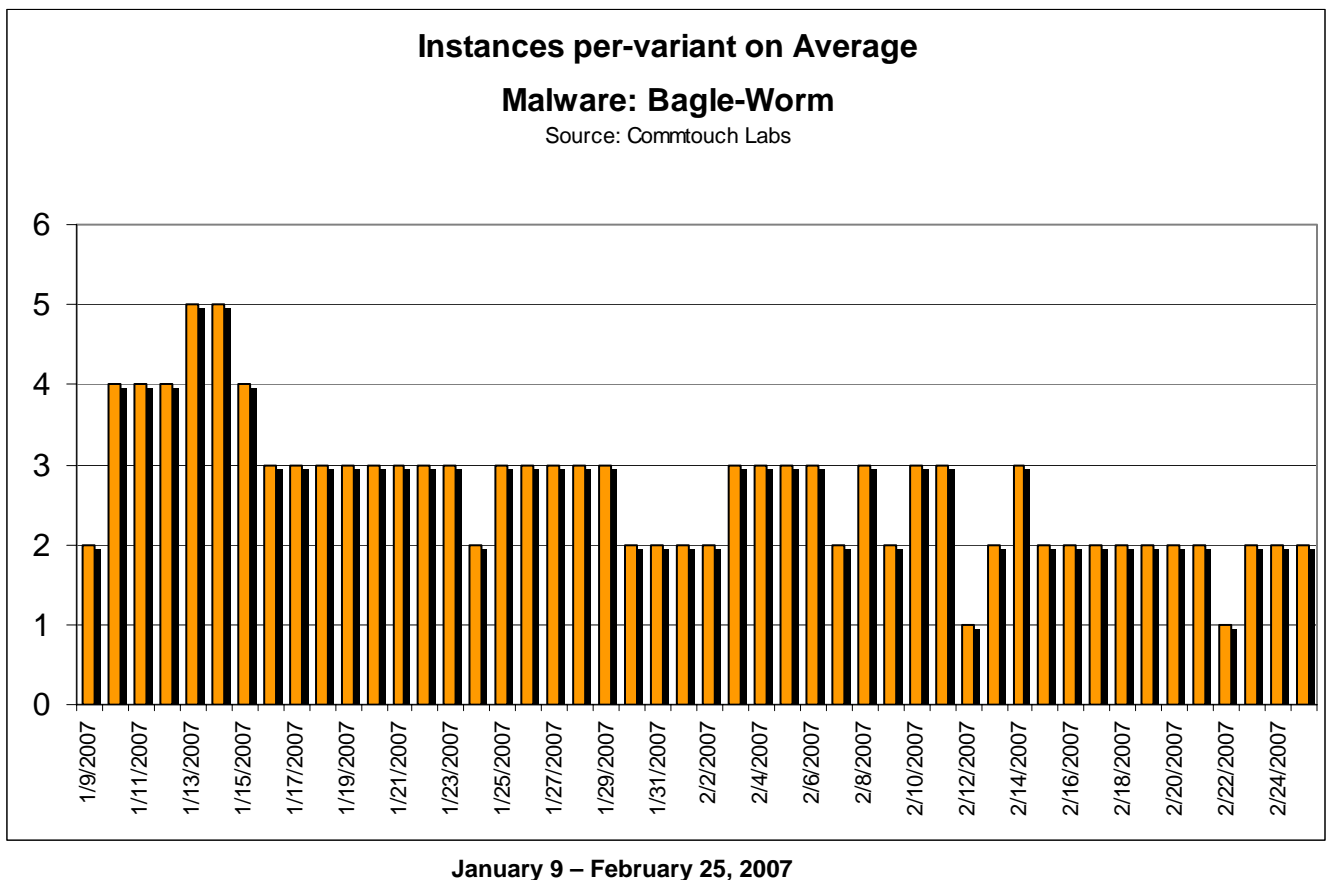
## Instances per Variant: Very Low Volume

The following graph illustrates the average number of instances, or copies of the same code, per variant each day of the report period.

The data lead to the following key conclusions:

- Bagle-Worm writers deliberately and consistently circulate low-volume variants.
- ‘Stealth’ outbreaks are engineered to stay below the radar of AV engines.

By distributing each malware variant in very low volumes (up to a few hundred instances), the malware effectively evades detection by many anti-virus solutions. By “flying under the radar” in this way, numerous malware variants never even reach the stage of being analyzed by the AV vendors to create a signature or heuristic.





## Subject Strings

The following list shows a sample of common subject strings of email messages found to contain the Bagle-Worm malware.

- |                     |                      |                      |
|---------------------|----------------------|----------------------|
| ■ new 14-feb-2007   | ■ price-07-feb-2007  | ■ price_ 09-feb-2007 |
| ■ pric 14-feb-2007  | ■ price-08-feb-2007  | ■ price_ 12-feb-2007 |
| ■ price 05-feb-2007 | ■ price-13-feb-2007  | ■ price_ 14-feb-2007 |
| ■ price 06-feb-2007 | ■ price-14-feb-2007  | ■ price_05-feb-2007  |
| ■ price 07-feb-2007 | ■ price_ 05-feb-2007 | ■ price_06-feb-2007  |
| ■ price 12-feb-2007 | ■ price_ 07-feb-2007 | ■ price_14-feb-2007  |
| ■ price 14-feb-2007 | ■ price_ 08-feb-2007 | ■ price14-feb-2007   |

## Password Protected Archive Names

The following list shows a sample of typical password-protected archive file names found to contain the Bagle-Worm malware. The current generation of Bagle distributes email messages with a password-encoded zip file and an image file containing the password. This is likely a social engineering tactic meant to make the attachments appear to be legitimate and perhaps entice the recipient to open the executable files. Zipping the .exe files may help the malware surpass rule-based anti-virus solutions that block suspicious file types.

- |                               |                            |
|-------------------------------|----------------------------|
| ■ latest_price05-feb-2007.zip | ■ new_price07-feb-2007.zip |
| ■ latest_price06-feb-2007.zip | ■ new_price08-feb-2007.zip |
| ■ latest_price07-feb-2007.zip | ■ new_price12-feb-2007.zip |
| ■ latest_price08-feb-2007.zip | ■ new_price13-feb-2007.zip |
| ■ latest_price09-feb-2007.zip | ■ new_price14-feb-2007.zip |
| ■ latest_price12-feb-2007.zip | ■ price05-feb-2007.zip     |
| ■ latest_price14-feb-2007.zip | ■ price07-feb-2007.zip     |
| ■ new_price05-feb-2007.zip    | ■ price12-feb-2007.zip     |
| ■ new_price06-feb-2007.zip    | ■ price14-feb-2007.zip     |



## Executable File Names

The following list shows typical file names of attached executables found to contain the Bagle-Worm malware. The data lead to the following key conclusions:

- Bagle-Worm utilizes randomization techniques to create a seemingly endless number of executable file names.

- |                    |                    |                    |
|--------------------|--------------------|--------------------|
| ■ agpcstko.exe     | ■ ivxmsytdaaoa.exe | ■ rcarkwhdcgqv.exe |
| ■ akyactgs.exe     | ■ jhrjpyeu.exe     | ■ rxgpolkggy.exe   |
| ■ asqbyrpbg.exe    | ■ lrpelohpumm.exe  | ■ sroaoaezyae.exe  |
| ■ bqnkagrax.exe    | ■ lyvcdiqnezns.exe | ■ tlkivjxsm.exe    |
| ■ cbymrjndnn.exe   | ■ lznkfmcsliuu.exe | ■ unawxjwbzdtw.exe |
| ■ cdtwplevjiiv.exe | ■ mwaltfjz.exe     | ■ veyikkbvurjx.exe |
| ■ coektgntikre.exe | ■ nazwavycji.exe   | ■ vurajvft.exe     |
| ■ dqjeaqpqbfgc.exe | ■ noaexugyav.exe   | ■ xrvzkoqwer.exe   |
| ■ dxygzpbygxx.exe  | ■ punblhtqw.exe    | ■ ypreogpgutpm.exe |
| ■ evppiequvrnp.exe | ■ qbnmbvovxa.exe   |                    |
| ■ fnmzcdmcp.exe    | ■ qosetjvey.exe    |                    |



## Conclusion

Bagle-Worm exemplifies how the use of massive-variants, each with a low number of instances, can be very effective at circumventing traditional signature and heuristic-based anti-virus solutions. The startling fact that the Bagle worm continues to thrive three years after it was first detected highlights the fundamental vulnerability of traditional reactive approaches.

### Commtouch Zero-Hour Virus Outbreak Protection

Commtouch's Zero-Hour Virus Outbreak Protection is an easily integrated component for security and messaging vendors and service providers, complementing traditional anti-virus offerings. The solution enables Commtouch licensing partners to provide their customers with immediate protection against email-borne malware threats, before signatures or updated heuristics are available.

For more information on Commtouch Zero-Hour Virus Outbreak Protection, write to [info@commtouch.com](mailto:info@commtouch.com) or visit [www.commtouch.com](http://www.commtouch.com).

---

Copyright © 2007 Commtouch Software Ltd. Recurrent Pattern Detection, RPD and Zero-Hour are trademarks, and Commtouch is a registered trademark, of Commtouch Software Ltd. U.S. Patent No. 6,330,590 is owned by Commtouch.