



## Q1 2007 Malware Outbreak Trends

### Server-side Polymorphic Malware Explodes Across Email

May 2, 2007

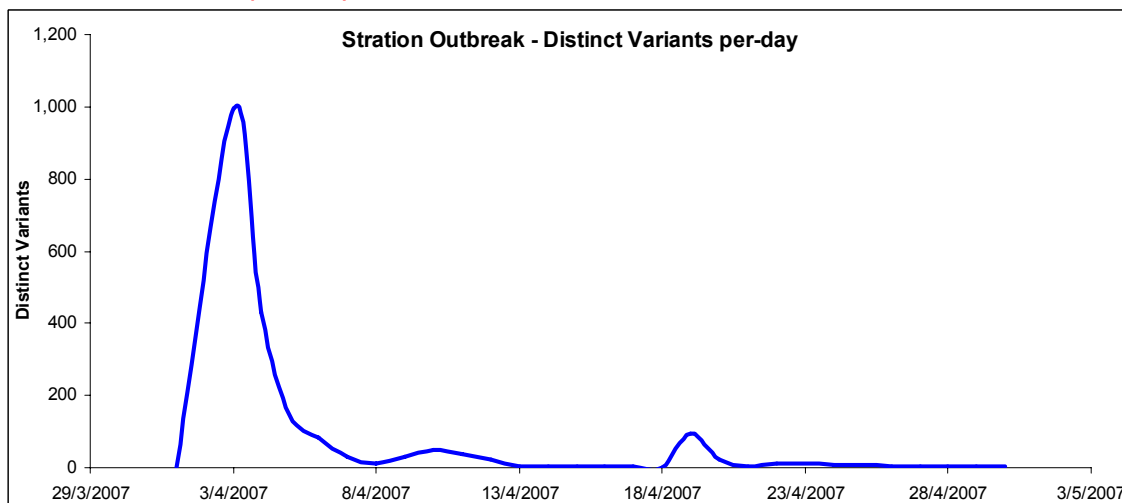
The threat of email-borne malware surged in the first quarter and into the second quarter of 2007. Fueled by the success of server-side polymorphic malware last year, writers of email-borne viruses also learned a few lessons in deception from spammers, and grew to become an even greater menace. By the end of 2006, malware writers had developed highly effective massive-variant distribution and infiltration techniques for bypassing anti-virus engines, and use of these methods grew during the first months of 2007. Virus writers maximized exploitation of the zero-hour vulnerability gap in traditional signature and heuristic based AV solutions. Server-side polymorphic malware is able to evade AV defenses by distributing massive quantities of malware variants in short, intense waves. In the first quarter of 2007, server-side polymorphic malware exploded across email, making every hour of an attack a revolving zero-hour, so now even the anti-virus solutions need protection from viruses.

### Virus writers crack open the zero-hour vulnerability

The emergence of server-side polymorphic malware cracked open the zero-hour vulnerability. Rapid simultaneous release of massive amounts of distinct variants allows each variant to do maximum damage before a suitable signature or heuristic can provide protection. This distribution method proved so effective against traditional AV solutions that it has now become widespread and was most popular type of email-borne malware in the first four months of 2007. Now that server-side polymorphic malware has become well established, numerous examples are circulating the Internet.

### Massive Distinct Variants

Distinct Variants per Day: Stration





In this type of outbreak, the malware writer generates a massive arsenal of unique permutations of the malicious code, known as variants, and then launches them all from multiple infection sources in quick succession, keeping ahead of signatures and heuristics.

**Stration/Warezov** first appeared on the scene over eight months ago. Since the malware is capable of releasing hundreds of new distinct variants each day, AVs have still not found a magic bullet to protect their customers against all possible variants, so the malware continues unabated. Most recently, on April 3, Stration/Warezov unleashed yet another barrage of 995 new distinct variants.

During the quarter, repeated waves of the **Feebs** malware were detected by the Commtouch Research Labs. At one point in early February, nearly 12,000 distinct variant were released during a single day.

The ever-varying malicious code cannot be stopped by a single signature or heuristic, so server-side polymorphic malware is enjoying new found longevity.

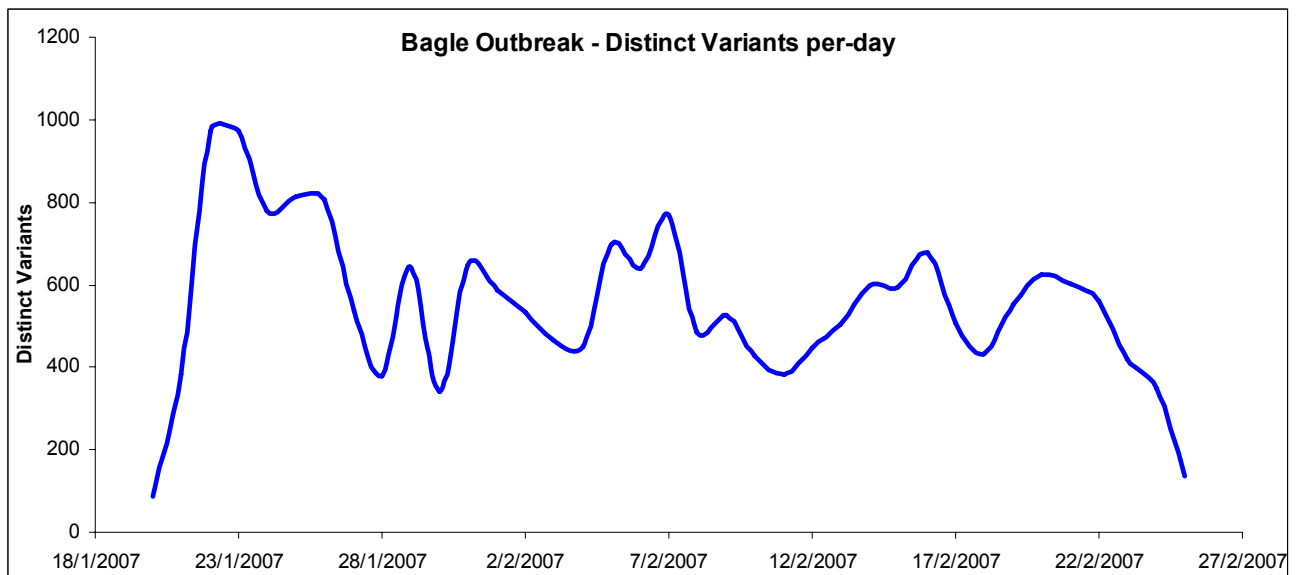
The **Bagle** virus first appeared over three years ago, and continues today as a server-side polymorphic malware.

### Massive Distinct Variants: Feebs

Report period: 13 January 2007 – 18 February 2007

Distinct variants for the entire period	29,778
Average distinct variants per-day	2,175
Max distinct variants in a single day	11,800

### New Distinct Variants per Day: Bagle





## Malware Takes a Lesson from Spam

Spammers have long known the importance of social engineering to entice innocent email users to open their illicit messages. Virus writers recently began adopting these techniques on a large scale to help them slip past email users' defenses. Many email users are suspicious of unsolicited email messages and have been warned time and again not to open strange attachments. Social engineering tactics that have become popular with malware writers use misleading executable names and electronic greetings.

### Misleading Executables

To overcome the 'do not open attachments' warning that has been drilled into email users' heads, virus writers are now disguising malicious executables with friendly, familiar file names. A recent outbreak of the **Storm** virus was distributed as an email attachment named 'video.exe.' The popularity of sending video files via email lowered the defenses of many people and led them to overlook the hazardous '.exe' extension.

The **Nurech** malware attempted to fool its victims by adding benign sounding file signatures such as '.doc', '.jpg' and '.pdf' before the '.exe'. Some typical examples of malware file names:

- rechnung-single.de.doc.exe
- rechnung-singles.jpg.exe
- rechnung.pdf.exe
- t-com.pdf.exe
- telekom.pdf.exe

### Electronic Greetings

Electronic greeting cards are another popular medium which has accustomed the public to fearlessly open links and attachments in email messages. Malware distributors are now taking sinister advantage of this by dressing up their malicious code files as greeting cards. This tactic is particularly plentiful around holidays when people's guards are down and they are used to getting electronic greeting cards as attachments to emails messages.

The **Tibs/Zhelatin** email-borne malware disguised itself as a friendly Valentine's Day greeting coupling affectionate subject greetings with docile sounding file names.

### Social Engineering: Tibs/Zhelatin

#### Sample subject strings:

5 reasons I love you  
a hug & roses  
a kiss for you  
a song to you

#### Sample file names:

flash postcard.exe  
greeting card.exe  
greeting postcard.exe  
postcard.exe



## Sensational Headlines and Enticing Offers

Email-borne malware writers also use sensational subjects that take advantage of piqued interest in topical current events. Recently viruses have been distributed with varying subject lines according to holidays and current events:

- usa missile strike: iran war just have started
- free ipods. details attached.
- mcafee update

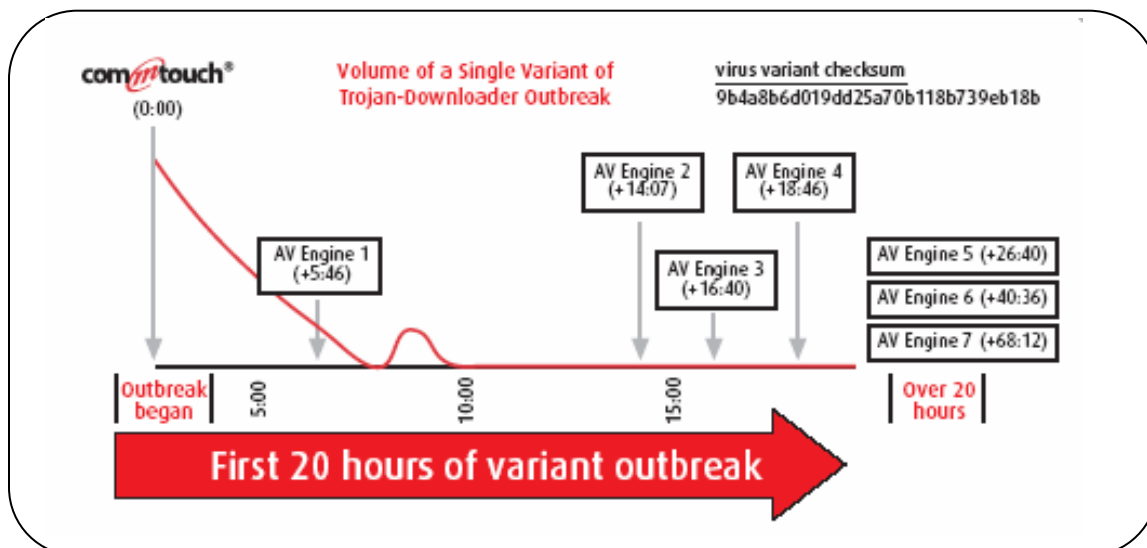
## Slamming Shut the Gates of Information

In response to the continued penetration of server-side polymorphic malware in the first few hours of each new outbreak, network administrators have been left to fend for themselves. Some have enacted broad network policies to block all '.exe' file attachments. This works well to prevent intrusion of malicious executables, but not all '.exe' files are malicious.

According to Commtouch Virus Outbreak Detection Research Labs, roughly half of all executable attachments sent via email are safe, business-critical files. Blocking all attachments with the '.exe' extension is highly restrictive, and would not be necessary if the anti-virus solution were capable of detecting and blocking each new email-borne malware at the zero hour.

## Dynamic Malware Outbreak Defense

The fierce massive-variant, low-volume outbreaks continue to penetrate for weeks, months and even years. This burgeoning method poses a formidable threat to even the most sophisticated heuristic and signature-based AV solutions. As the server-side polymorphic malware distribution techniques have become widespread, the once appealing "zero-hour" doctrine of early protection has been rendered ineffective. In the face of massive-variant attacks launched in continuous waves of short bursts lasting for weeks to months, there is no longer a critical first hour of an outbreak: every hour is now a zero-hour.





Traditional anti-virus solutions have gotten faster at chasing down malware, but they have also trapped themselves in the paradigm of pursuit. In this scenario, the virus writers are always breaking ahead with new variants, and AV solutions are perpetually chasing after them. Commtouch takes a different approach to virus defense. Instead of focusing on hunting for new viruses and racing to catch them with a signature or heuristic, Commtouch monitors billions of messages each week across the globe, in order to identify and block new malware outbreaks the very moment they emerge.

Commtouch Zero Hour Virus Outbreak Protection delivers continuous real-time malware detection throughout massive-variant outbreaks. Based on patented Recurrent Pattern Detection (RPD™) technology, Commtouch identifies and blocks email-borne malware in real-time, providing immediate protection against new variants. As virus outbreak patterns continue to develop, real-time virus outbreak detection may prove the most effective response to coming challenges.

## Appendix: Q1 2007 Top Malware Outbreak Snapshots

- Bagle
- Feeps
- Nurech
- Stration/Warezov

Data for all reports was provided by Commtouch Virus Outbreak Detection Research Labs, which analyzes email messages proactively for messaging threats.

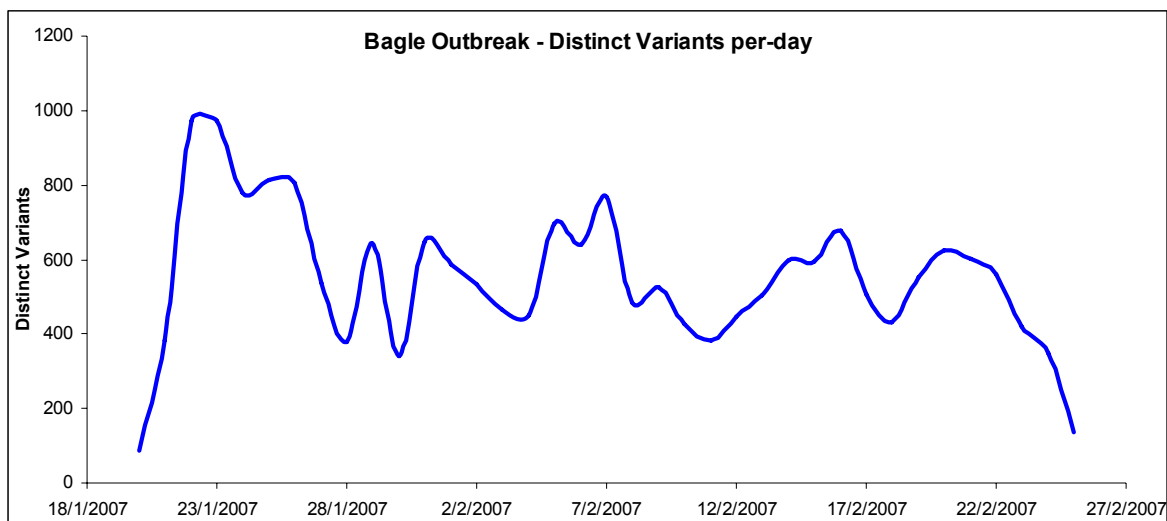


## Malware Outbreak Snapshot: Bagle

### Detection highlights

<b>Report Period:</b>	<b>1 January 2007 – 25 February 2007</b>
Distinct variants for report period	18,594
Average distinct variants per-day	549
Max distinct variants in a single day	974
Sample pwd-protected archive names	latest_price14-feb-2007.zip new_price05-feb-2007.zip price12-feb-2007.zip
Sample Subject strings	new 14-feb-2007 pric 14-feb-2007 price 05-feb-2007 price 06-feb-2007

### Daily Distinct Variants



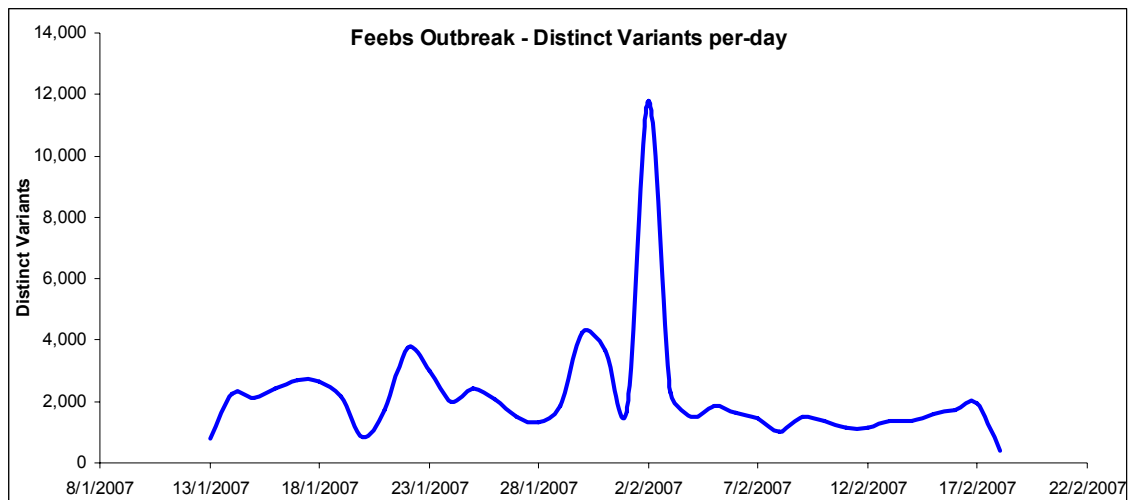


## Malware Outbreak Snapshot: Feebz

### Detection highlights

<b>Report Period:</b>	<b>13 January 2007 – 18 February 2007</b>
Average distinct variants per-day	2,175
Average distinct variants per-day	2,175
Max distinct variants in a single day	11,800
Sample archive names	mail.zip message.zip msg.zip
Sample executable files	data.hta message.hta msg.hta
Sample Subject strings	hello  you have chance to save up to 70% on cialis!  you'll see full details about pavel's enter the kettlebell!

### Daily Distinct Variants



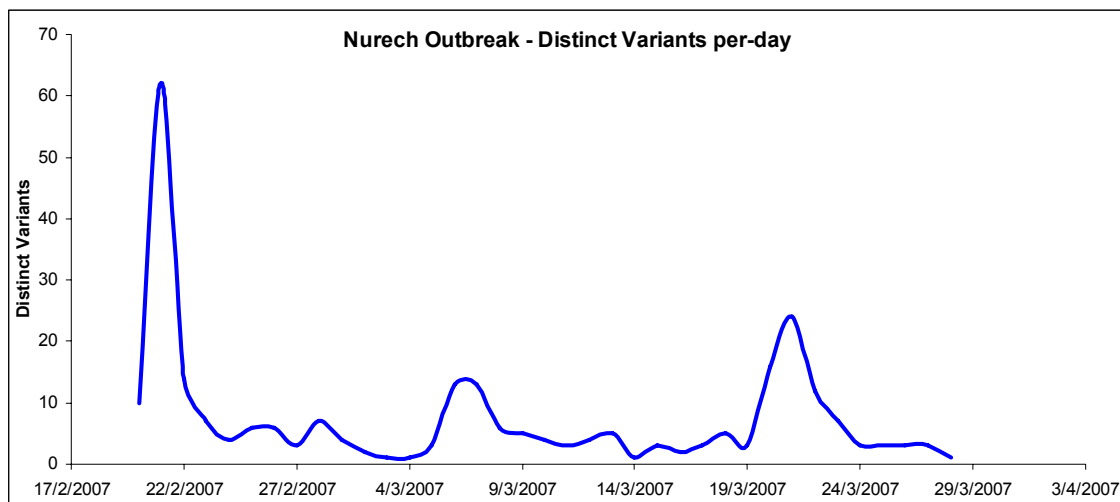


## Malware Outbreak Snapshot: Nurech

### Detection highlights

<b>Report Period:</b>	<b>20 February 2007 – 28 March 2007</b>
Distinct variants for report period	191
Average distinct variants per-day	7
Max distinct variants in a single day	62
Sample archive names	9341251.zip 375367.zip 492799.zip
Sample executable files	rechnung-single.de.doc.exe rechnung.pdf.exe rechnung189.doc.exe
Sample Subject strings	single.de lastschrift nr. 71871 www.single.de anmeldung id 15866 rechnung single.de anmeldung id 48928

### Daily Distinct Variants



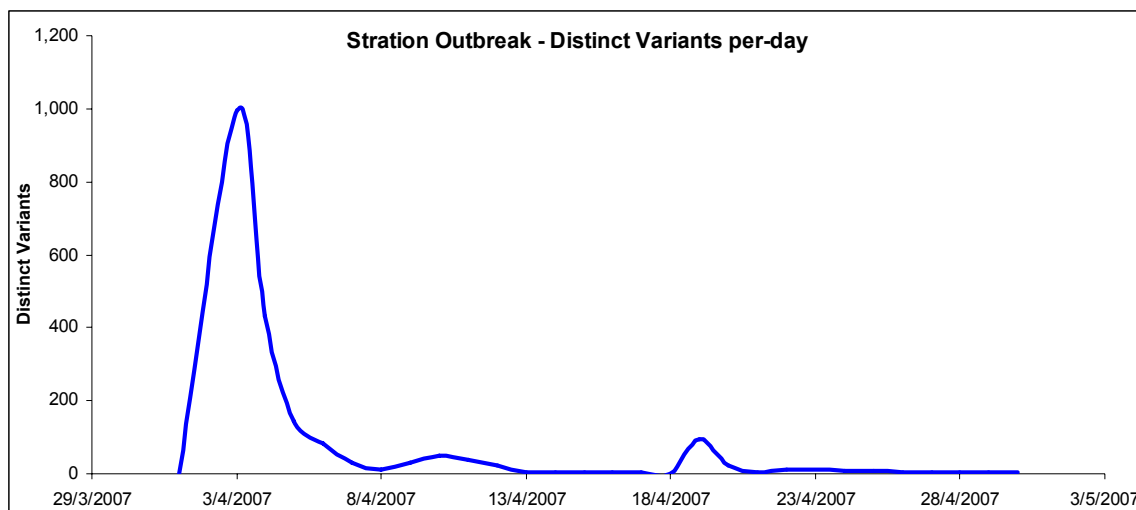


## Malware Outbreak Snapshot: Stration/Warezov

### Detection highlights

<b>Report Period:</b>	<b>1 April 2007 – 30 April 2007</b>
Distinct variants for report period	1,831
Average distinct variants per-day	70
Max distinct variants in a single day	995
Sample archive names	update-kb3125-x86.zip update-kb2703-x86.zip update-kb3140-x86.zip
Sample executable files	update-kb3125-x86.exe update-kb2703-x86.exe update-kb3140-x86.exe
Sample Subject strings	[adult_movies] mail server report. [muscle-worship] mail server report. [moneyplant] mail server report.

### Daily Distinct Variants: Server-Side Polymorphic Malware





## About Commtouch

Commtouch Software Ltd. (NASDAQ: CTCH) is dedicated to protecting and preserving the integrity of the world's most important communications tool -- e-mail. Commtouch has over 16 years of experience developing messaging software and is a global developer and provider of proprietary anti-spam, Zero-Hour virus protection and Reputation Service solutions. Using core technologies including RPD (Recurrent Pattern Detection™), the Commtouch Detection Center analyzes billions of email messages per week to identify new spam and malware outbreaks within minutes of their introduction into the Internet. Integrated by scores of OEM partners, Commtouch technology protects thousands of organizations, with hundreds of millions of users in over 100 countries. Commtouch is headquartered in Netanya, Israel, and has a subsidiary in Sunnyvale, Calif. For more information, see: <http://www.commtouch.com>. The site includes the Commtouch online lab detailing spam statistics and charts.

## About Halon Security

Halon Security, headquartered in Gothenburg, Sweden, develops and manufactures security products with hardware firewalls as their specialty. H/OS is based on BSD, the market's safest operating system. Advanced functionality for antispam and antivirus, Quality of Service, the ability to schedule every services in the appliances, hardware failure avoidance, and Internet provider switching enables Halon Security firewall users to get maximum IT security and performance. Today, Halon Security's firewalls are available in Europe, Asia, and the Americas. For more information go to: <http://www.halonsecurity.com>.

---

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.

Copyright © 2007