



Malware Outbreak Trend Report: Storm-Worm

January 31, 2007

Outbreak Description

The Storm worm – named as such because early messages leveraged the recent major European storm in its subject line – has been inundating inboxes for many days, with tabloid-style email Subject lines like “230 dead as storm batters Europe” and “First nuclear act of terrorism!” and later on “a bouquet of love” and the like. The malware is distributed via email messages in order to infect computers with zombies that can then be used to launch massive spam and malware campaigns.

By creating Subject lines that seem just plausible enough, and attachments with benign-sounding names like “full clip.exe” and “read more.exe,” malware writers have been able to lure unwary recipients into clicking on attached executable files via social engineering tactics.

The Storm worm contains a staggering number of distinct, low-volume and short-lived variants, which are released from multiple sources at brief time intervals. This outbreak follows the trend developed in 2006 with malware such as Stration/Warezov, Feebs, Scanio, Tibs/Nuwar, and many others.

This server-side polymorphic malware consists of thousands of distinct variants, ranging from just a few instances (copies of the same code in recurrent messages) to a few thousands of instances per variant. Commtouch identified and blocked over 40,000 distinct variants of the Storm worm, and there were time periods during those days when the malware accounted for nearly 17% of all global Internet email traffic.

By distributing so many variants simultaneously, the malware distributors overwhelm signature- and heuristic-based anti-virus engines. They effectively guarantee that AV engines will not be able to produce one single signature to protect against all variants. The short lifespan of each variant and the rapid-fire distribution also makes it impossible for these engines to block all of the variants in time, before infection has occurred.

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 was provided by Commtouch Virus Outbreak Detection (VOD) Research Labs, which analyzes email messages proactively for messaging threats.

Report period: 18 January 2007 – 30 January 2007

Detection highlights

First Encountered Instance

Initial Detection	2007-01-18 22:05 GMT
MD5 Checksum of first detection	3812d78fe6a557062980fd41632fe128
Executable Files	full story.exe full video.exe video.exe
Subject String	british muslims genocide

Additional Highlights as of Publication Date

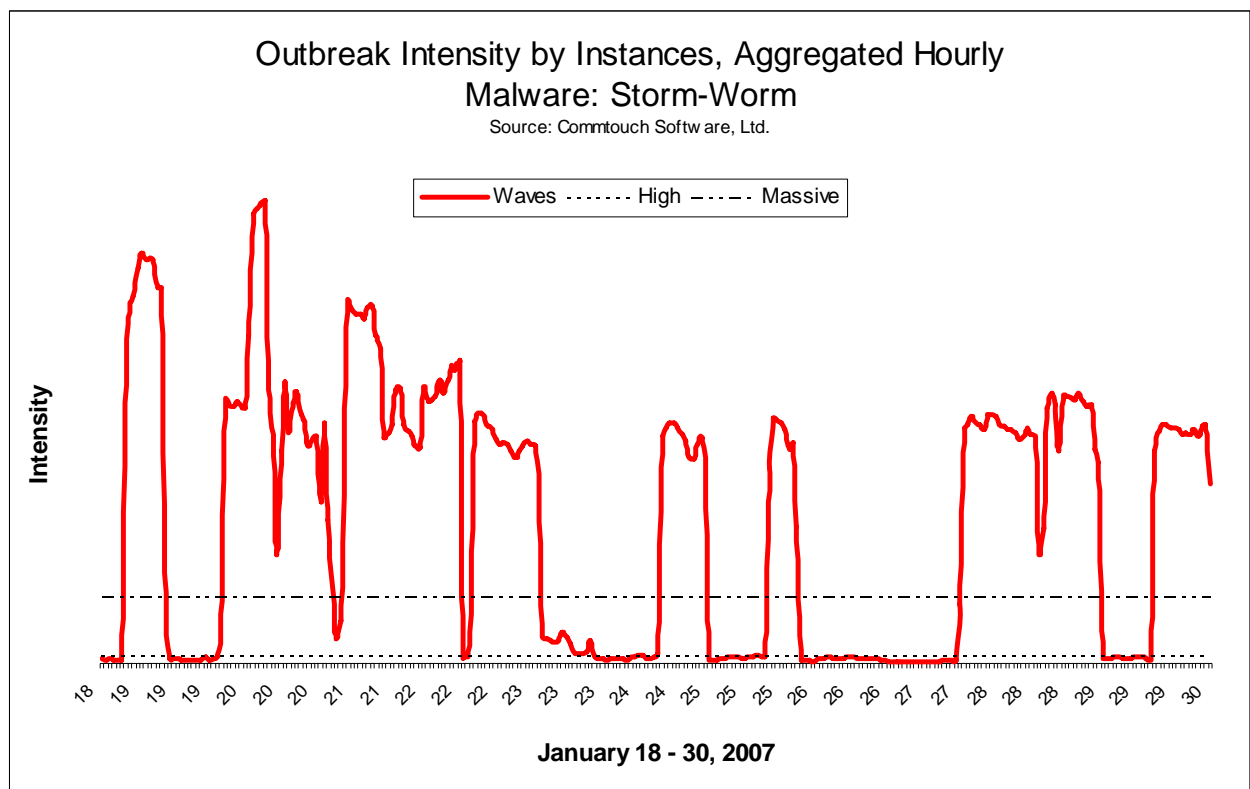
Distinct variants for the entire period	42,652
Average distinct variants per-day	3,824
Max distinct variants in a single day	7,893



Outbreak Intensity by Instances: Multiple Massive Waves

The following graph illustrates the changes in distribution intensity of the Storm-Worm outbreak at hour-long intervals 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:

- Storm-Worm is a massive outbreak
- Storm-Worm is released in successive waves, often multiple waves per day.
- On average, the waves are equal in their intensity
- Storm-Worm is still in progress after almost two weeks since its inception

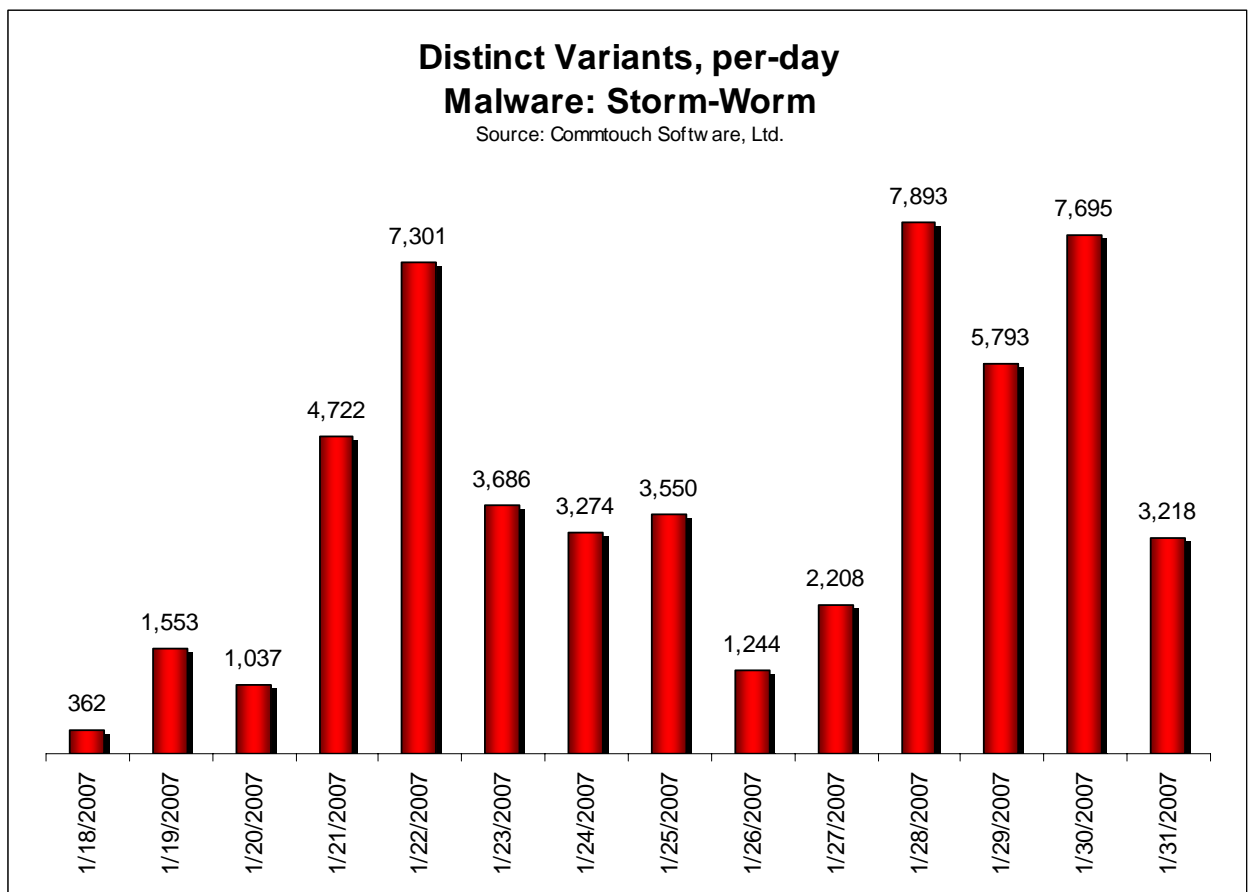




Distinct Variants Graph: Server-Side Polymorphic Malware

The following graph illustrates the number of distinct variants circulating the Internet each day of the outbreak. The data lead to the following key conclusions:

- Storm-Worm is distributed via a massive amount of distinct variants each day
- Even if some variants overlap, the staggering amount is overwhelming
- By blasting Internet users with thousands of different malware variants for several days, the originators of Storm-Worm virtually ensure that traditional signature-based and heuristic anti-virus will not be able to catch all of them.



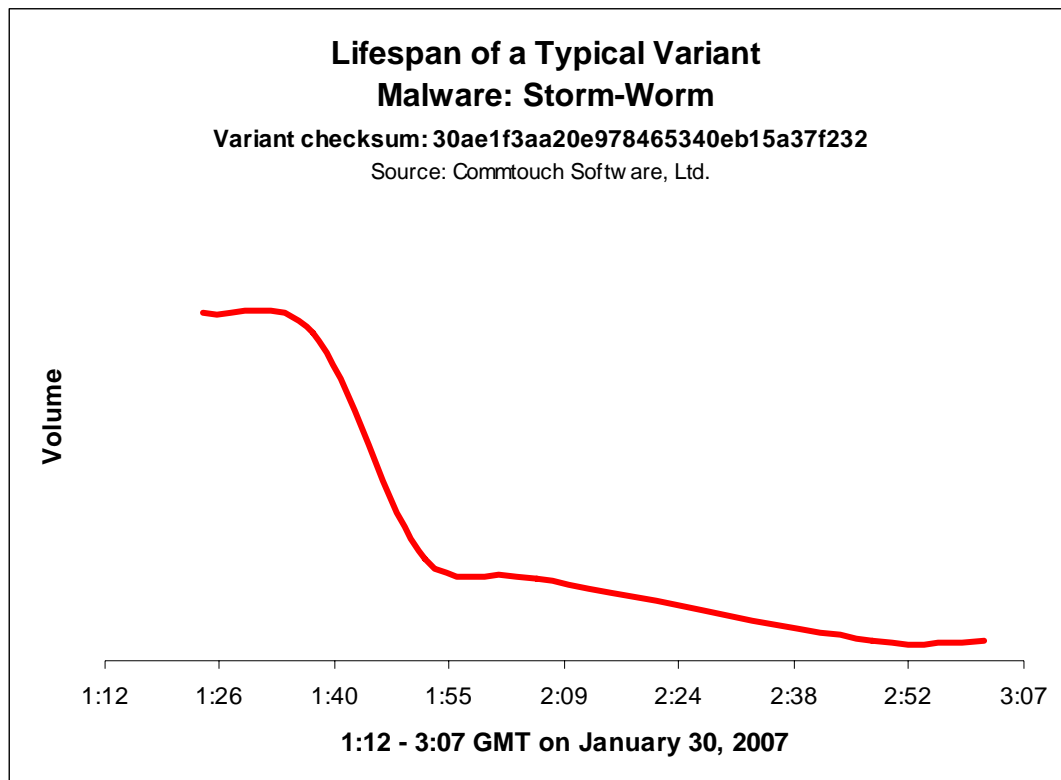


Lifespan of a Typical Variant: Extremely Short

The graph illustrates a typical variant's lifespan. The data lead to the following key conclusions:

- Each variant is distributed for only a few hours and is no longer circulating the Internet by the time that a suitable signature is propagated to end-users

A single variant of the Storm-Worm lasts typically two to three hours, and this is provided that it was carried by more than a single email message. Commtouch's Virus Outbreak Detection (VOD) Research Lab detected that 75% of the variants do not reappear on later days during the outbreak. Since developing an anti-virus signature or heuristic can take several hours, and propagation to subscribers can take up to several days, fighting thousands of consecutive two-hour malware variants with signatures is virtually impossible. Signatures or heuristics will only be effective on those variants that recur.





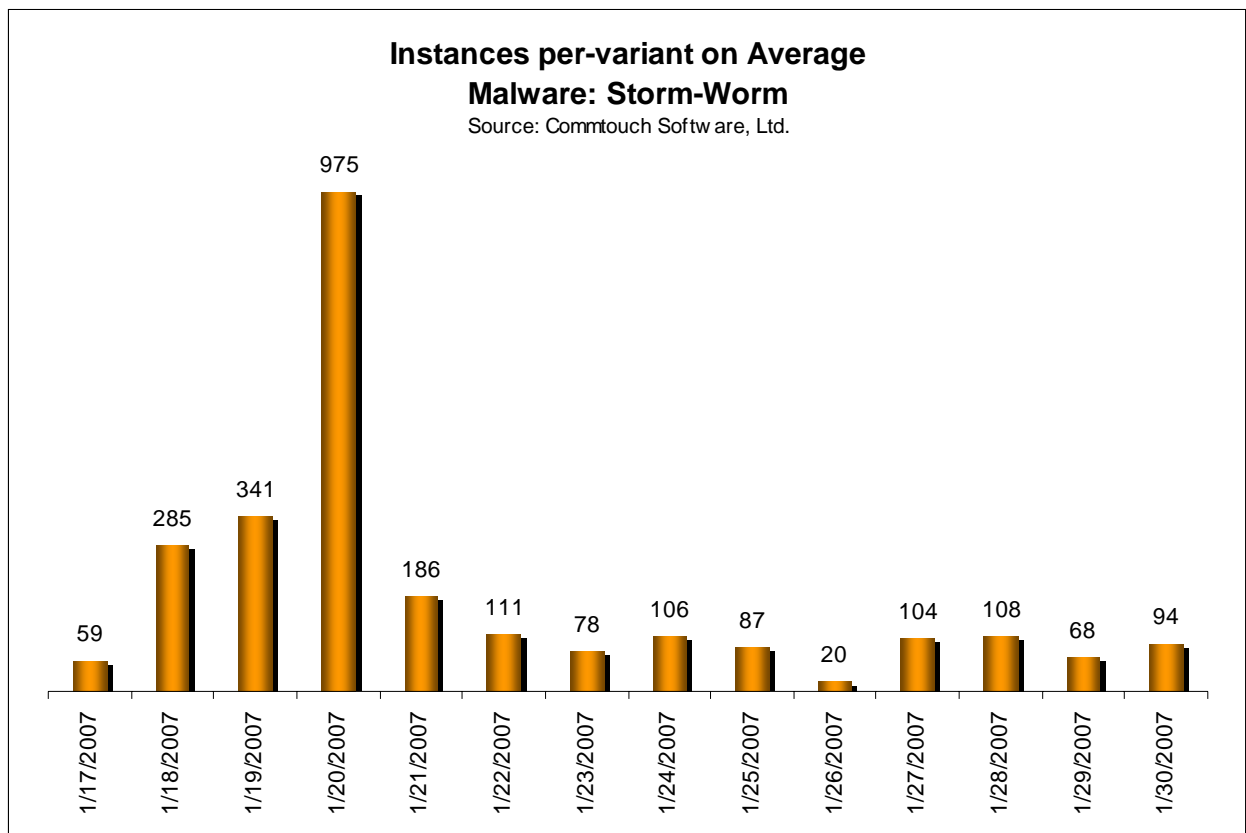
Instances per Variant: Low Volume

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

The data lead to the following key conclusions:

- Storm-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 (dozens to hundreds of 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.





Comparative Information about Storm-Worm Catch Times

The following chart illustrates the catch times of leading signature-based and heuristic anti-virus engines and the Commtouch Zero-Hour™ Virus Outbreak Protection service, which is delivered as a complementary additional layer to traditional AV solutions.

The data lead to the following key conclusions:

- Storm-Worm successfully evades many traditional AV engines during the first hours of inception on each variant participating the test

Catch times of the AV engines represented were provided by AV-Test.org. Commtouch's catch-time was provided by Commtouch.

Variant Appearance Date	MD5 checksum	AV-Test.org ID	Commtouch®	CA eTrust	McAfee	Microsoft	Panda	Sophos	Trend Micro
23/01/2007	dc49dfc97d9698ebede280e8daa7fd7b	2007-01-23_05-16_0001			18:14	30:25	22:04	3:47	9:58
23/01/2007	fe3226e158c99a8c32d82da9b042a87f	2007-01-23_05-16_0001		20:25	14:23	26:34	18:13		6:07
23/01/2007	b487b7dbcf0f8610c62c89e764f1c477	2007-01-23_05-16_0001			16:25	28:36	20:15	1:58	8:09
23/01/2007	871c71605c7432459b0bd2611ea1160e	2007-01-23_05-16_0001			17:55	30:06	21:45	3:28	9:39
23/01/2007	e4b040a3b13997478413993a24e9041e	2007-01-23_05-16_0001			17:25	29:36	21:15	2:58	9:09

Note: Time listed Commtouch is the difference between the detection time, per-scanner, as reported by AV-Test.org and Commtouch detection time as retrieved from Commtouch RPD™ database. Commtouch detection time is not included in AV-Test.org reports.

	Zero Hour detection
	Blocked some of the attack (delay time is noted in hh:mm)
	No detection during analysis period

Deceptive Subject Strings

The following lists typical Subject strings in messages found to contain the Storm-Worm malware. The data lead to the following key conclusions:

- Storm-Worm writers use social engineering methods to lure their victims to open messages containing malware
- Storm-Worm uses tabloid-style Subject strings based on current events and holidays
 - 230 dead as storm batters europe.
 - 5 reasons i love you
 - a bouquet of love
 - a day in bed coupon
 - a hug & roses
 - a killer at 11, he's free at 21 and kill again!
 - a kiss for you



- a kiss so gentle
- a little (sex) card
- a monkey rose for you
- a red hot kiss
- a relaxing coupon
- a romantic place
- a song to you
- a special flower for you
- a special kiss
- a sweet love
- a token of my love
- a weekend getaway
- against all odds
- all for you
- all that matters
- angel of love
- awaiting your love
- baby, i'll be there
- back together
- between us
- bewitching moonlight
- brand new love
- breakfast in bed coupon
- british muslims genocide
- bubble bath coupon
- can't wait to see you!
- chinese missile shot down russian aircraft
- chinese missile shot down russian satellite
- chinese missile shot down usa aircraft
- chinese missile shot down usa satellite
- crazy way to say i luv u
- cuddle me please
- cuddle up
- cyber love
- dancing with you
- dinner coupon
- doing it for you
- dream date coupon
- dream girl
- emptiness inside me
- envoi du message impossible
- error mail
- eternity of your love
- evening romance
- every inch of your body
- everyone needs someone
- executable file violation
- executable or multimedia attachments
- falling in love with you
- feeling horny?
- fidel castro dead.
- fields of love
- first nuclear act of terrorism!
- for better of for worse
- for you
- for you....my love
- forever and ever
- forever in love
- from ksg
- from this day forward
- full heart
- hand in hand
- happiness and continued success!
- happy 2007!
- happy new year!
- happy world religion day!
- he blessed our lives
- heart is breaking
- heart of mine
- hey cutie
- hold me (distant love)
- hold on



- how much i love you
- hugging my pillow
- hugo chavez dead.
- i always knew
- i am complete
- i am lost in you
- i believe
- i can't function
- i dream of you
- i give to you
- i love thee
- i love you mower
- i love you so
- i love you soo much
- i love you with all i am
- i still love you
- i think of you
- i win with you
- i wish
- i woof you
- i would do anything
- i would give you anything
- i'll be your man
- if i could
- if i knew
- in love
- in my heart
- inside my heart
- internet love
- it's your move
- just you
- just you & me
- kiss coupon
- kisses, hugs & roses
- last night was hot

Misleading Executables

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

- Storm-Worm exploits prevalence of video streaming as news medium and users' tendency to consume news in this way
- Storm-Worm exploits popularity of online greeting cards

- click here.exe
- flash postcard.exe
- full video.exe
- greeting postcard.exe
- more here.exe
- full clip.exe
- full news.exe
- greeting card.exe
- postcard.exe
- read more.exe
- read news.exe
- full story.exe
- full text.exe
- video.exe



Conclusion

Storm-Worm is yet another example of the latest email-borne malware trend. It has all four characteristics of a well-established server-side polymorphic malware:

- Storm-Worm is a massive outbreak that continuously hits for weeks, uninterrupted
- Storm-Worm uses vast amount of distinct malware variants
- Storm-Worm variants circulate in low volume
- Storm-Worm variants are short-lived and hardly ever recur

As a result, Storm-Worm successfully manages to evade most traditional AV engines that are based on signature or heuristic rule propagation.

Commtouch Zero-Hour Virus Outbreak Protection

Commtouch's Zero-Hour Virus Outbreak Protection is an easily integrated component for security & 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 or visit 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.