

STORMY WEATHER: A QUANTITATIVE ASSESSMENT OF THE STORM WEB THREAT IN 2007

Raimund Genes, Anthony Arrott, David Sancho
Trend Micro, Germany

Email {raimund_genes, anthony_arrott,
david_sancho}@trendmicro.com

ABSTRACT

The mixed web threat known as Storm is widely acknowledged as the most significant digital security event of 2007. Storm combines the global epidemic aspects of traditional viruses and worms with the stealth and economic activity of today's massive botnets.

Historically, malware outbreaks have been fast-spreading, single-purposed and soon over. Storm continued to spread for many months in successive bursts using different techniques. It sustained its potency by recruiting hundreds of thousands of infected computers into a gigantic botnet. Its purpose appears to be a service-for-hire for multiple fraudulent web activities.

The many months duration over which the Storm infection spread and its successive methods of attack provide far more data to threat researchers than past virus and worm outbreaks. Studying the development of the Storm botnet has been compared to watching an ant colony grow; whereas traditional virus outbreaks are more like studying a bomb explosion.

Conditions before the initial appearance of the Storm worm in January 2007 are compared with measurements made during the various stages of Storm's evolution throughout 2007. Storm provides a first opportunity for quantitative analysis of what may prove to be a new generation of intensive malware outbreaks.

BACKGROUND

On 19 January 2007 a new web threat was discovered to be infecting thousands of computers worldwide using an email message with a subject line about a recent weather disaster, '230 dead as storm batters Europe' [1]. During the weekend there were six subsequent waves of the attack [2]. By 22 January 2007, what became popularly known as the Storm Worm accounted for 8% of all new infections globally [3].

But what appeared at first to be a traditional computer virus outbreak exhibited a novel resilience to anti-virus remedies as it sustained itself through successive waves of infection. Major waves of malware infection and elevated spam volumes occurred in April, June, July and September of 2007. What emerged was a complex adaptable web threat utilizing many of the latest malware techniques in clever coordination.

The sustained attacks of the Storm web threat throughout 2007 may well mark a milestone in the evolution of malicious software. Identified components of this threat have been assigned various names by anti-virus research labs. These include: Storm

(*F-Secure*), Nuwar (*McAfee*, *ESET*), Peacomm (*Symantec*, *Microsoft*), Tibs (*BitDefender*), Zhelatin (*Kaspersky*), Dorf (*Sophos*), Small.EDW (*Trend Micro*) and CME-711 (MITRE). However, much overlap in naming continues to exist among the anti-virus vendors as the myriad of ever-changing components of Storm are identified. Manifestations of Storm are also known by their URL domains, by the subject lines of malicious emails used to distribute its malware (e.g. 'Russian missile shot down Chinese satellite'), and by the filenames of attachments (e.g. 'ReadMore.exe').

The effectiveness of Storm despite its extended period of general exposure has been attributed to several factors that distinguish it from previous malware. These factors have been summarized by Porras *et al.* [4]:

- Smart social engineering: Storm infection links are sent in emails that entice would-be victims by using highly topical and constantly changing spam campaigns, e.g. subject lines about recent weather disasters [5], or holidays [6].
- An ability to spread using client-side vulnerabilities: merely clicking on the wrong URL link from an unsolicited email may be enough to infect one's computer, and the apparent pool of users willing to do this may be in the millions.
- An ability to lure victims to malicious URLs by hijacking existing chat sessions [7].
- An effectively obfuscated command and control (C&C) protocol overlaid on the Overnet P2P network.
- Actively updating the spambot client binaries to adapt to the latest OS upgrades, malware removal heuristics and security patches.

The overall character and malicious purpose of Storm can be summarized according to four dimensions of web threat categorization proposed by Arrott & Perry [8]:

How does Storm infect computers?

Storm infects host computers either by users opening email attachments or by users visiting infected websites. The email messages usually link to an executable attachment (e.g. 'Full Story.exe') or a link to an infected website (e.g. '[click for full story](#)'). In either case, a user click on the link allows Storm to download software that turns the victim's computer into a remotely controlled botnet zombie.

What does Storm do to make money for its perpetrators?

Storm generates income for its perpetrators by enabling 'botnets for rent' in the underground crimeware economy. Rented botnets can be used as powerful spam engines for various advertising and marketing frauds. Rented botnets can also be used in predatory denial of service attacks on targeted websites.

How does Storm do it, technically?

Storm operates as several instances of remotely controlled networks (botnets) of infected computers (zombies) [9]. The botnets can be configured to have their zombies launch spam

email campaigns [10]. Since each zombie has its own IP address, it is exceedingly difficult to identify spam by its sender.

Similarly, zombies can be commanded to participate in distributed denial of service attacks (DDoS) [11]. When thousands upon thousands of zombies with random IP addresses are instructed to focus on a single website, the targeted website can be rendered inoperable in the flood of indistinguishable access requests.

How does Storm protect itself from detection and removal?

In addition to the operational or 'payload' malicious code, Storm infects its hosts with rootkits that operate underneath the host operating system and are able to mask the existence of malicious code running in memory.

Also, Storm provides periodic updates and replacements of the malicious software on the infected hosts. These periodic deliveries may be part of why Storm attacks come in waves.

Finally, the botnet control of the thousands of Storm zombies is itself managed in several innovative ways that protect the individual zombie identities and maintain overall operational integrity of the botnet. These include decentralized control, rotating activation, enhanced encryption and frequent code replacement [12].

MEASUREMENTS

Detections of specific malware components associated with Storm on infected computers worldwide are used to correlate the prevalence of computer infection to the timeline of Storm attacks and the subsequent bursts of spam. An important limitation of these measurements to keep in mind is that anti-virus researchers cannot measure the prevalence of a computer infection until after the threat has been identified and characterized, whether by digital signature or behavioural means. Hence the precise timing and actions of the perpetrators of web threats is typically limited to inference.

Timeline

While some malware components of what would come to be known as Storm were identified earlier, 17 January 2007 is generally considered the launch date of Storm. (The distributed denial of service attacks on several anti-spam websites on 12 January 2007 [11] may have been a pre-emptive strike by Storm's perpetrators in order to make more effective the general assault that began on 17 January 2007.)

Unlike past computer virus outbreaks, Storm in 2007 consisted of successive waves of elevated computer infections initiated on particular dates throughout the year. The most distinguishing features of these successive waves were the massive bursts of spam volume following a distinct change in the malware and distribution techniques used by Storm in each wave. Consequently, the initiation date of each wave is associated with the tactic employed in the subsequent spam burst.

Although exact dates vary among reports, for purposes of our analysis the following timeline of Storm outbreaks in 2007 is adopted from Porras *et al.* [4]:

- 17 Jan 07 – European Storm Spam
- 12 Apr 07 – Worm Alert Spam
- 27 Jun 07 – E-card (applet.exe)
- 4 July 07 – 231st B-day
- 2 Sep 07 – Labor Day (labor.exe)
- 5 Sep 07 – Tor Proxy
- 10 Sep 07 – NFL Tracker
- 17 Sep 07 – Arcade Games.

Malware detection

Records of malware file detections were obtained throughout 2007 from computers using the *Trend Micro HouseCall AV* utility. *HouseCall* scan reports from approximately 100,000 PCs worldwide were collected and analysed for each week. From the scan reports, the percentage of computers infected with a Storm-related malware file was determined. Storm-related malware infections included the following *Trend*-designated threats: TROJ_DUMADOR, BKDR_DUMADOR, TROJ_AGENT.JV, TROJ_SMALL.EDW, TROJ_TIBS, WORM_NUWAR and WORM_ZHELATIN.

Weekly changes in the percentage of computers with Storm-related infections were correlated with the initiation dates of each wave of Storm attack. The outbreaks in late June and early July have been grouped as a single outbreak, as have the outbreaks in September 2007 (see Figure 1).

Following each wave of Storm attacks, AV detections of Storm-related malware files were initially suppressed. This was eventually followed by increased detections as AV products and services responded to the innovations of the Storm perpetrators.

Correlation with spam volumes

The predominant outcomes of the 2007 Storm attacks were massive increases in spam during the weeks following each successive wave of infection. The early waves resulted in elevated spam in the order of tens of millions messages while the later attacks led to increases of over a billion spam messages [12]. Also with each attack the elevated spam was sustained for

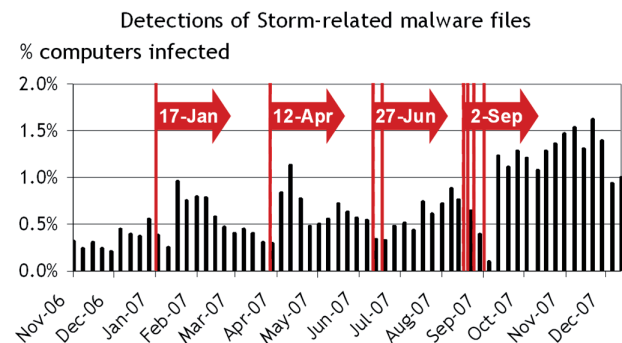


Figure 1: Detections of Storm-related malware files are measured as the weekly average percentage of computers infected by Storm (black bars). This is correlated with the onset dates of the successive waves of Storm attacks during 2007.

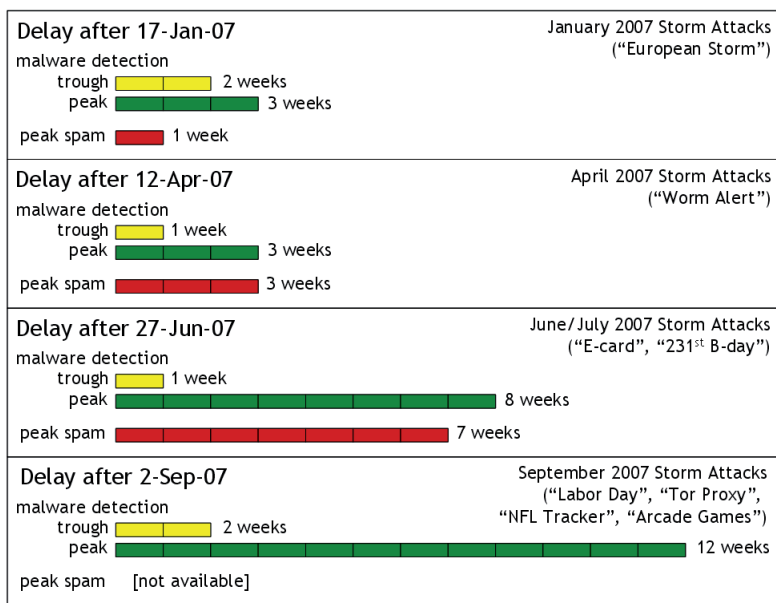


Figure 2: Delays from the initiation of each Storm attack wave until: (a) the trough of initial suppression of AV malware detection (yellow); (b) the subsequent peak of AV detections (green); and (c) the peak of spam elevation resulting from the Storm attacks (red).

longer and longer periods. We use the delay between the initiation of a particular wave until the week of peak spam elevation as an indicator of the sustainability of each Storm wave. During the first three Storm waves of 2007 ('European Storm' in January; 'Worm Alert' in April, and 'E-card'/'231st B-day' in June/July) the delay to peak spam elevation steadily increased from one week to three weeks to eight weeks, respectively (see Figure 2).

While Storm malware detections were consistently suppressed in the first week or two after the initiation of Storm attacks, the delay until AV products reached peak detection steadily increased with each wave from three weeks following the January and April waves to eight weeks in June/July and 12 weeks after the September attacks (see Figure 2).

IMPLICATIONS

The measurements presented here provide only one view of the Storm web threat in 2007. We envision this to be but one building block which, when combined with other studies, may facilitate a fuller characterization of complex coordinated web threats like Storm and the development of more effective countermeasures to mitigate their damage to computer users.

The better web threat researchers are able to characterize Storm, the more effectively countermeasures can be made to combat it and similar innovative web threats. This not only applies to the technical actions of Storm on individual infected host computers but also to the overall recruitment and management of the massive Storm botnets [8,13], to the way these botnets mount effective spam campaigns [10] and to how these botnets evade detection [14].

Each new view into the workings of Storm provides not only a better understanding of its complexity but also typically

suggests a potential innovative countermeasure. The spam campaign analysis of Kreibich *et al.* raises the possibility of anti-spam countermeasures utilizing intelligence of Storm's background 'target liveness' testing and email address harvesting [10]. Holz *et al.* have demonstrated that knowledge of the communication protocols of distributed botnets like those of Storm can be used to mount 'pollution attacks' that disrupt command and control of the botnet's zombies [9].

However, with its combined use of malicious email attachments, infected websites, rootkits and botnets to mount spam campaigns and DDoS attacks, Storm highlights the urgent need for even more integrated web threat security countermeasures. This requires combining and correlating threat information derived from anti-spam, anti-malware and web-filtering solutions.

Cloud-based reputation services can perform ongoing cross-correlation analyses of spam source domains, infected website URLs and executable malware files without the inherent delays associated with the distribution and storage of threat information in individual computers and networks. Internet security vendor *Trend Micro* currently processes over five billion queries a day to its email, URL and file reputation services. Automated root cause analyses of these queries are cross-correlated among spam, bad URLs and malware files to rapidly update in-the-cloud databases for the three types of reputations [15].

REFERENCES

- [1] BBC News. Storm chaos prompts virus surge. January 2007. <http://news.bbc.co.uk/1/hi/technology/6278079.stm>.
- [2] Espiner, T. 'Storm worm' slithers on. ZDNet. January 2007. <http://news.zdnet.co.uk/security/0,1000000189,39285565,00.htm>.
- [3] Keizer, G. 'Storm' spam surges, infections climb. Information Week. January 2007. <http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=196902579>.
- [4] Porras, P.; Saidi H.; Yegneswaran V. A multi-perspective analysis of the storm (peacomm) worm. SRI International Technical Report, October 2007. <http://www.cyber-ta.org/pubs/StormWorm/>.
- [5] Kawamoto, D. Storm Worm rages across the globe. CNET News. January 2007. http://news.cnet.com/Storm-worm-rages-across-the-globe/2100-7349_3-6151414.html?hhTest=1&tag=item.
- [6] Albright, N. Latest stormworm sharing Labor Day greetings. Digital Intelligence and Strategic Operations Group. September 2007. <http://www.disog.org/2007/09/latest-stormworm-filenames.html>.

- [7] Florio, E. Mespam meets zunker (and targets German users). Symantec Security Response Log. May 2007. <https://forums.symantec.com/syment/blog/article?message.uid=305945>.
- [8] Arrott, A.; Perry, D. New approaches to categorizing economically motivated digital threats. Proceedings of the 17th Virus Bulletin International Conference (VB2007). http://uk.trendmicro.com/imperia/md/content/campaigns/predator2008/uk/wp01_virusbulletin_080111us.pdf.
- [9] Holz, T.; Moritz Steiner, M.; Dahl, F.; Biersack, E.; Freiling, F. Measurements and mitigation of peer-to-peer-based botnets: a case study on storm worm. USENIX Workshop on Large-Scale Exploits and Emergent Threats. April 2008. http://www.usenix.org/events/leet08/tech/full_papers/holz/holz.pdf.
- [10] Kreibich, C.; Kanich, C.; Levchenko, K.; Enright, B.; Voelker, G.M.; Paxson, V.; Savage, S. On the spam campaign trail. USENIX Workshop on Large-Scale Exploits and Emergent Threats. April 2008. http://www.usenix.org/event/leet08/tech/full_papers/kreibich/kreibich_html/.
- [11] Stewart, J. Storm worm DDoS attack. Secureworks Research Center. February 2007. <http://www.secureworks.com/research/threats/storm-worm>.
- [12] Smith, B. A storm (worm) is brewing. Computer, vol 41 #2 pp.20-22. February 2008. <http://doi.ieeeecomputersociety.org/10.1109/MC.2008.38>.
- [13] Sarat, S.; Terzis, A. Measuring the storm worm network. HiNRG Technical Report. Johns Hopkins University. October 2007. <http://www.cs.jhu.edu/~sarat/storm.pdf>.
- [14] Stinson, E.; Mitchell, J.C. Towards systematic evaluation of the evadability of bot/botnet detection methods. USENIX Workshop on Offensive Technologies. July 2008. http://www.usenix.org/event/woot08/tech/full_papers/stinson/stinson_html/.
- [15] Trend Micro. Smart protection network. June 2008. http://itw.trendmicro.com/smart-protection-network/pdfs/SmartProtectionNetwork_WhitePaper.pdf.