# The Passing Storm

## The Storm/Nuwar Botnet

Everybody's heard of it, but what is it really?
(And does it still matter?)

Pierre-Marc Bureau
David Harley, BA, CISSP, FBCS, CITP
Andrew Lee, CISSP
Cristian Borghello, CISSP

# Table of Contents



This white paper is based on a French language article for Misc by Pierre-Marc Bureau called "Les Changements Climatiques et les Logiciels Malicieux" ("Climate Change and Malware") and also includes updated material from other papers and articles by David Harley, Andrew Lee and Cristian Borghello.

# Introduction

To adapt to changes in environmental conditions, which happen fast these days, malware has to evolve. Some of the ways in which malware can adapt are clearly illustrated by the ongoing evolution of the so-called Storm Worm. The Storm botnet is generally agreed to have reduced in size since the huge estimates of compromised machines that characterized much of 2007. Nonetheless, the threat continues to attract a great deal of media attention, mainly because of its comparatively novel peer-to-peer network model, its constant updating and adaptability, and the continued effectiveness of its spam campaigns.

The Storm Worm received its name (despite the fact that it's not exactly a worm, or even a single malicious program – particular components may be detected by quite different names, as shown below) after the Kyrill storm that hit Europe in the beginning of 2007. At that time, the authors of the malware used the media attention generated by the storm to persuade users to download and execute a file attached to electronic mail messages.

The name of the Storm Worm creates significant confusion, since no anti-malware vendors use this label. Many vendors, including Microsoft, McAfee and ESET, name this threat Nuwar. On the other hand, Kaspersky uses the label Zhelatin, while Symantec uses Peacomm. To add to the confusion, many detection mechanisms label Storm Worm threat components differently: often they are named according to the run-time packer used to compress and obfuscate them, so they may be flagged with names such as Tibs or Xpack. It is to be noted that these packers are also used by other threats, so that the names are not unique to this family of malware. Indeed, two of the present authors have used Storm-related malware as examples of the major problem the anti-malware industry and its customers have with naming issues. This issue was addressed in a conference paper by two of the present authors presented at the Virus Bulletin conference in Autumn, 2008.[1]

## Various Vendor Names for a Single Storm-Related Sample

| | |
|---|---|
| TR/Crypt.XPACK.Gen | Trojan.Crypt.AP |
| (Suspicious) - DNAScan | Trojan.Crypted-16 |
| Suspicious File | VirTool.Win32.LDE |
| a variant of Win32/Nuwar.CG | Troj/Dorf-BA |
| Trojan.Peacomm | Trojan.Crypt.XPACK.Gen |

Because of the nature of heuristic and generic detection,[2] different components will trigger different heuristic "tripwires" at different stages in their evolution, so the labels by which they are detected may also vary widely across products that use proactive detection techniques rather than relying on conventional signature detection. Thus, a very broad range of names is used in the CME (Common Malware Enumeration) entry for CME-711,[3] a collection of sample identifiers generally associated with the Storm botnet:

- Win32.Small.dam
- W32/Downloader.AYDY
- TR/Dldr.Small.DBX
- Win32/Pecoan
- Trojan.Downloader-647
- Win32/Fuclip.A
- W32/Small.DAM!tr
- Small.DAM
- Downloader.Tibs
- Trojan-Downloader.Win32.Small.dam
- Downloader-BAI!M711
- Win32/Nuwar.N@MM!CME-711
- W32/Tibs.gen12
- Trj/Alanchum.NX!CME-711
- Troj/DwnLdr-FYD
- Trojan.Peacomm
- TROJ_SMALL.EDW

# What is a Botnet?

The term "bot" (derived from "robot") is a general term applied to many types of automated software, often with entirely legitimate purposes such as software that performs administrative and support tasks in IRC (Internet Relay Chat) or IM (Instant Messaging). In the malware arena, however, a botnet is a network of linked systems, controlled remotely, having been compromised by one or more malicious bots or agents and used for attacks that can be carried out more effectively by many linked machines than by individual systems.[4]

Bots do not constitute a single class of malware like viruses or worms, but belong to the general class of Trojans—programs that pretend to carry out some desirable operation, but instead (or also) perform other functions that the victim wouldn't expect and wouldn't want to be executed. Some bots self-replicate (and may therefore be described as viruses or worms), whereas others rely for propagation on external mechanisms such as spamming, tricking the recipient into running malicious code using social engineering.

A bot compromises a victim system without the knowledge of its owner. However, its impact does not depend on how it is manipulated as a single compromised system, but as one of a network of thousands or tens of thousands of other compromised machines. The bot listens for instructions from a remote attacker, or else allows "backdoor access" so that the remote attacker can gain access to the compromised system. The mechanisms by which systems are controlled remotely are referred to as "Command and Control" (C&C). Many botnets have used one or more C&C servers to control compromised systems over IRC (Internet Relay Chat), but we now see a wide range of mechanisms and protocols used.

While IRC remains a common channel for communication between the bot controller and compromised machines that constitute the botnet, other mechanisms are being used more and more. Some communicate over HTTP (not necessarily over port 80). Storm has used eDonkey to communicate via Overnet and the Kademlia protocol peer-to-peer (P2P) protocol. Other botnets such as Nugache have used similar approaches, with varying degrees of success.

A system controlled by an active bot is often called a drone or zombie, and such systems may be compromised (zombified or infected) by a number of vectors:

- Self-launching 0-day exploits using such vulnerabilities as buffer and stack overflows (often implemented as drive-by downloads where just visiting a web site from an unpatched computer is enough to launch malicious code). Software vulnerabilities in browsers or network services can be exploited to execute malicious code to download and/or install malware.
- Links to malicious sites are often distributed in malicious email: despite the lingering presence of many old-style mass mailers distributed as executable attachments, email is now primarily used to distribute malicious links rather than attachments, as this approach is less susceptible to email filtering.
- User-launched email attachments may also install agent malware, or download an installer, though this is far less common with newer threats, as noted in our Mid-Year Global Threat Report for 2008: see http://www.eset.com/threat-center/case_study/GlobalThreatRprtHalfYr20080807.pdf.
- Probes sent over local shares by previously compromised machines may also be an infection vector.

# Storm History

The spam campaign that occurred in January 2007 was only the Storm gang's first global operation.[5] Since then, this malware has continually evolved and adapted: this section gives an overview of that evolution.

# Social Engineering themes

The Storm gang has used a range of social engineering tactics to entice users into opening a malicious attachment or visiting malicious websites, so that their systems will be compromised.

The following table outlines some of the different social engineering themes that have been used by the Storm Worm to incite users into executing their malware. The varying length of time for which each technique is used suggests that the gang monitors their effectiveness in terms of persuasion and tunes its strategies in response. This increases the effectiveness of their botnet, though changing the angle of attack before the world gets too used to a current social engineering theme is also a useful survival technique.

| Theme | Time of usage |
|---|---|
| Actuality events (news items) | December 2006 - May 2007 |
| Electronic greeting cards | June - August 2007 |
| Electronic postcards | 1-Aug-07 |
| VPN Connector | August 2007 (only one day) |
| Beta program | August 2007 (only one day) |
| Video | August - September 2007 |
| Labor day | September 2007 (only one day) |
| Tor installation package | September 2007 (only one day) |
| NFL Season | 1-Sep-07 |
| Arcade game download | September - October 2007 |
| Halloween | October - November 2007 |
| Screen Saver | Christmas 2007 |
| New Year Greetings | 8-Jan-08 |
| Valentine's Day | 1-Feb-08 |
| Electronic greeting cards | 1-Mar-08 |
| April Fools Day | 1-Apr-08 |
| Fake video codecs | April - May 2008 |
| Fake reports of another Chinese earthquake and the consequent probable cancellation of the Olympics | June 2008 |

One of the social engineering themes most used by Nuwar is the fake postcard / electronic card. Figure 1 shows an example captured in March 2008.

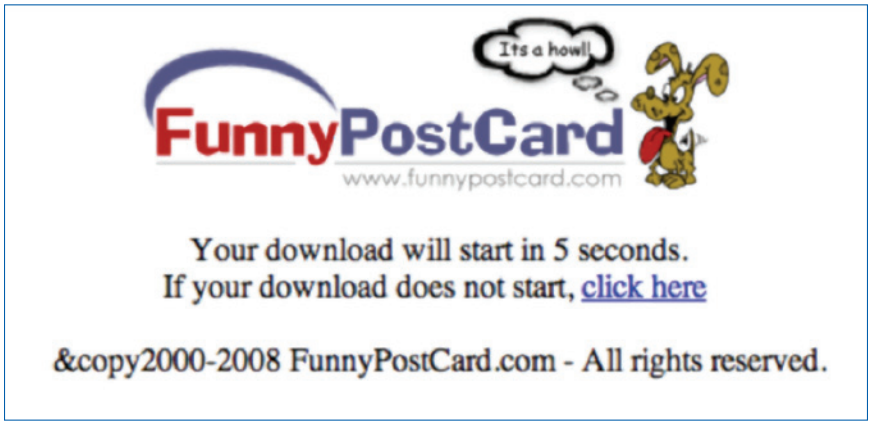


**Figure 1: Fake Virtual Postcard**

Other approaches include malware passed off as free games (Figure 2).


**Figure 2: Fake Games Used as a Lure to Trick Victims into Downloading Malware**

Nuwar's authors release software updates very frequently. The websites that are used to distribute the malware may serve a different file as often as every 30 minutes. The difference between files in terms of functionality is often minor or non-existent, but the difference is enough to evade signatures used in many antivirus products that don't use advanced heuristics and anti-packing techniques.

The Storm botnet is a good example of a completely decentralized (peer to peer) Command and Control network. Historically, it has relied on the Overnet protocol[5] to find resources needed by infected PCs to function effectively as part of the botnet. Examples of such resources include updated versions of the malware, instructions concerning spam content and targets, targets for distributed denial of service attacks (DDoS) and so on. Information flows are encrypted, perhaps reflecting increasing use of legitimate security technologies for criminal purposes – consider, for instance, the recent use of dual-key encryption to compromise user data and force them to buy information that will enable them to retrieve an encrypted file (ransomware).[6]

# How the Storm Botnet has been Used

Botmasters use distributed processing techniques to implement jobs that are rather resource-intensive when performed on single machines, like circumventing Captcha screens using OCR technology. Many of the brute force attacks for which malicious botnets are commonly used require high volumes of participating machines rather than algorithmic complexity so that a large network of desktop machines with a broad range of specifications may be as effective as a smaller group of top-of-the-range, brand new servers.

The Storm botnet has been used for a wide variety of criminal purposes:

- Sending "pump and dump" e-mails (sometimes with the somewhat innovative use of MP3 attachments)[7]
- Common spam, for instance chemical/medical supplies
- Self-propagation through e-mails
- Hosting phishing sites, registering domain names resembling those of well-known banks and directing web requests for these entries to computers infected with Nuwar and running web servers that serve a fake login page.
- Dissemination of banking Trojans, designed to steal banking information.
- Denial of Service attacks (notably against the Stration gang and against anti-malware researchers: three requests in a row for a malicious program from a specific site is assumed to be action on the part of law enforcement or the anti-malware community, and an attack is triggered automatically).

# Does Size Matter?

The real size of the Storm botnet has varied widely over its lifetime, and attempts to estimate its exact size have varied even more widely.[8, 9] The use of fast flux domains and C&C models intended to introduce adaptive self-protective techniques, redundancy and resilience, make precise assessment impractical.

There are certainly bigger botnets such as Kraken out there nowadays,[10] but they don't have the same variety of operation and evolution. In any case, we feel that while stories of botnets running into hundreds of thousands and even into seven figures make good headlines, they focus on the wrong issues. Sheer size may be an issue in terms of some attack processes, but smaller, more adaptable botnets may survive better in the long run.

# Technical Details

Infection Vectors

- Storm infection is very dependent on social engineering, as previously detailed.
- Infection and compromise may also be executed by exploits hosted on web pages advertised through spam
- It's frequently copied to external drives as _install.exe.

Binary Protection

- A completely new packer is released with each new wave of propagation as the malware is spammed out.
- Some binaries are armored with anti-emulation tricks and detection for the presence of a debugger, suggesting that an anti-malware researcher is attempting to analyze the program)
- Code injection
  - The first .EXE drops a system driver and registers it as a system service
  - When loaded, the driver will inject code into services.exe
  - This technique makes the debugging of this program very hard and also conceals its execution and behavior from some security systems.

# Communication Mechanism

Storm communicates with other infected hosts and its controller through a decentralized network, using the Kadmelia protocol, rather than the more commonly used IRC (Internet Relay Chat) or HTTP (Hyper Text Transfer Protocol).[11, 12] Use of a P2P (Peer-to-Peer) communication channel adds resilience to the botnet, since there is no central point to shut down, so no single point of failure (SPoF). Since infected computers don't to use a predefined port number to communicate on their P2P network, they need to keep track of the coordinates used by other nodes participating in the network. Storm Worm binaries always come with a configuration file that contains the coordinates of ten other systems (???) that participate in the Storm botnet. The coordinates include the IP address of the system, its UDP port and a hash that serves as a unique identifier for each peer.

When a computer is infected, it needs to establish a connection with the P2P network. To do so, the computer sends connection requests to the nodes present in its initial list of peers. The systems that are online at that time respond in turn to the newly-infected system with a list of other peers to which they can connect. To establish a reliable connection to the P2P network, a computer will connect to thousands of different nodes[13] before it can use that connection to search for information.

The controller of the Storm Worm uses the P2P network to send commands to participating drones and collect feedback information. In reality, the Storm Worm does not sit waiting to receive commands from its controller: it searches for instructions on its peer-to-peer network. The infected computers will search for a certain hash to find the information they are looking for. This hash is calculated so as to incorporate the date, meaning that a new hash is generated and searched for every day. The content of the search request is a block of binary data encrypted with RSA. The decrypted content is usually a URL pointing to an update module: this is then downloaded and executed by infected computers.

# Communication Encoding

In the fall of 2007, the Storm gang decided to encode all its communication, probably in an effort to avoid detection from intrusion detection systems and to fool researchers that were snooping on their network. The encoding is very basic: that is, an XOR operation with a 40 byte key[14] included in every Storm binary. For more information on encoding and encryption used inside the Storm botnet, we recommend Joe Stewart's work on the topic.[15]

# Conclusions

While security software can mitigate the direct impact of Nuwar and other bot-related malware on individual systems, the wider effects of botnet activity need additional countermeasures. DDoS attacks, for instance, may be somewhat mitigated by firewall, switch and router configuration. Local monitoring and blocking of SMTP traffic from systems other than authorized mail servers can reduce the impact of spam, fraudulent and malicious email spread over open relays and open proxies, while locked down desktops with minimum user privilege make it harder for all malware to execute and self-install.

Signature-based solutions such as "conventional" anti-virus (AV) and Snort signatures are largely reactive, but remain effective in many cases, especially where supplemented with proactive solutions such as ESET's advanced heuristics. The sheer weight of numbers and the speed at which new variants and sub-variants are released necessitates the use of sophisticated behavioral analysis techniques to maintain detection capability. Increased use of runtime packers and obfuscators has lessened the effectiveness of even the most advanced heuristics (though the use of packing is increasingly used as a heuristic in its own right), and persistent repacking slows down the process of analysis and signature generation for specific variants and sub-variants.

A multi-layered security strategy where signature detection is supplemented by generic filtering, intrusion detection and protection and other preventative controls, as well as backup and recovery strategies, remains an operational necessity. Malware has moved towards a black economy model[16] where the gang works according to a sophisticated business model, and the Storm botnet is a classic example of this trend.

The evolution of the Storm Worm is fascinating. Its authors and controllers did not invent anything new, they have simply been planning and executing their operations in an extremely professional way. To our knowledge, there are no other malware families quite so well organized and controlled. For example, before every propagation wave, the malware authors produce a completely new packer around their creation to reduce detection from security solutions. Also, the biggest Storm activity spikes have always occurred at times where beleaguered network administrators are less likely to be able to react to crises, such as Christmas time or after the Kyrill Storm.

There are persistent rumors stating that the authors of the Storm Worm are operating from Russia and that their identity is known to law enforcement agencies.[17] Whether this is so or not, there is some evidence suggesting that the Storm botnet is being abandoned. At the time of writing this paper, the Storm Worm botnet's size is slowly decreasing and the media are already reading the last rites[18] over it, largely because the spam traffic it has carried has practically disappeared.[19]

This decrease in size is mostly due to the fact that the bot herders are not presently maintaining the botnet, which makes it far easier to find and disinfect compromised computers. We are probably witnessing the end of the era of huge botnets (Storm had more than half a million infected computers at the beginning of 2008). Big botnets became victims of their success. By being very effective and "noisy", they attracted too much attention from the media and from security researchers. In the future, we will have to face a larger number of botnets but each will tend to consist of fewer infected computers and attract less media attention.

Nonetheless, it may be premature to throw dirt onto the coffin. If the Warezov team can return to the fray after nearly a year of dormancy,[20] with some new wrinkles and a new delivery mechanism, it's perfectly possible for the Storm team to come back in some form. The kind of inventiveness in bot management and social engineering characteristic of Storm is, unfortunately, unlikely to have expired completely. In any case, there is likely to be a long-lived residual population of infected machines which some blackhat is going to find a use for, sooner or later.

Hopefully, though, this article will contribute to raising awareness of the kind of social engineering that Storm exploited so well in its heyday. While the specific tricks and traps used by the bad guys may be constantly revised and updated, most psychological manipulation can be mitigated by a little experience and knowledge of tricks previously used and a healthy dose of skepticism.

## References & Further Reading


1. David Harley & Pierre-Marc Bureau: "A Dose by any other Name"; Virus Bulletin Conference Proceedings, 2008
2. David Harley & Andrew Lee: "ESET Heuristic Analysis Report - March 2007"; http://www.eset.com/download/whitepapers/HeurAnalysis(Mar2007)Online.pdf
3. http://cme.mitre.org/data/list.html#711
4. David Harley & Andrew Lee: "Net of the Living Dead"; http://www.eset.com/download/whitepapers/NetLivingDead(20080225).pdf
5. Joe Stewart: "Storm Worm DDoS Attack"; http://www.secureworks.com/research/threats/storm-worm
6. http://antivirus.about.com/b/2008/06/09/gpcode-ransomware-just-got-worse.htm
7. MessageLabs: "The Expanding Spammers Toolbox: Latest Stock Spam Technique Launched with 15 Million MP3 Emails"; http://www.messagelabs.com/resources/press/6418. Digital Intelligence and Strategic Operations Group: "Opps [sic], guess I pissed off Storm!, http://www.disog.org/2007/09/opps-guess-i-pissed-off-storm.html
8. Jimmy Kuo: "Storm Drain"; http://blogs.technet.com/antimalware/archive/2007/09/20/storm-drain.aspx
9. Holz et al.: "Measurements and Mitigation of Peer-to-Peer-based Botnets: A Case Study on StormWorm"; http://honeyblog.org/junkyard/paper/storm-leet08.pdf
10. Gregg Keizer:" RSA - Top botnets control 1M hijacked computers"; http://www.computerworld.com.au/index.php/id;1183357273
11. Maymounkov et al.: "Kademlia: A Peer-to-peer Information System Based on the XOR Metric"; http://pdos.csail.mit.edu/~petar/papers/maymounkov-kademlia-lncs.pdf
12. "KadC, a p2p library"; http://kadc.sourceforge.net/
13. Pierre-Marc Bureau: "Nuwar Traffic Analysis"; http://www.eset.com/threat-center/blog/?p=87
14. Dan Goodin: "The balkanization of Storm Worm botnets"; http://www.theregister.co.uk/2007/10/15/storm_trojan_balkanization/
15. Joe Stewart: "Protocols and Encryption of the Storm Botnet"; http://www.blackhat.com/presentations/bh-usa-08/Stewart/BH_US_08_Stewart_Protocols_of_the_Storm.pdf
16. Andrew Lee, Pierre-Marc Bureau: "From Fun to Profit: the Evolution of Malware"; http://www.eset.com/download/whitepapers/FromFunToProfit(20080207).pdf
17. John Leyden: "Russian FSB 'protecting' Storm Worm gang"; http://www.theregister.co.uk/2008/01/31/storm_worm_protection/
18. John Leyden: "Storm botnet blows itself out: but will the zombie network rise again?", http://www.theregister.co.uk/2008/10/14/storm_worm_botnet_rip/
19. Dark Reading: "Storm may finally be over"; http://www.darkreading.com/document.asp?doc_id=165798&WT.svl=news2_1
20. Dan Goodin: "Warezov botnet rises from the grave: undead spam"; http://www.theregister.co.uk/2008/10/16/warezovs_second_coming/

## Glossary

| | |
|---|---|
| **Botnet** | A virtual network of zombie (drone) machines compromised by the installation of a bot and under the control of a bot master (controller). |
| **C&C (Command and Control)** | Channel for communication between the bot controller and the drone (zombie) PCs that constitute his botnet. Used to control compromised machines and direct attacks. |
| **CAPTCHA** | "Completely Automated Public Turing test to tell Computers and Humans Apart". Normally uses a graphic meant to be readable as text by a human but not by a computer other than the one that generated it. |
| **DDNS** | Dynamic DNS |
| **DDoS** | Distributed Denial of Service |
| **Fast Flux** | A technique used by botnets to manipulate DNS in order to hide sites associated with phishing and malicious software, making use of adaptive networks of compromised hosts utilized as proxies. |
| **DNS** | Domain Name System (or Service): handles mapping of IP addresses to domain names. |
| **DoS** | Denial of Service: an attack that damages a site or system's ability to provide a service or execute a function. |
| **Drive-by Download** | Download of a program to a system without the system user's knowledge or action, especially from a web page. |
| **Drone** | Another term for a zombie: a computer system compromised by the installation of a bot. |
| **Extortion** | Illegally obtaining money by threats, e.g. of implementing or continuing a Denial of Service attack.. |
| **Keylogging** | Capture of sensitive information such as login information by monitoring and logging keystrokes, especially when subsequently forwarded to a remote attacker. |
| **Optical Character Recognition (OCR)** | Programmatic technique for extracting textual information and editable text from a graphic image. Nowadays much used, unfortunately, as a technique for 'breaking" a captcha. |
| **Packer** | See"Runtime Packer" |
| **Phishing** | A generic name for various forms of fraud in which the scammer tries to trick victims into giving away sensitive data, usually financial, using spoofed email and web sites. |
| **Port** | In this context, a number that identifies the channel |

| | |
|---|---|
| | used by an Internet service (for example, TCP/25 is SMTP–Simple Mail Transfer Protocol.) |
| **Pump and Dump** | An email scam where the recipient is encouraged to buy stock at a low price on the promise that it will appreciate dramatically in value in the very near future. However, the scammer already holds a significant quantity of the stock and sells the hyped stock at a profit. When the hype stops and the market notices that everyone is selling, the price plummets again. |
| **Runtime Packer** | A type of program originally intended to compress an executable so that it takes less space on disk, decompressing itself into memory when needed. Malware authors noticed long ago that passing a known malicious program through one or more packers results in obfuscation of the code, making it harder for malware-specific scanners to recognize an already-known program. However, the use of a packer can sometimes be used as a heuristic to identify probably malicious code. |
| **Zombie** | Synonym for drone: a PC compromised by a bot, and therefore under the control of a bot master. |


**Corporate Headquarters**

ESET, spol. s r.o.
Aupark Tower
16th Floor
Einsteinova 24
851 01 Bratislava
Slovak Republic
Tel. +421 (2) 59305311
www.eset.sk

**Americas & Global Distribution**

ESET, LLC.
610 West Ash Street
Suite 1900
San Diego, CA 92101
U.S.A.
Toll Free: +1 (866) 343-3738
Tel. +1 (619) 876-5400
Fax. +1 (619) 876-5845
www.eset.com





TPS20081202