Storm Worm DDoS Attack

- **Date:** February 8, 2007
- **Author:** Joe Stewart

A number of anti-spam websites came under a distributed denial-of-service attack on January 12, 2007. The trojan responsible for the attack was one of several dropped onto systems infected by a seeding of the email virus which later came to be called "Storm Worm", also W32/Small.DAM and Trojan.Peacomm.

Researching further back in time, we find that variants of the same malware family were released in similar fashion in November, December and early January. Many AV companies labeled the previous variant "Win32/Nuwar".

P2P Botnet Functionality

When Storm Worm runs, it attempts to link up with other infected hosts via peer-to-peer networking. Through this conduit it gets a URL which points to a second-stage executable, which in turn downloads additional stages onto the infected system.

Those stages are usually named game0.exe through game5.exe, and each component has a specific function to serve.

```
game0.exe - Backdoor/downloadergame1.exe - SMTP relaygame2.exe - Email address stealergame3.exe - Email virus spreadergame4.exe - DDoS attack tool game5.exe - Updated copy of Storm Worm dropper
```

The master component is run from a kernel rootkit driver (%windir%\system32\wincom.sys) which inserts its code into the services.exe process. This is the part which is responsible for linking up via the P2P network.

The protocol in use is actually the eDonkey/Overnet protocol, which has been adapted by the virus author as a means to distribute the second-stage URL without being shut down as it might be if the URL was hard-coded in the body of the virus or was downloaded from another website.

The P2P component has a hard-coded list of over 100 peers in the body of the trojan, which it stores in %windir%\system32\wincom.ini.

```
D943283AB63746B8E62436682728DDD4=5511238154BD00D6E46BF02E64D940E37EECCC982584A8=573349B6124A00AA71F6CB9B9BB53D9FA47B74B189E67E=8002DE60541D0091692CA8A8B7F9DA5E68E749CD8E9BF6=968C8C30276A0090574FE5893DC69889C2E041CE549CF7
```

The part in front of the equals sign is the peer hash, the part following is the IP address and port. For example, 5511238154BD00 = 0x55.0x11.0x23.0x81:0x54BD or 85.17.35.129:21693. These peers are contacted to see if they have a particular hash the trojan is looking for. They in turn direct the infected client to other peers which may have the hash, until one is found.

In a normal eDonkey/Overnet P2P exchange, the hash value is the MD4 sum of a file located on a peer. In the Storm Worm P2P code, the hash value doesn't actually correspond to a file, it is generated using an algorithm which takes as input the current system time and a random number between 0 and 31, outputting one of 32 possible hashes for any given day.

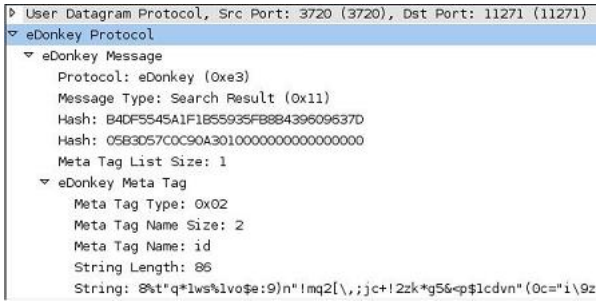


Illustration 1: eDonkey/Overnet protocol in use by Storm Worm

When a peer responds with a search result containing this hash, it returns the searched-for hash, and also provides a "result" hash in the response packet (the result hash is 05B3D57C0C90A3010000000000000000 in the illustration). This hash is used as a decryption key by the Storm Worm P2P code, in concert with a second decryption key which is hard-coded in the body of the trojan itself. Also in the response packet is a single meta-tag named "id". The body of this tag contains an encrypted string which contains the URL of the second-stage executable. No files are ever transferred between hosts; the meta-tag and the result hash are the only things the trojan needs from the peers in order to find the download site.

DDoS Functionality

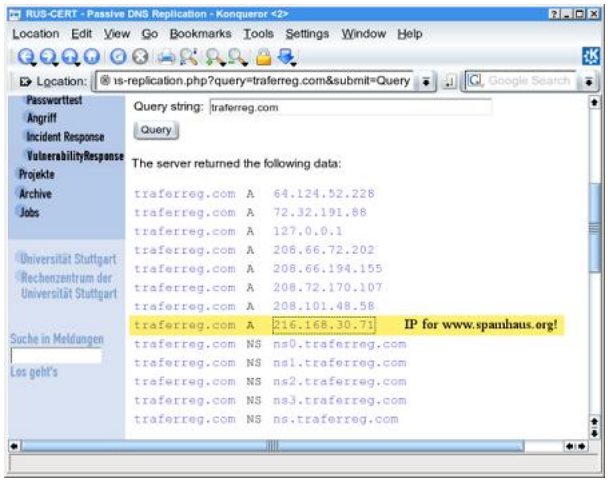
The DDoS attack is conducted by game4.exe. It receives the target IP address and attack type by downloading a configuration file from a hard-coded website in the body of the trojan. Attacks can be a port 80 TCP syn flood, or an ICMP ping flood, or both. The configuration file specifies the target by IP address only; the tool has no provisions to resolve DNS names to addresses.

In addition to the anti-spam sites we saw being attacked, the configuration file has also been seen containing IP addresses for websites associated with the Warezov virus - another spam system, probably operated by a competing spam group. It seems that this spam group is prone to attack anyone that interferes with its business model, be it anti-spammer or spammer, or in some cases, third-party services. For example, one IP address being attacked was capitalcollect.com, a money transfer service. Following is a partial list of IP addresses seen targeted by the Storm Worm DDoS component during the time we were monitoring its control mechanism:

Target IP Address	Corresponding Domain Names
67.15.52.145	stockpatrol.com
63.251.19.36	spamnation.info
216.118.117.38	esunhuitionkdefunhsadwa.com (Warezov)
208.66.194.155	krovalidajop.com, traferreg.com (Warezov)
66.246.246.69	shionkertunhedanse.com (Warezov)
69.72.215.236	capitalcollect.com
208.66.72.202	adesuikintandefunhandesun.com (Warezov)
66.246.252.206	huirefunkionmdesa.com (Warezov)

Table 1: Partial list of IPs attacked by Storm Worm

On Jan 30, the spamhaus.org website also came under attack from traffic closely resembling the packets closely resembling the earlier attacks. However, it soon became clear that it was an unintended target - apparently the Warezov spammer(s), in an attempt to deflect the DDoS attack, changed the DNS "A" records for some of their domains to point to the spamhaus.org IP address. When the Storm Worm DDoS controller file was updated to reflect the new IP address, the attack on spamhaus.org began.



It is worth mentioning that multiple DDoS attacks have occurred in the December and January timeframe, targeted at anti-spam sites and anti-rootkit software developers. An attack was even launched against the personal website of the author of this analysis, in retaliation for research into botnet-controlled pump-and-dump stock spam. These attacks have been determined to be from no fewer than three independent and unrelated botnets. We see now the spam war is escalating to new levels. It could be that the spammers have been emboldened by the successful attack on BlueFrog last year, which shut down a service that was affecting the spammers' ability to conduct their "business." With no repercussions from that attack, or even older attacks which shut down certain DNS blocklists, it seems that more spammers are willing and able to attack anyone who threatens their profit potential.