

Selected Virus Outbreaks June 2006

June 2006, similar to the previous month, was characterized by many low-intensity multi-variant attacks. Some were variants of recent virus outbreaks, and others were much older viruses coming back in new forms (e.g. MyDoom, MyTob, Netsky). The rapid "spraying" of dozens or hundreds of virus variants simultaneously virtually guarantees that some versions will get past each of the AV vendors. Below are some samples of viruses that got past many of the leading vendors at the "Zero Hour."

Outbreak Variant	MD5 checksum	AVTest-Org Reference ID	Commtouch	Benchmark Data from AV-Test.org							
				CA eTrust	Kaspersky	McAfee	Norman	Panda	Sophos	Symantec	Trend Micro
Bagle	eb12fa0712add965e5cdfefb9d91035	2006-06-22/19_17/01	Zero Hour detection	12:27	2:06	9:08	21:03	7:43	3:01	8:25	4:29
Bagle	078af2d67761d3502919875d625af1e3	2006-06-22/20_10/01	Zero Hour detection	12:25					2:59	8:23	4:27
Breblipot	95f902ad83a712d6c209b37a4b5f9ade	2006-06-19/20_40/01	Zero Hour detection	12:41	3:16			11:31	0:58	11:29	3:18
Ebay	c758167de38ef7453db628a24af769e1	2006-07-01/15_00/01	Zero Hour detection	30:08	7:05	22:36	Had not released signature at time of publication		1:32		16:14
Lovegate	f4d1c205d39b5c2c0f5bc674bec23132	2006-07-01/15_00/01	Zero Hour detection	Had not released signature at time of publication	Had not released signature at time of publication						
Lovegate	ae71ef266239d62f2a0ef9ac304f042b	2006-07-01/15_00/01	Zero Hour detection	Had not released signature at time of publication	Had not released signature at time of publication						
Mydoom	e3f4fb53db6abcafcbe0a28a65392470	2006-06-28/22_19/03	Zero Hour detection	Had not released signature at time of publication	Had not released signature at time of publication						
Mytob	4cfd4b80998e9a5c86a906e2ba4c563c	2006-06-29/08_54/01	Zero Hour detection	Had not released signature at time of publication							
Scano	14fec4c8658cb2b1e4e5d98f606a67f	2006-07-01/15_00/01	Zero Hour detection	Had not released signature at time of publication							38:57
Netsky	0816290bef98e984da10798d39de6de6	2006-06-07/19_39/01	Zero Hour detection	Had not released signature at time of publication							
Feebs	962df2b2be43cdfc492b665c36d86807	2006-06-05/14_02/01	Zero Hour detection	Had not released signature at time of publication	21:06				85:00		
Feebs	2505442e53a92825ba1849ec10979278	2006-06-05/14_02/01	Zero Hour detection	Had not released signature at time of publication	16:23				80:17		

	Zero Hour detection
	Blocked some of the attack (delay time is noted in hh:mm)
	Had not released signature at time of publication

Note: Time listed 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.