KoreLogic SECURITY

KoreLogic Malware Testing Project
Executive Summary

Contents:

Check Point Software contracted with KoreLogic, an independent security consulting firm, to create and use a complete malware life cycle test environment. This executive summary was written by Check Point Software to summarize results from KoreLogic. Details of specific malware tested were deleted from this summary in order to avoid making it easier for criminals to hack into systems.

KoreLogic Malware Testing Project
Executive Summary

Background: Changing Threat Landscape Requires New Testing Methods

Competitive testing of consumer security software has not changed in the last decade, and is no longer an accurate measurement of product effectiveness. Consumer anti-malware testing is primarily based on file scanning to detect known malware signatures, with separate testing that identifies specific malware behaviors. Current testing is conducted in static lab environments to provide test results that are standardized and reproducible. In today's dynamic threat landscape, these monolithic, static testing methods do not simulate typical user experience and do not accurately and comprehensively measure anti-malware effectiveness in the real world. A new testing methodology is needed, one that is comprehensive and dynamic.

Methodology: Creating A Dynamic Life Cycle Test Environment

ZoneAlarm, a division of Check Point, contracted with KoreLogic, an independent security consulting firm, to create a complete malware life cycle test environment. The environment was deployed to assess the effectiveness of ZoneAlarm Internet Security Suite versus key competitors in detecting, mitigating and blocking the effects of malware. Competing products tested were Trend Micro Internet Security 2007, Norton Internet Security 2007, McAfee Total Protection 2007, and Microsoft Windows Live OneCare. The testing program ran from March through May, 2007.

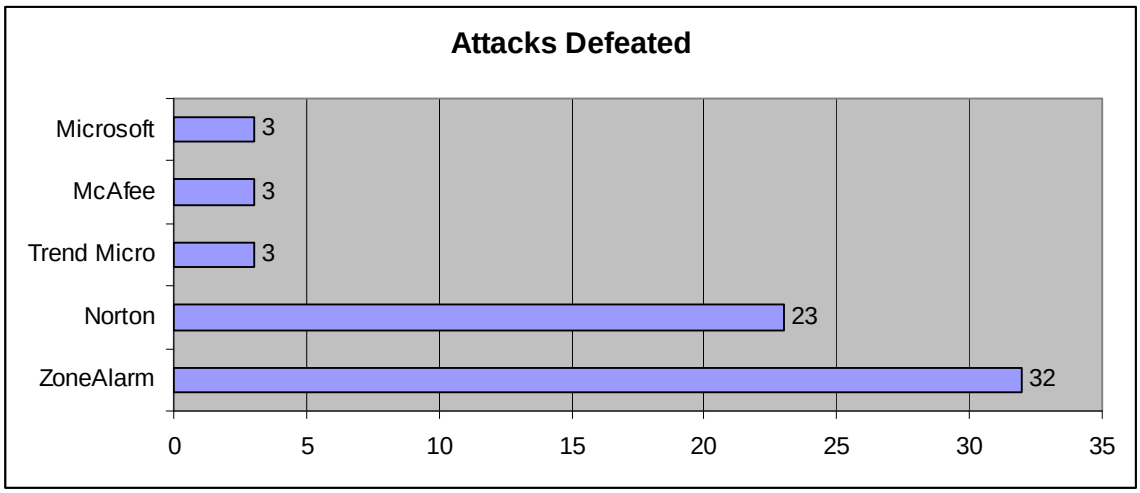
The automated test environment consisted of a malware server that distributed test payloads to a network of four PC nodes typical of Windows XP home environments. Dynamic activity was recorded by an in-band harvester that observed malware/system activity within each of the four PC nodes while the malware was active. A second, out-of-band harvester collected test data at the beginning and end of the test cycle. Results from both harvesters were combined to create a baseline malware profile prior to installation of the security products. The tests were run again after installation of the security suites, and results compared to the baseline to measure individual product mitigation effectiveness. Test results from each of the four PC nodes were compared. Any inconsistency between nodes was resolved through further testing until consistent results were achieved.

Seven test series were conducted (malware in self-extracting executable, malware extracted to C; drive, malware launched; tests conducted at boot time and after 1 and 5 minutes) to measure all phases of malware deployment and all major attack vectors. A proof of concept of the test environment was run using a cross section of 23 malware variants selected to represent all major malware categories: adware, bots, rootkits, spyware, trojans, viruses and worms. All testing was run on Windows XP SP2.

Results of Tests – Highlights

Boot Time Vulnerability: Test results uncovered vulnerabilities in defending against malware that deploys at boot time. This was a major vulnerability for most products except ZoneAlarm.

Summary of boot time test results:



Results of individual boot time tests:

Test Series 2.1: malware extracted to C: drive, detection at boot time

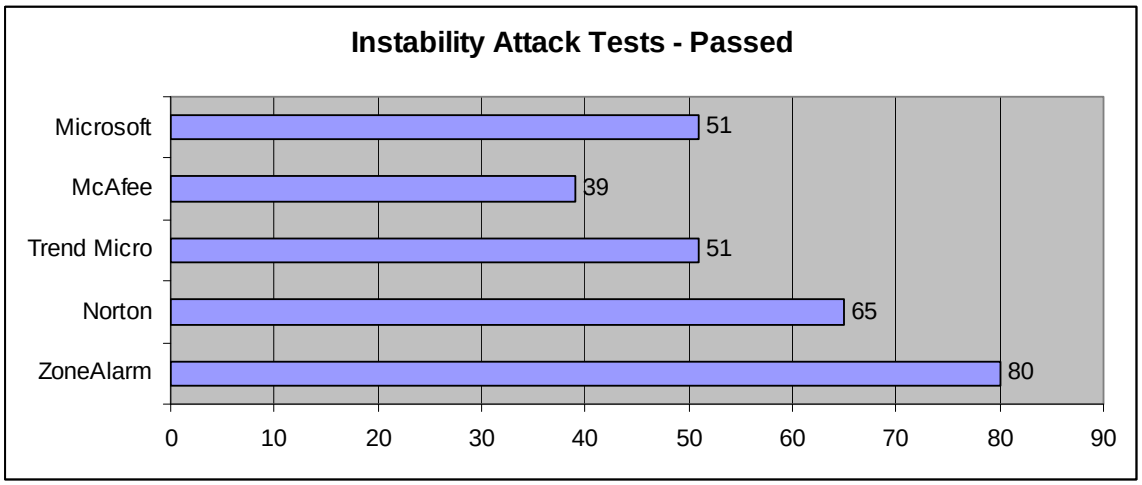
Product	Pass	Fail	Partial Fail
ZoneAlarm	16	7	0
Norton	10	9	4
Trend Micro	1	22	0
McAfee	1	22	0
Microsoft	1	22	0

Test Series 3.1: malware launch after extracted to C: drive, detection at boot time

Product	Pass	Fail	Partial Fail
ZoneAlarm	16	7	0
Norton	13	9	0
Trend Micro	2	21	0
McAfee	2	21	0
Microsoft	2	21	0

Stability Under Siege: The test methodology also measured product stability and robustness, the ability of a product to provide a consistent level of protection across multiple attack vectors and deployment conditions. ZoneAlarm results were identical across all test series. Norton demonstrated better stability than other products which showed much lower stability across tests.

Summary of instability attack test results:



Results of individual instability attack tests:

ZoneAlarm	Pass	Fail	Partial Fail
Series 2.1	16	7	0
Series 2.2	16	7	0
Series 3.1	16	7	0
Series 3.2	16	7	0
Series 3.3	16	7	0

Norton	Pass	Fail	Partial Fail
Series 2.1	10	9	4
Series 2.2	14	9	0
Series 3.1	13	9	0
Series 3.2	14	9	0
Series 3.3	14	9	0

Trend Micro	Pass	Fail	Partial Fail
Series 2.1	1	22	0
Series 2.2	14	5	4
Series 3.1	2	21	0
Series 3.2	17	5	1
Series 3.3	17	5	1

McAfee	Pass	Fail	Partial Fail
Series 2.1	1	22	0
Series 2.2	12	11	0
Series 3.1	2	21	0
Series 3.2	12	11	0
Series 3.3	12	11	0

Microsoft	Pass	Fail	Partial Fail
Series 2.1	1	22	0
Series 2.2	16	7	0
Series 3.1	2	21	0
Series 3.2	16	7	0
Series 3.3	16	7	0