Defeating malware has two components: 1. Detecting malware. 2. Removing the detected malware and its files. The common assumption is that antivirus and anti-malware products would do both equally well. This isn't true according to the latest results from AV-TEST, an independent testing laboratory.

Testing methodology

The goal of the evaluation was to simulate real-world infection scenarios and test the top antivirus and anti-malware products' ability to remove malware and repair the damage it had caused.

AV-TEST researchers employed two test scenarios for the antivirus products:

1. The antivirus or repair/recovery product was deployed on the test system that had already been infected with malware.
2. The antivirus or repair/recovery product was deactivated on the clean test system and then reactivated after the test system had been infected.

The products were tested over a ten-month period from September 2013 through June 2014 against 55 to 60 malware samples found in the wild at various times during that time. The testing window and protocol were to reflect the constantly changing threat landscape and evolution of malware threat families. In an effort to outwit antivirus makers, malicious code authors iterate and release variants of malware over the span of several months. These variants are intended circumvent the signature updates released by antivirus makers.

While most testing of antivirus products correctly places detection of malware as a primary metric, that was not the goal in this test. Because AV-TEST researchers were specifically evaluating for malware remediation (removal and clean up), they used only malware samples that had been previously identified as such by all the tested products. Even with this being the case, two products, Avira Free Antivirus and Microsoft Security Essentials (Windows 7 was the test operating system), failed at detecting some malware samples during testing.

The four criteria from the AV-TEST report:

1. Was the malware detected or not?
2. Were the active components completely removed?
3. Did any harmless file remnants remain, and were all the changes to the system reversed?
4. Did the security and clean-up software perfectly remove and restore everything?

Antivirus/Anti-Malware products tested:

- Avast! Free Antivirus 9.0
- AVG Antivirus Free 2014
- Avira Free Antivirus
- Bitdefender Internet Security 2014
- ESET Smart Security 7
- F-Secure Internet Security 2014
- Kaspersky Internet Security 2014
- Malwarebytes Anti-Malware Free
- Microsoft Security Essentials
- Norton Internet Security 2014

Specialized recovery and repair tools tested:

- Avira Cleaner
- Disinfect 2013
- F-Secure Removal Tool
- Hitman Pro
- Kaspersky Removal Tool
- Norton Power Eraser
- Panda Cloud Cleaner

Malwarebytes

Malware removal efficacy: 17 security products tested for malware removal and repair

AV-TEST antivirus/anti-malware products overall test results

Manufacturer/Product	Gradual testing of removal and system repair (number of malware samples)				Number of malware samples tested	Tested system repair
	Malware not detected	Active malware components not removed	Only harmless file remmants left behind	Complete removal, clean system		
Malwarebytes Anti-Malware Free	0	0	0	60	60	100.0%
Bitdefender Internet Security 2014	0	0	1	59	60	99.4%
F-Secure Internet Security 2014	0	0	4	56	60	97.8%
Kaspersky Internet Security 2014	0	0	4	56	60	97.8%
Norton Internet Security 2014	0	0	5	55	60	97.2%
ESET Smart Security 7	0	0	9	51	60	95.0%
AVG Antivirus Free 2014	0	2	3	55	60	96.1%
Avast! Free Antivirus 9.0	0	4	4	52	60	93.3%
Microsoft Security Essentials	1	7	4	48	60	88.8%
Avira Free Antivrus	2	1	7	50	60	91.7%

AV-TEST antivirus/anti-malware products detailed test results

Test Section 1: The antivirus solution was installed on an already infected system	Gradual testing of removal and system repair (number of malware samples)				Number of malware samples tested
	Malware not detected	Active malware components not removed	Only harmless file remmants left behind	Complete removal, clean system	
Avast! Free Antivirus 9.0	0	2	2	26	30
AVG Antivirus Free 2014	0	1	1	28	30
Avira Free Antivirus	1	0	5	24	30
Bitdefender Internet Security 2014	0	0	1	29	30
ESET Smart Security 2014	0	0	2	28	30
F-Secure Internet Security 2014	0	0	2	28	30
Kaspersky Internet Security 2014	0	0	1	29	30
Malwarebytes Anti-Malware Free	0	0	0	30	30
Microsoft Security Essentials	1	4	3	22	30
Norton Internet Security 2014	0	0	2	28	30
Test Section 2: The antivirus solution was deactivated and reactivated after the system was infected					
Avast! Free Antivirus 9.0	0	2	2	26	30
AVG Antivirus Free 2014	0	1	2	27	30
Avira Free Antivirus	1	0	2	26	30
Bitdefender Internet Security 2014	0	0	0	30	30
ESET Smart Security 2014	0	0	7	23	30
F-Secure Internet Security 2014	0	0	2	28	30
Kaspersky Internet Security 2014	0	0	3	27	30
Malwarebytes Anti-Malware Free	0	0	0	30	30
Microsoft Security Essentials	0	3	1	26	30
Norton Internet Security 2014	0	0	3	27	30

AV-TEST repair and recovery products overall test results

Manufacturer/Product	Gradual testing of removal and system repair (number of malware samples)				Number of malware samples tested	Tested system repair
	Malware not detected	Active malware components not removed	Only harmless file remmants left behind	Complete removal, clean system		
Kaspersky Removal Tool	0	0	1	54	55	99.4%
Norton Power Eraser	0	0	12	43	55	92.7%
Disinfect 2013	0	0	48	7	55	70.9%
Hitman Pro	0	1	10	44	55	92.7%
Panda Cloud Cleaner	0	2	0	53	55	97.6%
Avira Cleaner	0	8	46	1	55	62.4%
F-Secure Removal Tool	0	11	8	36	55	81.8%

TEST repair and recovery products detailed test results

Test Section 1: The antivirus solution was installed on an already infected system	Gradual testing of removal and system repair (number of malware samples)				Number of malware samples tested
	Malware not detected	Active malware components not removed	Only harmless file remmants left behind	Complete removal, clean system	
Avira Cleaner	0	5	21	1	27
Disinfect 2013	0	0	22	5	27
F-Secure Removal Tool	0	7	6	14	27
Hitman Pro	0	1	0	26	27
Kaspersky Removal Tool	0	0	1	26	27
Panda Cloud Cleaner	0	1	0	26	27
Norton Power Eraser	0	0	11	16	27
Test Section 2: The antivirus solution was deactivated and reactivated after the system was infected					
Avira Cleaner	0	3	25	0	28
Disinfect 2013	0	0	26	2	28
F-Secure Removal Tool	0	4	2	22	28
Hitman Pro	0	0	10	18	28
Kaspersky Removal Tool	0	0	0	28	28
Panda Cloud Cleaner	0	1	0	27	28
Norton Power Eraser	0	0	1	27	28

Conclusions

While the threat posed by an incomplete removal that leaves active malware components behind is apparent, "harmless" malware file remnants can still prove to be problematic. File remnants take up memory resources and can create false positive readings during subsequent malware scans. If an antivirus or clean up tool can't completely restore the system, the user is faced with reinstalling the operating system and updating—a process that often takes several hours. Any system restoration result short of complete malware removal burdens the user.

As the AV-TEST testing reveals, complete system restoration ("total system repair")—returning a system to its pre-infection state without any malware files remaining—is out of reach for most of the tested products. In fact, just a slim majority of the tested products were capable of removing malware and restoring the system without any active malware components remaining in place.

Only one, Malwarebytes Anti-Malware Free, successfully removed all malware files, active and harmless, and restored the system to its clean pre-infection state.

For more information on the AV-TEST repair performance test: http://www.av-test.org/en/news/news-single-view/17-software-packages-in-a-repair-performance-test-after-malware-attacks/.