Remediation-Testbericht

Der Test wurde im Auftrag der Enigma Software Group von AV-TEST GmbH durchgeführt
Bericht vom: 15. Februar 2017, aktualisiert am 15. Februar 2017

Zusammenfassung

Im Januar 2017 hat AV-TEST die Leistungsfähigkeit der Remediation-Funktionen von SpyHunter geprüft, ein Produkt der Enigma Software Group. Durchgeführt wurde der Test auf einem sauberen Windows 7-System (SP1, 64 Bit) und das gleiche Disk Image wurde auf mehreren baugleichen Rechnern verwendet.

Der Malware-Korpus für den Remediation-Test umfasste 20 Schädlinge und der Testablauf wurde in zwei Phasen unterteilt. In der ersten Testphase wurde zunächst das Image mit einem Malware-Sample infiziert und im nächsten Schritt der Versuch unternommen, das Sicherheitsprodukt zu installieren, den Rechner zu scannen und die erkannte Bedrohung zu entfernen. In der zweiten Testphase wurde die Antiviren-Lösung deaktiviert, damit das System infiziert werden konnte. Daraufhin wurde die AV-Lösung wieder aktiviert und das System neu gestartet um sicherzustellen, dass sämtliche Komponenten der Sicherheitslösung einwandfrei funktionieren. Im letzten Schritt wurde versucht, das System zu säubern und einen zusätzlichen Systemscan durchzuführen.

SpyHunter hat jeweils in Testphase 1 und Testphase 2 erfolgreich die Gesamtzahl von 20 vorhandenen Schädlinge entfernt und damit in beiden Fällen eine Bestleistung gezeigt.

Es gelang der Software, alle aktiven Komponenten der Malware zu neutralisieren und darüber hinaus sämtliche davon im System verbliebenen Dateireste zu löschen.

Übersicht

Angesichts der stetig steigenden Anzahl an Bedrohungen, die mittlerweile entwickelt und über das Internet verbreitet werden, steigt auch das Risiko, dass Systeme infiziert werden. Während noch vor wenigen Jahren neue Bedrohungen alle paar Tage veröffentlicht wurden, muss im heutigen Bedrohungsszenario mit mehreren tausend neuen Schadprogrammen pro Stunde gerechnet werden.

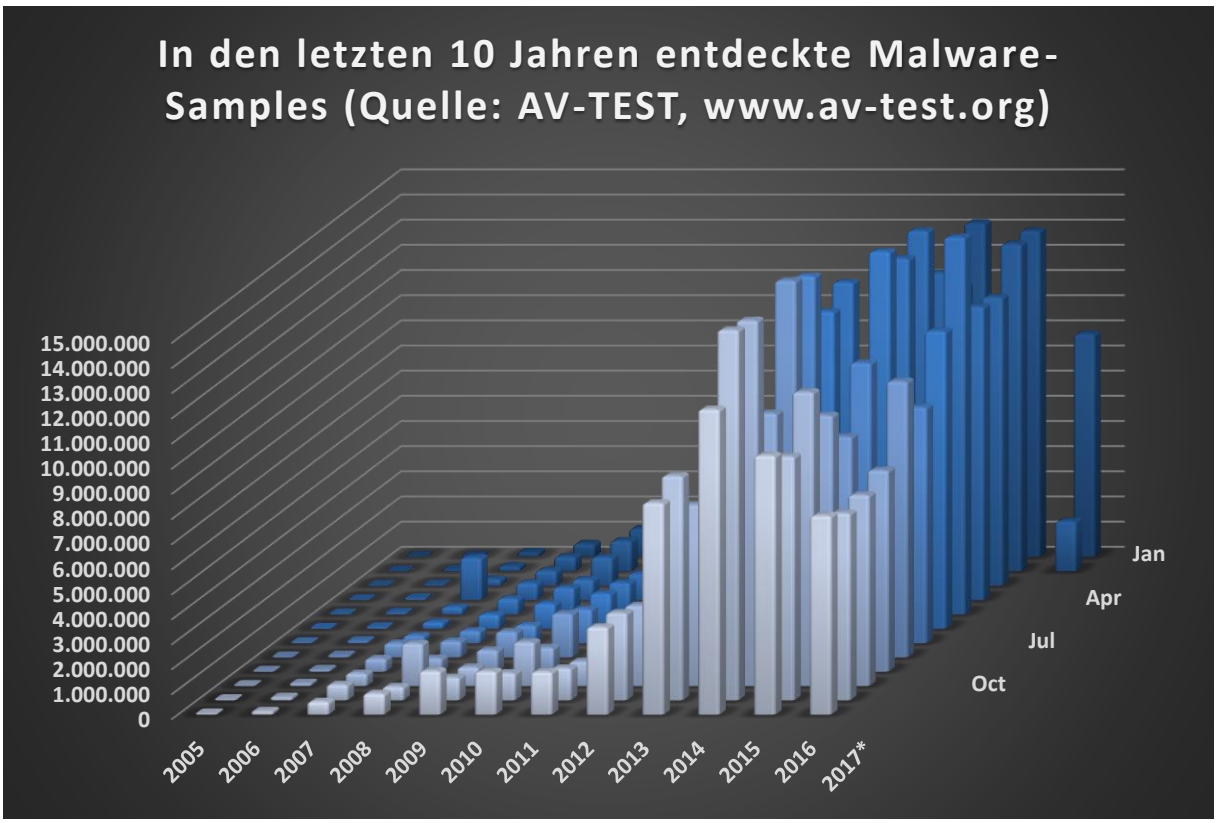


Abbildung 1: Neue Malware-Samples pro Jahr

Während AV-TEST in 2000 noch über 170.000 neue Malware-Samples sammelte, war die Anzahl an Schädlingen bis 2013 bereits auf über 80 Millionen gestiegen. Der Blick auf die Angaben in Abb. 1 zeigt, dass sich der Anstieg auch in 2016 fortgesetzt hat. Derzeit befinden sich mehr als 600 Millionen Malware-Samples in der AV-TEST-Datenbank.

Hersteller von Sicherheitssoftware müssen beim Schutz ihrer Kunden eine ungeheure Menge an neuen Schädlingen bewältigen. Diese Menge kann zu Problemen führen, denn es ist nicht in jedem Fall möglich, einen Rechner rechtzeitig vor Bedrohungen zu schützen. Selbst wenn eine aktualisierte Antiviren-Software auf dem Rechner installiert ist, kann dieser trotzdem infiziert werden, wenn mehrere Stunden von der Entdeckung eines neuen Schädlings bis zur Bereitstellung passender Signaturen vergehen. In einigen Fällen kann es dann schon zu spät sein. Infektionen können wirtschaftlichen Schaden verursachen, beispielsweise wenn vertrauliche Daten gestohlen werden oder der Rechner nicht mehr effektiv genutzt werden kann, bis der Schädling vollständig aus dem System entfernt worden ist.

Vor diesem Hintergrund gewinnen Remediation-Techniken zunehmend an Bedeutung, wenn ein infizierter Rechner schnell wieder einsatzbereit sein muss. Es ist jedoch zwingend erforderlich, dass der Reinigungsprozess beim Einsatz dieser Technik in zwei Punkten zuverlässig abläuft:

1. Der Schädling und sämtliche Schädlingskomponenten müssen entfernt und verseuchte Systeme wiederhergestellt werden.
2. Saubere Programme sowie das System selbst dürfen im Laufe des Reinigungsprozesses nicht in Mitleidenschaft gezogen werden.

Getestetes Produkt

Der Test wurde im Januar 2017 durchgeführt und AV-TEST hat die zum Testzeitpunkt verfügbare aktuellste Software-Version verwendet:

- SpyHunter von Enigma Software Group

Testmethodik und Bewertung

Plattform

Alle Tests wurden auf baugleichen Rechnern mit folgender Hardware durchgeführt:

- Intel Xeon Quad-Core X3360 CPU
- 4 GB RAM
- 500 GB HDD (Western Digital)
- Intel Pro/1000 PL (Gigabit Ethernet) NIC

Als Betriebssystem wurde Windows 7 (SP1, 64 Bit) inklusive der in der Version installierten Hotfixes und am 3. Januar 2017 verfügbaren Patches eingesetzt.

Testmethodik

Der Remediation-Test wurde in zehn Schritten unter Beachtung der folgenden Methodik durchgeführt:

1. **Sauberes System für jede Malware**. Die Testsysteme wurden jeweils gereinigt und wiederhergestellt, bevor sie mit einem einzelnen Malware-Sample infiziert wurden.
2. **Physische Rechner**. Für den Testablauf wurden ausschließlich physische Rechner genutzt, während virtuelle Umgebungen nicht zum Einsatz kamen.
3. **Internetzugang**. Es bestand zu jeder Zeit vollständiger Internetzugriff für die Rechner, um bei Bedarf während des Tests in der Cloud nachzufragen.
4. **Produktkonfiguration**. Bei sämtlichen Produkten und den dazugehörigen Remediation-Tools oder bootfähigen Rettungs-Tools wurden die Standardeinstellungen verwendet, entsprechend der Konfiguration bei Auslieferung.
5. **Infektion der Test-Rechner**. Ein natives System wurde mit einem Schädling infiziert und dann neu gestartet. Es musste sichergestellt werden, dass der Schädling vollständig lauffähig war.
6. **Schädlingsfamilien und Schadsoftware (Payloads)**. Bei den Testsamples wurde darauf geachtet, dass sie nicht aus der gleichen Schädlingsfamilie stammten oder die gleiche Schadsoftware nutzten.
7. **Remediation unter Einsatz sämtlicher verfügbarer Produktfunktionen**.
    a. Es soll versucht werden, das Sicherheitsprodukt mit den Standardeinstellungen zu installieren. Die Produktangaben für die Entfernung von Malware müssen vollständig befolgt werden.

b. Sollte a. nicht durchführbar sein, sollte man es mit einem ***stand-alone Fix-Tool bzw. einem Rettung-Tool*** versuchen (sofern verfügbar).
c. Sollte b. nicht möglich sein, sollte zur Eliminierung der Bedrohung eine stand-alone ***Boot-Lösung*** eingesetzt werden (sofern verfügbar).

8. **Prüfung der Malware-Entfernung.** Die Überprüfung des Rechners erfolgte manuell, kontrolliert wurde die vollständige Entfernung und der Verbleib von Dateiresten.
9. **Bewertung der Performance bei der Malware-Entfernung.** Die Performanceleistung des Tools und der gesamten Sicherheitslösung wurde unter Verwendung eines vereinbarten Punktesystems bewertet.
10. **Übermäßige Remediation-Auswirkungen.** In dem Test wurde ebenfalls geprüft, inwieweit eine Sicherheitslösung aggressive Methoden bei der Säuberung des Systems einsetzt. So gibt es beispielsweise Produkte, die Hosts-Dateien oder sogar ganze Verzeichnisse komplett entfernen, obwohl dies nicht für einen erfolgreichen Remediationsablauf erforderlich ist. Sollten solche Methoden eingesetzt werden, führt dies zu Punktabzügen bei der Bewertung.

Bewertung der Wirksamkeit

Nach dem folgenden System wurden für jedes getestete Malware-Sample Punkte vergeben:

a. Malware wurde vollständig entfernt (3 Punkte)
b. Malware wurde erkannt und entfernt, es blieben nur inaktive Dateireste zurück (2 Punkte)
c. Es wurde etwas entdeckt und teilweise entfernt, Reste der Schadsoftware waren jedoch noch aktiv (1 Punkt)
d. Die Malware wurde nicht entdeckt und somit nicht entfernt (0 Punkte)

Bei der Punktevergabe wurde nicht berücksichtigt, welche der verfügbaren Techniken zur Entfernung der Malware benötigt wurden. Es sollte jedoch jede Technik zum Einsatz kommen. Wenn ein Produkt die Einträge in der Hosts-Datei entfernt, die zu dem entsprechenden Produkt gehören, dabei einen sauberen Rechner zurücklässt, und die Funktionalität sowie die Aktualisierbarkeit des Produkts gewährleistet bleibt, sollte das Produkt für seine Remediationsleistung die volle Punktzahl erhalten, selbst wenn Einträge anderer Sicherheitssoftware-Anbieter in der Hosts-Datei zurückbleiben.

Samples

Das Testset umfasste 20 Schadprogramme, mit denen Windows 7 (SP1, 64 Bit) infiziert werden konnte.

Testergebnisse

Sowohl in der ersten als auch in der zweiten Testphase erzielte das Produkt der Enigma Software Group mit hundert Prozent die bestmögliche Wertung. Die Ergebnisse beider Testphasen werden in Abb. 2 dargestellt.

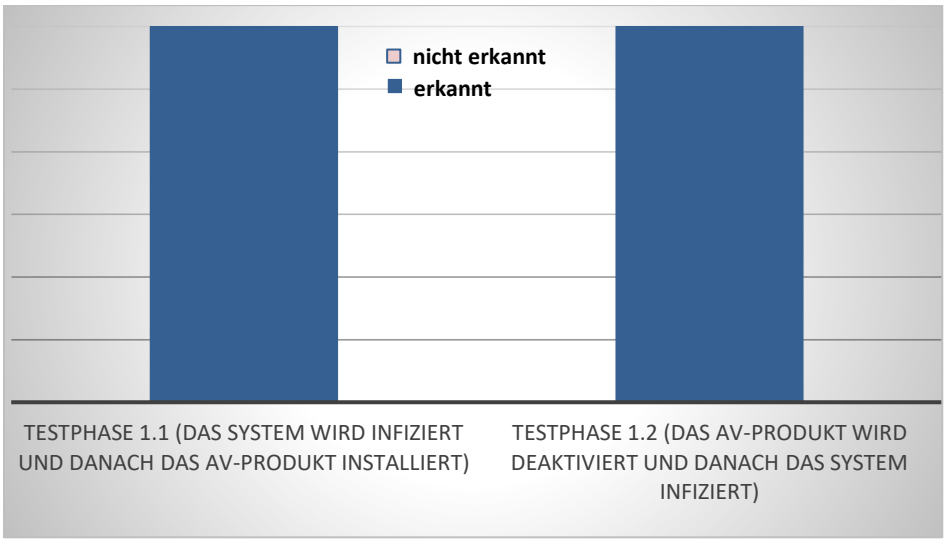
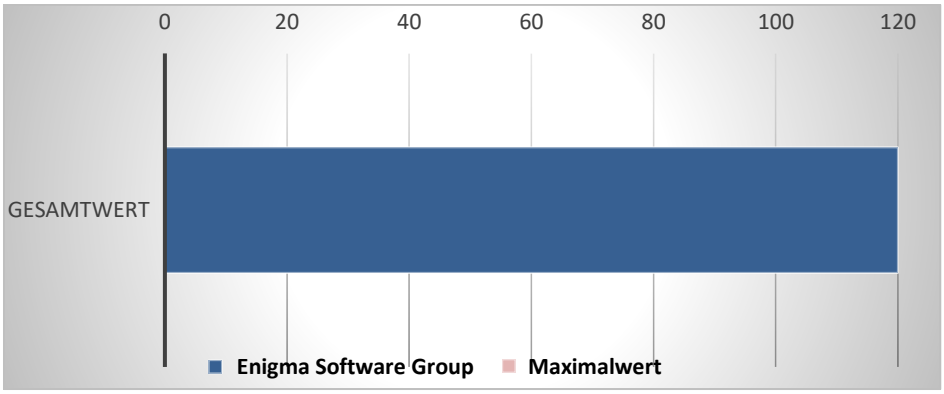


Abbildung 2: Remediation-Ergebnis - Testphasen 1.1 und 1.2

Der Maximalwert, der in diesem Test zu erreichen war, lag bei 120 Punkten. Wie in Abb. 3 deutlich wird, erreichte Enigma Software Group den Gesamtwert von 120 Punkten. Bei der Prüfung der Performance in Hinblick auf die Reinigungsleistung in Testphase 1.2 konnte SpyHunter das System vollständig reinigen.

Die Software erzielte in der Testphase 1.1 ein ebenso perfektes Ergebnis, indem ihr eine 100-prozentige Säuberung des infizierten Systems gelang.



Anhang

Information zur getesteten Softwareversion

Entwickler, Hersteller	Produktbezeichnung	Programmversion	Engine/Signaturversion
Enigma Software Group	SpyHunter 4	4.24.3.4750	2017.01.17v01

Liste der im Remediation-Test verwendeten Malware-Samples

(SHA256)
0x0248aef55dd424770217a568e6d6e621b08f010faecc3bdc889e815bdba562b7
0x2e9b4aa0d8f1fe0c8f75faaad8fea213cc982678925e883199d4e73316830e27
0x379d26795c02cd028f5fc33210b598228a8f23f9926bac365668e1044c30f496
0x3963f5795ab1c34ffe7ae23424b82631d24908c3c25bb5b703fba8403f63e7a8
0x496badd81af03f9a74f3fc321225d8376dc6aff613e2d2e4328fabf33fbe3853
0x4e5212dc24b5d6b3b6281db2ed33bc8b271151c11a1a7b6fc16d5a843aef7bc4
0x4f5bff64160044d9a769ab277ff85ba954e2a2e182c6da4d0672790cf1d48309
0x534ceed806ec84ae75fdd2e3f1c837cb1e263f52e03a73366a199f45456acfc2
0x5847e0b50f7279000e7335af0b0925b413718810cf5591d8ea253ae55893a197
0x6bf17b1dc8eb3b0ae6412bd2d71fe73832e9b4c7ba259d9d13e46427401c4145
0x73e7b43fed5fe22d58ba0c36080eb70f00640ea9e615d8e5ce1785d76d1f2a76
0x814d8c756520ebc86fcf8f544a352d17bb7636333a206c27bc0710320fabd279
0x90c1e0eb0eb37300e2177b465b9289daa910f2df2a6b5e63f3504958f7a71bc8
0x931339d73c08813699f40ff613083fc393e17fe99c1bdbdb2ea8038816b1c289
0xb3cf3567fab18b8a39277b33d0a89b2f0f79a7f2a3583ad663fd5d80f6c49546
0xd32ee2cf13429517274cda35c341861ab9d947533163da3154b74ca40b8161f6
0xd861451d5ee19419ac829bdba0622ce9e1edcc6ef9f1a6f5257ee0744771ae76
0xece08e1c4d119df6217853b7ef22bff31e0c58f9d204878b2e28e6ff9e1ba782
0xefbd13ee753e4b879616a020bdb77212abdf637e6c288ab48672276bb69d24d2
0xf93c7b95df816eed946a5028f44f3e9185baf63ccbcf66047331cfb3b5a2654a

Copyright © 2017 AV-Test GmbH, Klewitzstraße 7, 39112 Magdeburg
Tel. +49 391 6075460, Fax: +49 391 6075469, Internet: http://www.av-test.org