Remediation-Testbericht

Der Vergleichstest wurde im Auftrag der Enigma Software Group von AV-TEST GmbH durchgeführt
Bericht vom: 20. August 2018, aktualisiert am 20. August 2018

Zusammenfassung

Im Juli 2018 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 10-System (RS3, 64 Bit) und das gleiche Disk Image wurde auf mehreren baugleichen Rechnern verwendet.

Der Malware-Korpus für den Remediation-Test umfasste 12 Schädlinge und der Testablauf wurde in zwei Phasen unterteilt. Testphase 1: In einem ersten Schritt wurde das Image mit einem Malware-Sample infiziert und in einem weiteren Schritt der Versuch unternommen, das Sicherheitsprodukt zu installieren, den Rechner zu scannen und die erkannte Bedrohung zu entfernen. Testphase 2: Zunächst 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 in beiden Testphasen eine sehr gute Leistung gezeigt und konnte im ersten und zweiten Testteil 10 der 12 Malware-Samples vollständig entfernen. Es gelang der Enigma-Software auch, 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.

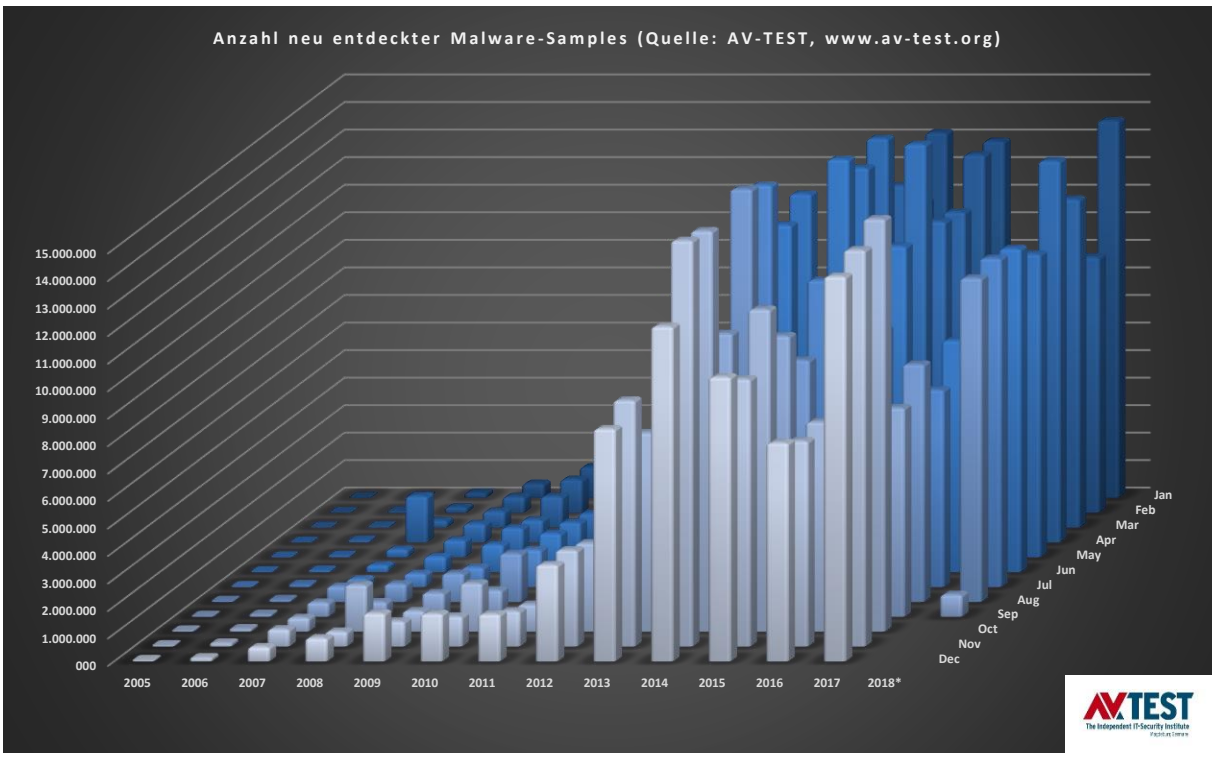


Abbildung 1: Neue Malware-Samples pro Jahr

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 Entwicklung der Zahlen in Abb. 1 zeigt, dass sich der Anstieg auch in den Folgejahren fortgesetzt hat. Derzeit befinden sich mehr als 800 Millionen Malware-Samples in der AV-TEST-Datenbank, und allein in der ersten Hälfte dieses Jahres haben die Erkennungssysteme von AV-TEST ca. 10 Millionen neue Samples pro Monat erfasst.

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 2018 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 10 (RS3, 64 Bit) inklusive der in der Version installierten Hotfixes und am 4. Juni 2018 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 12 Schadprogramme, mit denen Windows 10 (RS3, 64 Bit) infiziert werden konnte.

Testergebnisse

Sowohl in der ersten als auch in der zweiten Testphase erzielte das Produkt der Enigma Software Group mit 97,2 Prozent ein sehr gutes Ergebnis. Die Ergebnisse beider Testphasen werden in Abb. 2 dargestellt.

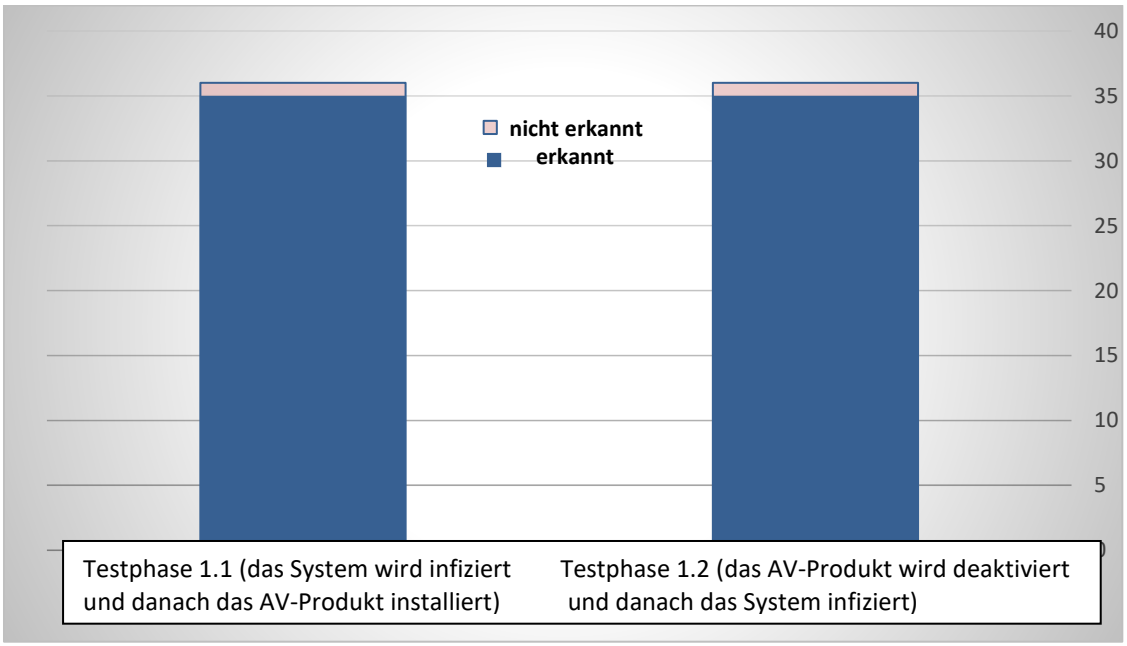
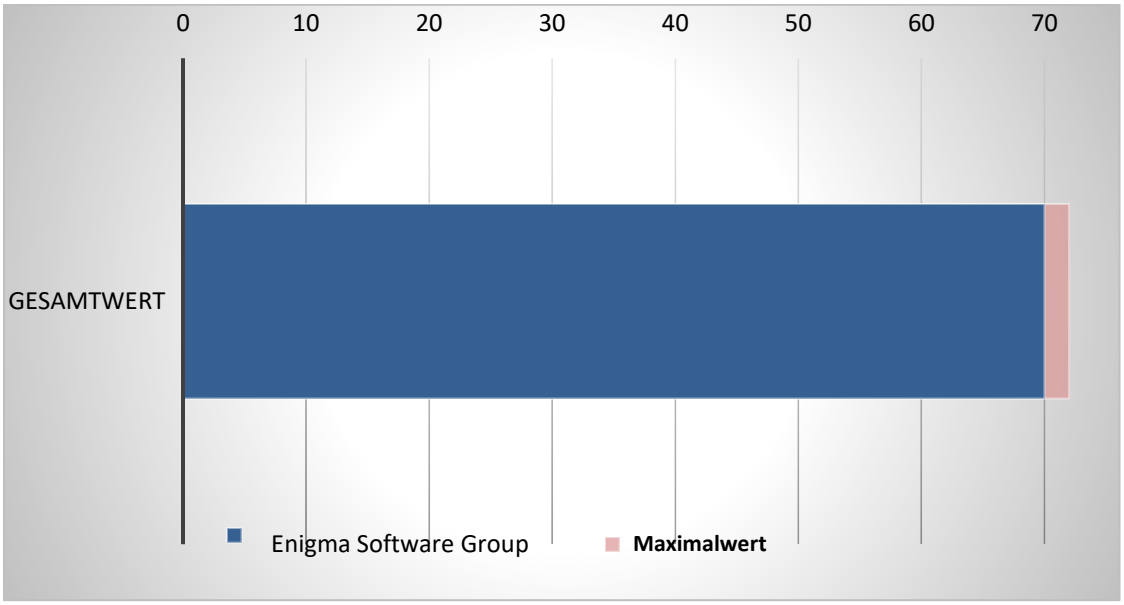


Abbildung 2: Remediation-Ergebnis - Testphasen 1.1 und +1.2

Bei der Prüfung der Performance in Hinblick auf die Reinigungsleistung konnte SpyHunter in 10 von 12 Sample-Fällen das System vollständig reinigen. In jeweils nur einem Fall pro Testphase war es dem Programm nicht gelungen, die Registry-Einträge der Malware zu löschen, was wiederum zu leichten Punktabzügen führte.

Der Maximalwert, der in diesem Test zu erreichen war, lag bei 72 Punkten. Wie in Abb. 3 deutlich wird, erreichte Enigma Software Group den Gesamtwert von 70 Punkten.



Anhang

Information zur getesteten Softwareversion

Entwickler, Hersteller	Produktbezeichnung	Programmversion
Enigma Software Group	SpyHunter 5	5.0.30.51

Liste der im Remediation-Test verwendeten Malware-Samples

(SHA256)
0x10864dff8bcea96f842f6642bca59199b677e28e6e174c3e4d7b65391b0698b0
0x2942841f850c59c1f7bedd1922aca54c886bad1eb51b90b32af7d6b6b6e5cab4
0x5ba58146b785d5e72993430d95960486cbf9bf9429e5e3bf4fa2fe2e88f4e250
0x69bb101c4c53fe2a87ed2200dd46b7d82d92c86943e47a31ce7922455b92d345
0x70179938e6c056df16b1403615cc553a10a90297601446f95d6ad004ca1e29eb
0x86958f2f177eed14d6164d48a18cb15c12516bdb59f1125471d966f3e212b989
0x980f254b3954b3d7ded9772cad328d6872491fbd645ac3dae3d277620cfb88b7
0xac186a20bbec078f08788cc8a4a746de0139a061a6d2588787d217f019c2eb90
0xb3548b485e919e043b935b071ad54f37e1c996046fcfbefae51d76a437ee6a93
0xd8a3f066a3b961b4c8623e0d30e3e867fd7a1c9187aa396de8457df70b602efe
0xe275e10bea80834252aea1b5dba9a817b278b5c4a6d0594b01b1605de0b66f79
0xf92dd910c0c00e5924a27bbffcdb303e5f724b3caf540e844c3f82a291cc7a30