Reparatur-Testbericht

Der Test wurde im Auftrag der EnigmaSoft Limited von AV-TEST GmbH durchgeführt
Berichtsdatum: 03. September 2018, letzte Aktualisierung am 04. September 2018

Kurzfassung

Im August 2018 führte AV-TEST einen Test der Reparaturleistung von SpyHunter der EnigmaSoft Limited durch. Der Test wurde auf einem System mit sauberem Windows 10 (RS3, 64 Bit) durchgeführt und dasselbe Disk-Image auf mehreren identischen PCs verwendet.

Der Malware-Testkorpus für den Reparaturtest bestand aus 12 Mustern und gliederte sich in zwei Abschnitte. Test-Abschnitt 1: Zunächst wurde das Image mit einem der Malware-Muster infiziert. Im nächsten Schritt wurde versucht, das Schutzprogramm zu installieren, den PC zu scannen und alle gefundenen Bedrohungen zu entfernen. Test-Abschnitt 2: Hier wurde zuerst die AV-Software deaktiviert, um das System infizieren zu können. Die AV-Software wurde anschließend wieder aktiviert und ein Reboot ausgeführt, um zu gewährleisten, dass alle Komponenten der AV-Software korrekt arbeiten. Danach wurde versucht, das System zu reparieren und einen zusätzlichen System-Scan durchzuführen.

SpyHunter erzielte in beiden Testabschnitten ein perfektes Ergebnis von 100 %. Die Enigma Software bereinigte alle aktiven Komponenten und entfernte sämtliche Malware-Artefakte vom System.

Übersicht

Durch die wachsende Anzahl der heute über das Internet veröffentlichten und verbreiteten Bedrohungen steigt auch die Infektionsgefahr bei Systemen. Vor wenigen Jahren noch erschienen nur alle paar Tage neue Viren. Heute sind es jede Stunde mehrere tausend neue Bedrohungen.

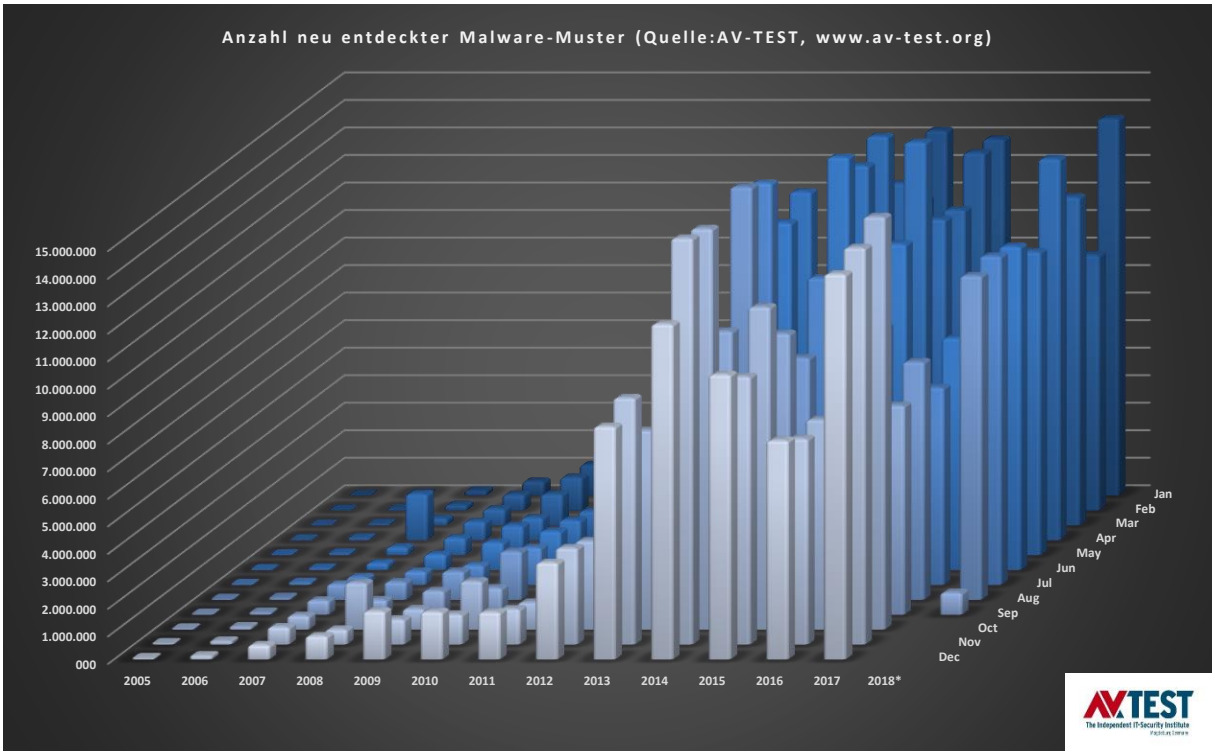


Abbildung 1: Neue Muster pro Jahr

Im Jahr 2000 bekam AV-TEST über 170.000 neue Muster, 2013 war die Anzahl neuer Muster auf über 80.000.000 angewachsen. In den Folgejahre stieg die Anzahl weiter an, wie die Grafik in Abbildung 1 zeigt. Die Datenbank von AV-TEST enthält derzeit mehr als 800 Millionen Malware-Muster. In der ersten Hälfte des Jahres 2018 registrierten die Erfassungssysteme von AV-TEST jeden Monat rund 10 Millionen neue Muster.

Die Menge an neuen Mustern muss von Anbietern von Anti-Malware-Software verarbeitet werden, um ihre Kunden vor Problemen zu schützen. Es ist aber nicht immer möglich, einen PC rechtzeitig zu schützen. Ein PC kann auch infiziert werden, wenn aktuelle Anti-Malware-Software installiert ist, da Signaturen nur alle paar Stunden bereitgestellt werden, was manchmal zu spät sein kann. Infektionen verursachen wirtschaftliche Verluste, weil vertrauliche Daten gestohlen werden oder der PC nicht mehr produktiv nutzbar ist, bis die Malware komplett von dem System entfernt wird.

Reparaturtechniken sind daher immer wichtiger geworden, um einen infizierten PC wieder nutzbar zu machen. Der Einsatz solcher Techniken setzt voraus, dass der Reinigungsprozess in zweierlei Hinsicht zuverlässig ist:

1. Die Malware und alle ihre Komponenten müssen entfernt und alle schädlichen Systemänderungen rückgängig gemacht werden
2. Saubere Anwendungen oder das System selbst dürfen durch den Reinigungsprozess nicht beschädigt werden

Getestetes Produkt

Der Test wurde im August 2018 durchgeführt. AV-TEST setzte dabei das zum Testzeitpunkt neueste verfügbare Release der folgenden Software ein:

- SpyHunter von EnigmaSoft Limited

Methodik und Scoring

Plattform

Alle Tests erfolgten auf identischen PCs mit folgender Hardware-Ausstattung:

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

Der Test wurde im August 2018 durchgeführt. AV-TEST verwendete die neueste Version der folgenden Software, die zum Testzeitpunkt verfügbar war.

Testmethode

Der Reparaturtest war nach der nachfolgend beschriebenen Methode in zehn Schritte unterteilt:

1. **Sauberes System für jedes Muster**. Die Testsysteme wurden in einen sauberen Zustand versetzt, bevor sie jeweils einem Malware-Muster ausgesetzt wurden.
2. **Physische Rechner**. Die verwendeten Testsysteme waren echte physische Rechner. Es wurden keine virtuellen Rechner eingesetzt.
3. **Internetzugang**. Die Rechner hatten jederzeit Zugang zum Internet, um gegebenenfalls In-the-Cloud-Abfragen zu nutzen.
4. **Produktkonfiguration**. Alle Produkte und ihre zugehörigen Reparatur-Tools oder bootfähigen Wiederherstellungs-Tools liefen mit den vorkonfigurierten Standard-Einstellungen.
5. **Infektion der Testrechner**. Ein nativer Rechner wurde mit einer Bedrohung infiziert und dann neu gestartet. Es musste sichergestellt werden, dass die Bedrohung im vollen Umfang lief.
6. **Musterfamilien und Payloads**. Die getesteten Muster kamen nicht aus derselben Familie und hatten auch nicht die gleichen Payloads.
7. **Reparatur unter Einsatz aller verfügbaren Produktkapazitäten**.

a. Versuchen, das Sicherheitsprodukt mit den Standardeinstellungen zu installieren. Darauf achten, dass die kompletten Produktanweisungen für das Entfernen eingehalten werden.
b. Wenn a. nicht funktioniert, eine Lösung mit ***Stand-Alone Fix-Tool/Rettungs-Tool*** (sofern verfügbar) versuchen.
c. Wenn b. nicht funktioniert, die Stand-Alone ***Boot-Lösung*** (sofern verfügbar) versuchen und für die Reparatur verwenden.

8. **Validieren der Entfernung**. Der PC wurde manuell inspiziert, um eine einwandfreie Entfernung und das Vorhandensein von Artefakten zu validieren.
9. **Scoring der Entfernleistung**. Die Effizienz des Tools und der Sicherheitslösung als Ganzes wurden mit Hilfe des vorgesehenen Scoring-Systems bewertet.
10. **Zu aggressive Reparatur**. Der Test ermittelte auch die Aggressivität eines Produkts bei der Reparatur. Manche Produkte entfernen beispielsweise die Hosts-Datei oder ein ganzes Verzeichnis komplett, auch wenn dies für eine erfolgreiche Reparatur nicht notwendig wäre. Dieses Verhalten spricht gegen das Produkt.

Effizienz-Rating

Für jedes getestete Muster werden Punkte nach folgendem System vergeben:

a. Malware komplett entfernt (3)
b. Malware gefunden und entfernt, nur inaktive Spuren übrig (2)
c. Es wurde etwas gefunden und teilweise entfernt, aber Malware-Spuren sind immer noch aktiv (1)
d. Malware wurde nicht gefunden, nichts entfernt (0)

Beim Scoring sollte unberücksichtigt bleiben, welche der verfügbaren Techniken erforderlich war, um die Malware zu entfernen. Allerdings sollten alle Techniken angewendet werden. Wenn ein Produkt die zu diesem Produkt gehörigen Einträge aus der Hosts-Datei löscht, den Rechner von Infektionen befreit und das Produkt funktionsfähig und aktualisierbar hinterlässt, ist ihm für die Reparatur die volle Punktzahl zu geben, auch wenn Einträge für andere Sicherheitsanbieter in der Hosts-Datei verbleiben.

Muster

Das Set enthielt 12 schädliche Dateien, die in der Lage waren, Windows 10 (RS3, 64 Bit) zu infizieren.

Testergebnisse

EnigmaSoft Limited schnitt in beiden Testabschnitten perfekt mit 100 % ab.
Die Ergebnisse beider Testabschnitte sind in Abbildung 2 dargestellt.

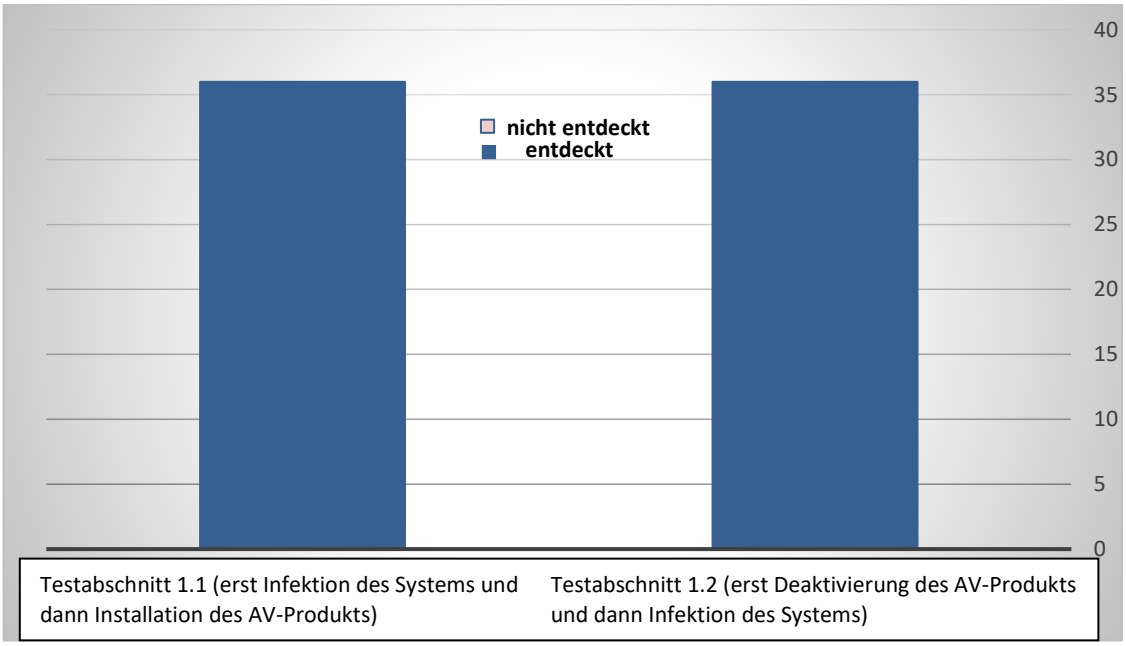
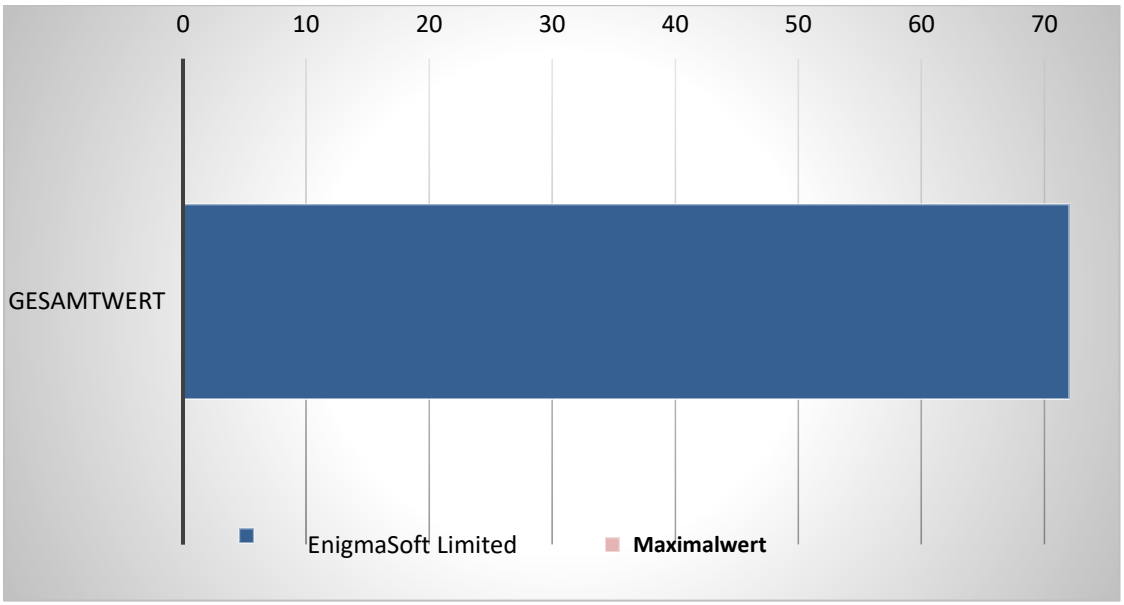


Abbildung 2: Reparaturergebnis – Testabschnitte 1.1 +1.2

Hinsichtlich der Reinigungsleistung konnte SpyHunter das System von allen 12 getesteten Mustern bereinigen. Außerdem wurden alle Artefakte und Registry-Einträge perfekt bereinigt.

Die erreichbare Höchstpunktzahl war 72. Wie in Abbildung 3 ersichtlich, erzielte EnigmaSoft Limited das überragende Ergebnis von 72 Punkten.



Anhang

Version der getesteten Software

Entwickler, Distributor	Produktname	Programmversion
EnigmaSoft Limited	SpyHunter 5	5.0.30.51

Liste der im Reparaturtest verwendeten Samples

(SHA256)
0x0bf737607d46bfa4434a8d62b2376b9fdd4b013bb1614bd5f089fa332feef0b2
0x179cb0ba8030ee09e2e7d5be3a9d0f1b20663a5e1f49e8d1d876b3f76e088476
0x3c5fc8acd9a0ef88795d2592fee6a20be800a3874a40f672700bf23707ca9f82
0x4ff747afb05bc711742f3617d92735a8435eb16c8954dbfe1e558cb7b5de7c3d
0x5400e496f79ad8d09b6be069ca680af2e359f81625993e15fa52a09b1444f78b
0x6287b31e3681973ecfc969ce082cc195badd8f571ce057695a021c9227ee63d4
0x6abef4b7e1d91fc80c7f83cfebffa1ac129333c4acb8e7779bd646a1e66129c3
0x7e8a7fd6bb805f8bd42d30c17490b9bd0a9602485efcb708abfca3e1d5b16c01
0xa058357700d6bbec06232492c40a88487f57e343f7a7c6180582b4d83714f1bd
0xc3519c9fc77812b3ad088174729fc3f712de69505659f73e4d277af6b4ba31ab
0xe67ddfdfdca394eb8a4ebf7fe64c7dc7459df1b3b050e680ce94ab51a2e54c0c
0xf4e496f3a1d094eddf13a93e92e22dbc6a224aa8e8e8664fdf7fdbb4b456485c