Remediation-Testbericht

Der Test wurde im Auftrag der Enigma Software Group von AV-TEST GmbH durchgeführt
Bericht vom: 19. Mai 2016, aktualisiert am 24. Mai 2016

Zusammenfassung

Im April und Mai 2016 hat AV-TEST die Leistungsfähigkeit der Remediation-Funktionen von SpyHunter geprüft, ein Produkt des Herstellers Enigma Software Group. Der Test wurde auf einem sauberen Windows 7-System (SP1, 64 Bit) durchgeführt und das gleiche Disk Image wurde auf mehreren baugleichen Rechnern verwendet.

Der Malware-Korpus für den Remediation-Test umfasste 20 Schädlinge und der Testablauf erstreckte sich über zwei Testphasen. Testphase 1: In einem ersten Schritt wurde das Image mit einem Malware-Sample infiziert. In einem weiteren Schritt wurde der Versuch unternommen, das Sicherheitsprodukt zu installieren, den Rechner zu scannen und die erkannte Bedrohung zu entfernen. Testphase 2: Zu Beginn dieser Testphase wurde die Antiviren-Lösung deaktiviert und das System infiziert. Als nächstes wurde die AV-Lösung wieder aktiviert und das System wurde neu gestartet um sicherzustellen, dass sämtliche Komponenten der Sicherheitslösung korrekt installiert und aktiviert wurden. Im letzten Schritt wurde versucht, das System zu säubern und einen zusätzlichen Systemscan durchzuführen.

Während der ersten Testphase gelang es SpyHunter, 19 der 20 Schadprogramme vollständig zu entfernen, welches ein sehr gutes Ergebnis darstellt. Während der zweiten Testphase wurden 16 der 20 Schädlinge entfernt, ein Ergebnis, das immer noch als gut eingestuft werden kann.

SpyHunter konnte die aktiven Komponenten der auf dem Rechner befindlichen Malware neutralisieren. Bei den meisten der übrig gebliebenen Dateien handelte es sich um ausführbare Dateien des Schadprogramms, welche im System unter "C:\Users\vtc\AppData\Roaming\" abgelegt wurden. Nur in einem einzigen Fall war SpyHunter nicht in der Lage, die aktiven Komponenten der Malware zu behandeln, so dass das System weiterhin infiziert blieb.

Übersicht

Angesichts der stetig steigenden Anzahl an Bedrohungen, die entwickelt und über das Internet verbreitet werden, steigt auch das Risiko einer Infektion. Noch vor wenigen Jahren wurden neue Bedrohungen alle paar Tage veröffentlicht. Dies hat sich gewaltig geändert und mittlerweile muss mit mehreren tausend neuen Schadprogrammen pro Stunde gerechnet werden.

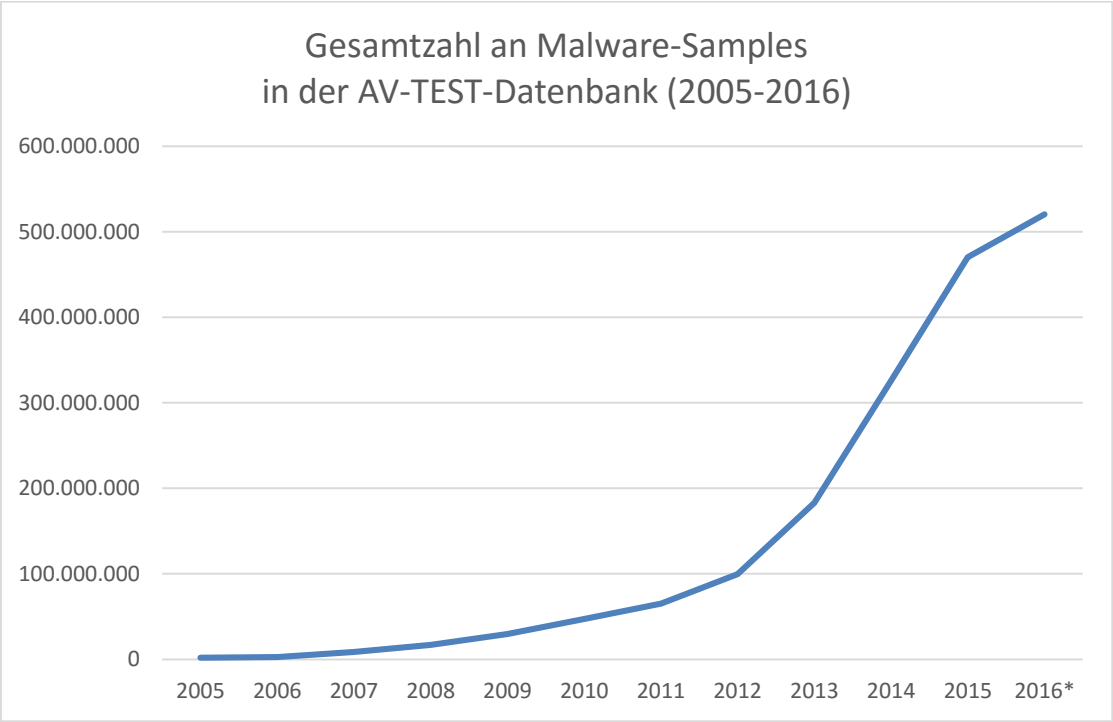


Abbildung 1: Neue Malware-Samples pro Jahr

Während AV-TEST in 2000 noch über 170.000 neue Malware-Samples sammelte, ist die Anzahl an Schädlingen bis 2013 auf über 80 Millionen gestiegen, und in 2016 steigen die Zahlen noch weiter an. Der Anstieg ist in Abb. 1 dargestellt. Derzeit befinden sich mehr als 500 Millionen Malware-Samples in der AV-TEST-Datenbank.

Vor dem Hintergrund dieser Entwicklung kann davon ausgegangen werden, dass allein die Bewältigung einer solchen Menge an neuen Schädlingen, der sich Hersteller von Sicherheitssoftware zum Schutz ihrer Kunden stellen müssen, zu Problemen führen kann. 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 ist es dann schon zu spät. Infektionen können bei Anwendern zu finanziellen Einbußen führen, 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.

Aus diesem Grund gewinnt der Bereinigungsaspekt zunehmend an Bedeutung, wenn ein infizierter Rechner schnell wieder einsatzbereit sein muss. Bei der Entfernung von Malware ist es zwingend erforderlich, dass der Reinigungsprozess in zwei Punkten zuverlässig abläuft:

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

Getestetes Produkt

Bei dem im April/Mai 2016 durchgeführten Test hat AV-TEST die folgende Software in ihrer jeweils aktuellsten 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 aller bis zum 1. Mai verfügbaren Patches und Hotfixes 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.** Während des Remediationprozesses sollten sämtliche verfügbaren Produktfunktionen zum Einsatz kommen.
    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, in welchem Maße 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 solch drastische Schritte für einen erfolgreichen Remediationsablauf nicht erforderlich sind. Sollten solche Methoden eingesetzt werden, führt dies zu Punktabzügen bei der Bewertung.

Bewertung der Wirksamkeit

Für jedes getestete Malware-Sample wurden nach dem folgenden Raster 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 eingesetzt wurde. 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 die Einträge anderer Sicherheitssoftware-Anbieter in der Hosts-Datei verbleiben.

Samples

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

Testergebnisse

In der ersten Testphase erzielte das Produkt der Enigma Software Group ein sehr gutes Ergebnis und ließ lediglich in einem Testfall Dateireste auf dem System zurück. In der zweiten Testphase erzielte SpyHunter 55 von 60 Punkten. Beide Testergebnisse werden in Abb. 2 dargestellt.

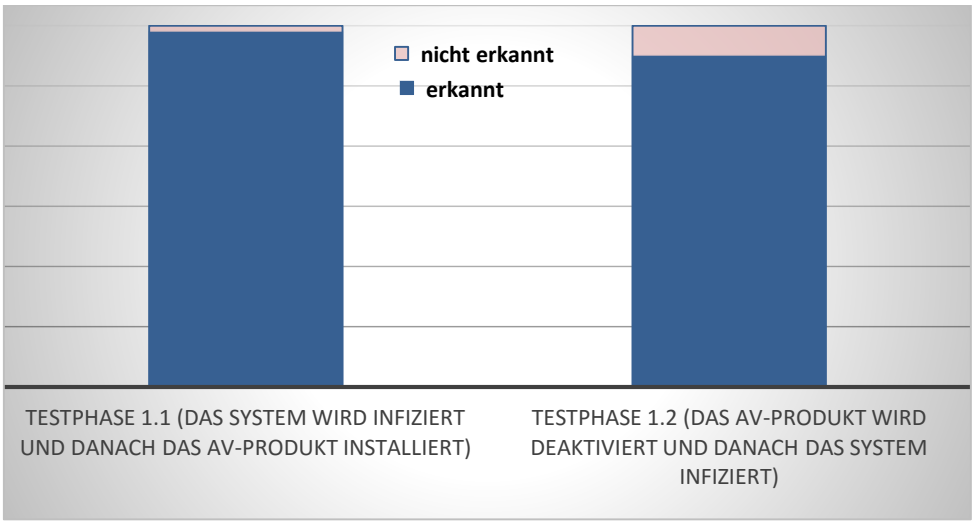
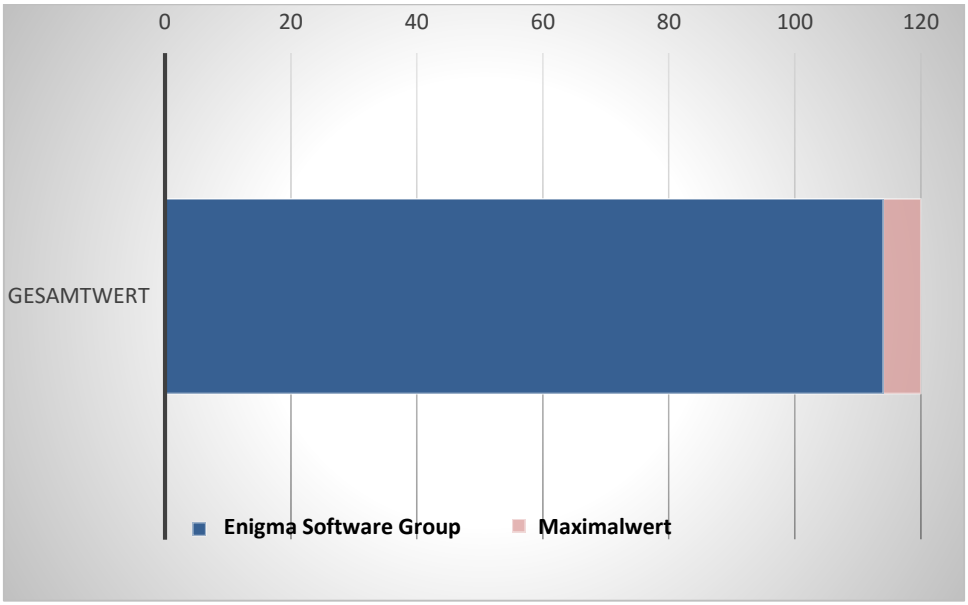


Abbildung 2: Remediation-Ergebnis - Testphasen 1.1 und 1.2

Der Maximalwert, der in diesem Test zu erreichen war, lag bei 120 Punkten. Der von Enigma Software Group erreichte Gesamtwert lag bei 114 Punkten, dargestellt in Abb. 3. Was die Performance in Hinblick auf die Reinigungsleistung angeht, zeigte sich während der zweiten Testphase, dass einige Infektionen nicht komplett beseitigt werden konnten. SpyHunter entfernte die aktiven Komponenten der auf dem Rechner befindlichen Malware. Bei den meisten Dateiresten handelte es sich um ausführbare Dateien der Schadprogramme, welche im System unter dem Ordner "C:\Users\vtc\AppData\Roaming\" abgelegt wurden. Nur in einem einzigen Fall war SpyHunter nicht in der Lage, die aktiven Komponenten der Malware zu behandeln und das System blieb weiterhin infiziert.

In der Testphase 1.1 erzielte das Produkt jedoch ein sehr gutes Ergebnis und erlaubte sich nur einen Fehler.



Anhang

Information zur getesteten Softwareversion

Entwickler, Hersteller	Produktbezeichnung	Programmversion	Engine/Signaturversion
Enigma Software Group	SpyHunter	4.22.4.4657	2016.04.26v1

Liste der verwendeten Malware-Samples (Remediation-Test)

(SHA256)
0x026bb4f1db988785351ab7d3889c3b322b69398042ae7d52e8e4740e9618eec1
0x02c6d5aeb2ab78f781d72ba60d6f7ff7f5928d47a26ca8dcc4a5c1398850e62a
0x1e3a054ed8051c06a78dc37922c2297a5c3da51a84beb99bc2a487381851ede4
0x1eaef8613ab91e13484646dcb61f5721858066850124a7de5ffce2767bad2ff0
0x2164f112693ab13ef45f159a0444ea64b94942518e829aa55b7d277722b87179
0x2656834a0380bc4c830daef09cfafd038fd5e7727303b09170a8fe37c35a1e34
0x32f0a426e80fb26d098a22bf624d3fb21342372a2135337e9f06ffc4af442846
0x3436da965e7fdbde9a9836acc712ff437d5e7c49a821366451308e11555924f1
0x406ada699acb288bfa2755a9ebe807aa86b90f475b332799f925d85b0d195c61
0x443660d22f3c4bfdb2c2ff4d3e25dafd01f7002bcde53ad7bac8b777e700123a
0x56e24a3dc8b07ea6e08e3d4e4ba96e1e9101aca932523c34350fafbcff02ac85
0x5c596c8afd4656946f0a9741f2be4bb088dda26f1ddcf41eb8c427fbb6d1c3ec
0x60eeb661ad33aa50d9ce1355f9e70afde317411f81e7d0890f38ae28ea79b1b4
0x659896ed065fd59fb843022022a7796ec76620000c7c29a009c7f399898845cb
0x70b64248b23182827c8f52be598a4a10bf0784dc1d97e8721a528ec9cec3acc9
0x76c9c0758ea91e38f8cf47fcc01d597a213eed5f2001ff5f8f7763df236e6baf

0x882ac415de83252554349e3221c7bb5028da1db36b55f196f3cf0a9861ef4597
0x95a1d1207cc0a75eaaeef1a985b8c8bbe15a314c43f2b4d593033cf426bb9212
0x9a679f8745896abd8fbe1586eabc3690858f6d966f4a9c5eb52b6f3b64cd35dd
0xa3efd281adaf729075ee466793fe2a2a6972b746d15e9578355957fc7e7daee2

Tel. +49 391 6075460, Fax +49 391 6075469, Internet http://www.av-test.org