Rapporto prova di riparazione

La prova è stata effettuata dalla AV-TEST GmbH per incarico della EnigmaSoft Limited.
Data del rapporto: 03 settembre 2018, ultimamente attualizzato il 04 settembre 2018

Riassunto

In agosto 2018 la AV-TEST ha condotto una prova della capacità di riparazione di SpyHunter della EnigmaSoft Limited. La prova è stata effettuata su un sistema con Windows 10 (RS3, 64 Bit) pulito, e la stessa immagine del disco è stata usata su diversi PC identici.

Il corpo di prova della malware per la prova di riparazione era costituito da 12 campioni ed era suddiviso in due passaggi: passaggio 1 del test: Prima l'immagine è stata contaminata con uno dei campioni di malware: nel prossimo passaggio è stato tentato di installare il programma di protezione, di effettuare una scansione del PC e di rimuovere i pericoli riscontrati. Passaggio 2 della prova: In questo caso è stato prima deattivato il software AV, per potere contaminare il sistema. Quindi il software AV è stato riattivato ed è stato effettuato un reboot, per assicurare che tutti i componenti di AV Software lavorino correttamente. Quindi è stato tentato di riparare il sistema e di effettuare un ulteriore scansione del sistema.

SpyHunter ha raggiunto un risultato perfetto del 100% in entrambe le sezioni del test. Il software di Enigma ha ripulito tutti i componenti attivi e rimosso dal sistema tutti gli artefatti di malware.

Sommario

A causa del numero crescente delle minacce pubblicate e diffuse attraverso internet, aumenta anche il pericolo d'infezione per i sistemi. Alcuni anni fa i virus apparivano solo in intervalli di alcuni giorni. Oggi ci sono migliaia di nuove minacce ogni ora.

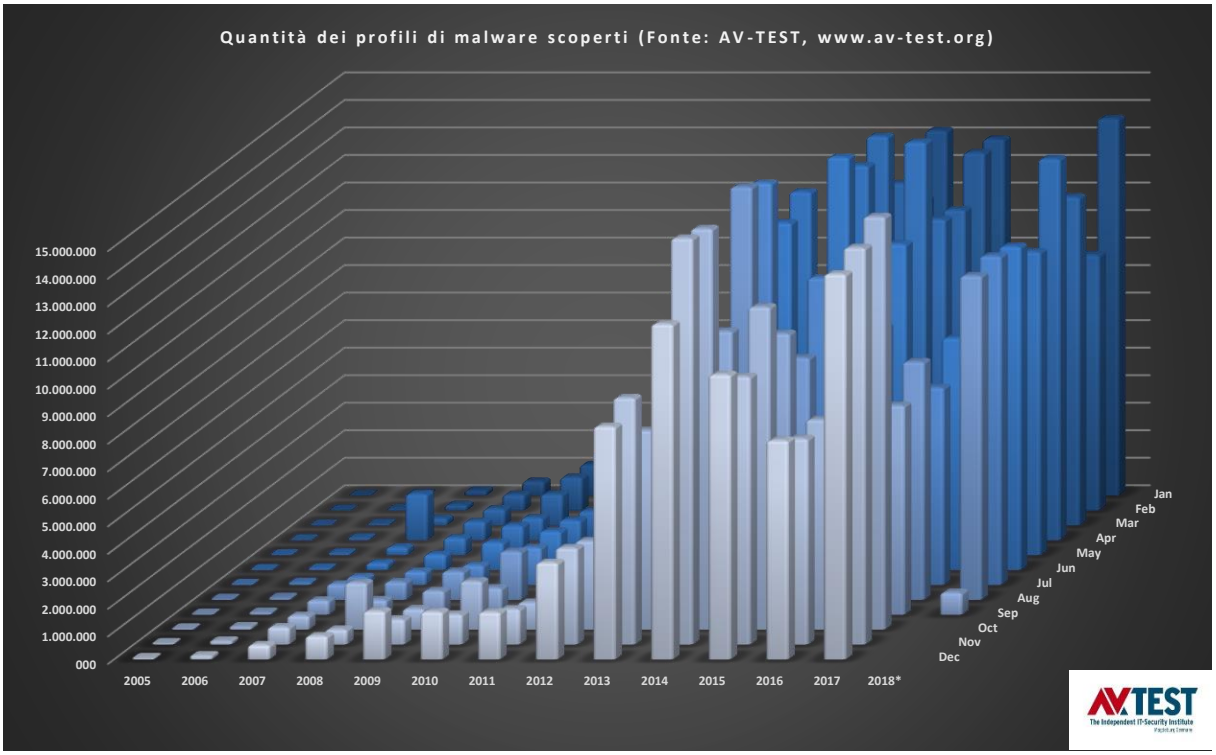


Immagine 1: Nuovi profili all'anno

Nell'anno 2000 AV-TEST ha ricevuto più di 170.00 nuovi profili, nel 2013 il numero dei nuovi profili era cresciuto a 80.000.000. Negli anni seguenti il numero è ulteriormente aumentato, come dimostra il grafico nell'immagine 1. La banca dati di AV-TEST contiene attualmente più di 800 milioni di profili malware. Nella prima metà dell'anno 2018, i sistemi di rilevazione di AV-TEST registrano circa 10 milioni di profili nuovi per ogni mese.

La quantità dei profili nuovi deve essere processata dai fornitori di programmi anti-malware, per proteggere da problemi i loro clienti. Però non è sempre possibile proteggere tempestivamente un PC. Un PC può anche essere infettato mentre è installato un software antivirus attuale, poiché i profili possono solo essere messi a disposizione ogni paio di ore, il ché ogni tanto può essere troppo tardi. Le infezioni causano perdite economiche, perché vengono rubati dati riservati o il PC non può più essere usato in modo produttivo, fino a quando il malware è rimosso interamente dal sistema.

Dunque le tecniche di riparazione per rendere di nuovo utilizzabile un PC infettato, sono diventate sempre più importanti. L'impiego di tali tecniche presuppone che il processo di pulizia sia efficiente sotto due aspetti:

1. Il malware e tutti i suoi componenti devono essere rimossi, e tutte le modifiche nocive del sistema devono essere annullate.
2. Il processo di pulizia non deve danneggiare I programmi già puliti o il sistema stesso.

Prodotto esaminato

La prova è stata effettuata in agosto 2018. AVTEST ha impiegato l'ultima versione disponibile alla data della prova del seguente software:

- SpyHunter dell'EnigmaSoft Limited

Metodo e punteggio

Plattforma

Tutte le prove sono state condotte su PC identici dotati del seguente hardware:

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

La prova è stata effettuata in agosto 2018. AV-TEST ha impiegato l'ultima versione del seguente software disponibile alla data della prova.

Metodo di prova

La prova di riparazione è stata suddivisa in dieci passi secondo il metodo descritto in seguito:

1. **Sistema pulito per ogni campione**. I sistemi di prova sono stati messi in stato pulito, prima di essere rispettivamente esposti a un profilo di malware.
2. **Computer fisici**. I sistemi di prova impiegati erano veri computer fisici. Non sono stati impiegati computer virtuali.
3. **Accesso a internet**. I computer potevano accedere a internet in qualsiasi momento, per fare uso di eventuali richieste nella nuvola informatica.
4. **Configurazione prodotto.** Tutti i prodotti e i loro strumenti di riparazione o gli strumenti di ripristino capaci al reboot operavano con le impostazioni standard preconfigurate.
5. **Infezione dei computer di prova**. Un computer nativo è stato infettato con un programma maligno ed è quindi stato riavviato. Occorreva assicurare che il programma maligno fosse pienamente operativo.
6. **Famiglie campioni e payloads**. I profili esaminati non provenivano dalla stessa famiglia e non contenevano neanche lo stesso payload.
7. **Riparazione con l'impiego di tutte le capacità disponibili del prodotto**

a. Tentare di installare il prodotto di sicurezza con le impostazioni standard. Quindi assicurare che siano osservate le complete istruzioni del prodotto per la rimozione.
b. Se a. non funziona, tentare una soluzione con uno ***strumento di riparazione stand-alone/strumento di salvataggio*** (se disponibile).
c. Se b. non funziona, tentare la ***soluzione di avvio*** stand-alone (se disponibile) e usarla per la riparazione.

8. **Validazione della rimozione**. Il PC è stato ispezionato manualmente, per validare una rimozione impeccabile e la presenza di artefatti.
9. **Scoring della prestazione di rimozione**. L'efficienza del programma e della soluzione di sicurezza complessiva è stata valutata con l'aiuto del sistema di scoring previsto.
10. **Riparazione troppo aggressiva**. Il test ha anche rilevato l'aggressività del prodotto durante la riparazione. Alcuni prodotti rimuovono per esempio il file hosts o anche un intero indice, anche se ciò non sarebbe necessario per una riparazione efficiente. Questo comportamento giustifica una valutazione negativa del prodotto.

Rating dell'efficienza

Per ogni profilo testato si assegnano punti secondo il seguente sistema:

a. Il malware è stato interamente rimosso (3)
b. Il malware è stato identificato e rimosso, restano solo tracce inattive (2)
c. E' stato trovato e parzialmente rimosso qualcosa, ma sono sempre ancora attive tracce del malware (1)
d. Il malware non è stato né identificato, né rimosso (0)

Il punteggio non dovrebbe considerare, quali tecniche siano state necessarie per rimuovere il malware. Però dovrebbe essere impiegate tutte le tecniche. Se un prodotto cancella tutte le registrazioni dal file hosts e lascia il prodotto in stato funzionante e attualizzabile, deve ottenere il pieno punteggio per la riparazione, anche se nel file hosts restano registrazioni per altri sistemi di sicurezza

Profili

Il campione contiene 12 file nocivi, i quali erano in grado di infettare Windows 10 (RS3, 64 Bit).

Risultati del test

EnigmaSoft Limited ha ottenuto un risultato perfetto del 100 % in entrambe le fasi del test.
I risultati delle due sezione di test sono riportate nell'immagine 2.

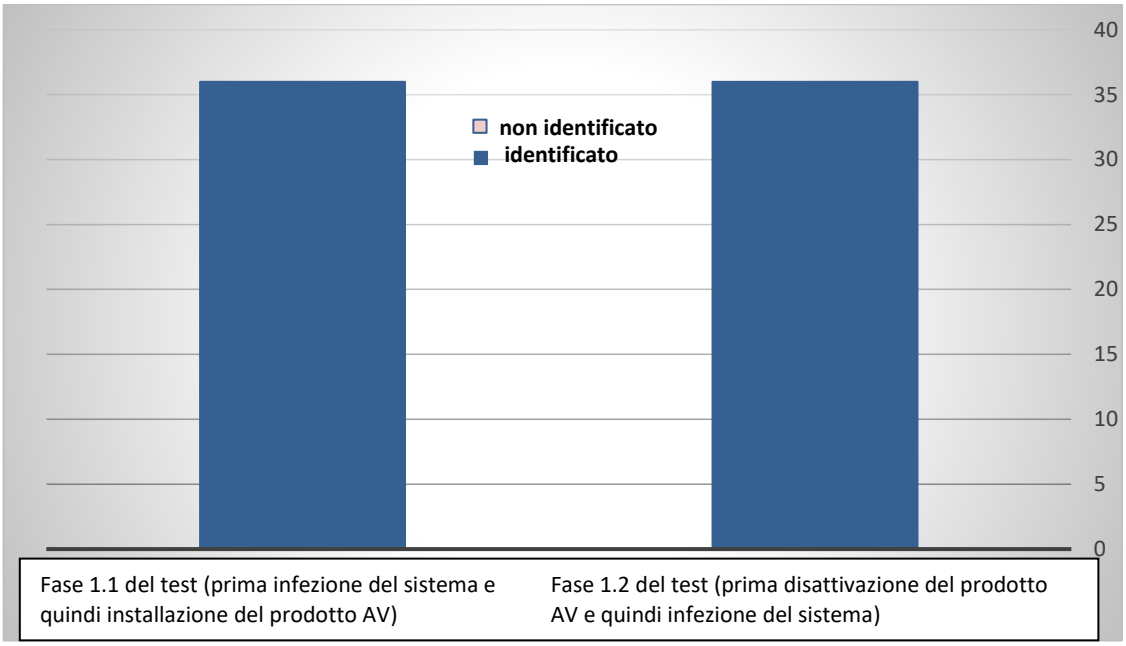
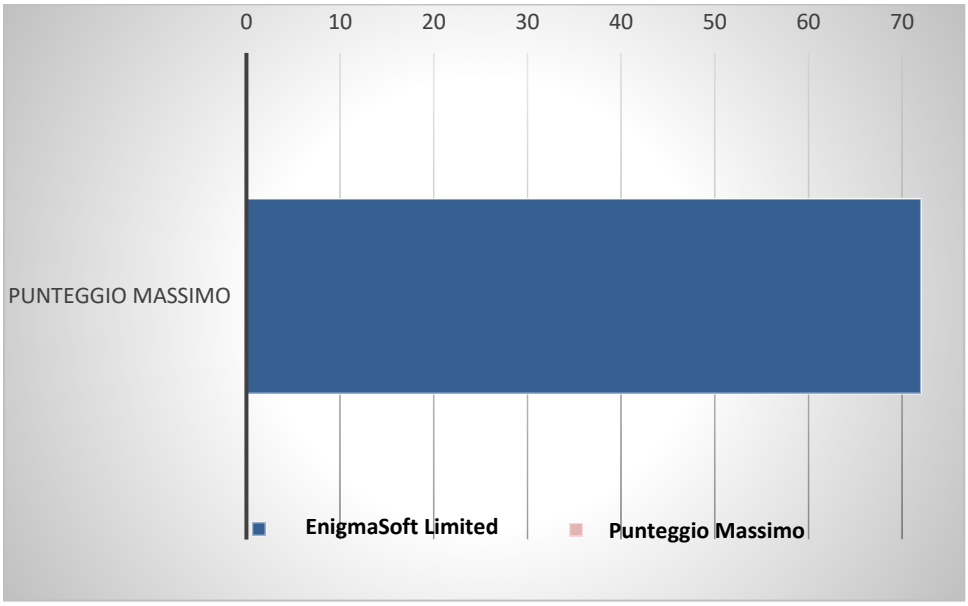


Immagine 2: Risultato della riparazione – Fasi 1.1 +1.2 del test

Per quanto riguarda la prestazione di pulizia, SpyHunter è stato in grade di pulire il sistema di tutti i 12 profili testati. Inoltre sono stati perfettamente eliminati tutti gli artefatti e le registrazioni del registry.

Il punteggio massimo raggiungibile era di 72. Come si rileva dall'immagine 3, EnigmaSoft Limited ha raggiunto l'eccellente risultato di 72 punti.



Allegato

Versione del software sottoposto a prova

Sviluppatore, distributore	Nome prodotto	Versione programma
EnigmaSoft Limited	SpyHunter 5	5.0.30.51

Elenco dei campioni utilizzati nella prova di riparazione

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