Infezione da malware

Per navigare in modo sicuro in Internet è indispensabile disporre di un programma antivirus e di un sistema operativo che si aggiorna automaticamente. Tuttavia può comunque capitare che un computer venga infettato da un malware. Riconoscetelo e reagite nel modo giusto!

Come si riconosce un'infezione da malware?
Possibili indizi:

- Segnalazione di infezione del programma antivirus.
- Messaggi di errore all'avvio o allo spegnimento del computer.
- Il computer risulta instabile – si verificano frequenti crash.
- Sistema lento, continuo sovraccarico della memoria RAM e/o del processore, continua attività del disco rigido.
- Il programma antivirus è disattivato (anche dopo che lo avete attivato esplicitamente).
- Non è più possibile aprire il sito Internet di uno o più fornitori di antivirus.

Per sapere come vi potete proteggere da un'infezione da malware, leggete la «fase 2 – Monitorare» (https://www.ebas.ch/it/2-monitorare-con-antivirus-e-firewall/) delle nostre «5 operazioni per la vostra sicurezza digitale» (https://www.ebas.ch/it/5-operazioni-per-la-vostra-sicurezza-digitale/) . Vi troverete anche un elenco di programmi antivirus, alcuni dei quali disponibili gratuitamente. Tuttavia, se avete un forte sospetto di aver subito un'infezione, l'importante è reagire correttamente.

I passaggi più importanti dopo un'infezione da malware:

1. Mantenere la calma, interrompere la connessione a Internet e controllare l'ultimo backup dei dati. (#step1)
2. Decidere se è necessario contattare uno specialista. (#step2)
3. Identificare e rimuovere il malware. (#step3)
4. Ultima via di scampo – riformattare e ripristinare. (#step4)

Il termine «malware» è un composto delle parole inglesi «malicious» (maligno) e «software». Si tratta di un termine generico per indicare qualsiasi genere di software che esegue funzioni dannose su un dispositivo (come virus, worm, cavalli di Troia e ransomware).

Copyright © 2024 – Tutti i diritti riservati. Scuola Universitaria Professionale di Lucerna – Informatica

Maggiori informazioni:
Infezione da malware – che cosa bisogna fare?

Fase 1: mantenere la calma, interrompere la connessione a Internet e controllare l'ultimo backup dei dati

Come prima cosa è opportuno interrompere la connessione a Internet (scollegare il cavo LAN risp. disattivare la WLAN). Controllare quindi a che data risale l'ultimo backup dei dati. È consigliabile eseguire un'ulteriore, nuova copia di sicurezza dei dati su un supporto di memorizzazione esterno diverso da quello usato per il backup normale.

Nota bene: non è da escludere che con il backup venga salvato anche il malware, fattore comunque non rilevante in un primo momento.

Fase 2: decidere se è necessario contattare uno specialista

Decidete allora se preferite rimuovere il malware da soli o se preferite richiedere l'intervento di un esperto. Diversi fornitori di antivirus offrono un servizio speciale per la rimozione del malware. Spesso si tratta di assistenza telefonica o di «rimozione del malware tramite assistenza remota». Questi servizi, tuttavia, sono a pagamento. In alternativa anche molti negozi specializzati in informatica offrono servizi di riparazione (in particolare per le infezioni da malware).

Fase 3: identificare e rimuovere il malware

Certi tipi di malware possono essere eliminati direttamente dal programma antivirus installato, ma non tutti. Se non è possibile rimuovere il malware con il vostro programma antivirus, è consigliabile utilizzare un cosiddetto «Second Opinion Virus Scanner» come:

- Malwarebytes (https://it.malwarebytes.com)
- HitMan Pro (https://www.hitmanpro.com)

Se non vi si riesce nemmeno in questo modo, occorre identificare esattamente il malware. La soluzione migliore consiste nel prendere nota della descrizione del malware (indicata dal programma antivirus) e cercare in Internet (usando un altro dispositivo, non infettato) istruzioni su come eliminarlo. La maggior parte dei fornitori di antivirus pubblica banche dati di malware che riportano informazioni utili su come rimuoverli. Se il vostro fornitore di antivirus ha messo a disposizione un CD avviabile, provate ad avviare il computer con quel CD per rimuovere il malware.

Banche dati di malware

- Avira (https://www.avira.com/it/support-virus-lab)
- Microsoft (https://www.microsoft.com/security/portal/)
- Broadcom-Symantec (https://www.broadcom.com/support/security-center/a-z)
- Trend Micro (https://www.trendmicro.com/vinfo/it/threat-encyclopedia/)

Strumenti di rimozione (Rmoval Tools)

Copyright © 2024 – Tutti i diritti riservati. Scuola Universitaria Professionale di Lucerna – Informatica

- Microsoft (https://support.microsoft.com/en-us/topic/remove-specific-prevalent-malware-with-windows-malicious-software-removal-tool-kb890830-ba51b71f-39cd-cdec-73eb-61979b0661e0)
- Norton-Symantec (https://support.norton.com/sp/en/us/home/current/solutions/kb20100824120155EN)

Per i malware più diffusi i fornitori di antivirus mettono a disposizione gratuitamente cosiddetti strumenti di rimozione o «removal tools» in grado di verificare se su un computer è presente un certo malware e, in tal caso, di eliminarlo automaticamente. Quando si scarica uno strumento di rimozione è indispensabile prestare attenzione alla fonte, che deve essere un sito Internet attendibile (p. es. il sito di un fornitore di antivirus noto): ci sono infatti programmi antivirus e strumenti di rimozione che vengono creati dai criminali informatici e contengono essi stessi il malware.

Fase 4: ultima via di scampo – riformattare e ripristinare

Se dopo tutte queste operazioni non si ottiene comunque il risultato sperato, occorre ripristinare il computer da zero (oppure ritornare alla fase 2 e chiedere consiglio a un esperto).

Per sapere come eseguire una nuova installazione pulita del sistema riducendo allo stesso tempo il rischio di una nuova infezione potete leggere le nostre istruzioni (per Windows 10) (https://www.ebas.ch/it/reinstallazione-di-windows-10/) .

Copyright © 2024 – Tutti i diritti riservati. Scuola Universitaria Professionale di Lucerna – Informatica