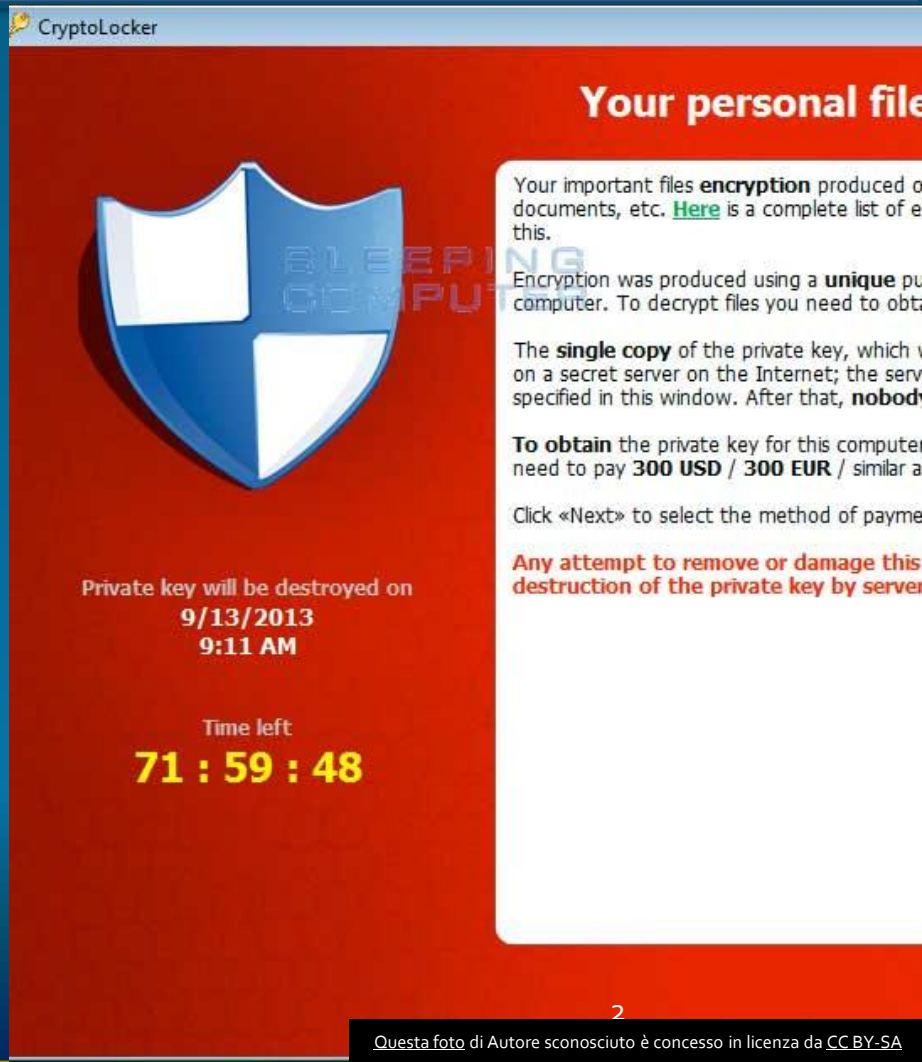
CYBER SECURITY

I Sintomi di un attacco

1. Messaggio di riscatto

- Questo è il periodo d'oro dei ransomware (come il famoso Cryptolocker), ossia malware (malicious software) creati per disturbare le attività di un computer, rubare informazioni sensibili o mostrare pubblicità indesiderate al fine di ottenere un riscatto in cambio della loro decriptazione.

- Se sei fortunato, alcuni dei messaggi ransomware provengono da programmi che non bloccano i tuoi dati (noti come scareware) e di conseguenza il riavvio del computer è sufficiente a farlo scomparire.



3. Barre degli strumenti del browser indesiderate

Questo è un segno molto comune di uso improprio del proprio computer.

La maggior parte dei browser (da Google, a FireFox) consente di rivedere le barre degli strumenti installate e attive, per cui basta rimuovere quelle che non sono state installate volontariamente e in ogni caso rimuovere anche quelle di cui si è incerti.

5. Popup di riscatto (e non) frequenti

- Questo segnale di violazione è uno dei più fastidiosi. Quando si ricevono popup di browser casuali da siti Web che normalmente non li generano, significa che il sistema è stato compromesso.
- In genere i popup casuali vengono generati da uno dei precedenti segnali sopra riportati. Ad esempio, bisogna sbarazzarsi di false barre degli strumenti o di altri programmi per non visualizzare più i popup maligni.

2. Messaggi antivirus falsi

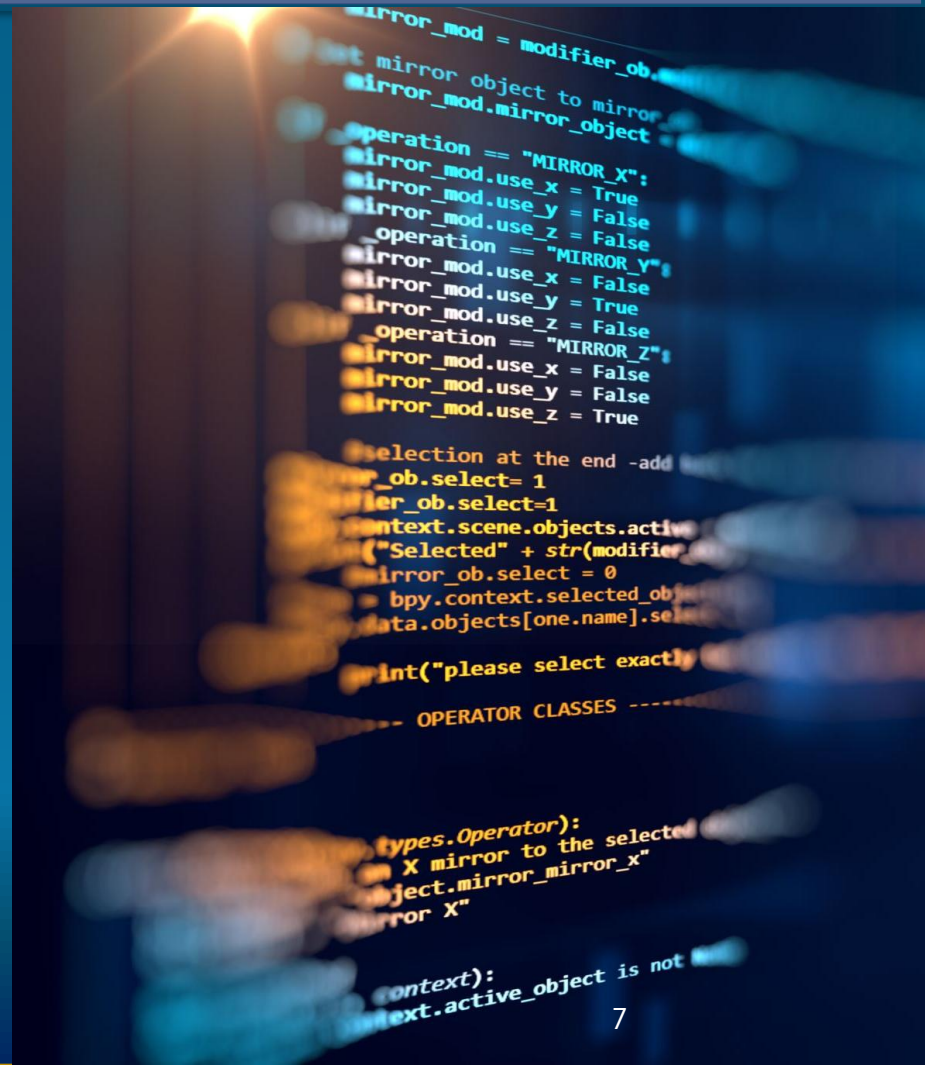
- Negli ultimi tempi si sono visti di meno ma non passano mai di moda: i falsi messaggi di avviso antivirus (diversi dal programma antivirus che stai usando) – considerati tra i segnali più certi che il tuo sistema è stato attaccato.
- Una volta che il messaggio è stato visualizzato, il danno è fatto e di conseguenza è troppo tardi per intervenire sull'intrusione.
- Come funziona? La falsa scansione, che scova sempre tonnellate di "virus", è un'esca per farti comprare il loro prodotto.
- Cliccando sul link fornito, si atterra su un sito web (che sembra sicuro) dove vengono chiesti il numero della carta di credito e i dati di fatturazione e il pagamento arriva direttamente nelle tasche degli hacker.

2. MESSAGGI ANTIVIRUS FALSI

- Che cosa fare? Non appena si nota il falso messaggio, spegnere il computer o avviare il sistema del computer in modalità provvisoria, senza rete e provare a disinstallare il software appena installato (spesso può essere disinstallato come un normale programma). In entrambi i casi, bisogna provare a ripristinare il sistema in uno stato precedente all'intrusione.

4. Ricerche Internet reindirizzate

- Molti hacker si guadagnano da vivere reindirizzando il tuo browser in un link diverso da quello che vuoi.
  Sfortunatamente, ad oggi molte delle ricerche Internet reindirizzate sono ben nascoste all'utente attraverso l'uso di proxy aggiuntivi, quindi i risultati fasulli non vengono mai restituiti per avvisare l'utente.



6. Sui social media arrivano richieste di amicizia non inviate da te

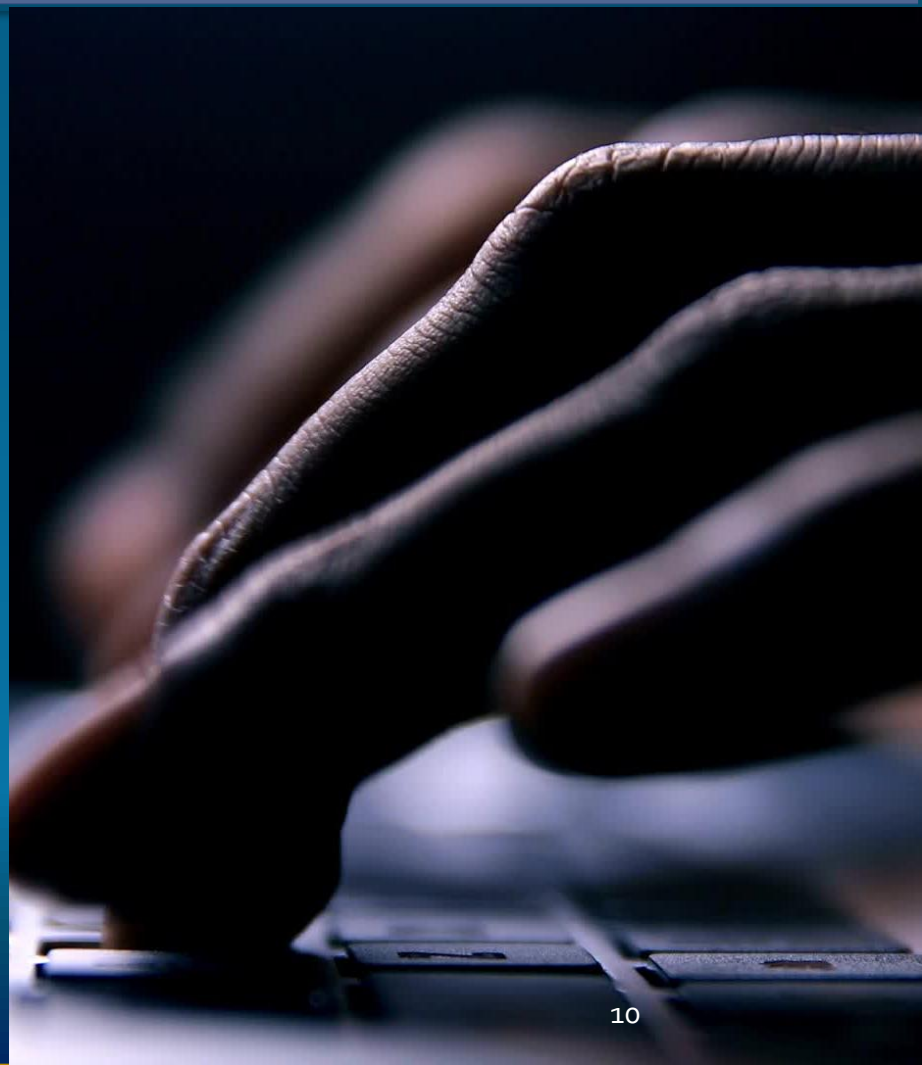
- A volte può capitare di ricevere richieste di amicizia sui social media quando si è già collegati con quella persona.
- Subito si pensa che la richiesta non è stata accettata per cui è stata inviata nuovamente; dopodiché si nota che il profilo di quella persona è privo di amici riconoscibili e non presenta nessuno dei post più vecchi.

6. Sui social media arrivano richieste di amicizia non inviate da te

- Oppure avviene la stessa problematica al contrario (ossia tu stai inviando nuove richieste). In entrambi i casi, l'hacker controlla il tuo profilo social e ha creato una seconda pagina fasulla simile oppure tu o un tuo amico avete installato un'applicazione fasulla del social media.
- In questo caso, la prima azione da compiere è avvertire gli amici comuni di non accettare la richiesta. Infine, contattare il sito per segnalare l'accaduto e cambiare il proprio metodo di autenticazione.

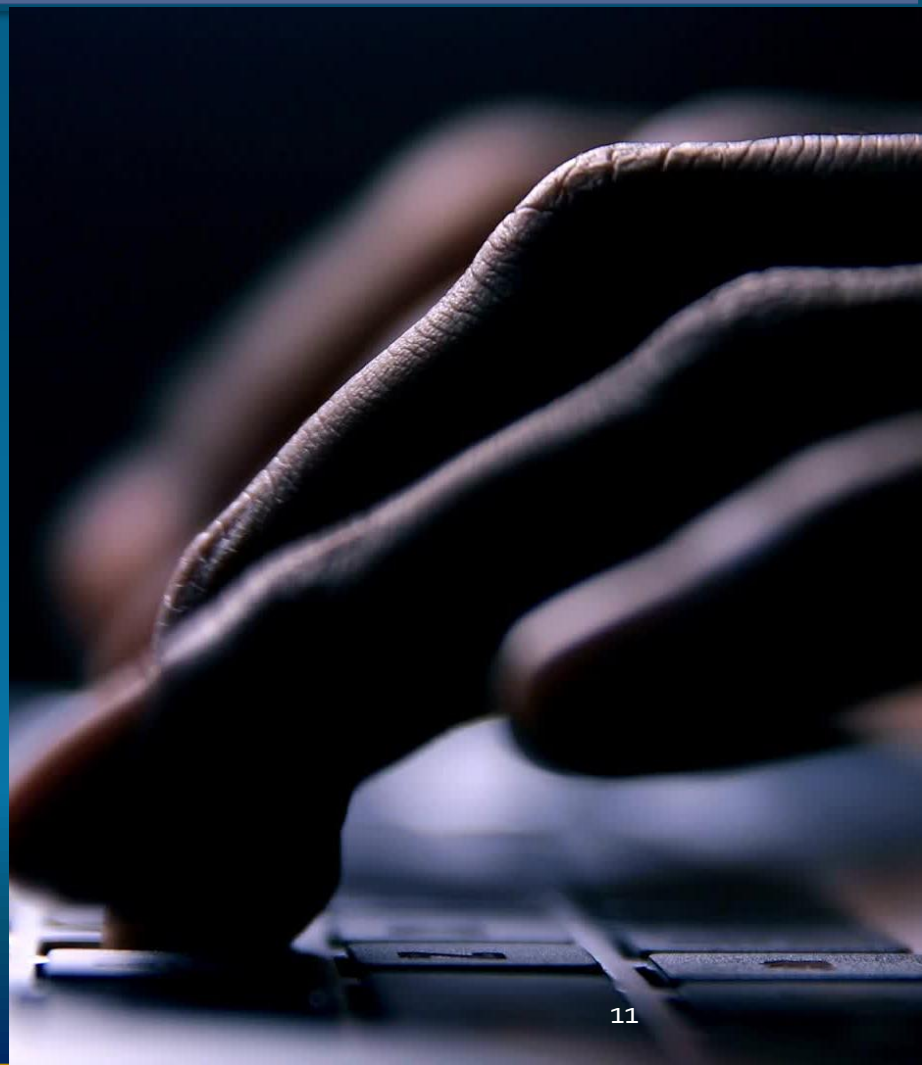
7. La password online non funziona

- Se stai digitando la tua password online correttamente e non funziona, potresti essere hackerato. Di solito è necessario riprovare, perché a volte i siti hanno delle problematiche tecniche che fanno sì che non venga accettata la password valida per un breve periodo di tempo.
- Ma se capisci che la tua password attuale non funziona più, probabilmente un hacker ha effettuato l'accesso al posto tuo e l'ha cambiata per tenerti fuori



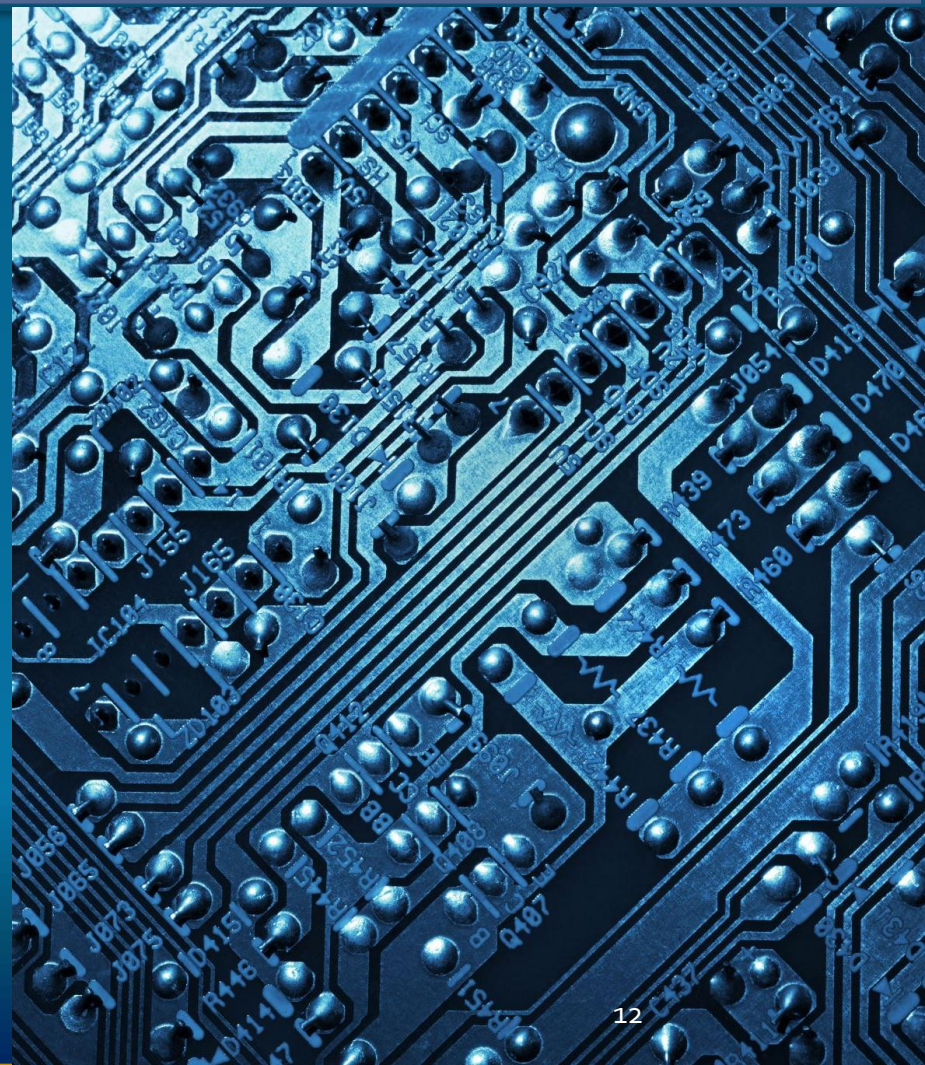
7. La password online non funziona

- La vittima ha risposto a un messaggio di posta elettronica ingannevole dall'aspetto autentico che presumibilmente apparteneva al servizio in cui è stata modificata password. L'hacker, in questo modo, raccoglie le informazioni di accesso, accede, modifica la password (e altre informazioni per complicare il recupero) e utilizza il servizio per rubare denaro alla vittima o ai conoscenti della vittima (fingendo di essere la vittima stessa).
- L'azione immediata da fare è modificare le credenziali di accesso e si potrebbe valutare anche l'utilizzo di servizi online che forniscono l'autenticazione a due fattori. Rende il tuo account molto più difficile da manomettere.



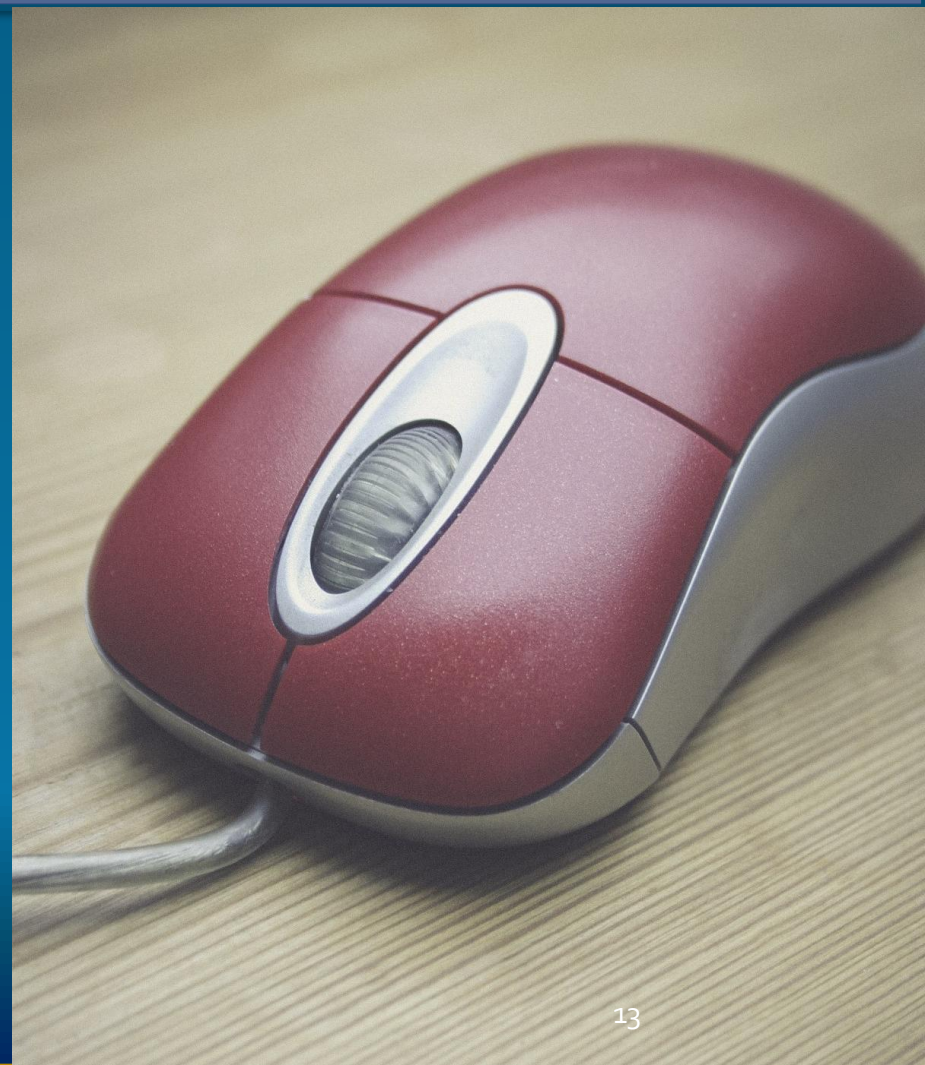
8. Installazioni inaspettate di software

- Installazioni di software indesiderate e inaspettate sono un importante segnale che il tuo sistema informatico è stato probabilmente violato.
- I malware infatti sono perlopiù programmi informatici – Trojan e worm – che funzionano modificando altri programmi sicuri per potersi nascondere meglio.
- Ci sono molti programmi gratuiti che mostrano tutti i programmi installati e consentono di disabilitarli. Ciò che conviene fare in ogni caso è disabilitare il programma non riconosciuto e riavviare il PC.



9. Il mouse si muove da solo tra i programmi

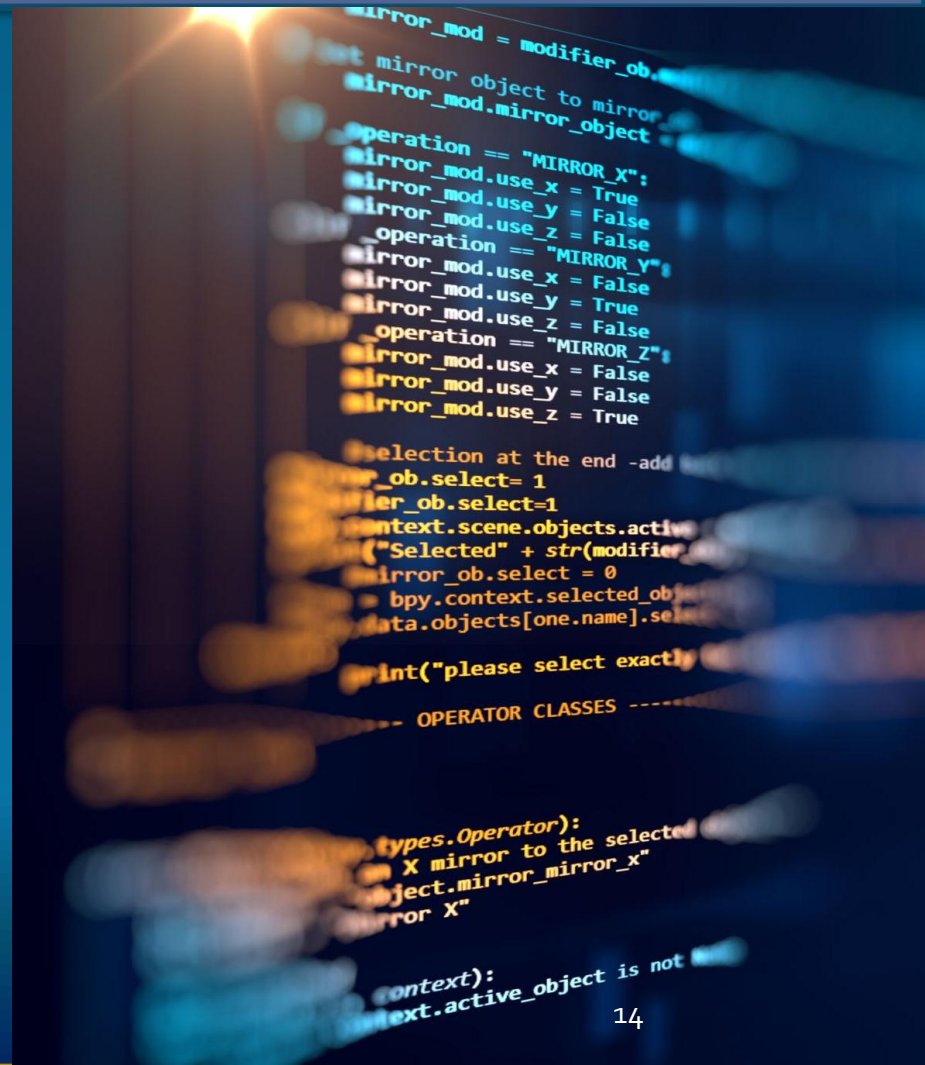
- Se il tuo puntatore del mouse si muove da solo mentre esegui delle selezioni che funzionano correttamente, sei stato sicuramente hackerato.
- Infatti, i puntatori del mouse si muovono spesso in modo casuale, solitamente a causa di problemi hardware.
- Tuttavia, se i movimenti implicano scelte corrette per eseguire programmi particolari, gli hacker sono coinvolti in qualche modo.



10. Software e Servizi Disabilitati e non riavviabili

Il software antimalware, Task Manager o Editor del Registro di sistema, è disabilitato e non può essere riavviato

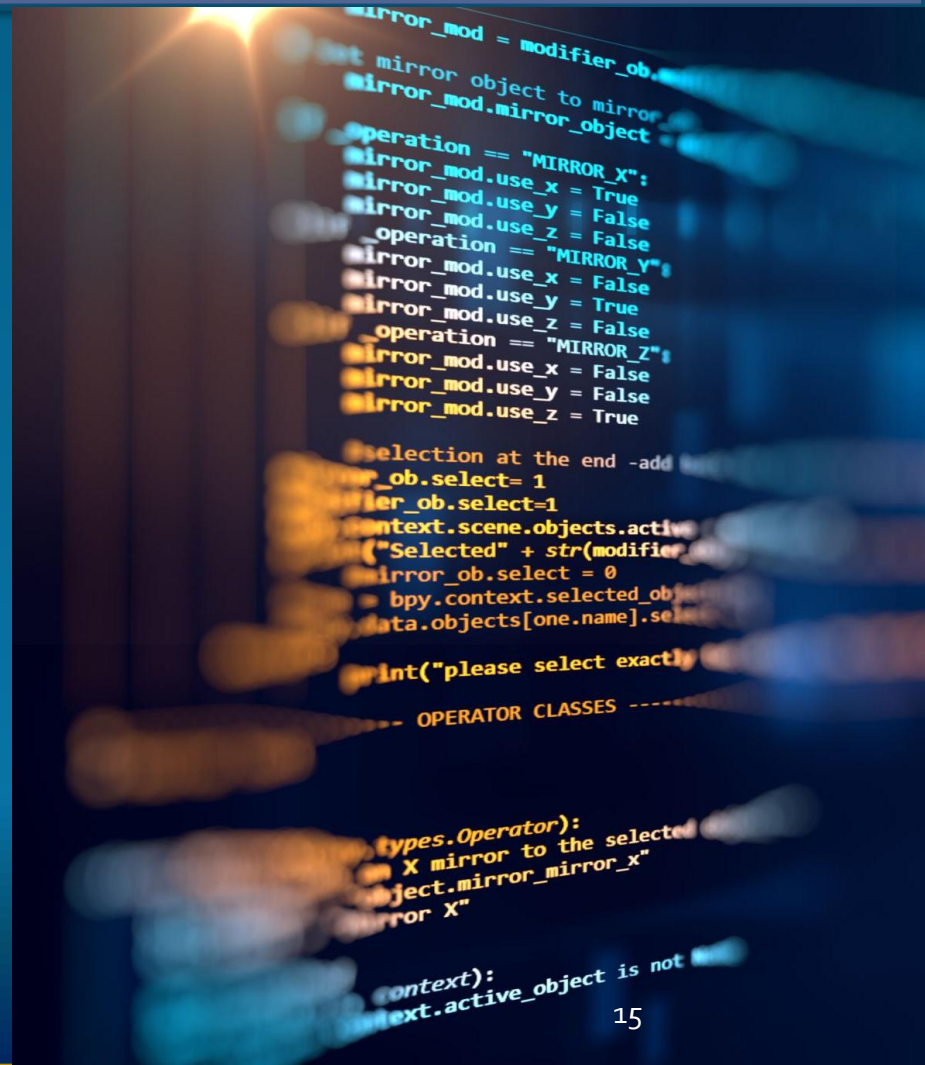
- Questo è un enorme segnale di intrusione ed è abbastanza dannoso. Se noti che il tuo software antimalware è disabilitato e non sei stato tu a disabilitarlo, probabilmente sei stato attaccato; specialmente se provi ad avviare Task Manager o Editor del Registro di sistema e questi non si avviano o iniziano a funzionare e scompaiono.



10. Software e Servizi Disabilitati e non riavviabili

Il software antimalware, Task Manager o Editor del Registro di sistema, è disabilitato e non può essere riavviato

- Il primo intervento da eseguire è un ripristino completo perché non si sa esattamente cosa è successo. Se si vuole fare qualcosa di meno drastico, si può provare ad eseguire Autoruns o Process Explorer (o programmi simili) che permettono di disinstallare o eliminare il software dannoso che causa i problemi.



11. Il tuo account online non ha soldi

- I criminali informatici di solito non rubano un po' di soldi; a loro piace spesso trasferire tutto o quasi tutto in valuta estera o in banca. Di solito il problema nasce dal tuo computer che viene compromesso o da te che rispondi a una truffa della tua banca o della tua società di trading azionaria preferita.
- In ogni caso, i cattivi accedono al tuo account, cambiano le tue informazioni di contatto e trasferiscono somme ingenti di denaro a loro stessi.

12. Ricezione di chiamate da negozi in merito al mancato pagamento delle merci spedite

- In questo caso, gli hacker hanno compromesso uno dei tuoi account, effettuato un acquisto e quest'ultimo l'hanno spedito in un posto diverso da casa tua.
- La prima azione da intraprendere include sicuramente la modifica dei nomi e delle password di accesso (non solo quello relativo al singolo account compromesso). Dopodiché sarà necessario chiamare le forze dell'ordine, avviare una causa e inizia a monitorare il tuo credito.
- Probabilmente passerai mesi a cercare di chiarire tutte le transazioni fasulle commesse a tuo nome, ma dovresti essere in grado di annullarne la maggior parte, se non tutte.