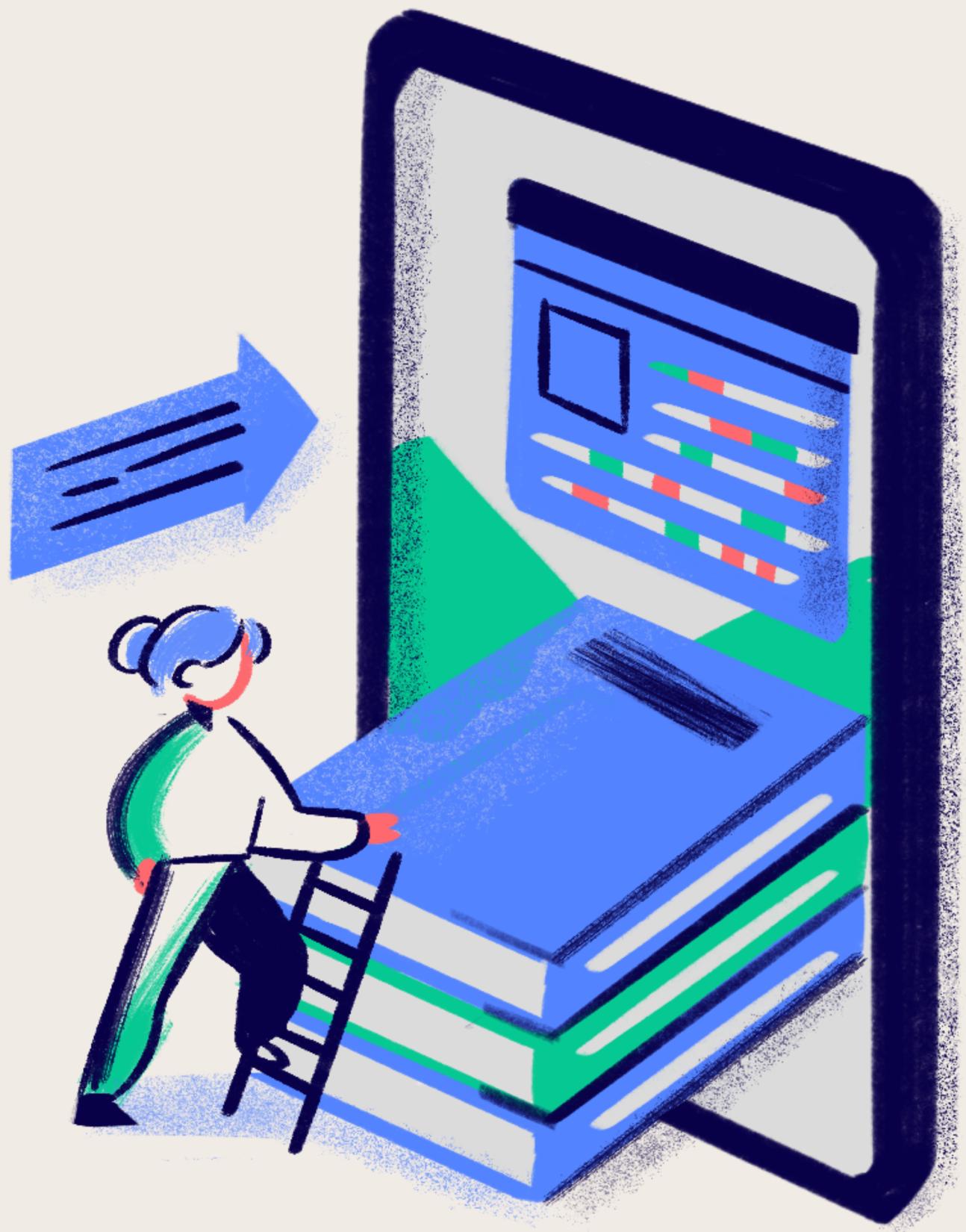


PRESENTATO DA ANDREA PANICUCCI

BW III :

TRACCIA 5



TRACCIA:

GINA (Graphical identification and authentication) è un componente lecito di Windows che permette l'autenticazione degli utenti tramite interfaccia grafica utenti di inserire username e password nel classico riquadro Windows, come quello in figura a destra che usate anche voi per accedere alla macchina virtuale.

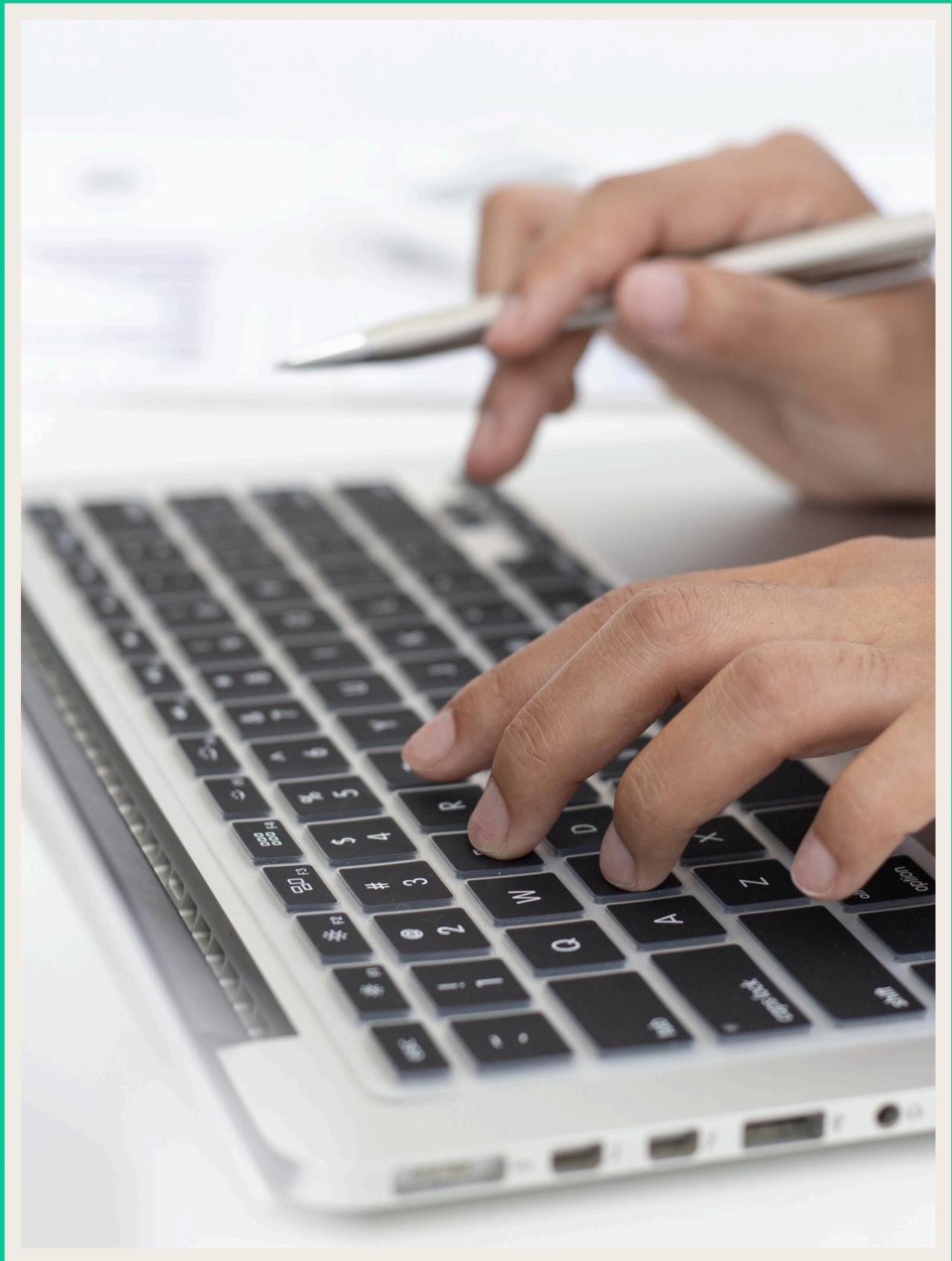
- Cosa può succedere se il file . dll lecito viene sostituito con un file . dll malevolo, che intercetta i dati inseriti? Sulla base della risposta sopra, delineate il profilo del Malware e delle sue funzionalità
- Unite tutti i punti per creare un grafico che ne rappresenti lo scopo ad alto livello.



SOSTITUZIONE FILE .DLL DANNOSO:

Se il file DLL legittimo della GINA viene sostituito con un file DLL dannoso, possono verificarsi gravi conseguenze per la sicurezza del sistema e la privacy dell'utente.

Il file dannoso potrebbe intercettare i dati inseriti dall'utente, come nome utente e password, e trasmetterli a malintenzionati.



POSSIBILI CONSEGUENZE:

- Furto di credenziali: Il file dannoso potrebbe registrare le credenziali di login digitate dall'utente, come nome utente e password. Queste informazioni potrebbero essere utilizzate per accedere illegalmente ad account personali, account aziendali o altri sistemi informatici.
- Installazione di malware: Il file dannoso potrebbe sfruttare l'accesso ottenuto per installare malware sul sistema dell'utente. Il malware potrebbe rubare dati sensibili, crittografare file per richiedere un riscatto, danneggiare il sistema operativo o svolgere altre attività dannose.
- Controllo del sistema: In casi estremi, il file dannoso potrebbe prendere il controllo completo del sistema dell'utente, consentendo ai malintenzionati di eseguire qualsiasi azione desiderata



PROFILO DEL MALWARE E FUNZIONALITÀ:

Scopo Principale:

- Rubare credenziali di accesso: Il malware mira a intercettare le credenziali di login digitate dall'utente, come nome utente e password, durante il processo di autenticazione grafica (GINA).

Funzionalità:

1. Intercettazione dei dati di login: Il malware si posiziona come componente GINA dannoso, sostituendo il file GINA legittimo del sistema.
2. Registrazione delle credenziali: Il malware registra le credenziali digitate dall'utente nel campo nome utente e password del riquadro di login di Windows.
3. Trasmissione delle credenziali: Le credenziali rubate vengono inviate a un server controllato dai malintenzionati.
4. Installazione di malware aggiuntivo: Il malware potrebbe sfruttare l'accesso ottenuto per installare altro malware sul sistema compromesso.
5. Controllo del sistema: In casi estremi, il malware potrebbe prendere il controllo completo del sistema.



MALWARE DANNOSO GINA

01	<i>Intercettazione Dati Login</i>	Attivazione, Monitoraggio e Registrazione tasti
02	<i>Registrazione Credenziali</i>	Archiviazione Locale, Trasmissione Remota(Server)
03	<i>Trasmissione Credenziali</i>	Metodo di Trasmissione e Destinazione
04	<i>Installazione Malware Aggiuntivo</i>	Download Malware, Funzionalità Aggiuntive (Keylogger, spyware)
05	<i>Controllo del Sistema</i>	Accesso Privilegiato, Attività Dannose (cancellare dati, bloccare l'accesso al sistema ecc)

PRESENTATO DA ANDREA PANICUCCI

**GRAZIE MILLE
PER
L'ATTENZIONE**

