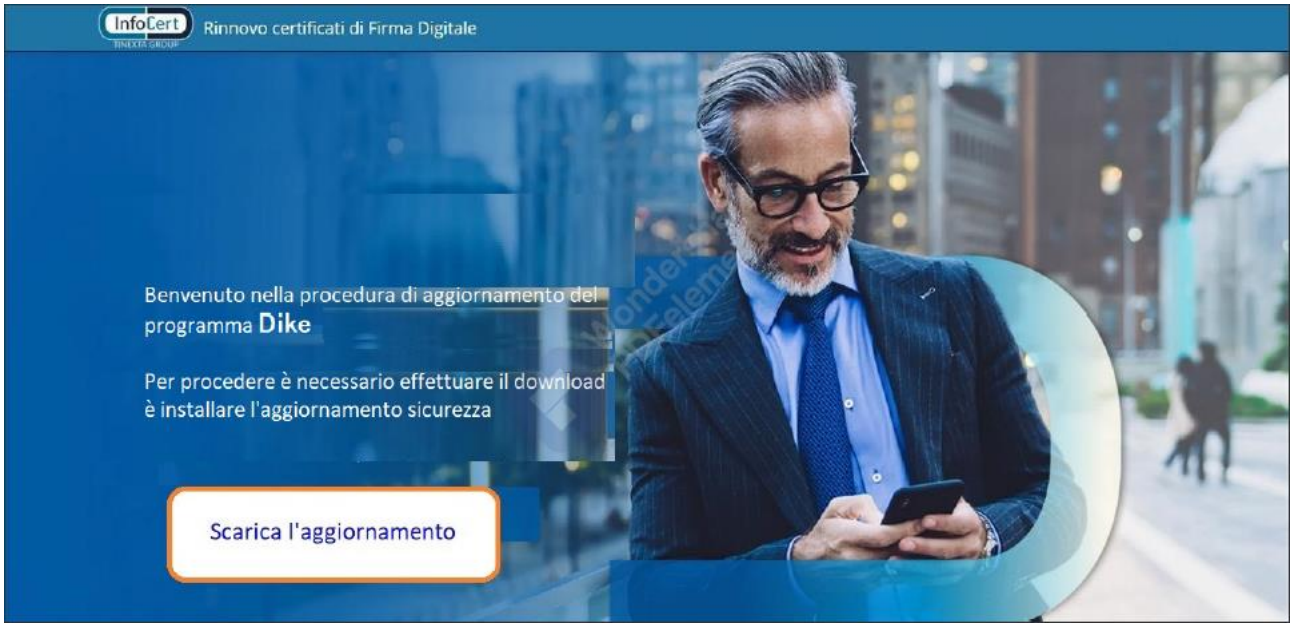
"Gentili Colleghe e Colleghi,
l'Agenzia per la Cybersicurezza nazionale ha recentemente individuato una campagna di *phishing*[1] attualmente in corso e volta alla distribuzione di un allegato ".pdf" il cui testo esorta la vittima ad effettuare quanto prima l'aggiornamento del software DIKE – noto strumento di firma digitale – tramite un apposito pacchetto di installazione ".msi" reperibile all'indirizzo web[2] presente all'interno del documento stesso.

Figura 1 – email di phishing

Figura 2 – Contenuto del file pdf



Qualora prelevato ed eseguito, il codice malevolo provvede all'installazione del software di controllo remoto legittimo *Atera Agent*, opportunamente configurato per ottenere persistenza sul sistema e monitorare il dispositivo target.

[1] E' una particolare tipologia di truffa realizzata sulla rete Internet attraverso l'inganno degli utenti. Si concretizza principalmente attraverso messaggi di posta elettronica ingannevoli.
[2] hxxps[:]//infocert-dike.firstcloudit[.]com/download/aggiornamenti/Windows/Dike_Infocert_upgrade.msi

Azioni di Mitigazione

Gli utenti e le organizzazioni possono far fronte a questa tipologia di attacchi verificando scrupolosamente le email ricevute e attivando le seguenti misure aggiuntive:

- fornire periodiche sessioni di formazione finalizzate a riconoscere il phishing;
- diffidare dalle comunicazioni inattese, prestando sempre attenzione agli URL che si intende visitare.

Si raccomanda pertanto la massima prudenza.