- **Oggetto:** CSIRT MIM - Avviso di sicurezza: diffusione del malware Qakbot del 14/09/ 2023
- **Data ricezione email:** 14/09/2023 16:53
- **Mittenti:** Noreply Ministero Istruzione - Gest. doc. - Email: noreply@istruzione.it
- **Indirizzi nel campo email 'A':** <noreply@istruzione.it>
- **Indirizzi nel campo email 'CC':**
- **Indirizzo nel campo 'Rispondi A':** <noreply@istruzione.it>

Testo email

Salve,

con la presente comunicazione il CSIRT-MIM vuole richiamare la sua attenzione riguardo la diffusione del malware denominato “Qakbot”, campagna malware veicolata tramite email.
In questa tipologia di attacco, i criminal hacker si avvalgono della disattenzione degli utenti nella speranza che aprano gli allegati di posta elettronica, con l’intento di carpire le credenziali di accesso.
Se il tentativo va buon fine, l’attaccante riesce a prendere il controllo della casella e-mail e può impersonare l’utente titolare perpetrando diversi danni sia all’Amministrazione sia all’utente stesso.
La campagna sopra descritta è stata recentemente oggetto di indagine internazionale da parte dell'FBI, un’operazione che ha portato allo smantellamento della botnet Qakbot e all'identificazione di oltre 700.000 computer infettati.
Per difendersi da questa e da altre campagne simili, che utilizzano come vettore la casella e-mail, occorre prestare particolare attenzione riguardo eventuali e-mail sospette che contengano incoerenze, anche lievi, nel corpo del messaggio o rispetto all’indirizzo del mittente.

Pertanto, qualora abbia ricevuto mail sospette o abbia aperto allegati sospetti, si consiglia di:
- Avviare una scansione antivirus completa del PC;
- Pulire la cache del browser (su Chrome: impostazioni -> nella barra superiore di ricerca inserire “Cancella dati di navigazione” -> Cancella dati di navigazione -> Selezionare “Cronologia di navigazione”, “Cookie e altri dati dei siti”, “Immagini e file memorizzati nella cache” -> Cliccare su “Cancella dati”);

In caso si tema di essere stati bersaglio di campagne malware o nel caso si siano stati cliccati allegati di dubbia affidabilità, è sempre una buona prassi richiede al proprio referente il reset della password della casella di posta e dell’utenza istituzionale.

Alcune misure di cautela per proteggersi efficacemente sono:
- Impostare la password: utilizzando una combinazione di caratteri alfanumerici e simboli per renderla più sicura;
- Attivare l'autenticazione a due fattori (MFA): Si consiglia di abilitare l'autenticazione a due fattori impostando un OTP sul proprio cellulare per rafforzare ulteriormente la sicurezza dell'account;
- Mantenere il software aggiornato: Verificare che i dispositivi privati da cui accedete a questa casella postale e tutte le applicazioni siano aggiornati con le ultime patch di sicurezza;
- Contrastare il phishing: Prestare attenzione a potenziali attacchi di phishing e i rischi che ne derivano, puntando a riconoscere e-mail o siti web sospetti;
- Eseguire Backup regolari: effettuare regolarmente il backup dei dati è importante per garantire che sia possibile ripristinarli a seguito di compromissione.

Le ricordiamo di prendere visione e di attenersi alle Politiche di Sicurezza pubblicate nell'apposita sezione dell'Area riservata del portale istituzionale: https://miur.gov.it/

CSIRT-MIM
Computer Security Incident Response Team
del Ministero dell’Istruzione e del Merito