PERCHÉ È IMPORTANTE MONITORARE IL LIVELLO DI ESPOSIZIONE DELLE CREDENZIALI

COME VENGONO COMPROMESSE LE CREDENZIALI?

PHISHING

- Tramite l'invio di e-mail camuffate da messaggi legittimi
- Ingannando gli utenti, inducendoli a rivelare le proprie credenziali
- Sfruttando l'invio di malware in grado di acquisire le credenziali

WATERING HOLES

- Prendendo di mira un sito di successo, come social media e intranet aziendali
- Inserendo uno o più malware nel codice di un sito internet normale
- Utilizzando malware che acquisiscano le credenziali dei visitatori

MALVERTISING

- Inserendo uno o più malware nelle reti che fanno pubblicità online in modo legittimo
- Creando malware che acquisiscano le credenziali dei visitatori

ATTACCHI WEB

- Sfruttando le vulnerabilità scoperte per stabilire un punto d'appoggio
- Con una scansione delle vulnerabilità degli asset aziendali che si collegano a internet
- Cercando all'interno della rete un modo per reperire le credenziali

Le password sono una soluzione del ventesimo secolo applicata a un problema attuale. Purtroppo, i nomi utente e le password sono, ancora oggi, il metodo più comune per accedere a servizi, quali reti aziendali, siti di social media e di e-commerce e molto altro ancora.

39%

Percentuale di adulti che, negli Stati Uniti, usano password identiche o molto simili per diversi servizi online

28.500

Numero medio di violazioni di dati, comprese le credenziali, segnalate da imprese con sede negli Stati Uniti

I nomi utente e le password rappresentano la chiave di accesso preferenziale per i malintenzionati. I criminali, che sanno come incunearsi tra le difese di un'azienda, possono rubare facilmente centinaia o, addirittura, migliaia di credenziali alla volta.

Il traffico criminale di credenziali rubate può fruttare decine di migliaia di dollari, sborsati dagli acquirenti, interessati all'acquisto di nomi utente e password. Quando tali credenziali vengono vendute a più acquirenti, le organizzazioni che subiscono simili violazioni possono diventare facilmente vittime di aggressioni digitali da parte di decine o, addirittura, centinaia di aggressori.

DA 1 A 8 $

Tipica gamma di prezzo delle credenziali compromesse

COSA PUÒ FARE UN MALINTENZIONATO CON LE TUE CREDENZIALI?

- Inviare spam da account di posta elettronica compromessi
- Alterare le proprietà dei siti e inserirvi contenuti dannosi
- Installare malware su sistemi compromessi
- Compromettere altri account utilizzando le medesime credenziali
- Estrarre dati sensibili (violazione dei dati)
- Furto d'identità

PROTEGGERSI DALLA COMPROMISSIONE DELLE CREDENZIALI

Anche se c'è sempre il rischio che degli aggressori riescano a compromettere i sistemi aziendali attraverso attacchi avanzati, la maggior parte delle violazioni di dati sfruttano vettori comuni, come vulnerabilità note, sistemi non aggiornati e dipendenti inconsapevoli. Le aziende possono proteggere i propri affari dai pericoli del dark web solo implementando una serie di strumenti, quali il monitoraggio dei sistemi, la prevenzione delle fughe di dati, l'autenticazione a più fattori, la formazione dei dipendenti in materia di sicurezza e molto altro ancora.