Come rompere la kill chain di un attacco per il controllo degli account

Riusciresti a riconoscere immediatamente la kill chain di un attacco informatico?

Esamina le varie fasi della **kill chain di un attacco per il controllo degli account** per sapere come bloccarla.

1

RICOGNIZIONE

Cosa aspettarsi
Violazione dei dati; furto di credenziali

COME DIFENDERSI

Implementare:

- Web Application Firewall
- Crittografia
- Controlli delle credenziali sulla base di violazioni note
- Solide policy di sicurezza

POSSIBILE REAZIONE DELL'AUTORE DELL'ATTACCO

I criminali potrebbero tentare di accedere ad un altro sito o di comprare le credenziali di accesso visto che ce ne sono miliardi disponibili sul dark web.

2

ARMAMENTO

Cosa aspettarsi
Leggero picco nel numero di accessi non riusciti

COME DIFENDERSI

Confermare se:

- Gli accessi vengono effettuati da utenti legittimi
- Il software di gestione dei bot viene adattato
- Gli endpoint di accesso sono protetti con l'MFA

POSSIBILE REAZIONE DELL'AUTORE DELL'ATTACCO

I criminali potrebbero adattare il loro software se il bot viene rilevato.

3

DELIVERY

Cosa aspettarsi
Picco di traffico; numero eccessivo di richieste di accesso

COME DIFENDERSI

Verificare:

- Controlli dei tassi delle richieste
- MFA
- Anomalie nel comportamento degli utenti
- Avanzate funzioni di rilevamento del software di gestione dei bot

POSSIBILE REAZIONE DELL'AUTORE DELL'ATTACCO

L'attacco viene fermato. La kill chain viene interrotta. Bot molto sofisticati ***potrebbero*** eludere temporaneamente il rilevamento.

4

EXPLOITATION

Cosa aspettarsi
Una singola richiesta proveniente da un utente; leggero incremento nel numero di accessi

COME DIFENDERSI

Controllare

- Anomalie nel comportamento degli utenti

POSSIBILE REAZIONE DELL'AUTORE DELL'ATTACCO

I criminali non possono agire su larga scala. Per sferrare singoli attacchi, i criminali ***potrebbero*** cercare il proprietario di un account sui social network.

5

AZIONE

Cosa aspettarsi
Picco nel numero di segnalazioni da parte di clienti che hanno subito un attacco per il controllo dell'account

COME DIFENDERSI

Monitorare:

- Continuamente il rischio per gli utenti fino alla loro disconnessione

POSSIBILE REAZIONE DELL'AUTORE DELL'ATTACCO

Il software di protezione dell'account blocca il tentativo di attacco. I criminali si arrendono.

Ecco come Akamai può aiutarti nella prevenzione del controllo degli account

Ulteriori informazioni

Akamai

@2021 Akamai Technologies | Assistenza | Data di pubblicazione: 6/21