Report Rilevamento Attacchi

Utente: Banana

TITOLO: Phishing

CATEGORIA: Attacchi basati sull’inganno umano (Ingegneria sociale)

ESITO:

Possibile attacco di tipo 'Phishing' rilevato.

DESCRIZIONE:

Il phishing è una tecnica di ingegneria sociale utilizzata da criminali informatici per indurre gli utenti a fornire volontariamente informazioni sensibili, come credenziali di accesso, numeri di carte di credito o altri dati personali. Gli attacchi di phishing si basano sull’inganno: l’attaccante si presenta come un’entità fidata, come una banca, un servizio online noto o un collega di lavoro, per ottenere la fiducia della vittima. Modalità di esecuzione: - L’utente riceve un’email, un SMS o un messaggio istantaneo che sembra provenire da una fonte legittima. - Il messaggio contiene spesso un link a un sito contraffatto, graficamente identico a quello ufficiale. - Una volta che la vittima inserisce i propri dati, questi vengono inviati direttamente al truffatore. - Esistono anche varianti più sofisticate, come il spear phishing, mirato a persone specifiche, e il vishing, condotto per telefono. Possibili conseguenze: - Accesso illegittimo a conti bancari o profili online. - Perdita di dati personali e aziendali. - Furto d’identità e danni reputazionali. - Possibilità che l’account compromesso venga usato per ulteriori truffe.

LIVELLO DI RISCHIO:

alto

CONTROMISURE:

Consigli pratici per la prevenzione: - Diffidare di messaggi che creano urgenza (“Il tuo account sarà sospeso!”, “Hai vinto un premio!”). - Verificare sempre l’indirizzo del mittente e il dominio dei link. - Non cliccare su allegati o collegamenti sospetti. - Attivare l’autenticazione a due fattori (2FA) per i propri account. - Utilizzare software antivirus e filtri antispam aggiornati.

Risposte Sì: 3 / 4

TITOLO: Supply Chain Attack

CATEGORIA: Attacchi a livello sistemico o industriale

ESITO:

Possibile attacco di tipo 'Supply Chain Attack' rilevato.

DESCRIZIONE:

Un Supply Chain Attack (attacco alla catena di fornitura) colpisce indirettamente un’organizzazione compromettendo fornitori o partner terzi. L’attaccante inserisce codice malevolo o sfrutta vulnerabilità nei software o hardware forniti da terzi.\ Modalità di esecuzione:\ - Compromissione di aggiornamenti software distribuiti da vendor legittimi.\ - Infiltrazione nei sistemi di un fornitore con accesso alla rete target.\ - Distribuzione di componenti hardware alterati.\ Possibili conseguenze:\ - Infezione di numerosi sistemi con un solo attacco.\ - Diffusione silenziosa e difficilmente rilevabile.\ - Impatto esteso a tutta l’infrastruttura aziendale o nazionale.

LIVELLO DI RISCHIO:

alto

CONTROMISURE:

Consigli pratici per la prevenzione:\ - Monitorare e valutare periodicamente i fornitori di software e hardware.\ - Applicare controlli di integrità e firma digitale sui pacchetti installati.\ - Segmentare la rete per limitare gli accessi da terze parti.\ - Effettuare audit di sicurezza su fornitori critici.

Risposte Sì: 3 / 4