certego

Vishing via Microsoft Teams

Rilevato un recente aumento dei tentativi di sfruttamento in Italia

Come prevenirlo →

SecOps Services
SECURITY OPERATIONS SERVICES

certego

Cosa sta succedendo?

Negli ultimi giorni
il nostro SecOps Team
ha rilevato un incremento
significativo di questi attacchi.

Gli attaccanti sfruttano le chiamate
per colpire direttamente
gli utenti aziendali.

SecOps Services
SECURITY OPERATIONS SERVICES

certego

Cos’è il Vishing via Teams?

È un attacco di ingegneria sociale.

I Threat Actor:

- Si fingono supporto IT o personale amministrativo
- Contattano l’utente tramite chiamata Teams
- Inducono a condividere credenziali o installare strumenti di accesso remoto

Obiettivo: ottenere il controllo delle macchine aziendali fino al Domain Controller, compromettendo l’intera organizzazione.

SecOps Services
SECURITY OPERATIONS SERVICES

certego

La dinamica tipica

1. Chiamata improvvisa su Teams
2. Segnalazione di un problema urgente che richiede un aggiornamento di sicurezza del sistema Windows
3. Richiesta di credenziali o attivazione di strumenti di accesso remoto
4. Accesso alla macchina e potenziale compromissione della rete

Un punto critico: di default, Teams consente chiamate da utenti esterni.

SecOps Services
SECURITY OPERATIONS SERVICES

certego

Attenzione alle configurazioni

- Valutare whitelist
  per consentire chiamate
  solo da fornitori noti

- Se non gestibile, bloccare i domini
  che terminano con onmicrosoft.com

  Spesso utilizzati in tenant di prova dai Threat Actor

SecOps Services
SECURITY OPERATIONS SERVICES

certego

Strumenti di accesso remoto

Gli attaccanti sfruttano tool già presenti sugli host, come soluzioni di Remote Support.

Si consiglia di:

- ! Limitarne l’utilizzo
- ! Monitorare internamente questi software

SecOps Services
SECURITY OPERATIONS SERVICES

Processi e formazione

Rafforzare le verifiche delle identità.

Fare particolare attenzione a richieste che comportano:

- Reimpostazione password
- Modifiche agli account
- Configurazioni degli host

Importante: formare gli utenti su questa modalità di attacco.

SecOps Services
SECURITY OPERATIONS SERVICES

certego

certego

PURE-PLAY

MDR