Gpi Phishing
AI POWERED PROTECTION

INSIGHT

Typosquatting e Homograph Attack: il nemico si nasconde in un solo carattere

"apple.com" non è "apple.com": come riconoscere e proteggersi dai domini-trappola

A cura del team CENANT di GPI Cyberdefence

4 novembre 2025 www.gpiphishing.com

INSIGHT

“apple.com” non è “apple.com”: come riconoscere e proteggersi dai domini-trappola

01 Il diavolo nei dettagli

Amaz0n.com. *Facbook.com*. *Poste-it.com*. A prima vista sembrano domini legittimi, e questa “prima vista” è esattamente ciò su cui conta l'attaccante. consiste nel registrare domini simili a quelli di marchi noti, sfruttando errori di battitura comuni o sostituzioni impercettibili, per attrarre utenti verso siti malevoli.

Il principio è semplice ma potente: l'utente riceve un'e-mail con un link, lo guarda velocemente, vede un dominio “familiare” e clicca. Non è una questione di ignoranza, è una questione di attenzione limitata in condizioni di stress o fretta.

02 Il livello successivo: l'IDN Homograph Attack

Se il **typosquatting** sfrutta gli errori di battitura, l'**IDN Homograph Attack** sfrutta qualcosa di più subdolo: la somiglianza visiva tra caratteri di alfabeti diversi. L'alfabeto cirillico, il greco, l'IPA latino contengono caratteri che appaiono identici a quelli latini ma hanno un codice Unicode diverso.[1]

Il dominio “apple.com”, con lettere cirilliche, è visivamente indistinguibile da “apple.com”, ma punta a un sito completamente diverso. Senza strumenti specifici, è impossibile distinguerli a occhio nudo.

03 Esempi reali

Nel 2017, un hacker ha registrato il dominio gοogle.com (con una 'G' maiuscola di un set Unicode diverso) creando una replica perfetta della homepage di Google che registrava credenziali di accesso.

La tecnica è stata usata contro PayPal, Apple, Microsoft, banche e istituzioni governative in tutto il mondo. Le varianti includono: lettere doppie (*goooogle.com*), omissioni (*gogle.com*), inversioni (*goolge.com*), sostituzioni numero/lettera (*amaz0n.com*) e caratteri Unicode ingannevoli.

> *Verificate sempre l'URL completo prima di inserire credenziali. Se il browser mostra "xn--" all'inizio del dominio, state guardando un indirizzo internazionalizzato che potrebbe essere un attacco homograph.*

04 Strategie di protezione per le aziende

04.1

Registrazione difensiva

registrare preventivamente le varianti più ovvie del proprio dominio aziendale (con e senza trattino, con TLD alternativi, con errori di battitura comuni).

04.2

Monitoraggio DNS

servizi dedicati avvisano in tempo reale quando vengono registrati domini simili al proprio — permettendo di agire prima che vengano usati in una campagna.

04.3

Formazione degli utenti

insegnare ai dipendenti a verificare sempre il dominio completo, con attenzione speciale alle e-mail ricevute, prima di inserire credenziali o dati sensibili.

RIFERIMENTI

1 IDN: *Internationalized Domain Name*, nome di dominio internazionalizzato che consente l'uso di caratteri al di fuori del set ASCII standard.

GPI PHISHING — CYBERSECURITY PLATFORM

Proteggi il tuo brand da typosquatting e homograph attack

Monitoraggio dei domini simili, alerting in tempo reale e formazione per riconoscere URL contraffatti.

Phishing
AI POWERED PROTECTION

www.gpiphishing.com