Lookalike Domains

Lookalike domains, also known as typosquatting domains or domain impersonation, are URLs that closely resemble legitimate domain names but with slight variations. These domains are often used for phishing attacks, brand abuse, or other malicious activities. In the context of attack surface management and internet scanning:

1. Definition: Lookalike domains use techniques such as character substitution, additional hyphenation, or top-level domain (TLD) variation to mimic legitimate websites.
2. Detection: ASM tools scan the internet to identify registered domains that closely resemble an organization's legitimate domains or brand names.
3. Threat types:
   - Phishing: Stealing credentials or personal information
   - Malware distribution: Infecting visitors with malicious software
   - Brand damage: Misleading customers or tarnishing reputation
   - Traffic diversion: Redirecting potential customers to competitor sites
4. Common techniques:
   - Misspellings: "goggle.com" instead of "google.com"
   - Character swaps: Using "rn" instead of "m"
   - Added words: "secure-paypal.com" instead of "paypal.com"
   - Different TLDs: "company.net" instead of "company.com"
5. Mitigation strategies:
   - Proactive registration of common misspellings
   - Monitoring and takedown services
   - User awareness training
   - Implementation of email authentication protocols (DMARC, SPF, DKIM)
6. Relevance to scanning:
   - Continuous internet-wide scans to detect new registrations
   - Analysis of SSL/TLS certificates for similar domain names
   - Monitoring of DNS records and changes

By including lookalike domain detection in attack surface management, organizations can protect their brand, prevent phishing attacks, and maintain customer trust.

Revision #1
Created 19 September 2024 15:54:43 by Admin
Updated 19 September 2024 15:56:50 by Admin