2023-04 DNSAI Bulletin on Account Take-Overs

The DNSAI has encountered multiple reports of an increase in account take-overs at retail registrars across the industry. This bulletin is intended to help registrars identify and prevent these attacks.

Issue Description

Multiple registrars have reported an increase in account take-over attacks. An account take-over is where an attacker logs into a customer account using stolen credentials, and uses that account to purchase domain names.

The attackers appear to be using email addresses and passwords that customers have re-used at other online services and were subsequently leaked online.

In these cases, the domains purchased by the attacker do not appear to follow a clear pattern so it is difficult to look for obvious abuse characteristics in the domains. Some fraudulently purchased domains appear to have been previously and legitimately registered, used, and expired. The attackers identified these domains as being used for accounts at other online services and available for registration, allowing the attackers to take over social media and other accounts or services.

The attackers are acquiring large volumes of domains (e.g., hundreds or more, in some cases), often with stolen credit card numbers and generating substantial amounts of credit card chargebacks and domain suspensions and deletes for registrars.

Identification

Compromised accounts have been identified using one more more of the following criteria:

- Large orders of domain names, or a large number of small orders for one account
- Dormant, or accounts that have been inactive for a long period of time reactivating

As well as common anti-fraud criteria:

- Accounts using multiple credit cards, or adding new cards
- Account geography not matching credit card geography

- Accounts coming from multiple IP addresses
- The same IP being used by multiple accounts
- IPs coming from VPN or cloud hosting providers

Prevention

Implementing some form of two factor authentication has been the most successful method of preventing these account take-overs, as attackers do not appear to control the email accounts or devices associated with the compromised account.

Many registrars use age-of-account as a factor in assessing the risk of a transaction, however reducing the amount of trust in older accounts has seen more of the fraudulent transactions flagged by anti-fraud systems.

Implementing warning flags in transactional systems based on the criteria for identification above can be useful for catching account takeovers and other types of fraud and abuse.