Use of Stolen Credentials

Credentials – Definitions

From Wikipedia

Information technology

Credentials in information systems are widely used to control access to information or other resources. The classic combination of a user account number or name and a secret password is a widely-used example of IT credentials. An increasing number of information systems use other forms of documentation of credentials, such as fingerprints, voice recognition, retinal scans, X.509 Public key certificate, and so on.

Cryptography

Credentials in cryptography establish the identity of a party to communication. Usually they take the form of machine-readable cryptographic keys and/or passwords. Cryptographic credentials may be self-issued, or issued by a trusted third party; in many cases the only criterion for issuance is unambiguous association of the credential with a specific, real individual or other entity. Cryptographic credentials are often designed to expire after a certain period, although this is not mandatory. An x.509 certificate is an example of a cryptographic credential.

Identification

Credentials that simply establish a person's identity are very widely used. Documentation usually consists of an identity card (sometimes a credential that is also used for other purposes, such as an automobile driver's license), a badge (often machine-readable), etc., issued by a trusted third party after some form of identity verification. Many identification documents use photographs to help ensure their association with their legitimate holders. Some also incorporate biometric information, passwords, PINs, and so on to further reduce the opportunities for fraud. Identification credentials are among the most widely counterfeited credentials.

From Dictionary.com

1. Usually, credentials. evidence of authority, status, rights, entitlement to privileges, or the like, usually in written form: Only those with the proper credentials are admitted.
2. anything that provides the basis for confidence, belief, credit, etc.

Application of the definitions for RAP Working Group

For the purposes of examining the registration abuse and the "use of stolen credentials", there are three usages that seem to apply:

1. "Identity credentials" – Credentials that establish identity (e.g. personal identification cards, stored personal information)
2. "Access credentials" – Credentials that control access to computer systems (e.g. username and password, digital certificates)
3. "Financial credentials" – Credentials that provide access to financial accounts (e.g. credit and debit cards).

Some blending of usages would apply in some cases as well. For example, the use of a stolen e-mail account to establish identity or the authority to modify access to financial credentials crosses multiple definitions.

Examination of abuses currently seen

Given the disparate nature of the uses and protections against abuse the types of credentials identified each have, it would seem prudent to examine them individually. Some commonalities may present themselves to allow for unified approaches to curbing registration abuses across all types of credentials too.

Identity Credentials

In general, stolen identity credentials allow a miscreant to assume or impinge the identity of another in order to perpetuate one of their own schemes. This can manifest itself in the use of purloined personal information to make a domain registration appear to be legitimate (e.g. false whois) or in allowing a perpetrator to assume control over access or financial credentials. The latter case can be explored in-depth in examining those other two credential types, but the former case is worth considering further.

1. Fraudsters use misappropriated identities of the actual individuals or institutions targeted by a particular scheme in conjunction with a domain registration. The fraudster wishes to make the domain name appear to be associated with the actual victim in order to make their scheme more viable to other victims, and/or their application for the domain legitimate.
2. Miscreants use identities of random, but real individuals/organizations in conjunction with a domain registration, unrelated to the actual fraud scheme. Use of real data may allow the miscreant to fool anti-fraud measures put in-place by the registrar. Victims of the actual scheme may be put at ease by the appearance of "real" verifiable domain ownership information in whois, or they may make complaints against innocent parties. The stolen identity data may well cause delays in authorities investigating the scheme, as innocent parties are scrutinized. The person who is "spoofed" in this instance may be the registrant for other domains, which may also allow the registration to get past anti-fraud measures, especially if the registrar being used is the same.
3. The miscreant uses stolen identities in conjunction with stolen financial credentials to bolster their fraud efforts when registering a domain. Including the stolen access information in whois and/or account information that matches stolen credit card data can help avoiding anti-fraud systems, as well as all the benefits mentioned above.

Access Credentials

A miscreant can do quite a bit of damage with stolen access credentials. Outside of reselling those credentials, the real value of stolen access credentials lies in what is possible to do with the systems to which those credentials provide access. Two possible attacks seem to be meaningful within the confines of "domain registration abuse" we're examining here. First, direct attacks against registrar/reseller systems using stolen access credentials for that service. Second, a perpetrator could launch an indirect attack via access credentials to other accounts.

1. A miscreant with direct access to a domain management account can make new domain registrations using funds or "credits" that account may have with the reseller or registrar. Obviously domains can be taken over, deleted, or otherwise sabotaged from such a compromised account, but those scenarios are likely outside the scope of "registration abuses". Further, a miscreant may be able to gain access to credit card information that is stored in such an account, or affect purchases with that card that directly benefit that criminal. Again, this is outside scope, as this is more of a theft problem than a domain registration issue, but it is likely a concern that could come up in discussions of this topic.
2. If a fraudster has access to an account that is used to verify identity or confirm change requests, like an e-mail account, they can either attempt to gain access/control over a domain management account, or use a domain registration verification process to register domains using someone else's account/identity. Some domain resellers may use legacy models based on the original e-mail based registration and modification system, which would allow for fraudulent domain registrations based on e-mail confirmations.
3. If a criminal has access via stolen credentials (or simply hacking) into a computer/server that is part of some automated domain registration system, they can subvert that system. With such control, new domains can be registered using the victim's automated access to registrar systems. Of course hijacking, sabotage, and other acts can be perpetuated as well, just as if the miscreant had access to an account with the registrar/reseller.

Financial Credentials

Abuses perpetrated with stolen financial credentials are fairly straightforward. The criminal can utilize those credentials to fraudulently register domains and other related resources. This is quite common practice with criminals today, with most of the domains registered in this manner being used to perpetuate other crime, fraud, and abuse. Such credentials include credit cards, debit cards, on-line banking, alternate payment systems (e.g. PayPal), ACH systems, and other various means for affecting payments for domain name transactions.

An interesting aspect for domain name registration via stolen financial credentials versus other types of fraud done via stolen financial credentials is the need to establish domain ownership information (whois and/or account) and domain deployment characteristics (nameservers) at the time of registration. This allows for some unique techniques to expose fraudulent registrations via stolen financial credentials.

Observed abuses

Use of stolen financial credentials would seem, at first glance, to be the primary abuse seen today. Thousands of domains are registered daily using such credentials to perpetuate all sorts of criminal and abusive schemes. However, there has been a shift of late in the way criminals are amassing infrastructure resources, with more emphasis being placed on obtaining access credentials to infrastructure elements. Some level of stolen identity credential abuse co-exists with these other abuses as well, so all three areas deem at least some consideration.

Roles for policy and other industry-wide approaches

These three types of uses of stolen credentials present different opportunities for mitigation efforts, both at the individual registrar/reseller level and across the industry. Some registrars and resellers see fairly frequent abuse, especially of stolen financial credentials, while others do not. There are opportunities for dissemination of best practices, plus potential for "minimum standards" for dealing with various types of abuse in this arena. Further, given the unique nature of domain names requiring access to a shared data system (the zone files) with detailed ownership/contact data in order to function and be in compliance, there may be ways to share information about fraudulent activities occurring at some registrars/resellers to curb those abuses across the industry. No formal system or policy for the latter currently exists.

Free-market forces have largely determined how different registrars and their resellers respond to these issues. There is a strong argument for allowing competition to dictate many of these responses, as there is continuous innovation in these areas, and many market participants compete on these features. Against that, is an apparent free-market failure, in which registrars/resellers who appear to be fairly weak in practices to prevent such fraudulent registrations are generally not being penalized. The large numbers of fraudulent domains obtained through the methods discussed previously with infrequent sanctions evidences this. So the question becomes one of balance, as is often the case in such industry issues.

Complicating these issues are the large number of business models currently employed by domain registration companies. "Retail" registrars who sell direct to individuals and businesses will most often process transactions with credit cards or alternate payment services. There are many other models out there however, including large "corporate" registrars that establish credit accounts, multi-level resellers, internal operations that register names on their own accounts, and more approaches seemingly daily. This makes it more difficult to find solutions that cover all players well. Perhaps concentrating on the areas that appear to have the highest incident of abuses would be prudent.

Models from other industries

Placeholder for information on how other industries deal with similar abuses. Examples could include payment card industry (PCI), healthcare (HIPPA), law firms, retailers and merchant risk, telecom and ISPs, etc.

Addressing use of Stolen Identity Credentials

Placeholder for now
Idea – regular dissemination of best practices for identifying stolen identities
Idea – provide policy framework to ALLOW information sharing between registrars on fraudulent domain registrations and registration attempts.
Idea – create information sharing clearinghouse to facilitate information sharing between registrars (and resellers) on fraudulent domain registrations and registration attempts. Data elements could include some aspects of stolen identity credentials.

Addressing use of Stolen Access Credentials

Placeholder for now
Idea – regular dissemination of best practices for protecting account access
Idea – adoption of minimum standards for protecting registrant login credentials (password aging, strong passwords, etc.)
Idea – codify registrant rights/responsibilities for account access security management – is there a potential for liability limitation for registrants vs. registrars vs. resellers?

Addressing use of Stolen Financial Credentials

Placeholder for now
Idea – regular dissemination of best practices for detecting stolen financial credentials
Idea – adoption of minimum standards for registrars/resellers who accept credit cards, alternative payments, and bank drafts/transfers. Look to PCI
Idea – provide policy framework to ALLOW information sharing between registrars on fraudulent domain registrations and registration attempts.
Idea – create information sharing clearinghouse to facilitate information sharing between registrars (and resellers) on fraudulent domain registrations and registration attempts. Data elements could include aspects of domain registrations including nameservers and contact details. Sharing of stolen credential information itself is highly problematic and would require a specialized third party if even possible. Locations of fraudulent registration attempts (IP addresses) may be feasible in some venues.