SAC 40
Measures to Protect Domain Registration Services Against Exploitation or Misuse

A Report from the ICANN
Security and Stability
Advisory Committee
(SSAC)
19 August 2009

Preface

This is a report by the Security and Stability Advisory Committee (SSAC) describing measures to protect registration services against misuse. The SSAC advises the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems. This includes operational matters (e.g., matters pertaining to the correct and reliable operation of the root name system), administrative matters (e.g., matters pertaining to address allocation and Internet number assignment), and registration matters (e.g., matters pertaining to registry and registrar services such as WHOIS). SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. The SSAC has no official authority to regulate, enforce or adjudicate. Those functions belong to others, and the advice offered here should be evaluated on its merits.

The contributors to this report, reference to the committee members' biographies and statements of interest, and committee members' objections to the findings or recommendations in this report, are at end of this report.

Introduction

Attacks against domain name registration accounts and malicious reconfiguration of Domain Name System (DNS) records are damaging security events. Incidents occurring over the past year demonstrate that the DNS and domain registration account access continue to be an attractive target of attackers. Activities resulting from unauthorized modification of information associated with a domain name registration, including malicious alteration of DNS configuration information for the purpose of using the DNS to direct traffic to a destination other than the intended host, *even temporarily*, can severely disrupt business operations and can cause financial and reputational harm.

Neither domain name registration account nor name resolution service hijacking are new attack vectors. In past reports and advisories, the ICANN Security and Stability Advisory Committee (SSAC) has studied issues that affect domain name registrations and DNS operation from a user (registrar customer, i.e., a registrant) perspective. We have identified situations where registrants have not acted to sufficiently protect domain names (e.g., failure to renew a registration or maintain accurate contact information). We have recommended measures that registrants can take to protect their business and operational interests with respect to domain names they register and manage.

This report relates recent incidents involving unauthorized access to domain registration accounts. The purpose of relating such events is not to embarrass or criticize registrars, resellers, *or* registrants. We do so because analysis of security events always reveals *something* each party could have done to prevent the event or its severity.

In this report, we call attention to certain high profile incidents involving domain name registration accounts to determine if there are common causes among the events that might reveal measures to reduce or mitigate certain threats and vulnerabilities. The report examines the incidents in sufficient detail to identify how accounts were compromised, the actions attackers performed once they had gained control of the account, and the consequences. The descriptions were derived from publicly available news stories and articles. These were complemented with information obtained through interviews with targeted registrars and their customers. We have intentionally omitted information identified by targeted parties as sensitive.

The report presents security measures used in other Internet business segments (e.g., financials, durable goods merchants) to protect customers from similar vulnerabilities. The report identifies practices registrars can share with customers so registrar and customer can jointly protect registered domains against exploitation or misuse, and discusses methods of raising awareness among registrants of the risks relating to even a temporary loss of control over domain names and associated DNS configurations. While certain registrars do differentiate themselves by offering high levels of service, this report seeks to encourage more registrars to consider whether opportunities exist to provide additional protection from attacks against domain registration accounts. The report also seeks to encourage registrars to consider emphasizing registration security measures as a way to differentiate their services in a highly competitive market.

What motivated this work?

Several high profile incidents involving unauthorized access to domain name accounts have occurred in the past twelve months. This flurry of attacks shares certain traits with those that motivated prior SSAC studies on domain name hijacking[1] and the unanticipated consequences associated with the non-renewal of domain names.[2,3] Some incidents are malicious acts against registrar staff and registration services (e.g., web-enabled domain account administration tools). Others employ social engineering and may have exploited routine and anticipated correspondence from a registrar to its customers.[4]

SSAC considered a series of incidents occurring from May 2008 through April 2009. From these, we identified vulnerabilities as well as policies and practices (business and operational) that were exploited to see whether a common thread might emerge. We noted the following as we studied these incidents.

(1) Many organizations have domain name registration accounts that contain high-value or business-critical names, domain names that could be as valuable to the organization as any tangible asset, trademark or intellectual property right the organization possesses.

(2) Many registration service providers operate with consumer-focused service objectives; i.e., the registration service is highly automated and focused on serving very large numbers of registrants at a high rate of transaction. Automation is extremely important in any business endeavor that attempts to provide service in a timely and scalable manner. Our study revealed that attackers have familiarized themselves with registrar behavior and will exploit certain aspects of automation; for example, knowing that electronic mail is the preferred method of notifying registrants of contact and configuration changes, renewals, etc., attackers often attempt to disrupt delivery to email addresses by modifying DNS configurations.

(3) Among the incidents we studied, the victims were frequently customers with business critical domain accounts operated by registration service providers with consumer-focused service objectives. In some cases, customers did not adequately assess the risk associated with the possible loss of control or access to their domain registration account until they were victimized; in other cases, the internal policies and monitoring activities in place prior to the incident were not sufficient to detect or block the attack.

---

[1] SAC007, Domain Name Hijacking Report, http://www.icann.org/announcements/hijacking-report-12jul05.pdf

[2] SAC011, Problems caused by non-renewal of a domain name associated with a DNS name server, http://www.icann.org/committees/security/renewal-nameserver-07jul06.pdf

[3] SAC010, Renewal Considerations for Domain Name Registrants, http://www.icann.org/committees/security/renewal-advisory-29jun06.pdf

[4] SAC028, Advisory on Registrar Impersonation Phishing Attacks (26 May 2008), http://www.icann.org/committees/security/sac028.pdf

Based on size and business reputation, some of the victims would seem to be sufficiently sophisticated with respect to internal security administration and risk management to recognize the asset value of their domain names, yet they did not appear to have included domain names in their risk assessment. Other victims, especially small and medium sized organizations or individuals, may not have fully understood the importance of their domains until such time as there is an issue. This is consistent with behavior regarding other risk areas. In many situations, an organization may recognize the value or business-critical nature of an asset, but may not provide adequate measures to protect that asset against threats until an incident occurs.

From a security perspective, registrants who believe their domain names are critical assets ought to make security an important selection criterion when choosing a registration service provider. The incidents SSAC studied reveal that registrants either do not understand the range of security services available from registration service providers or they do not appreciate that there *is* a range of security services to choose from. One registrar commented to SSAC that registrants believe registration services are pretty much the same, concluding that since all registrars sell the same product sourced from the same registries, the security measures the registrars provide is presumably the same. The incidents we describe in the next section assisted SSAC in concluding that differences among registration service providers are not well understood outside the domain name community.

Attacks against domain name registration accounts

While a comprehensive list of events related to this topic is beyond the scope of this report, we present summaries of certain high profile attacks against domain name registration accounts to provide context for subsequent discussion and analysis. While the summaries quote liberally from public sources, SSAC also consulted with registrars involved in the incidents as well as organizations victimized by the attackers and gratefully acknowledges their cooperation.

Comcast (May 2008)

Comcast is the largest cable television provider, second largest Internet service provider, and among the largest residential telephone providers in the United States.[5] At the time of the incident, Comcast had registered approximately 200 domains through Network Solutions, Inc.[6] On 28 May 2008, attackers gained access to Comcast's domain registration account at Network Solutions. Initially, the attackers maliciously altered certain contact information, presumably for notoriety's sake.[7] Comcast staff received email notification of the change and restored the correct information.

[5] Comcast entry at en.wikipedia.org/wiki/Comcast
[6] Comcast.net Domain Hijacked at Network Solutions, http://www.domainnamenews.com/featured/comcastnet-domain-hijacked-at-network-solutions/1619
[7] How was Comcast.net hacked?, http://blogs.zdnet.com/security/?p=1224

The attackers claim that they called a Comcast administrator to describe the vulnerability and their exploit. The attackers claim to have used a combination of social engineering and a technical hack to gain access to the domain registration account.[8] Network Solutions reported that there was no security breach or social engineering of their staff and that the DNS changes were made by someone with the customer's login information.[9] In a *Wired Magazine* article, the attackers claim that a Comcast manager "scoffed at their claim and hung up on them."[10] The attackers accessed the account a second time. This time, they altered the DNS configuration of the domain comcast.net and redirected traffic to a defacement web site hosted on servers they had compromised. However, Comcast staff did not receive change notifications via email from Network Solutions. Both the technical and administrative contacts recorded in the domain registration record used email addresses assigned from Comcast registered domains. By altering the DNS configuration, the attackers had effectively prevented Comcast staff from receiving email notifications of account activity: they simply could not be delivered. The attack was effective and made headlines worldwide. According to *Wired Magazine,* "The attack began at around 11:00 p.m. Eastern Time and the hackers owned Comcast.net until 4:00 or 5:00 a.m. Even when Comcast regained control, it took hours longer for the change to fully propagate through the DNS, leaving some customers without webmail access as late as 11:30 Thursday morning." A 29 May 2008 article in *The Register* comments that "the attack shows that old-fashioned account compromises are also sufficient to alter substantial amounts of web traffic".[11]

CheckFree (December 2008)

CheckFree (now FIServ) is the leading global provider of information management and electronic commerce systems for the financial services industry.[12] On December 2, 2008, an attacker gained control of CheckFree's domain registration account at Network Solutions.[13] The attacker modified the DNS configuration of several domains, including checkfree.com and mycheckfree.com. Customers who attempted to log into accounts to make use of online bill payment services were redirected to an impersonation web server in the Ukraine that attempted to install malicious code that contained an Adobe Reader exploit.[14] CheckFree restored the correct DNS configuration within eight hours of the attack, but as in the case of other similar incidents, propagation of the changes throughout the global DNS infrastructure took hours longer.[15]

---

[8] Comcast.net name hijacked, http://www.internetidentity.com/2008/June-2008.html

[9] Comcast account access issue – clarification, http://blog.networksolutions.com/2008/comcast-account-access-issue-clarification/

[10] Comcast Hijackers Say They Warned the Company First, http://blog.wired.com/27bstroke6/2008/05/comcast-hijacke.html

[11] Potty-mouthed hackers steal comcast.net keys, go for a spin, http://www.theregister.co.uk/2008/05/29/comcast_domain_hijacked/

[12] FIServ, http://en.wikipedia.org/wiki/Fiserv

[13] DNS attack hijacks payment website, http://www.techworld.com/security/news/index.cfm?newsid=107959

[14] Network Solutions phishing attack preceded CheckFree domain takeover, http://*www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9122722*

[15] http://www.internetidentity.com/2008/Nov-Dec-2008-FIN.html#cf

The "Security Fix" blog of The *Washington Post* noted that the attacker accessed the account by using the correct login information. In the same article, Network Solutions emphasized that the attacker did not breach its systems to obtain the login credentials.[16] It remains unclear (or undisclosed) exactly how the attacker gained the user account and credentials.

ICANN, Photobucket, RedTube (June 2008)

On 26 June 2008, ICANN itself was victimized by a group of hackers who gained unauthorized access to ICANN's domain registration account at Register.com. According to an ICANN press release, the attack was "sophisticated, combining both social and technological techniques."[17] According to ICANN's director of IT, attackers altered the DNS configurations of several domains – icann.net, iana-servers.com, icann.com, internetassignednumbersauthority.com and iana.com – so that visitor traffic was routed to defacement web site published at free web hosting accounts operated by Atspace.com. Speculation that the attack was politically motivated was based on the timing of the incident (outset of the ICANN Paris meeting where public discussions regarding new GTLDs were held) and the defacement message itself. ICANN IT staff detected the DNS changes and Register.com restored the correct configuration information shortly after being notified by ICANN. However, as was the case in the Comcast incident, the malicious DNS configuration information remained in the global DNS for an estimated 24-48 hours[18] while corrected information propagated worldwide.

The hacker group that claimed responsibility for the ICANN attack used similar tactics and the same free web-hosting provider in subsequent attacks. Photobucket is an image hosting, video hosting, slideshow and photo sharing website acquired by Fox Interactive Media in 2007.[19] On 18 June 2008, the same hacker group claimed responsibility for an attack against Photobucket that resulted in a service interruption to Photobucket users.[20] The group perpetrated yet another defacement attack on 7 February 2009 against the adult material hosting site, RedTube.[21] ,[22]

DomainZ (April 2009)

DomainZ (Domainz.net.nz) is a New Zealand based MelbourneIT subsidiary company and registrar. On 21 April 2009, notoriety-seekers used a structured query language

---

[16] Digging Deeper into the CheckFree attack, http://voices.washingtonpost.com/securityfix/2008/12/digging_deeper_into_the_checkf.html

[17] ICANN Response to Recent Security Threats, http://www.icann.org/en/announcements/announcement-03jul08-en.htm

[18] Turkish criminal hackers hijack ICANN sites, http://news.cnet.com/8301-10789_3-9980713-57.html

[19] Photobucket, http://en.wikipedia.org/wiki/Photobucket

[20] Photobucket's DNS records hijacked by Turkish hacking group, http://blogs.zdnet.com/security/?p=1285

[21] Popular porn site attacked by prudes, http://www.securecomputing.net.au/News/102818,popular-porn-site-hacked-by-prudes.aspx

[22] Turkish Hackers Take Out Top Porn Site, http://www.darkreading.com/security/perimeter/showArticle.jhtml;jsessionid=FV31FLACFRJQYQSNDLPSKH0CJUNN2JVN?articleID=208803672&subSection=Security

(SQL) injection attack on a password retrieval page at DomainZ to collect the account credentials of several high profile registrants, including Coca-Cola, Fanta, F-secure, HSBC, Microsoft, Sony and Xerox. The attackers modified the DNS configuration records of the domains registered under .CO.NZ to point to name servers registered under a .INFO domain **(**turkguvenligi.info). These servers hosted unauthorized zone information that resolved the hacked domains to defacement web sites hosted by the attackers. Certain visitor traffic landed at malicious web pages that targeted the brand name (e.g., Microsoft); other traffic was redirected to political protest pages.

What do these incidents reveal?

The similarities among the Comcast, ICANN, Photobucket and RedTube attacks illustrate that registration account attackers are of a similar breed to web, file transfer, and other Internet applications in the following manner: once a vulnerability is successfully exploited in the field, attackers will share the exploit and scan targets for the same or similarly vulnerable targets.

SSAC notes the following from these incidents.

For some registrars:

1. All an attacker needs to gain control of an organization's entire domain name portfolio (and to hamper authorized access to that portfolio) is a user account and password.

2. Attackers need only guess, phish, or apply social engineering techniques on a single point of contact to gain control of a domain registration account.

3. Attackers scan domain account registration and administration portals for web application vulnerabilities (e.g., SQL injection). A successful exploit of vulnerable application code can result in the disclosure of account credentials for many domain accounts.

4. Email is the preferred and often the only method by which some registrars attempt to notify a registrant of account activity. (We discuss additional contact methods in later sections).

5. Attackers can block delivery of email notifications to targeted registrants by altering DNS configuration information so that email notifications will not be to any recipient in the domains the attacker controls through a compromised account (e.g., registrant's identified administrative or technical contact email addresses hosted in the domain).

6. Access to and the ability to modify contact and DNS configuration information for all the domains in a registration account is commonly granted through a single user account and password.

7. Even when unauthorized modification of DNS information is discovered quickly, the process of restoring DNS information to correct for a malicious configuration can be a lengthy one that is inherent in the distributed nature of the DNS and related to time to live (TTL) values.

Customers are unfamiliar with registration protection measures

Some registrars are good at securing their business and protecting their customers. They apply best practices for securing web applications, name and hosting servers. They monitor systems and accounts for suspicious activities. Registrar support staff responds to abuse or criminal complaints efficiently. However, in an industry as broad as domain registration services, as is the case with any class of e-merchant or online business, it is inevitable that some registrars may prove vulnerable to known attack vectors. Others, even the best, may prove vulnerable to attacks that were not considered in a security audit or that have never been seen before.

From the incidents discussed in this report (and other similar incidents cited in SAC012 and occurring since its publication), it is clear that registrar processes have been and continue to be exploited by attackers. Given the size and diversity of the industry, this is not unusual. Registrars have been and will continue to be targets for attackers. *Just as customers of financial institutions may be victimized by attacks against an online banking portal, so may domain name registrants be victimized by attacks against registrar domain administration pages.*

It is ultimately the responsibility of the registrant to assess the risk of attack against domain names and DNS configuration and to choose a registration service that reduces the registrant's exposure to attack to an acceptable degree. However, registrars generally do not call attention to the protective measures they offer, and absent methods to compare registration security services, customers may erroneously conclude that all registrars are the same with respect to security, and either choose poorly or indifferently.

Registrars have different target markets and service models

With these in mind, SSAC considered the broad array of domain name registration services and determined that domain name registration is largely supported through two service models.

One popular service model offers domain name registration services at modest to low prices. Service delivery is highly automated and designed with an emphasis on processing transactions quickly, in high volume, in a consistent and repeatable manner that often minimizes opportunities for human error. Correspondence with customers is typically supported through email messages that deliver notifications or convey simple (often, step-by-step) instructions to guide customers through an obligatory process (for example, an annual WHOIS accuracy review). Automated trouble reporting through a ticketing system is common. Generally, automation seems to trump human involvement; in most cases, human intervention is typically sought by customers when automation does not perform as expected or understood, or when the customer has a problem that automated processes cannot resolve or an incident to report. Common, observable

security measures to protect domain accounts and DNS configuration against abuse typically include secure sockets layer (SSL)-protected domain account login and domain portfolio administration, email notification when changes are made to the DNS or contact information associated with the account, privacy services (protected or delegated WHOIS services as discussed in SAC023[23]), and domain transfer protection (registrar lock, auth (authorization) code confirmation between losing and acquiring registrar).[24]

A second registration service model offers protective measures to meet the needs of customers who place a high value on their domain names, consider their domain names and online presence to be business-critical, or recognize that their business or brands may be highly-targeted for abuse or criminal activities. These customers recognize threats to domain names and want to minimize or mitigate the risk of loss, configuration error, alteration of contact or DNS configuration information, or misuse of their domains, and they have gathered enough information to make an informed decision to seek out particular registrars who satisfy such requirements. Such registrars provide security measures to safeguard against the non renewal of the customer's domain names due to technical errors or oversight, to protect the customer from domain name hijacking through unauthorized modification of registration records, and to prevent unauthorized, malicious DNS configuration. The business model for these registrars is focused on handling individual transactions with a very low probability of error. The registrar caters to customers who place a premium on domain portfolio protection and are willing to pay a premium for human assistance (in particular, assistance by an account specialist assigned to the customer). Customers may, for example, want the security a verbal or written confirmation from the customer's authorized contact prior to executing a change request and real-time monitoring of DNS configuration and name resolution services from registrars.

Typically, the above-mentioned measures are part of a broader package that emphasizes brand equity protection. Brand equity protection measures seek to mitigate risks including trademark abuse (i.e., unauthorized use of a trademark or brand to attract Internet users to a web site other than the trademark/brand holder), domain registrations that target the brand holder (visually similar, "homographic" domains used for phishing or fraud attacks), and revenue or traffic diversion, backordering (efforts to register domains on behalf of a customer that are already registered by other parties should they become available again), and defensive registrations (registering a trademark or name in all top level domains).

Who needs protection from domain account and DNS hijacking?

Strong protective measures against malicious alteration of domain account or DNS configuration information are typically familiar to and sought after by organizations that have significant investments in domain portfolios or brand equity concerns and the means

[23] SAC023, Is the WHOIS Service a Source for email Addresses for Spammers? http://www.icann.org/en/committees/security/sac023.pdf

[24] Certain registrars implement anti-abuse and security measures to protect internal (business-critical) systems, processes and databases. These are generally transparent to a registrar's customers.

and willingness to pay to protect their brands. However, *registrants should not conclude that only companies with brands or intellectual property to protect need protection from domain account hijacking or malicious alternation of DNS configuration information*. Many organizations that live or die by their online presences may not use domain names that are associated with brand(s). Still others could easily do business under any of the domain names they might register. Such organizations would nonetheless suffer harm or financial loss if the names they were to assign to their web, mail and other Internet services did not resolve to Internet Protocol (IP) addresses where their organizations hosted these services.

Given that certain organizations *would* benefit by choosing registration services that would meaningfully reduce the risk associated with loss of a domain name(s) or malicious alteration of DNS configuration information, we sought to identify possible reasons why such organizations might choose a registrar for reasons other than security measures. Some possible reasons follow:

Perceived cost: In some cases, an organization assumes or incorrectly concludes that the cost of registering domains through a registrar that offers strong protective measures against domain account and DNS hijacking is prohibitive.

Awareness: Certain customers would be willing to pay for strong protective measures against domain account and DNS hijacking but are unaware that such services exist.

Bad intelligence: In some cases, an organization has concluded from the limited information available that all registrars have similar protective measures.

"Your service bundle is a poor fit for my organization": In some cases, an organization would be willing to pay for certain strong protective measures against domain account and DNS hijacking, but unwilling or unable to pay for the services certain registrars (are perceived to) bundle, e.g., strong measures plus brand equity protection.

Some additional questions are worth considering in this context:

Are only organizations that seek to protect their brands interested in stronger registration protective measures?

No. Many organizations must balance the desire to protect not only their brands but also their online presence against the cost of protection. Strong registration protective measures are frequently offered as a complement to brand equity protection. Strong registration protective measures, perhaps offered in addition to basic registration services – as an opt-in service or "for fee" or both – could make desirable security features accessible to organizations that are motivated to invest in security measures to reduce the potential for loss of availability resulting from exploitation or misuse.

Should organizations other than those with brand concerns consider domain names when they assess risk and manage assets?

Yes. SSAC reports have explained the adverse effects registrants face when domain names are hijacked, including financial loss, embarrassment and reputational harm. [25] SSAC reports also explain the issues related to non-renewal of domain names and the problems that can be caused by non-renewal of a domain name associated with a DNS name server.[26] In particular, SSAC notes in SAC010 that "domain names should be regarded as assets that have a marketable value, either through a brokered or direct sale, or as a means of generating recurring revenue" and that "Registrants who do not renew registered domain names, voluntarily or unintentionally, should be aware that every domain name is potentially of value to some … and that new registrants may use a lapsed domain name in ways that prove harmful to the former registrant."[27]

What protective measures could be offered to organizations that treat domain names as assets to help them manage risk and mitigate threats against their investments in and dependence upon domain names?

Certain measures used in other Internet business segments (e.g., financials, durable goods e-merchants) could be usefully and practically applied to protect registration services. Before considering specific measures, and for the benefit of registrants in particular, it is worth re-examining first principles: specifically how do asset, provisioning and risk management frameworks used by large organizations apply to domain name registrations? Why consider a domain name registration an asset?

Prior SSAC reports explain that a domain name is an identity by which an entity – a merchant, a financial or educational institution, a for- or not-for-profit business or enterprise, an individual or product – is known or conducts business on the Internet. It can be the same name a corporation registers as its DBA (doing business as), the name of a celebrity, author, political figure or other personality. Individuals and organizations alike treat names (brands, service marks, trademarks) in the physical world as assets and take measures to protect them against misuse (articles of incorporation, patents, copyrights, etc.). A domain name often is the same as an organization's brands, service marks, trademarks and thus registrants should take measures to protect such names not merely by registering them but by protecting them against exploitation or misuse. Domain name registration assures the global uniqueness of a domain and binds the domain to a registrant for as long as the registrant continues to pay renewal fees for a registration and meets contractual obligations (e.g., acceptable use, registration accuracy). It is thus equivalent to other network management disciplines such as asset, risk and provisioning.

---

[25] SAC007: Domain Name Hijacking Report (12 July 2005) http://www.icann.org/announcements/hijacking-report-12jul05.pdf

[26] SAC011: Problems caused by the non-renewal of a domain name associated with a DNS Name Server (7 July 2006) http://www.icann.org/en/committees/security/renewal-nameserver-07jul06.pdf

[27] SAC010: Renewal Considerations for Domain Name Registrants (29 June 2006) http://www.icann.org/committees/security/renewal-advisory-29jun06.pdf

Domain names also are user-friendly identifiers that can be resolved using the DNS to determine the Internet addresses of hosts that provide services for that domain (web, mail, social networks, voice…). The operational value of the domain – specifically, the assurance that name resolution is highly available and that names in a domain resolve as intended – is of immeasurable importance to most organizations.

For example, in the context of an asset and risk management program, it is possible to:

- Identify the value of an asset (tangible or intangible);
- List the ways in which that value is threatened (loss, theft, misuse);
- Determine how the threat can be realized, i.e., what makes the domain name vulnerable to attack or exploitation?
- Determine the probability or risk that each threat poses;
- Determine how the risk can be mitigated or reduced;
- Determine the cost of mitigating or reducing the risk to an acceptable level of risk and cost; and
- Determine the appropriate budget and implement risk mitigation or reduction.

If a domain name is an asset, then it demands the same rigor as other inventoried, valued, or sensitive assets. Considered in this light, domain name registration management appears to share many characteristics of provisioning management in large scale networks. For example, the primary operations in provisioning and in domain name registration are {add, drop, change}. Best practices applied in provisioning management seek to assure that these operations are performed in proper sequence, by authorized parties, in a timely and auditable manner, with low probability of omission, intrusion or error. Such best practices should extend to domain name registration management and registration services should seek to satisfy similar best practices.

The security measures that protect domain name registrations should be as important to an organization as the security measures an organization provides for intranet, remote database, and other application access that an organization deems business-critical. To minimize the likelihood of omission, intrusion or error in domain name registration management, customers who assign meaningful asset value to domain name registrations should seek authentication, authorization, and auditing services that approximate the same service they implement for other business-critical applications. Certain of these measures can be implemented by the customer. Others could be incorporated into registration services by registrars who determine that providing additional security measures offers a way to differentiate them in a highly competitive market. We consider these in some detail in the following sections.

Measures to prevent domain account and DNS hijacking

In this section we describe measures that certain registrars offer today as part of a broader set of services, often in conjunction with online reputation (brand equity) protection. Next, we describe measures registrars could offer that parties interviewed during SSAC's consideration of the 2008 incidents identified as desirable or essential. Finally, we

consider measures that large enterprises use to secure remote application access as well as measures financial institutions and e-merchants provide to protect customer accounts. Whether offered as individual opt-in services or as a service bundle, these measures would improve domain registration account security for customers that are motivated to and willing to invest in protective measures to reduce the risk of domain account exploitation or misuse. Registrars are encouraged to consider whether inclusion of these measures creates opportunities or as a means to differentiate them in a competitive market.

Customers (registrants) play a critical role in protecting domain names. In this section we describe briefly certain complementary measures that customers can and should take to (a) secure their roles in registrant-registrar work flows associated with domain registration creation and renewal and (b) secure contact and configuration information maintenance and change processes. Registrars can recommend such measures via existing or new frequently asked questions (FAQs) or other means to customers who hold critically important domain portfolios. For example, registrars are encouraged to make this report known to and available to customers and to encourage customers to review this report and implement measures they deem necessary to reduce or mitigate those risks they feel most seriously threaten their domain name portfolios.

SSAC believes that a service offering that caters to domain registration protection has a greater adoption potential and can be more comprehensive than the sum of initiatives and independent implementations of small and medium-sized organizations. We base this assertion on the observed success of Unified Threat Management (UTM) security devices: security systems that bundle firewall, anti-spam, anti-virus, and other security services. These have had greater penetration and more market success in the small and medium business (SMB) segments than best of breed combinations of security systems that offer one security feature. We believe that offering additional security services can be as influential in domain registration for SMBs as UTM has proved to be.

Protecting access to domain portfolio

The measures described in this section are intended to protect against unauthorized access to the customer's domain name account via a registrar or reseller's online (web) user interface or helpdesk, and customer care telephone services.

Registration verification. A registration model that is optimized for high volume transaction rates and rapid provisioning of domain names often is not optimized to verify that the registrant is who he claims to be and that no fraud or crime is being committed during payment. Antiphishing studies,[28,29] experience with combating botnets (Srizbi, Conficker), and fast flux attack networks illustrate that domain registration accounts are a key resource for criminal activities and will continue to be so. Verification of the point of contact information submitted by the registrant at registration and each time contact

[28] APWG Phishing Activity Trends Report, 2nd Half 2008, http://www.antiphishing.org/reports/apwg_report_H2_2008.pdf

[29] Global Phishing Survey: Domain Name Use and Trends in 2H2008 http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey2H2008.pdf

information is modified can reduce impersonation and domain abuse. Registrars are encouraged to consider offering email registration verification; domain registration is completed only when the registrant confirms his email address by visiting a hyperlink embedded in an activation email the registrar sends. As an added measure, certain financial institutions will call the telephone number a customer submits rather than use email. The company provides a confirmation number over the phone, which the customer types into a web form to activate an account or authorize a transaction. SSAC acknowledges that a measure of this kind adds delay to processing of a registration and delivery of a product (the registration and name resolution of the registered domain name), but registrars are encouraged to weigh this against the value of reducing abuse not only for the customer but the Internet community at large. An added benefit is that registrars who are visibly proactive in securing the Internet's name system accrue a positive reputation and are typically recommended by security professionals and business colleagues over others that are less so.

Improve password-based authentication system. The predominant authentication method among registrars is a simple username and password. Registrars are not obligated to impose minimum length, maximum lifetime or complexity checks on passwords and may not protect against brute-force guessing attacks by limiting the number of incorrect login attempts. Commonly accepted best security practices recommend that these measures should be present in any password based authentication system.

System Registration. E-merchants and financial institutions now complement improved password systems by allowing a customer to register the personal computer (PC) or IP address from which he will administer an account.

Multi-factor authentication. E-merchants, financial institutions and even online (role-playing) game operators offer customers the option of adding a hardware token authenticator as a second *factor* for verifying the customer's identity during account login. The token adds "something you have" to the "something you know" information a password represents. This two-factor authentication makes it more difficult for an attacker to break into a domain account: even if the attacker guesses or obtains the account login and password, he must also gain possession of the token. Numerous implementations of two-factor authentication exist today, and the technology scales to very large populations of customers. SSAC notes that VeriSign has submitted a proposal for a Registry-Registrar Two-Factor Authentication Service through ICANN's Registry Services Evaluation Process (RSEP). The proposal requests that "the username and passwords currently used to process update, transfer and/or deletion requests will be augmented with dynamic pass codes" as a voluntary optional service for registrars.[30] Phase 1 of VeriSign's proposed rollout would add two-factor authentication between registry and registrar. A second phase would make this service available for requests from a registrant to their registrar, and including the one-time-password in the extensible provisioning protocol (EPP) transaction from the registrar to the registry. SSAC encourages registrars to review this proposal and consider the benefits they can gain by participating. In addition to considering two-factor authentication as described here,

[30] VeriSign Registry-Registrar Two-Factor Authentication Service http://www.icann.org/en/registries/rsep/

SSAC recommends that registrars also take into account authentication methods and guidelines such as the National Institute of Standards and Technology (NIST) - Electronic Authentication Guideline.[31]

Challenge systems. Certain financial institutions collect answers to a set of personal identifying questions during account setup. The institution randomly selects a subset of these questions and challenges anyone who attempts to login to answer them. Still others will challenge the user with a secret image-caption pair. When a customer first logs into his account he must select a secret image. He then submits an image caption. During the verification process the customer must provide the caption for the image before he is asked to enter a password. Registrars are encouraged to offer this security measure as an opt-in service for those customers who would accept the additional challenges as part of the cost/inconvenience of protecting domain names and preventing DNS configuration abuse.

Per domain access controls. Access to a domain registration account affords unrestricted access to all domains registered under that account, to users and attackers alike. A real world analog of the commonly encountered registration account access control model is a cabinet model bank safe: once you open this kind of safe, you can pretty much do as you please. Compare this to a bank vault containing safety deposit boxes: here, a customer or intruder must not only gain entry to the vault but also obtain key(s) to each safety deposit box. Registrars are encouraged to consider offering a similar access model to customers who seek greater protection; for example, an opt-in feature would grant customers the ability to control which points of contact are able to make changes to contact and DNS confirmation information, initiate or authorize a domain transfer, etc.

Multiple, unique points of contact. Organizations benefit from maintaining accurate points of contact information in domain registration records. Certain organizations also benefit from making each required point of contact a unique individual or position in the organization: this spreads the risk of any insider claiming ownership of or attempting to hijack a domain name from his employer or employer's customer. SSAC recommends these measures to registrants who want to protect domains against insider abuse. These measures also present an opportunity for registrars that would manage contact information on behalf of registrants. For example, a registrar could check for and require unique points of contact information, especially for a preferred means of correspondence (email address) as an opt-in service feature. The registrant as well as the registrar can use unique points of contact to create a granular privilege model. For example, some organizations may want to ensure that only the registrant point of contact can transfer a domain, or that only the technical point of contact can change DNS configuration (other models exist, and these are presented here for illustrative purposes only). Registrars may encourage registrants to choose these measures by combining them with others, such as interactive confirmation or multi-recipient notification processes.

[31] http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

Change notifications or confirmations. Some organizations protect against unauthorized or erroneous changes by creating a workflow whereby certain actions require confirmations from multiple parties. Multiple confirmations improve an organization's defences against impersonation: an attacker must socially engineer or impersonate not just one party, but two. Certain organizations may be interested in opting into a service where registrars check for and require multiple, unique points of contact. By doing so, such organizations can extend the same kinds of workflows they use internally to encompass changes to points of contact, domain transfers, or DNS configuration. For organizations that do not have such workflows, registrars could offer an optional service to enable such workflows on behalf of the customer. For example, at initial registration a registrar's change confirmation service could check that the customer has submitted a unique point of contact for each required contact associated with the domain. It also could allow the customer to select which points of contact must be notified upon a request to change DNS configuration, or require that both the technical and administrative contact respond by phone or email before making a change requested by one party. In addition, change confirmation can help avoid a vindictive or opportunistic domain transfer. Consider, for example, a situation where an employee designated as a point of contact has left the organization and the organization failed to change the contact information from this employee to his replacement. If the employee left disgruntled, he might attempt to claim the domain through a domain transfer. In the change confirmation scenario, other contacts are required to confirm the transfer and the transfer attempt could be blocked.

Multi-recipient notifications. Registrars routinely use electronic email to correspond with customers. SAC028, Registrar Impersonation Phishing Attacks, mentions several common correspondences including:

- Domain name renewal notices;
- Domain name order confirmations;
- Registration request confirmations;
- Changes to domain contact and DNS information;
- WHOIS data accuracy reminders;
- Notices of domain name expiry or cancellation; and
- Promotions, advertising for (new) services and features.

Offering the option of sending such correspondences to multiple recipients helps a customer in several ways. For example, the customer might avoid falling victim to a registrar impersonation phishing attack: one of the customer's recipients might be duped by the phish email but another might recognize the bogus email and alert the registrar and other contacts in his organization. Similarly, if the registrar were to deliver domain name renewals to multiple recipients, it would provide a safeguard against a situation where customer error or oversight would otherwise cause a registration to lapse. For example, a renewal might lapse if the only recipient of a renewal notice were on extended leave and away from email. In a multi-recipient scenario, this lapse in registration might be avoided if other recipients were to receive renewal notices. Registrars can also consider methods that certain financial institutions use to assist customers in identifying unauthorized access to accounts. The registrar can attempt to deliver notifications or confirmations

using both the original and changed versions of the contact information, to improve the likelihood that the correspondence reaches the correct destination regardless of whether the change is intended or fraudulently submitted, and regardless of whether the correspondence was sent before or after the change has gone into effect.

Multiple delivery methods for critical correspondence. Rather than rely entirely on electronic email to correspond with customers, registrars could offer to deliver critical notifications via telephone, fax, postal or courier services to customers who seek additional protection. Such services would make unauthorized transfers very difficult for an attacker. Customers who expect to renew critically important domain names "forever" would welcome the safeguard (and in the normal course of events, it has no impact). Customers who execute transfers of critically important domains may also consider that the delay introduced to a transfer "transaction" is acceptable after conducting a risk/benefit analysis.

Engaging the customer. Many large organizations are accustomed to outsourcing Internet access, security and network management. Managed services also have become popular among small- and medium-size businesses. Managed service providers (MSP) promote a customer-provider partnership. Through FAQs or awareness programs and education delivered through webinars or podcasts, the MSP explains how customers can best take advantage of the services they offer. As a complement to the measures described above, registrars could educate and encourage registrants to:

- Identify multiple domain account points of contact
- Include point of contact information administration in the Employee Resource Management process to assure that when a terminated employee's credentials are rescinded, all domain registration point of contact information associated with that employee is changed as well.
- Impose a password change policy.
- Periodically verify contacts.
- Proactively monitor domain name registration.
- Assign email addresses for all registration points of contact from a different domain than the registered domain name. (Some registrants may want to create multiple domain registration accounts as an additional safeguard.)
- Treat transfer attempts as a security event (check and re-check).
- Use a separate domain for registration contact email accounts from domains used for other business purposes. For example, assign email addresses for example.info's points of contact from example.net.

- Create role accounts: e.g., domainadmincontact@example.com, domainregistrantcontact@example.biz, domaintechnicalcontact@example.net. (Note that when role accounts are used, periodic checks of such accounts are strongly recommended to confirm that the role account is monitored by registrant staff without interruption due to personnel, administrative or operational changes within the organization.)

- Alias multiple recipients for a role account for notifications. Use this form of mail explosion to provide "blanket delivery" for critical registrar correspondence to increase the likelihood that the correspondence is received and processed in a timely manner.

Inform the customer. Registrars should make efforts to be as clear about the kinds of security measures they provide as they are about other competitive offerings. For example, a registrar that routinely submits its operations to an independent security audit and passes the audit could call public attention to this self-imposed discipline. Alternatively, ICANN and registrars could jointly identify an independent security auditor and contract with that auditor to define a prescribed set of security measures. Registrars could *voluntarily* ask to have the auditor run the audit against their operations. Registrars who pass the audit could be distinguished for having satisfied the security benchmarking exercise through some form of trust mark or seal. Similar programs are available from SSL Certificate issuing authorities.[32,33] SSAC notes that credit card processing is common among registrars and that the Payment Card Industry Security Audit Procedures for merchant and service provider compliance with Data Security Standard requirements may be relevant here.[34]

Measures from prior SSAC Reports. Many registrars have implemented some or all of the measures recommended in Section 5.2 of SAC007, Domain Name Hijacking Report, *Steps registrars can take to protect domain names.* These are summarized here for the sake of providing a compendium of new and previously recommended measures:

1. Use a unique EPP authInfo code value for each registered domain name (not for each domain registrant account). Some registrars use a single EPP authInfo code value for all domains held by the same registrant. This practice exposes all names a customer has registered to a hijacking based on a single code.

2. Establish a uniform default setting of domain locks across registrars. Many registrars already automatically lock domain names. Registrars must provide sufficiently direct means to unlock domain locks, so as to not unduly deny a legitimate transfer request from a verified domain name registrant.

3. Investigate additional methods to improve accuracy of registrant records. Consider more frequent or alternate forms of correspondence (e.g., telephone as

[32] Thawte Site Seal, https://www.thawte.com/ssl-digital-certificates/trusted-site-seal/index.html?click=site-seal-tile
[33] VeriSign Secured Seal®, http://www.verisign.com/ssl/secured-seal/
[34] PCI Security Standards Council, https://www.pcisecuritystandards.org/

an alternative to email) to encourage registrants to their information up to date and to detect registration abuse.

4. Collect emergency point of contact information from registrants, registrars, and resellers for parties who are suited to assist in responding to an urgent restoration of domain name incident.[35] Define escalation processes (emergency procedures) that all parties agree can be instituted in events where emergency contacts are not available.

5. Consider measures to improve authentication and authorization used in all registrar business processes.

6. Protect registrant information that can be used to facilitate fraud and impersonation, and theft of a domain name. As a default, treat any information that is used in registrant authentication processes as private. Consider treating this information with the same or similar measures to measures used to protect credit card or other financial information.

7. Improve auditing of resellers' compliance with record keeping requirements.

8. Ensure that resellers understand record keeping requirements of registrars (and ICANN), and improve compliance with these requirements.

9. Provide clear and readily accessible information to registrants regarding domain locking and domain name protection measures offered by registrars.

Protecting DNS configuration information from abuse

One purpose in gaining unauthorized access to a domain registration account is to gain control of an organization's name resolution service. An attacker modifies the name or IP address of a target's name servers to point to a system they operate, typically a computer he has previously compromised. The attacker hosts a DNS server and a zone file for the attacked domain name on the compromised computer. The attacker's DNS server resolves names from the attacked domain and redirects them to malicious or defaced web sites (as was the case in Comcast, ICANN, Panix, and Hush communications incidents described here and in SAC007). Certain attackers do not maliciously alter DNS configuration information; rather, they use compromised domain registration accounts to add their own name servers to a list of otherwise legitimately operated name servers. This serves to conceal the name servers they use in the *double flux* variants of fast flux attacks[36] and can also encumber take downs. Both extend the duration of phishing, spam, fraud, or criminal attacks.

The measures described in the prior section are applicable to those intended to protect against unauthorized use of a customer's domain name account to maliciously alter or stealthily add DNS configuration information. In particular, the following measures,

[35] See also SAC 038, Registrar Abuse Contacts, http://www.icann.org/committees/security/sac038.pdf
[36] SAC 025 Fast Flux Hosting and DNS, http://www.icann.org/committees/security/sac025.pdf

provided as optional services by a registrar or performed by the registrant, would provide important safeguards against DNS configuration attacks:

- Require multi-factor authentication for DNS configuration changes.
- Require confirmations of change from multiple contacts using email, possibly via media other than email. (Note: the same types of multi-step verification methods described earlier might be applied here.)
- Deliver notifications to multiple contacts when changes performed.
- Monitor DNS changes for anomalies or abuse.

Again, through FAQs, training, and education, registrars should encourage customers to routinely monitor DNS configuration activity (changes and additions). Registrars also should encourage customers to verify that names within their domain resolve to intended IP addresses. In addition, registrars should urge customers to maintain a history of DNS configurations for all domains and should help them understand the value of applying a timestamp and digital signature to this information.

Findings

From the incidents and related study in this Report, SSAC makes the following additional findings.

Finding (1) Differences exist among registrars as to their vulnerability to attack and the degree of protection they provide against attacks on domain accounts. Many domain registrants do not appear to have sufficient information to assess the extent to which a registrar is able to protect its domain accounts from attack and DNS configurations from malicious alteration.

Finding (2) While there are a large number of registrars that offer consumer-focused domain name registration services, and a smaller number of registrars and "brand management" organizations that offer security services to high-profile, highly targeted domain name holders (typically as part of an overall brand equity protection service), SSAC notes that *"pure play, secure" registration service providers* are rare, in part due to the fact that evaluating security measures does not play as prominent a role in customer decisions when choosing a registrar as it should.

Finding (3) Registrars could make more information about their security services available to allow customers to make informed decisions. Voluntarily submitting operations to an independent security audit and publicizing successful outcomes of such audits would allow customers to choose a registrar based on security requirements as well as cost and other ancillary features (such as web and DNS hosting).

Finding (4) Registrar services (and registrants) place greater confidence on the single factor authentication for login to accounts than the method merits. This authentication method has been repeatedly circumvented using various forms of social engineering, brute force attacks, and other techniques.

Finding (5) Attackers target DNS configuration when they succeed in compromising a domain registration account. Due to the distributed nature of the DNS, the effects of altering DNS configuration information persist beyond recovery and mitigation efforts by registrars. Malicious or incorrect DNS information can persist in locations throughout the Internet for the full duration of the TTL value associated with the altered DNS resource record(s). Attackers may alter the TTL specifically for this purpose.

Finding (6) Commonly, once a user is authenticated at a registration account portal or login, the user (or imposter) has *global* privileges and can modify contact information as well as DNS configuration information. Making granular access controls available to customers as an optional service – in particular, the ability to limit the type of actions each point of contact is able to perform with regard to changing contact and DNS configuration information and authorizing transfers – could reduce or mitigate the risk of exploitation or misuse of domain names and name resolution services associated with those names.

Finding (7) Registration service providers rely more heavily on unconfirmed email to deliver security-related correspondence (e.g., change notifications) than email delivery assurance and security characteristics merit. Attackers often defeat this method of correspondence by preventing email delivery when they modify the DNS configuration of domains through compromised registration accounts. Offering customers choices of alternative contact media or extending notification services to include some form of confirmation of receipt could reduce or mitigate the risk of exploitation or misuse of domain names and name resolution services associated with those names.

Recommendations

SAC007 made specific recommendations for registrars; notably,

Recommendation SAC007-(8): *Registrars should improve registrant awareness of the threats of domain name hijacking and registrant impersonation and fraud, and emphasize the need for registrants to keep registration information accurate. Registrars should also inform registrants of the availability and purpose of the Registrar-Lock, and encourage its use. Registrars should further inform registrants of the purpose of authorization mechanisms (EPP authInfo), and should develop recommended practices for registrants to protect their domains, including routine monitoring of domain name status, and timely and accurate maintenance of contact and authentication information.*

Based on our analyses of recent incidents, the related study, and our Findings, SSAC makes the following recommendations:

Recommendation (1) Registrars are encouraged to offer stronger levels of protection against domain name registration service exploitation or misuse for customers who want or need them. Measures enumerated in this report can be offered as optional services to customers, individually or bundled.

Recommendation (2) Registrars should expand existing FAQs and education programs they offer to registrants to include security awareness. Registrars should make information concerning the services they offer to protect domain registration accounts more accessible to customers so that they can make informed decisions regarding protective measures when they choose a registrar.

Recommendation (3) Registrars should consider the value of voluntarily having an independent security audit performed on their operations as a component of their security due diligence.

Recommendation (4) ICANN and registrars should study whether registration services would generally improve and registrants would benefit from having an approved independent third party that will, *at the request of a registrar*, perform a security audit based on a prescribed set of security measures. ICANN would distinguish registrars that voluntarily satisfy the benchmarks of this security audit through a trusted security mark program that is implemented in a manner similar to the way that SSL certificate issuing authorities provide trust marks or seals for web site operators who satisfy that authority's security criteria.

Acknowledgments

The committee wishes to thank the following members for their time, contributions, and review during SSAC's study of this matter:

Jaap Akkerhuis
KC Claffy
Steve Crocker
Patrik Fältström
Duncan Hart
Jeremy Hitchcock
Rodney Joffe
Warren Kumari
Danny McPherson
Dave Piscitello
Dan Simon
John Schnizlein
Bruce Tonkin
Rick Wesson
Richard Wilhelm

Statements of Interest

SSAC member biographical information and Statements of Interest are available at: http://www.icann.org/en/committees/security/biographies.htm.

Objections

No committee member objected to the publication of this report.