
2009년 8월 19일

**SAC 40: 도메인 등록 서비스의
불법 이용이나 남용을 방지하는 방법**

ICANN
보안 및 안정성 자문위원회
(Security and Stability Advisory Committee, SSAC)
보고서

서문

이 문서는 보안 및 안정성 자문위원회(SSAC)에서 작성한 보고서로 등록 서비스의 남용 방지법에 관해 설명합니다. SSAC는 인터넷 명명 및 주소 할당 시스템의 보안 및 무결성과 관련된 문제에 관하여 ICANN 커뮤니티와 이사회에 조언하는 일을 합니다. 운영상의 문제(예: 루트 이름 시스템의 정확하고 신뢰할 수 있는 운영에 관한 문제), 관리상의 문제(예: 주소 할당 및 인터넷 번호 할당에 관한 문제), 그리고 등록 문제(예: WHOIS 등과 같은 등록기관 및 등록업체에 관한 문제)가 여기에 속합니다. SSAC는 인터넷 번호 등록 및 주소 할당 서비스의 위협 평가와 위협 분석에 상시 참가함으로써 안정성과 보안에 대한 주요 위협이 어디에 존재하는지 평가하고 그에 따라 ICANN 커뮤니티에 조언합니다. SSAC는 단속, 시행 또는 선고할 공적인 권한이 없습니다. 이것은 타 기관에서 수행할 임무로서, 여기에서 말하는 조언은 타기관의 재량에 의해 평가되어야 합니다.

이 보고서의 기고자는 위원회 회원의 약력과 관심사 진술, 이 보고서에 공개된 사실이나 권장사항에 대한 위원회 회원의 이의사항을 이 보고서의 마지막에 인용해 놓았습니다.

소개

도메인 이름 등록 계정에 대한 공격 및 악의적인 도메인 이름 시스템(DNS) 레코드 재구성은 파괴적인 보안 사고에 해당합니다. 작년 한 해 동안 발생한 사고들은 DNS 및 도메인 등록 계정 액세스가 계속적으로 공격자들의 관심의 대상이 되어 왔음을 입증합니다. 원래 의도했던 호스트 외의 다른 목적지로 트래픽을 전환하기 위해 DNS를 사용할 목적으로 DNS 구성 정보를 악의적으로 변경하는 등 도메인 이름 등록과 관련된 정보의 무단 변경으로 인한 활동들은 비록 그 활동이 *일시적이라 하더라도* 비즈니스 운영에 심각한 혼란을 줄 수 있으며 재정적인 손해를 입히고 평판을 떨어뜨릴 수 있습니다.

도메인 이름 등록 계정이나 이름 분석 서비스 하이재킹은 전혀 새로운 공격 수단이 아닙니다. 과거 보고서와 상황 보고를 통해 ICANN 보안 및 안정성 자문위원회(SSAC)는 사용자(고객, 즉 등록자)의 관점에서 도메인 이름 등록 및 DNS 조작에 영향을 미치는 문제들을 연구해 왔습니다. SSAC는 등록자가 도메인 이름을 충분히 보호할 수 있는 조치를 취하지 못해 온 현 상황에 대해 파악했습니다(예: 등록을 갱신하지 못하거나 정확한 담당자 정보를 관리하지 못한 경우). SSAC는 등록자의 사업과 등록자가 등록 후 관리하는 도메인 이름에 관한 운영상 이익을 보호하기 위해 취할 수 있는 방법들을 추천해 왔습니다.

이 보고서는 도메인 등록 계정 무단 액세스와 관계 있는 최근의 사고들에 관해 설명된 보고서입니다. 이와 같은 사고들을 다루는 이유는 등록업체, 재판매업자 또는 등록자를 곤경에 빠뜨리거나 비판하려는 목적이 아닙니다. 이것은 항상 보안 사고를 분석하면 사고 발생을 방지하거나 사고의 심각성을 줄이기 위해 각 당사자가 취할 수 있었던 조치를 밝혀낼 수 있기 때문입니다.

이 보고서는 도메인 이름 등록 계정과 관계 있는 큼직한 특수한 사고들에 주목함으로써 사고의 공통 원인이 존재하는지 판단하고자 합니다. 특정한 위협을 줄이거나 취약성을 경감할 수 있는 방법을 알아낼 수 있기 때문입니다. 이 보고서는 계정의 훼손 과정을 파악하기 위해 사고에 관한 충분한 조사를 실시할 것이며 계정을 통제할 수 있게 되었을 때 공격자들이 수행하는 행동과 그 결과를 상세히 조사할 것입니다. 사고 설명은 공개적으로 입수할 수 있는 뉴스 스토리와 기사에서 발췌했으며 기타 대상 등록업체 및 업체의 고객들에 대한 인터뷰에서 입수한 정보로 이 설명을 보충하였습니다. 대상 당사자들이 민감하게 여기는 정보는 의도적으로 생략하였습니다.

이 보고서는 유사한 취약성으로부터 고객을 보호하기 위하여 다른 인터넷 사업 부문(예: 금융, 내구재 사업)에 사용되는 보안 방법을 제시합니다. 등록업체에서 고객과 공유할 수 있는 실제 경험을 파악함으로써 등록업체와 고객이 함께 등록된 도메인을

이 문서는 더 많은 독자들이 이해할 수 있도록 영문판 원본을 번역한 문서입니다. 국제인터넷주소기구(Internet Corporation for Assigned Names and Numbers, ICANN)는 번역의 진실성을 증명하기 위해 노력했습니다. 영어는 ICANN의 공식 언어이며 이 문서의 영문판 원본은 유일하게 신뢰할 수 있는 공식 문서입니다. 영문판 원본을 원하시면 다음 주소를 방문해 주십시오.
<<http://www.icann.org/committees/security/sac040.pdf>>.

2009년 8월 19일

3 / 28 페이지

불법 이용이나 남용으로부터 보호하고 도메인 이름 및 관련 DNS 구성에 대한 통제권을 일시적으로 상실한 경우와 관련된 위험까지도 등록자들간에 인식시킬 수 있는 방법에 대해 논의하였습니다. 수준 높은 서비스를 제공하여 회사를 차별화하는 업체도 있지만 이 보고서를 통해 더 많은 등록업체들이 도메인 등록 계정 공격에 대비한 추가 보호를 제공할 수 있는 기회를 고려하도록 적극 장려할 것입니다. 또 등록업체들이 고도의 경쟁적인 시장에서 서비스를 차별화할 하나의 방법으로 등록 보안 방법을 강조할 것을 고려해 보도록 적극 장려할 것입니다.

이 연구의 동기는?

과거 12개월 동안 도메인 이름 계정에 대한 무단 액세스와 관련하여 여러 건의 끔직한 사고들이 발생하였습니다. 이러한 공격의 혼란은 과거 도메인 이름 하이재킹¹ 및 도메인 이름 비갱신과 관련된 예상치 못한 결과들에 관하여 SSAC의 연구를 촉발하게 동기를 부여했던 사고들과 유사한 특징이 있습니다.^{2,3} 몇몇 사고는 등록업체 직원 및 등록 서비스(예: 웹 기반 도메인 계정 관리 도구)에 대한 악의적인 행위에서 비롯되었습니다. 사회 공학적 침입 수법을 이용한 사례와 등록업체가 고객에게 보내는 일상적으로 예상되는 통신을 이용한 사례도 있었습니다.⁴

SSAC는 2008년 5월부터 2009년 4월까지 발생한 일련의 사고들을 주시했습니다. 이로부터 우리는 일반적인 사고의 맥락이 드러날 수 있는지 여부를 알아보기 위해 이용할 수 있었던 정책 및 관리 기준(비즈니스 및 운영상의 관리 기준)은 물론 취약성을 파악하였습니다. 우리는 이 사고들을 조사하면서 다음과 같은 사실을 알게 되었습니다.

- (1) 많은 조직들은 도메인 이름 등록 계정에 높은 가치를 지니거나 업무상 중요한 이름, 조직이 소유하는 유형 자산, 상표 또는 지적재산권으로서 조직에 대한 가치를 지닐 수 있는 도메인 이름 등을 포함합니다.
- (2) 많은 등록 서비스 제공업체들은 고객 위주의 서비스를 목표로 운영됩니다. 즉, 등록 서비스는 고도로 자동화되어 있고 높은 트랜잭션 속도에서 매우 많은 등록자들에게 서비스를 제공하는 데 집중되어 있습니다. 서비스를 시기 적절하게, 확장 가능한 방법으로 제공하려고 노력하는 사업가들에게 자동화는 매우 중요합니다. 연구 결과 공격자들은 등록업체의 행동을 숙지해 왔으며 자동화의 특수한 측면을 이용할 것으로 밝혀졌습니다. 예를 들어 등록자에게 담당자, 구성 변경, 갱신 등을 통보하는 데 선호되는 방법이 이메일이라는 사실을 알게 되면 공격자들은 종종 DNS 구성을 변경함으로써 메일이 이메일 주소로 전달되는 것을 방해하려 시도합니다.

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>

이 문서는 더 많은 독자들이 이해할 수 있도록 영문판 원본을 번역한 문서입니다. 국제인터넷주소기구(Internet Corporation for Assigned Names and Numbers, ICANN)는 번역의 진실성을 증명하기 위해 노력했습니다. 영어는 ICANN의 공식 언어이며 이 문서의 영문판 원본은 유일하게 신뢰할 수 있는 공식 문서입니다. 영문판 원본을 원하시면 다음 주소를 방문해 주십시오. <<http://www.icann.org/committees/security/sac040.pdf>>.

(3) 조사 대상이 된 사고의 피해자들은 종종 고객 중심의 서비스를 목표로 하는 등록 서비스 제공업체들에 의해 업무상 중요한 도메인 계정이 운영되는 고객들이었습니다. 어떤 경우에는 고객들이 피해를 입기 전까지 자신들의 도메인 등록 계정에 대한 통제권 또는 액세스 권한을 상실할 가능성과 관련된 위험을 충분히 평가하지 못했습니다. 또 어떤 경우에는 사고 발생 전 준비했던 내부 정책과 활동 모니터링이 충분하지 못하여 공격을 감지하거나 차단할 수 없었습니다.

규모 및 회사의 명성으로 보아 일부 피해자는 도메인 이름의 자산 가치를 인식할 정도로 내부 보안 관리 및 위험 관리에 관하여 매우 철저한 것처럼 보일 수도 있을 것입니다. 그러나 이들은 도메인 이름을 위험 평가에 포함시키지 않은 것으로 나타났습니다. 또 다른 피해자들, 특히 중소기업이나 개인의 경우에는 문제가 발생할 때까지 도메인의 중요성을 충분히 이해하지 못했던 것 같습니다. 이것은 다른 위험 영역에 관해서도 일치되는 양상입니다. 많은 상황에서 조직은 자산의 가치 또는 업무상 중요성을 인식할 수 있으나 사고가 발생할 때까지 위험에 대비하여 자산을 보호할 충분한 방안을 제시하지 못할 수 있습니다.

보안의 측면에서 볼 때 도메인 이름을 중요한 자산으로 여기는 등록자들은 등록 서비스 제공업체를 선정할 때 보안을 중요한 선정 기준으로 삼아야 합니다. SSAC가 연구한 사고들은 등록자들이 등록 서비스 제공업체로부터 이용 가능한 보안 서비스의 범위를 이해하지 못하거나 등록 서비스 제공업체로부터 선택할 수 있는 일련의 보안 서비스가 *존재한다*는 사실조차 알지 못하는 것으로 나타났습니다. SSAC에 진술한 한 등록업체의 말에 따르면 등록자들은 등록 서비스가 거의 같다고 믿으며 따라서 모든 등록업체가 같은 등록기관에서 공급되는 동일 제품을 판매하며 등록업체에서 제공하는 보안 조치는 아마 똑같은 것이라고 결론을 내린다고 합니다. 다음 절에서 설명할 사고들은 SSAC가 도메인 이름 커뮤니티 밖에서는 등록 서비스 제공업체간 차이점이 잘 이해되지 않는다는 결론을 내리는 데 도움을 준 사례들입니다.

도메인 이름 등록 계정에 대한 공격

이 주제와 관련된 종합적인 사고 목록은 이 보고서의 범위 밖이지만, 뒤에 이어질 토론과 분석의 배경을 제공할 목적으로 도메인 이름 등록 계정을 공격한 끔찍한 특수 공격 사례들을 요약하여 제시하겠습니다. 이 요약은 공개 출처로부터 자유로이 인용한 것이지만 SSAC는 공격자에게 피해를 입은 조직 외에도 사고에 연루된 등록업체에 대해서도 자문을 구했으며 이분들의 협조에 큰 감사를 드립니다.

Comcast (2008년 5월)

Comcast는 미국 최대의 케이블 TV 제공업체이자 두 번째로 큰 인터넷 서비스 제공업체이자 최대의 주택용 전화통신 제공업체중 하나입니다.⁵ 사고 발생시 Comcast는 Network Solutions, Inc.를 통해 약 200개의 도메인을 등록했습니다.⁶ 공격자들은 2008년 5월 28일에 Network Solutions에서 Comcast의 도메인 등록 계정에 대한 액세스 권한을 얻었습니다. 처음에 공격자들은 특정 담당자 정보를 악의적으로 변경하였는데, 아마도 세상에 명성을 떨치려고 할 목적이었던 것으로 추정됩니다.⁷ Comcast 직원들은 변경 사실을 이메일로 통보받았고 올바른 정보로 복구하였습니다.

공격자들은 자신들이 Comcast 관리자에게 취약성과 불법 이용에 관해 해명해 달라고 요청했다고 주장합니다. 공격자들은 도메인 등록 계정에 대한 액세스 권한을 얻기 위해 사회 공학적 침입과 해킹 기술을 복합적으로 사용했다고 주장합니다.⁸ Network Solutions는 자사 직원에 대한 보안 위반이나 사회 공학적 침입이 없었으며 DNS 변경은 고객의 로그인 정보를 갖고 있는 누군가에 의해 저질러졌다고 보고했습니다.⁹ *와이어드 매거진*<Wired Magazine> 기사를 통해 공격자들은 Comcast 관리자가 자신들의 주장을 비웃고 책임을 뒤집어 씌웠다고 주장했습니다.¹⁰ 그리고 공격자들은 두 번째로 계정에 액세스했습니다. 이들은 이번에는 도메인 comcast.net의 DNS 구성을 변경하고 그들이 손상시켰던 서버에 호스트된 변조 웹 사이트로 트래픽을 리디렉트하였습니다. 그러나 Comcast 직원은 변경 사실을 Network Solutions로부터 이메일로 통보받지 못했습니다. 기술 담당자와 행정 담당자 모두 Comcast의 등록 도메인에서 할당받은 사용된 이메일 주소를 도메인 등록 기록에 기록했습니다. 공격자들은 DNS 구성을 변경함으로써 Comcast 직원들이 계정 활동을 이메일로 수신하지 못하도록 효과적으로 차단했습니다. 이들은 정말 이메일을 받을 수 없었습니다. 공격은 효과적었고 전세계적으로 대서특필되었습니다. *와이어드 매거진*<Wired Magazine>에 따르면, “공격은 미 동부 표준시로 오후 약 11:00경에 시작되었으며 해커들은 오전 4:00시 또는 5:00시경까지 Comcast.net을 점거했습니다. Comcast가 통제권을 되찾았을 때에도 DNS를 통해 변경 내용이 완전히 전파되기까지는 수 시간이 걸렸으며 일부 고객들은 목요일 아침 11:30분까지 웹 메일에 액세스할 수 없었습니다.” 2008년 5월 29일 *더 레지스터*<The Register> 기사에서는 “이번 공격은 구식적인 계정 침투만으로도 상당량의 웹 트래픽을 변경하기에 충분하다는 것을 보여 준다.”고 논평하였습니다.¹¹

5 Comcast 정보 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>

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/

이 문서는 더 많은 독자들이 이해할 수 있도록 영문판 원본을 번역한 문서입니다. 국제인터넷주소기구(Internet Corporation for Assigned Names and Numbers, ICANN)는 번역의 진실성을 증명하기 위해 노력했습니다. 영어는 ICANN의 공식 언어이며 이 문서의 영문판 원본은 유일하게 신뢰할 수 있는 공식 문서입니다. 영문판 원본을 원하시면 다음 주소를 방문해 주십시오. <<http://www.icann.org/committees/security/sac040.pdf>>.

CheckFree (2008년 12월)

CheckFree(현재는 FIServ)는 금융 서비스 산업 부문을 대상으로 한 세계적 정보 관리 및 전자 상거래 시스템 제공업체입니다.¹² 2008년 12월 2일, 공격자들은 Network Solutions에서 CheckFree의 도메인 등록 계정에 대한 통제권을 얻었습니다.¹³ 공격자들은 checkfree.com과 mycheckfree.com을 비롯한 여러 도메인의 DNS 구성을 변경하였습니다. 온라인 지불 및 전자 청구서 발행을 이용하기 위해 계정에 로그인을 시도했던 고객들은 Adobe Reader 불법 이용을 포함한 악의적 코드를 설치하려고 시도한 우크라이나의 위장 웹 서버로 리디렉션되었습니다.¹⁴ CheckFree는 공격이 발생한 지 8시간만에 올바른 DNS 구성을 복구하였으나, 다른 유사한 사고의 경우와 마찬가지로 글로벌 DNS 인프라 구조를 통해 변경 내용이 전파되는 데에는 수 시간이 더 걸렸습니다.¹⁵

워싱턴 포스트지의 “Security Fix” 블로그는 공격자들이 올바른 로그인 정보를 사용하여 계정에 액세스했다고 언급했습니다. 같은 기사에서, Network Solutions사는 공격자들이 로그인 자격 증명을 얻기 위해 시스템을 파괴하지 않았다고 강조하였습니다.¹⁶ 공격자들이 사용자 계정과 자격 증명을 정확히 어떤 방법으로 얻게 되었는지는 미지수로(또는 비공개로) 남아 있습니다.

ICANN, Photobucket, RedTube (2008년 6월)

2008년 6월 26일, ICANN도 Register.com의 ICANN 도메인 등록 계정에 무단 액세스 권한을 얻은 해커 그룹에 의해 피해를 보았습니다. ICANN 보도 자료에 따르면, 이 공격은 “사회적 침입 수법과 테크니컬한 기술을 결합한 정교한 공격이었습니다.”¹⁷ ICANN의 IT 관리자에 따르면, 공격자들은 icann.net, iana-servers.com, icann.com, internetassignednumbersauthority.com 및 iana.com 등 여러 도메인의 DNS 구성을 변경하여 방문자 트래픽이 Atspace.com에서 운영하는 무료 웹 호스팅 계정에 공개된 변조 웹 사이트로 라우팅되도록 했습니다. 그 공격이 정치적인 동기에서 비롯되었다는 추측을 하게 된 것은 사고가 발생한 타이밍과(새 GTLD에 관한 공개 토론이 개최된 ICANN 파리 회의가 시작되었을 때) 변조 메시지 자체 때문입니다. ICANN IT 직원들은 DNS 변경을 발견하고 Register.com은 ICANN로부터 통보 받은 후 곧 올바른 구성 정보를 복원하였습니다. 그러나, Comcast 사고의 사례와 마찬가지로

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>

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>

이 문서는 더 많은 독자들이 이해할 수 있도록 영문판 원본을 번역한 문서입니다. 국제인터넷주소기구(Internet Corporation for Assigned Names and Numbers, ICANN)는 번역의 진실성을 증명하기 위해 노력했습니다. 영어는 ICANN의 공식 언어이며 이 문서의 영문판 원본은 유일하게 신뢰할 수 있는 공식 문서입니다. 영문판 원본을 원하시면 다음 주소를 방문해 주십시오. <<http://www.icann.org/committees/security/sac040.pdf>>.

전세계로 수정된 정보가 전파되는 동안 악의적인 DNS 구성 정보가 24~48 시간 동안 글로벌 DNS에 남아 있던 것으로 추정됩니다.¹⁸

ICANN 공격을 자신들이 했다고 주장하는 해커 그룹은 유사한 전술 및 이후 공격과 동일한 무료 웹 호스팅 제공업체를 사용했습니다. Photobucket은 2007년 Fox Interactive Media사가 인수한 이미지 호스팅, 비디오 호스팅, 슬라이드쇼 및 사진 공유 웹 사이트입니다.¹⁹ 2008년 7월 18일, 같은 해커 그룹이 Photobucket에 대한 공격을 자신들이 했다고 주장하였고 Photobucket 사용자에게 서비스가 중단되는 결과를 가져왔습니다.²⁰ 해커 그룹은 2009년 2월 7일, 성인물 호스팅 사이트인 RedTube에 대해 또 다른 변조 공격을 감행했습니다.²¹·²²

DomainZ (2009년 4월)

DomainZ(Domainz.net.nz)는 뉴질랜드 기반의 MelbourneIT 자회사이자 등록업체입니다. 2009년 4월 21일, 이름을 날리고 싶어하는 사람들이 코카콜라, 환타, F-secure, HSBC, 마이크로소프트, 소니 및 제록스 등 여러 큰 기업의 계정 자격 증명을 수집하기 위해 DomainZ의 암호 조회 페이지에 대해 구조적 질의어(SQL) 삽입 공격을 감행하였습니다. 공격자들은 .CO.NZ에 등록된 도메인의 DNS 구성 기록을 .INFO 도메인에 등록된 서버 이름을 지칭하도록 변경했습니다(turkguvenligi.info). 이들 서버는 해킹된 도메인으로 분석되는 무단 존(Zone) 정보를 공격자들이 호스트한 변조 웹 사이트에 호스트했습니다. 특정 방문자 트래픽은 브랜드 이름(예: Microsoft)을 타겟으로 한 악의적인 웹 페이지에 랜딩되었고 다른 트래픽은 정치적으로 항거하는 페이지로 리디렉트되었습니다.

이러한 사고가 드러내는 것은 무엇인가?

Comcast, ICANN, Photobucket 및 RedTube 공격의 유사성은 등록 계정 공격자들이 웹, 파일 전송 및 기타 인터넷 응용 프로그램에 대해 다음과 같은 의미에서 유사한 부류라는 것을 보여 줍니다. 일단 한 분야에서 취약성을 성공적으로 이용했다면 공격자들은 불법 이용을 공유하고 대상을 스캔하여 동일하거나 유사하게 취약한 대상을 찾습니다.

SSAC는 이 사고들을 통해 다음과 같은 사실을 알아냈습니다.

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=FV31FLACFRJQYQSNLPSKH0CJUNN2JVN?articleID=208803672&subSection=Security>

몇몇 등록업체의 경우:

1. 모든 공격자들은 조직의 전체 도메인 이름 포트폴리오에 대한 통제권을 얻기 위해(또한 포트폴리오에 대한 정당한 액세스를 방해하기 위해) 사용자의 계정과 암호가 필요합니다.
2. 공격자들은 도메인 등록 계정에 대한 통제권을 얻기 위하여 한 명의 담당자에 대해 사회 공학적 침입 수단을 추측, 피싱 또는 적용하기만 하면 됩니다.
3. 공격자들은 도메인 계정 등록과 관리 포털을 스캔하여 웹 응용 프로그램의 취약성(예: SQL 삽입)을 조사합니다. 공격에 취약한 응용 프로그램 코드를 성공적으로 이용하면 수많은 도메인 계정에 대해 계정의 자격 증명을 공개할 수 있게 됩니다.
4. 이메일은 종종 일부 등록업체가 등록자에게 계정 활동을 통보하기 위해 선호하는 방법이자 종종 유일한 방법이 되기도 합니다. (이후의 섹션에서 다른 통신 연락 방법에 관해 논의하도록 하겠습니다).
5. 공격자들은 DNS 구성 정보를 변경함으로써 타겟으로 삼은 등록자에 대한 이메일 통보 전달을 차단할 수 있습니다. 따라서 이메일 통보는 손상된 계정을 통해 공격자가 통제하는 도메인 내의 모든 수령자에게 전달되지 못할 것입니다(예: 등록자가 파악한 도메인에 호스트된 관리자 또는 기술 담당자의 이메일 주소).
6. 하나의 사용자 계정과 암호를 통해 통상적으로 등록 계정내 모든 도메인에 대하여 담당자 정보 및 DNS 구성 정보에 액세스하고 이를 변경할 수 있는 권한을 얻게 됩니다.
7. DNS 정보의 무단 변경이 신속히 발견되었을지라도 악의적인 구성을 수정하기 위해 DNS 정보를 복원하는 프로세스는 긴 시간이 걸릴 수 있습니다. 이것은 분산적인 DNS의 특징과 회생 시간(TTL)과 관련하여 내재된 문제입니다.

고객들은 등록 보호 방안에 대해 잘 모릅니다.

사업을 보안하고 고객을 보호하는 데 능숙한 일부 등록업체도 있습니다. 이러한 업체들은 웹 응용 프로그램, 이름 및 호스팅 서버를 보안하기 위한 모범 사례를 적용합니다. 이들은 시스템과 계정에 의심되는 활동이 있는지 감시합니다. 등록업체는 남용이나 범죄 고소에 대응할 직원을 지원합니다. 그러나, 도메인 등록 서비스만큼이나 광범위한 업계에서는 전자 상거래나 온라인 사업등의 업종에서 볼 수 있듯이 일부 등록업체가 알려진 공격 수단에 대해 취약하다는 사실이 드러날 수밖에 없습니다. 다른 등록업체가 나와봐야 보안 감사 시 고려되지 않았던 공격 또는 전에 본 적이 없던 공격에 취약하다는 사실이 드러날 수 있습니다.

이 문서는 더 많은 독자들이 이해할 수 있도록 영문판 원본을 번역한 문서입니다. 국제인터넷주소기구(Internet Corporation for Assigned Names and Numbers, ICANN)는 번역의 진실성을 증명하기 위해 노력했습니다. 영어는 ICANN의 공식 언어이며 이 문서의 영문판 원본은 유일하게 신뢰할 수 있는 공식 문서입니다. 영문판 원본을 원하시면 다음 주소를 방문해 주십시오.
<<http://www.icann.org/committees/security/sac040.pdf>>.

이 보고서에서 논의했던 사고들 가운데(또한 SAC012에서 인용한 기타 유사한 사고들과 간행 이래 발생한 사고들) 등록업체 프로세스가 공격자들에 의해 이용당해 왔고 계속 이용당하고 있다는 사실이 명백합니다. 산업의 규모와 다양성을 고려한다면 이것은 이상한 일이 아닙니다. 등록업체들은 지금까지 그래왔고 앞으로도 계속 공격자들의 타겟이 될 것입니다. *금융기관의 고객들이 온라인 뱅킹 포털에 대한 공격으로 피해를 입을 수 있는 것과 마찬가지로 도메인 이름 등록자들은 등록업체 도메인 관리 페이지에 대한 공격으로 피해를 입을 수 있습니다.*

도메인 이름과 DNS 구성에 대한 공격 위험을 평가하고 등록업체의 공격 노출을 허용 가능한 수준까지 낮추는 등록 서비스를 선택하는 것은 궁극적으로 등록업체의 책임입니다. 그러나, 등록업체들은 대개 이들이 제공하는 보호 방안, 등록 보안 서비스를 비교하기 위한 방법의 부재에 대해서는 주의를 환기시키지 않으며 고객들은 모든 등록업체가 보안에 관하여 동일하다고 그릇된 판단을 할 수 있고 불완전하거나 냉담한 선택을 할 수 있습니다.

등록업체는 서로 다른 목표 시장과 서비스 모델을 갖고 있다.

이를 염두에 두고 SSAC는 광범위한 도메인 이름 등록 서비스를 고려하여 도메인 이름 등록이 대개 두 개의 서비스 모델을 통해 지원된다고 결론을 내렸습니다.

한 가지 대중적인 서비스 모델은 도메인 이름 등록 서비스를 중저가에 제공합니다. 서비스의 제공의 고도로 자동화되어 있으며 종종 인간이 실수할 가능성을 최소화하는 일관성있고 반복된 방법으로 신속한 대량 트랜잭션을 강조하여 설계되었습니다. 고객들과의 통신은 보통 통보를 전달하거나 의무적인 프로세스를 통해 고객들에게 안내할 단순한 지침(예를 들면 연간 WHOIS 정확도 검토)을 전달하기 위한 이메일 메시지를 통해 지원됩니다. 티켓팅 시스템을 통한 자동화된 문제 보고도 흔히 볼 수 있습니다. 대개, 자동화는 인간의 개입보다 나은 것처럼 보입니다. 대부분의 경우 자동화가 예상한 대로 기능을 수행하지 못하거나 잘못 이해된 경우 또는 고객에게 자동화된 프로세스로 해결할 수 없는 문제가 있거나 보고할 사고가 있는 경우 고객들은 인간의 개입을 추구하게 됩니다. 남용에 대비하여 도메인 계정과 DNS 구성을 보호하는 흔히 볼 수 있는 보안 조치로는 보안 소켓 계층(SSL)으로 보호되는 도메인 계정 로그인과 도메인 포트폴리오 관리, DNS 또는 계정, 개인정보 서비스와 관련된 담당자 정보가 변경되었을 때 이메일 통보(SAC023에서 논의한 보호되거나 위임된 WHOIS 서비스²³), 그리고 도메인 양도 방지(등록업체 잠금, 등록업체의 도메인 손실 및 취득 사이 인증 코드 확인) 등이 있습니다.²⁴

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

²⁴ 특정 등록업체는 업무상 중요한 내부 시스템, 프로세스 및 데이터베이스를 보호하기 위하여 남용 방지 조치 및 보안 조치를 이행합니다. 대개 이러한 조치들은 등록업체 고객들이 쉽게 알 수 있습니다.

이 문서는 더 많은 독자들이 이해할 수 있도록 영문판 원본을 번역한 문서입니다. 국제인터넷주소기구(Internet Corporation for Assigned Names and Numbers, ICANN)는 번역의 진실성을 증명하기 위해 노력했습니다. 영어는 ICANN의 공식 언어이며 이 문서의 영문판 원본은 유일하게 신뢰할 수 있는 공식 문서입니다. 영문판 원본을 원하시면 다음 주소를 방문해 주십시오.
<<http://www.icann.org/committees/security/sac040.pdf>>.

두 번째 등록 서비스 모델은 도메인 이름에 높은 가치를 부여하고 자사의 도메인 이름과 온라인 존재를 업무상 중요하게 여기는 고객들 또는 자신들의 사업이나 브랜드가 남용 또는 범죄 활동의 타겟이 될 가능성이 높다고 인식하는 고객들의 요구에 부합하는 보호 방안을 제공합니다. 이러한 고객들은 도메인 이름에 대한 위협을 인식하고 담당자나 DNS 구성 정보의 손실, 구성 오류, 변경 또는 도메인의 오용 등에 관한 위협을 최소화하거나 경감시키고 싶어 하며 이러한 요구사항을 충족시키는 특별한 등록업체를 찾기 위해 현명한 결정을 내리는 데 도움이 될 만한 충분한 정보를 수집해 왔습니다. 이와 같은 등록업체들은 기술적인 오류나 간과로 인한 고객의 도메인 이름 비갱신으로부터 보호하고, 등록 기록의 무단 변경을 통한 도메인 이름 하이재킹으로부터 고객을 보호하고, 무단의 악의적 DNS 구성을 방지하기 위한 보안 조치를 제공합니다. 이러한 등록업체의 비즈니스 모델은 오류가 발생할 확률이 매우 낮은 개인 트랜잭션 관리에 집중되어 있습니다. 등록업체는 도메인 포트폴리오의 보호에 프리미엄을 붙이는 고객들의 요구를 충족시키며 인적 도움, 특히 고객에게 지정된 계정 전문가의 도움을 받기 위해 프리미엄을 지불할 용의가 있습니다. 예를 들어 고객들은 변경 요청, DNS 구성 실시간 모니터링 및 등록업체의 이름 분석 서비스를 실행하기 앞서 인증된 고객 담당자로부터 구두 또는 서면으로 보안에 대한 승인을 받고 싶어할 수 있습니다.

보통 위에서 언급한 방법들은 브랜드 자산가치 보호에 역점을 두는 더욱 광범위한 종합적 조치에 속합니다. 브랜드 자산가치 보호 방법은 상표의 남용(예: 인터넷 사용자를 웹 사이트로 유인하기 위해 상표/브랜드 소유자 이외의 사람이 상표 또는 브랜드를 무단 이용하는 경우), 브랜드 소유자를 타겟으로 삼은 도메인 등록(피싱 또는 사기 공격에 사용되는 시각적으로 유사한 "상동" 도메인), 수입 또는 트래픽의 전환, 백오더(다른 당사자가 이미 등록한 도메인을 다시 사용할 수 있게 될 경우 고객 대신 등록해 주는 것), 그리고 방어 등록(상표나 이름을 모든 상위 레벨 도메인에 등록하는 것) 등을 포함한 위협을 경감시키는 역할을 합니다.

누가 도메인 계정과 DNS의 하이재킹으로부터 보호받아야 하는가?

도메인 계정이나 DNS 구성 정보의 악의적 변경에 대비한 강력한 보호 방안은 보통 도메인 포트폴리오나 브랜드 자산가치가 있는 사업 및 수단에 상당한 투자를 했고 브랜드를 보호하기 위해 대가를 지불할 의향이 있는 조직들이 잘 알고 있고 찾는 대상입니다. 그러나, *등록자는 보호해야 할 브랜드나 지적재산권을 소유한 회사들만이 도메인 계정 하이재킹이나 악의적인 DNS 구성 정보 변경으로부터 보호받을 필요가 있다고 결론내려서는 안 됩니다.* 온라인상 존재에 의해 사느냐 죽느냐가 결정되는 수많은 조직들은 브랜드와 관련된 도메인 이름을 사용할 수 없습니다. 그러나 몇몇 회사들은 여전히 등록될 수 있는 어떠한 도메인 이름으로도 손쉽게 사업을 운영할 수 있습니다. 그럼에도 불구하고 이러한 조직들은 웹, 메일 또는 기타 인터넷 서비스에 할당하려는 이름이 조직에서 서비스를 호스트한 인터넷 프로토콜(IP) 주소로 분석되지 못할 경우 손해를 입거나 재정적인 손실을 입게 될 것입니다.

이 문서는 더 많은 독자들이 이해할 수 있도록 영문판 원본을 번역한 문서입니다. 국제인터넷주소기구(Internet Corporation for Assigned Names and Numbers, ICANN)는 번역의 진실성을 증명하기 위해 노력했습니다. 영어는 ICANN의 공식 언어이며 이 문서의 영문판 원본은 유일하게 신뢰할 수 있는 공식 문서입니다. 영문판 원본을 원하시면 다음 주소를 방문해 주십시오.
<<http://www.icann.org/committees/security/sac040.pdf>>.

특정 조직들은 도메인 이름이나 악의적인 DNS 구성 정보 변경과 관련한 위험을 의미 있는 수준으로 경감시킬 등록 서비스를 선택함으로써 혜택을 보게 될 것이라는 가정 하에 우리는 이러한 조직들이 보안 수단 외의 다른 이유 때문에 등록업체를 선정할 수 있을 가능한 원인들을 파악하려고 노력했습니다. 몇 가지 가능한 이유를 나열하면 다음과 같습니다.

인지된 비용: 어떤 경우에는 도메인 계정과 DNS 하이재킹에 대한 강력한 보호 방안을 제공하는 등록업체를 통해 도메인을 등록하는 비용이 엄청나게 비싸다고 조직에서 추정하거나 잘못된 결론을 내릴 수 있습니다.

인식: 도메인 계정과 DNS 하이재킹에 대한 강력한 보호 수단에 대해 대가를 지불할 의향이 있는 고객도 있지만 그와 같은 서비스가 존재한다는 사실을 잘 모르고 있습니다.

정보의 부족: 조직에서 입수할 수 있는 정보가 제한적이어서 등록업체가 유사한 보호 방안을 갖고 있다고 결론을 내린 몇몇 경우도 있습니다.

“귀하가 제공하는 번들 서비스는 저희 회사에는 맞지 않습니다”: 어떤 경우에는 조직에서 도메인 계정 및 DNS 하이재킹에 대한 강력한 특정 보호 수단에 대해 대가를 지불할 용의는 있으나 예를 들어 강력한 보호 수단과 더불어 브랜드 자산가치 보호를 제공하는 등 특정 등록업체가 번들로 제공하는(또는 번들로 제공한다고 인식하는) 서비스에 대해서는 대가를 지불할 용의가 없거나 지불할 능력이 없습니다.

이러한 상황에서 몇 가지 추가 질문들을 고려해 볼 가치가 있습니다.

브랜드를 보호하려고 노력하는 조직들만이 더 강력한 등록 보호 수단에 관심을 갖고 있는가?

아닙니다. 수많은 조직들의 경우 자사 브랜드뿐 아니라 온라인상 존재를 보호하려는 열망이 보호 비용과 균형을 이루어야 합니다. 강력한 등록 보호 방안은 브랜드 자산가치 보호에 대한 보완책으로서 종종 제공됩니다. 아마도 기본적인 등록 서비스에 추가하여 옵트인(사용자의 사전 동의를 받는) 서비스 또는 무료로 제공하는 방식으로 제공되는 강력한 등록 보호 수단들은 불법 이용이나 오용 때문에 이용도를 잃게 될 가능성을 줄일 보안 수단에 투자하려는 조직들이 액세스할 수 있는 바람직한 보안 기능이 될 수 있습니다.

브랜드에 관심이 없는 조직에서도 위험을 평가하고 자산을 관리할 때 도메인 이름을 고려해야 할까요?

이 문서는 더 많은 독자들이 이해할 수 있도록 영문판 원본을 번역한 문서입니다. 국제인터넷주소기구(Internet Corporation for Assigned Names and Numbers, ICANN)는 번역의 진실성을 증명하기 위해 노력했습니다. 영어는 ICANN의 공식 언어이며 이 문서의 영문판 원본은 유일하게 신뢰할 수 있는 공식 문서입니다. 영문판 원본을 원하시면 다음 주소를 방문해 주십시오.
<<http://www.icann.org/committees/security/sac040.pdf>>.

예. SSAC 보고서에 따르면 도메인 이름이 하이재킹되었을 때 재정상의 손실과 장애, 명예훼손 등 부정적인 영향을 등록업체가 받게 된다고 설명합니다.²⁵ 또한 SSAC 보고서는 도메인 이름의 비갱신과 관련된 문제들 및 DNS 이름 서버와 관련하여 도메인 이름을 비갱신할 경우 발생할 수 있는 문제들도 설명합니다.²⁶ 특히 SSAC는 SAC010에서 “도메인 이름은 중개인을 통하든, 직접 거래하든간에 시장성이 있는 가치로, 또는 경상수입을 창출하는 수단으로 여겨서는 안 된다.”

“등록된 도메인 이름을 자발적으로 또는 우연히 갱신하지 않은 등록자들은 모든 도메인 이름이 어느 정도 ...의 가치를 갖는다는 사실과 신규 등록자들은 이전 등록자에게 해로운 것으로 입증된 시간이 경과된 도메인 이름을 사용할 수 있다는 사실을 인식해야 한다.”라고 언급합니다.²⁷

도메인 이름을 위험을 관리하고 투자에 대해 위험과 도메인 의존성을 경감하는 데 도움이 되는 자산으로 여기는 조직들에 대해서는 어떠한 보호 방안을 제공할 수 있습니까?

다른 인터넷 사업 부문(예: 금융, 내구재, 전자 상거래)에 사용되는 특정 수단들이 실제로 등록 서비스를 보호하기 위해 사용됩니다. 특수한 수단들을 고려하기 앞서 특히 등록자의 이익을 위하여 첫 번째 원리를 다시 조사할 가치가 있습니다. 특히 대규모 조직에서 사용하는 자산, 프로비저닝(사용자 등록/변경 관리 작업), 위험 관리 체계가 도메인 이름 등록에 어떻게 적용되는가? 도메인 이름 등록을 자산으로 여기는 이유는 무엇인가?

과거의 SSAC 보고서에서는 도메인 이름을 상인, 금융기관 또는 교육기관, 영리 또는 비영리 법인이나 기업체, 개인이나 제품 등 어느 엔티티가 인터넷상에서 알려져 있거나 사업을 영위할 때 사용하는 아이덴티티로 설명했습니다. 이것은 법인이 DBA(사업자 등록명)로 등록하는 이름과 같은 이름이 될 수도 있고 유명인, 저자, 정치인 또는 기타 인물의 이름일 수도 있습니다. 현실적으로는 개인과 조직 모두 이름(브랜드, 서비스 표장, 상표)을 자산으로 취급하며 이름을 남용하지 못하도록 보호하는 방안을 선택하는 실정입니다(정관, 특허, 저작권 등을 통해). 도메인 이름은 종종 조직의 브랜드, 서비스 표장, 상표와 동일하며 따라서 등록자는 단순한 등록만이 아니라 불법 이용이나 오용에 대비하여 보호함으로써 이와 같은 이름을 보호할 수 있는 방안을 선택해야 합니다.

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>

이 문서는 더 많은 독자들이 이해할 수 있도록 영문판 원본을 번역한 문서입니다. 국제인터넷주소기구(Internet Corporation for Assigned Names and Numbers, ICANN)는 번역의 진실성을 증명하기 위해 노력했습니다. 영어는 ICANN의 공식 언어이며 이 문서의 영문판 원본은 유일하게 신뢰할 수 있는 공식 문서입니다. 영문판 원본을 원하시면 다음 주소를 방문해 주십시오. <<http://www.icann.org/committees/security/sac040.pdf>>.

도메인 이름 등록은 전 세계적으로 하나밖에 없는 도메인의 고유성을 보장하며 등록자가 등록 갱신료를 지불하고 계약상 의무(예: 허용 가능한 사용, 정확한 등록)를 준수하기만 하면 그 도메인이 등록자에게 속하도록 합니다. 따라서 이것은 자산, 위험, 프로비저닝 등 다른 네트워크 관리 규율과 같습니다.

또한 도메인 이름은 그 도메인에 대한 서비스(웹, 메일, 소셜 네트워크, 음성...)를 제공하는 호스트의 인터넷 주소를 판단하기 위해 DNS를 사용하여 분석할 수 있는 사용자 친화적인 식별자입니다. 도메인의 운영적 가치, 특히 이름 분석의 이용도가 높다는 점과 도메인내에서 그 이름이 의도한 대로 분석된다는 점은 대부분의 조직에 있어 헤아릴 수 없이 중요한 요소가 됩니다.

예를 들어 자산 및 위험 관리 프로그램의 경우 다음이 가능합니다.

- 자산의 가치 파악(무형이든 유형이든).
- 가치가 위협받는 방식 나열(상실, 도난, 오용).
- 위협이 어떻게 현실화될 수 있는지, 도메인 이름이 공격이나 불법 이용에 취약하도록 만드는 요인은 무엇인지 판단하십시오.
- 각 위협이 제시하는 확률 또는 위험을 판단하십시오.
- 위험을 경감시키거나 줄이는 방법을 판단하십시오.
- 위험이나 비용을 허용 가능한 수준으로 경감시키거나 줄이는 비용을 판단하십시오.
- 적절한 예산을 결정하고 위험을 경감하거나 줄이십시오.

도메인 이름이 자산인 경우 기타 목록에 기입되거나 가치가 평가되거나 민감한 자산과 동일한 엄격성이 필요합니다. 이러한 관점에서 생각해 볼 때 도메인 이름 등록 관리는 대규모 네트워크내 프로비저닝 관리의 수많은 특성들을 공유하는 것처럼 보입니다. 프로비저닝과 도메인 이름 등록의 주요 작업{추가, 중지, 변경}을 그 예로 들 수 있습니다. 프로비저닝 관리에 적용된 모범 사례에서는 이들 작업이 적절한 순서대로, 인증된 당사자에 의해, 시기 적절하고 감사가 가능한 방법으로, 누락이나 침입 또는 오류 가능성이 낮은 상태에서 수행되도록 노력합니다. 그와 같은 모범 사례는 도메인 이름 등록 관리에까지 확장되어야 하며 등록 서비스는 유사한 모범 사례의 목표를 충족하도록 노력해야 합니다.

도메인 이름 등록을 보호하는 보안 조치는 인트라넷, 원격 데이터베이스 및 기타 회사에서 업무상 중요하다고 생각하는 응용 프로그램 액세스를 위해 조직에서 제공하는 보안 수단만큼이나 중요한 것으로 여겨져야 합니다. 도메인 이름 등록에 의미 있는 자산가치를 부여하는 고객들은 도메인 이름 등록 관리중 누락, 침입, 오류가 발생할 가능성을 최소화하기 위해 업무상 중요한 다른 응용 프로그램을 위해 구현하는 서비스에 준하는 인증, 허가, 감사 서비스를 찾아보아야 합니다. 이러한 보안 조치중

이 문서는 더 많은 독자들이 이해할 수 있도록 영문판 원본을 번역한 문서입니다. 국제인터넷주소기구(Internet Corporation for Assigned Names and Numbers, ICANN)는 번역의 진실성을 증명하기 위해 노력했습니다. 영어는 ICANN의 공식 언어이며 이 문서의 영문판 원본은 유일하게 신뢰할 수 있는 공식 문서입니다. 영문판 원본을 원하시면 다음 주소를 방문해 주십시오. <<http://www.icann.org/committees/security/sac040.pdf>>.

고객에 의해 구현될 수 있는 것도 있습니다. 또 추가 보안 조치를 제공하는 것이 고도의 경쟁 시장에서 회사를 차별화하는 방법이라고 판단하는 등록업체의 경우 등록 서비스에 보안 조치를 통합시킬 수 있습니다. 다음 절에서 이에 대해 좀 더 상세히 고려해 보도록 하겠습니다.

도메인 계정과 DNS 하이재킹을 방지하는 수단

이 절에서는 특정 등록업체들이 더 광범위한 서비스 집합의 일부로서 종종 온라인 명예(브랜드 자산가치) 보호와 연계하여 제공하는 수단들에 관해 설명합니다. 그 다음으로, 등록업체가 제공할 수 있는 수단들 가운데 SSAC에서 2008년에 발생한 사고들을 고찰하는 동안 인터뷰를 실시한 대상 당사자들이 바람직하거나 없어서는 안 된다고 식별한 수단에 관해 설명하도록 하겠습니다. 마지막으로 금융 기관 및 전자상거래 기관들이 고객 계정을 보호하기 위해 제공하는 방법 외에도 대기업들이 원격 응용 프로그램 액세스를 보안하기 위하여 사용하는 방법에 대해 생각해 보겠습니다. 개인별 옵트인 서비스나 서비스 번들로 제공되는 이러한 방법들은 도메인 계정 불법 이용 또는 오용 위험을 줄이기 위해 보호 수단에 투자할 의향이 있거나 투자하도록 자극을 받은 고객들을 위하여 도메인 등록 계정의 보안을 향상시킬 것입니다. 등록업체들은 이러한 수단이 삽입될 경우 기회가 발생하는지 아니면 경쟁 시장에서 업체를 차별화할 수단으로 여겨야 할지 고려하는 것이 좋습니다.

고객(등록자)은 도메인 이름 보호에 관해 중요한 역할을 수행합니다. 이 절에서 우리는 고객들이 (a) 도메인 등록 생성 및 갱신과 관련한 등록자-등록업체간 작업 흐름에서 자신들의 역할을 보안하고 (b) 담당자 정보와 구성 정보 관리 및 변경 프로세스를 보안하기 위해 취할 수 있고 취해야만 하는 특수한 보완적 조치에 관해 간략히 설명할 것입니다. 등록업체는 이러한 조치들을 기존의 질문 또는 자주 묻는 질문들(FAQ)을 통해 권장하거나 매우 중요한 도메인 포트폴리오를 보유하고 있는 고객에 대해서는 다른 방법을 통해 권장할 수 있습니다. 예를 들어, 등록업체에서 고객들에게 이 보고서를 알리고 이용하도록 장려하는 것도 좋은 방법이며, 이 보고서를 고객들이 검토하고 도메인 이름 포트폴리오를 가장 심각하게 위협한다고 느끼는 위험들을 줄이거나 경감시키기 위해 필요하다고 생각되는 조치들을 이행하도록 장려할 수 있습니다.

SSAC는 도메인 등록 보호를 위해 제공하는 서비스가 더 크게 채택될 가능성이 있으며 중소기업의 이니셔티브와 독립적 구현을 모두 합한 것보다 좀 더 포괄적일 수 있다고 믿습니다. 우리가 이렇게 단언할 수 있는 이유는 방화벽, 스팸 방지, 바이러스 방지 및 기타 보안 서비스를 번들로 제공하는 보안 시스템인 통합위험관리(UTM) 보안 장치의 성공을 목격했기 때문입니다. 이 보안 장치들은 중소기업(SMB) 부문에 있어 하나의 보안 기능을 제공하는 보안 시스템중 가장 좋은 시스템들을 선택하고 이를 연계해서 사용하는 것보다 시장 침투력이 더 크고 시장에서 더 많이 성공해 왔습니다. 우리는 추가 보안 서비스 제공이 통합위험관리(UTM)에서 입증된 경우처럼 중소기업(SMB)의 도메인 등록에도 영향력을 미칠 수 있을 것으로 믿습니다.

이 문서는 더 많은 독자들이 이해할 수 있도록 영문판 원본을 번역한 문서입니다. 국제인터넷주소기구(Internet Corporation for Assigned Names and Numbers, ICANN)는 번역의 진실성을 증명하기 위해 노력했습니다. 영어는 ICANN의 공식 언어이며 이 문서의 영문판 원본은 유일하게 신뢰할 수 있는 공식 문서입니다. 영문판 원본을 원하시면 다음 주소를 방문해 주십시오.
<<http://www.icann.org/committees/security/sac040.pdf>>.

도메인 포트폴리오에 대한 액세스 보호

이 절에서 설명한 조치들은 등록업체나 재판매업자의 온라인(웹) 사용자 인터페이스 또는 도움말 데스크 및 고객 관리 전화 서비스를 경유하여 고객의 도메인 이름 계정에 무단으로 액세스하는 것을 방지할 목적으로 설명되었습니다.

등록 확인. 대용량의 트랜잭션 처리 속도 및 도메인 이름의 신속한 프로비저닝을 위해 최적화되는 등록 모델은 종종 등록자의 신원을 확인하고 지불 과정에서 사기 또는 범죄가 발생하지 않는지 확인할 수 있는 용도로는 최적화되어 있지 않습니다. 안티피싱 연구,^{28·29} 봇넷(Srizbi, Conficker 웹)과의 전쟁 경험 및 패스트 플렉스 공격 네트워크는 도메인 등록 계정이 범죄 활동의 핵심 공급처이며 앞으로도 그럴 것임을 예증합니다. 등록시 및 담당자 정보가 변경될 때마다 등록자가 제출한 담당자 정보의 문제점을 확인하면 위장과 도메인의 남용을 줄일 수 있습니다. 등록업체들은 이메일 등록 확인 기능을 제공하는 방안을 고려하는 것이 좋습니다. 이메일 등록 확인 기능을 사용할 경우 도메인 등록은 등록자가 등록업체에서 발송한 활동 이메일에 첨부된 하이퍼링크를 클릭, 방문함으로써 이메일 주소를 확인할 때에만 완료됩니다. 추가 방법으로서 어떤 금융기관에서는 이메일을 사용하기보다는 고객이 제출하는 전화번호를 이용할 것입니다. 회사는 전화를 통해 승인 번호를 제공하는데 이 번호를 고객이 웹 양식에 입력하여 계정을 활성화시키거나 트랜잭션을 인증하게 됩니다. SSAC는 이러한 종류의 방법이 등록 처리 및 제품 배송을 더욱 지연시킨다는 점을 인정하지만(등록 및 등록된 도메인 이름의 분석) 등록업체는 이러한 단점을 고객을 위할뿐 아니라 크게는 인터넷 커뮤니티를 위하여 남용을 줄일 수 있다는 장점과 레버리지하는 좋습니다. 인터넷 이름 시스템을 보안하기 위해 사전 행동적으로 두드러진 활동을 보이는 등록업체는 좋은 평판을 자연스럽게 얻게 된다는 추가 이점이 있으며 보통 보안 전문가들과 비즈니스 동업자들이 보안에 덜 활동적인 등록업체에 대해 적극적인 보안 활동을 권장하는 이유이기도 합니다.

암호 기반의 인증 시스템 개선. 등록업체간에 가장 널리 퍼진 인증 방법은 사용자 이름 및 암호를 사용하는 간단한 방법입니다. 등록업체들은 암호에 대해 최소 암호 길이, 최대 유효 기간 또는 복잡성 검사를 강요할 의무가 없으며 부정확한 로그인 시도 횟수를 제한하는 방법으로는 무작위 추측 공격에 대비하지 못할 수 있습니다. 흔히 채택되는 최상의 보안 관리 기준에서는 다음과 같은 방법이 암호 기반 인증 시스템에 존재해야 한다고 권장합니다.

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

이 문서는 더 많은 독자들이 이해할 수 있도록 영문판 원본을 번역한 문서입니다. 국제인터넷주소기구(Internet Corporation for Assigned Names and Numbers, ICANN)는 번역의 진실성을 증명하기 위해 노력했습니다. 영어는 ICANN의 공식 언어이며 이 문서의 영문판 원본은 유일하게 신뢰할 수 있는 공식 문서입니다. 영문판 원본을 원하시면 다음 주소를 방문해 주십시오. <<http://www.icann.org/committees/security/sac040.pdf>>.

시스템 등록. 전자 상거래 상인과 금융기관은 이제 고객이 계정을 관리할 개인 컴퓨터 주소나 IP 주소를 등록할 수 있도록 허용함으로써 개선된 암호 시스템을 보완합니다.

다단계 인증. 전자 상거래 상인, 금융기관 및 (역할을 수행하는) 온라인 게임 운영자까지도 고객에게 계정 로그인 과정에서 고객의 신원을 확인할 두 번째 요소로서 하드웨어 토큰 인증자를 추가하는 옵션을 제공합니다. 토큰은 암호가 나타내는 "사용자가 알고 있는 어떤" 정보에 대해 "사용자가 갖고 있는 무언가"를 더해 줍니다. 이러한 2단계 인증(이중 인증)은 공격자가 도메인 계정에 침입하는 것을 더욱 어렵게 만듭니다. 공격자가 계정 로그인 및 암호를 추측하거나 입수했다 하더라도 토큰도 입수해야 합니다. 오늘날 2단계 인증을 구현한 수많은 사례가 존재하며 매우 많은 고객들에게 해당 기술을 확대하고 있습니다. SSAC는 VeriSign사가 ICANN의 등록기관 평가 프로세스(RSEP)를 통해 등록기관-등록업체 2단계 인증 서비스 제안서를 제출했다고 말합니다. 이 제안서는 등록업체가 자발적으로 제공하는 옵션 서비스로서 "업데이트, 이전 및/또는 삭제 요청을 처리하기 위해 현재 사용되는 사용자 이름 및 암호를 동적인 패스 코드로 보강할 것"을 요구합니다.³⁰ VeriSign이 제안한 단계적 도입의 단계 1에서는 등록기관과 등록업체간에 2단계 인증을 추가하게 될 것입니다. 단계 2에서는 이 서비스를 등록자가 등록업체에 신청하면 이용할 수 있도록 만들 것입니다. 여기에는 등록업체에서 등록기관으로의 EPP(extensible provisioning protocol) 트랜잭션에서 1회용 패스워드를 사용하는 것이 포함됩니다. SSAC는 등록업체들이 이 제안을 검토하고 참여할 때 얻을 수 있는 이익을 고려할 것을 적극 권장합니다. SSAC는 여기에서 설명한 2단계 인증 외에도 미국 국립표준기술원(NIST) - 전자 인증 가이드라인 등과 같은 계정 인증 방법과 가이드라인 또한 고려하도록 등록업체에 권장합니다.³¹

질의 시스템 어떤 금융기관들은 계정을 만드는 과정에서 신원을 확인하는 일련의 질문에 대한 답변을 수집합니다. 기관에서는 이들 질문의 하위 집합을 무작위로 선택하고 그 질문에 답하기 위해 로그인하는 사람에게 질의하기도 합니다. 또 어떤 기관들은 사용자에게 비밀 이미지 및 이미지 설명에 관하여 질의합니다. 고객이 그의 계정으로 처음 로그인할 때 비밀 이미지를 선택해야 합니다. 그런 다음 이미지 설명을 제출합니다. 검증 프로세스가 진행되는 동안 고객은 암호를 입력하라는 요청을 받기 전에 이미지에 대한 설명을 입력해야 합니다. 등록업체들은 이러한 보안 방법을 옵트인(사용자의 사전 동의를 받는) 서비스로 제공하는 것이 좋습니다. 이것은 도메인 이름을 보호하고 DNS 구성의 남용을 방지하기 위한 비용 및 불편에 질의까지 추가되는 것을 감수하고자 하는 고객들을 위한 것입니다.

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

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

도메인 액세스 제어에 따른 인증. 도메인 등록 계정으로 액세스하면 그 계정에 등록된 모든 도메인에, 사용자에게든, 공격자에게든 똑같이 무제한적으로 액세스할 수 있습니다. 실생활에서 흔히 볼 수 있는 등록 계정 액세스 제어 모델은 캐비닛 모델 은행 금고(Bank Safe)입니다. 이러한 유형의 금고는 한 번 개설하면 원하는 대로 훨씬 많은 금고를 개설할 수 있습니다. 이 방법을 안전 금고가 들어 있는 은행 지하금고와 비교해 보십시오. 여기에서 고객이나 침입자는 금고실에 들어가야 할뿐 아니라 각각의 안전 금고 키를 입수해야 합니다. 등록업체는 강화된 보안을 찾는 고객들에게 유사한 액세스 모델을 제공하는 방안을 고려하는 것이 좋습니다. 예를 들어, 오픈 기능은 담당자 정보 및 DNS 확인 정보를 변경하고 도메인 이전을 개시 또는 인증하는 등의 작업을 할 수 있는 담당자를 관리하는 기능을 고객에게 부여하게 될 것입니다.

고유한 여러 명의 담당자. 조직은 도메인 등록 기록에 정확한 담당자를 관리함으로써 이익을 볼 수 있습니다. 특정 조직에서는 각 필수 담당자를 조직내 고유한 개인이나 직책으로 한정함으로써 이익을 볼 수도 있습니다. 이 경우에는 내부자가 고용자나 고용자의 고객의 도메인 이름에 대한 소유권을 주장하거나 하이재킹하려고 시도할 수 있는 위험이 높아집니다. SSAC는 내부자의 도메인 남용을 방지하기 원하는 등록업체에 대하여 이러한 방법들을 추천합니다. 또 이러한 방법들은 등록자를 대신하여 담당자 정보를 관리하려는 등록업체에게는 기회가 될 것입니다. 예를 들어 등록업체는 고유한 담당자 정보를 확인하고 요구할 수 있습니다(특히 오픈 서비스 기능으로 선호되는 통신 수단인 이메일 주소에 대해서). 등록업체뿐 아니라 등록자도 고유한 담당자를 사용하여 세분화된 레벨에서 권한 모델을 만들 수 있습니다. 예를 들어 어떤 조직에서는 등록자의 담당자만이 도메인을 이전할 수 있게 하거나 기술 담당자만이 DNS 구성을 변경할 수 있도록 하려 합니다(기타 모델의 예가 존재하며 이것은 단지 설명에 도움을 줄 목적으로 여기에서 제시한 것 뿐입니다). 등록업체는 등록자들이 이러한 방안을 각각을 처리할 때마다 묻는 인터랙티브 컨퍼메이션(interactive confirmation)이나 복수 수신자 통지 프로세스 등 다른 방안과 결합하여 선택하도록 장려할 수 있습니다.

변경 통지 또는 승인. 일부 조직들은 작업 흐름을 만들어 무단 변경 또는 실수에 의한 변경을 방지합니다. 이 경우 특정 조치가 있을 시에 작업 흐름에 따라 여러 당사자의 승인을 요구하게 됩니다. 다중 승인은 위장에 대한 조직의 방어 기능을 향상시킵니다. 이 경우 공격자는 단 한 명의 당사자가 아니라 두 명을 사회 공학적으로 침입시키거나 위장시켜야 합니다. 어떤 조직에서는 등록업체가 고유한 여러 담당자를 확인하고 요구하는 오픈 서비스에 관심을 가질 수 있습니다. 이와 같이 함으로써 조직들은 내부적으로 사용하는 동종 유형의 작업 흐름을 확장시켜 담당자, 도메인 이전 또는 DNS 구성에 대한 변경을 포괄할 수 있습니다. 이와 같은 작업 흐름을 갖추지 못한 조직인 경우 등록업체는 고객을 대신하여 이와 같은 작업 흐름을 활성화시킬 선택적인 서비스를 제공할 수 있습니다. 예를 들어, 최초 등록시 등록업체의 변경 승인 서비스로 고객이 도메인과 연결된 각 필수 담당자에 대하여 고유한 연락처를 제출했는지 확인할 수 있습니다. 또 고객들이 DNS 구성을 변경하라는 요청을 받으면 어느 담당자에게

이 문서는 더 많은 독자들이 이해할 수 있도록 영문판 원본을 번역한 문서입니다. 국제인터넷주소기구(Internet Corporation for Assigned Names and Numbers, ICANN)는 번역의 진실성을 증명하기 위해 노력했습니다. 영어는 ICANN의 공식 언어이며 이 문서의 영문판 원본은 유일하게 신뢰할 수 있는 공식 문서입니다. 영문판 원본을 원하시면 다음 주소를 방문해 주십시오. <<http://www.icann.org/committees/security/sac040.pdf>>.

통지해야 하는지 선택할 수 있으며, 또는 기술 담당자와 행정 담당자 모두 어느 당사자가 요청한 변경을 수행하기 전에 전화나 이메일로 응답해 줄 것을 요청할 수 있습니다. 또한 변경 승인은 보복적이거나 기회주의적 도메인 이전을 방지하는 데 도움이 됩니다. 예를 들어 담당자로 지명된 피고용자가 조직을 떠났고 조직이 이 피고용자의 연락처 정보를 후임자의 정보로 변경하지 못한 경우를 생각해 봅시다. 만일 피고용자가 불만을 품고 조직을 떠났다면 그는 도메인 이전을 통해 도메인을 되찾으려고 시도할 수도 있습니다. 변경 승인 시나리오에서는 이전을 승인하기 위해 다른 연락처가 필요하며 이전 시도는 차단될 수 있습니다.

복수 수신자 통지. 등록업체에서는 고객들과 연락하기 위하여 이메일을 정기적으로 사용합니다. SAC028, 등록업체 위장 피싱 공격에서는 다음과 같이 흔히 볼 수 있는 여러 가지 통신 연락에 관해 언급합니다.

- 도메인 이름 갱신 공지
- 도메인 이름 주문 승인
- 등록 요청 승인
- 도메인 관리자 및 DNS 정보 변경
- WHOIS 데이터 정확성 리마인더
- 도메인 이름 기한만료 또는 취소 공지
- (신규) 서비스 및 기능에 대한 홍보, 광고

이와 같은 연락 방법을 복수 수신자에게 전송하는 옵션을 제공하면 여러 면에서 고객에게 도움이 될 수 있습니다. 예를 들어 고객은 등록업체 위장 피싱 공격에 희생되는 것을 피할 수 있습니다. 고객의 수신자중 한 명이 피싱 메일에 속을 수 있으나 또 다른 수신자는 위조 이메일임을 알아 보고 등록업체 및 조직내 다른 담당자에게 경고할 수 있습니다. 마찬가지로 등록업체에서 도메인 이름 갱신 통지를 복수 수신자에게 전달한다면 고객의 실수나 간과로 등록이 실패하는 상황에서 보호받을 수 있을 것입니다. 예를 들어 갱신 통지를 받는 사람이 단 한 사람이라면 수신자가 휴가가 연장되어 이메일을 받지 못할 경우 갱신은 실패될 수 있을 것입니다. 복수 수신자 시나리오에서는 다른 수신자가 갱신 통지를 받을 경우 이러한 등록의 실패를 피할 수 있습니다. 또 등록업체는 계정에 대한 무단 액세스를 고객이 파악하도록 도움을 주기 위하여 특정 금융기관에서 사용하는 방법을 고려해 볼 수도 있습니다. 등록업체는 변경이 의도한 것이든, 허위로 제출된 것이든 상관없이, 변경이 효력을 갖기 전에 통신 연락이 전송되든 효력을 가진 후 전송되든 상관없이 올바른 목적지에 도달할 확률을 높이기 위해 연락처 정보의 원본과 변경본을 모두 이용하여 통지나 승인을 전달할 수 있습니다.

중요한 통신 연락의 복수 전달 방법. 등록업체는 고객에게 연락하기 위해 전적으로 이메일에 의존하기보다는 추가적인 보호 방법을 찾는 고객에게 보낼 중요한 통지를 전화, 팩스, 우편 또는 택배 서비스를 통해 전달하는 방안을 제안할 수 있습니다.

이 문서는 더 많은 독자들이 이해할 수 있도록 영문판 원본을 번역한 문서입니다. 국제인터넷주소기구(Internet Corporation for Assigned Names and Numbers, ICANN)는 번역의 진실성을 증명하기 위해 노력했습니다. 영어는 ICANN의 공식 언어이며 이 문서의 영문판 원본은 유일하게 신뢰할 수 있는 공식 문서입니다. 영문판 원본을 원하시면 다음 주소를 방문해 주십시오. <<http://www.icann.org/committees/security/sac040.pdf>>.

이러한 서비스는 공격자의 무단 전송을 매우 어렵게 만들 것입니다. 정말 중요한 도메인 이름을 "영구적으로" 갱신할 것이 예상되는 고객들의 경우 보안 수단을 환영할 것입니다(그리고 대개는 지장이 없습니다). 정말 중요한 도메인의 이전을 실행하는 고객들은 위험/이익 분석을 실시한 후 이전 "트랜잭션"으로 추가되는 지연을 감수할만 것인지 고려할 수 있습니다.

고객 끌기. 수많은 대기업들은 인터넷 액세스, 보안 및 네트워크 관리를 아웃소싱하는 데 익숙해져 있습니다. 관리형 서비스 또한 소규모 기업, 중견기업간에 널리 보급되었습니다. 관리형 서비스 사업자(Managed service providers, MSP)는 고객-사업자 파트너십을 홍보합니다. FAQ나 각성 프로그램 및 웹 세미나나 팟캐스트(인터넷 음악 방송)를 통해 제공되는 교육 등으로 MSP는 자신들이 제공하는 서비스를 고객들이 가장 잘 이용할 수 있는 방법에 대해 소개합니다. 위에서 설명한 방법의 보완책으로서, 등록업체는 등록자를 교육하고 다음과 같이 권장할 수 있습니다.

- 여러 개의 도메인 계정이 있는 담당자를 파악할 것
- 피고용자 리소스 관리 절차에 담당자 정보 관리를 포함시켜 기한이 만료된 피고용자의 자격 증명이 폐기되었을 때 그 피고용자와 연결된 모든 도메인 등록 담당자 정보 또한 변경되도록 할 것.
- 암호 변경 정책을 의무화할 것.
- 주기적으로 연락처를 확인할 것.
- 도메인 이름 등록을 사전 행동적으로 모니터링할 것.
- 등록된 도메인 이름과 다른 도메인으로부터 모든 등록 담당자의 이메일 주소를 할당할 것. (일부 등록업체는 추가적인 보안 조치로서 여러 개의 도메인 등록 계정을 만들기 원할 것입니다.)
- 이전 시도를 보안 이벤트로 취급할 것(검사 및 재검사).
- 등록 담당자 이메일 계정에는 비즈니스 용도로 사용되는 도메인과 다른 별도의 도메인을 사용할 것. 예를 들어 example.info 의 담당자에 대해서는 example.net 에서 이메일 주소를 할당합니다.
- 공유 계정을 만듭니다. 예:
domainadmincontact@example.com, domainregistrantcontact@example.biz,
domaintechnicalcontact@example.net. (공유 계정이 사용될 경우 직원, 관리자가
개입하거나 조직내 운영상의 변화 없이 등록업체 직원이 공유 계정을 모니터링하는지
확인하기 위해 이러한 계정에 대해 주기적으로 검사할 것을 강력히 권장합니다.)

이 문서는 더 많은 독자들이 이해할 수 있도록 영문판 원본을 번역한 문서입니다. 국제인터넷주소기구(Internet Corporation for Assigned Names and Numbers, ICANN)는 번역의 진실성을 증명하기 위해 노력했습니다. 영어는 ICANN의 공식 언어이며 이 문서의 영문판 원본은 유일하게 신뢰할 수 있는 공식 문서입니다. 영문판 원본을 원하시면 다음 주소를 방문해 주십시오.
<<http://www.icann.org/committees/security/sac040.pdf>>.

- 통지용 공유 계정에 대해 복수 수신자 명칭을 붙입니다. 중요한 등록업체 통신 연락의 경우 이러한 형태의 묶음 메일을 사용하여 "종합 배달" 서비스를 제공하십시오. 통신 연락을 적절한 때 수신하고 처리할 확률이 높아집니다.

고객에게 알리기. 등록업체는 기타 경쟁력 있는 제공물과 마찬가지로 제공하는 보안 조치의 종류에 관하여 숨김없이 알리기 위해 노력해야 합니다. 예를 들어 독립 보안 감사기관에 운영 내용을 정기적으로 제출하고 감사를 통과하는 등록업체는 이 자체 규율에 일반인이 주목하도록 만들 수 있습니다. 선택적으로, ICANN와 등록업체가 공동으로 독립 모안 감사기관을 알아 보고 그 감사기관과 계약을 맺어 규정된 일련의 보안 조치를 정의할 수 있습니다. 등록업체는 자사 운영에 대한 감사를 실시할 감사기관을 둘 것을 *자발적으로* 요청할 수 있습니다. 감사를 통과한 등록업체는 몇 가지 형태의 신뢰의 마크 또는 씬을 사용하여 보안 벤치마킹 실습에 합격한 업체로 구분할 수 있습니다. SSL 인증서 발행 기관에서 제공하는 유사한 프로그램을 이용할 수 있습니다.^{32,33} SSAC는 신용카드 처리는 등록업체중 흔히 있는 일이며 여기에서는 상인들을 위한 결제카드 산업의 보안 감사 절차 및 서비스 제공업체의 데이터 보안 기준 요건 준수가 타당할 수 있다고 언급합니다.³⁴

과거 SSAC 보고서에 보고된 방안들. 수많은 등록업체들이 SAC007, 도메인 이름 하이재킹 보고서 5.2절에서 권장하는 *도메인 이름을 보호하기 위해 등록업체에서 취할 수 있는 조치들*을 전부 또는 일부 이행했습니다. 새로 권장하는 조치 및 이전에 권장했던 조치들의 개략적 내용을 제공하기 위해 여기에 요약하였습니다.

1. 등록된 각 도메인 이름에 대하여(각각의 도메인 등록자 계정에 대해서가 아님) 고유한 EPP 국제 도메인 인증 정보 코드값을 사용하십시오. 일부 등록업체는 동일한 등록자가 보유한 모든 도메인에 대해 하나의 EPP 국제 도메인 인증 정보 코드값을 사용합니다. 이 경우 단일 코드를 기반으로 한 하이재킹에 고객이 등록한 모든 이름들이 노출됩니다.
2. 등록업체간에 획일적으로 기본 설정의 도메인 락을 설치하십시오. 수많은 등록업체들이 이미 도메인 이름을 자동으로 잠급니다. 등록업체는 검증된 도메인 이름 등록자의 합법적인 이전 요청을 부당하게 지연시키는 일이 없도록 도메인 락을 잠금 해제하는 직접적인 수단을 충분히 제공해야 합니다.
3. 등록자 기록의 정확성을 향상시킬 수 있는 추가 방법을 조사하십시오. 등록자들이 자신의 정보를 최신 정보로 관리하고 등록의 남용을 발견해 내도록 격려하기 위해 더욱 잦은 연락 또는 다른 형태의 연락 방법(예: 이메일 대신 전화 사용)을 고려해 보십시오.

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/>

이 문서는 더 많은 독자들이 이해할 수 있도록 영문판 원본을 번역한 문서입니다. 국제인터넷주소기구(Internet Corporation for Assigned Names and Numbers, ICANN)는 번역의 진실성을 증명하기 위해 노력했습니다. 영어는 ICANN의 공식 언어이며 이 문서의 영문판 원본은 유일하게 신뢰할 수 있는 공식 문서입니다. 영문판 원본을 원하시면 다음 주소를 방문해 주십시오. <<http://www.icann.org/committees/security/sac040.pdf>>.

4. 비상시 담당자 정보는 등록자, 등록업체 및 재판매업자로부터 도메인 이름 사고 발생시 긴급 복구 대응에 도움을 줄 적절한 당사자의 정보를 수집하십시오.³⁵ 단계적 확대 프로세스(비상 절차)를 정의하여 비상 담당자 부재시 동의하는 모든 당사자들이 사고에 관여할 수 있도록 하십시오.
5. 등록업체의 모든 비즈니스 절차에서 사용되는 인증 및 허가를 개선할 방안을 고려해 보십시오.
6. 도메인 이름의 사기, 위장, 도난을 용이하게 감행하는 데 사용될 수 있는 등록 정보를 보호하십시오. 등록 인증 프로세스에서 사용되는 모든 정보는 기본적으로 개인 정보로 취급합니다. 이 정보를 신용카드나 기타 금융 정보를 보호하는 데 사용되는 수단과 동일하거나 유사한 수단으로 취급하는 방안을 고려하십시오.
7. 재판매업자의 기록 관리 요구사항 준수 여부에 대한 감사 수준을 높이십시오.
8. 재판매업자가 등록업체(및 ICANN)의 기록 관리 요구사항을 이해하는지 확인하고 이러한 요구사항에 대한 준수 수준을 높이십시오.
9. 등록업체에서 제공하는 도메인 잠금 및 도메인 이름 보호 수단에 관하여 등록자에게 분명하고 쉽게 접근 가능한 정보를 제공하십시오.

DNS 구성 정보가 남용되지 않도록 보호하기

도메인 등록 계정에 대한 무단 액세스 권한을 얻으려 하는 한 가지 목적은 조직의 이름 분석 서비스에 대한 통제권을 얻기 위함입니다. 공격자는 이름 또는 타겟의 이름 서버의 IP 주소를 변경하여 공격자가 운영하는 시스템, 즉 보통은 이전에 훼손시켰던 컴퓨터를 가리키게 만듭니다. 공격자는 DNS 서버와 공격받은 도메인 이름에 대한 존 파일을 훼손된 컴퓨터에 호스팅합니다. 공격자의 DNS 서버는 공격받은 도메인의 이름을 분석하여 악의적이거나 가치가 소멸된 웹 사이트(이 문서와 SAC007에서 설명한 Comcast, ICANN, Panix 및 Hush 통신 사고와 마찬가지로)로 리디렉트합니다. 어떤 공격자들은 DNS 구성 정보를 악의적으로 변경하지 않습니다. 오히려 훼손된 도메인 등록 계정을 사용하여 자신의 이름 서버를 다른 합법적으로 운영되는 이름 서버 목록에 추가합니다. 이것은 패스트 플럭스 공격³⁶의 변종인 *더블 플럭스*로 공격자들이 사용하는 이름 서버를 숨기는 역할을 하며 분해를 막을 수도 있습니다. 두 가지 모두 피싱 공격, 스팸 공격, 사기 또는 범죄 공격의 기간을 연장하는 역할을 합니다.

이전 절에서 설명한 방법들은 고객의 도메인 이름 계정을 무단으로 이용하여 DNS 구성 정보를 악의적으로 변경하거나 은밀히 추가하려는 사람들에게 적용할 수 있습니다. 특히,

³⁵ SAC 038 참조, 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>

이 문서는 더 많은 독자들이 이해할 수 있도록 영문판 원본을 번역한 문서입니다. 국제인터넷주소기구(Internet Corporation for Assigned Names and Numbers, ICANN)는 번역의 진실성을 증명하기 위해 노력했습니다. 영어는 ICANN의 공식 언어이며 이 문서의 영문판 원본은 유일하게 신뢰할 수 있는 공식 문서입니다. 영문판 원본을 원하시면 다음 주소를 방문해 주십시오. <<http://www.icann.org/committees/security/sac040.pdf>>.

등록업체에서 옵션 서비스로 제공하거나 등록자가 수행하는 다음 방법들은 DNS 구성 공격에 대한 중요한 보호 장치를 제공하게 될 것입니다.

- DNS 구성 변경에 대한 다단계 인증이 필요합니다.
- 이메일 또는 이메일 외의 미디어를 사용하여 여러 담당자로부터 변경 승인을 받아야 합니다. (참고: 앞서 설명한 동일한 유형의 다단계 검증 방법을 여기에도 적용할 수 있습니다.)
- 변경을 수행했을 때 여러 명의 담당자에게 통지합니다.
- DNS 변경에 이상 또는 남용 사실이 있는지 모니터링합니다.

재차 말하지만 FAQ, 훈련 및 교육을 통해 등록업체는 고객들이 DNS 구성 활동(변경 및 추가)을 정기적으로 모니터링하도록 장려해야 합니다. 또 등록업체는 고객들이 도메인내의 이름이 의도했던 IP 주소로 분석되는지 확인하도록 권장해야 합니다. 또 등록업체에서는 고객들이 모든 도메인에 대한 DNS 구성 이력을 관리하도록 강조해야 하며 타임스탬프와 디지털 서명을 이 정보에 사용하는 것이 왜 가치가 있는지 이해하도록 도움을 줘야 합니다.

발견 사실

이 보고서에서 다룬 사고 및 관련 연구로부터 SSAC는 다음과 같은 추가 사실을 발견하게 되었습니다.

발견한 사실(1) 등록업체의 공격에 대한 취약성과 도메인 계정에 대한 공격에 대비해 등록업체들이 제공하는 보호 정도에 관해서는 차이가 존재합니다. 많은 도메인 등록자들은 등록업체가 공격 및 DNS 구성의 악의적 변경으로부터 도메인 계정을 어느 범위까지 보호할 수 있는지 평가할 만한 충분한 정보를 갖지 않은 것으로 보입니다.

발견한 사실(2) 소비자 중심의 도메인 이름 등록 서비스를 제공하는 대단히 많은 등록업체와 타겟이 주로 되는 큼직한 도메인 이름 소유자에게 보안 서비스를 제공하는(보통 전반적인 브랜드 자산가치 보호 서비스의 일환으로) 소수의 등록업체 및 "브랜드 경영" 조직들은 존재하지만 SSAC는 “순수 보안” 등록 서비스 제공업체는 드물다는 사실을 알게 되었습니다. 이것은 부분적으로는 보안 수단의 평가가 고객이 등록업체를 선정할 때 내리는 결정에 중요한 역할을 하지 못한다는 사실 때문입니다.

발견한 사실(3) 등록업체들은 보안 서비스에 관한 더 많은 정보를 입수할 수 있도록 만들어 고객들이 현명한 결정을 할 수 있게 도움을 줄 수 있습니다. 독립 보안 감사에 대한 자발적 운영 제출과 감사의 성공적인 결과를 공개하는 것은 고객이 비용 및 기타 보조 기능(웹 및 DNS 호스팅 등)외에도 보안 요구사항 위주로 등록업체를 선정하는데 도움을 줄 것입니다.

발견한 사실(4) 등록업체 서비스(및 등록자)는 계정 로그인에 대해서는 방법상의 장점보다도 1단계 인증을 더 많이 신뢰합니다. 이러한 인증 방법은 다양한 형태의 사회 공학적 침입 수단, 무차별 대입 공격(brute force) 및 기타 기법을 사용한 교묘한 함정에 반복적으로 당해 왔습니다.

발견한 사실(5) 공격자들은 도메인 등록 계정을 계속적으로 훼손시킬 때 DNS 구성을 타겟으로 삼았습니다. DNS의 분산적인 성격 때문에 DNS 구성 정보를 변경한 효과는 등록업체의 복구 및 위기 완화 노력 이후까지 지속되었습니다. 악의적이거나 부정확한 DNS 정보는 변경된 DNS 리소스 기록과 연결된 TTL 값의 전체 지속 기간동안 인터넷 도처에서 지속될 수 있습니다. 이러한 목적을 달성하기 위해 공격자들은 특히 TTL을 변경할 수 있습니다.

발견한 사실(6) 보통 사용자가 등록 계정 포털이나 로그인에서 인증을 받게 되면 그 사용자(즉, 사기꾼)는 **글로벌**한 권한을 얻게 되며 DNS 구성 정보는 물론 연락처 정보도 변경할 수 있습니다. 세분화된 액세스 관리 - 특히 연락처와 DNS 구성 정보 변경 및 정당한 이전에 관해 각 담당자가 수행할 수 있는 조치 유형을 제한할 수 있는 기능 - 를 옵션 서비스로 고객이 이용할 수 있도록 만들면 도메인 이름과 그 이름에 연결되는 이름 분석 서비스를 불법 이용하거나 오용할 위험을 줄이거나 경감시킬 수 있습니다.

발견한 사실(7) 등록 서비스 제공업체는 보안과 관련된 통신문(예: 변경 통지)을 전달하기 위하여 이메일 전달 보증 및 보안 특성의 장점보다는 미확인 이메일에 의존하는 경우가 훨씬 더 많습니다. 공격자들은 훼손된 등록 계정을 통해 도메인의 DNS 구성을 변경할 때 종종 이메일 전달을 방해함으로써 이러한 통신 방법을 공격합니다. 대체 연락 매체에 대한 선택권을 고객에게 제공하거나 몇 가지 형태의 수신 확인 등을 포함하도록 통지 서비스를 확대하면 도메인 이름과 그 이름에 연결되는 이름 분석 서비스를 불법 이용하거나 오용할 위험을 줄이거나 경감시킬 수 있습니다.

권장사항

SAC007은 등록업체를 위한 특수 권장사항으로 작성되었습니다. 그 중에서 특히 주목할 만한 몇 가지를 소개합니다.

권장사항 SAC007-(8): 등록업체는 도메인 이름 하이재킹 및 등록자 위장과 사기 위협에 대한 등록자의 인식을 개선시켜야 합니다. 또한 등록자가 등록 정보를 정확히 관리할 필요성을 강조해야 합니다. 등록업체는 등록자에게 등록업체 락(Registrar-Lock)의 이용 가능성과 목적을 알려야 하며 사용을 장려해야 합니다. 등록업체는 등록자에게 인증 메커니즘(EPP 국제 도메인 인증 정보)에 관한 정보를 추가로 제공해야 하며 정기적인 도메인 이름 상태 모니터링, 시기 적절하고 정확한 연락처 관리 및 인증 정보 관리를 포함, 등록자의 도메인을 보호하기 위한 권장 관리 기준을 개발해야 합니다.

최근 사고, 관련 연구, 발견한 사실들에 대한 분석을 기반으로 SSAC는 다음과 같은 권장사항을 제정하였습니다.

권장사항 (1) 등록업체는 도메인 이름 등록 서비스의 불법 이용이나 오용에 대비한 강력한 보안 수준을 원하거나 필요로 하는 고객에게 제공하는 것이 좋습니다. 이 보고서에서 열거한 방법들을 개별적으로, 혹은 번들로 묶어서 고객에게 옵션 서비스로 제공할 수 있습니다.

권장사항 (2) 등록업체는 보안 인식을 포함하여 등록자에게 제공하는 기존의 FAQ 및 교육 프로그램을 확대해야 합니다. 등록업체는 도메인 등록 계정을 보호하기 위해 업체에서 제공하는 서비스와 관련된 정보에 고객이 접근하기 쉽도록 만들어 고객들이 등록업체를 선택할 때 보호 수단에 관한 현명한 결정을 내릴 수 있도록 해야 합니다.

권장사항 (3) 등록업체는 보안 실사의 한 구성 요소로서 업체의 운영에 대해 독립 보안 감사를 자발적으로 수행하는 의의에 대해 생각해 봐야 합니다.

권장사항 (4) ICANN과 등록업체는 등록업체의 신청에 의해 규정된 일련의 보안 수단을 위주로 보안 감사를 수행할 인증된 독립 감사기관을 돕으로써 등록 서비스가 대체로 개선되고 등록자들이 이익을 보게 될 것인지 여부를 조사해야 합니다. ICANN은 SSL 인증 발행 기관에서 기관의 보안 기준을 충족시키는 웹 사이트 운영자에게 신뢰 마크나 씬을 제공하는 것과 유사한 방법으로 수행되는 신뢰받는 보안 마크 프로그램을 통해 이러한 보안 감사 벤치마킹을 자발적으로 이행하는 등록업체를 식별할 것입니다.

이 문서는 더 많은 독자들이 이해할 수 있도록 영문판 원본을 번역한 문서입니다. 국제인터넷주소기구(Internet Corporation for Assigned Names and Numbers, ICANN)는 번역의 진실성을 증명하기 위해 노력했습니다. 영어는 ICANN의 공식 언어이며 이 문서의 영문판 원본은 유일하게 신뢰할 수 있는 공식 문서입니다. 영문판 원본을 원하시면 다음 주소를 방문해 주십시오.
<<http://www.icann.org/committees/security/sac040.pdf>>.

감사의 글

본 주제에 관한 SSAC의 연구가 진행되는 동안 시간을 내어 기고해 주시고 검토해 주신 다음 회원분들께 감사의 뜻을 전합니다.

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

관심분야 설명

SSAC 회원의 약력과 관심 분야 설명을 보시려면 다음 주소를 방문하십시오.

<http://www.icann.org/en/committees/security/biographies.htm>.

이의

위원회 회원 중 이 보고서의 간행에 이의를 제기한 회원은 없었습니다.

이 문서는 더 많은 독자들이 이해할 수 있도록 영문판 원본을 번역한 문서입니다. 국제인터넷주소기구(Internet Corporation for Assigned Names and Numbers, ICANN)는 번역의 진실성을 증명하기 위해 노력했습니다. 영어는 ICANN의 공식 언어이며 이 문서의 영문판 원본은 유일하게 신뢰할 수 있는 공식 문서입니다. 영문판 원본을 원하시면 다음 주소를 방문해 주십시오. <<http://www.icann.org/committees/security/sac040.pdf>>.

2009년 8월 19일

페이지

28 / 28