infoblox®

유사 공격에 대한 심층 분석

새로운 연구, 최신 위협 벡터 밝혀내

2023년 4월

유사 도메인 표적 모두

목차

요약

이미 인터넷 초창기부터 위협 행위자들은 비슷해 보이는 도메인으로 사용자를 속여 악성 웹사이트를 방문하도록 유도해 왔습니다. 유사 도메인이라고 하는 이러한 도메인은 피싱 공격과도 같으므로, 보안 인식 교육에는 이러한 도메인에 대한 링크 검사 방법을 배우는 것이 포함됩니다.

그러나 인식 제고 캠페인과 기술 발전에도 불구하고 유사 도메인은 소비자와 조직에 지속적인 위협으로 작용하고 있으며, 위협 행위자들은 그 전략을 끊임없이 바꿔서 공격을 지속하고 있습니다. 소비자부터 정부, 주요 소매 브랜드부터 소규모 레스토랑, 세계적으로 유명한 기술 기업부터 우리 회사처럼 잘 알려지지 않은 기업까지, 모두가 공격 대상입니다. 이 백서에서는 실제 도메인과 캠페인의 예를 통해 '모두가 표적'이라는 사실을 확인할 수 있습니다. 틈새 산업에 속한 소기업인 Infoblox조차 표적이 되고 있습니다.

이 보고서는 산업 및 사용자 그룹 전반의 실제 사례를 보여줌으로써 현재의 위협 환경을 설명합니다. Infoblox는 수년간 유사 도메인을 탐지해 왔으며 매일 700억 건 이상의 도메인 이름 시스템(DNS) 이벤트를 분석하여 새로운 잠재적 위협을 찾아내고 있습니다. 이 백서에서는 2022년 1월부터 2023년 3월까지의 탐지에 중점을 두었습니다. 30만 개가 넘는 looKaliKe 도메인중에서 이러한 공격과 관련된 도전 과제와 위험을 강조하는 세트를 선별했습니다.

유사 도메인은 많은 경우 이메일 스팸, 광고, 소셜 미디어 및 SMS 메시지를 통한 불특정 다수의 소비자 대상의 광범위한 공격과 관련됩니다. 매일 소프트웨어, 금융 기관 및 택배 배송 서비스를 사칭하는 수천 개의 새로운 도메인이 등록됩니다. 사용자의 자격 증명을 도난하거나 컴퓨터에 멀웨어를 감염시키는 것을 목표로 하는 피싱 공격은 너무 만연하며 허술한 경우가 많아서 "이메일만 안 열면 피싱 사기 당할 일도 없지롱" 같은 수많은 밈의 원천이 되었습니다. 우스꽝스럽게 묘사되는 경우가 많지만 피싱은 상당한 규모의 산업입니다. APWG(Anti-Phishing Working Group)는 2022년 3분기에 피싱이 기록적인 수준에 도달했다고 보고했습니다.[1]

[ ] **이 백서의 모든 도메인은 악의적이든 정상적이든 변조되었습니다. 마침표 주위에 괄호를 배치하여(*[.]*) 클릭 가능한 링크가 되지 않도록 도메인을 변조했습니다.**

700억 건 이상

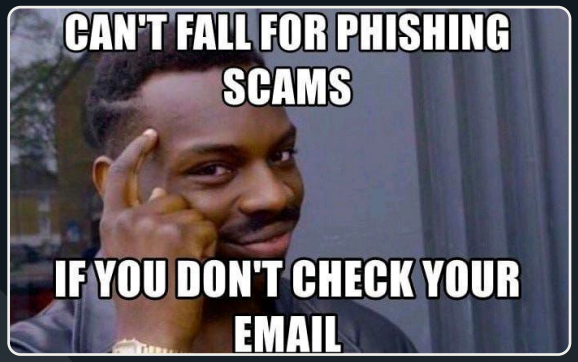
Infoblox는 매일 700억 건 이상의 DNS 이벤트를 분석하여 새로운 위협을 식별합니다.

30만 개 이상

이러한 공격의 어려움과 위험을 강조하기 위해 이 보고서용으로 선별된 유사 도메인의 수.

피싱 밈의 예시.

2019년에 작성된 이 트윗이 그 예입니다.[2]



이미지 출처: 이 밈의 출처는 알 수 없음

하지만 유사 도메인은 소비자에게만 위협이 되는 것이 아니라 기업 네트워크에 대한 액세스 권한을 획득하는 데에도 사용됩니다.

최근 공개된 정보에 따르면 악의적인 공격자가 직원을 속여 다단계 인증(MFA) 자격 증명을 제공하도록 유도한 표적 공격이 발견되었습니다. 대부분의 경우 유사 도메인은 회사를 사칭할 뿐 아니라 MFA 키워드를 포함하고 있어 연결이 안전하다는 직원의 착각을 더욱 확고히 했습니다. 공격자들은 전 세계의 인터넷 서비스 제공업체, 은행 및 암호화폐, 소프트웨어 및 서비스, 보험사 등 다양한 업종에 걸쳐 크고 작은 기업을 표적으로 삼고 있는 것으로 나타났습니다. 이러한 공격은 2022년 초에 시작되어 시간이 지날수록 더욱 확산되고 있습니다.

유사 도메인 사용으로 수익을 얻을 수 있는 이유는 이 공격이 비대칭 공격이기 때문입니다. 사용자는 자신의 재정과 고용주의 정보를 보호하기 위해 항상 경계를 늦추지 말아야 합니다. 저렴한 도메인 등록 가격과 대규모 공격 분산 능력은 행위자에게 유리하게 작용합니다. 공격자는 규모의 이점을 보유하며, 악의적인 활동을 식별하는 기술이 지난 몇 년간 발전했음에도 불구하고 공격을 방어하는 쪽에서는 공격자들을 따라잡기 위해 고군분투하고 있습니다.

유사 피싱이 번창하고 있을 뿐만 아니라 유사 피싱의 사용이 더욱 복잡해지고 있습니다. 이는 DNS 레코드에서 가장 명확하게 드러납니다. Infoblox의 조사에 따르면, 유사 도메인은 기존의 피싱 및 타이포스쿼팅 목적 외 다양한 용도로도 활용되고 있으며, 네임서버나 스피어 피싱 메일 배포 등 이전에 보고되지 않은 방식으로도 사용되고 있습니다. 유사 도메인만 호스팅하며 소비자와 정부 직원 모두를 대상으로 삼는 탄력적인 대규모 네트워크도 존재합니다.

Infoblox는 여러 알고리즘을 사용하여 유사 도메인을 식별합니다. 당사는 쇼핑, 은행, 소프트웨어 및 금융 부문에서 자주 대상이 되는 표적의 변종 감시, 고객이 지정한 도메인의 변종 감시, 유사 도메인을 전문으로 하는 DNS 인프라 행위자 감시 등 여러 방법을 병용합니다. 이러한 다각적인 접근 방식을 통해 위협 환경을 폭넓게 파악할 수 있습니다.

중요 참고 사항: 이 보고서에는 실제로 존재하는 유사 도메인의 폭과 깊이를 보여주는 여러 예가 포함되어 있으며, 이러한 예시는 특정 주체의 성공적인 공격 또는 위반을 암시하지 않습니다.

배경

다른 우수한 연구 논문과 마찬가지로 이 백서도 몇 가지 배경 정보로 시작합니다. 대부분 용어들인데, 대다수의 독자가 배경 부분은 건너뛴다는 사실을 잘 알고 있으므로 간략하게 작성했습니다.

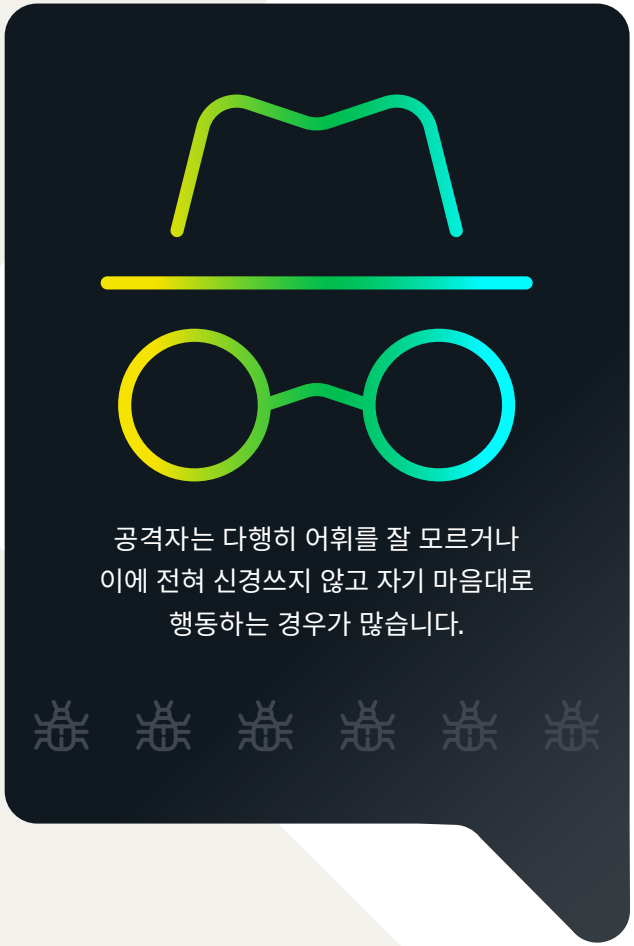
악성 유사 도메인(알려진 도메인과 동일하거나 매우 유사하게 보이는, 공격자가 등록한 등록 도메인)은 익히 알려져 있으며 지속적으로 발생하는 사이버 환경 내 위협입니다. 일반적으로 유사 도메인은 공격적일 뿐 아니라 방어적으로도 사용됩니다. 공격적으로는 사람의 시선이 닿는 모든 곳에서 속임수를 쓰는 데 사용됩니다. 공격자는 유사 도메인을 사용하여 돈을 훔치거나, 자격 증명 또는 액세스 권한을 획득하거나, 개인 식별 정보를 수집하거나, 멀웨어를 배포하거나 광고 수익을 얻고자 시도합니다. 유사 도메인은 정치적 목적이나 브랜드 평판을 훼손하기 위한 목적으로도 사용됩니다. 요약하자면, 사이버 범죄자들에게 유사 도메인은 목적을 달성하기 위한 수단입니다. 방어적인 사용으로는 많은 조직이 공격자의 도메인 소유 및 사용을 방지하기 위해 자사 도메인과 유사한 도메인을 미리 등록하는 경우가 있습니다.

유사 도메인은 다양한 형태로 나타납니다. DNS 분야에서 유사 도메인은 다음과 같은 특징을 지닐 수 있습니다.

- **호모그래프**
- **타이포스쿼팅**
- **콤보스쿼팅**
- **사운드스쿼팅**

원래 표적 도메인과 거의 구별할 수 없거나 객관적으로 매우 뚜렷하게 구별될 수 있습니다. 유사 도메인이 공격 벡터로서 성공을 거둘 수 있었던 이유는 많은 부분 개인에게 가해지는 부담 때문입니다.

이어지는 내용에서 다루겠지만, 유사 도메인은 이메일 발신자 주소부터 피싱 URL, 멀웨어 명령 및 제어(C2)에 이르기까지 공격의 모든 요소에서 발견됩니다. 유사 도메인은 일반적으로 주소 레코드(A/AAAA)와 관련이 있지만, 네임서버(NS), 포인터(PTR) 및 Canonical Name(CNAME) 레코드에 사용되는 유사 도메인도 발견되었습니다. 이러한 유사 도메인은 이메일, SMS, 문자 메시지, 보안이 침해된 웹사이트, 악성 광고 네트워크, 전화 통화 등을 통해 배포될 수 있습니다. 다음 섹션에서는 다양한 형태의 유사 도메인에 관해 간략하게 설명하고 각각의 예를 살펴봅니다.



이게 다 타자기 때문이야

사실 오늘날 이 문제의 근원은 타자기가 처음 등장한 시대까지 거슬러 올라갈 수 있습니다. 많은 오래된 타자기에는 0 또는 1 키가 없었는데, 타이피스트가 대문자 O와 소문자 L을 사용하여 이 숫자들을 입력할 것으로 예상되었기 때문입니다.[4]

호모그래프(동형의이어, 원래HOMOGLYPHS)

영어로 호모그래프(동형이의어)라는 단어는 "철자가 같지만 반드시 동일하게 발음되는 것은 아니며 의미가 다른 두 단어"를 의미하지만, 동형이의어라는 용어는 오랫동안 보안 연구 문헌에서 "시각적으로 동일하게 보이는 두 도메인"이라는 의미로 사용되어 왔습니다.[3] 더 정확한 용어는 homoglyph입니다. 이러한 도메인은 서로 비슷하게 보이며 경우에 따라 구별하기 어려울 수도 있습니다. 연구 문헌과의 일관성을 위해 이 문서에서는 잘못된 용어인 '호모그래프'를 그대로 사용합니다.

이러한 형태의 유사 도메인은 동일한 문자 집합 또는 알파벳의 여러 문자가 서로 비슷하게 보인다는 사실을 악용합니다. 예를 들어 0(숫자 0)과 O(대문자 "o"), 또는 "l"(소문자 "L")과 "I"(대문자 "i")가 있습니다. 일부 글꼴은 이 문제를 더욱 악화시킵니다. 대표적인 예로 g0ogle.com과 Infoblox.com을 들 수 있는데, 여기서 Google의 'o'는 0으로, Infoblox의 'i'는 소문자 'L'로 각각 대체됩니다.

인터넷의 발전에 따라 월드 와이드 웹에 로그인하는 영어 화자가 아닌 사람들이 증가하면서 IDN(다국어 도메인 이름)의 필요성이 커졌습니다. IDN은 라틴어가 아닌 스크립트로 된 문자를 하나 이상 포함하는 도메인입니다. 유니코드의 도입으로 이러한 도메인이 부상할 수 있었습니다. IDN과 함께 새로운 형태의 유사 문자인 IDN 호모그래프도 등장했습니다. 이러한 호모그래프는 homogrαph이지만, 다른 문자 집합의 문자나 비슷해 보이는 알파벳이 사용됩니다. Gabrilovich와 Gontmakher는2002년 논문 "The Homograph Attack"에서 IDN hoмograph의 강력함을 보여주었습니다. 저자들은 실제 Microsoft 도메인인 microsoft[.]com에 대해 키릴 문자 "c"와 "o"를 포함하는 유사 도메인을 등록했습니다.[5] 결과적으로 도메인 www.microsoft[.]com은 실제 Microsoft 도메인과 시각적으로 구별할 수 없었습니다.

Unicode Consortium은 특정 문자열에 사용할 수 있는, 혼동하기 쉬운 여러 문자를 보여주는 도구를 출시했습니다.[6] 문자열 “hi”에 사용할 수 있는 유니코드 문자 변형은 무려 684가지입니다. “infoblox”와 같은 문자열의 경우 이 수는 2조 2천억 개 이상으로 늘어납니다.어떤 변형은 유사 도메인에 상대적으로 덜 효과적입니다. 예를 들어, Unicode Consortium은“৯”(확장된 아랍어-인도 숫자 '5')를 “o”(라틴 소문자 “O”)와 혼동될 수 있는 문자로 등록했습니다.

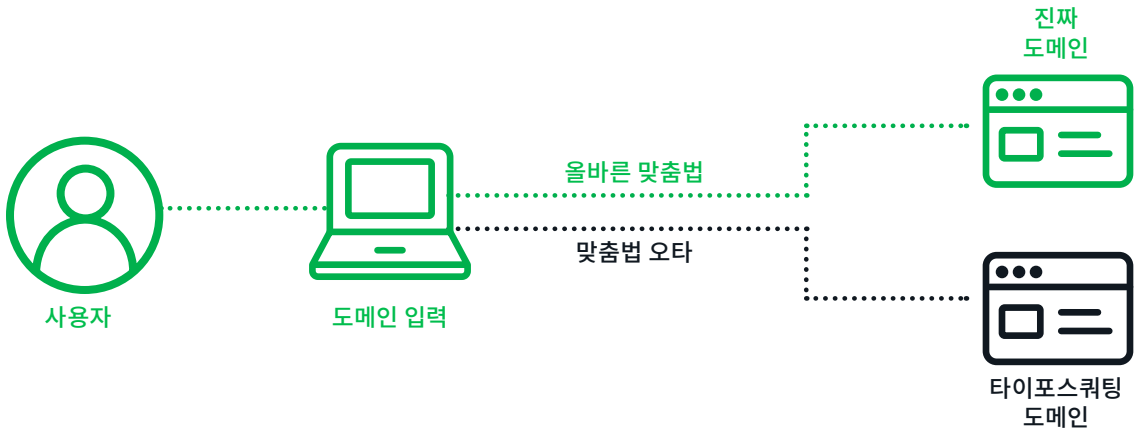
분명히, *infৡblৡx[.]com*은 그다지 효과적인 유사 도메인이 아닙니다. 그러나 일반적으로 사용되는 *Arial* 글꼴로 표시된 경우 올바른 도메인인 *{infoblox[.]com} and {infoblox[.]com}*(벨로러시아어 또는 우크라이나어 소문자 *"i"*와 아르메니아어 소문자 *"vo"*를 *"n"* 대신 입력한)과의 차이점을 알 수 있을까요? 저희조차 이를 구별할 수 없습니다.

타이포스쿼팅

타이포스쿼트 도메인은 인기 있는 도메인 이름과 사용자의 오타 또는 고장난 키보드로 입력할 때 발생하는 입력 오류를 악용합니다. 이 용어는 일반적으로 광고 수익 창출을 목적으로 등록했지만 사용되지 않는 도메인과 관련됩니다. 예를 들어, 저희 저자 중 한 명은 최근 appfolio[.]com(자산 관리 그룹과 임대인에게 SaaS 솔루션을 제공하는 유명 소프트웨어 회사)을 통해 호스팅되는 자산 관리 그룹의 온라인 포털에서 임대료를 지불하려고 했습니다. 하지만 오타를 내는 바람에 하마터면 appfollio[.]com을 방문할 뻔했습니다. 이 도메인은 2013년에 등록되었지만 현재 사용되지 않습니다.

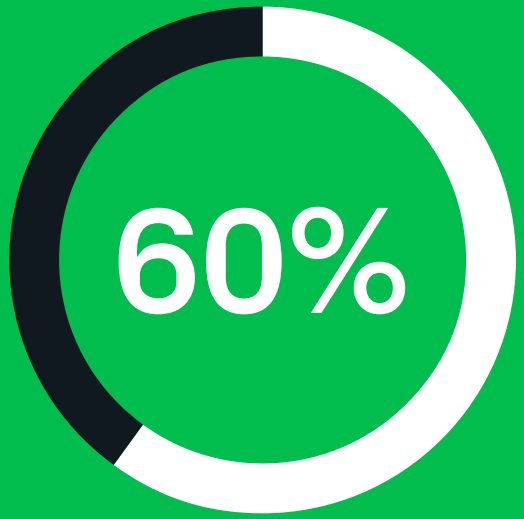
흥미롭게도 Appfolio의 또 다른 타이포스쿼트 도메인인 apfolio[.]com은 Appfolio의 소유로 보입니다. 이 도메인은 올바른 도메인으로 리디렉션되고, 등록자, 등록 조직 및 등록 기관이 동일하며, 올바른 도메인이 appfolio[.]com이 등록된 지 한 달 만에 등록되었습니다. 이는 방어적인 유사 도메인 사용의 예입니다. 안타깝게도 조직이 모든 유사 변형을 등록하기에는 가능성이 너무 많으므로 악의적인 행위자가 유리합니다.

타이포스쿼트는 주로 수익 창출 방법으로 인식되지만, 범죄 목적으로 악용될 수 있습니다. 타사 광고를 판매하거나 합법적인 도메인 소유자에게 판매하는 데 사용되기도 하나, 추후 설명할 "블랙햇" 제휴 마케팅 프로그램이나 멀웨어 C2 도메인으로도 사용될 수 있습니다. 브랜드와 회사는 사이버스쿼팅 방지 소비자 보호법에 따라 타이포스쿼팅에 대한 민사 보호를 받습니다. 이러한 법적 조치의 위협으로 인해 도메인 플리핑/파킹 커뮤니티에서 타이포스쿼트는 일종의 수익 창출 "블랙햇"으로 간주되며, iGoldrush와 같은 진지한 도메인 플리퍼들은 수익 창출 목적의 타이포스쿼팅을 하지 말도록 권장합니다.[7]



타이포스쿼팅의 예시

gikthub[.]com
5whatsapp[.]com
Hdfcbank[.]vip
royalbsank[.]com
sportybet[.]city
bamgkokbank[.]com
1337x[.]asia
moneycont5rol[.]com



1,000일 이상 활성화된 악의적인 콤보스쿼팅 도메인의 비율

최초 발견 후 100일 후에 하나 이상의 공개 차단 목록에 등재된 악성 콤보스쿼팅 도메인의 비율

콤보스쿼팅

콤보스쿼팅은 인기 브랜드나 회사 이름을 다른 키워드와 결합한 유사 도메인입니다. 이러한 키워드로는 support, help, security, and mail과 같은 용어가 자주 사용됩니다. 예를 들어, wordpresssupport[.]ru, wordpresssupport[.]store, wordpress-security[.]cloud 등이 활용됩니다. 이러한 도메인은 모두 러시아의 동일한 IP 주소에서 호스팅되며, 인기 웹 콘텐츠 소프트웨어인 WordPress와 비슷해 보입니다. support와 security가 포함된 도메인 이름은 WordPress 사용자용임을 나타냅니다. 이러한 도메인은 WordPress 사이트를 하이재킹하기 위해 자격 증명을 수집하거나 결제 세부 정보 및 상세 개인식별정보(PII)를 수집하는 데 사용될 수 있습니다.

행위자는 콤보스쿼트 도메인을 직접 생성할 뿐 아니라 사전 도메인 생성 알고리즘(DDGA)을 사용하여 유사 도메인을 생성할 수도 있습니다. 이 방법을 사용하면 단 몇 초 만에 수많은 브랜드나 회사의 후보 도메인을 수없이 생성할 수 있습니다. 운이 좋으면 알고리즘이 도메인에 적합한 키워드만으로 후보 도메인을 생성할 수 있습니다. 최고의 게임 플랫폼인 Steam의 사용자 커뮤니티는 콤보스쿼트 DDGA를 사용하는 행위자들이 주로 공략하는 표적입니다. 최근에 관찰된 도메인 세트의 예로는 steamcommiunity[.]com[.]ru, steamcommucnity[.]com[.]ru, steamcommunityjp[.]top, steamcommunityiq[.]top 등이 있습니다. 참고로 이 도메인 세트에서는 타이포스쿼팅과 콤보스쿼팅이 공존합니다.

Kitsin 등은 2017년에 콤보스쿼팅에 관한 종단 연구를 수행하여 약 4680억 개의 DNS 레코드(액티브 및 패시브 데이터 세트 모두에서 추출)를 분석한 결과, 충격적인 결과를 발견했습니다.

- **콤보스쿼트 도메인은 타이포스쿼팅 도메인보다 100배는 더 만연합니다.**
- **악의적인 콤보스쿼팅 도메인의 60%가 1,000일 이상 활성화된 상태입니다.**
- **악의적인 콤보스쿼팅 도메인의 20%가 최초 파악으로부터 100일 후에 하나 이상의 공개 차단 목록에 등재되었습니다.**
- **콤보스쿼트 도메인은 전년 대비 더 많이 파악되었습니다.[8]**

***Infoblox*는 콤보스쿼트 도메인의 보급에 관한 저자들의 결론에 동의합니다. 저희 분석에 따르면, 순수 타이포스쿼트나 순수 호모그래프(*IDN* 등)보다 콤보스쿼트 도메인이 더 많이 발견되었습니다.**

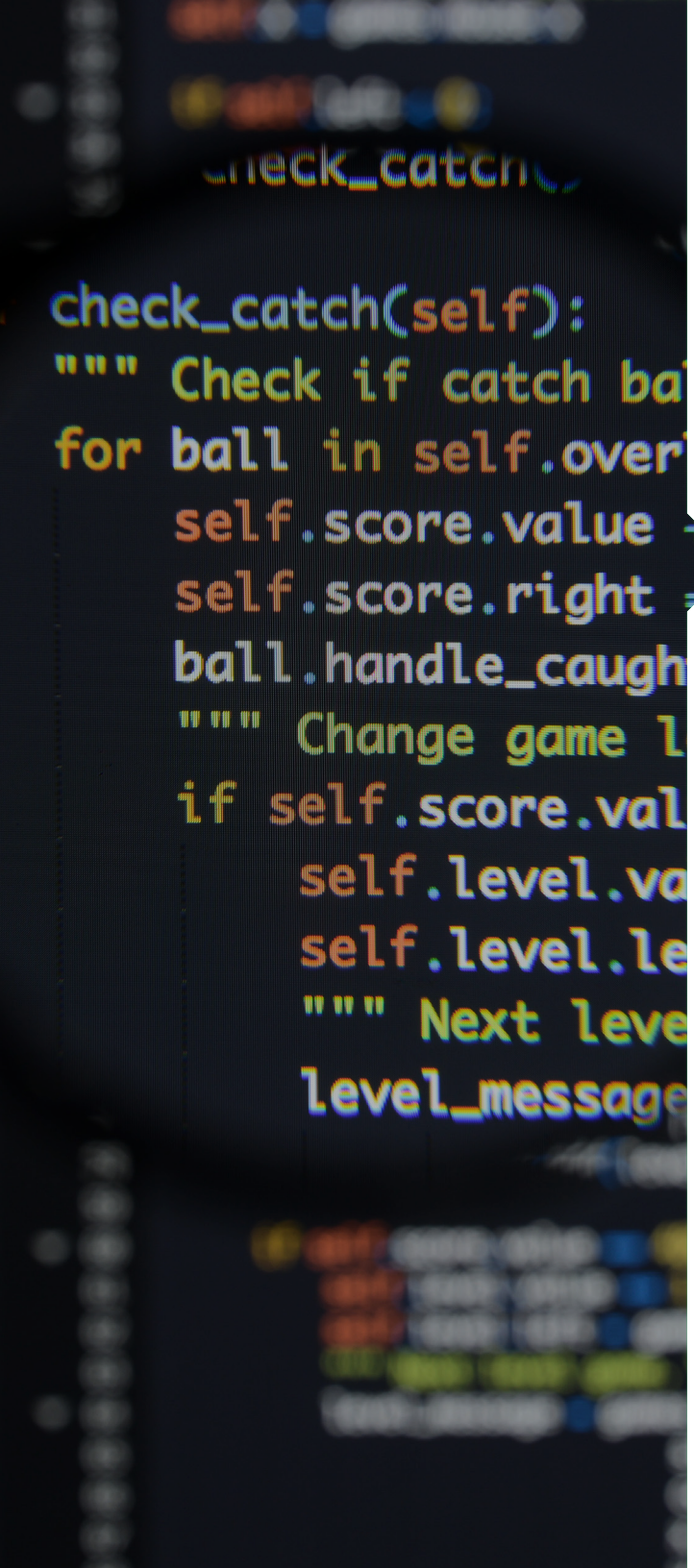
사운드스쿼팅

사운드스쿼트 도메인은 소리는 같지만 철자가 다른 단어인 동음이의어의 사용을 활용합니다. 사운드스쿼팅(Soundsquatting)은 2014년 문헌에 처음 등장했으며, 가장 최근에 확인된 형태의 유사 도메인입니다.[9] 사운드스쿼팅은 최근 Alexa, Siri, Google Voice와 같은 스마트 스피커의 확산으로 인해 연구자에게 더 많이 주목받고 있습니다.[10] 사운드스쿼트 도메인은 비슷하게 들리고 보일 수 있다는 점에서 여타 유사 도메인 유형과 겹치는 부분이 있습니다. Infoblox는 순수한 사운드쿼팅 도메인, 즉 시각적으로 비슷하지는 않지만 비슷하게 들리는 도메인은 드물다는 것을 발견했습니다. 일반적으로 이러한 도메인은 텍스트 기반 유사성 기술로도 찾을 수 있습니다.

참고로 현존하는 유사 도메인은 저희가 제시한 분류에 딱 맞지 않는 경우가 많다는 점에 유의해야 합니다. 유사 도메인의 효과를 극대화하기 위해 여러 양식이 병용됩니다. 파악된 콤보스쿼트 도메인 중 다수는 타이포스쿼트 및 호모그래프(IDN 또는 기타)의 요소도 포함합니다. 예를 들어 타이포스쿼트가 호모그래프의 요소를 활용하고, 사운드스쿼트가 타이포스쿼트의 요소를 활용하는 식입니다. 이로 인해 공격자가 방어자보다 앞서나가는 비대칭적인 위협 환경이 조성됩니다.

소리를 악용한 공격

Alexa, Siri, Google Voice와 같은 음성 인식 기술이 등장하면서 사운드스쿼팅이 급격히 확산되었습니다.



기타 유사 도메인 형태

이 백서에서는 유사 도메인 및 현재의 위협 환경에서 유사 도메인이 어떤 역할을 하는지에 초점을 맞추지만, 취약한 사용자를 악용할 수 있는 다른 유형의 유사 도메인도 존재합니다. 그 중 주목할 만한 하나의 예는 최근 파이썬 PyPi 패키지에서 발견되었습니다.

https://infosec.exchange/@tweedge@cybersecurity.theater/109846797159938702

Python과 같은 인기 프로그래밍 언어의 패키지 관리자는 도메인과 동일한 약점이 있습니다. 즉, 누구나 보안 위험이 있을 수도 있고 없을 수도 있는 코드가 포함된 패키지를 어떤 이름으로든(해당 이름이 이미 사용되지 않는 한) 업로드할 수 있습니다. 2016년에 보안 연구원 Nikolai Tschacher는 이러한 방식으로 타이포스쿼팅을 사용하여 17,000개 이상의 별도 호스트가 임의의 코드를 실행하도록 했습니다.[11] 또한 2021년에 보안 연구원 Alex Birsan은 Tschacher의 아이디어를 확장하여 "종속성 혼동"이라는 용어를 고안했습니다.[12]

Birsan은 여러 오픈 소스를 통해 주요 기업의 비공개 내부 패키지 이름을 찾아냈습니다. 여기에는 웹사이트에서 소스 코드를 탐색하고, GitHub에서 패키지를 찾거나 공개 포럼에서 패키지 이름을 찾는 것도 포함됩니다. 그런 다음 Birsan은 비공개 내부 패키지와 같은 이름의 패키지를 공개 패키지 관리자에 업로드했습니다. 마지막으로 Birsan은 자동화된 CI/CD 파이프라인을 활용하여 공개 패키지와 비공개 내부 패키지를 '혼동'시켰습니다. 자동화된 파이프라인은 비공개 패키지를 가져와 설치하는 대신 Birsan의 공개 패키지를 찾아서 가져왔습니다. 그런 다음 Birsan은 DNS 유출을 사용하여 의도된 비공개 패키지가 아닌 임의의 코드가 실행되었음을 알렸습니다. Birsan은 이러한 유사 도메인 기술을 통해 35개의 조직을 침해할 수 있었으며, 때로는 패키지를 업로드한 지 몇 시간 만에 침해에 성공하기도 했습니다.

유사 도메인의 유형이나 유사 도메인이 사용되는 전문 분야에 관계없이 유사 도메인은 지속적인 위협입니다. 유사 도메인을 연구하는 데 따르는 어려움 중 하나는 정의되지 않았다는 것입니다. 계산할 수 있는 것보다 많은 가능성이 있고 무엇이든 표적이 될 수 있습니다. 다음 섹션에서는 표적, 배포 방법, 인프라, 효과적인 이유, 과제, 문제에 대한 Infoblox의 솔루션 등 현존하는 다양한 형태의 유사 도메인에 관한 구체적인 사례를 소개합니다.

모두가 표적이다

이러한 예에서 예기치 못한 표적을 하나 이상 찾으실 수 있을 겁니다.

DNS의 유사 도메인을 검토한 결과 얻은 가장 강력한 결론 중 하나는 모든 사람이 표적이라는 것입니다: Infoblox는 모든 예상 표적뿐만 아니라 소규모 회사 및 서비스의 유사 도메인도 찾았습니다. 이러한 도메인은 악의적인 행위자가 직장과 가정에서 개인을 먹잇감으로 삼는 데 사용됩니다.

Akamai가 최근 언급했듯이, 대다수의 유사 도메인은 대규모 표적이 영향을 받은 후에야 언론에 보도됩니다.[13] Infoblox의 목표는 "전형적인" 표적뿐 아니라 충분히 보도되지 않았으며 간과된 표적도 함께 조명하는 것입니다. 이를 보여주기 위해 선별된 몇몇 예가 본문에 언급되었습니다. 또한 이러한 예가 여러 산업에 미치는 영향과 다양한 방법론의 사용에 대해서도 추후 자세히 알아보겠습니다.

그들은 우리를 표적으로 삼습니다!

Infoblox는 전 세계 직원 수가 2,000명 미만인 중소기업입니다.

Infoblox는 DNS, DHCP(Dynamic Host Configuration Protocol), IP 주소 관리 서비스(IPAM) 시장(통칭 DDI)에서 큰 점유율을 차지하고 있지만, 이러한 산업은 상당히 특수한 분야이며 Infoblox는 유명한 회사도 아닙니다. 악의적인 공격자가 Infoblox를 알고 있다는 사실도 놀랍지만, 유사 도메인을 이용하여 적극적으로 공격한다는 것은 더욱더 놀라운 일입니다. 그럼에도 불구하고 Infoblox의 직원과 고객을 속이기 위해 생성된 도메인이 대거 발견되었습니다. Infoblox의 복리후생 포털을 포함한 내부 서비스 및 Infoblox 제품 이름의 유사 도메인도 작년에 등록되었습니다.

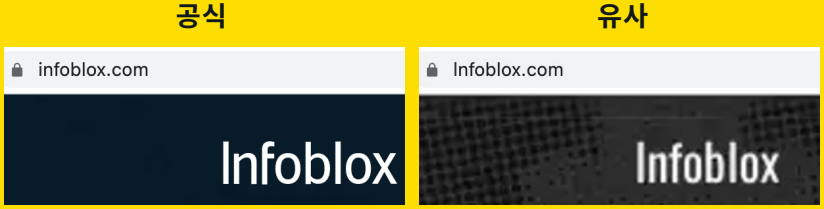


그림 2. 공식 infoblox[.]com 웹사이트(좌)와 유사 도메인인 Infoblox[.]com(우)의 비교

다음의 등록된 도메인은 Infoblox의 소유가 아닙니다.

호모그래프 **Infoblox[.]com**	소문자 "L"을 대문자 "i"로 가장한 유사 도메인이 2022년 7월에 등록되었습니다. 이 도메인은 매물로 올라왔지만 사이트의 왼쪽 상단에 저희 회사 웹사이트의 렌더링과 구별하기 어려운 렌더링이 있습니다. 그림 2의 비교를 살펴보세요.
타이포스쿼트 **infobloxbenifits[.]com**	이 도메인은 2022년 4월에 중국에서 등록되었으며 직원 복리후생 포털의 철자를 약간 바꾼 형태입니다. 이 도메인은 현재 Bodis에 파킹되어 있습니다.
TLD 스쿼트 **infoblox[.]info**	2022년 8월에 악용 가능성이 높은 등록대행기관인 Sav[.]com을 통해 다른 최상위 도메인 또는 TLD가 등록되었습니다. 이 도메인은 사용자가 도메인을 판매할 수 있는 dan[.]com에 파킹되어 있습니다.
콤보스쿼트 **infobloxgrid[.]com**	전 세계 수천 명의 고객이 사용하는 Infoblox의 주력 온프레미스 제품과 유사한 콤보스쿼트입니다. 네트워크 관리자는 Infoblox의 특허받은 Grid™ 기술을 활용하여 다양한 네트워크 애플리케이션을 하나의 단일 시스템으로 결합할 수 있습니다. 이 도메인은 dan[.]com에서도 제공되며, 2022년 4월에 등록되었습니다.
콤보스쿼트 **infoblox-updater[.]com**	도메인 내에서 "업데이트" 또는 "지원"과 같은 일반적인 소프트웨어 단어를 사용하는 기법의 예입니다. 이 경우 고객은 Infoblox 시스템 업데이트와 관련이 있다고 생각하고 속임수에 넘어가 거짓 시스템에 연결할 수 있습니다. 기술 회사의 이름이나 제품은 이러한 유형의 콤보스쿼트 도메인에 자주 활용되며, 이러한 콤보스쿼트 도메인은 피싱 도메인 또는 멀웨어 C2로 악용될 수 있습니다. 다른 예로는 dev[.]gitlabs[.]me와 jira[.]atlas-sian[.]net가 있습니다. 두 도메인 모두 지능형 지속적 위협(APT) 공격자 Iron Tiger에 의해 SysUpdate 멀웨어에서 사용됩니다.[14]

Infoblox와 같은 기술 소기업을 노리는 것 외에도 레스토랑, 로펌, 기타 소기업을 사칭하는 다양한 유사 사례가 발견되고 있습니다.

게다가 행위자 한 명이 유명 브랜드와 소규모 비즈니스를 모두 미끼로 사용할 수도 있습니다. Infoblox가 추적해온 한 행위자는 뉴욕 시에 있는 Cotenna 레스토랑의 유사 도메인을 만들고 웹사이트를 복제했는데, 이는 레스토랑 손님들이 신용 카드로 온라인 예약을 하도록 유인할 목적으로 추정됩니다.[15] cotenna[.]nyc 사이트는 2022년 4월에 등록되었으며, 레스토랑 웹사이트 cotenna[.]com과 비슷합니다. 이 행위자는 Twitter 같은 대형 소셜 미디어 회사를 표적으로 한 유사 도메인도 보유하고 있습니다.

다음 섹션에서는 오늘날 가장 많이 표적이 되는 산업과 도메인이 성공적인 공격에 이용될 수 있는 여러 방법에 대해 자세히 살펴보겠습니다. 모두가 표적이 될 수 있으므로, 유사 도메인 30만 개에 대한 검토를 바탕으로 가장 악성 활동이 많이 발생한 영역을 집중적으로 살펴보겠습니다.

모두를 표적으로 삼는 유사 도메인

amėricafirst[.]com ınstagram[.]dev,
caterpillarespaña[.]com
steamcommunlty.net[.]ru
boatairbuds[.]in
secure1-scotiabank[.]com
saveukraine[.]xyz
expressvpn-app[.]com

조직 10,000개 이상

2022년 7월 Microsoft는 10,000개 이상의 조직이 실시간으로 사용자의 MFA 자격 증명을 도난하도록 고안된 AitM 공격의 표적이 되었다고 경고했습니다.

1,600개 이상

조사 결과, 1,600개 이상의 도메인이 기업 유사 도메인 및 MFA 유사 도메인 기능을 모두 포함하는 것으로 나타났습니다.

직원을 표적으로 삼다

최근까지 여러 기업은 다단계 인증(MFA)을 사용하면 내부 네트워크를 피싱 공격으로부터 보호할 수 있다고 생각했습니다.

그러나 2023년 초에 Coinbase는 직원들이 자사 내부용 MFA 로그인의 유사 도메인을 이용한 스피어 피싱 공격의 표적이 되었다고 밝혔습니다.
이 사실이 밝혀진 직후, 유사한 공격의 표적이 된 다른 회사들의 관련 신고가 잇달아 있었습니다. 피해자들의 신고에 따르면, 악의적인 행위자가 직원들에게 SMS 메시지와 이메일을 보내 내부 시스템에 로그인하도록 촉구하는 것으로 파악되었습니다. 일부 경우 전화 통화도 이루어졌으며, 통화 중 공격자는 직원이 웹 브라우저에서 방문할 수 있는 도메인 이름을 제공했습니다. 공격자는 AitM(Adversary-in-the-Middle) 기술을 사용하여 직원들이 회사의 실제 네트워크와 상호 작용하고 있다고 믿게 했습니다. 직원들에게 MFA 코드를 입력하라는 메시지가 표시되었으며, 공격자는 이 코드를 캡처하여 내부 시스템에 액세스하는 데 사용했습니다.

Microsoft는 2022년 7월에 10,000개 이상의 조직이 실시간으로 사용자의 MFA 자격 증명을 도난하도록 설계된 AitM 공격의 표적이라고 경고했습니다.[16] 이러한 공격은 Outlook 365 인증 사용에 해당했지만, Microsoft는 2023년 2월에 MFA 공격을 가능하게 하는 피싱 키트가 2022년 7월에 판매되었으며 널리 사용된다고 추가로 보고했습니다.[17] Twilio를 비롯한 다른 회사들도 2022년 여름에 유사한 공격이 발생했다고 발표했으나, Coinbase의 피해 사실이 밝혀지기 전까지는 공격 범위가 잘 알려지지 않았습니다.[18]

이 사건을 조사하기 위해 "mfa", "okta", "2fa" 등의 키워드를 사용하여 MFA를 모방한 유사 도메인의 소급 분석을 실시했습니다. 조사 결과, 2022년 초부터 이러한 공격에 상당수의 유사 도메인의 이용되었으며, 2022년 7월부터는 광범위한 표적과 뚜렷한 활동 증가가 발견되었습니다. 1,600개 이상의 도메인이 기업 및 MFA 유사 기능을 모두 포함했습니다. 공격 대상은 Coinbase, Reddit, Twilio와 같은 대기업부터 전 세계의 주요 은행, 소프트웨어 회사, 인터넷 서비스 제공업체, 정부 기관, 게임 플랫폼에 이르기까지 다양했습니다. 또한 소규모 기술 회사, 식료품점, 소매업체도 표적이 되었지만 보고가 미흡했습니다.

잘 알려지지 않은 표적의 예로는 여러 개의 MFA 유사 도메인이 WECC(Western Electricity Coordinating Council, 미국 서부전력조정협의회)를 사칭한 사례가 있습니다.
WECC는 미국 서부의 여러 지역에서 벌크 전기 시스템의 신뢰성을 높입니다. WECC의 유사 도메인에는 wecc-okta[.]org, wecc-oktc[.]org, wecc-okta[.]com 등이 있습니다. 이러한 도메인은 모두 2023년 2월에 등록되었으며 IP 주소가 동일합니다.

또 다른 놀라운 예는 미국의 여러 자동차 대리점으로 구성된 Feldman Auto Group입니다.
이 회사는 미국 배우 Mark Wahlberg와 브랜딩 관계에 있다는 점 외에는 특이점이 없으며, 미 중서부에 18개 지점을 둔 중견 기업입니다.[19] 이 도메인의 유사 MFA 도메인인 feldmanauto-okta[.]comm은 2023년 1월 말에 등록되었습니다.

MFA 유사 도메인의 표적 기업 중 일부는 보다 불확실합니다.
도메인 frb-okta[.]com은 연방준비은행(Federal Reserve Bank), First Reserve Bank 또는 폴란드 의류 회사인 Farbokta의 사이트와 유사할 수 있는, 별다른 특징이 없는 FRBOkta 로고가 표시된 로그인 프롬프트를 표시합니다.[20] 대부분의 경우 표적이 어떤 기업인지 확신할 수 없으며 피싱 키트가 활성화된 지 얼마 되지 않았을 수 있습니다. 그림 3의 로그인 스크린샷을 보고 직접 추측해 보세요.

이러한 AITM 공격은 2022년 소비자들, 특히 게임 내 구매를 보호하기 위해 MFA를 사용하는 게임 커뮤니티 사용자들을 상대로 사용되기도 했습니다.
저희가 알고 있는 한 사례에서는 피해자가 인기 온라인 게임 Twitch 생방송에서 사이트를 방문하도록 유인당했습니다. 피해자가 MFA 자격 증명을 입력한 후 홈 네트워크에 대한 짧은 서비스 거부(DoS) 공격을 당해 몇 분 동안 인터넷이 중단되었으며, 게임 계정으로 돌아갔을 때는 구매한 아이템이 모두 도난당한 뒤였습니다. 보통 게이머라고 하면 부모님 집 지하실에 사는 *10*대를 떠올리겠지만, 인앱 구매에 지출된 비용은 게임 운영을 가능하게 할 정도이며 로블록스부터 카운터스트라이크까지 여러 게임의 플레이어들은 짭짤한 수익을 선사하는 표적이었습니다.

FRBOKTA.COM MFA 유사 도메인

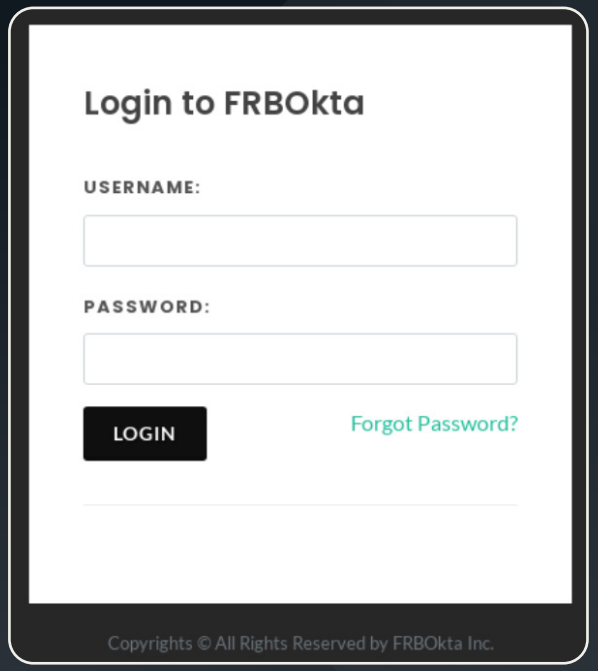


그림 3. FRBOkta가 언급된, 별다른 특징이 없는 로그인 페이지가 표시되는 frb-okta[.]com 웹사이트. 이미지 출처: URLScan.[21]

터키 정부 부처 유사 페이지

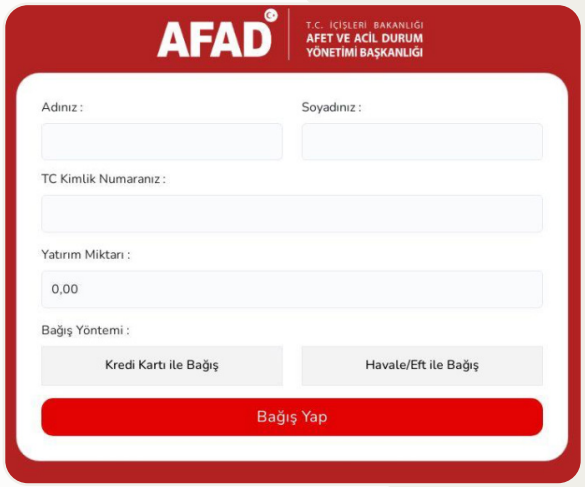


그림 4. AFAD 유사 도메인 afadestek[.]net
이미지 출처: DomainTools.

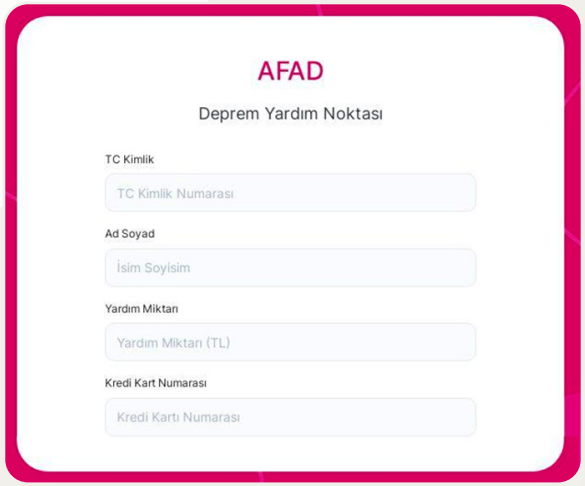


그림 5. AFAD 유사 도메인 afadbagislari[.]net
이미지 출처: DomainTools.

선행을 하는 사람들을 표적으로 삼다

돈을 훔치려는 사기꾼은 종종 부당한 이득을 취하기 위해 누구보다 먼저 전 세계적인 사건과 재난을 이용하곤 합니다.

Infoblox는 사기꾼들이 코로나19와 같은 보건 위기나 러시아의 우크라이나 침공과 같이 뉴스로 보도된 사건을 재빨리 이용한다는 사실을 발견했습니다. 안타깝게도 2023년에는 2월 초 터키-시리아 지진이라는 인도주의적 위기가 발생했습니다.[22] 2월 6일 첫 지진이 발생한 후 여러 사기 도메인이 터키 내무부 재난 및 비상 관리청(AFAD)의 웹사이트를 모방하려고 시도했습니다. 이러한 도메인은 정규화된 도메인 이름에 'AFAD'를 사용하여 합법적인 도메인 afad[.]gov[.]tr처럼 보이려 했습니다. 아래 예는 새로 등록된 도메인으로, 긴 정규화된 도메인 이름(FQDN)을 가지고 있지만 모두 'AFAD'로 시작합니다.

더 긴 FQDN을 사용하면 사기꾼이 여러 AFAD 관련 캠페인에 사용할 수 있는 합법적인 도메인의 변형을 더 많이 제공하게 됩니다.

콤보스쿼팅 외에도 이러한 사이트 중 일부는 합법적인 AFAD 로고를 사용하여 방문자가 사이트에 기부하도록

- **afad-kizilay[.]yardim-yap[.]net**
- **afad-kizilay[.]yardimbagis[.]net**
- **afad-online-odeme-bagis[.]net**
- **afadtr[.]bagislama[.]net**

속입니다. 예를 들어, 사기 사이트인 afadestek[.]net은 2월 7일에 등록되었으며 그림 4와 같이 합법적인 터키 AFAD 사이트와 유사한 웹 디자인을 보여줍니다. 기계 번역에 따르면, 이 사이트는 전자 송금을 통해 신용 카드 또는 우편환으로 기부금을 모으고 이름, 성과 주민등록번호와 같은 PII를 수집하는 것으로 보입니다.

다른 사기성 도메인은 공식 AFAD 로고를 사용하지 않고 기부자로부터 최대한 많은 금액을 뜯어내기 위해 빠르게 만들어졌습니다. 이러한 예로는 afadbagislari[.]net과 afadyardimyap[.]net이 있습니다. 두 사이트 모두 같은 IP 주소에서 호스팅됩니다. 많은 경우 유사 도메인에 전용 인프라가 사용되며, 이에 관해서는 나중에 자세히 살펴보겠습니다. 두 사이트 모두 그림 5와 같이 콘텐츠와 레이아웃이 동일하며 , 신용 카드 결제를 통해 지진 구호를 위한 기부를 하도록 요청합니다.

암호화폐를 표적으로 삼다

유사 도메인은 빠르게 돈을 벌려는 사기꾼 외에도 자격 증명 도난에 사용됩니다.

대다수의 사람들은 사용자의 자격 증명을 탈취하려고 시도하는 일반적인 "피싱" 웹사이트를 생각할 때 유사 도메인을 떠올릴 것입니다. 암호화폐의 인기가 높아지면서 이제 공격자는 마켓플레이스, 지갑 및 거래소를 포함한 암호화폐 금융 서비스를 표적으로 삼습니다. Infoblox는 인기 있는 미국 기반 거래소인 Coinbase를 매우 성공적으로 모방한 유사 도메인을 다수 발견했습니다. 그림 6은 이러한 사이트 중 하나를 보여줍니다.[23]

예를 들어 아래 표의 도메인은 2023년 1월에 등록되었습니다.

표 1. Coinbase 암호화폐 거래소와 유사한 도메인의 예입니다.

securefinancialcoinbase[.]com	reconfirminfocoinbase[.]com
secureaccountreverify-coinbase[.]com	reconfirmaccount-coinbase[.]com
secure4-coinbase[.]com	kyc-reverifycoinbase[.]com
secure2reconfirm-accountcoinbase[.]com	ap-coinbase[.]com
secure2financial-coinbase[.]com	accountupdate-financialcoibase[.]com
secure2-financialcoinbase[.]com	2farecoverycoinbase[.]com
secure-2faupdatecoinbase[.]com	recovery-financialcoinbase[.]com
2fa-accountupdatecoinbase[.]com	2fa-updatecoinbase[.]com

2023년 2월에 NFT(Non-Fungible Token, 대체 불가능한 토큰)의 거래 금액이 20억 달러에 도달하면서 행위자들은 투자자로부터 돈을 훔치기 위한 노력의 일환으로 전통적인 암호화폐 너머로 빠르게 확장했습니다.[24] 예를 들어, 2022년 10월에 Blur 마켓플레이스가 개장하고 몇 달 후에는 Blur 토큰이 출시되어 2022년 5월 이래 기록적인 NFT 투자를 주도했습니다.[25] 제품 출시 직후부터 Blur의 유사 도메인이 확인되었으며, 플랫폼의 인기가 높아지면서 Blur 유사 도메인들이 급증했습니다.

COINBASE 유사 도메인

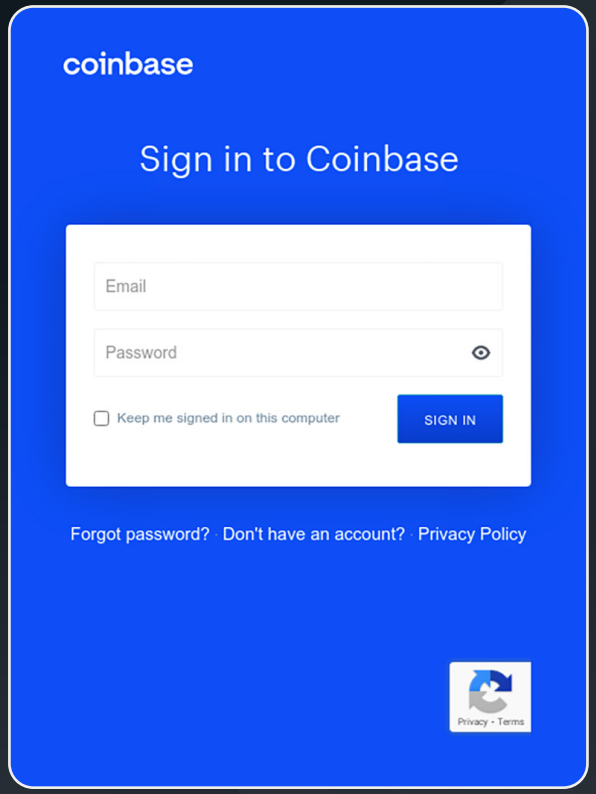


그림 6. Coinbase의 유사 도메인 click-coinbase[.]com
이미지 출처: DomainTools.

BLUR NFT 닮은꼴

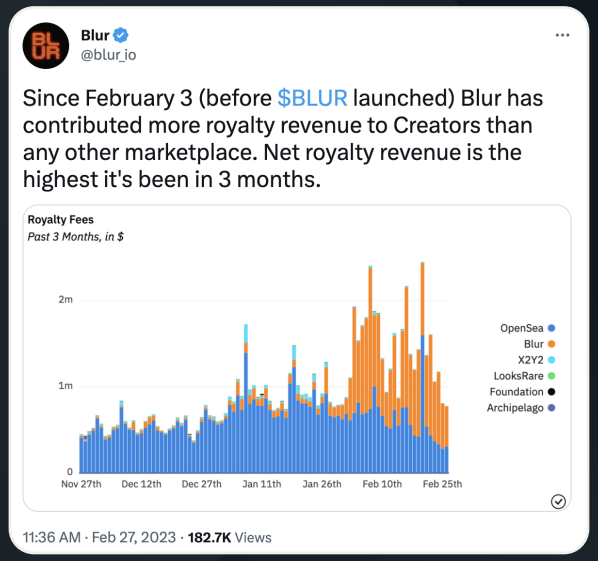


그림 7. Blur NFT 마켓플레이스는 2023년 2월에 20억 달러 상당의 NFT 거래를 발생시킨 주요 동인 중 하나입니다.[26]
이미지 출처: Infoblox

2023년 2월 14일 Blur Token의 출시를 앞두고 Blur 관련 유사 도메인의 수가 5~6배 증가했습니다. 2023년 3월에 가격이 다소 하락했음에도 불구하고 이러한 패턴은 사기를 쳐서 빠르게 돈을 벌기 위해 암호화폐 세계의 추세를 따라가려는 행위자의 의지를 보여줍니다.

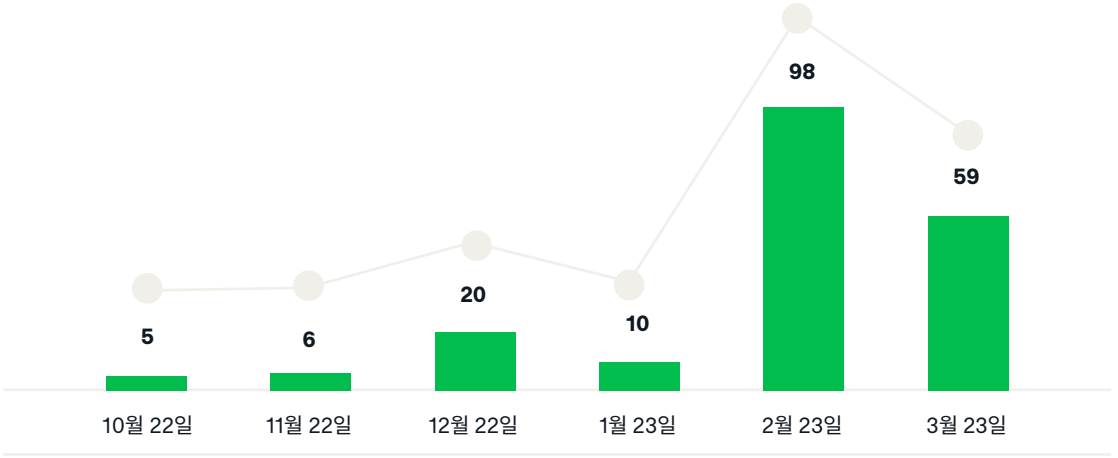


그림 8. 2022년 10월 마켓플레이스 발표 이후 Blur 관련 유사 도메인이 급증했습니다.

Infoblox는 암호화폐 관련 유사 도메인을 전문으로 하는 여러 행위자를 추적합니다. 이러한 행위자들은 Blur및 Blur의 경쟁사인 Yuga Labs(ApeCoin 및 인기 있는 NFT Bored Ape Collection의 소유주) 등 시장의 모든 주요 주체를 표적으로 삼습니다. 아래 표에는 이러한 도메인 중 일부가 나와 있습니다. 이런 행위자들이 사용하는 기법으로는 최상위 도메인(TLD)을 약간 변경하는 행위, 한 글자 추가하기, 특히 인식하기 어려운 유니코드 도메인 이름 등이 있습니다. 아래 표를 보면 apecoíns[.]com의 'i'에에 악센트 기호가 있습니다. DNS에서는 이 도메인이 xn--apecons-cza[.]com으로 표시되기 때문에 유사 도메인으로 인식하기가 다소 어려운 수준이지만, 웹 브라우저에서는 원본과 거의 구별할 수 없습니다.

표 2. Blur 토큰과 Yuga Labs 유사 도메인의 예.

Blur 유사 도메인 [blur.io]	**Yuga Labs 유사 도메인 [yuga.com]**
blurclaim[.]com	yugaslabs[.]com
blurdrop[.]com	apecoíns[.]com
blurnft[.]pw	apecoinstake[.]world
blur-nft[.]org	yugas[.]app
blur-coin[.]com	ape-claim[.]com

또한 YouTube를 벡터로 사용하여 공격 대상을 도메인으로 유인하는 비교적 새로운 형태의 암호화폐 관련 유사 도메인도 존재합니다.

이러한 사기 수법은 합법적인 제품과 관련된 것처럼 보이는 가짜 협찬 제안을 사용하여 인기 있는 YouTube 크리에이터를 스피어피싱하는 위협 행위자로 시작됩니다.[27]
이메일은 홍보할 소프트웨어의 사본 또는 협찬 계약이 포함된 PDF 파일과 같이 협찬 제안과 관련이 있다고 주장되는 파일을 다운로드하여 열도록 크리에이터에게 요청합니다.[28] 실제로 이러한 파일은 열리면 피해자의 브라우저에서 세션 쿠키를 훔치는 멀웨어 페이로드입니다. 공격자는 다단계 인증이 활성화되어 있더라도 도난당한 쿠키를 통해 피해자의 YouTube 계정에 액세스할 수 있습니다.

크리에이터의 YouTube 계정에 액세스한 공격자는 채널의 이름과 프로필 사진을 공격 테마에 맞게 (많은 경우 Elon Musk 또는 그의 회사 중 하나와 관련된 내용으로) 변경하여 채널이 해킹되었다는 사실을 알기 어렵게 만들려고 시도합니다.[29]
공격자는 자신의 흔적을 더욱 효과적으로 숨기기 위해 채널의 기존 동영상을 삭제하거나 숨길 수도 있습니다. 그런 다음 공격자는 채널의 기존 구독자를 유인하기 위해 Elon Musk의 Ark Invest 연설과 같은 암호화폐 관련 비디오의 편집된 버전을 스트리밍하기 시작합니다.

편집된 동영상에는 사용자들이 공격자의 암호화폐 관련 유사 도메인을 방문하도록 지시하는 텍스트 오버레이가 포함되어 있으며, 스트림 설명에도 도메인 링크가 명시되어 있습니다.
도메인 자체가 전형적인 고수익 투자 사기인데, 피해자가 특정 금액의 암호화폐를 특정한 지갑 주소로 보내면 그 대가로 송금액의 두 배를 돌려준다고 약속하는 식입니다. 이러한 공격에서 유사 도메인의 목적은 편집한 동영상과 브랜드를 변경한 YouTube 채널과 주제를 일치시켜 제안의 신뢰도를 높이는 것입니다.

TESLA 유사 도메인

그림 9. Tesla의 가상화폐 관련 유사 도메인 tesla-online [.] net이 특정 주소로 암호화폐를 보내면 그 대가로 두 배나 많은 금액을 받을 수 있다고 사용자에게 권유하는 모습. 이미지 출처: Infoblox.

소셜 미디어 및 모바일 사용자를 표적으로 삼다

Instagram과 Twitter와 같은 소셜 미디어 플랫폼은 Apple과 같은 주요 브랜드와 마찬가지로 자주 유사 도메인 피싱의 표적이 됩니다.

모든 인기 브랜드와 서비스가 지속적으로 이러한 공격의 표적이 되고 있지만, 지금의 위협을 설명하기 위해 다음 세 브랜드의 예를 들어보겠습니다. Apple ID와 같은 범용 ID 플랫폼과 소셜 미디어가 등장하기 전에는 악의적인 공격자들이 이메일 계정에 침입하려고 시도했습니다. 하지만 소셜 미디어와 범용 ID 플랫폼이 우리 생활에 깊숙이 들어와 있는 오늘날, 이러한 유사 도메인은 지속적인 위협으로 작용하고 있습니다.

위협 행위자는 인플루언서나 유명인의 계정뿐만 아니라 모든 사람의 소셜 미디어 계정을 노립니다. Instagram은 콤보스쿼트, 호모그래프 등 많은 유사 도메인이 있습니다. 이러한 도메인은 종종 동시에 등록된 도메인 클러스터로 나타나는데, 이는 이러한 도메인이 DDGA를 사용하여 생성된 조직적인 캠페인의 일부임을 시사합니다. 아래 예는 모두 브랜드를 'help'나 'feedback'과 같은 단어와 결합한 Instagram 세트의 일부입니다.

표 3. Instagram 지원 유사 도메인의 예

help-instagram-notice[.]com	help-instagram-about[.]com
feedback-instagram[.]com	help-Instagram-notice[.]com
help-Instagram-about[.]com	help-Instagram-notice[.]gq

이러한 도메인은 사용자가 Instagram의 저작권 규칙을 위반했다고 주장하고, 이의 제기를 하려면 사용자 이름을 입력하라고 요청하는 내용을 표시합니다(그림 *10* 및 *11* 참조).

인스타그램 유사 도메인

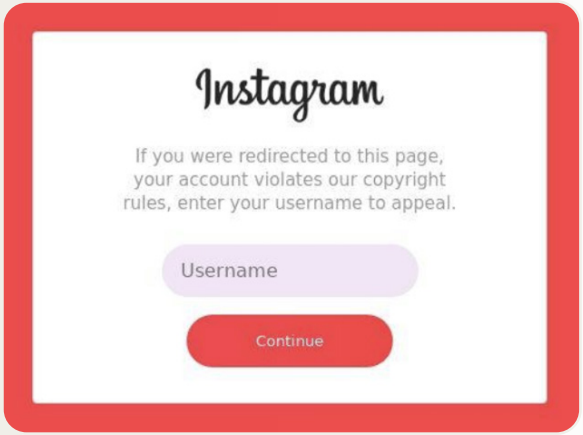


그림 10. Instagram 유사 도메인 help-Instagram-notice[.]com은 저작권 침해 이의 제기 클릭 행동 유도를 표시합니다. 이미지 출처: DomainTools.[30z]

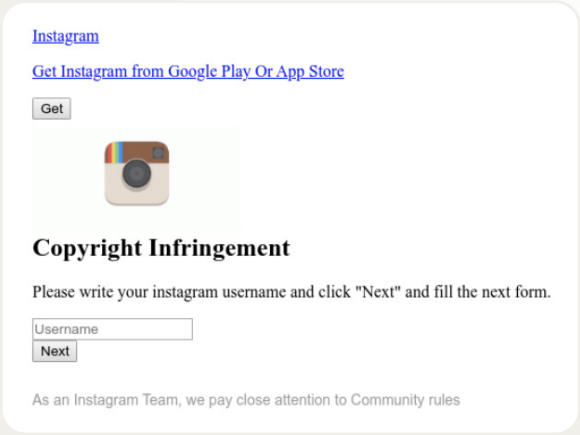


그림 11. 또 다른 저작권 침해 이의 제기 행동 유도를 표시하는 Instagram 유사 도메인 help-instagram-about[.]com. 이미지 출처: URLScan.[31]

TWITTER 유사 도메인

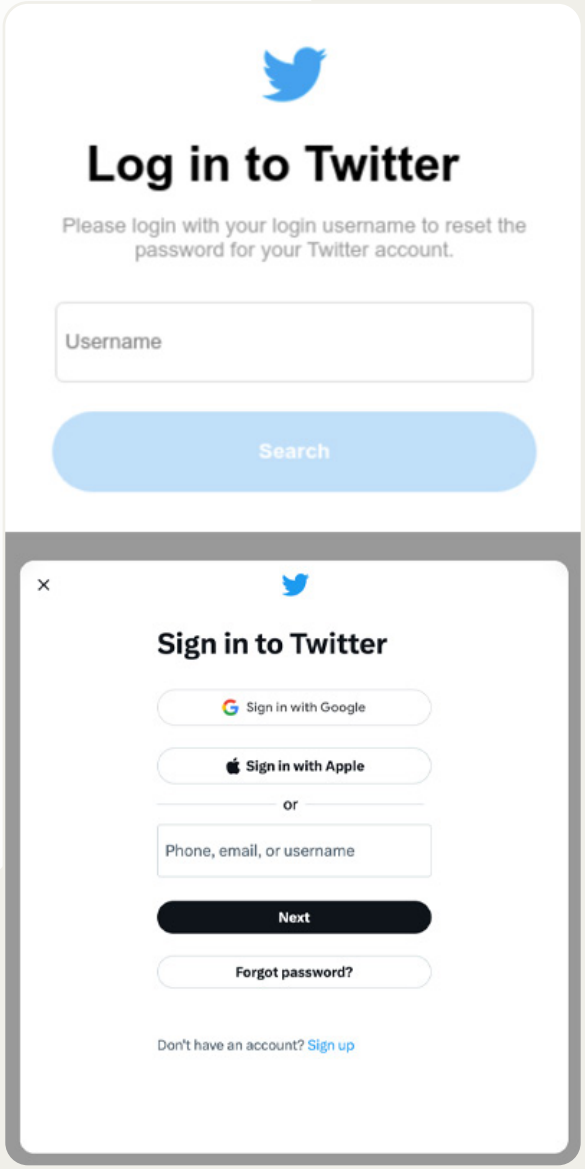


그림 12. Twitter의 유사 도메인인 help-twitter-centre[.]net이 표시하는 진짜 포털과 매우 비슷한 비밀번호 재설정 포털. 상단은 피싱 이미지, 하단은 원본 이미지입니다.
이미지 출처: DomainTools.[32]

또 다른 Instagram 유사 도메인은 대문자 "i" 대신 소문자 "L"을 사용하여 모두가 원하는 "파란색 체크 표시"(Instagram이 공인을 인증하는 수단)를 표적으로 삼습니다.
아이러니하게도 Instagram은 사칭 방지 수단으로서 유명인이나 유명 기업을 대상으로 파란색 체크 표시를 도입했습니다. 악의적 행위자가 유사 도메인을 이용하여 사칭을 방지하기 위한 솔루션을 표적으로 삼는 것을 그냥 지나쳐서는 안 됩니다.

몇 가지 예는 다음과 같습니다.

표 4. Instagram 인증 유사 도메인의 예	
Instagram-blueticket-form[.]ml	Instagram-contactbluebadge[.]ga
Instagram-verification-badges-service[.]com	Instagrambluetickverifcation[.]cf
Instagramverifybadge-contact[.]cf	Instagram-badgecentre[.]gq

Infoblox는 Instagram 유사 도메인을 추적하는 과정에서 행위자들이 한 곳의 소셜 미디어에만 주력하지 않는다는 점을 발견했습니다.

Instagram의 "저작권 침해" 유사 도메인과 함께 Twitter 유사 도메인도 호스팅되었습니다. 이러한 Twitter 유사 도메인은 사용자의 자격 증명을 피싱하는 콤보스쿼트 도메인이었으며, 랜딩 페이지는 합법적인 비밀번호 재설정 포털처럼 보입니다(그림 *12* 참조).

소셜 미디어의 유사 도메인 외에도, Infoblox의 조사 과정에서 Apple 기기 간 클라우드 저장 및 동기화를 제공하는 Apple 클라우드 서비스인 iCloud의 유사 도메인도 종종 발견되었습니다. 이러한 도메인은 상대적으로 소수의 키워드를 사용했으며, "apple", "findmy", "id", "icloud"가 가장 자주 발견되었습니다. Apple 관련 유사 도메인도 적지 않았습니다.

다음은 스페인어를 화자를 표적으로 삼는 것으로 보이는 경우를 포함한 몇 가지 예시입니다.

표 5. Apple 관련 서비스를 표적으로 삼는 유사 도메인.	
supportid-apple[.]com	sopport-apple[.]com
soporte-latam[.]us	soporte-appleid[.]com
Icloud-web-app[.]com	icloud-fndmy[.]com

모든 사람을 표적으로 삼다

Google의 탐지 알고리즘은 매일 수천 개의 새로운 유사 도메인을 식별합니다. 규모와 관계없이 악의적인 행위자가 돈이나 신원을 도난할 수 있는 모든 회사 또는 서비스가 표적이 됩니다. 마지막으로 온라인에서 관찰한 여러 유사 도메인과 이러한 도메인의 표적을 살펴보겠습니다.

표 6. 유사 도메인 및 이러한 도메인의 표적.

유사 도메인	유사 도메인의 표적
mee6bot[.]ru	Discord 봇, Mee6
vulcan[.]pm	Discord 봇, Vulcan
o365-outlook[.]com, ms-o365[.]com, o365-outlook[.]com, https-o365[.]com	Microsoft Office 365
myato-refund[.]online	호주 국세청
checkscam22[.]com, checkscams[.]online, checkscammer[.]xyz	사기 확인 웹사이트
xpressvpn[.]business, expressvpn-app[.]com, expressvpn-okta[.]com	Express VPN
anpost-paymentduty[.]com, ups-pay-deliveryfee[.]info, caddeliverypostca[.]com	우편 및 배달 서비스
crarebate-info[.]com	캐나다 세금 환급
ebl-ch[.]com	스위스 에너지 회사 EBL
op-fi-palvelut[.]co, op-fi-io[.]in	핀란드 디지털 뱅킹 및 보험 서비스 Op[.]fi
boatairbuds[.]in, boatbudsmusc[.]in, boatflashsale[.]in, boatmusicairbud[.]in	인도 기술 기업 BoAt
pumauaeshoes[.]com, pumanzsale[.]com, pumaireland[.]com, vejaoutletcanada[.]ca	제화 회사
secure1-scotiabank[.]com,r-scotiabank[.]com, chasebank-jpm[.]com, thetrustnationalbank[.]com, américafirst[.]com	은행
sprint-ldg[.]com, tds-telecom[.]com, teistra[.]ne, 1111systems-okta[.]com, t-mobile-okta[.]us, vzw-sso[.]com	인터넷 및 클라우드 서비스 제공업체
sso-authentication[.]de, sso-securelogin[.]com, service-sys-2fa[.]com	다단계 인증 및 싱글사인온 도메인

유사 도메인은 어떻게 사용되나요?

지금까지 유사 도메인의 정의와 몇 가지 예시를 살펴보았습니다. 다음으로 유사 도메인이 어떻게 이용되는지 알아보겠습니다.

여기서 '방법'이란 배포 방법을 의미합니다. Infoblox는 유사 도메인이 다음과 같이 여러 방법으로 배포된다는 사실을 확인했습니다.

- **SMS 메시지**
- **전화 통화**
- **소셜 미디어 사이트의 다이렉트 메시지**
- **이메일**
- **QR코드에 내장**
- **월드 와이드 웹의 도메인**

문자 발송

휴대폰 문자 메시지(SMS)에 대한 스팸 필터가 개선되었음에도 불구하고, SMS를 이용하여 '스미싱'으로 통칭되는 피싱 메시지를 전달하는 사례는 지속적으로 증가하고 있습니다.

공격자는 대량의 메시지를 빠르게 배포하고, 이메일 피싱 공격으로부터 보호하기 위해 마련된 일부 보안 메커니즘을 피할 수 있습니다. SMS는 광범위한 소비자 공격과 조직 직원을 대상으로 삼는 좁은 범위의 스피어피싱 공격에 모두 사용됩니다. 이 섹션에서는 SMS 및 유사 도메인을 사용하여 소비자와 정부 직원을 공격한 두 위협 행위자에 대해 알아봅니다.

Infoblox는 거의 1년간 저희가 'OpenTangle'이라고 부르는 유사 도메인 스미싱 행위자를 추적해왔습니다. Infoblox가 파악한 바에 따르면, 이 행위자는 달리 보고된 적이 없습니다. 처음에 OpenTangle은 금융기관, 인터넷 제공업체, 온라인 소매업체의 유사 도메인을 사용하여 서구 소비자들을 표적으로 삼았습니다. 이 행위자가 최근에 정부 직원과 하청업체를 표적으로 삼기 시작했습니다. Infoblox는 OpenTangle 이 활동을 시작한 약 2년 전부터 이 행위자가 관리하는 1500개 이상의 유사 도메인을 발견했습니다. OpenTangle의 도메인 중에는 mtbsuportz0610[.]com, americafirst0nline[.]com, 및 mygov03-ato[.]com 등이 있습니다.

여러 유사 도메인을 사용하는 기법에 주목하세요.

본문의 저자 중 한 명은 M&T Bank의 유사 도메인을 비롯한 OpenTangle로부터 저자와 관련이 없는 문자를 여러 통 받았습니다. 캠페인 초기에 OpenTangle은 스미싱 문자에 URL 단축 링크를 포함했는데, 이를 통해 혼란을 야기할 수 있기를 바랐을 것입니다. 그러나 2022년 5월부터 OpenTangle은 유사 도메인으로 수법을 바꾸었습니다. 그림 *13*은 사용자의 자격 증명을 요청하는 뱅킹 캠페인의 예를 보여줍니다.

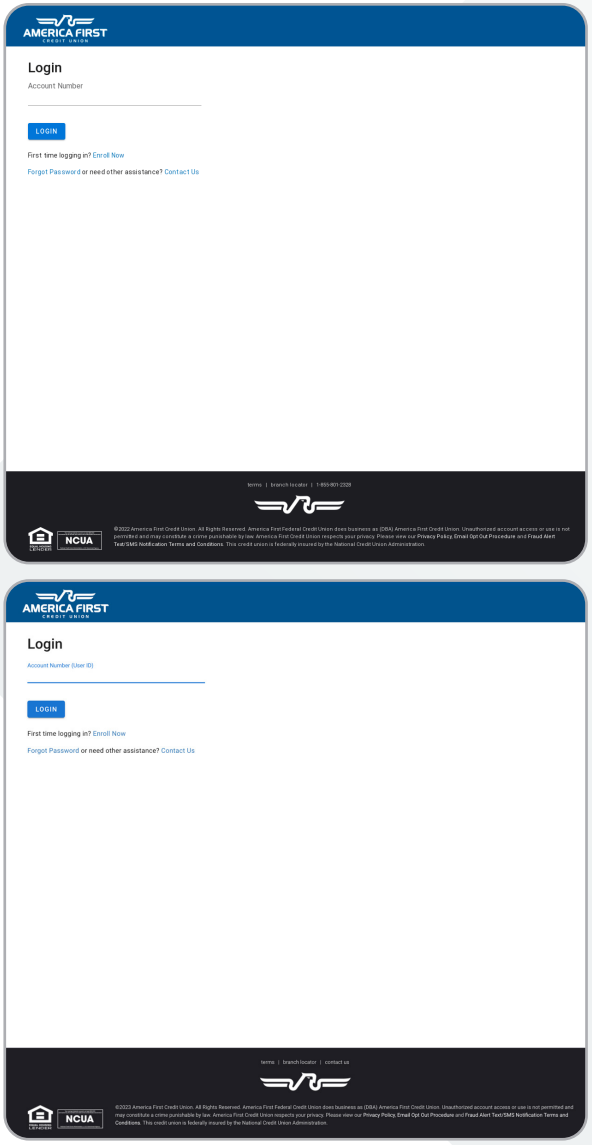


그림 13. America First Credit Union 계좌 소유자를 표적으로 삼는 americafirst0nline[.]com 도메인의 피싱 페이지. 상단의 이미지는 피싱 페이지, 하단의 이미지는 진짜 페이지입니다. 이미지 출처: URLScan.[33]

OpenTangle은 지난해부터 AitM 피싱 키트를 사용하여 MFA를 악용하기 시작했습니다. 이전의 캠페인은 표준적인 피싱 로그인 페이지를 사용하고 일반적으로 소비자를 표적으로 삼았으나, 그림 *14*는 이들이 캠페인을 어떻게 발전시켰는지 보여줍니다. 이 예에서 OpenTangle은 호주 정부 myGov 계정 소유자를 대상으로 단순 로그인이 아닌 MFA 코드를 요청했습니다. 또한 사용자가 악성 웹사이트를 방문하도록 설득하기 위해 2022년에 등장한 또 다른 기술인 헬프데스크에 전화할 수 있는 링크를 포함했습니다.

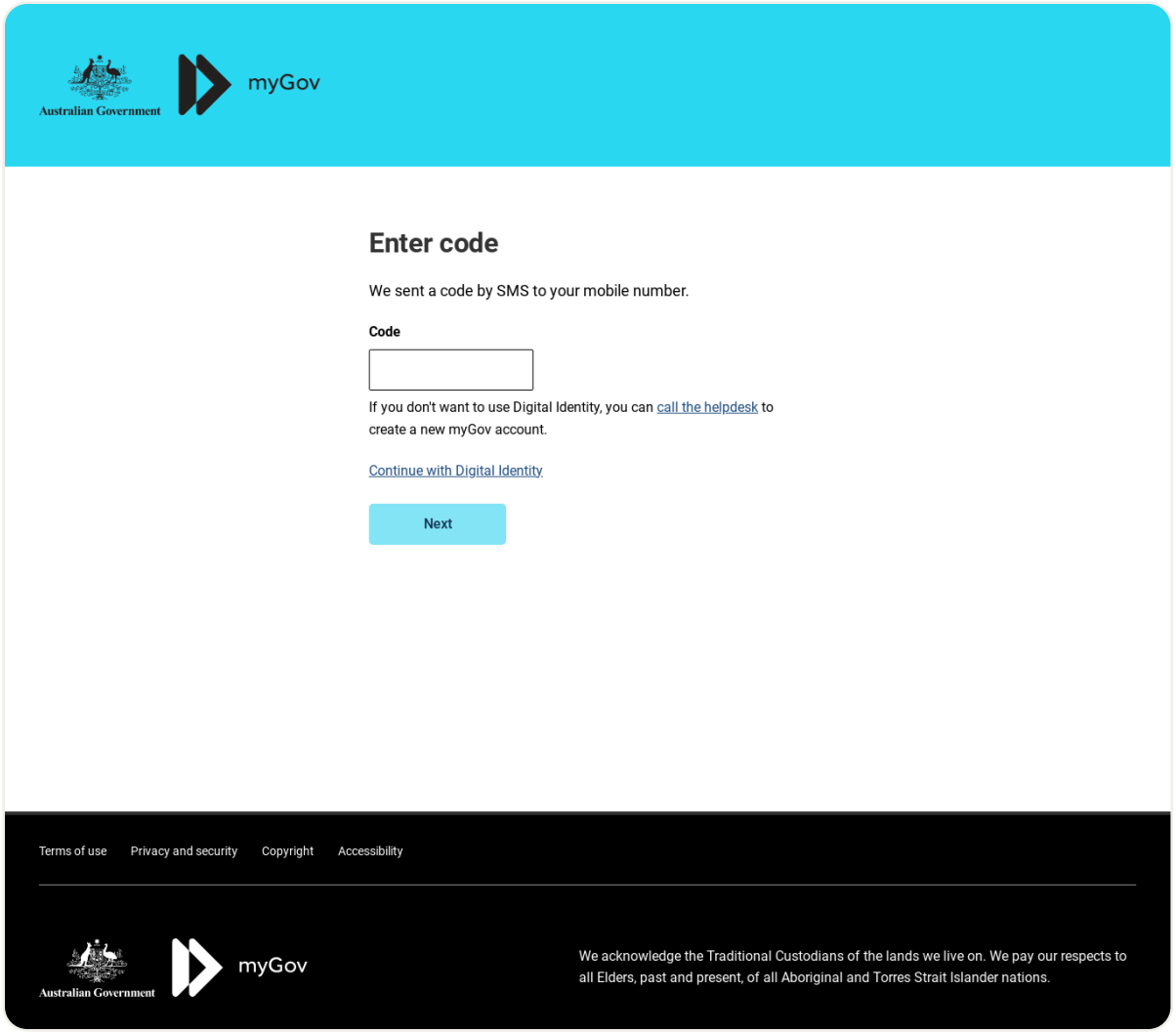


그림 14. 호주 정부의 정부 클라우드용 온라인 포털인 myGov를 모방한 OpenTangle 유사 도메인 www.mygovsupport-ato[.]com. 이미지 출처: URLScan.[34]

Scamélie는 행위자가 스미싱 메시지를 사용하여 유사 도메인을 퍼뜨리는 또 다른 예입니다.

Infoblox가 Scamélie라고 지칭하는 행위자는 주로 프랑스어권 국가를 표적으로 삼는 느슨하게 연계된 그룹 및 개인들의 집합체로, 다양한 사기에 연루되어 있습니다. Infoblox는 이들이 유럽과 UAE 전역에서 보다 일반적인 타게팅에 관여한 사실을 파악했습니다. Scamélie의 유사 도메인은 주로 ISP, 은행, 정부 서비스 및 배달업체를 사칭합니다. 이 그룹의 느슨한 관계로 인해 여행사, 스포츠 의류 회사, 식료품점 등 예상치 못한 기업을 대상으로 한 사기가 발생하기도 했습니다.

Scamélie의 유사 도메인은 많은 경우 대규모 클라우드 제공업체 또는 "방탄" 호스팅 회사에서 호스팅됩니다. 경우에 따라 사기꾼은 자체 호스팅 제공업체나 제휴 관계가 아닌 다른 사기꾼이 만든 호스팅 제공업체를 사용합니다. Infoblox는 대상 도메인과 범용 도메인(my-account, resolve-an-issue 등) 모두가 도난당한 ID를 통해 등록되고 가상 신용카드 또는 암호화폐로 결제되는 것을 확인했습니다.

범죄자는 신용카드 정보를 수집한 후 피해자의 은행 또는 신용카드 발급사 직원으로 가장하여 피해자에게 전화를 겁니다.
그들은 피해자의 신용카드 정보가 도난당했지만 문제 해결을 도와주겠다고 설명합니다. 그런 다음 발신자는 피해자가 계정 보안을 위해 발신자에게 소리 내어 읽어줘야 하는 MFA 코드를 두 개가 전송될 것이라고 말합니다. 실제로 공격자는 실시간으로 피해자로부터 돈을 훔치기 위해 MFA 코드를 필요로 합니다. 첫 번째 MFA 코드는 송금 금액을 늘리며, 두 번째 코드는 거래를 진행할 수 있게 합니다. 통화의 효율성을 높이기 위해 행위자는 1순위로 젊은 여성 및/또는 원어민의 의심을 불러일으키지 않는 수준의 프랑스어를 구사하는 발신자를 고용합니다.

조직화되지 않은 그룹인 Scamélie는 추적하거나 분석하기가 어렵습니다. 이들은 주로 피해자 기준으로 야간에 스미싱을 하며, 단 몇 시간 또는 며칠 만에 도메인을 다운시킵니다. 이들은 더 나아가 안티 봇 및 안티 스크래핑 스크립트를 사용하여 보안 연구자들을 방해합니다.

SCAMÉLIE 닮은꼴 예시

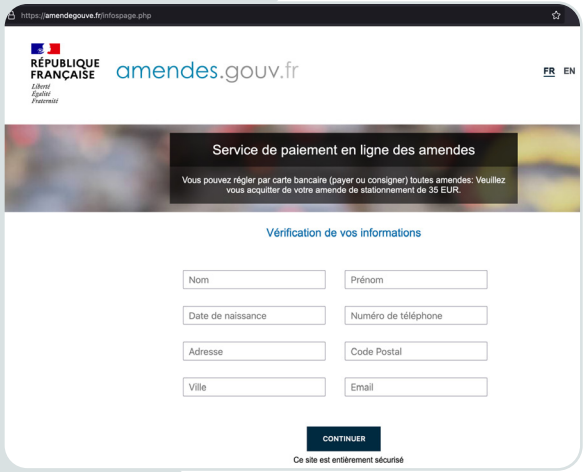


그림 15. 프랑스 정부 서비스 포털을 사칭하는 Scamélie의 유사 도메인 amendegouve[.]fr. 이미지 출처: Infoblox.

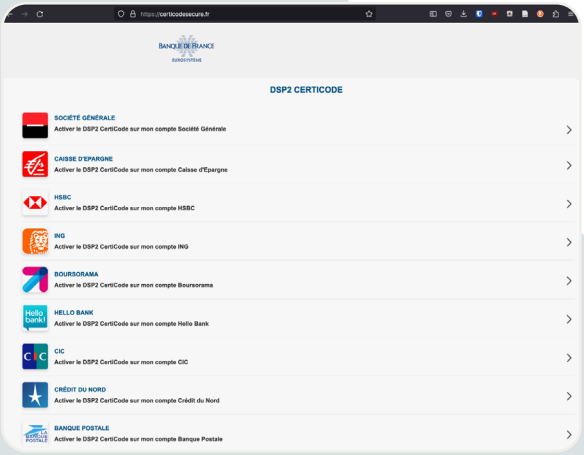


그림 16. 프랑스 은행 서비스를 스푸핑하고 피해자가 은행 계좌 정보를 연결하도록 유인하는 Scamélie의 유사 도메인 사이트 certicodesecure[.]fr. 이미지 출처: Infoblox.

전통적인 수법인 전화 통화

CISA(사이버 보안 및 인프라 보안부)는 2023년 1월 26일 RMM(원격 모니터링 및 관리 소프트웨어)의 악의적인 사용에 대한 CSA(사이버 보안 권고)를 발표했습니다.[35]

CISA는 2022년 10월에 악의적 공격자가 전화번호가 포함된 피싱 이메일을 보내 사용자에게 전화를 걸도록 유도하는 캠페인을 발견했습니다. 이 이메일은 고객 지원 메시지를 가장하여 전달되도록 설계되었으며, 사용자가 해당 전화번호로 전화를 걸면 공격자는 악성 도메인을 방문하도록 유도했습니다. 사용자가 그렇게 하면 실행 파일이 다운로드된 후 두 번째 악성 도메인에 접속하여 추가 RMM 소프트웨어가 다운로드됩니다. 이 소프트웨어(AnyDesk 및 ScreenConnect)는 합법적이지만, 지속성을 위해 행위자의 RMM 서버에 연결하도록 사전 구성되어 있었습니다.

사용된 도메인은 유명 서비스와 유사했으며, 스크립트와 발신자의 페르소나를 만드는 데 사용된 추가적인 소셜 엔지니어링으로 인해 전화로 도메인을 전달 받은 피해자가 이에 접속할 가능성은 더욱 높았습니다. Infoblox는 데이터를 소급 검토한 결과, 이 공격자가 CSA가 밝힌 것보다 더 오랫동안 활동했다는 증거를 발견했습니다.[36] 이러한 캠페인은 적어도 2021년 봄부터 전개되었으며, 이는 CISA와 Silent Push가 별도의 문건을 통해 설명한 사건이 발생하기 1년 이상 전의 일입니다. 또한 도메인 재사용도 일부 확인되었습니다. 예를 들어, Amazon의 유사 도메인인 amzsupport[.]live는 2020년 4월에 전개된 캠페인의 일환으로 이용되었다가 2021년 10월에 다시 사용되었습니다.

2023년 초 기업 내부 시스템의 MFA 보호에 대한 공격이 밝혀지면서 공격자들이 피해자에게 전화를 걸어 IT 부서를 사칭하는 경우도 있는 것으로 밝혀졌습니다. 이러한 행위는 피해자가 첫 프롬프트에 응답하지 않은 이후에 이루어졌으며, 사용자가 유사 도메인을 방문해야 할 이유의 정당성을 제시하기 위해 이용되었습니다. 이들의 말에 따른 사용자들로 인해 행위자들은 회사 자격 증명을 도난할 수 있었습니다.

스팸 발송

교활한 행위자들이 스미싱과 전화를 통해 유사 도메인을 유포하고 피해자를 현혹하는 와중에도 피싱 이메일은 계속해서 이용되었습니다.

Infoblox는 매일 수만 건의 악성 스팸 이메일을 분석하여 지속적으로 유사 도메인을 배포하는 수많은 캠페인을 밝혀내고 있습니다. 이러한 캠페인 중 몇 가지를 소개하며 피싱 이메일에 대한 지속적인 모니터링이 중요하다는 점을 강조하고자 합니다.

미국 대형 통신 회사인 Xfinity를 표적으로 한 캠페인이 이러한 예에 속합니다. Xfinity 유사 도메인은 DGA와 비슷한 특징을 지니며, xfnity<short 또는 partial word>.com의 형태를 띱니다. “Xfinity”의 첫 “i”가 없어서 철자가 틀렸음에 주목하세요. 또한 행위자는 발신자 이름이 진짜처럼 보이도록 키릴 대문자 “X”를 사용하여 “Xfinity Mobile”이라고 표시했습니다. 발신 이메일은 자체 도메인을 사용했으며, 사용자 이름도 noreply-corporate@xfnitycard[.]com와 같은 noreply-<keyword> 패턴으로 구성, DGA와 유사한 특징이 있는 것으로 보입니다. 행위자들은 각 이메일에 고유한 도메인을 사용하지 않았습니다. 일부 경우 같은 도메인을 재사용하되 키워드를 변경했습니다(예: noreply-corporate@xfnitycard[.]com, noreply-active@xfnitycard[.]com).

표 7. Xfinity 유사 도메인.

xfnitykuri[.]com	xfnitycomp[.]com
xfnitystarter[.]com	xfnityhlaty[.]com
xfnityersa[.]com	xfnityothie[.]com
xfnitykaris[.]com	xfnityrkles[.]com
xfnityrayton[.]com	xfnitycard[.]com

캠페인에서 확인된 도메인은 미끼 파킹(decoy parking)이라는 기술을 사용합니다. 이 기술은 도메인을 직접 방문하면 파킹된 것처럼 보이지만, 실제로는 도메인의 메일 서버가 활성 상태이고 악성 이메일을 보내는 기술입니다. Infoblox는 미끼 파킹이 상당히 만연하며, 다른 공급 업체에서는 보고하지 않는다는 사실을 발견했습니다. 그림 *17*은 미끼 파킹 페이지의 예입니다.

XFINITY 유사 도메인

그림 17. Xfinity의 유사 도메인인 xfnityrayton[.]com이 표시하는 미끼 파킹 페이지. 이미지 출처: URLScan.[37]

WEDO MACHINERY 유사 도메인

Dear you

Good day !
How are you?
How is your project going?
Do you receive my message?

Hope we can establish long term cooperation.

We got recommendation of your company from our UK partner about

below order as attached

Please confirm if your can deliver the products specifield

Mrs. ConnieXu
Mob: 0086 131 0941 7901 [WhatsApp/Wechat]

Wedo Machinery (Zhangjiagang) CO., LTD.

Add: Zhenbei Road, Leyu Town, Zhangjiagang City, Jiangsu Province, China.

그림 18. Wedo Machinery를 미끼로, 유사 도메인 acobat-adobe[.]com을 멀웨어 C2로 이용하는 악성 스팸 캠페인의 본문. 이미지 출처: Infoblox

Infoblox의 분석 결과, 유포된 악성 Word 문서에서 이러한 Xfinity 유사 도메인이 발견되었습니다.

캠페인 주제는 행동 유도의 기능을 겸비했으며, 주된 내용은 "[공지] 서비스가 종료될 우려가 있습니다" 또는 "[조치 필요] 카드에 대금을 청구할 수 없습니다. 오류를 해결하세요"와 같이 결제가 거부되거나 서비스가 종료될 수 있다는 위협이었습니다. 이러한 이메일의 본문은 고객 지원팀에서 보낸 것처럼 꾸며졌으며, 케이스 세부 정보는 첨부파일에서 확인하라고 요구했습니다.

Infoblox가 파악한 또 다른 캠페인은 중국의 재활용 업체인 Wedo Machinery를 이용해서 랜섬웨어 로더를 확산시켰습니다. 이 캠페인을 통해 176개의 이메일이 발송되었는데, 각 이메일에는 Zmutzy로 식별된 하나의 실행 가능한 파일이 포함된 .zip 파일이 첨부되어 있었습니다. 그림 *18*은 이 캠페인을 통해 발송된 이메일의 예입니다. 캠페인에는 *'PO-0097(1).zip', 'PO-29862K.zip'*이라는 두 가지 이름의 파일이 포함되었습니다. Zmutzy 로더는 유사 도메인 acrobat-adobe[.]com을 사용하여 추가 페이로드를 다운로드합니다.

QR 코드 사용

Infoblox는 직접적인 암호화폐 유사 도메인 외에도 QR 피싱이 이용되고 있음을 파악했습니다. QR 피싱은 URL 랜딩 페이지를 알아보기 어렵게 하고 악성 콘텐츠를 전달하게 위해 QR 코드를 유사 도메인과 함께 사용하는 기법이며, 무료 경품을 받아가라며 사용자를 유인해서 암호화폐 지갑 계정 정보를 알려주게 만듭니다.

한 예로, QR 코드는 자금을 도난하는 데 사용된 메커니즘인 bridge[.]walletconnect[.]com 링크로 피해자를 리디렉션했습니다. 이 사기 사례에서는 공격자들이 Twitter 계정 @adidas_weare를 개설하여 신뢰도를 높이고 유사 도메인을 공유했습니다(그림 *19* 참조). 이 계정은 2023년 2월 21일 기준으로 16,000명의 팔로워를 보유하고 있었으나, 다행히도 현재는 삭제 또는 정지된 상태입니다.

공격자들은 Porsche 자동차와 Adidas 의류 또는 신발을 비롯한 다양한 가짜 경품을 광고했습니다. 도메인은 주로 "adidas" 또는 "porsche"라는 키워드를 포함하는 콤보스쿼트입니다. 유사 도메인(아래 그림 *20* 참조)을 방문한 사용자는 증정되는 아이템을 받을 수 있는 QR 코드를 스캔한 다음 공격자가 사용자의 자금에 접근할 수 있는 탈중앙화 애플리케이션인 WalletConnect로 이동하라는 요청을 받았습니다.

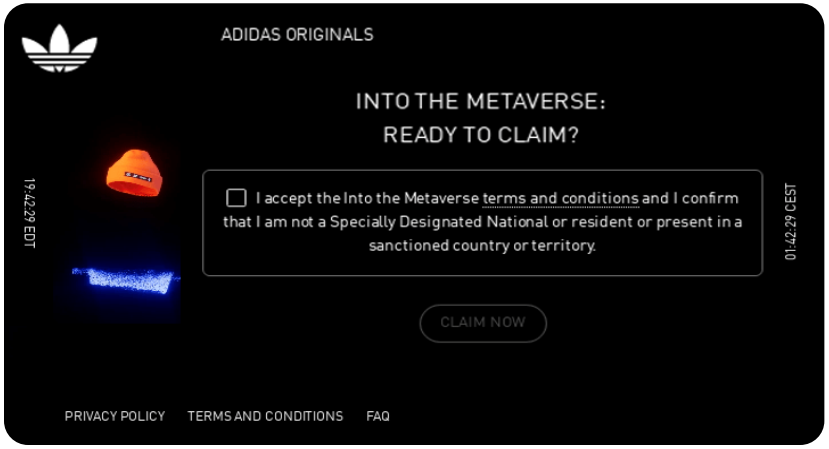


그림 20. 사용자가 무료 제품을 받기 위해 클릭하도록 유도하는 Adidas 유사 도메인 adidas-go[.]com. 이미지 출처: URLScan.[39]

사용자가 QR 코드를 스캔하고 자신의 암호화폐 지갑을 탈중앙화 애플리케이션에 연결하면 공격자는 사용자로부터 암호화폐를 탈취할 수 있습니다. 이러한 도메인은 공유 네임서버를 사용하며 러시아 IP 주소로 확인된 185[.]149[.]120[.]83에서 호스팅됩니다. 이 IP 주소는 공격자에 의해 완전히 제어되며, 이더리움 스마트 계약의 속도와 확장성을 개선하는 솔루션인 Arbitum뿐만 아니라 Blur와 유사한 다른 솔루션도 포함합니다.

ADIDAS 유사 도메인

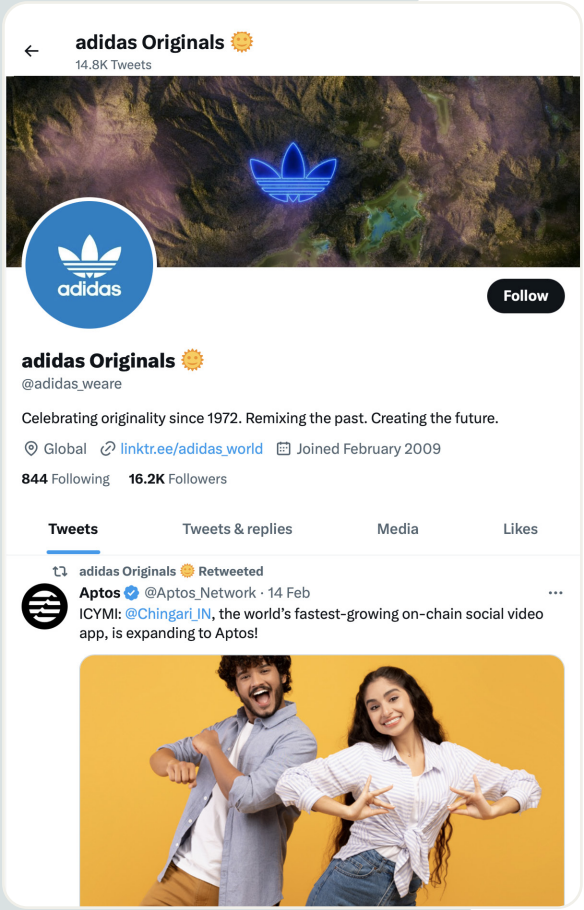


그림 19. Adidas Originals의 Twitter 계정인 @adidasoriginals의 유사 계정 @adidas_weare. 이미지 출처: Infoblox.

DNS 사용

유사 도메인은 웹사이트 도메인으로만 존재하지 않으며,

다음과 같은 여러 DNS 기능에서도 사용되는 것으로 확인되었습니다.

- **네임서버**
- **메일 서버**
- **CNAME 레코드**
- **PTR 레코드**

대부분의 경우 이러한 도메인은 일반적인 A 레코드나 웹사이트가 없으며, 파킹된 것처럼 보일 수 있습니다. 이는 이전 섹션에서 설명한 미끼 파킹이 실제로 구현된 형태입니다. 또한 공격자는 DNS에서 C2 통신 및 리디렉션을 위해 유사 도메인을 사용하기도 합니다.

네임서버

유사 네임 서버의 예인 도메인 bitkeep[.]dev 및 flutter[.]direct는 2022년 11월에 등록되었습니다. 이 두 도메인은 각기 다른 도메인의 유사 도메인이지만, 같은 인프라를 이용합니다. BitKeep은 모든 암호화폐 거래의 단일 허브를 목표로 하는 탈중앙화 멀티체인 암호화폐 지갑입니다. BitKeep의 공식 도메인은 bitkeep[.]com이며, 5년간 영업 중이고 800만 명 이상의 사용자를 보유한 기업입니다.[40] Flutter는 단일 코드베이스에서 모바일, 웹, 데스크톱용 네이티브 컴파일 애플리케이션을 제작하기 위한 Google의 휴대용 사용자 인터페이스(UI) 툴킷입니다. Flutter의 공식 도메인은 flutter[.]dev입니다.[41]

합법적인 도메인은 모두 기본 도메인에서 웹 콘텐츠를 호스팅하지만, 유사 도메인은 그렇지 않습니다. 최초 등록 시 두 도메인 모두 다른 도메인인 get-flutter[.]com의 네임서버 역할을 하고 있었습니다. 이 도메인은 또 다른 Flutter 유사 도메인입니다. 당시 이러한 도메인은 스위스의 역외 호스팅 제공업체 Private Layer에서 호스팅되었습니다. 이 네트워크는 flutter[.]vision도 호스팅했습니다. 악의적인 활동과 관련이 있다고 단정할 수는 없으나, 이러한 도메인은 유사 도메인을 비정상적인 목적으로 활용하는 패턴을 보여주고 있습니다. 이들 도메인은 경험 많은 연구원도 분석하기가 어렵고 위협 인텔리전스 알고리즘을 트리거할 가능성도 낮습니다.

메일 서버

네임서버 외에도 메일 서버로 유사 서버가 사용되는 것을 보았습니다. 유명 가전 브랜드인 Whirlpool을 표적으로 삼는 도메인 whirlpoolmxonline[.]com 및 whirlpoolservicesmx[.]com은 같은 인프라를 공유합니다. 이러한 도메인은 세이셸에 위치한 저품질 VPS 및 호스팅 제공업체인 Lyra Hosting이 소유한 같은 IP 주소에서 호스팅되며, 동일한 네임서버를 공유합니다.

이러한 도메인은 2차 도메인(SLD) 이름을 사용하여 Whirlpool을 직접 타게팅하지만, 각 도메인 내에서 다른 주요 가전 브랜드도 표적으로 삼고 있음을 보여주는 특징도 파악되었습니다. SLD whirlpoolmxonline[.]com은 세 개의 하위 도메인(mabe-onlinemx[.]whirlpoolmxonline[.]com, samsung-onlinemx[.]whirlpoolmxonline[.]com, lg-onlinemx[.]whirlpoolmxonline[.]com)이 있습니다. Mabe는 멕시코의 가전제품 회사입니다. SLD whirlpoolservicesmx[.]com은 하위 도메인이 없지만, 이 도메인과 연결된 SSL 인증서의 내역 체인을 보면 whirlpoolmxonline[.]com과 유사한 가전제품 브랜드인 www[.]lgservicesmx[.]mabeservice[.]com 및 *.lgservicesmx[.]com을 표적으로 삼는 것으로 나타났습니다.

유사 도메인이 메일 서버로 사용된 경우, 이메일 헤더만 보면 합법적인 것처럼 보이기 때문에 엔드포인트에서 피싱 이메일을 탐지하기가 더욱 어려워집니다.

멀웨어 C2

앞의 이메일 배포 섹션에서는 Zmutzy 랜섬웨어 로더를 확산시키는 것으로 확인된 악성 스팸 캠페인이 유사 도메인 acrobat-adobe[.]com을 멀웨어 C2 서버로 사용함을 언급했습니다. 유사 도메인은 진짜 도메인과 함께 네트워크 트래픽에 쉽게 섞여 들어갈 수 있으므로 멀웨어 C2에 적합합니다. 슬로바키아 보안 소프트웨어 회사인 ESET의 연구원들은 2023년 2월에 메시징 애플리케이션 Telegram으로 가장한 FatalRAT(원격 액세스 트로이 목마)용 멀웨어 C2를 발견했습니다.[42]

표 8. 멀웨어 C2로 기능하는 Telegram 유사 도메인.

12-03.telegramxe[.]com	12-25.telegraem[.]org
12-25.telegraxm[.]org	12-25.telegraem[.]org

악성 .exe 파일을 호스팅하는 도메인은 Telegram뿐 아니라 WhatsApp, Skype, Google Chrome, Firefox의 유사 도메인이기도 했습니다.

리디렉션

유사 도메인은 리다이렉트로도 이용될 수 있습니다. Infoblox는 방문자를 조건부로 랜딩 도메인 lotto60[.]com으로 리디렉션하는 C2 도메인인 choto[.]xyz로 리디렉션하는 대규모 타이포스쿼트 도메인 네트워크를 발견했습니다. 공격자는 아마도 보안 연구자들의 탐지 및 탐색을 방지할 목적으로 choto[.]xyz에서 리버스 프록시 서비스와 Cloudflare 봇 보호 기능을 사용합니다. 랜딩 도메인은 사기성 제휴 마케팅 프로그램을 실행하는 것으로 보입니다. 문서 객체 모델(DOM)을 분석해 보면 분석 ID G-DT4YWT5VP8로 Google 애널리틱스에 방문자 데이터를 전송하는 인라인 gtag() 함수가 HTML에 포함되어 있음을 알 수 있습니다. 또한 Infoblox는 원격 액세스 트로이 목마 Nighthawk로 확인된 파일 서명과 일치하는 잠재적 악성 파일이 공격자의 제휴 마케팅 실적을 부풀릴 뿐 아니라 HTTP를 통해 lotto60[.]com을 요청하는 것을 확인했습니다.[43]

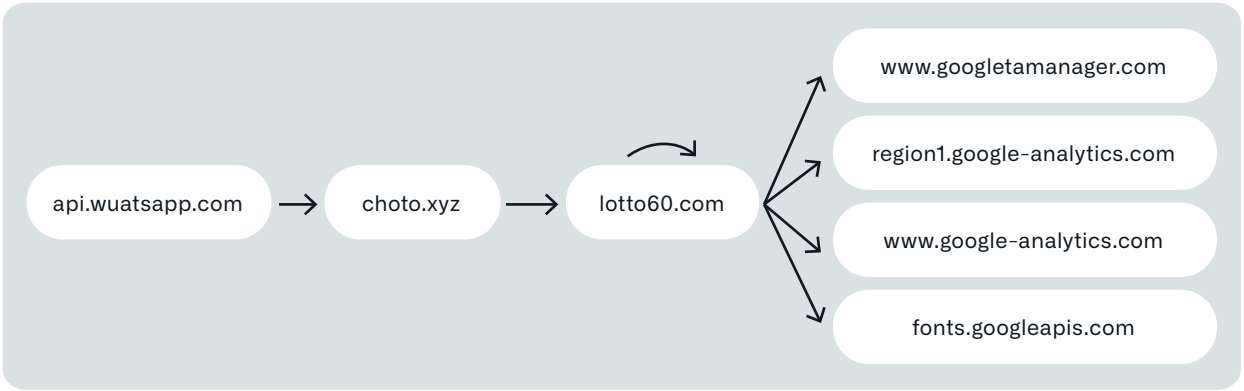


그림 21. 타이포스쿼트 도메인에서 Google 애널리틱스로의 리디렉션 체인 예. 이미지 출처: URLQuery.[44]

1단계 타이포스쿼트 도메인은 여러 회사를 사칭합니다. 몇 가지 예는 다음과 같습니다. →

표 9. 사기성 제휴 마케팅 캠페인으로의 리디렉션으로 기능하는 유사 도메인.

gi6hub[.]com	whatysapp[.]com
bankofamegica[.]com	babgkokbank[.]com
intuhit[.]com	scotiasbank[.]com

이러한 타이포스쿼트는 일반적으로 1~3개월 동안 파킹된 후 리디렉션으로 사용됩니다. 행위자는 심혈을 기울여 타이포스쿼트 도메인을 제작했습니다. 각각의 틀린 문자는 미국 영어 QWERTY 키보드의 올바른 문자 바로 옆에 있습니다. 이는 키보드를 보면서 한 자 한 자 입력하지 않는 이상 타이핑을 하는 사람이라면 누구나 하루에도 여러 번 범할 수 있는 실수입니다.

효과적인 이유

혹시 지금까지 이 백서 곳곳에 숨겨놓은 유사 단어 19개를 알아차리셨나요? 몇몇은 특히 알아차리기가 어려울 수 있습니다.

힌트: 이러한 유사 단어가 6개 더 있습니다. 한 번 찾아보세요.

지금까지 구체적인 표적과 유사 도메인의 배포 인프라에 대해 알아보았습니다. 그렇다면 유사 도메인이 이토록 효과적인 이유는 무엇이며, 어떻게 이렇게나 지속적인 위협으로 작용할 수 있는 것일까요?

이에 대한 답변은 복잡하며, 심리학, 기술적 구현, 그리고 사람의 실수를 모두 포함합니다. **실수야말로 우리 인간의 특징이니까요.**

심리언어학

심리학적으로 인간의 뇌는 독서 중 단락(이 경우, 말 그대로 전류가 의도치 않게 저항이 가장 적은 경로로 흐른다는 의미)을 일으킵니다. 여러분은 아마도 다음과 같은 내용의 밈을 본 적이 있을 것입니다.

켐브리지 대학교 연구에 따르면, 단어의 철자 순서와 상관없이 중요한 것은 첫 글짜와 마지막 글자가 제자리에 있는 것 뿐잎니다. 이럴게 쓰인 글이 엉맹진장이어도 읽는 데 지장이 없슴니다. 사람의 뇌는 글자를 하나한나 읽는 것이 아나라 단어 전체를 읽기 때문임니다.

케임브리지에서 이런 내용의 연구를 발표한 적이 없으므로 이 주장은 근거가 없지만, 기본 개념은 일리가 있는 것으로 보입니다. 예를 들어, 최근 실제로 진행된 연구에 따르면 "엉망으로 쓰인 단어를 보면 알려진 단어와 비교하는 시각적 표현이 활성화된다"고 합니다.[45] 심리언어학의 근본적인 질문들을 증명하거나 반증하는 것은 본문의 논점을 벗어나지만, 심리언어학이 어떻게 유시 도메인의 효과에 중요하게 기여하는지 보여드리고자 합니다.

구체적으로, 인간 뇌의 단락은 호모그레푸 및 타이포스쿼트에 관해 중요한 역할을 합니다. Infoblox[.]com과 같은 도메인을 보는 사람의 두뇌는 이 도메인 이름의 각 글자를 분석하지 않으므로, 첫 번째 문자가 실제로 대문자 "i"가 아니라 소문자 "L"이라는 것을 알아차리지 못할 수 있습니다.

비슷한 이유로 도메인 goooogle[.]com을 본 사람의 뇌가 "o"가 두 개가 아니라 세 개라는 사실을 미처 인식하지 못해서 그만 클릭하게 될 수 있습니다.

퓨니코드 지원: 성공과 실패

웹 브라우저는 IDN(국제화 도메인 네임) 호모그레프 공격으로부터 사용자를 보호할 수 있는 수단을 갖추고 있습니다. 첫 번째이자 가장 눈에 띄는 방어선은 유니코드 도메인을 앞에 "xn--"이 붙은 형태가 특징이며 육안으로는 의미가 없어 보이는 퓨니코드로 "변환"하는 것입니다. 이는 퓨니코드가 문자, 숫자와 하이픈만 포함하는 ASCII(미국 정보교환 표준 코드) 문자의 훨씬 더 제한된 하위 집합에 유니코드 문자를 매핑하기 때문입니다. 각 주요 브라우저는 퓨니코드 도메인을 지원합니다. Google은 Chromium에서 도메인의 국제화 버전과 퓨니코드 버전 중 어떤 것을 표시할지 여부를 결정하는 알고리즘과 관련된 휴리스틱을 자세히 설명합니다.[46] Mozilla도 비슷한 설명을 제공합니다.[47]

Mozilla는 IDN 표시 알고리즘에 관한 설명에서도 다음과 같은 유익한 정보를 제공했습니다.

> **이 문제에 대한 저희의 답변은, 자사의 고객이 서로에게 사기를 치는 일을 방지하는 것은 궁극적으로 등록기관의 책임이라는 것입니다. 브라우저에 일부 제한을 마련했으나, 저희는 웹에서 비라틴어 스크립트를 위한 공정한 경쟁의 장을 유지하는 동시에 등록기관의 이러한 역할까지 도맡을 수 있는 입장이 아닙니다. 등록기관은 이러한 부분을 적절하게 점검할 수 있는 유일한 주체입니다. 저희는 비라틴어 스크립트 사용자를 차별하지 않을 것입니다.**

2017년에 보안 연구자 Xudong Zheng은 이미 퓨니코드로 된 도메인 xn--80ak6aa92e[.]com을 등록했습니다. 이 도메인은 “apple[.]com”으로 변환되며, "apple"의 라틴 문자 모양을 모방한 키릴 문자를 포함합니다.[48] 당시 Internet Explorer, Microsoft Edge, Safari, Brave, Vivaldi 브라우저는 취약하지 않았지만 Chrome, Firefox와 Opera는 취약한 것으로 나타났습니다. 현재는 Firefox만 퓨니코드를 계속 변환하여 사용자를 이러한 공격에 취약하게 만들고 있습니다(다만 Infoblox는 최근에 Internet Explorer나 Microsoft Edge에서는 이 도메인을 테스트하지 않았습니다).

퓨니코드란?

퓨니코드는 유니코드 문자를 ASCII로 변환하는 데 사용되는 특수 인코딩입니다. ASCII는 더 작고 제한된 문자 집합입니다. 퓨니코드는 IDN(국제화 도메인 네임)을 인코딩하는 데 사용됩니다.

IIDN 호모그래프를 사용한 IMESSAGE 스미싱

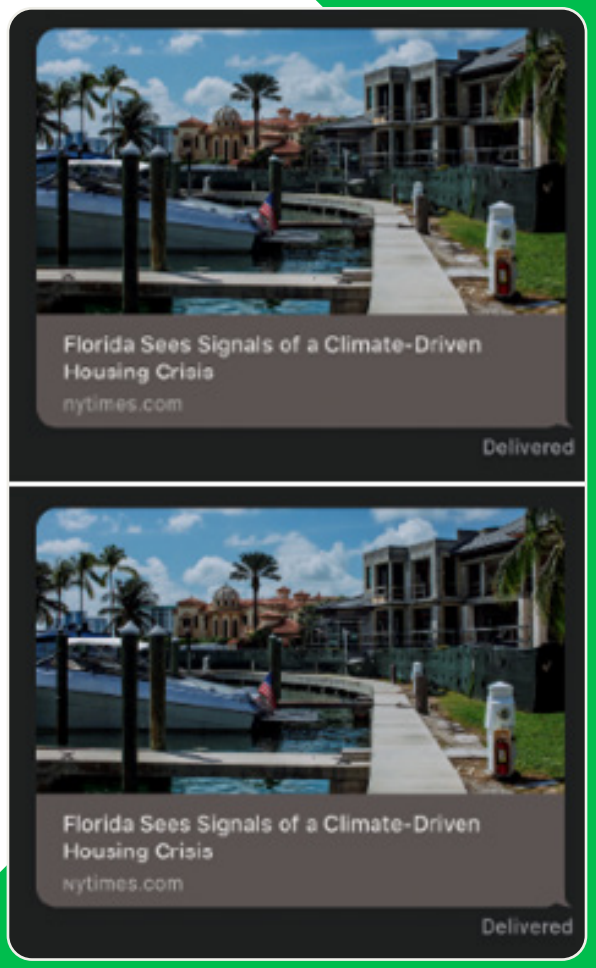


그림 22. 상단 이미지는 iMessage를 통해 전송된 실제 New York Times 기사를 나타냅니다(이미지 제공: Tyler Butler). 하단 이미지는 IDN 호모그래프 도메인에서 스푸핑된 NYT 기사를 보여줍니다(이미지 제공: Tyler Butler).

Hu 등은 IDN 호모그래프 공격에 대한 브라우저 기반 방어의 효과에 관한 종단 분석과 정량적 분석을 수행했습니다.[49]

이들은 다음 세 가지 질문에 대한 답을 모색했습니다.

1. 주요 브라우저는 어떤 정책을 구현하고 있으며 이러한 정책을 얼마나 잘 이행하고 있는가?
2. 기존 정책을 체계적으로 우회할 수 있는 방법이 있는가?
3. 인터넷 사용자는 IDN 호모그래프를 얼마나 잘 인식할 수 있는가? 브라우저 정책을 우회하는 이러한 IDN 호모그래프는 기만적인가?

질문에 답하기 위해 저자들은 2015년 1월부터 2020년 4월까지 5년간 주류 브라우저 5가지(Chrome, Firefox, Safari, Microsoft Edge, Internet Explorer)를 조사했습니다. 처음 두 질문의 답을 얻기 위해 9,000개의 테스트 사례를 만들었고, 세 번째 질문의 답을 찾기 위해 사용자 연구를 실시했습니다. Chrome과 Edge는 퓨니코드에 상응하는 IDN 호모그래프 대신 퓨니코드를 표시하는 데 가장 성공적이었습니다. 두 브라우저 모두 전체 실패율(퓨니코드 대신 IDN 버전 표시)이 20.62%였습니다. Safari와 Firefox는 전체 실패율이 각각 42.91% 와 44.46%로 결과가 훨씬 나빴습니다. IDN 카테고리에 따라 브라우저마다 실패율이 달랐습니다. 더 나아가 저자들은 인터넷 사용자들이 호모그래프 IDN을 식별하는 데 어려움을 겪고 있으며, 브라우저가 차단한 IDN은 진위 여부를 판단하기가 가장 어려운 것들이라는 사실을 발견했습니다. 사용자의 48.8%는 이러한 IDN이 진짜라고 생각한 반면 48.5%는 진짜가 아니라고 생각했고, 2.7%는 아예 구분하지 못했습니다.

지금까지는 데스크톱 브라우저에만 초점을 맞추었지만, 이 백서 앞부분에서 설명한 유사 스미싱 공격에서 보았듯이 IDN 호모그래프 도메인은 모바일 기기에서도 꽤 효과적이며 오히려 더 해로울 수도 있습니다. 화면 크기가 작고, 주소창이 작고 링크 미리 보기가 전반적으로 부족하면 유사 공격이 더 효과적일 수 있습니다. 링크 미리 보기가 있더라도 IDN 호모그래프는 모바일 기기에서 여전히 효과적일 수 있습니다. 2021년에 보안 연구자 Tyler Butler는 iMessage에서 IDN 호모그래프를 사용한 스미싱이 존재할 가능성에 대해 발표했습니다.[50] iMessage는 뛰어난 링크 미리 보기 기능을 제공하지만, 요령 있는 공격자는 충분히 비슷한 유사 도메인과 웹 페이지의 스타일 편집 작업을 통해 이를 아주 쉽게 우회할 수 있습니다. Butler의 지적대로, 이런 형태의 공격은 잘못된 정보를 퍼뜨리거나, 자격 증명을 도용하거나, 표적 멀웨어나 스파이웨어를 전달하는 데 사용될 수 있습니다.

Butler는 Apple이 호모그레푸를 '시각적으로 구별할 수 있다'는 이유로 이 취약점에 대한 조치를 취하지 않을 것이라고 밝혔다고 설명했습니다. 어떻게 생각하시나요? 그림 22에서 차이점이 보이시나요?

인간의 실수는 끝이 없고 용서는 신성하지만 자동화는 지혜롭다

월드 와이드 웹에는 다른 사람의 실수를 잘 용서하지 않는 사람들이 있습니다. 앞서 언급했듯이, 행위자들은 타이포스쿼트 도메인을 사용하여 다른 사람의 자연스러운 철자 오류를 먹잇감으로 삼습니다. 행위자가 타이포스쿼트의 효과를 발휘시키기 위해 해야 할 일은 그럴듯한 도메인을 등록하고 기다리는 것 뿐입니다. 언젠가는 누군가가 오탈자를 저지르고 방문할 생각이 없었던 도메인에 방문하게 될 것입니다. 물론 악의적인 행위자는 기다리기만 하는 것이 아니라 사람들이 클릭하도록 적극적으로 유도합니다. 그리고 빠르게 변화하는 세상에서 사람들은 애초에 실수를 저질렀다는 사실조차 깨닫지 못하는 경우가 많습니다.

궁극적으로 유사 도메인을 이 이름으로 부르는 이유는 인간을 속이려는 목적으로 유명 도메인과 유사하게 보이기 때문입니다. 보시다시피 일부 유사 도메인은 여타 유사 도메인보다 더 효과적이지만, 도메인 이름을 무엇으로 지정하는지는 유사 도메인의 효과에서 일부를 차지할 뿐입니다. 유사 도메인이 배포되는 방식도 캠페인의 전반적인 성공에 큰 영향을 미칠 수 있습니다. okta[.]Infoblox[.]com나 okta-Infoblox[.]com 와 같은 Okta 또는 MFA 유사 도메인을 예로 들어보겠습니다. 도메인을 방문하기 전에 각 도메인 이름을 여러 번 확인하는 신중한 사람(행운을 빕니다)은 SLD(2단계 도메인)의 "i"가 실제로 소문자 "L"이라는 것을 알아차릴 수도 있습니다. 그러나 이러한 유사 도메인을 고용주의 온라인 프로필에 있는 전화번호로 전송된 그럴듯한 SMS 메시지 등과 함께 활용하면 상황이 달라질 수 있습니다. 여기에 긴급하게 행동을 촉구하는 전화 통화까지 걸려오면 완전히 설득되게 됩니다. 물론 이는 유사 도메인을 사용하는 일반적인 캠페인이 아니라 모든 요소가 총동원된 가상의 스피어피싱 예이지만, 요점은 유사 도메인 기법이 여러 가지 방법으로 도메인과 DNS 인프라의 여러 부분에 효과적으로 적용될 수 있다는 점입니다.

자주 인용되는 속담인 "한 번 속지 두 번 속냐"는 유사 도메인에는 적용되지 않는다는 뜻입니다. 가장 예리한 눈썰미와 보안 인식이 투철한 개인조차도 유사 도메인의 희생양이 될 수 있으며, 이러한 실수를 계속 반복할 수 있습니다. 이 전쟁에서는 악의적인 행위자들이 우위를 점하고 있지만, 아직 패배한 것은 아닙니다. Infoblox는 조직이 공격에 대응하고 효과적으로 방어할 수 있는 역량을 갖추도록 지원하는 DNS 수준의 솔루션을 제공합니다.

IOCs

이 백서의 전체 목록은 *GitHub* (*https://github.com/infobloxopen/threat-intelligence*)에서 확인할 수 있습니다.

INFOBLOX 솔루션

유사 도메인은 그 효과와 대규모 탐지의 어려움으로 인해 공격자들에게 여전히 애용됩니다. 합법적인 표적을 모방하려는 의심스러운 도메인을 자동으로 식별하는 것이 어렵기 때문에 문제는 더욱 더 복잡합니다. 이로 인해 기업 도메인이나 공급망을 사칭하는 유사 도메인에 대한 기업과 정부 기관의 우려는 점점 더 커지고 있습니다.

Infoblox BloxOne Threat Defense(B1TD) Advanced는 유사 위협에 대한 독특하고 광범위하며 포괄적인 솔루션을 제공합니다. Infoblox는 대규모 DNS를 활용하여 매일 수십만 개의 새로운 SLD에 일련의 분석을 적용할 수 있습니다. 여기에는 IDN 호모그래프의 시각적 유사성 자동 평가와 같은 유사 도메인 감지를 위한 여러 분석이 포함됩니다.

고객은 자주 표적이 되는 도메인 중에서 선택하거나 특수 유사 도메인의 모니터링과 분석을 위한 맞춤 목록을 만들 수 있습니다. 이 심층 분석의 결과는 유사 도매인 보고 UI를 통해 확인할 수 있습니다. 이 UI는 탐지된 유사 도메인이 의심스럽거나 피싱 활동과 연관된 경우에도 플래그를 지정합니다. 전반적으로 고객의 특정 환경과 위험 허용 수준의 요구에 맞게 정책을 맞춤화할 수 있습니다. 또한 상세 도메인 데이터에는 B1TD 고급 UI와 API를 통해 액세스할 수 있는 중요한 주석이 포함되어 있습니다. 이러한 상세 도메인 데이터는 더욱 신속한 위협 조사와 보다 효과적인 사고 대응을 가능하게 하는 컨텍스트를 제공합니다.

이러한 유사 도메인 위협 탐지 기능은 BloxOne Threat Defense에서 제공하는 많은 서비스 중 하나일 뿐이며, 이를 통해 다른 솔루션에서는 파악할 수 없는 위협을 파악하고 위협 라이프사이클 초기에 공격을 멈출 수 있습니다. 또한 광범위한 자동화와 생태계 통합을 통해 SecOps의 효율성을 높이고, 기존 보안 스택의 효율성을 높이고, 디지털 및 원격 업무를 안전하게 보호하고, 사이버 보안에 소요되는 총 비용을 절감할 수 있습니다.

자세히 알아보기

infoblox.com 방문

LinkedIn에서 Infoblox 팔로우

Twitter에서 Infoblox 팔로우

참조

[1] https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf

[2] https://twitter.com/kgroupcompanies/status/1188878363068391425

[3] https://en.wikipedia.org/wiki/IDN_homograph_attack

[4] https://i.imgur.com/68oL4U9.jpg

[5] https://www.researchgate.net/publication/220420915_The_Homograph_Attack

[6] https://util.unicode.org/UnicodeJsps/confusables.jsp

[7] https://www.igoldrush.com/domain-guide/domain-legal-issues/cybersquatting-and-typosquatting

[8] https://dl.acm.org/doi/pdf/10.1145/3133956.3134002

[9] https://core.ac.uk/download/pdf/34615371.pdf

[10] https://iris.polito.it/retrieve/handle/11583/2970511/1dd2efbb-9eed-4db5-be4f-ecfcc362572c/_Workshop__Data_driven_Soundsquatting_Generation%20(7).pdf

[11] https://incolumitas.com/2016/06/08/typosquatting-package-managers/

[12] https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610

[13] https://www.akamai.com/blog/security-research/combosquatting-keyword-analysis-support

[14] https://www.trendmicro.com/content/dam/trendmicro/global/en/research/23/c/iron-tiger-sysupdate- reappears-adds-linux-targeting/IOCs-iron-tiger-sysupdate-reappears-adds-linux-targeting.txt

[15] https://urlscan.io/result/41e8b29f-55cc-4887-9186-41a064ffb2ac/

[16] https://thehackernews.com/2022/07/microsoft-warns-of-large-scale-aitm.html

[17] https://thehackernews.com/2023/03/microsoft-warns-of-large-scale-use-of.html

[18] https://www.hackread.com/hackers-employee-accounts-twilio-internal-system/

[19] https://www.feldmanauto.com/

[20] https://urlscan.io/result/98f407d6-96b4-4652-bd38-aa44470b5b78/

[21] https://urlscan.io/result/98f407d6-96b4-4652-bd38-aa44470b5b78/

[22] https://blogs.infoblox.com/cyber-threat-intelligence/scammers-first-on-the-scene-for-turkiyes-disaster-of-the-century/

[23] https://urlscan.io/result/4f295f57-7d46-49e9-94f6-d90858a4cfeb/

[24] https://www.coindesk.com/web3/2023/03/02/nft-trading-volumes-hit-2b-in-february-highest-since-luna-crash-thanks-to-blur/

[25] https://nftnow.com/guides/blurs-token-just-dropped-heres-what-you-need-to-know/

[26] https://twitter.com/blur_io/status/1630290782211981312/

[27] https://www.wired.com/story/youtube-bitcoin-scam-account-hijacking-google-phishing/

[28] https://twitter.com/FoolishBB/status/1627059614654279682

[29] https://www.bleepingcomputer.com/news/security/fake-crypto-giveaways-steal-millions-using-elon-musk-ark-invest-video/

[30] https://www.domaintools.com/

[31] https://urlscan.io/result/8e94bf31-7295-47e8-9de4-756743937f46/

[32] https://www.domaintools.com/

[33] https://urlscan.io/result/7f3c8f83-1922-4570-a9b1-1542e32ccc89/

[34] https://urlscan.io/result/f60f5548-4b54-4a97-add5-1f37a89f4e7e/#summary

[35] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-025a

[36] https://blogs.infoblox.com/cyber-threat-intelligence/cyber-campaign-briefs/dont-dial-that-number-distribution-of-phishing-lookalikes-through-fake-support-calls/

[37] https://urlscan.io/result/41a6ef99-fef1-4d08-80e1-623123280b6a/

[38] https://walletconnect.com/

[39] https://urlscan.io/result/a79ba8e3-9f9a-4a9c-b54b-b26a300afc23/

[40] https://bitkeep.com/

[41] https://docs.flutter.dev/

[42] https://www.welivesecurity.com/2023/02/16/these-arent-apps-youre-looking-for-fake-installers/

[43] https://www.virustotal.com/gui/file/ 271229d5d007baf5324fb2705b7a0b3751bd228bbdb08a86e7b7e2856bbf9b08

[44] https://urlquery.net/report/ef86060b-39e3-4e41-a480-a2b138ee0a49

[45] https://elifesciences.org/articles/54846

[46] https://chromium.googlesource.com/chromium/src/+/main/docs/idn.md

[47] https://wiki.mozilla.org/IDN_Display_Algorithm

[48] https://www.xudongz.com/blog/2017/idn-phishing/

[49] https://www.usenix.org/system/files/sec21-hu-hang.pdf

[50] https://tbutler.org/2021/04/16/considering-the-plausibility-of-idn-homograph-attacks

infoblox.

Infoblox는 네트워킹과 보안을 통합하여 비교할 수 없는 성능과 보호를 제공합니다. 포춘지 선정 100대 기업과 신생 혁신 기업에서 신뢰를 받으며, 사용자의 디바이스에 대한 실시간 가시성과 제어 기능을 제공하여 조직 내부에서 발생하는 위협을 조기에 차단할 수 있습니다.

본사
2390 Mission College Blvd, Ste.501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com