infoblox®

UM OLHAR MAIS APROFUNDADO SOBRE OS ATAQUES LOOKAL1KE

UM NOVO ESTUDO REVELA OS VETORES DE AMEAÇAS MAIS RECENTES

Abril de 2023

OS DOMÍNIOS LOOKALIKE ATINGEM TODOS

ÍNDICE GERAL

RESUMO EXECUTIVO

Desde o surgimento da internet, os agentes de ameaças têm usado domínios visualmente semelhantes para enganar os usuários e levá-los a visitar sites mal-intencionados. Esses domínios, chamados de domínios lookalike, estão tão relacionados a ataques de phishing que o treinamento em conscientização de segurança inclui aprender a inspecionar links em busca deles.

No entanto, apesar das campanhas de conscientização e dos avanços tecnológicos, os domínios lookalike representam uma ameaça persistente para consumidores e organizações, essas ameaças estão sempre sendo aprimoradas pelos agentes. Todos são alvos: de consumidores a governos, de grandes marcas de varejo a pequenos restaurantes, de empresas de tecnologia mundialmente renomadas a empresas menos conhecidas, como a nossa. Neste artigo, você verá que "todo mundo é um alvo" com exemplos de domínios e campanhas reais. Como uma empresa de menor porte em um setor bastante específico, até mesmo nós somos alvo de ataques.

Este relatório descreve o cenário atual de ameaças, trazendo exemplos do mundo real em todos os setores e grupos de usuários. A Infoblox vem detectando domínios lookalike há anos e analisa mais de 70 bilhões de eventos de domain name system (DNS) diariamente para encontrar ameaças potenciais e novas. Para este artigo, focamos nas detecções de janeiro de 2022 a março de 2023. Dos mais de 300.000 domínios lookalike, selecionamos uma amostra que destaca os desafios e os riscos associados a esses ataques.

Os domínios Lookalike estão frequentemente associados a ataques não direcionados e abrangentes por meio de spam por e-mail, publicidade, mídias sociais e mensagens de SMS. Todos os dias, há milhares de novos domínios registrados que imitam softwares populares, instituições financeiras e serviços de entrega de encomendas. Os ataques de phishing que visam roubar credenciais de usuários ou infectar máquinas com malware são tão predominantes e, muitas vezes, tão pouco sofisticados que se tornaram fonte de vários memes, incluindo «você não pode cair em golpes de phishing se não checar o seu e-mail». Embora frequentemente retratado de forma cômica, o phishing é um problema sério. O Anti-Phishing Working Group (APWG) relatou que o phishing atingiu um nível recorde no terceiro trimestre de 2022.[1]

> [ ] ***Todos os indicadores neste artigo foram neutralizados, independentemente do seu status como maliciosos ou legítimos. Desabilitamos os indicadores colocando colchetes entre os pontos [.] e, assim, impedimos que ele se torne um link clicável.***

70+ BILHÕES

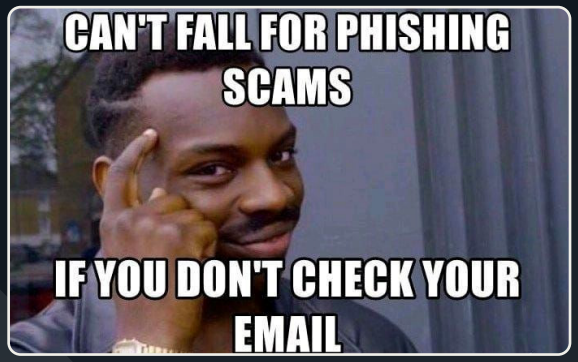
A Infoblox analisa diariamente mais de 70 bilhões de eventos de DNS a fim de identificar novas ameaças.

300K

domínios lookalike foram selecionados para este artigo, destacando o desafio e o risco desses ataques.

UM EXEMPLO DE UM MEME DE PHISHING.

Um exemplo é esse tweet de 2019.[2]



Crédito da imagem: A origem desse meme é desconhecida.

Os domínios falsos não são apenas uma ameaça para os consumidores, eles também são utilizados para obter acesso às redes corporativas.

Divulgações recentes mostraram ataques direcionados nos quais agentes mal-intencionados enganaram funcionários fazendo com que eles informassem suas credenciais de autenticação multifator (MFA). Na maioria dos casos, os domínios lookalike não apenas imitavam a empresa, mas também incluíam palavras-chave de MFA, fazendo com que os usuários acreditassem que a conexão era segura. Percebemos que os agentes mal-intencionados têm como alvo empresas grandes e pequenas, em muitos setores, incluindo provedores de serviços de internet, bancos e criptomoedas, software e serviços, e seguradoras em todo o mundo. Esses ataques começaram no início de 2022 e ganharam força ao longo do tempo.

A utilização dos domínios lookalike é lucrativo porque se trata de um ataque assimétrico. Os usuários devem estar sempre atentos para proteger suas contas pessoais e as informações dos seus empregadores. Os baixos custos de registros de domínios e a possibilidade de espalhar ataques em larga escala dão aos agentes uma vantagem. Eles têm a vantagem da escala e, embora as técnicas para identificar atividades mal-intencionadas tenham melhorado ao longo dos anos, os defensores têm dificuldade em acompanhar o ritmo.

Não apenas o lookalike phishing está prosperando, mas uso de lookalikes se tornou mais complexo, de uma forma que é revelada mais claramente nos registros DNS. Nossa pesquisa mostra que os domínios falsos estão sendo usados para mais finalidades, além das tradicionais de phishing e typosquatting. Eles também estão sendo usados de maneiras não vistas antes: por exemplo, como nameservers e para distribuição de e-mails de spear phishing. Existem grandes redes dedicadas que atendem apenas os domínios lookalike e visam tanto consumidores quanto funcionários do governo.

A Infoblox possui vários algoritmos capazes de identificar domínios lookalike. Usamos uma combinação de métodos que inclui: observar variantes de alvos comuns nos setores de compras, bancos, software e financeiro; observar variantes de domínios especificados pelos clientes; e observar agentes de infraestrutura de DNS especializados em domínios falsos. Essa abordagem multifacetada nos oferece uma ampla cobertura dos cenários de ameaças.

NOTA IMPORTANTE: Este relatório contém vários exemplos que ilustram a amplitude e a profundidade dos domínios lookalike não havendo a intenção de sugerir ataques bem-sucedidos ou violações de qualquer entidade.

HISTÓRICO

Como todos os bons trabalhos de pesquisa, vamos começar com algumas informações básicas. Vamos falar principalmente de vocabulário. Sabemos que a maioria dos leitores ignora a seção de histórico, por isso a mantivemos resumida.

Lookalikes maliciosos: domínios registrados por invasores que parecem iguais ou muito semelhantes a um domínio conhecido, são uma ameaça bem conhecida e persistente no cenário cibernético. Em geral, os lookalikes têm aplicações tanto ofensivas quanto defensivas. No sentido ofensivo, são usados para enganar onde quer que existam olhos humanos. Os agentes mal-intencionados usam os lookalikes para roubar dinheiro, obter credenciais ou acessos, coletar informações de identificação pessoal, espalhar malware ou ganhar dinheiro com anúncios. Eles também são usados para fins políticos e para manchar a reputação de uma marca. Em resumo, eles são um meio para atingir um objetivo dos criminosos cibernéticos. No sentido defensivo, muitas organizações registram proativamente domínios semelhantes aos seus para evitar que os invasores façam isso.

Os lookalikes assumem diferentes formas. No espaço DNS, os domínios podem ser:

- **Homógrafos**
- **Combosquats**
- **Typosquatting**
- **Soundsquats**

Podem ser praticamente indistinguíveis do domínio-alvo original ou objetivamente bem diferentes. Grande parte do sucesso dos domínios falsos como vetor de ataque se deve ao ônus imposto às pessoas.

Como veremos, os lookalikes podem ser encontrados em todos os elementos de um ataque, desde endereços de remetentes de e-mail até URLs de phishing, comando e controle de malware (C2). Embora geralmente associados a registros de endereço (A/AAAA), também encontramos domínios falsos usados para registros nameserver (NS), ponteiro (PTR) e nomes canônicos (CNAME). Eles podem ser implantados através de e-mails, SMS ou mensagens de texto, websites comprometidos, redes de publicidade maliciosa e ligações telefônicas. Na seção a seguir, descrevemos brevemente as diferentes formas de lookalikes e daremos exemplos de cada uma delas.

A CULPA É DA MÁQUINA DE ESCREVER

Na verdade, essa questão moderna remonta aos primeiros dias das máquinas de escrever. Em muitas máquinas de escrever antigas, não havia teclas 0 ou 1, pois esperava-se que os datilógrafos usassem letras maiúsculas O e L minúsculas para representar esses dígitos.[4]

HOMÓGRAFOS (OU HOMOGLIFOS)

Embora a palavra homógrafo signifique "duas palavras que são escritas da mesma forma, porém não necessariamente pronunciadas da mesma maneira e que têm significados diferentes", o termo homógrafo tem sido usado por muitos anos na literatura de pesquisa de segurança com o significado: "dois domínios que parecem visualmente iguais".[3] Um termo mais preciso seria homoglyph. Esses domínios são parecidos entre si e, em alguns casos, podem ser quase indistinguíveis. *Para fins de consistência com a literatura de pesquisa, usaremos o termo homógrafo neste artigo.*

Esse tipo de lookalike aproveita o fato de que muitos caracteres do mesmo conjunto de caracteres, ou alfabeto, se parecem entre si. Por exemplo, 0 (o dígito zero) e O (letra maiúscula de "o"), ou "l" (letra minúscula de "L") e "l" (letra maiúscula de "i"). Alguns tipos de fontes acentuam ainda mais esse problema. Alguns exemplos clássicos são g0ogle.com e lnfoblox.com, nos quais o "o" no Google é substituído por um zero (0) e o "i" em lnfoblox é substituído por um "L" minúsculo, respectivamente.

À medida que a Internet evoluiu e mais pessoas que não falam inglês começaram a se conectar à World Wide Web, cresceu a necessidade por nomes de domínio internacionais (IDNs). Um IDN é um domínio que contém pelo menos um caractere em escrita não latina; a introdução do Unicode possibilitou o aumento desses domínios. Com os IDNs, surgiu uma nova forma de lookalike: o homógrafo IDN. Ele continua sendo um homógrafo, mas usa caracteres de outros conjuntos de caracteres ou alfabetos que são parecidos. Gabrilovich e Gontmakher mostraram o poder dos homógrafos IDN em seu artigo de 2002 "The Homograph Attack". Os autores acharam um homógrafo do domínio autêntico da Microsoft, microsoft[.]com que continha as letras cirílicas "c" e "o".[5] O resultado final é um domínio www.microsoft[.]com, que é visualmente indistinguível do domínio autêntico da Microsoft.

O Unicode Consortium publicou uma ferramenta que mostra o grande número de caracteres confundíveis disponíveis para uma determinada string.[6] A string "hi" tem 684 variações com caracteres unicode; para uma string como "infoblox", o número sobe para mais de 2,2 trilhões de variações. Algumas variações são menos eficazes para um lookalike do que outras. Por exemplo, o Unicode Consortium lista "৯" (número cinco do alfabeto árabe-indiano) como um caractere potencialmente confundível com "o" (letra latina minúscula de "O").

Claramente, inf৯bl৯x[.]com não é um lookalike muito eficaz, mas você consegue ver a diferença entre os domínios quando colocados na fonte Arial, comumente usada, {infoblox[.]com} e {infoblox[.]com}(contendo um "i" minúsculo em bielorrusso ou ucraniano e a letra armênia minúscula "vo", escrita como "n")? Nós também não conseguimos.

TYPOSQUATS

Os domínios typosquat se aproveitam de nomes de domínios populares e de erros de digitação que os usuários cometem, ou que são causados por digitações em teclados defeituosos. Esse termo geralmente está associado a domínios registrados, mas não utilizados, com o objetivo de atrair dinheiro com publicidade. Por exemplo, um dos autores estava recentemente tentando pagar o aluguel por meio do portal on-line do seu grupo de administração de imóveis, hospedado no appfolio[.]com (uma empresa de software bem conhecida que oferece soluções SaaS para grupos de gerenciamento de propriedades e proprietários). Em vez disso, ele digitou errado e quase entrou no appfollio[.]com, que foi registrado em 2013, mas atualmente está sem uso.

Curiosamente, outro domínio typosquat para a Appfolio, apfolio[.]com, parece ser de propriedade da Appfolio. Ele redireciona para o domínio correto e tem o mesmo registrante, empresa registrante e registrador, e foi registrado apenas um mês após o domínio legítimo appfolio[.]com. Este é um exemplo do uso defensivo de lookalikes. Infelizmente, os agentes mal-intencionados estão em vantagem porque simplesmente existem muitas possibilidades para que as organizações consigam registrar todas as variações semelhantes.

Os typosquats são vistos primariamente como um método de monetização, mas podem ter um propósito malicioso. Embora sejam usados para vender anúncios de terceiros ou para vender ao proprietário legítimo do domínio, também podem ser usados para programas de marketing de "blackhat" e como domínios C2 de malware, conforme mostraremos mais adiante. As marcas e empresas têm proteção civil contra typosquatting de acordo com a Anticybersquatting Consumer Protection Act. Devido a essa ameaça de ação legal, o typosquatting é visto como uma forma "blackhat" de monetização na comunidade de compra e venda de domínios, e grandes especialistas em compra e venda de domínios, como a iGoldrush, recomendam evitar o typosquatting para obtenção de lucro.[7]

EXEMPLOS DE TYPOSQUAT

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

de domínios de combosquatting abusivos ficam ativos por mais de 1.000 dias

de domínios de combosquatting abusivos aparecem em pelo menos uma lista de bloqueio pública 100 dias após as resoluções iniciais

COMBOSQUATTING

Combosquatting é uma forma de lookalike que combina nomes populares de marcas ou empresas com outras palavras-chave. Termos como suporte, ajuda, segurança e e-mail são comuns. Considere, por exemplo, wordpresssupport[.]ru, wordpresssupport[.]store e wordpress-security[.] cloud. Esses domínios estão todos hospedados no mesmo endereço IP baseado na Rússia e se parecem com WordPress, o popular software de conteúdo da web. A inclusão de suporte e segurança no domínio indica que eles se destinam a usuários do WordPress. Eles podem ser usados para reunir credenciais para sequestrar sites da WordPress ou coletar detalhes de pagamento e informações de identificação pessoal (PII).

Além de gerar domínios combosquat por conta própria, os agentes mal-intencionados também podem usar algoritmos de geração de domínio de dicionários (DDGAs) para criar lookalikes. Em segundos, milhares de opções de domínios podem ser gerados para uma grande variedade de marcas ou empresas. Por pura sorte, o algoritmo pode criar opções de domínios com as palavras-chave certas para que sejam eficazes. A comunidade de usuários do Steam, uma das principais plataformas de jogos, é um alvo comum para os agentes mal-intencionados que usam combosquat DDGAs. Alguns exemplos de domínios em uma amostra observada recentemente são: steamcommiunity[.]com[.]ru, steamcommucnity[.]com[.]ru, steamcommunityjp[.]top, e steamcommunityiq[.]top. Observe a sobreposição entre typosquatting e combosquatting nessa amostra de domínios.

Kitsin e outros pesquisadores realizaram um estudo longitudinal de combosquatting em 2017, analisando cerca de 468 bilhões de registros DNS (provenientes de conjuntos de dados ativos e passivos) e encontraram resultados preocupantes:

- **Os domínios combosquat prevalecem 100 vezes mais, comparados aos domínios typosquatting**
- **60% dos domínios de combosquatting abusivos ficam ativos por mais de 1.000 dias**
- **20% dos domínios de combosquatting abusivos aparecem em pelo menos uma lista de bloqueio pública 100 dias após as resoluções iniciais**
- **As resoluções de domínios combosquat aumentaram em relação ao ano anterior[8]**

Concordamos com a conclusão dos autores sobre a prevalência de domínios combosquat. Encontramos mais domínios combosquat do que typosquats puros ou homóGrafos puros (IDN ou outros), por meio das nossas análises.

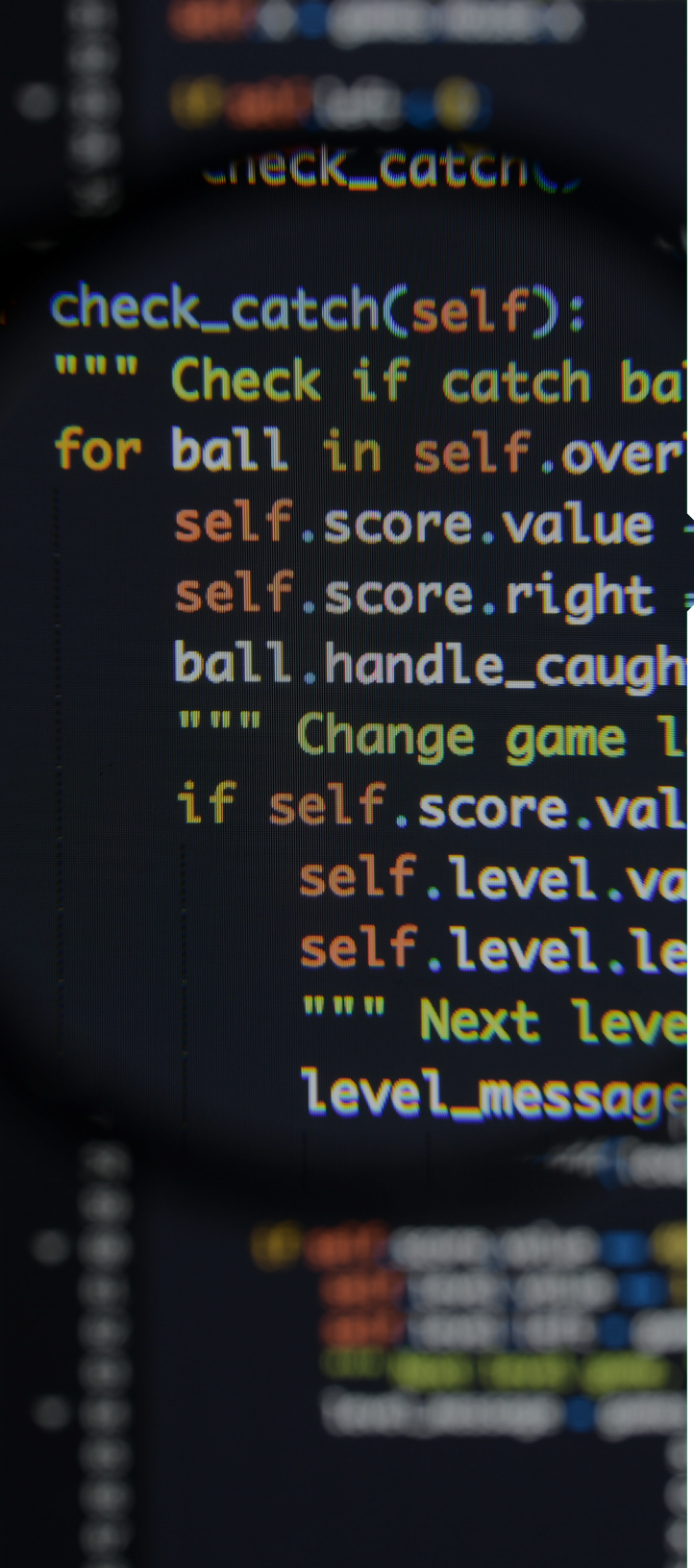
SOUNDSQUATTING

Os domínios de soundsquat aproveitam o uso de homófonos, palavras que têm o mesmo som, mas têm uma grafia diferente. O soundsquatting é a forma de lookalike mais identificada recentemente, a primeira vez que esta prática apareceu na literatura foi em 2014.[9]
O soundsquatting tem recebido mais atenção dos pesquisadores recentemente devido à proliferação de alto-falantes inteligentes, como Alexa, Siri e Google Voice.[10] Os domínios de soundsquat se sobrepõem a outros tipos de domínios lookalike, pois podem tanto soar quanto parecer semelhantes. Descobrimos que os domínios de soundsquatting puros, ou seja, aqueles que não são visualmente semelhantes mas têm sons iguais, são raros; geralmente esses domínios também podem ser encontrados por técnicas de similaridade baseadas em texto.

É importante observar que os lookalikes em uso muitas vezes não se encaixam em categorias bem definidas como as que apresentamos aqui. Uma combinação de formas é usada para maximizar a eficácia de um domínio lookalike. Muitos dos domínios combosquat que vemos têm elementos de typosquats e homógrafos (IDN ou não). Os typosquats utilizam elementos de homógrafos, os soundsquats utilizam elementos de typosquats e assim por diante. O resultado final é um cenário assimétrico de ameaças no qual os agentes mal-intencionados podem deixar os defensores em desvantagem.

O SOM DO ATAQUE

A prevalência do soundsquatting decolou com o advento da tecnologia ativada por voz, como Alexa, Siri e Google Voice.



OUTRAS FORMAS DE LOOKALIKES

Embora o foco deste artigo esteja nos domínios lookalikes e em seu papel no cenário atual de ameaças, existem outros tipos de semelhanças que podem explorar usuários vulneráveis. Um exemplo considerável sobre isso foi encontrado recentemente em pacotes Python PyPi.

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

Os gerenciadores de pacotes para linguagens de programação populares, como Python, estão sujeitos aos mesmos pontos fracos que os domínios. Qualquer pessoa pode fazer upload de um pacote com qualquer nome (desde que esse nome ainda não tenha sido utilizado) contendo código, que pode estar livre ou não, de riscos de segurança. Em 2016, o pesquisador de segurança Nikolai Tschacher utilizou o typosquatting para forçar mais de 17.000 hosts distintos a executar código arbitrário.[11] Em seguida, em 2021, o pesquisador de segurança Alex Birsan pegou a ideia de Tschacher e a expandiu, popularizando o termo “confusão de dependências”.[12]

Birsan encontrou nomes de pacotes privados e internos de grandes empresas através de diversas fontes abertas. Isso incluiu pesquisar o código-fonte em sites, procurar pacotes no GitHub ou até mesmo encontrar nomes de pacotes em fóruns públicos. Em seguida, ele fez o upload dos pacotes com o mesmo nome dos pacotes privados e internos para gerenciadores de pacotes públicos. Por fim, Birsan utilizou pipelines de CI/CD automatizados, “confundindo” os pacotes públicos com os pacotes privados e internos. Em vez de importar e instalar os pacotes privados, os pipelines automatizados encontraram e importaram os pacotes públicos do Birsan. Emseguida, Birsan utilizou a exfiltração de DNS para ser notificado de que seu código arbitrário, e não o pacote privado pretendido, havia sido executado. Essa técnica de lookalike permitiu que ele invadisse 35 organizações, às vezes em questão de horas após fazer o upload de seus pacotes.

Independentemente do tipo de lookalike ou da área em que é utilizado, os lookalikes representam uma ameaça persistente. Parte do desafio de estudá-los é que eles são indefinidos, existem tantas possibilidades que fica difícil computá-las e qualquer coisa pode ser um alvo. Nas seções seguintes, mostraremos exemplos específicos dessas várias formas de lookalikes em uso, incluindo alvos, métodos de implantação, infraestrutura, por que são eficazes, desafios e soluções da Infoblox para o problema.

TODOS SÃO UM ALVO

Acreditamos que você encontrará pelo menos um alvo surpreendente em nossos exemplos.

Uma das descobertas mais impactantes da nossa análise de domínios no DNS foi que todos são alvos: encontramos lookalikes para todos os alvos, incluindo empresas menores e serviços. Esses domínios são utilizados por agentes mal-intencionados para atacar pessoas tanto no ambiente de trabalho quanto em casa.

Conforme observado pela Akamai recentemente, a maioria das campanhas de lookalike só recebe atenção da mídia quando um grande alvo é afetado.[13] Nosso objetivo é trazer à tona tanto esses alvos pouco reportados e ignorados quanto aqueles considerados "típicos". Alguns exemplos são mostrados aqui para demonstrar esse ponto, mas também destacaremos o impacto em diferentes setores, e o uso de várias metodologias será detalhado mais adiante.

NÓS TAMBÉM SOMOS ALVO!

A Infoblox é uma empresa de menor porte com menos de 2.000 funcionários em todo o mundoe.

Embora tenhamos uma grande participação nos mercados DNS, Dynamic Host Configuration Protocol (DHCP) e IP Address Management (IPAM), conhecidos como DDI, esse setor é bastante específico e a Infoblox não é um nome muito conhecido. É de se surpreender que os agentes mal-intencionados estejam cientes sobre nós, e que sejamos visados ativamente com domínios lookalike. No entanto, encontramos muitos domínios criados para enganar nossos funcionários e clientes. Lookalikes de serviços internos, incluindo nosso portal de benefícios, bem como nomes dos nossos produtos foram registrados no último ano.

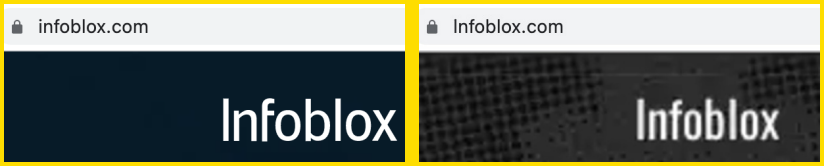


Figura 2. Comparação entre os logotipos do site oficial da infoblox[.]com (E) e do lookalike Infoblox[.]com (D)

Alguns domínios registrados que não pertencem à Infoblox incluem:

Homógrafo **Infoblox[.]com**	O uso de um "L" minúsculo para se passar por um "i" maiúsculo foi registrado em julho de 2022 e, embora esteja à venda, o site mostra no canto superior esquerdo uma renderização que é quase indistinguível daquela que aparece em nosso site corporativo. *Veja uma comparação na Figura 2.*
Typosquat **infobloxbenifits[.]com**	Esse domínio foi registrado na China em abril de 2022 e apresenta um pequeno erro de digitação no nosso portal de benefícios para funcionários. Atualmente, este domínio está com a Bodis, onde está estacionado.
TLD Squat **infoblox[.]info**	Um novo domínio de alto nível, ou TLD, foi registrado em agosto de 2022 através do registrador Sav[.]com, conhecido por ser amplamente utilizado de forma inadequada. Ele está estacionado no dan[.]com, que permite aos usuários vender domínios.
Combosquat **infobloxgrid[.]com**	Um combosquat semelhante ao nosso produto principal usado por milhares de clientes em todo o mundo. Nossa tecnologia Grid™ patenteada permite que os administradores de rede combinem diversos aplicativos de rede em um único sistema. Esse domínio também está disponível em dan[.]com e foi registrado em abril de 2022.
Combosquat **infoblox-updater[.]com**	Exemplo da técnica de usar palavras comuns de software no domínio, como "atualização" ou "suporte". Nesse caso, um cliente pode ser enganado ao se conectar a um sistema falso pensando que existia alguma relação com as atualizações do sistema da Infoblox. Nomes ou produtos de empresas de tecnologia são frequentemente usados para esse tipo de domínio combosquat, que pode ser usado como domínio de phishing ou malware C2. Outros exemplos incluem dev[.]gitlabs[.]me e jira[.]atlas-sian[.]net, ambos usados pelo agente de advanced persistent threat (APT), Iron Tiger em seu malware SysUpdate.[14]

Além de visar pequenas empresas de tecnologia como a nossa, vimos uma ampla gama de lookalikes que são variações enganosas de restaurantes, escritórios de advocacia e outras pequenas empresas.

Além disso, um único agente pode usar marcas conhecidas e pequenas empresas como iscas. Um agente que a Infoblox acompanha há algum tempo criou domínios lookalike para o restaurante Cotenna em Nova York, e copiou seu site, provavelmente para atrair visitantes para fazer reservas on-line utilizando cartões de crédito.[15] O site cotenna[.]nyc foi registrado em abril de 2022 e é semelhante ao site do restaurante cotenna[.]com. Esse mesmo agente tem domínios lookalike direcionados a grandes empresas de mídia social, como o Twitter.

Nas seções a seguir, abordaremos mais detalhadamente os setores que são mais visados atualmente, bem como algumas das várias maneiras pelas quais os domínios podem ser usados para um ataque bem-sucedido. Como todos são alvos, destacaremos as áreas nas quais vimos as atividades mais maliciosas, com base em uma análise de 300.000 domínios lookalike.

TODOS PODEM SER ALVOS DE DOMÍNIOS LOOKALIKE

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

10K+ ORGS

Em julho de 2022, a Microsoft alertou que mais de 10.000 organizações foram alvo de ataques AitM projetados para roubar credenciais MFA dos usuários em tempo real.

1.600+

Nossa pesquisa encontrou mais de 1.600 domínios que continham uma combinação de recursos lookalike corporativos e MFA.

ELES VISAM OS FUNCIONÁRIOS

Até pouco tempo atrás, muitas empresas achavam que o uso da autenticação multifatorial (MFA) protegia suas redes internas contra ataques de phishing.

Mas, no início de 2023, a Coinbase revelou que seus funcionários foram alvo de ataques de spear phishing que usavam domínios lookaliKe para o login MFA interno da empresa. Esta revelação foi prontamente seguida por relatos de outras empresas, confirmando que também foram alvo de ataques semelhantes. Com base nos relatos das vítimas, sabemos que os agentes mal-intencionados enviaram mensagens SMS aos funcionários, bem como e-mails, solicitando que eles se conectassem aos sistemas internos. Em alguns casos, ligações telefônicas também faziam parte do plano, durante essas ligações, o agente mal-intencionado fornecia um nome de domínio para que o funcionário visitasse em seu navegador. Os invasores usaram o adversary-in-the-middle (AitM) para convencer os funcionários de que eles estavam interagindo com a rede real da empresa. Os funcionários eram solicitados a fornecer um código MFA, que era então capturado pelo invasor e usado para obter acesso aos sistemas internos.

A Microsoft alertou, em julho de 2022, que mais de 10.000 organizações foram alvo de ataques AitM projetados para roubar credenciais de MFA dos usuários em tempo real.16 Esses ataques eram específicos para o uso da autenticação do Outlook 365, mas a Microsoft informou ainda, em fevereiro de 2023, que um kit de phishing, que permitia ataques de MFA, estava disponível para venda em julho de 2022 e era amplamente utilizado.[17] Outras empresas, incluindo a Twilio, haviam divulgado ataques semelhantes no verão de 2022, mas a amplitude dos ataques não foi bem divulgada até as revelações da Coinbase.[18]

Para investigar esse incidente, realizamos uma análise retrospectiva de domínios lookalike que imitavam a MFA usando palavras-chave como “mfa”, “okta” e “2fa”. Nossa pesquisa constatou uma ampla variedade de alvos e um nítido aumento na atividade a partir de julho de 2022, embora tenha havido um número significativo de domínios lookalike utilizados para esses ataques no início do ano. Mais de 1.600 domínios continham uma combinação de recursos lookalike corporativos e MFA. Os alvos variaram desde grandes corporações, como Coinbase, Reddit e Twilio, até grandes bancos, empresas de software, provedores de serviços de internet, entidades governamentais e plataformas de jogos em todo o mundo. Também foram alvos, mas com pouca divulgação, empresas menores de tecnologia, supermercados e varejistas.

Como exemplo de alvos menos conhecidos, vários domínios lookalike MFA imitavam a Western Electricity Coordinating Council (WECC).
TA WECC promove a confiabilidade do sistema elétrico em massa para uma grande parte do oeste dos Estados Unidos. Os lookalikes incluíam o wecc-okta[.]org, wecc-oktc[.]org e wecc-okta[.]com. Todos foram registrados em fevereiro de 2023 e compartilham um endereço IP.

Outro exemplo surpreendente é a Feldman Auto Group, que contempla várias concessionárias de automóveis nos Estados Unidos.
Embora a empresa tenha uma relação de marca com o ator americano Mark Wahlberg, é uma empresa de tamanho moderado, com 18 unidades no centro-oeste.[19] Um MFA semelhante a este domínio, feldmanauto-okta[.]com, foi registrado no final de janeiro de 2023.

Alguns dos alvos corporativos dos domínios lookalike MFA são mais incertos.
O domínio frb-okta[.]com mostra um prompt de login com um logotipo FRBOkta indefinido que poderia ser o Federal Reserve Bank, First Reserve Bank ou um site semelhante ao da empresa de roupas polonesa Farbokta.[20] Em muitos casos, não podemos ter certeza sobre quem era o alvo, e o kit de phishing pode ter ficado ativo por pouco tempo. *Incluímos uma captura de tela do login na Figura 3 para que você possa fazer suas próprias suposições.*

Esses ataques AitM também foram usados contra consumidores em 2022, especialmente aqueles da comunidade de jogos que utilizam MFA para proteger suas compras.
Em um caso conhecido pelos autores, as vítimas foram atraídas para visitar um site a partir de uma transmissão ao vivo do Twitch de um jogo online popular. Depois de inserir suas credenciais de MFA, elas sofreram um breve ataque de negação de serviço (DoS) contra sua rede doméstica, causando uma interrupção na internet por vários minutos. Quando conseguiram retornar para sua conta do jogo, todas as suas compras tinham sido roubadas. *Podemos pensar nos jogadores como adolescentes que moram com os pais, mas a quantidade de dinheiro gasta em compras no aplicativo torna os jogos e seus jogadores, do Roblox ao Counter-Strike, um alvo lucrativo.*

LOOKALIKE MFA FRBOKTA.COM

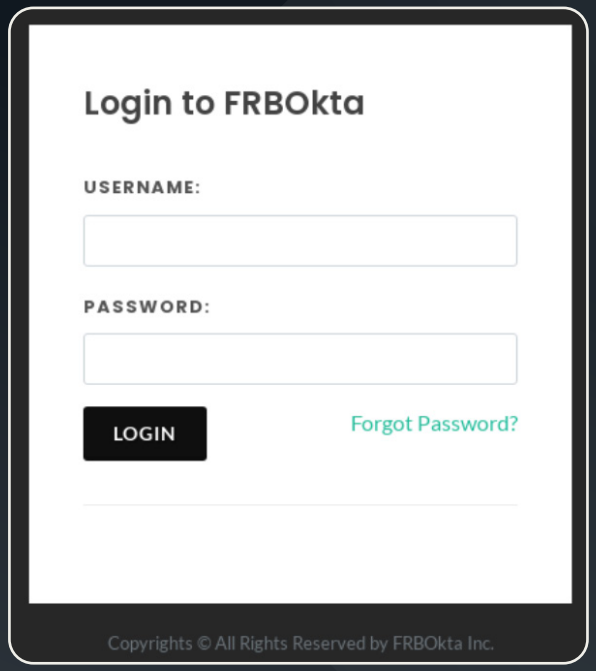


Figura 3. O site frb-okta[.]com mostra uma página de login indefinida com uma referência ao FRBOkta. Crédito da imagem: URLScan.[21]

PÁGINA LOOKALIKE DO MINISTÉRIO TURCO

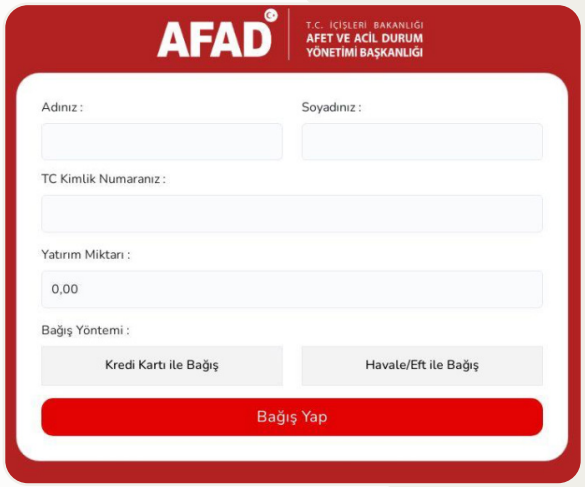


Figura 4. lookalike AFAD afadestek[.]net.
Crédito da imagem: DomainTools.

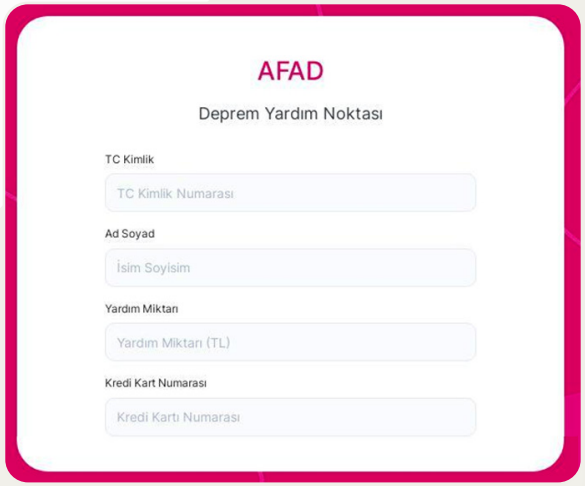


Figura 5. Domínio lookalike AFAD afadbagislari[.]net.
Crédito da imagem: DomainTools.

ELES VISAM OS QUE FAZEM O BEM

Os golpistas que procuram roubar dinheiro geralmente são os "primeiros a responder" quando se trata de usar eventos e desastres mundiais para ganhos ilícitos.

A Infoblox descobriu que os golpistas são rápidos em tirar proveito de qualquer evento noticiado, como crises de saúde como a COVID-19 ou a invasão russa na Ucrânia. Infelizmente, 2023 trouxe uma crise humanitária com o terremoto turco-sírio no início de fevereiro.[22] Após o terremoto inicial em 6 de fevereiro, vários domínios fraudulentos tentaram imitar sites da AFAD (Autoridade de gerenciamento de emergências e desastres) da Turquia.Esses domínios incluíam "AFAD" no nome de domínio totalmente qualificado, tentando imitar o domínio legítimo afad[.]gov[.]tr. Os exemplos abaixo são de domínios recém-registrados e, embora tenham um nome de domínio totalmente qualificado (FQDN) extenso, todos começam com "AFAD".

O uso de FQDNs mais longos proporciona aos fraudadores mais permutações do domínio legítimo para uso em várias campanhas com o tema AFAD:

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

Além do combosquatting, alguns desses sites usam o logotipo legítimo da AFAD para ajudar a induzir os visitantes a fazerem doações. Por exemplo, o site fraudulento afadestek[.]net foi registrado em 7 de fevereiro e tinha um design web semelhante ao site legítimo da AFAD turca, conforme mostrado na *Figura 4*. De acordo com a tradução automática, ele parece coletar doações por cartão de crédito ou ordens de pagamento por meio de transferência eletrônica, além de coletar informações de identificação pessoal, como nome, sobrenome e números de identidades.

Outros domínios fraudulentos nem se deram ao trabalho de usar o logotipo oficial da AFAD e foram rapidamente criados para maximizar a quantidade de dinheiro que poderiam extrair dos doadores. Dois exemplos são: afadbagislari[.]net e afadyardimyap[.]net, ambos hospedados no mesmo endereço IP. A infraestrutura dedicada para lookalikes é comum e será discutida com mais detalhes posteriormente. Ambos os sites apresentam o mesmo layout e conteúdo, mostrados na *Figura 5*, solicitando doações para ajudar as vítimas do terremoto por meio de pagamentos com cartão de crédito.

ELES VISAM AS CRIPTOMOEDAS

Além dos golpistas que buscam ganhar dinheiro rápido, os lookalikes são muito usados para roubar credenciais.

Um domínio lookalike é provavelmente o que a maioria das pessoas leigas imagina quando pensa em um site genérico de "phishing" que tenta obter credenciais dos usuários. Com o aumento da popularidade das criptomoedas, os invasores têm como alvo esses serviços financeiros, incluindo plataformas, carteiras e exchanges. Encontramos uma série de lookalikes muito convincentes da popular exchange Coinbase, sediada nos EUA. Um desses sites é mostrado na *Figura 6*.[23]

Os domínios da tabela abaixo, por exemplo, foram registrados em janeiro de 2023:

Tabela 1. Exemplos de domínios semelhantes aos da corretora de criptomoedas Coinbase.

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

Com o crescimento dos tokens não fungíveis (NFTs), cujas negociações atingiram mais de 2 bilhões de dólares em fevereiro de 2023, os agentes mal-intencionados agiram rapidamente para ampliar suas operações além das criptomoedas tradicionais, buscando roubar dinheiro dos investidores.[24] Por exemplo, a plataforma de negociação Blur foi inaugurado em outubro de 2022 e o Blur token foi lançado alguns meses depois, gerando um investimento recorde em NFTs a partir de maio de 2022.[25] Começamos a ver lookalikes do Blur logo após o lançamento do produto e, em seguida, observamos um aumento drástico à medida que a plataforma crescia em popularidade.

LOOKALIKE COINBASE

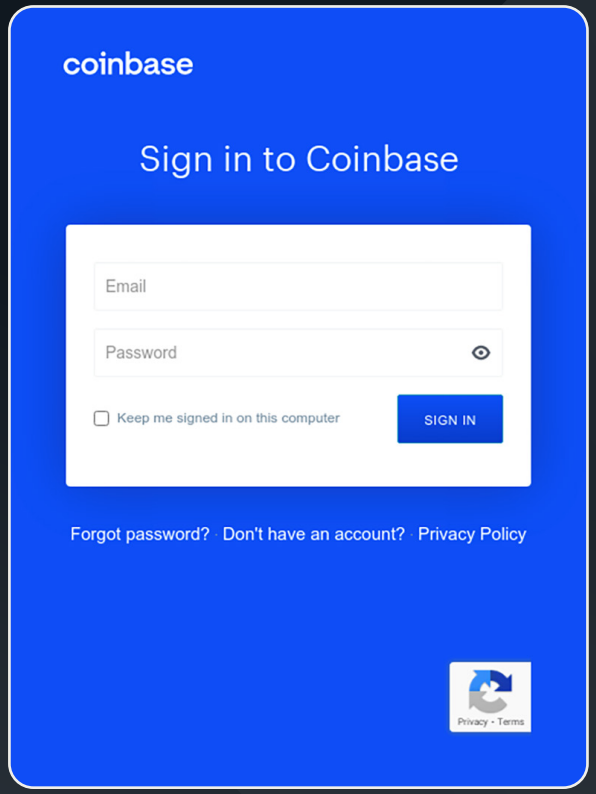


Figura 6. Lookalike Coinbase click-coinbase[.]com. Crédito da imagem: DomainTools.

LOOKALIKE NFT BLUR

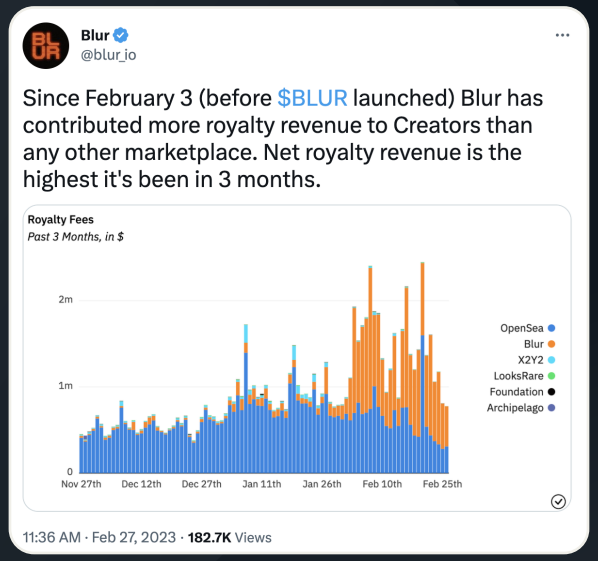


Figura 7. O mercado de NFT da Blur está entre os principais impulsionadores dos US$ 2 bilhões em negociações de NFT observados em fevereiro de 2023.[26] Crédito da imagem: Infoblox

Na preparação para o lançamento do Blur Token em 14 de fevereiro de 2023, vimos um aumento de cinco a seis vezes no número de lookalikes relacionados à Blur. Mesmo com a quantidade caindoum pouco em março de 2023, esse padrão demonstra a disposição dos agentes mal-intencionados de acompanhar as tendências do mundo das criptomoedas para ganhar dinheiro rápido.

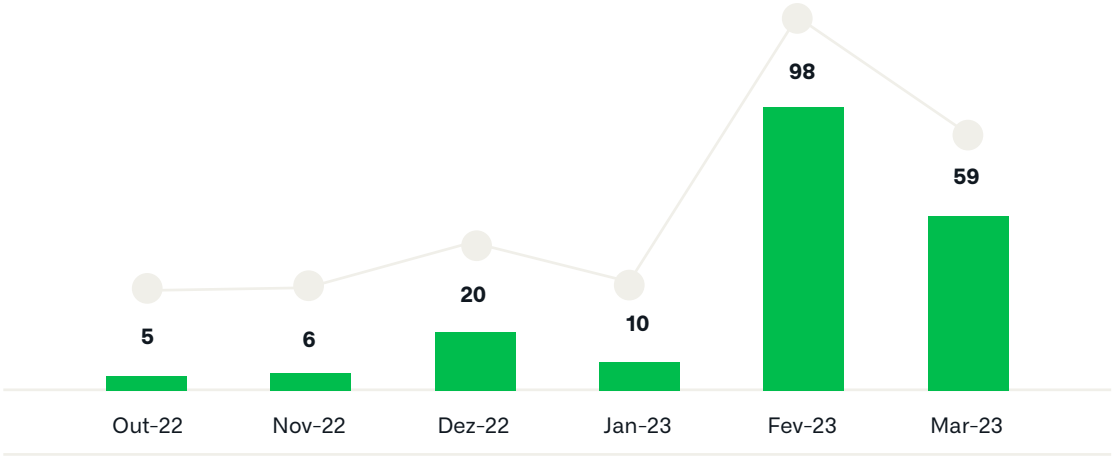


Figura 8. Aumento significativo de lookalikes relacionadas à Blur desde o anúncio em outubro de 2022.

A Infoblox rastreia vários agentes mal-intencionados que se especializaram em lookalikes relacionados a criptomoedas. Esses agentes têm como alvo todas as principais entidades do mercado, incluindo a Blur e sua concorrente Yuga Labs, dona da ApeCoin e da popular NFT Bored Ape Collection. Na tabela abaixo, apresentamos uma pequena amostra desses domínios. As técnicas usadas por esses agentes incluem alterações simples no domínio de primeiro nível (TLD), a adição de uma única letra e nomes de domínio unicode, que podem ser particularmente difíceis de reconhecer. Observe na tabela abaixo que há um acento sobre o "i" em apecoíns[.]com. No DNS, esse domínio se parece com xn--apecons-cza[.]com, o que é um pouco difícil de reconhecer como lookalike, mas em um navegador da web ele seria praticamente indistinguível do original.

Tabela 2. Exemplos de domínios lookalikes Blur token e Yuga Labs.

Domínios lookalikes Blur [blur.io]	**Domínios lookalikes Yuga Labs [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

Há também lookalikes menos tradicionais relacionados a criptomoedas que usam o YouTube como um vetor para atrair alvos para seus domínios.

Esses esquemas começam com os agentes de ameaças fazendo spearphishing com criadores de conteúdo populares do YouTube ofertando patrocínios falsos que parecem estar relacionados a produtos legítimos.[27]
Os e-mails solicitam que o criador de conteúdo baixe e abra um arquivo supostamente relacionado à oferta de patrocínio, como uma cópia do software que está sendo promovido, ou um arquivo PDF que contém um contrato de patrocínio.[28] Na realidade, esses arquivos são cargas de malware que, quando abertas, roubam cookies da sessão do navegador da vítima. Os cookies roubados permitem que o invasor obtenha acesso à conta no YouTube, mesmo com a autenticação multifator ativada.

Quando o invasor tem acesso à conta do criador de conteúdo no YouTube, ele tenta disfarçar o fato de que o canal foi hackeado alterando seu nome e foto de perfil para combinar com o tema do seu ataque, que geralmente é algo relacionado ao Elon Musk ou a uma de suas empresas.[29]
O invasor também pode excluir ou ocultar os vídeos existentes do canal para encobrir ainda mais suas atividades. Em seguida, começa a transmitir uma versão editada de um vídeo relacionado a criptomoedas, como o discurso do Elon Musk na Ark Invest, a fim de atrair os assinantes existentes do canal.

These edited videos include a text overlay directing users to visit the attacker's cryptocurrency-related |ooKa|ike domain, and a link to the domain is also included in the description of the stream.
Os domínios são golpes padrão do tipo "dobre seu dinheiro" que levam as vítimas a enviar uma certa quantia de criptomoeda para um endereço de carteira específico, com a promessa de que receberão o dobro desse valor. Nesses ataques, o objetivo do domínio lookalike é aumentar a credibilidade da oferta, combinando seu tema com o vídeo editado e o canal renomeado do YouTube.

LOOKALIKE TESLA

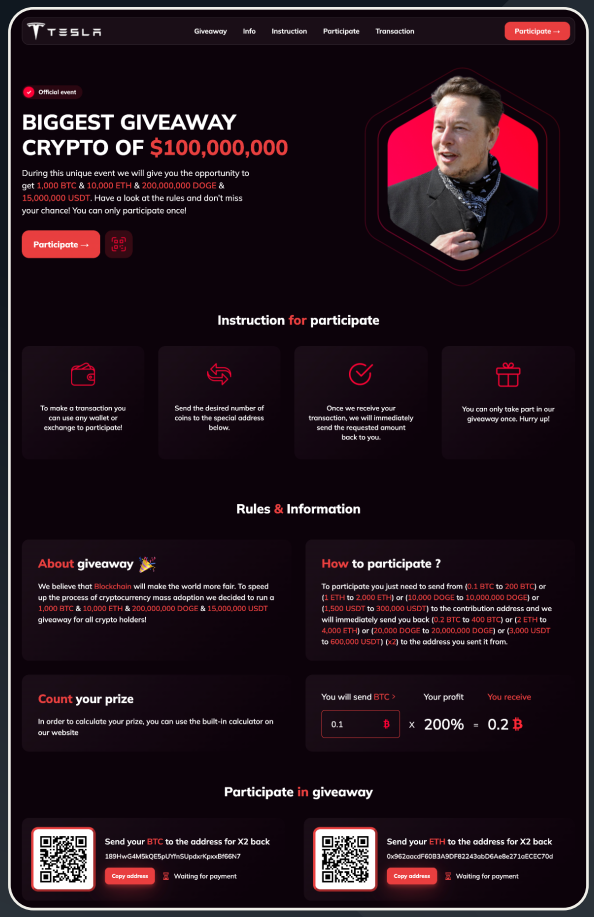


Figura 9. Domínio lookalike Tesla relacionado à criptomoeda, tesla-online[.]net, solicitando que os usuários enviem criptomoedas para endereços específicos a fim de receber o dobro em troca. Crédito da imagem: Infoblox.

ELES VISAM AS REDES SOCIAIS E OS USUÁRIOS DE DISPOSITIVOS MÓVEIS

Plataformas de redes sociais, como Instagram e Twitter, assim com grandes marcas como a Apple, também são alvos populares de phishings lookalikes.

Todas as marcas e serviços populares são continuamente visados nesses ataques, mas usaremos apenas alguns exemplos dessas três marcas como ilustração da ameaça atual. A coleta de credenciais não é novidade, antes do surgimento das redes sociais e das plataformas de ID universal, como Apple ID, os agentes mal-intencionados já tentavam invadir contas de e-mail. No entanto, com a profunda interligação das redes sociais e das plataformas de identificação universal em nossas vidas, esses lookalikes representam uma ameaça persistente.

Os agentes mal-intencionados perseguem as contas de redes sociais de qualquer pessoa, não apenas de influenciadores e celebridades. Há muitos lookalikes para o Instagram - alguns combosquats, outros homógrafos. Muitas vezes, esses domínios apareceram em clusters de domínios registrados simultaneamente, sugerindo que faziam parte de uma campanha coordenada criada usando uma DDGA. Os exemplos abaixo fazem parte de um conjunto do Instagram que combina a marca com palavras, como ajuda e feedback.

Tabela 3. Exemplos de domínios lookalike do suporte do Instagram.

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

O conteúdo desses domínios alega que o usuário violou as regras de direitos autorais do Instagram e pede que ele digite seu nome de usuário para fazer uma contestação. ***Veja as Figuras 10 e 11.***

LOOKALIKE INSTAGRAM

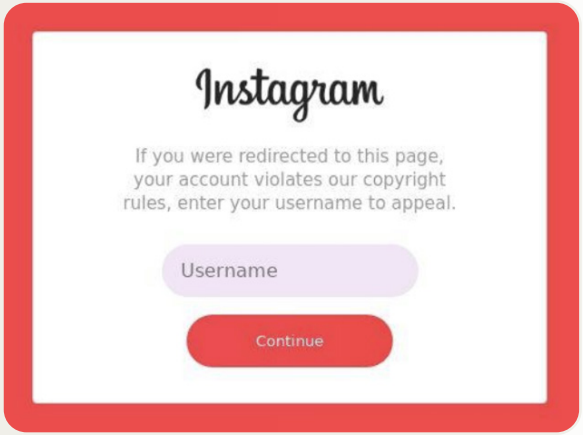


Figura 10. O lookalike do Instagram help-Instagram-notice[.]com mostra uma chamada para ação contra a violação de direitos autorais. Crédito da imagem: DomainTools.[30z]

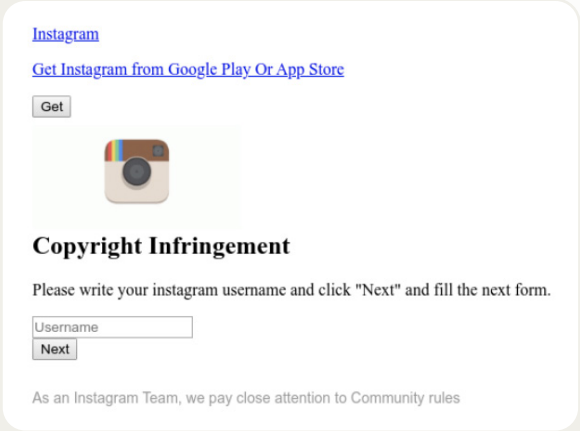


Figura 11. Lookalike do Instagram help-instagram-about[.]com, mostrando outra chamada para ação contra a violação de direitos autorais. Crédito da imagem: URLScan.[31]

LOOKALIKE TWITTER

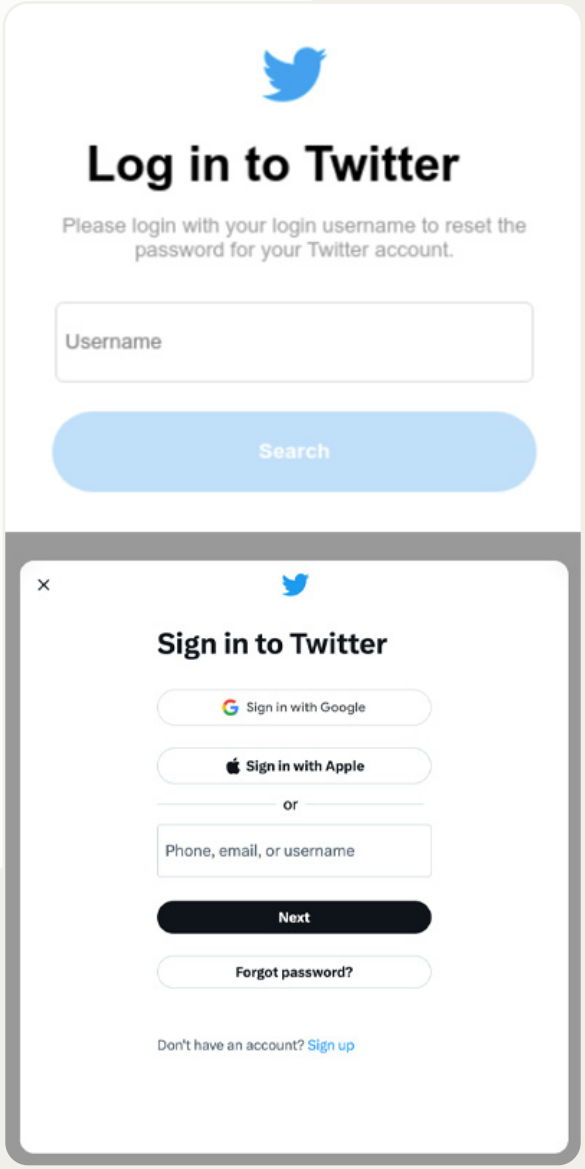


Figura 12. Portal lookalike de redefinição de senha do Twitter, help-twitter-centre[.]net. A imagem de phishing está na parte superior e a legítima está na parte inferior. Crédito da imagem: DomainTools.[32]

Outros lookalikes do Instagram têm como alvo o cobiçado "selo azul" (a verificação do Instagram para uma figura pública), usando um "L" minúsculo no lugar de um "i" maiúsculo. Ironicamente, o Instagram criou o selo azul para personalidades ou empresas conhecidas como uma forma de combater a falsificação de identidade. *Não duvide que os agentes maliciosos usem lookalikes para atacar as próprias soluções anti-lookalikes.*

Alguns exemplos são:

Tabela 4. Exemplos de domínios lookalikes para verificação do Instagram.	
Instagram-blueticket-form[.]ml	Instagram-contactbluebadge[.]ga
Instagram-verification-badges-service[.]com	Instagrambluetickverifcation[.]cf
Instagramverifybadge-contact[.]cf	Instagram-badgecentre[.]gq

Ao rastrear os lookalikes do Instagram, descobrimos que os agentes mal-intencionados não colocaram todos os ovos em uma única cesta.

Os lookalikes do Twitter foram hospedados junto com os lookalikes de "violação de direitos autorais" do Instagram. Esses looka1ikes do Twitter eram domínios combosquat de phishing para obter as credenciais dos usuários, e as páginas de destino pareciam ser um portal legítimo de redefinição de senha. *Veja a Figura 12.*

Além dos lookalikes de redes sociais, durante nossa pesquisa, vimos com frequência lookalikes do iCloud, o serviço de nuvem da Apple que oferece armazenamento em nuvem e sincronização entre dispositivos Apple. Esses domínios utilizavam um número relativamente pequeno de palavras-chave, as palavras que apareceram com mais frequência foram "apple", "findmy", "id" e "icloud". Não faltaram domínios lookalike relacionados à Apple.

Below are a few examples, including some that appear to target Spanish-speaking users:

Tabela 5. Domínios lookalike direcionados a serviços relacionados à Apple.	
supportid-apple[.]com	sopport-apple[.]com
soporte-latam[.]us	soporte-appleid[.]com
lcloud-web-app[.]com	icloud-fndmy[.]com

TODOS SÃO VISADOS

Nossos algoritmos de detecção identificam milhares de novos domínios lookalike todos os dias. Qualquer empresa ou serviço, grande ou pequeno, em que agentes mal-intencionados possam roubar dinheiro ou identidades, será alvo. Encerraremos esta seção com uma variedade de domínios lookalike observados por nós e seus alvos.

Tabela 6. Domínios lookalike e seus alvos.

Domínios lookalike	Alvo lookalike
mee6bot[.]ru	Discord bot, Mee6
vulcan[.]pm	Discord bot, Vulcan
o365-outlook[.]com, ms-o365[.]com, o365-outlook[.]com, https-o365[.]com	Microsoft Office 365
myato-refund[.]online	Australian Tax Office
checkscam22[.]com, checkscams[.]online, checkscammer[.]xyz	Sites de verificação de golpes
xpressvpn[.]business, expressvpn-app[.]com, expressvpn-okta[.]com	Express VPN
anpost-paymentduty[.]com, ups-pay-deliveryfee[.]info, caddelivery postca[.]com	Serviços postais e de entrega
crarebate-info[.]com	Reembolso de imposto canadense
ebl-ch[.]com	Empresa suíça de energia EBL
op-fi-palvelut[.]co, op-fi-io[.]in	Op[.]fi, banco digital finlandês e serviços de seguro
boatairbuds[.]in, boatbudsmusc[.]in, boatflashsale[.]in, boatmusicairbud[.]in	Empresa indiana de tecnologia BoAt
pumauaeshoes[.]com, pumanzsale[.]com, pumaireland[.]com, vejaoutletcanada[.]ca	Empresas de calçados
secure1-scotiabank[.]com,r-scotiabank[.]com, chasebank-jpm[.]com, thetrustnationalbank[.]com, amèricafirst[.]com	Bancos
sprint-ldg[.]com, tds-telecom[.]com, teistra[.]ne, 1111systems-okta[.]com, t-mobile-okta[.]us, vzw-sso[.]com	Provedores de serviços de internet e nuvem
sso-authentication[.]de, sso-securelogin[.]com, service-sys-2fa[.]com	Autenticação multifatorial e domínios de logon único

COMO OS LOOKALIKES SÃO UTILIZADOS?

Agora que já falamos sobre o que são os lookalikes e alguns exemplos de quem são os alvos, vamos falar sobre como são usados.

Por “como”, queremos dizer quais são os métodos de implantação. A Infoblox viu lookalikes serem implantados de várias maneiras diferentes, como:

- **Mensagens SMS**
- **Chamadas telefônicas**
- **Mensagens diretas em redes sociais**
- **E-mails**
- **Incorporados em QR codes**
- **Domínios na World Wide Web**

ELES ENVIAM MENSAGENS DE TEXTO

Apesar dos aprimoramentos nos filtros de spam para mensagens de texto (SMS) de telefones celulares, o uso de SMS para enviar mensagens de phishing, geralmente chamado de smishing, continua aumentando.

Os agentes mal-intencionados são capazes de distribuir rapidamente um grande número de mensagens e evitar alguns dos mecanismos de segurança implementados para proteção contra ataques de phishing por e-mail. O SMS é usado tanto em ataques amplos a consumidores, quanto em ataques restritos de spearphishing a funcionários de organizações. Nesta seção, descreveremos dois agentes de ameaças que usaram SMS e domínios lookalike para atacar consumidores e funcionários do governo.

Por quase um ano, a Infoblox tem rastreado um agente mal-intencionado de smishing, que chamamos de OpenTangle. Até onde sabemos, esse agente não foi relatado em nenhum outro lugar. Inicialmente, o OpenTangle visava os consumidores ocidentais usando lookalikes de instituições financeiras, provedores de internet e varejistas on-line. Recentemente, ele começou a visar funcionários e prestadores de serviços do governo. Temos conhecimento de mais de 1.500 domínios lookalike controlados pelo OpenTangle desde que ele começou a operar, há cerca de dois anos. Alguns dos domínios do OpenTangle incluem mtbsuportz0610[.]com, americafirst0nline[.]com, and mygov03-ato[.]com.

Observe o uso de diferentes técnicas de lookalike.

Um dos autores deste artigo recebeu vários textos do OpenTangle, incluindo lookalikes do M&T Bank, com o qual o autor não tem nenhuma relação. No início de suas campanhas, o OpenTangle incluiu links de URL encurtados em seus textos de smishing, talvez esperando que o disfarce fosse bem-sucedido. No entanto, em maio de 2022, ele mudou para domínios lookalike. *Figura 13* mostra um exemplo de uma de suas campanhas bancárias em que as credenciais do usuário são solicitadas.

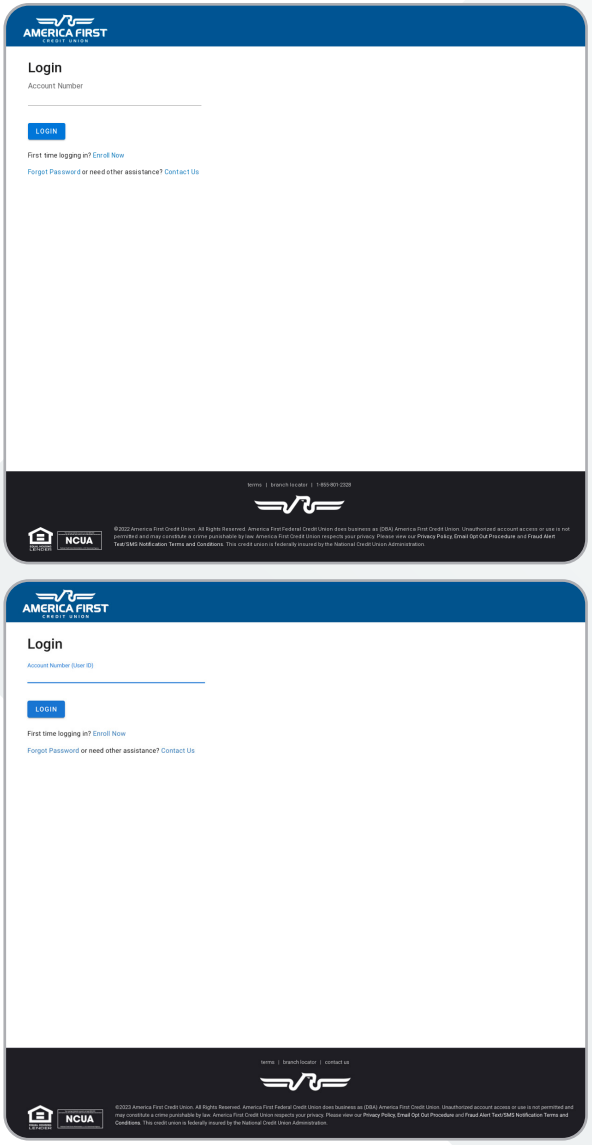


Figura 13. Uma página de phishing no domínio americafirst0nline[.]com direcionada aos correntistas do America First Credit Union. A imagem de phishing está na parte superior e a legítima está na parte inferior. Crédito da imagem: URLScan.[33]

OpenTangle começou a explorar o MFA usando kits de phishing AitM no ano passado. Enquanto suas campanhas anteriores usavam páginas de login de phishing padrão e geralmente tinham como alvo os consumidores, a *Figura 14* mostra um exemplo de como houve avanço em suas campanhas. Nesse caso, os alvos são os titulares das contas myGov, do governo australiano, e solicitam um código MFA, em vez de um simples login. Também foi incluído um link para ligar para o helpdesk, outra técnica que surgiu em 2022 como um meio de convencer os usuários a visitar sites maliciosos.

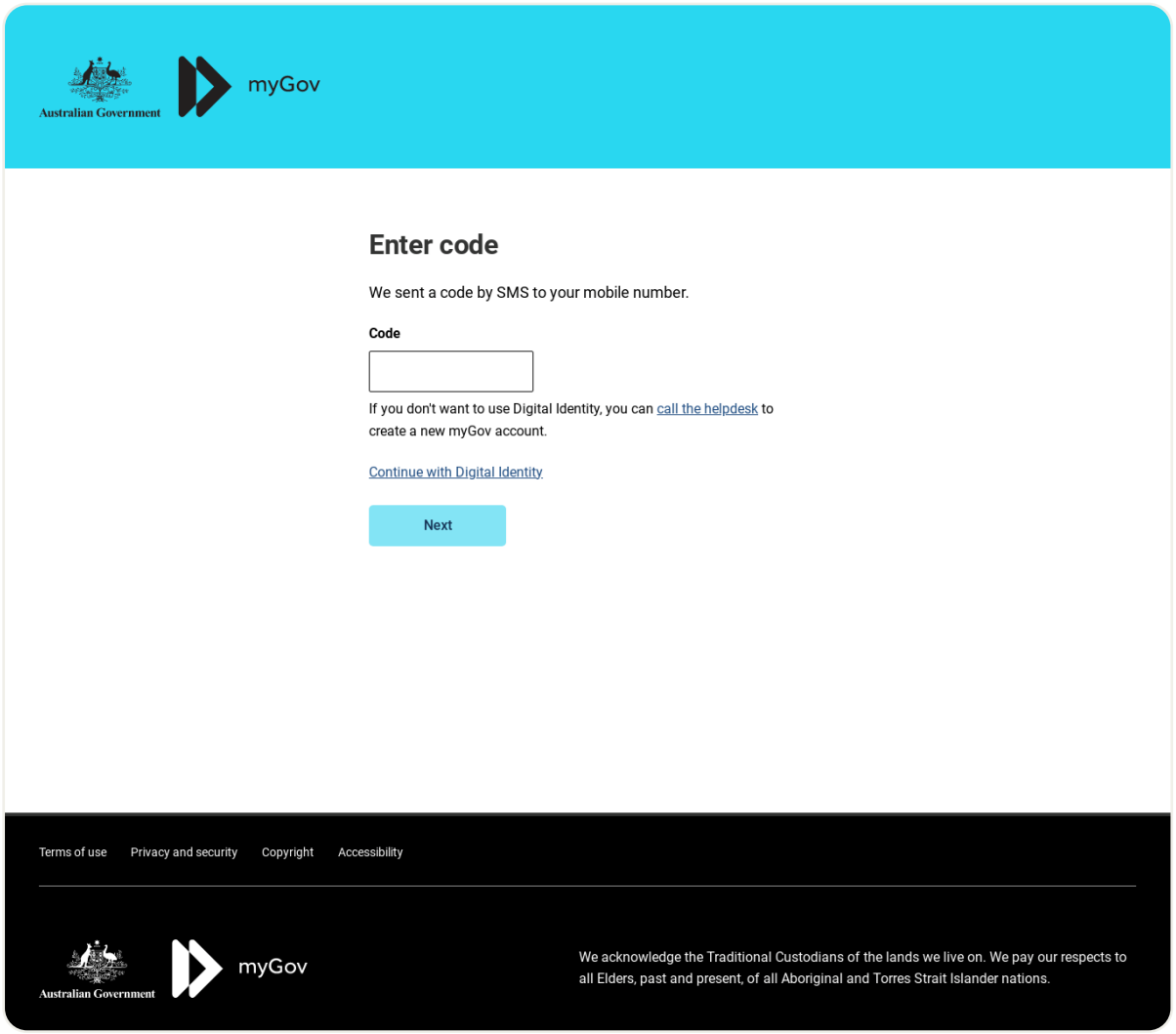


Figura 14. Domínio lookalike OpenTangle, www.mygovsupport-ato[.]com, imitando o myGov, o portal on-line do governo australiano. Crédito da imagem: URLScan.[34]

O Scamélie é outro exemplo de um agente que usa mensagens de smishing para espalhar lookalikes.

O agente mal-intencionado que chamamos de Scamélie, é uma coleção de grupos e indivíduos afiliados envolvidos em uma longa lista de golpes originados, e principalmente direcionados, a países de língua francesa. Também o vimos envolvido em uma segmentação mais geral na Europa e nos Emirados Árabes Unidos. Os domínios lookalike do Scamélie se fazem passar principalmente por ISPs, bancos, serviços governamentais e empresas de entrega. Devido à afiliação solta do grupo, também vimos golpes envolvendo empresas menos esperadas, como empresas de viagens, fabricantes de artigos esportivos e supermercados.

Os domínios lookalÏke do Scamélie geralmente são hospedados em grandes provedores de nuvem ou empresas de hospedagem "à prova de balas". Em alguns casos, os golpistas criaram seus próprios ou usam provedores de hospedagem configurados por outros golpistas não afiliados. Vimos tanto domínios direcionados, quanto domínios de uso geral (minha conta, resolver um problema etc.) registrados por meio de identidades roubadas e pagos com cartões de crédito virtuais ou criptomoedas.

Depois que os golpistas coletam as informações do cartão de crédito, eles ligam para a vítima, fazendo-se passar por um funcionário do banco ou do emissor do cartão de crédito.
Eles explicam que as informações do cartão de crédito foram roubadas, mas que eles ajudarão a solucionar o problema. Em seguida, o autor da chamada diz que a vítima receberá dois códigos MFA que deverão ser informados ao autor da chamada para garantir a segurança da conta. Na realidade, o invasor precisa dos códigos MFA para roubar o dinheiro em tempo real. O primeiro código MFA aumenta o limite da transferência eletrônica, e o segundo permite que a transação seja concluída. Para aumentar a eficácia das suas chamadas, o golpista contrata pessoas que são, idealmente, mulheres jovens e/ou pessoas que falam francês de uma maneira que não levante suspeitas de um falante nativo.

Como se trata de um grupo não organizado, é difícil de rastrear e analisar o Scamélie. Eles costumam aplicar os golpes durante a noite e retiram os domínios do ar depois de apenas algumas horas ou dias. Eles usam scripts anti-bot e anti-scraping para dificultar ainda mais a análise por parte dos pesquisadores de segurança.

SCAMÉLIE EXEMPLOS LOOKALIKE

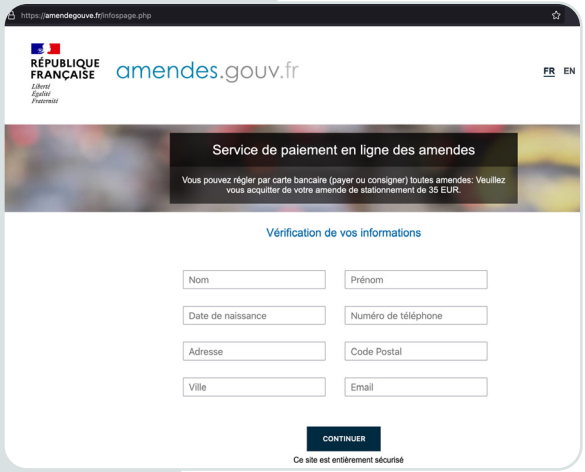


Figura 15. Um lookalike Scamélie, amendegouve[.]fr, imitando um portal de serviços do governo francês. Crédito da imagem: Infoblox.

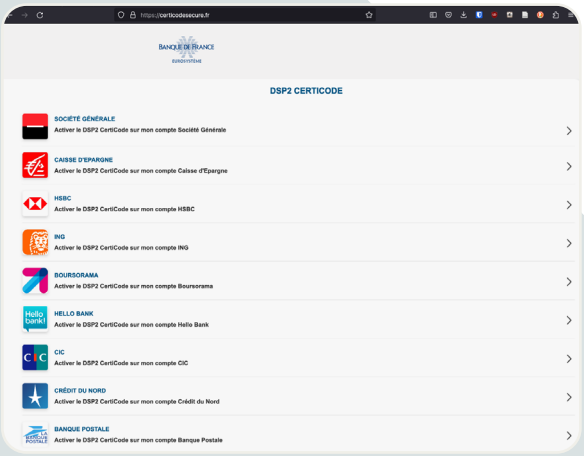


Figura 16. Um lookalike do Scamélie, certicodesecure[.]fr, falsificando um serviço bancário francês e induzindo as vítimas a vincular informações bancárias. Crédito da imagem: Infoblox.

ELES FAZEM CHAMADAS TELEFÔNICAS À MODA ANTIGA

A Cybersecurity and Infrastructure Security Agency (CISA) divulgou um aviso de segurança cibernética (CSA) no dia 26 de janeiro de 2023 sobre o uso malicioso de software de monitoramento e gerenciamento remoto (RMM).[35]

A CISA identificou uma campanha em outubro de 2022, na qual agentes mal-intencionados enviavam e-mails de phishing contendo um número de telefone e solicitavam que os usuários ligassem para esses números. O e-mail foi criado para se passar por uma mensagem de suporte ao cliente e, quando os usuários ligavam para o número de telefone, os golpistas os guiavam até um domínio malicioso. Quando o usuário fazia isso, um arquivo executável era baixado e, em seguida, entrava em contato com um segundo domínio malicioso, do qual era baixado um software RMM adicional. Esses softwares - AnyDesk e ScreenConnect - eram legítimos, porém pré-configurados para se conectar ao servidor RMM do agente.

Os domínios usados são lookalikes de serviços conhecidos, a probabilidade de a vítima aceitar o domínio é ainda maior quando elas os recebem por telefone, por causa da engenharia social adicional utilizada para criar os scripts e as personas de quem faz a chamada. Realizamos uma análise retroativa dos nossos dados e encontramos evidências de que o agente mal-intencionado está ativo há mais tempo do que o indicado no CSA.[36] Essas campanhas estavam ativas desde meados de 2021 pelo menos, mais de um ano antes dos incidentes que a CISA ea Silent Push descreveram, em artigos separados. Também vimos a reutilização de alguns domínios. Por exemplo, o domínio amzsupport[.]live, um lookalike da Amazon, fez parte de uma campanha ativa em abril de 2020, e depois voltou a ser usado em outubro de 2021.

À medida que os ataques contra a MFA dos sistemas internos corporativos vieram à tona no início de 2023, foi descoberto que, em alguns casos, os agentes mal-intencionados telefonavam para a vítima, fingindo ser do departamento de TI. Essa abordagem foi feita depois que a vítima não respondeu à solicitação inicial, dando mais legitimidade para convencer o usuário a visitar o domínio lookalike. Com essa ação, os usuários acabaram permitindo que o golpista roubasse suas credenciais corporativas.

ELES ENVIAM SPAM

Embora já tenhamos visto golpistas habilidosos usando smishing e ligações telefônicas para espalhar lookalikes e enganar as vítimas, o e-mail de phishing nunca saiu de moda.

A Infoblox analisa dezenas de milhares de e-mails de malspam todos os dias, revelando um fluxo aparentemente interminável de campanhas que distribuem domínios lookalike. Destacaremos algumas dessas campanhas e enfatizaremos a importância de as organizações manterem um monitoramento rigoroso dos e-mails de phishing.

Uma dessas campanhas tem como alvo a Xfinity, uma grande empresa americana de telecomunicações. Esses domínios lookalike possuem características de DGA e têm o formato "xfnity" <palavra encurtada ou parcial>. com. Observe que "Xfinity" está escrito incorretamente porque está faltando o primeiro "i". O agente mal-intencionado também garantiu que o nome do remetente parecesse legítimo, "Xfinity Mobile", que usa uma letra maiúscula cirílica "X". Os e-mails dos remetentes usavam seus próprios domínios e pareciam ter características semelhantes às de DGA também no nome de usuário, com o formato noreply-<palavra-chave>, como em: noreply-corporate@xfnitycard[.]com. Eles não usaram domínios exclusivos para cada e-mail. Em alguns casos, os domínios foram repetidos, mas a palavra-chave foi alterada, como em: noreply-corporate@xfnitycard[.]com e noreply-active@xfnitycard[.]com.

Tabela 7. Domínios lookalike Xfinity.

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

Os domínios identificados na campanha utilizam uma técnica que chamamos de "decoy parking": quando um domínio é visitado diretamente e parece estar estacionado, mas, na realidade, o servidor de e-mail do domínio está ativo e enviando e-mails maliciosos. Descobrimos que o decoy parking é bastante comum e não é relatado por outros fornecedores. *Veja na Figura 17 um exemplo de uma página de decoy parking.*

LOOKALIKE XFINITY

Figura 17. Página decoy parking exibida pelo lookalike do Xfinity, xfnityrayton[.]com.
Crédito da imagem: URLScan.[37]

LOOKALIKE WEDO MACHINERY

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.

Figura 18. Corpo da campanha de malspam usando a Wedo Machinery como isca e o domínio lookalike, acrobat-adobe[.]com, como um malware C2. Crédito da imagem: Infoblox

Nossa análise encontrou esses lookalikes do Xfinity em documentos do Word maliciosos.

Os assuntos das campanhas serviram como incentivo para ação e giraram em torno de pagamentos recusados ou ameaças de encerramento de serviço, como "[Aviso] Seu serviço corre o risco de ser encerrado" ou "[Ação necessária] Não conseguimos efetuar a cobrança em seu cartão, corrija seus dados". O corpo desses e-mails foi estruturado como se fosse do suporte ao cliente, pedindo aos destinatários que "abrissem o anexo para obter mais detalhes".

Outra campanha identificada pela Infoblox utilizava uma empresa de reciclagem chinesa, a Wedo Machinery, para lançar um carregador de ransomware. Identificamos 176 e-mails dentro dessa campanha, cada um com um arquivo .zip contendo um único arquivo executável identificado como Zmutzy. *Veja na Figura 18 um exemplo de e-mail.* Vimos dois nomes de arquivos nessa campanha: PO-0097(1).zip e PO-29862K.zip. O carregador do Zmutzy usa um domínio lookalike acrobat-adobe[.]com para baixar cargas úteis adicionais.

ELES USAM QR CODES

Além dos lookalikes diretos de criptomoedas, observamos o uso de phishing QR, em que um QR code é usado para ofuscar um destino de URL e fornecer conteúdo malicioso, em conjunto com domínios lookalikes criados para incentivar os usuários a reivindicar prêmios e fornecer informações sobre sua conta de criptomoedas.

Em um exemplo, o QR code redirecionou a vítima para um link bridge[.]walletconnect[.]com, um mecanismo usado para roubar fundos. Nesse golpe, os agentes mal-intencionados criaram uma conta no Twitter, @adidas_weare, para ter credibilidade e compartilhar seus domínios lookalikes. *Veja a Figura 19.* A conta conseguiu 16.000 seguidores em 21 de fevereiro de 2023, felizmente, ela já foi excluída ou retirada do ar.

Os agentes mal-intencionados anunciavam prêmios falsos, incluindo carros Porsche e roupas ou sapatos Adidas. Os domínios eram predominantemente combosquats e continham as palavras-chave “Adidas” ou “Porsche”. Ao visitar os domínios lookalike, conforme mostrado abaixo na Figura 20, era solicitado que os usuários digitalizassem um QR code com o qual eles conseguiriam reivindicar o prêmio, redirecionando-os para a aplicação descentralizada, WalletConnect, que fornecia ao golpista acesso aos recursos do usuário.[38]

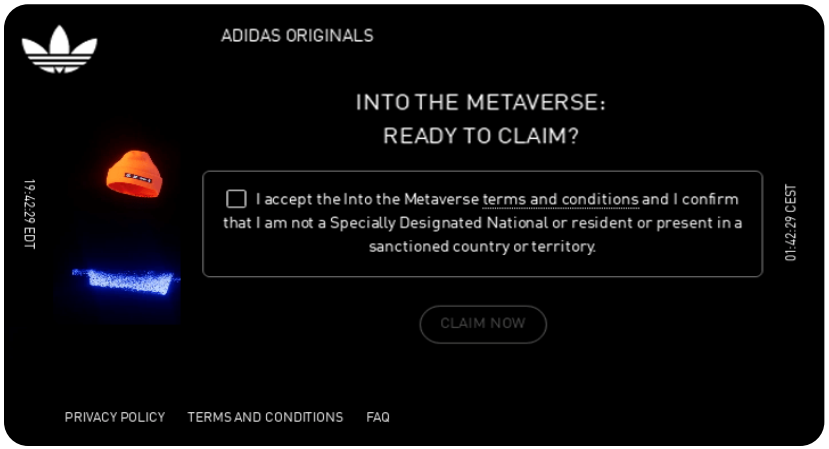


Figura 20. Domínio lookalike Adidas, adidas-go[.]com, atraindo usuários a clicar e reivindicar um prêmio.
Crédito da imagem: URLScan.[39]

Se os usuários escanearem o QR code e vincularem suas carteiras de criptomoedas ao sistema descentralizado, os agentes mal-intencionados conseguem extorquir criptomoedas do usuário. Esses domínios usam servidores de nomes compartilhados e estão hospedados em um endereço IP com resolução russa, 185[.]149[.]120[.]83, que é totalmente controlado por agentes mal-intencionados e contém outros lookalikes do Blur, bem como do Arbitum, uma solução para melhorar a velocidade e a escalabilidade dos contratos inteligentes da Ethereum.

LOOKALIKE ADIDAS

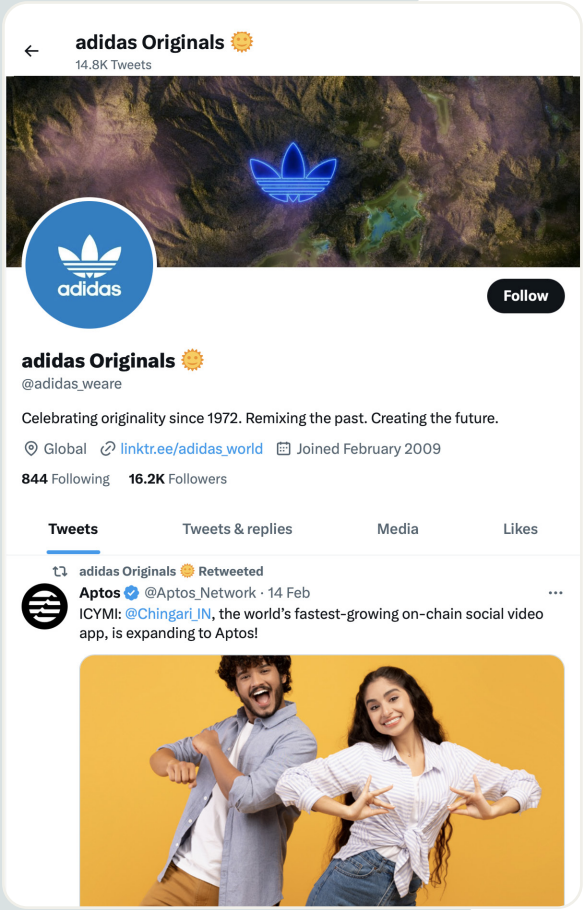


Figura 19. Conta lookalike do Twitter, @adidas_weare da Adidas Originals @adidasoriginals.
Crédito da imagem: Infoblox.

ELES USAM DNS

Lookalikes não ocorrem apenas como domínios de sites.

Descobrimos que eles estão sendo usados em várias capacidades de DNS, incluindo:

- **Servidor de nome**
- **Servidor de e-mail**
- **Registros CNAME**
- **Registros PTR**

Na maioria dos casos, esses domínios não terão um registro A típico ou presença em um site e, geralmente, podem parecer estacionados, uma implementação de decoy parking que descrevemos em uma seção anterior. Os invasores também usam domínios lookalike para redirecionamento e comunicação C2 no DNS.

SERVIDOR DE NOMES

Como um exemplo de servidores de nomes lookalike, os domínios bitkeep[.]dev e flutter[.]direct foram registrados em novembro de 2022. Ambos são lookalikes de domínios diferentes, mas compartilham uma infraestrutura. A BitKeep é uma carteira de criptomoedas descentralizada e multi-cadeia que tem como objetivo ser um único hub para todas as transações de criptomoedas. O domínio oficial da BitKeep é bitkeep[.]com, a empresa está em operação há cinco anos e tem mais de 8 milhões de usuários.[40] A Flutter é a ferramenta de interface de usuário (UI) portátil da Google para criar aplicativos compilados nativamente para dispositivos móveis, web e desktop a partir de um único código-fonte. O domínio oficial da Flutter é flutter[.]dev.[41]

Ambos os domínios legítimos hospedam conteúdo da web no domínio principal, mas nenhum dos domínios lookalike faz o mesmo. Quando registrados inicialmente, ambos os domínios estavam atuando como servidores de nomes para outro domínio, get-flutter[.]com, que é outro lookalike da Flutter. Naquela época, os domínios estavam hospedados no provedor de hospedagem offshore suíço Private Layer. Essa rede também hospedou o flutter[.]vision. Embora não possamos atribuir definitivamente esses domínios a atividades mal-intencionadas, eles demonstram um padrão de utilização de domínios lookalike para fins não tradicionais. Eles se mostram bastante desafiadores de analisar, mesmo para pesquisadores experientes, e é improvável que acionem muitos algoritmos de inteligência contra ameaças.

SERVIDORES DE E-MAIL

Além dos servidores de nomes, vimos lookalikes sendo usados como servidores de e-mail. Os domínios whirlpoolmxonline[.]com e whirlpoolservicesmx[.]com têm como alvo a grande marca de eletrodomésticos Whirlpool e compartilham uma infraestrutura comum. Eles estão hospedados no mesmo endereço IP, de propriedade da Lyra Hosting, um provedor de hospedagem e VPS de baixa qualidade localizado em Seychelles, e compartilham servidores de nomes comuns.

Embora eles visem diretamente a Whirlpool com o nome de domínio de segundo nível (SLD), também identificamos características em cada domínio que mostram que outras grandes marcas de eletrodomésticos também são visadas. O SLD whirlpoolmxonline[.]com tem três subdomínios: mabe-onlinemx[.]whirlpoolmxonline[.]com, samsung-onlinemx[.]whirlpoolmxonline[.]com e lg-onlinemx[.]whirlpoolmxonline[.]com. A Mabe é uma empresa mexicana de eletrodomésticos. O SLD whirlpoolservicesmx[.]com não tem subdomínios, mas a cadeia histórica de certificados SSL associados ao domínio aponta para o direcionamento de marcas de eletrodomésticos semelhantes como whirlpoolmxonline[.]com: www[.]lgservicesmx[.]mabeservice[.]com e *.lgservicesmx[.]com.

Usar lookalikes como servidores de e-mail oferece um desafio adicional para detectar e-mails de phishing em um endpoint devido à aparência de legitimidade dos cabeçalhos de e-mail à primeira vista.

C2s de MALWARE

Na seção anterior sobre implantação de e-mail, mencionamos como uma campanha de malspam, que estava distribuindo o carregador de ransomware Zmutzy, usou o domínio lookalike acrobat-adobe[.]com, como um servidor C2 de malware. Os lookalikes são perfeitos para C2s de malware porque podem se misturar facilmente ao tráfego de rede ao lado de domínios legítimos. Pesquisadores da ESET, uma empresa eslovaca de software de segurança, identificaram C2s de malware para o FatalRAT (trojan de acesso remoto) se passando pelo Telegram, o aplicativo de mensagens, em fevereiro de 2023.[42]

Tabela 8. Lookalikes do Telegram funcionando como C2s de malware.

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

Os domínios que hospedavam os arquivos .exe maliciosos também eram lookalikes do Telegram, WhatsApp, Skype, Google Chrome e Firefox.

REDIRECIONAMENTOS

Os lookalikes também podem ser usados como redirecionamentos. Identificamos uma grande rede de domínios typosquat que redirecionam os visitantes para o choto[.]xyz, um domínio C2 que redireciona condicionalmente as vítimas para o domínio de destino lotto60[.]com. O agente mal-intencionado usa serviços de proxy reverso e proteção de bots Cloudflare no choto[.]xyz, presumivelmente para evitar a detecção e a exploração por pesquisadores de segurança. O domínio de destino parece estar executando um programa fraudulento de marketing de afiliados. Ao analisar o modelo de objeto do documento (DOM), podemos ver que o HTML contém uma função gtag() incorporada que envia dados do visitante para o Google Analytics com o ID de análise G-DT4YWT5VP8. Além de aumentar os números de marketing de afiliados do agente mal-intencionado, vimos o lotto60[.]com sendo solicitado por HTTP por arquivos potencialmente maliciosos, que correspondem às assinaturas de arquivo confirmadas como sendo o trojan de acesso remoto Nighthawk.[43]

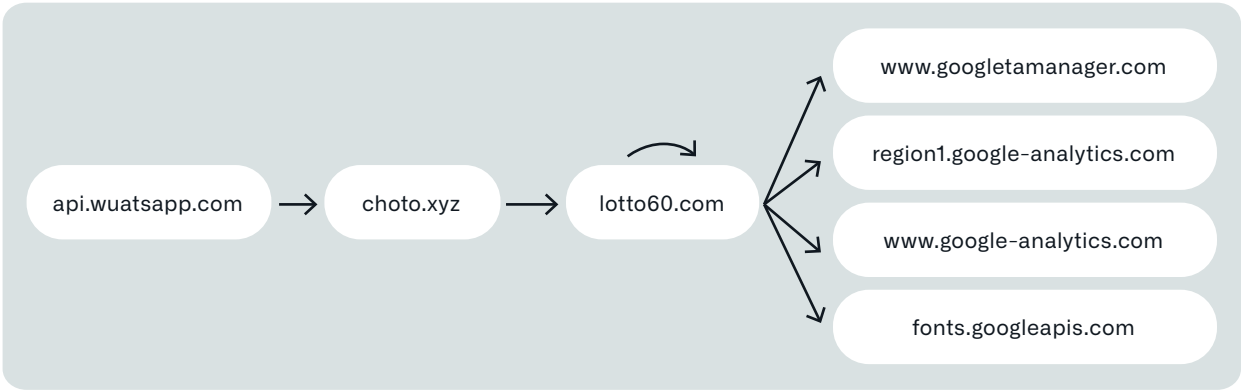


Figura 21. Exemplo de cadeia de redirecionamento de um domínio typosquat para o Google Analytics. Crédito da imagem: URLQuery.[44]

Os domínios typosquat de primeiro estágio imitam uma variedade de empresas. Alguns exemplos incluem →

Tabela 9. Lookalikes funcionando como redirecionamentos em uma campanha fraudulenta de marketing de afiliados.

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

Esses typosquats normalmente ficam estacionados por um a três meses antes de serem usados como redirecionamentos. O agente mal-intencionado demonstrou muito cuidado na criação desses domínios typosquat. Cada caractere incorreto está diretamente próximo ao caractere correto em um teclado QWERTY em inglês dos EUA. Esses são erros que qualquer digitador comum poderia cometer várias vezes em um único dia, exceto aqueles que ainda digitam “caçando as letras”.

POR QUE ELES SÃO EFICIENTES?

Caro leitor, você notou as 19 palavras lookalikes que espalhamos neste artigo até agora? Algumas são muito difíceis de ver!

Dica: Existem mais 6. Veja se você consegue encontrá-los.

Até agora, falamos sobre alguns alvos específicos, bem como a infraestrutura dos métodos de implantação de domínios lookalike. Mas por que eles são tão eficazes? O que os torna uma ameaça tão persistente?

A resposta é complicada e envolve aspectos de psicologia, implementações técnicas e erros humanos simples - **afinal de contas, é isso que nos torna humanos!**

PSICOLINGUÍSTICA

Psicologicamente, o cérebro humano entra em curto-circuito (nesse caso, estamos nos referindo à definição literal de uma corrente que segue um caminho não intencional de menor resistência) durante a leitura. Você provavelmente já viu um meme que dizia algo como:

> ***De aorcdco com uma peqisusa da Unviresiade de Cmabrigde, não ipmtroa em qaul odrem as ltetras em uma plavra etãso, a úncia ciosa ioptrmante é que a piremria e a útlima lttera etsejam no lgaur crrtoeo. O resto pode ser uma bagunça total e você ainda consegue ler sem problemas. Isso ocorre porque a mente humana não lê cada letra isoladamente, mas a palavra como um todo.***

Embora a alegação seja infundada no sentido de que nenhuma pesquisa desse tipo em Cambridge foi publicada, o conceito fundamental parece ter mérito. Por exemplo, uma pesquisa recente sugere que "ver uma palavra embaralhada, ativa uma representação visual que é comparada a palavras conhecidas".[45] Embora provar ou refutar questões fundamentais da psicolinguística esteja fora do escopo deste artigo, queremos mostrar como a psicolinguística desempenha um papel importante na eficácia dos lookɑlikes.

Especificamente, esse curto-circuito do cérebro humano desempenha um papel importante quando se trata de ʜomógrafos e typosquats. Quando você vê um domínio como lnfoblox[.]com, o seu cérebro não analisa necessariamente cada letra individual desse nome de domínio e, portanto, talvez nunca perceba que o primeiro caractere é, na verdade, um "L" minúsculo e não um "i" maiúsculo.

Por motivos semelhantes, quando você vê o domínio goooogle[.]com, o seu cérebro pode não parar para reconhecer que há três letras "o" em vez das duas corretas... pelo menos, não até que seja tarde demais e você já tenha clicado nela.

SUPORTE PUNYCODE: SUCESSOS E FALHAS

Os navegadores da web têm maneiras de defender os usuários contra ataques de hom0grafos de nomes de domínio internacionalizados (IDN). A primeira e mais proeminente linha de defesa é "traduzir" o domínio unicode para punycode, que pode ser reconhecido pelo "xn--" inicial e parece ser sem sentido para o olho humano não treinado. Isso ocorre porque o punycode mapeia os caracteres unicode para um subconjunto muito mais limitado de caracteres da American Standard Code for Information Interchange (ASCII), que contém apenas letras, dígitos e hifens. Todos os principais navegadores têm suporte para domínios punycode. O Google fornece uma descrição detalhada da heurística envolvida no algoritmo que determina se deve ser exibida a versão internacionalizada, ou a versão punycode de um domínio no Chromium.[46] A Mozilla fornece uma descrição semelhante.[47]

A Mozilla também oferece esse texto inspirador na descrição de seu algoritmo de exibição de IDN:

> ***Nossa resposta a essa questão é que, no final das contas, cabe aos registros garantir que seus clientes não possam enganar uns aos outros. Os navegadores podem impor algumas restrições técnicas, mas não estão em posição de fazer esse trabalho por eles, mantendo ao mesmo tempo um ambiente equitativo para scripts não latinos na web. Os registros são os únicos em posição de implementar a verificação adequada. Da nossa parte, queremos garantir que não tratamos scripts não latinos como cidadãos de segunda classe.***

Em 2017, o pesquisador de segurança Xudong Zheng registrou um domínio em Punycode, xn--80ak6aa92e[.]com, que se traduz para "apple[.]com", contendo caracteres cirílicos que imitam a aparência dos caracteres latinos em "apple".[48] Na época, os navegadores Internet Explorer, Microsoft Edge, Safari, Brave e Vivaldi não estavam vulneráveis, mas Chrome, Firefox e Opera estavam. Atualmente, apenas o Firefox continua traduzindo o punycode, deixando os usuários vulneráveis ao ataque (não testamos recentemente o domínio no Internet Explorer ou no Microsoft Edge).

O QUE É PUNYCODE?

Punycode é uma codificação especial usada para converter caracteres unicode em ASCII, que é um conjunto de caracteres menor e mais restrito. O Punycode é usado para codificar nomes de domínios internacionalizados (IDNs).

SMISHING IMESSAGE USANDO HOMÓGRAFOS DE IDN

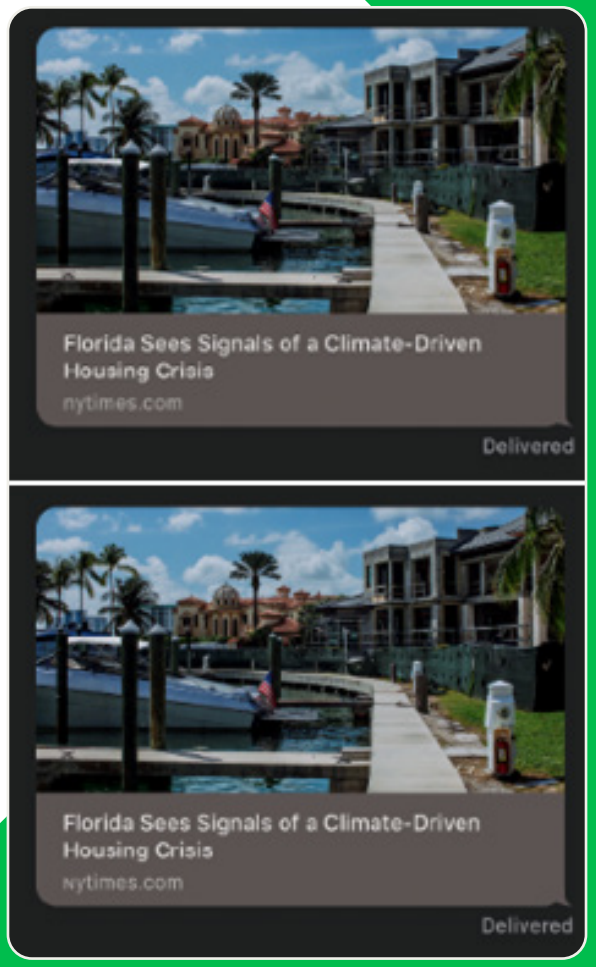


Figura 22. Imagem superior cedida por Tyler Butler mostrando um artigo real do New York Times enviado via iMessage. Imagem inferior cedida por Tyler Butler mostrando um artigo falsificado do NYT em um domínio homógrafo de IDN.
Crédito da imagem: Tyler Butler.

Hu e outros autores realizaram uma análise longitudinal e quantitativa sobre a eficácia das defesas baseadas em navegador contra ataques homógrafos de IDN.[49]

Eles se propuseram a responder a três perguntas:

1. Quais são as políticas implementadas pelos principais navegadores e como elas são aplicadas?
2. Existem maneiras de contornar sistematicamente as políticas existentes?
3. Até que ponto os internautas conseguem reconhecer homógrafos de IDN, e esses homógrafos que conseguem contornar as políticas do navegador, são mais ou menos enganosos?

Para responder às perguntas, os autores analisaram cinco navegadores principais (Chrome, Firefox, Safari, Microsoft Edge e Internet Explorer) ao longo de cinco anos (de janeiro de 2015 a abril de 2020). Eles geraram 9.000 casos de teste para responder às duas primeiras perguntas e realizaram um estudo de usuário para responder à terceira. O Chrome e o Edge foram mais bem-sucedidos na exibição de punycode em vez de seus homógrafos IDN correspondentes, ambos tiveram uma taxa de falha geral (mostraram a versão IDN em vez do punycode) de 20,62%. O Safari e o Firefox foram muito piores, com um taxa de falha geral de 42,91% e 44,46%, respectivamente. Cada navegador apresentou taxas de falha diferentes, dependendo da categoria do IDN. Além disso, os autores descobriram que os internautas têm dificuldade para identificar IDNs homógrafos, e os IDNs bloqueados pelos navegadores foram os mais problemáticos para determinar a autenticidade: 48,8% dos usuários acharam que eram homógrafos, 48,5% dos usuários acharam que não eram e 2,7% não souberam dizer.

Até agora, nos concentramos apenas em navegadores de desktop. Mas, como vimos nos ataques lookalikes de smishing descritos anteriormente neste artigo, os domínios homógrafos de IDN também estão bem à vontade em dispositivos móveis. Na verdade, podem ser mais prejudicais. Tamanhos de tela menores, barras de endereços menores e uma impossibilidade de visualização de links podem levar a ataques lookalikes mais eficazes. Mesmo quando é possível visualizar links, os homógrafos de IDN ainda podem ser eficazes em dispositivos móveis. Em 2021, o pesquisador de segurança Tyler Butler publicou sobre a plausibilidade do smishing usando homógrafos de IDN no iMessage.50 O iMessage oferece visualizações ricas de links, mas um invasor experiente pode contornar isso facilmente com um domínio lookalike bom o suficiente e um pouco de estilização para a própria página da web. Como Butler observa, essa forma de ataque pode ser usada para espalhar desinformação, roubar credenciais ou espalhar malwares e spywares direcionados.

Butler descreve que a Apple alegou que não abordará a vulnerabilidade devido ao fato de que os homógrafos são "visualmente distinguíveis". *Considerando a Figura 22, o que você acha? Você consegue identificar a diferença?*

ERRAR É HUMANO, PERDOAR É DIVINO... MAS AUTOMATIZAR É SENSATO

Na World Wide Web, alguns seres humanos não são tão tolerantes com os erros dos outros. AComo já mencionamos, os agentes mal-intencionados usam domínios typosquat para se aproveitar dos erros ortográficos naturais das pessoas. Tudo o que um invasor precisa fazer para que um typosquat seja eficaz é registrar um domínio plausível e esperar. É isso. Mais cedo ou mais tarde, algum humano cometerá esse erro de ortografia e chegará a um domínio que nunca pretendeu visitar. É claro que os golpistas não apenas esperam, eles atraem proativamente as pessoas para que elas cliquem. E nesse mundo em constante movimento, muitas vezes nem percebemos que cometemos um erro inicialmente.

No final das contas, os lookalikes são chamados assim por um motivo: eles são semelhantes a domínios conhecidos com a intenção de enganar seres humanos. Como vimos, alguns lookalikes são mais eficazes do que outros, mas a escolha do nome de domínio é apenas uma parte da eficácia. A maneira como um domínio lookalike é implantado também pode ter um impacto significativo no sucesso geral da campanha. Veja, por exemplo, um lookalike ou MFA do Okta como okta[.]lnfoblox[.]com ou okta-lnfoblox[.]com. Uma pessoa perspicaz que verifica três vezes cada nome de domínio antes de visitá-lo (boa sorte para encontrar uma dessas pessoas) pode perceber que o "i" no domínio de segundo nível (SLD) é, na verdade, um "L" minúsculo. Mas essa semelhança, combinada com uma mensagem SMS bem elaborada para o número de telefone que consta no perfil on-line, por exemplo, pode fazer a diferença. Acrescente à equação uma ligação telefônica com uma chamada urgente para ação e o jogo estará encerrado. É claro que esse é um exemplo fictício (com todos os componentes sendo usados) de spearphishing, e não uma campanha geral que utiliza lookalikes, mas a questão permanece: as técnicas de lookalike podem ser aplicadas com eficácia a domínios de várias maneiras, e a várias partes da infraestrutura de DNS.

Tudo isso para dizer que o provérbio frequentemente citado "Errar uma vez é humano, errar duas vezes é burrice" não se aplica aos lookalikes. Até mesmo as pessoas mais perspicazes e preocupadas com a segurança podem ser vítimas de um lookalike, e fazer isso de novo e de novo. Os atores mal-intencionados estão em vantagem nessa guerra, mas ela ainda não está perdida. A Infoblox tem soluções no nível de DNS para garantir que as organizações consigam revidar e se defender de forma eficaz.

IOCs ***A lista completa deste artigo pode ser encontrada no GitHub em: https://github.com/infobloxopen/threat-intelligence***

SOLUÇÕES INFOBLOX

Domínios lookalike continuam populares entre os golpistas devido à sua eficácia e à dificuldade de detecção em grande escala. O desafio é agravado pela dificuldade de identificar automaticamente um domínio suspeito que tem a intenção de imitar um alvo legítimo. Isso fez com que as empresas e os órgãos governamentais se preocupassem cada vez mais com domínios lookalike que se fazem passar por domínios corporativos ou pela cadeia de suprimentos.

O BloxOne Threat Defense (B1TD) Advanced da Infoblox oferece uma solução única, ampla e abrangente contra ameaças lookalike. Aproveitando o DNS em grande escala, a Infoblox pode aplicar uma série de análises a centenas de milhares de novos SLDs todos os dias. Isso inclui várias análises para detecções lookalike, como uma avaliação automática de semelhanças visuais em IDNs homógrafos.

Os clientes podem escolher entre domínios comumente visados ou criar uma lista personalizada para monitoramento e análises especializadas de lookalikes. Os resultados dessa análise aprofundada podem ser acessados por meio do lookalike Reporting UI, que também sinaliza instâncias em que o lookalike detectado está associado a atividades suspeitas ou de phishing. No geral, as políticas podem ser personalizadas para atender às necessidades do ambiente específico de um cliente e ao nível de tolerância ao risco. E os dados de domínios detalhados incluem anotações valiosas que estão acessíveis por meio das interfaces do usuário B1TD Advanced e APIs, fornecendo aos clientes um contexto que pode acelerar as investigações de ameaças e tornar as respostas a incidentes mais eficazes.

Esses recursos de detecção de ameaças lookalike são apenas um dos muitos serviços oferecidos pelo BloxOne Threat Defense que permitem ver ameaças que outras soluções não veem e interromper os ataques ainda no início do seu ciclo de vida. Por meio da automação abrangente e da integração do ecossistema, é possível gerar maior eficiência em SecOps, aumentar a eficácia da stack de segurança existente, proteger os esforços digitais e de trabalho em qualquer lugar, além de reduzir o custo total de cibersegurança.

PARA MAIS INFORMAÇÕES

Visite infoblox.com

Siga-nos no LinkedIn

Siga-nos no Twitter

REFERÊNCIAS

[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.

O Infoblox une rede e segurança para oferecer desempenho e proteção incomparáveis. Reconhecida por empresas presentes na lista Fortune 100 e por inovadores emergentes, fornecemos visibilidade e controle em tempo real sobre quem e o que se conecta à sua rede, para que sua organização opere com maior velocidade e detecte ameaças mais cedo.

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

+1.408.986.4000
www.infoblox.com