infoblox®

UNO SGUARDO APPROFOND1TO AGLI ATTACCHI LOOKAL1KE

UN NUOVO STUDIO RIVELA I PIÙ RECENTI VETTORI DI MINACCIA

April 2023

I DOMINI LOOKALIKE PRENDONO DI MIRA TUTTI

INDICE DEI CONTENUTI

EXECUTIVE SUMMARY

Sin dall'avvento di Internet i threat actors hanno utilizzato domini visivamente simili per ingannare gli utenti e indurli a visitare siti web dannosi. Questi domini, chiamati domini lookalike, ormai sono sinonimo di attacchi di phishing, tanto che i corsi di sensibilizzazione alla sicurezza includono indicazioni su come ispezionare i link per individuarli.

Tuttavia, nonostante le campagne di sensibilizzazione e i progressi della tecnologia, i domini lookalike rappresentano una minaccia persistente per i consumatori e le organizzazioni, questi vengono costantemente aggiornati dai threat actors. Tutti sono un bersaglio: dai consumatori ai governi, dai grandi marchi di vendita al dettaglio ai piccoli ristoranti, dalle aziende tecnologiche di fama mondiale a quelle meno conosciute come la nostra. In questo documento, vedrai che "tutti sono un bersaglio" con esempi di domini e campagne reali. Essendo un'azienda di dimensioni modeste in un settore abbastanza di nicchia, anche noi siamo presi di mira.

Questo report descrive l'attuale panorama delle minacce, mostrando esempi reali nei vari settori e gruppi di utenti. Infoblox rileva da anni i domini lookalike e analizza ogni giorno oltre 70 miliardi di eventi DNS (Domain Name System) per trovare minacce nuove e potenziali. Per questo documento, ci siamo concentrati sui rilevamenti da gennaio 2022 a marzo 2023. Da oltre 300.000 domini looKaliKe, abbiamo curato un set che evidenzia le sfide e i rischi associati a questi attacchi.

I domini lookälike sono spesso associati ad attacchi ampi e non mirati contro i consumatori tramite e-mail di spam, pubblicità, social media e messaggi SMS. Ogni giorno ci sono migliaiadi nuovi domini registrati che imitano software popolari, istituzioni finanziarie e servizi di consegna postali. Gli attacchi di phishing che mirano a rubare le credenziali degli utenti o a infettare le macchine con malware sono così diffusi, e spesso così poco sofisticati, che sono diventati una fonte di numerosi meme, tra cui "non puoi cadere nelle truffe di hishing, se non controlli la tua e-mail". Sebbene sia spesso descritto come comico, il phishing è un settore serio. L'Anti-Phishing Working Group (APWG) riferisce che il phishing ha raggiunto un livello record nel terzo trimestre del 2022.[1]

[ ] ***Tutti gli indicatori in questo documento sono stati neutralizzati, indipendentemente dal fatto che siano dannosi o legittimi. Abbiamo modificato gli indicatori inserendo delle parentesi sui punti [.] e impedendo così che diventassero link cliccabili.***

70+ MILIARDI

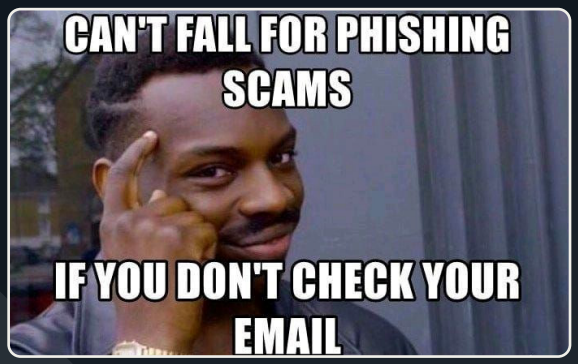
Infoblox analizza quotidianamente oltre 70 miliardi di eventi DNS per identificare nuove minacce.

300.0

I domini lookalike sono stati presi in esame per questo report per evidenziare la sfida e il rischio di questi attacchi.

UN ESEMPIO DI MEME SUL PHISHING.

Un esempio è questo tweet del 2019.[2]



Credito immagine: l'origine di questo meme è sconosciuta.

Ma i domini lookalike non sono solo una minaccia per i consumatori: vengono utilizzati per accedere alle reti aziendali.

Recenti rivelazioni hanno rivelato attacchi mirati in cui attori malintenzionati hanno ingannato i dipendenti inducendoli a fornire le proprie credenziali di autenticazione a più fattori (MFA). Nella maggior parte dei casi, i domini lookalike non solo imitavano l'azienda, ma includevano anche parole chiave MFA, accrescendo ulteriormente l'illusione per i dipendenti che la connessione fosse sicura. Abbiamo scoperto che gli attori hanno preso di mira aziende grandi e piccole, in molti settori verticali, tra cui fornitori di servizi Internet, servizi bancari e criptovalute, software e servizi informatici e compagnie assicurative a livello globale. Questi attacchi sono iniziati all'inizio del 2022 e hanno guadagnato slancio nel tempo.

L'uso di domini l00kalike è redditizio perché si tratta di un attacco asimmetrico. Gli utenti devono essere sempre vigili per proteggere le loro finanze personali e le informazioni dei loro datori di lavoro. I prezzi economici di registrazione dei domini e la capacità di distribuire attacchi su larga scala danno agli attori il sopravvento. Gli aggressori hanno il vantaggio della scala e, mentre le tecniche per identificare le attività dannose sono migliorate nel corso degli anni, i difensori faticano a tenere il passo.

Non solo il phishing con lookalike è fiorente, ma l'uso dei lookalike è diventato più complesso in un modo che si rivela più chiaramente nei record DNS. La nostra ricerca mostra che i domini lookalike vengono sfruttati al di là dei tradizionali scopi di phishing e typosquatting. Vengono utilizzati anche in modi non osservati in precedenza: ad esempio, come nameserver e per la distribuzione di e-mail di spear phishing. Esistono grandi reti resilienti che servono solo domini lookalike e che si rivolgono sia ai consumatori che ai dipendenti pubblici.

Infoblox dispone di più algoritmi per identificare i domini lookalike. Utilizziamo una combinazione di metodi, tra cui: l'osservazione di varianti di bersagli comuni nei settori dello shopping, bancario, dei software e finanziario; osservando le varianti di domini specificati dai clienti e osservando le infrastrutture DNS di attori malevoli specializzati in domini lookalike. Questo approccio poliedrico ci offre un'ampia copertura del panorama delle minacce.

> ***NOTA IMPORTANTE: questo report contiene una serie di esempi che illustrano l'ampiezza e la profondità dei domini lookalike in circolazione; non hanno lo scopo di implicare attacchi riusciti o violazioni di qualsiasi entità.***

CONTESTO

Come tutti i buoni documenti di ricerca, inizieremo con alcune informazioni di base. Questo è per lo più vocabolario. Sappiamo che la maggior parte dei lettori salta la sezione sul contesto, quindi sarà breve.

I lookalike dannosi, ovvero domini registrati dagli aggressori che sembrano uguali o molto simili a un dominio noto, sono una minaccia ben nota e persistente nel panorama informatico. Generalmente parlando, i lookalike hanno applicazioni sia offensive che difensive. In senso offensivo, i lookalike sono usati per ingannare ovunque ci possano essere esseri umani. Gli attori utilizzano i lookalike per rubare denaro, ottenere credenziali o accessi, raccogliere informazioni di identificazione personale, distribuire malware o guadagnare entrate pubblicitarie. Sono utilizzati anche per scopi politici e per offuscare la reputazione del marchio. In breve, sono un mezzo per raggiungere un fine per i criminali informatici. In senso difensivo, molte organizzazioni registrano in modo proattivo domini simili ai propri, per evitare che gli aggressori li rivendichino e li utilizzino.

I lookalike assumono forme diverse. Nello spazio DNS, i domini possono essere:

- **Omografi**
- **Typosquat**
- **Combosquat**
- **Soundsquat**

Possono essere quasi indistinguibili dal dominio di destinazione originale o oggettivamente ben distinti. Gran parte del successo dei domini lookalike come vettore di attacco è dovuto alla pressione esercitata sulle persone.

Come vedremo, i lookalike possono essere trovati in ogni elemento di un attacco, dagli indirizzi dei mittenti delle e-mail, agli URL di phishing e al comand and control (C2) del malware. Sebbene di solito siano associati ai record di indirizzi (A/AAAA), abbiamo anche trovato lookalike utilizzati per i record del nameserver (NS), del pointer (PTR) e del canonical name (CNAME). Possono essere distribuiti tramite e-mail, SMS o messaggi di testo, siti web compromessi, reti di malvertising e telefonate. Nella sezione seguente, descriviamo brevemente le diverse forme di lookalike e forniamo esempi di ciascuna.

LA COLPA È DELLA MACCHINA DA SCRIVERE

In effetti, questo problema moderno può essere fatto risalire agli albori delle macchine da scrivere. Su molte vecchie macchine da scrivere, non c'erano i tasti 0 o 1, poiché ci si aspettava che i dattilografi usassero la lettera O maiuscola e la L minuscola per rappresentare queste cifre.[4]

OMOGRAFI (O MEGLIO OMOGLIFI)

Sebbene la parola omografo significhi "due parole che sono scritte allo stesso modo, ma non necessariamente pronunciate allo stesso modo e con significati diversi", il termine omografo è stato usato per molti anni nella letteratura di ricerca sulla sicurezza per indicare "due domini che appaiono visivamente uguali".[3] Un termine più accurato è omoglifi. Questi domini sembrano simili l'uno all'altro e in alcuni casi possono essere quasi indistinguibili. *Per coerenza con la letteratura di ricerca, in questo documento utilizzeremo il termine errato omografo.*

Questa forma di lookalike sfrutta il fatto che molti caratteri dello stesso set di caratteri, o alfabeto, si assomigliano tra loro. Ad esempio, 0 (la cifra zero) e O (lettera "o" maiuscola), oppure "l" (lettera "L" minuscola) e "I" (lettera "i" maiuscola). Alcuni caratteri accentuano ulteriormente questo problema. Esempi classici di ciò sono g0ogle.com e lnfoblox.com, in cui la "o" in Google è sostituita rispettivamente con uno zero (0) e la "i" in lnfoblox è sostituita con una "L" minuscola.

Con la maturazione di Internet e l'aumento di persone non anglofone che si collegano al World Wide Web, la necessità di nomi di dominio internazionalizzati (IDN) è cresciuta. Un IDN è un dominio che contiene almeno un carattere in caratteri non latini; l'introduzione di Unicode ha permesso l'ascesa di tali domini. Con gli IDN è arrivata una nuova forma di lookalike: l'omografo IDN. Si tratta sempre di un omografo, ma che utilizza caratteri di altri set di caratteri o alfabeti simili. Gabrilovich e Gontmakher hanno mostrato il potere degli oMografi IDN nel loro articolo del 2002 "The Homograph Attack". Gli autori hanno registrato un lookalike dell'autentico dominio Microsoft microsoft[.]com che conteneva le lettere cirilliche "c" e "o".[5] Il risultato finale è un dominio www.microsoft[.]com che è visivamente indistinguibile dal dominio Microsoft autentico.

Il Consorzio Unicode ha pubblicato uno strumento che mostra il vasto numero di caratteri confondibili disponibili per una determinata stringa.[6] La stringa "hi" (ciao) ha 684 varianti con caratteri Unicode; per una stringa come "infoblox" il numero arriva a oltre 2,2 trilioni di variazioni. Alcune variazioni sono meno efficaci per un lookalike rispetto ad altre. Ad esempio, il Consorzio Unicode elenca "৯" (cifra 5 indo-araba estesa) come potenziale carattere confondibile per "o" (lettera "O" latina minuscola).

Chiaramente, inf৯bl৯x[.]com non è un lookalike molto efficace; ma riesci a notare la differenza, se entrambi sono scritti utilizzando il carattere Arial di uso comune, tra il dominio corretto {infoblox[.]com} e {infoblox[.]com}(che contiene una "i" minuscola bielorussa o ucraina e la lettera minuscola armena "vo", scritta come una "n")? Nemmeno noi ci riusciamo.

TYPOSQUAT

I domini typosquat sfruttano i nomi di dominio popolari e gli errori di battitura che gli utenti commettono, o che sono causati dalla digitazione su tastiere non funzionanti. Questo termine è solitamente associato ai domini registrati, ma lasciati inutilizzati, allo scopo di attirare fondi pubblicitari. Ad esempio, uno degli autori stava recentemente cercando di pagare l'affitto tramite il portale online del proprio gruppo di gestione immobiliare, ospitato tramite appfolio[.]com (una nota società di software che offre soluzioni SaaS a gruppi di gestione immobiliare e proprietari). Invece, ha digitato male e ha quasi visitato appfollio[.]com, che è stato registrato nel 2013 ma è attualmente parcheggiato.

È interessante notare che un altro dominio apparentemente typosquat per Appfolio, apfolio[.]com, sembra essere di proprietà di Appfolio. Reindirizza al dominio corretto e ha lo stesso registrante, organizzazione registrante e registrar ed è stato registrato solo un mese dopo il dominio legittimo appfolio[.]com. Questo è un esempio dell'uso difensivo dei lookalike. Sfortunatamente, i malintenzionati hanno il sopravvento perché ci sono semplicemente troppe possibilità per permettere alle organizzazioni di registrare tutte le varianti di lookalike.

I typosquat sono percepiti principalmente come un metodo di monetizzazione, ma possono avere uno scopo nefasto. Sebbene vengano utilizzati per vendere pubblicità di terze parti o per essere rivenduti al legittimo proprietario del dominio, possono anche essere utilizzati per programmi di marketing di affiliazione "blackhat" e come domini C2 del malware, come mostreremo più avanti. I marchi e le aziende hanno una protezione civile contro il typosquatting ai sensi dell'Anticybersquatting Consumer Protection Act. A causa di questa minaccia di azione legale, il typosquatting è visto come una forma "blackhat" di monetizzazione nella comunità del flipping/parking di domini, e i flipper di domini seri come iGoldrush raccomandano di non usare il typosquatting a scopo di lucro.[7]

ESEMPI DI TYPOSQUAT

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

dei domini combosquat abusivi sono attivi per più di 1.000 giorni

dei domini combosquat abusivi appaiono in almeno una blocklist pubblica 100 giorni dopo le risoluzioni iniziali

COMBOSQUATTING

Il combosquatting è una forma di lookalike che combina nomi di marchi o società popolari con altre parole chiave. Termini come "support" (supporto), "help" (aiuto), "security" (sicurezza) e "mail" (posta) sono comuni. Considera, ad esempio, wordpresssupport[.]ru, wordpresssupport[.]store e wordpress-security[.]cloud. Questi domini sono tutti ospitati sullo stesso indirizzo IP con sede in Russia e assomigliano a WordPress, il popolare software per i contenuti web. L'inclusione di "support" e "security" nel nome di dominio indica che questi sono destinati agli utenti di WordPress. Potrebbero essere usati per raccogliere credenziali per dirottare siti WordPress o raccogliere dati di pagamento e informazioni di identificazione personale (PII, Personally Identifiable Information).

Oltre a generare domini combosquat, gli attori hanno anche la possibilità di utilizzare algoritmi di generazione di domini da dizionario (DDGA, Dictionary Domain Generation Algorithm) per creare lookalike. In pochi secondi, è possibile generare migliaia di domini candidati per una moltitudine di marchi o aziende. Per pura fortuna, l'algoritmo può creare domini candidati con le parole chiave giuste affinché il dominio sia efficace. La comunità di utenti di Steam, una delle principali piattaforme di gioco, è un obiettivo comune per gli attori che utilizzano DDGA per combosquat. Alcuni esempi di domini all'interno di un set osservato di recente sono: steamcommiunity[.]com[.]ru, steamcommucnity[.]com[.]ru, steamcommunityjp[.]top e steamcommunityiq[.]top. Notare la sovrapposizione tra typosquatting e combosquatting in questo set di domini.

Kitsin et al. hanno condotto uno studio longitudinale sul combosquatting nel 2017, analizzando circa 468 miliardi di record DNS (provenienti da set di dati attivi e passivi) e hanno trovato risultati inquietanti:

- **I domini combosquat sono 100 volte più diffusi dei domini typosquat**
- **Il 60% dei domini combosquat abusivi è attivo per più di 1.000 giorni**
- **Il 20% dei domini combosquat abusivi appare in almeno una blocklist pubblica 100 giorni dopo le risoluzioni iniziali**
- **La risoluzione dei domini combosquat è aumentata di anno in anno[8]**

Concordiamo con le conclusioni degli autori sulla prevalenza dei domini combosquat. Troviamo più domini combosquat che semplici typosquat o omoGrafi puri (IDN o altro) attraverso le nostre analisi.

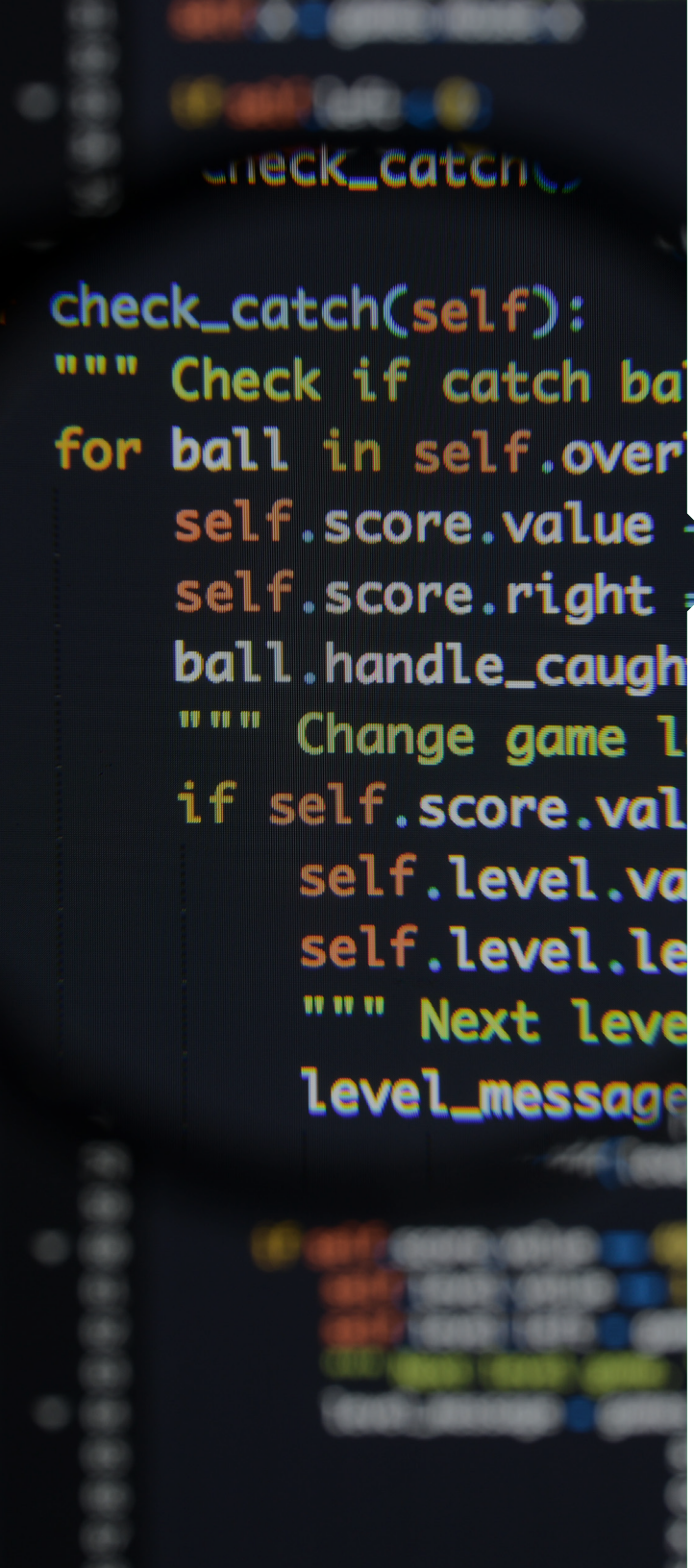
SOUNDSQUATTING

I domini soundsquat sfruttano l'uso di omofoni, parole che hanno lo stesso suono ma hanno un'ortografia diversa. Il soundsquatting è la forma di lookalike identificata più di recente, apparsa per la prima volta in letteratura nel 2014.[9] Il soundsquatting ha recentemente attirato maggiore attenzione da parte dei ricercatori a causa della proliferazione di servizi vocali intelligenti come Alexa, Siri e Google Voice.[10] I domini soundsquat si sovrappongono ad altri tipi di domini lookalike, in quanto potrebbero suonare e sembrare simili. Abbiamo riscontrato che i domini soundsquat puri, cioè quelli che non appaiono visivamente simili ma suonano allo stesso modo, sono rari; generalmente questi domini possono essere trovati anche con tecniche di somiglianza basate su testo.

È importante notare che i lookalike in circolazione spesso non rientrano in categorie ordinate come abbiamo descritto qui. Per massimizzare l'efficacia di un dominio lookalikę viene utilizzata una combinazione di forme. Molti dei domini combosquat che vediamo hanno elementi di typosquat e omografi (IDN o altro). I typosquat utilizzano elementi di omografi, i soundsquat utilizzano elementi di typosquat e così via. Il risultato finale è un panorama di minacce asimmetriche in cui gli aggressori possono lasciare i difensori con il fiato sospeso.

SUONA L'ATTACCO

La prevalenza del soundsquatting è decollata con l'avvento della tecnologia ad attivazione vocale come Alexa, Siri e Google Voice.



ALTRE FORME DI LOOKALIKE

Sebbene questo documento si concentri sui domini lookalike e sul loro ruolo nell'attuale panorama delle minacce, esistono altri tipi di lookalike che possono sfruttare gli utenti vulnerabili. Un esempio notevole di questi ultimi è stato recentemente trovato nei pacchetti Python PyPi.

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

I gestori di pacchetti per i linguaggi di programmazione più diffusi, come Python, sono soggetti alle stesse debolezze dei domini. Chiunque può caricare un pacchetto con qualsiasi nome (purché non sia già stato preso) contenente codice che può o meno essere privo di rischi per la sicurezza. Nel 2016, il ricercatore di sicurezza Nikolai Tschacher ha utilizzato il typosquatting in questo modo per costringere più di 17.000 host distinti ad eseguire codice arbitrario.[11] Poi, nel 2021, il ricercatore di sicurezza Alex Birsan ha ripreso l'idea di Tschacher e l'ha ampliata, coniando il termine "dependency confusion".[12]

Birsan ha trovato i nomi dei pacchetti privati e interni delle principali aziende attraverso varie fonti open sources. Ciò includeva l'esplorazione del codice sorgente sui siti web, la ricerca di pacchetti su GitHub o persino la ricerca dei nomi dei pacchetti nei forum pubblici. Poi, ha caricato pacchetti con lo stesso nome di pacchetti privati e interni sui gestori di pacchetti pubblici. Infine, Birsan ha utilizzato pipeline CI/CD automatizzate, "confondendo" i pacchetti pubblici con i pacchetti private interni. Invece di importare e installare i pacchetti privati, le pipeline automatizzate hanno trovato e importato i pacchetti pubblici di Birsan. Birsan ha poi utilizzato l'esfiltrazione DNS per notificargli che il suo codice arbitrario, e non il pacchetto privato previsto, era stato eseguito. La tecnica di lookalike di Birsan gli ha permesso di violare 35 organizzazioni, a volte entro poche ore dal caricamento dei suoi pacchetti.

Indipendentemente dal tipo di lookalike o dal settore di competenza in cui viene utilizzato un lookalike, essi sono una minaccia persistente. Parte della sfida di studiare i lookalike è che sono indefiniti: ci sono più possibilità di quante se ne possano calcolare e tutto è un bersaglio. Nelle sezioni seguenti, mostriamo esempi specifici di queste varie forme di lookalike in circolazione, compresi i target, i metodi di distribuzione, l'infrastruttura, il motivo della loro efficacia, le sfide e le soluzioni di Infoblox al problema.

TUTTI SONO UN BERSAGLIO

Pensiamo che troverai almeno un bersaglio sorprendente nei nostri esempi.

Uno dei risultati più importanti della nostra analisi dei domini lookalike nel DNS è che tutti sono un bersaglio: abbiamo trovato lookalike per tutti i bersagli previsti, ma anche per le aziende e i servizi più piccoli. Questi domini sono utilizzati da attori malintenzionati per depredare le persone al lavoro e a casa.

Come ha notato di recente Akamai, la maggior parte delle campagne lookalike ricevono pubblicità solo quando viene colpito un grande bersaglio.[13]
Il nostro obiettivo è quello di fare luce sulle campagne sottostimate e trascurate, oltre ai bersagli "tipici". In questo documento vengono mostrati alcuni esempi selezionati per dimostrare questo punto, ma evidenzieremo anche l'impatto su diversi settori industriali e l'uso di varie metodologie in modo più dettagliato in seguito.

PRENDONO DI MIRA NOI!

Infoblox è un'azienda di dimensioni modeste con meno di 2000 dipendenti in tutto il mondo.

Sebbene deteniamo un'ampia quota del mercato DNS, DHCP (Dynamic Host Configuration Protocol) e IPAM (IP Address Management), noti collettivamente come DDI, questo settore è piuttosto specifico e Infoblox non è certo un nome familiare. Si potrebbe essere sorpresi dal fatto che i malintenzionati siano a conoscenza di noi, tanto meno che ci prendano di mira attivamente con domini lookalike. Tuttavia, abbiamo trovato molti domini progettati per ingannare sia i nostri dipendenti che i nostri clienti. Lookalike di servizi interni, incluso il nostro portale dei benefit, così come dei nomi dei nostri prodotti sono stati registrati nell'ultimo anno.

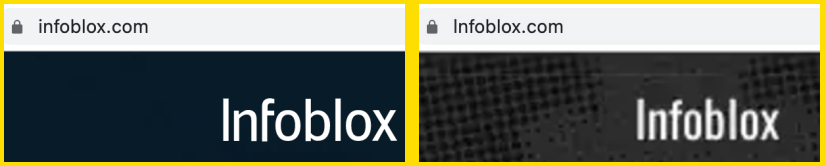


Figura 2. Un confronto dei loghi tra il sito ufficiale infoblox[.]com (sinistra) e il lookalike Infoblox[.]com (destra)

Alcuni domini registrati che non sono di proprietà di Infoblox includono:

Omografo **Infoblox[.]com**	L'utilizzo di una "L" minuscola per impersonare una "i" maiuscola è stato registrato nel luglio 2022 e, sebbene sia offerto in vendita, il sito mostra nell'angolo in alto a sinistra un rendering quasi indistinguibile da quello del nostro sito web aziendale. *Vedere il confronto nella Figura 2.*
Typosquat **infobloxbenifits[.]com**	Questo dominio è stato registrato in Cina nell'aprile 2022 ed è un leggero refuso del nostro portale di vantaggi per i dipendenti. Questo dominio è attualmente parcheggiato presso Bodis.
TLD Squat **infoblox[.]info**	Un diverso dominio di primo livello, o TLD (Top-Level Domain), è stato registrato nell'agosto 2022 tramite il registrar altamente abusato Sav[.]com. È parcheggiato su dan[.]com, che consente agli utenti di vendere domini.
Combosquat **infobloxgrid[.]com**	Un lookalike combosquat basato sul nostro prodotto on-premise di punta utilizzato da migliaia di clienti in tutto il mondo. La nostra tecnologia Grid brevettata consente agli amministratori di rete di combinare diverse applicazioni di rete in un unico sistema. Questo dominio è disponibile anche all'indirizzo dan[.]com ed è stato registrato nell'aprile 2022.
Combosquat **infoblox-updater[.]com**	Un esempio della tecnica di utilizzo di parole comuni del linguaggio tecnico all'interno del dominio, come "update" (aggiornamento) o "support" (supporto). In questo caso, un cliente potrebbe essere indotto a connettersi con un sistema falso, pensando che sia legato agli aggiornamenti del sistema Infoblox. I nomi o i prodotti delle aziende tecnologiche sono spesso sfruttati per questo tipo di dominio combosquat, che potrebbe essere utilizzato come dominio di phishing o come C2 del malware. Altri esempi sono dev[.]gitlabs[.]me e jira[.]atlas-sian[.]net, entrambi utilizzati dall' APT, (Advanced Persistent Threat) Iron Tiger nel suo malware SysUpdate.[14]

Oltre a prendere di mira piccole aziende tecnologiche come la nostra, abbiamo visto una vasta gamma di lookalike che sono varianti ingannevoli di ristoranti, studi legali e altre piccole imprese.

Inoltre, un singolo attore può utilizzare sia marchi noti che piccole imprese come esche. Un attore che Infoblox segue da tempo ha creato domini lookalike per il ristorante Cotenna di New York City e ha copiato il loro sito web, presumibilmente per indurre i visitatori a effettuare prenotazioni online con le loro carte di credito.[15] Il sito cotenna[.]nyc è stato registrato nell'aprile 2022 ed è un lookalike del sito web del ristorante cotenna[.]com. Questo stesso attore ha domini lookalike rivolti a grandi aziende di social media come Twitter.

Nelle sezioni che seguono, approfondiremo i settori che sono più presi di mira oggi, nonché alcuni dei molti modi in cui i domini possono essere utilizzati per un attacco di successo. Poiché tutti sono un bersaglio, evidenzieremo le aree in cui abbiamo riscontrato il maggior numero di attività dannose, sulla base di un'analisi di 300.000 domini lookalike.

I DOMINI LOOKALIKE PRENDONO DI MIRA TUTTI

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

10.000+ ORGANIZZAZIONI

Nel luglio 2022 Microsoft ha avvertito che oltre 10.000 organizzazioni erano state bersaglio di attacchi AitM progettati per rubare le credenziali MFA dagli utenti in tempo reale.

1.600+

La nostra ricerca ha rilevato che oltre 1.600 domini contenevano una combinazione di funzionalità lookalike aziendali e MFA.

PRENDONO DI MIRA I DIPENDENTI

Fino a poco tempo fa, molte aziende ritenevano che l'uso dell'autenticazione a più fattori (MFA) aveva protetto le loro reti interne dagli attacchi di phishing.

Ma all'inizio del 2023, Coinbase ha rivelato che i suoi dipendenti erano stati presi di mira da attacchi di spear phishing che utilizzavano domini lookaliKe per l'accesso MFA interno dell'azienda. Questa rivelazione è stata rapidamente seguita da rapporti di conferma da parte di altre aziende che erano state prese di mira da attacchi simili. Sulla base delle segnalazioni delle vittime, sappiamo che i malintenzionati hanno inviato ai dipendenti messaggi SMS ed e-mail, esortandoli ad accedere ai sistemi interni. In alcuni casi sono state coinvolte anche telefonate durante le quali l'aggressore ha fornito un nome di dominio che il dipendente poteva visitare nel proprio browser web. Gli aggressori hanno usato tecniche adversary-in-the-middle (AitM) per rassicurare i dipendenti sul fatto che stavano interagendo con la rete reale dell'azienda. Ai dipendenti è stato richiesto un codice MFA, che è stato poi acquisito dall'aggressore e utilizzato per accedere ai sistemi interni.

Microsoft aveva avvertito nel luglio 2022 che oltre 10.000 organizzazioni erano state bersaglio di attacchi AitM progettati per rubare le credenziali MFA dagli utenti in tempo reale.[16] Questi attacchi erano specifici per l'uso dell'autenticazione di Outlook 365, ma Microsoft ha inoltre riferito nel febbraio 2023 che un kit di phishing che abilitava gli attacchi MFA era disponibile in vendita nel luglio 2022 ed era ampiamente utilizzato.[17] Altre società, tra cui Twilio, avevano rivelato attacchi simili nell'estate del 2022, ma l'entità degli attacchi non è stata ben pubblicizzata fino alle rivelazioni di Coinbase.[18]

Per indagare su questo incidente, abbiamo eseguito un'analisi retrospettiva dei domini lookalike che imitavano l'MFA utilizzando parole chiave come "mfa", "okta" e "2fa". La nostra ricerca ha rilevato un'ampia gamma di bersagli e una netta impennata dell'attività a partire dal luglio 2022, anche se all'inizio dell'anno è stato utilizzato un numero significativo di domini lookalike per questi attacchi. Oltre 1.600 domini contenevano una combinazione di funzionalità lookalike aziendali e MFA. I bersagli andavano dalle grandi aziende segnalate come Coinbase, Reddit e Twilio, alle principali banche, aziende di software, fornitori di servizi Internet, enti governativi e piattaforme di gioco in tutto il mondo. Sono state prese di mira, ma sottostimate, anche le aziende tecnologiche più piccole, i negozi di alimentari e i rivenditori.

Come esempio di bersagli meno noti, più domini lookalike per l'MFA hanno imitato il Western Electricity Coordinating Council (WECC).
Il WECC promuove l'affidabilità del sistema elettrico interconnesso per gran parte degli Stati Uniti occidentali. I lookalike includevano wecc-okta[.]org, wecc-oktc[.]org e wecc-okta[.]com. Tutti sono stati registrati nel febbraio 2023 e condividono un indirizzo IP.

Un altro esempio sorprendente è Feldman Auto Group, che comprende diversi concessionari di automobili negli Stati Uniti.
Sebbene l'azienda abbia un rapporto di branding con l'attore americano Mark Wahlberg, per il resto è un'azienda di dimensioni moderate con 18 sedi nel Midwest.[19] Un lookalike MFA di questo dominio, feldmanauto-okta[.]com, è stato registrato a fine gennaio 2023.

Alcuni dei bersagli aziendali dei lookalike MFA sono più incerti.
Il dominio frb-okta[.]com mostra un prompt di accesso con un logo FRBOkta indistinto, che potrebbe essere la Federal Reserve Bank, la First Reserve Bank, o un lookalike di un sito come quello dell'azienda di abbigliamento polacca, Farbokta.[20] In molti casi, non possiamo essere certi di quale fosse il bersaglio, e il kit di phishing potrebbe essere stato attivo solo per un breve periodo. *Abbiamo incluso uno screenshot dell'accesso nella Figura 3 per rendere l'idea.*

Questi attacchi AitM sono stati utilizzati anche contro i consumatori nel 2022, in particolare quelli della comunità dei videogiochi che utilizzano l'MFA per proteggere gli acquisti dei giochi.
In un caso noto agli autori, la vittima è stata indotta a visitare un sito da un livestream di Twitch di un popolare gioco online. Dopo aver inserito le credenziali MFA, ha subito un breve attacco DoS (Denial of Service) contro la propria rete domestica, che ha creato un'interruzione di Internet per diversi minuti. Quando è riuscito a tornare al proprio account di gioco, tutti i suoi acquisti erano stati rubati. *Potremmo pensare ai giocatori come a degli adolescenti che vivono in casa con i genitori, ma la quantità di denaro speso in acquisti in-app rende i videogiochi e i loro giocatori, da Roblox a Counter-Strike, un bersaglio redditizio.*

LOOKALIKE MFA FRBOKTA.COM

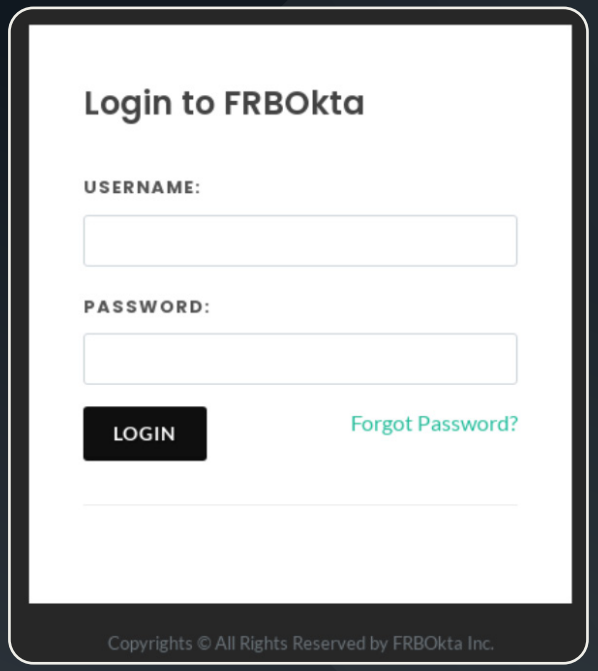


Figura 3. Il sito web frb-okta[.]com mostra una pagina di accesso indistinta con un riferimento a FRBOkta. Credito immagine: URLScan.[21]

PAGINA LOOKALIKE DEL MINISTERO TURCO

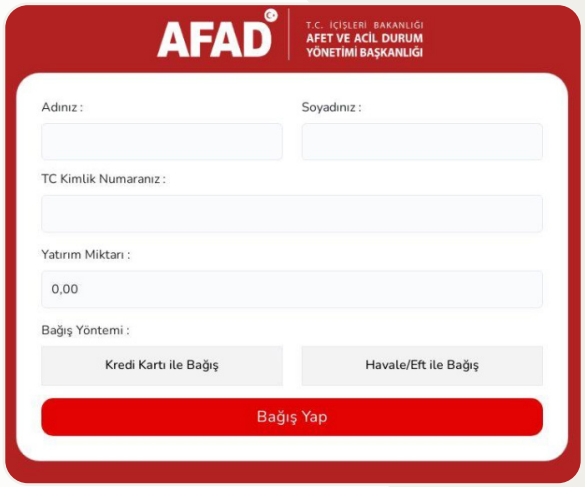


Figura 4. Lookalike dell'AFAD afadestek[.]net
Credito immagine: DomainTools.

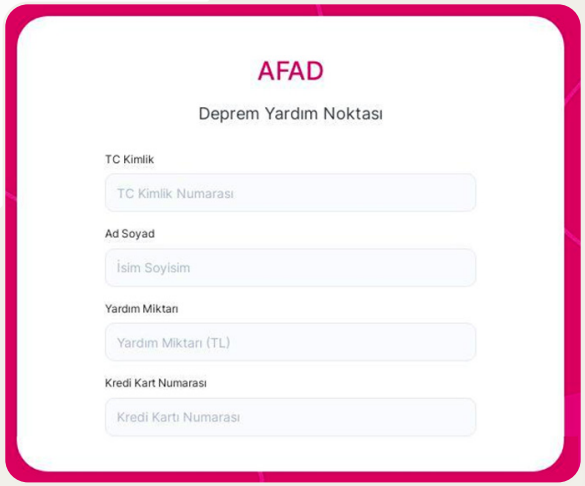


Figura 5. Dominio lookalike dell'AFAD afadbagislari[.]net
Credito immagine: DomainTools.

PRENDONO DI MIRA I BENEFATTORI

I truffatori che cercano di rubare denaro sono spesso il "primo soccorso" quando si tratta di utilizzare gli eventi e i disastri mondiali per guadagni illeciti.

Infoblox ha riscontrato che i truffatori sono pronti ad approfittare di qualsiasi evento di cronaca, come le crisi sanitarie come il COVID-19 o l'invasione russa dell'Ucraina. Purtroppo, il 2023 ha portato una crisi umanitaria con il terremoto turco-siriano all'inizio di febbraio.[22] Dopo il terremoto iniziale del 6 febbraio, diversi domini fraudolenti hanno cercato di imitare i siti web dell'Autorità per la gestione dei disastri e delle emergenze (AFAD) del Ministero dell'Interno turco. Questi domini hanno sfruttato il termine "AFAD" nel nome di dominio completo, cercando di assomigliare al dominio legittimo afad[.]gov[.]tr. Gli esempi seguenti sono domini che sono stati registrati di recente e, sebbene abbiano un nome di dominio completo (FQDN, Fully Qualified Domain Name) lungo, iniziano tutti con "AFAD".'

L'uso di FQDN più lunghi offre ai truffatori più permutazioni del dominio legittimo da utilizzare in più campagne a tema AFAD:

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

Oltre al combosquatting, alcuni di questi siti utilizzano il logo legittimo dell'AFAD per indurre i visitatori a fare donazioni. Ad esempio, il sito fraudolento afadestek[.]net è stato registrato il 7 febbraio e mostrava un web design simile a quello del legittimo sito turco dell'AFAD, come mostrato nella *Figura 4*. Secondo la traduzione automatica, sembra raccogliere donazioni tramite carta di credito o vaglia postale tramite trasferimento elettronico di fondi, oltre a raccogliere informazioni personali come nome e cognome e dati di identità.

Altri domini fraudolenti non si sono preoccupati di utilizzare il logo ufficiale dell'AFAD e sono stati rapidamente resi operativi per massimizzare la quantità di denaro che potevano estrarre dai donatori. Due esempi sono afadbagislari[.]net e afadyardimyap[.]net, entrambi ospitati dallo stesso indirizzo IP. L'infrastruttura dedicata per i lookalike è comune e sarà discussa in dettaglio in seguito. Entrambi i siti presentano lo stesso layout e lo stesso contenuto, come mostrato nella *Figura 5*, chiedendo donazioni per gli aiuti per i terremotati tramite pagamenti con carta di credito.

PRENDONO DI MIRA LE CRIPTOVALUTE

A parte i truffatori che cercano di guadagnare velocemente, i lookalike sono molto usati per rubare credenziali.

Un dominio lookalike è probabilmente ciò che la maggior parte delle persone comuni ha in mente quando pensa a un generico sito web di "phishing" che tenta di ottenere le credenziali dagli utenti. Con l'aumento della popolarità delle criptovalute, gli aggressori prendono di mira questi servizi finanziari, compresi i marketplace, i portafogli e gli exchange. Abbiamo trovato una serie di lookalike molto convincenti del popolare exchange Coinbase, con sede negli Stati Uniti. Uno di questi siti è mostrato nella *Figura 6*.[23]

I domini nella tabella seguente, ad esempio, sono stati registrati nel gennaio 2023:

Tabella 1. Esempi di domini lookalike dell'exchange di criptovalute 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

Con la crescita degli NFT (Non-Fungible Token), i cui scambi hanno raggiunto oltre 2 miliardi di dollari nel febbraio 2023, gli attori si sono rapidamente espansi oltre le criptovalute tradizionali nei loro sforzi per rubare denaro agli investitori.[24]
A titolo di esempio, il marketplace Blur è stato aperto nell'ottobre 2022 e il token Blur è stato lanciato qualche mese più tardi, determinando un investimento record in NFT dal maggio 2022.[25] Abbiamo iniziato a vedere i lookalike di Blur subito dopo il lancio del prodotto e poi abbiamo assistito a un drammatico aumento dei lookalike man mano che la piattaforma aumentava di popolarità.

LOOKALIKE DI COINBASE

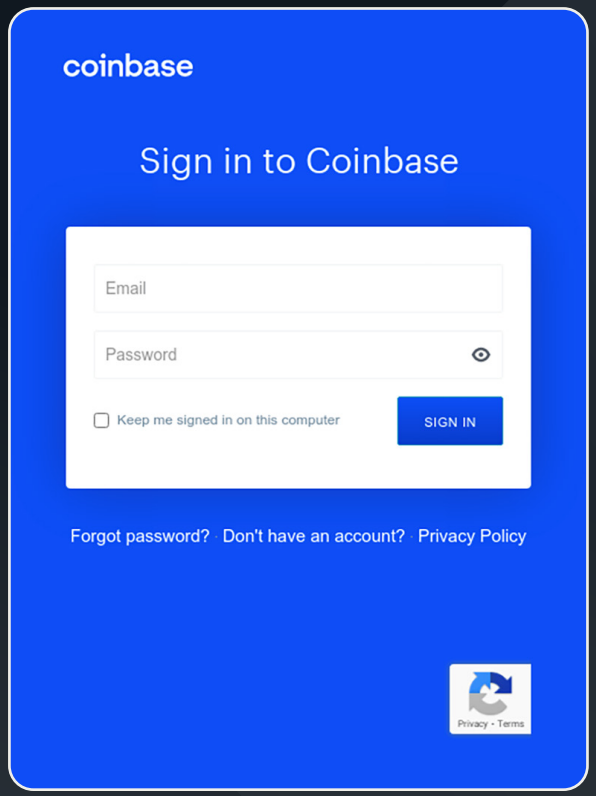


Figura 6. Lookalike di Coinbase click-coinbase[.]com
Credito immagine: DomainTools.

LOOKALIKE DI BLUR

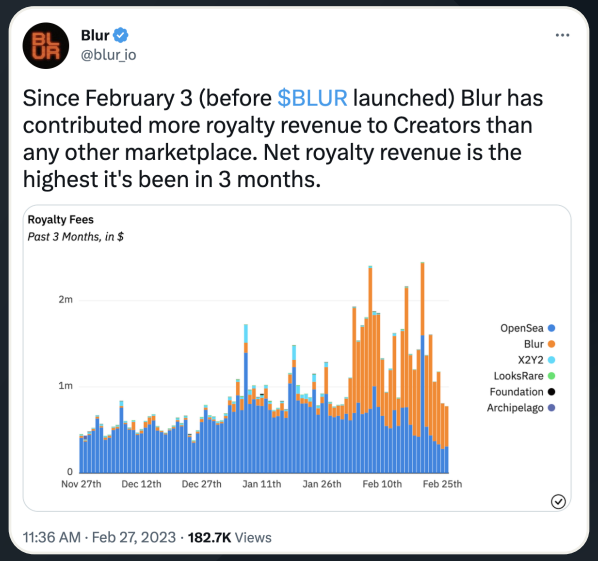


Figura 7. Il marketplace NFT Blur è tra i principali fattori trainanti dei 2 miliardi di dollari di transazioni NFT registrati nel febbraio 2023.[26]
Credito immagine: Infoblox

In vista del rilascio del token Blur il 14 febbraio 2023, abbiamo assistito a un aumento da cinque a sei volte del numero di lookalike relativi a Blur. della quantità nel marzo 2023, questo schema dimostra la volontà degli attori di tenersi al passo con le tendenze del mondo delle criptovalute, al fine di ottenere un guadagno veloce tramite le truffe.

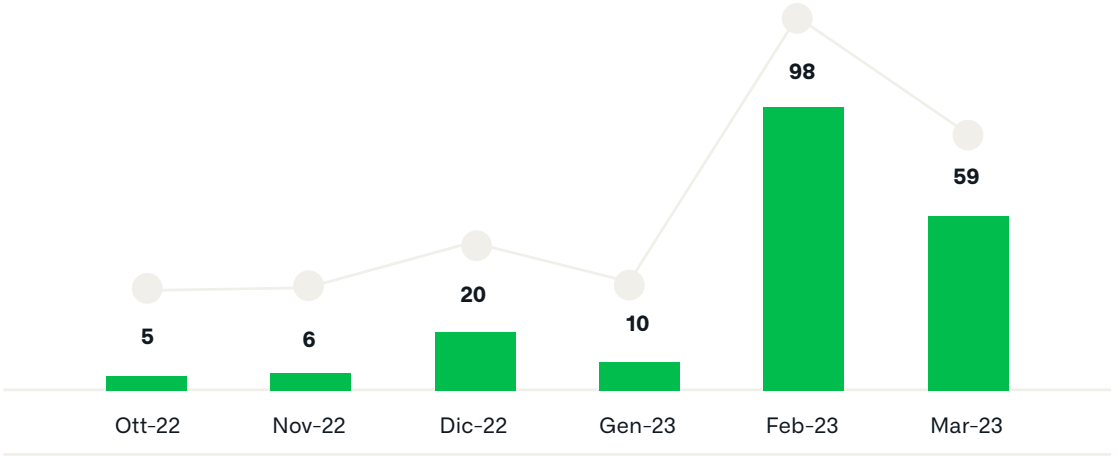


Figura 8. Drastico aumento dei lookalike relativi a Blur dall'annuncio del marketplace nell'ottobre 2022.

Infoblox tiene traccia di più attori specializzati in lookalike legati alle criptovalute. Questi attori prendono di mira tutte le principali entità del mercato, tra cui Blur e il suo concorrente Yuga Labs, proprietario di ApeCoin e della popolare NFT Bored Ape Collection. Nella tabella seguente forniamo un piccolo campione di questi domini. Le tecniche utilizzate da questi attori includono semplici modifiche al dominio di primo livello (TLD), l'aggiunta di una sola lettera e i nomi di dominio Unicode, che possono essere particolarmente difficili da riconoscere. Notare che nella tabella sottostante, c'è un accento sulla "i" in apecoíns[.]com. Nel DNS questo dominio equivale a xn--apecons-cza[.]com, che è un po' difficile da riconoscere come lookalike, ma in un browser web sarebbe praticamente indistinguibile dall'originale.

Tabella 2. Esempi di domini lookalike di Blur e Yuga Labs.

Domini lookalike di Blur [blur.io]	**Domini lookalike di 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

Ci sono anche dei lookalike meno tradizionali legati alle criptovalute che utilizzano YouTube come vettore per attirare i bersagli verso i loro domini.

Queste truffe iniziano con i threat actors che prendono di mira famosi creator di YouTube con attacchi di spear phishing utilizzando false offerte di sponsorizzazione che sembrano essere correlate a prodotti legittimi.[27] scaricare e aprire un file presumibilmente correlato all'offerta di sponsorizzazione, come una copia del software promosso o un file PDF contenente un contratto di sponsorizzazione.[28] In realtà, questi file sono payload di malware che, una volta aperti, rubano i cookie di sessione dal browser della vittima. I cookie rubati consentono all'aggressore di accedere all'account YouTube della vittima, anche se l'autenticazione a più fattori è abilitata.

Una volta che l'aggressore ha accesso all'account YouTube del creator, cerca di offuscare il fatto che il canale è stato violato cambiandone il nome e la foto del profile per abbinarli al tema del proprio attacco, che spesso è legato a Elon Musk o a una delle sue aziende.[29]
L'aggressore può anche eliminare o nascondere i video del canale per coprire ulteriormente le proprie tracce. L'aggressore inizia poi a trasmettere una versione modificata di un video relativo alle criptovalute, come il discorso di Elon Musk su Ark Invest, per attirare gli iscritti esistenti del canale.

Questi video modificati includono un testo in sovrimpressione che indirizza gli utenti a visitare il dominio lookalike legato alle criptovalute dell'aggressore, e un link al dominio è incluso anche nella descrizione dello stream.
I domini stessi sono truffe standard del tipo "raddoppia il tuo denaro", che spingono le vittime a inviare una certa quantità di criptovaluta a un indirizzo di portafoglio specifico, con la promessa di ricevere in cambio il doppio della somma. In questi attacchi, lo scopo del dominio lookalike è aumentare la credibilità dell'offerta abbinando il tema al video modificato e al canale YouTube rinominato.

LOOKALIKE DI TESLA

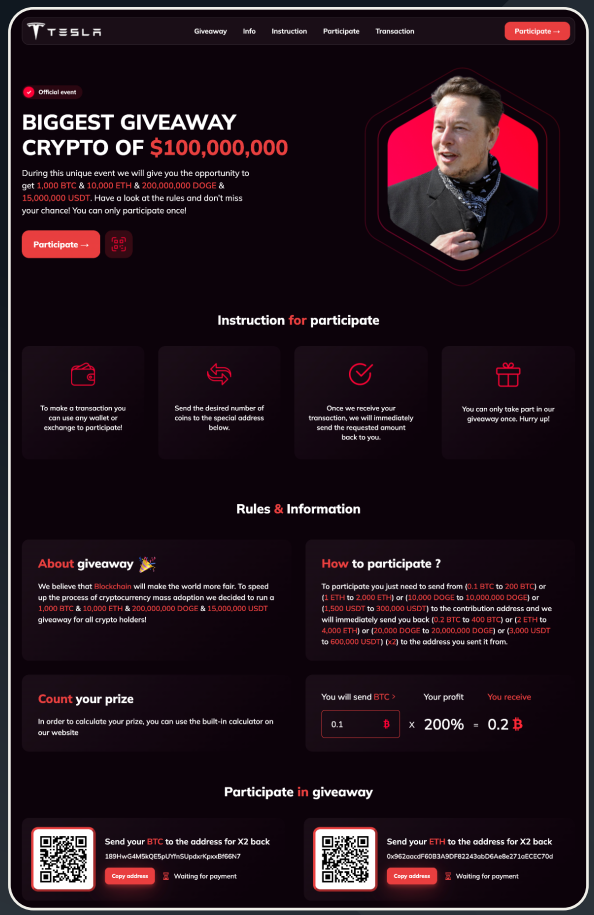


Figura 9. Dominio lookalike di Tesla tesla-online[.]net relativo alle criptovalute che spinge gli utenti a inviare criptovaluta a indirizzi specifici per ricevere in cambio il doppio. Credito immagine: Infoblox.

PRENDONO DI MIRA I SOCIAL MEDIA E GLI UTENTI MOBILI

Anche le piattaforme di social media, come Instagram e Twitter, insieme a marchi importanti come Apple, sono bersagli popolari per il phishing con lookalike.

Tutti i marchi e i servizi più diffusi sono continuamente presi di mira da questi attacchi, utilizzeremo solo alcuni esempi di questi tre marchi per illustrare la minaccia attuale. La raccolta di credenziali non è una novità; prima della comparsa dei social media e delle piattaforme di ID universali come l'ID Apple, i malintenzionati cercavano di entrare negli account e-mail. Tuttavia, dato che i social media e le piattaforme di ID universali sono ormai profondamente legati alle nostre vite, questi lookalike rappresentano una minaccia persistente.

Gli attori delle minacce prendono di mira gli account di social media di chiunque, non solo agli account di influencer e celebrità. Ci sono molti lookalike per Instagram: alcuni combosquat, altri omografi. Spesso tali domini apparivano in gruppi di domini registrati simultaneamente, suggerendo che facessero parte di una campagna coordinata creata utilizzando un DDGA. Gli esempi seguenti fanno tutti parte di un set Instagram che combina il marchio con parole come "help" e "feedback".

Tabella 3. Esempi di domini lookalike di supporto di Instagram.

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

Il contenuto di questi domini afferma che l'utente ha violato le norme sul copyright di Instagram e chiede all'utente di inserire il proprio nome utente per fare ricorso contro il verdetto; *vedere le Figure 10 e 11.*

LOOKALIKE DI INSTAGRAM

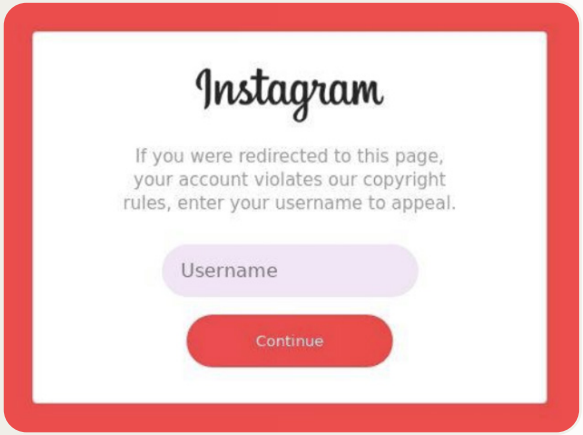


Figura 10. Il lookalike di Instagram help-Instagram-notice[.]com presenta un invito all'azione relativo al ricorso per violazione del copyright.
Credito immagine: DomainTools.[30]

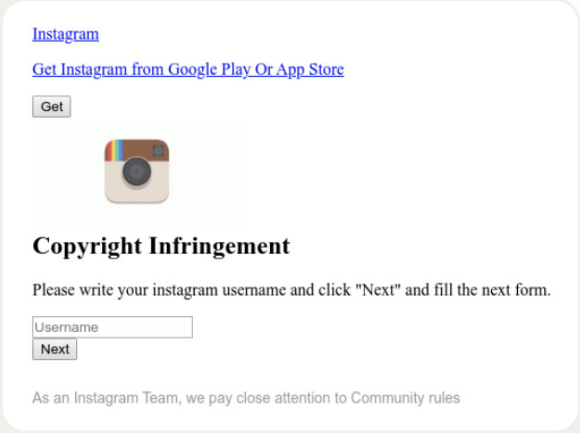


Figura 11. Il lookalike di Instagram help-instagram-about[.]com, che mostra un altro invito all'azione relativo al ricorso per violazione del copyright.
Credito immagine: URLScan.[31]

LOOKALIKE DI TWITTER

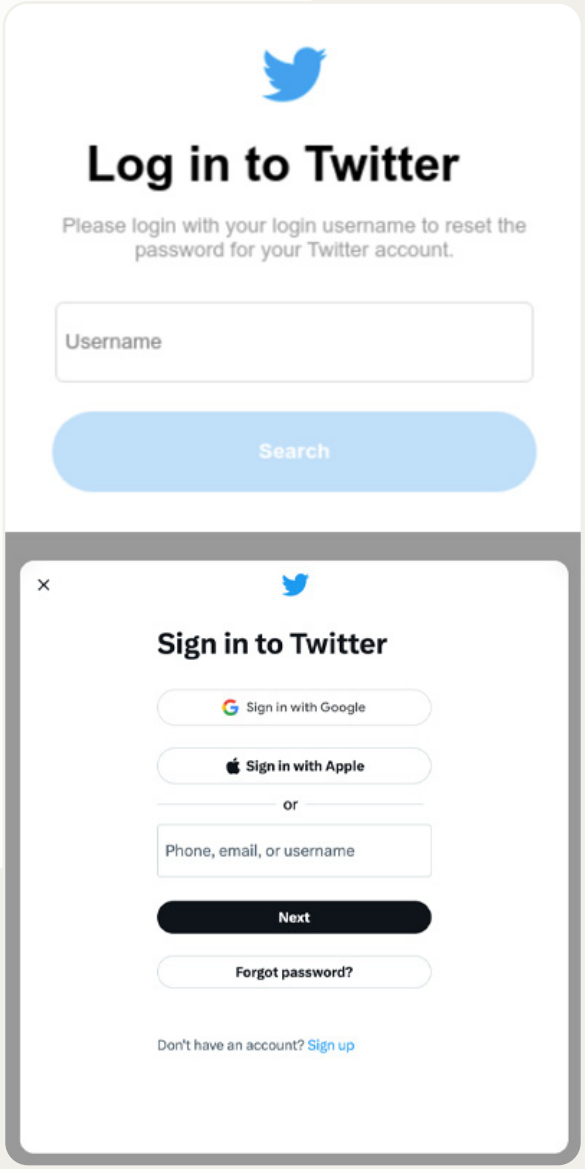


Figura 12. Convincente portale di reimpostazione della password sul lookalike di Twitter help-twitter-centre[.]net. L'immagine di phishing è in alto, quella legittima è in basso.
Credito immagine: DomainTools.[32]

Altri lookalike di Instagram prendono di mira l'ambito "segno di spunta blu" (l'approccio di Instagram alla verifica come personaggio pubblico), utilizzando una "L" minuscola al posto della "i" maiuscola.
Ironicamente, Instagram ha introdotto il segno di spunta blu per le personalità o le aziende famose come modo per combattere l'impersonificazione. *Non credere che i malintenzionati non utilizzino i lookalike per colpire le soluzioni anti-lookalike.*

Alcuni esempi sono:

Tabella 4. Esempi di domini lookalike per la verifica di Instagram.	
Instagram-blueticket-form[.]ml	Instagram-contactbluebadge[.]ga
Instagram-verification-badges-service[.]com	Instagrambluetickverifcation[.]cf
Instagramverifybadge-contact[.]cf	Instagram-badgecentre[.]gq

Monitorando i lookalike di Instagram, abbiamo scoperto che gli attori non hanno preso di mira un singolo social media.

Anche i lookalike di Twitter sono stati ospitati insieme a quelli di Instagram per la "violazione del copyright". Questi looka1ike di Twitter erano domini combosquat di phishing per le credenziali degli utenti e le pagine di destinazione sembrano essere un portale legittimo per la reimpostazione della password; *vedere la Figura 12.*

Oltre ai lookalike dei social media, durante la nostra ricerca abbiamo visto spesso lookalike di iCloud, il servizio cloud di Apple che offre archiviazione e sincronizzazione cloud tra i dispositivi Apple. Questi domini hanno sfruttato un numero relativamente piccolo di parole chiave; abbiamo osservato più frequentemente "apple", "findmy", "id" e "icloud". Non sono mancati i domini lookalike legati ad Apple.

Di seguito sono riportati alcuni esempi, tra cui alcuni che sembrano essere rivolti agli utenti di lingua spagnola:

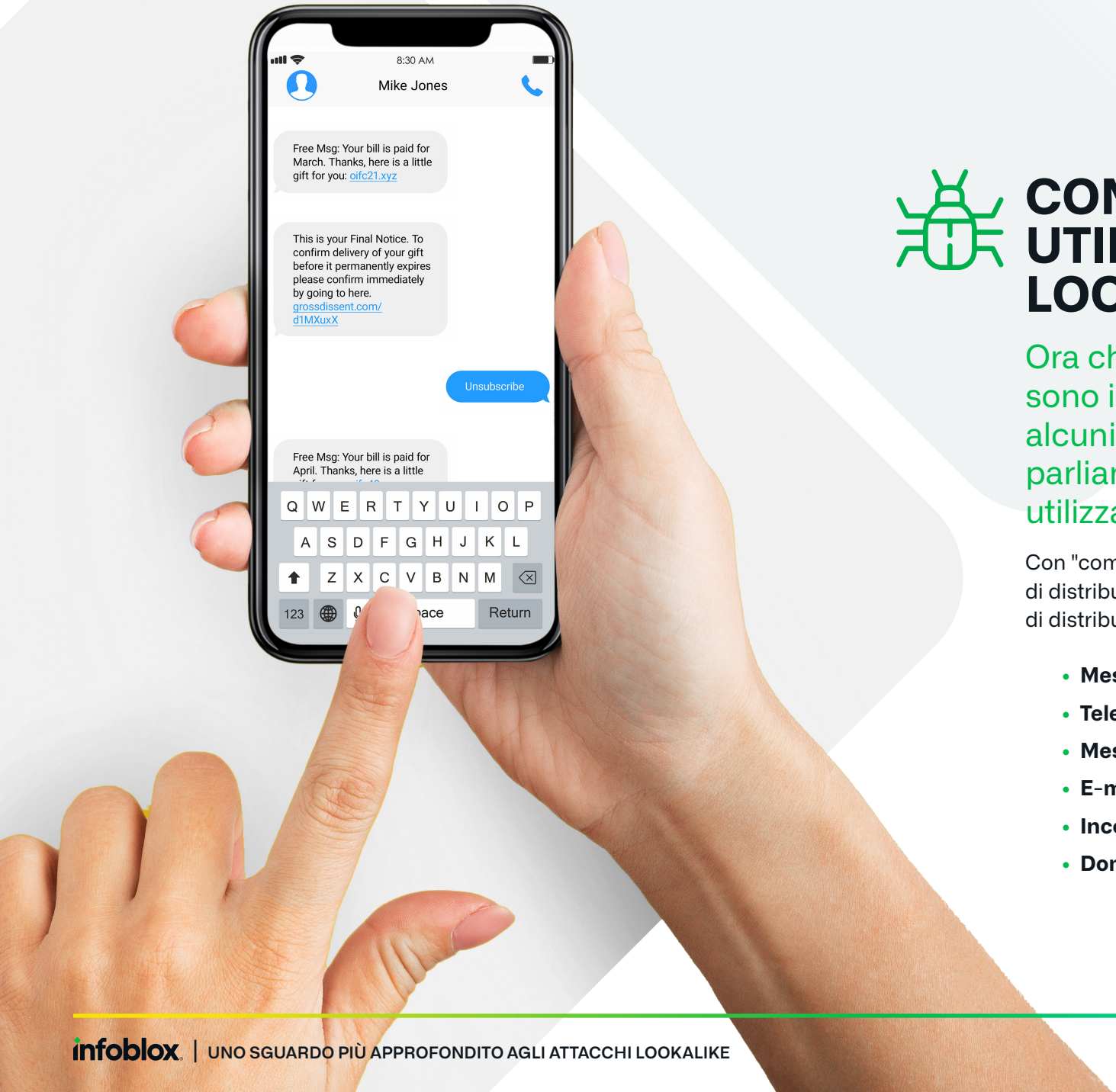
Tabella 5. Domini lookalike che prendono di mira i servizi legati ad Apple.	
supportid-apple[.]com	sopport-apple[.]com
soporte-latam[.]us	soporte-appleid[.]com
lcloud-web-app[.]com	icloud-fndmy[.]com

PRENDONO DI MIRA TUTTI

I nostri algoritmi di rilevamento identificano migliaia di nuovi domini lookalike ogni giorno. Qualsiasi azienda o servizio, grande o piccolo, ai qualii attori malintenzionati possono rubare denaro o identità sarà preso di mira. Chiuderemo questa sezione con un assortimento di domini lookalike che abbiamo visto in circolazione e il loro bersaglio.

Tabella 6. Domini lookalike e relativi bersagli.

Domini lookalike	Bersaglio del lookalike
mee6bot[.]ru	Bot di Discord, Mee6
vulcan[.]pm	Bot di Discord, Vulcan
o365-outlook[.]com, ms-o365[.]com, o365-outlook[.]com, https-o365[.]com	Microsoft Office 365
myato-refund[.]online	Ufficio Australiano delle Imposte
checkscam22[.]com, checkscams[.]online, checkscammer[.]xyz	Siti web di controllo delle truffe
xpressvpn[.]business, expressvpn-app[.]com, expressvpn-okta[.]com	Express VPN
anpost-paymentduty[.]com, ups-pay-deliveryfee[.]info, caddeliverypostca[.]com	Servizi postali e di consegna
crarebate-info[.]com	Rimborso fiscale canadese
ebl-ch[.]com	L'azienda energetica svizzera EBL
op-fi-palvelut[.]co, op-fi-io[.]in	Op[.]fi, servizio bancario e assicurativo digitale finlandese
boatairbuds[.]in, boatbudsmusc[.]in, boatflashsale[.]in, boatmusicairbud[.]in	L'azienda tecnologica indiana BoAt
pumauaeshoes[.]com, pumanzsale[.]com, pumaireland[.]com, vejaoutletcanada[.]ca	Aziende calzaturiere
secure1-scotiabank[.]com,r-scotiabank[.]com, chasebank-jpm[.]com, thetrustnationalbank[.]com, amèricafirst[.]com	Banche
sprint-ldg[.]com, tds-telecom[.]com, teistra[.]ne, 1111systems-okta[.]com, t-mobile-okta[.]us, vzw-sso[.]com	Provider di servizi Internet e cloud
sso-authentication[.]de, sso-securelogin[.]com, service-sys-2fa[.]com	Autenticazione a più fattori e domini Single Sign-On



COME VENGONO UTILIZZATI I LOOKALIKE?

Ora che abbiamo spiegato cosa sono i lookalike e presentato alcuni esempi di bersagli, parliamo di come vengono utilizzati.

Con "come" intendiamo i loro metodi di distribuzione. Infoblox ha osservato vari modi di distribuzione, come ad esempio:

- **Messaggi SMS**
- **Telefonate**
- **Messaggi diretti sui siti di social media**
- **E-mail**
- **Incorporazione nei codici QR**
- **Domini sul World Wide Web**

MANDANO MESSAGGI

Nonostante i miglioramenti nei filtri antispam per i messaggi di testo (SMS) sui telefoni cellulari, l'uso degli SMS per recapitare messaggi di phishing, spesso chiamato smishing, continua a crescere.

Gli attori sono in grado di distribuire rapidamente un gran numero di messaggi ed evitare alcuni dei meccanismi di sicurezza messi in atto per proteggere dagli attacchi di phishing via e-mail. Gli SMS vengono utilizzati sia per gli attacchi generici ai consumatori, sia per gli attacchi di spear phishing di tipo ristretto ai danni dei dipendenti delle organizzazioni. In questa sezione descriveremo due attori delle minacce che hanno utilizzato gli SMS e i domini lookalike per attaccare i consumatori e i dipendenti pubblici.

Per quasi un anno, Infoblox ha monitorato un attore di smishing con lookalike persistente che chiamiamo OpenTangle. A nostra conoscenza, questo attore non è stato segnalato altrove. Inizialmente, OpenTangle ha preso di mira i consumatori occidentali, utilizzando dei lookalike di istituzioni finanziarie, provider di servizi Internet e rivenditori online. Di recente, l'attore ha iniziato a prendere di mira i dipendenti e gli appaltatori del governo. Siamo a conoscenza di oltre 1.500 domini lookalike controllati da OpenTangle da quando ha iniziato a operare circa due anni fa. Alcuni dei domini di OpenTangle includono mtbsuportz0610[.]com, americafirst0nline[.]com e mygov03-ato[.]com.

Notare il suo uso di diverse tecniche di lookalike.

Uno degli autori di questo articolo ha ricevuto molteplici messaggi da OpenTangle, tra cui dei lookalike di M&T Bank, con cui l'autore non ha alcuna affiliazione. All'inizio delle sue campagne, OpenTangle includeva link URL abbreviati nei propri messaggi di smishing, forse sperando che l'offuscamento avesse successo. Tuttavia, a partire dal maggio 2022, ha iniziato a optare per i domini lookalike. La *Figura 13* mostra un esempio di una delle sue campagne bancarie, in cui vengono richieste le credenziali dell'utente.

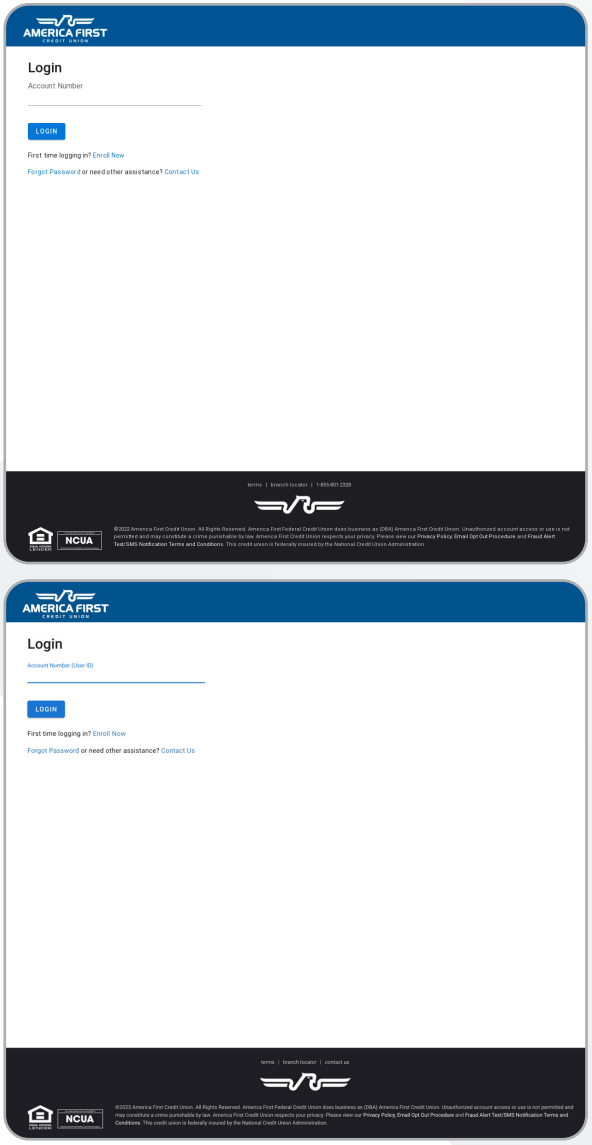


Figura 13. Una pagina di phishing sul dominio americafirst0nline[.]com rivolta ai titolari di conti America First Credit Union. L'immagine in alto è la pagina di phishing, l'immagine in basso è la pagina legittima.
Credito immagine: URLScan.[33]

OpenTangle ha iniziato a sfruttare l'MFA utilizzando i kit di phishing AitM nell'ultimo anno. Mentre le sue campagne precedenti utilizzavano pagine di accesso standard per il phishing e in genere si rivolgevano ai consumatori, la *Figura 14* mostra un esempio dell'avanzamento delle sue campagne. In questo caso, hanno preso di mira i titolari di un account myGov del governo australiano e hanno richiesto un codice MFA, anziché un semplice accesso. Includevano inoltre un link per chiamare l'helpdesk, un'altra tecnica emersa nel 2022 come mezzo per convincere gli utenti a visitare siti web dannosi.

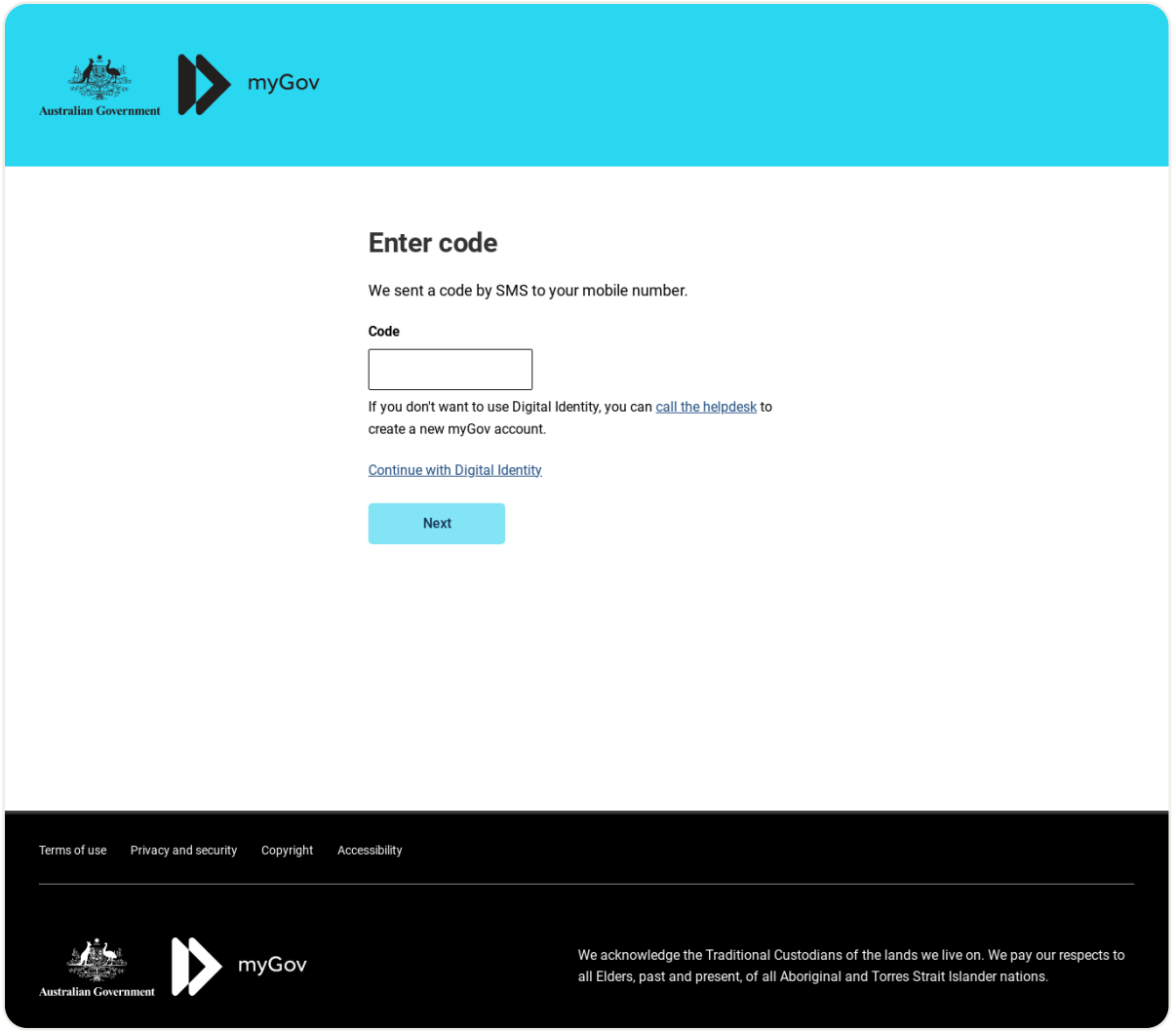


Figura 14. Dominio lookalike di OpenTangle www.mygovsupport-ato[.]com, che imita myGov, il portale online del governo australiano per il cloud governativo. Credito immagine: URLScan.[34]

Scamélie è un altro esempio di un attore che utilizza messaggi di smishing per diffondere lookalike.

L'attore che chiamiamo Scamélie è un insieme di gruppi e individui parzialmente affiliati, coinvolti in una lunga lista di truffe provenienti da Paesi francofoni e principalmente rivolte a questi ultimi. Li abbiamo visti anche impegnati in un targeting più generale in Europa e negli Emirati Arabi Uniti. I domini lookalike di Scamélie impersonano principalmente ISP, banche, servizi governativi e società di consegna. A causa dell'affiliazione libera del gruppo, abbiamo assistito anche a truffe ai danni di aziende meno conosciute, come compagnie di viaggio, aziende di abbigliamento sportivo e negozi di alimentari.

I domini lookalÏke di Scamélie sono spesso ospitati su grandi provider di cloud o società di hosting "a prova di proiettile". In alcuni casi, i truffatori hanno creato i propri hosting provider o utilizzano hosting provider creati da altri truffatori non affiliati. Abbiamo visto sia domini presi di mira che domini generici (my-account, resolve-an-issue, ecc.) registrati tramite identità rubate e pagati con carte di credito virtuali o criptovalute.

Una volta che gli attori hanno raccolto i dati della carta di credito, chiamano la vittima, fingendosi un dipendente della banca o dell'emittente della carta di credito della vittima.
Spiegano che i dati della carta di credito della vittima sono stati rubati, ma che aiuteranno a risolvere il problema. Il chiamante dice poi che la vittima riceverà due codici MFA che dovranno essere riletti al chiamante per la sicurezza del conto. In realtà, l'aggressore ha bisogno dei codici MFA per rubare denaro alla vittima in tempo reale. Il primo codice MFA aumenta l'importo del bonifico bancario e il secondo consente l'esecuzione della transazione. Per aumentare l'efficacia delle proprie chiamate, l'attore impiega chiamanti che sono idealmente donne e/o persone giovani in grado di parlare francese in un modo che non susciti il sospetto di un madrelingua.

Essendo un gruppo non organizzato, Scamélie è difficile da monitorare e analizzare. Spesso realizzano attacchi di smishing durante la notte delle loro vittime e chiudono i loro domini dopo solo un paio d'ore o giorni. Utilizzano script anti-bot e anti-scraping per ostacolare ulteriormente i ricercatori di sicurezza.

ESEMPI DI LOOKALIKE DI SCAMÉLIE

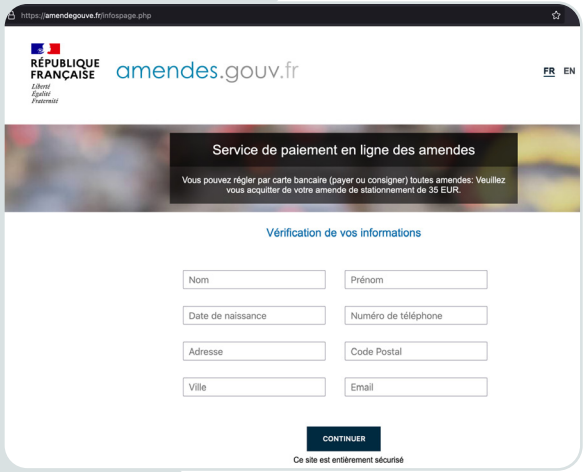


Figura 15. Un lookalike di Scamélie amendegouve[.]fr, che imita un portale di servizi governativi francesi.
Credito immagine: Infoblox.

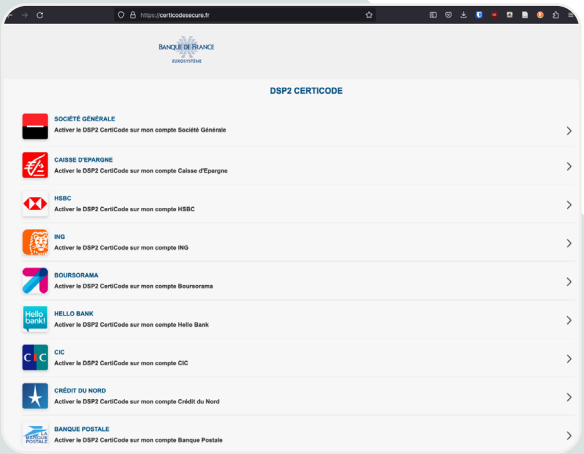


Figura 16. Un sito lookalike di Scamélie certicodesecure[.]fr, che falsifica un servizio bancario francese e invoglia le vittime a collegare i dati del proprio conto bancario.
Credito immagine: Infoblox.

USANO TELEFONATE VECCHIO STILE

Il 26 gennaio 2023 la Cybersecurity and Infrastructure Security Agency (CISA) ha pubblicato un avviso di sicurezza informatica (CSA, Cybersecurity Advisory) sull'uso dannoso del software di monitoraggio e gestione remota (RMM, Remote Monitoring and Management).[35]

Nell'ottobre 2022 la CISA ha identificato una campagna in cui i malintenzionati inviavano e-mail di phishing contenenti un numero di telefono e invitavano gli utenti a chiamare. L'e-mail è stata progettata per sembrare un messaggio di assistenza clienti e, quando gli utenti chiamavano il numero di telefono, gli attori li invitavano a visitare un dominio dannoso. Quando l'utente lo faceva, veniva scaricato un file eseguibile e poi veniva contattato un secondo dominio dannoso, da cui veniva scaricato un software RMM aggiuntivo. Questi software, AnyDesk e ScreenConnect, erano legittimi, ma preconfigurati per connettersi al server RMM dell'attore per la persistenza.

I domini utilizzati sono lookalike di servizi noti; la probabilità di accettare il dominio è ancora più alta per le vittime a cui è stato fornito per telefono, a causa del social engineering utilizzata per creare gli scipt e i personaggi dei chiamanti. Abbiamo eseguito una revisione retroattiva dei nostri dati e abbiamo trovato prove che l'attore è stato attivo per più tempo di quanto indicato dal CSA.[36] Queste campagne erano attive almeno dalla primavera del 2021, oltre un anno prima degli incidenti che CISA e Silent Push, in articoli separati, hanno descritto. Abbiamo anche assistito al riutilizzo dei domini. Ad esempio, il dominio amzsupport[.]live, un lookalike di Amazon, faceva parte di una campagna attiva nell'aprile 2020 e poi è stato utilizzato di nuovo nell'ottobre 2021.

Quando gli attacchi contro la protezione MFA dei sistemi aziendali interni sono venuti alla luce all'inizio del 2023, è stato rivelato che in alcuni casi gli attori telefonavano alla vittima, fingendo di far parte del suo reparto IT. Questo veniva fatto dopo che la vittima non aveva risposto alla richiesta iniziale ed era una soluzione utilizzata per fornire ulteriore legittimità alla necessità che l'utente visitasse il dominio lookalike. Gli utenti che hanno seguito le istruzioni hanno permesso all'attore di rubare le loro credenziali aziendali.

MANDANO SPAM

Sebbene abbiamo visto attori astuti utilizzare lo smishing e le telefonate per distribuire i lookalike e intrappolare le vittime, l'e-mail di phishing non è mai passata di moda.

Infoblox analizza decine di migliaia di e-mail di malspam ogni giorno, rivelando un flusso apparentemente infinito di campagne che distribuiscono domini lookalike. Evidenzieremo alcune di queste campagne, ma ricordiamo l'importanza che le organizzazioni mantengano un monitoraggio diligente delle e-mail di phishing.

Una di queste campagne si rivolge a Xfinity, un'importante azienda di telecomunicazioni americana. Questi lookalike hanno caratteristiche simili a DGA e sono della forma xfnity<parola breve o parziale>. com. Notare che "Xfinity" è scritto in modo errato perché manca la prima "i". L'attore si è anche assicurato che il nome del mittente apparisse legittimo, mostrandosi come "Xfinity Mobile", che utilizza una lettera "X" maiuscola cirillica. Le e-mail del mittente utilizzavano i propri domini mostrando anche caratteristiche simil DGA nel nome utente, costituite dallo schema noreply- <parola chiave>, ad esempio noreply-corporate@xfnitycard[.]com. Gli attori non hanno utilizzato domini univoci per ogni e-mail. In alcuni casi, i domini sono stati ripetuti, ma la parola chiave è stata modificata, come in: noreply-corporate@xfnitycard[.]com e noreply-active@xfnitycard[.]com.

Tabella 7. Domini lookalike di Xfinity.

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

I domini identificati nella campagna utilizzano una tecnica che abbiamo chiamato "decoy parking": quando un dominio viene visitato direttamente e sembra parcheggiato, ma in realtà il mail server del dominio è attivo e invia e-mail dannose. Abbiamo riscontrato che il decoy parking è abbastanza comune e non viene segnalato da altri fornitori. *Vedere la Figura 17 per un esempio di pagina di decoy parking.*

LOOKALIKE DI XFINITY

Figura 17. Pagina di decoy parking esposta dal lookalike di Xfinity xfnityrayton[.]com. Credito immagine: URLScan.[37]

LOOKALIKE DI 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 della campagna di malspam che utilizza Wedo Machinery come esca e il dominio lookalike acrobat-adobe[.]com come C2 del malware. Credito immagine: Infoblox

La nostra analisi ha trovato questi lookalike di Xfinity in documenti Word distribuiti e dannosi.

Gli argomenti della campagna fungevano anche da invito all'azione e erano incentrati sul rifiuto del pagamento o sulla minaccia di interruzione del servizio, come "[Annuncio] Il tuo servizio è a rischio di interruzione" o "[Richiede azione] Non possiamo addebitare l'importo sulla tua carta, correggi questo errore". Il corpo di queste e-mail è stato realizzato in modo tale da sembrare provenire dall'assistenza clienti, chiedendo ai destinatari di "vedere l'allegato per i dettagli del caso".

Un'altra campagna identificata da Infoblox ha utilizzato un'azienda di riciclaggio cinese, Wedo Machinery, per rilasciare un loader di ransomware. W Abbiamo identificato 176 e-mail all'interno di questa campagna, ciascuna con un file .zip contenente un singolo eseguibile identificato come Zmutzy. *Vedere la Figura 18 per un esempio di un'e-mail all'interno della campagna.* Abbiamo osservato due nomi di file all'interno della campagna: PO-0097(1).zip e PO-29862K.zip. Il loader di Zmutzy utilizza il dominio lookalike acrobat-adobe[.]com per scaricare payload aggiuntivi.

USANO I CODICI QR

Oltre ai lookalike diretti delle criptovalute, abbiamo osservato l'uso del phishing con codice QR, in cui un codice QR viene utilizzato per offuscare la destinazione di un URL e fornire contenuti dannosi, in combinazione con i domini lookalike creati per invogliare gli utenti a reclamare premi gratuiti e fornire informazioni sull'account del portafoglio di criptovalute.

In un esempio, il codice QR ha reindirizzato la vittima a un link bridge[.]walletconnect[.]com, un meccanismo utilizzato per rubare fondi. In questa truffa, gli attori hanno creato un account Twitter, @adidas_weare, per creare credibilità e condividere i loro domini lookalike; *vedere la Figura 19*. L'account ha accumulato 16.000 follower al 21 febbraio 2023; fortunatamente, l'account è stato eliminato o rimosso.

Gli attori hanno pubblicizzato falsi omaggi di diversi articoli tra cui auto Porsche e abbigliamento o scarpe Adidas. I domini sono prevalentemente combosquat contenenti le parole chiave "adidas" o "porsche". Dopo aver visitato i domini lookalike, come mostrato di seguito nella *Figura 20*, agli utenti veniva chiesto di scansionare un codice QR che consentisse loro di richiedere l'articolo regalato, quindi venivano reindirizzati all'applicazione decentralizzata, WalletConnect, che fornisce all'attore l'accesso ai fondi dell'utente.

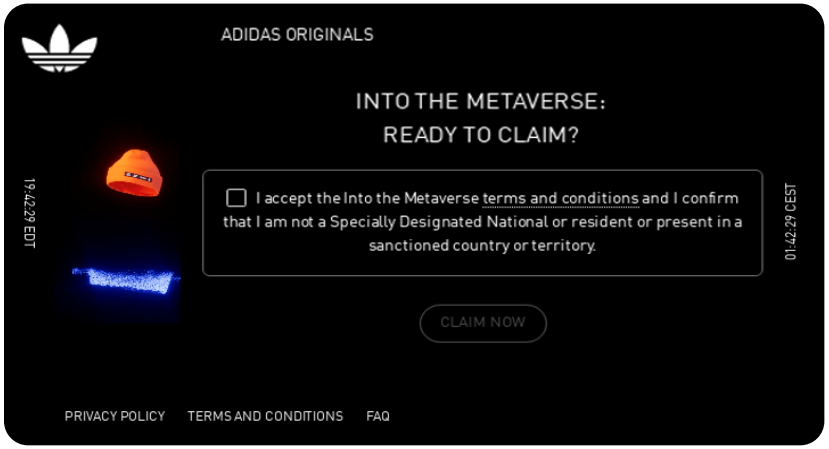


Figura 20. Dominio lookalike di Adidas adidas-go[.]com che invoglia gli utenti a fare clic per richiedere un articolo gratuito. Credito immagine: URLScan.[39]

Se gli utenti scansionano il codice QR e collegano i loro portafogli di criptovalute all'applicazione decentralizzata, gli attori sono in grado di estorcere criptovalute all'utente. Questi domini utilizzano nameserver condivisi e sono ospitati su un indirizzo IP con risoluzione russa, 185[.]149[.]120[.]83, che è completamente controllato dagli attori e contiene altri lookalike di Blur e Arbitum, una soluzione per migliorare la velocità e la scalabilità degli smart contract di Ethereum.

LOOKALIKE DI ADIDAS

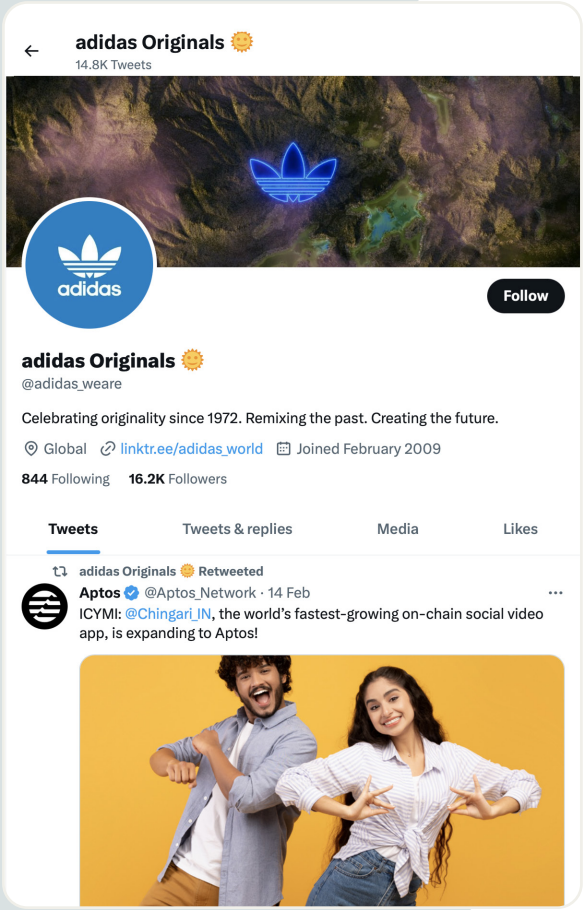


Figura 19. L'account Twitter lookalike @adidas_weare di Adidas Originals @adidasoriginals. Credito immagine: Infoblox.

USANO IL DNS

I lookalike non si presentano solo come domini di siti web.

Abbiamo riscontrato che vengono utilizzati in diverse funzionalità DNS, tra cui:

- **Nameserver**
- **Mail server**
- **Record CNAME**
- **Record PTR**

Nella maggior parte dei casi, questi domini non avranno un tipico record A o la presenza di un sito web e potrebbero spesso apparire parcheggiati, un'implementazione del decoy parking che abbiamo descritto in una sezione precedente. Gli aggressori utilizzano anche domini lookalike per il reindirizzamento e le comunicazioni C2 nel DNS.

NAMESERVER

Come esempio di nameserver looƘalike, i domini bitkeep[.]dev e flutter[.]direct sono stati registrati nel novembre 2022. Entrambi sono lookalike di domini diversi, ma condividono un'infrastruttura. BitKeep è un portafoglio di criptovalute multi-chain decentralizzato che mira a essere un unico hub per tutte le transazioni di criptovaluta. Il dominio ufficiale di BitKeep è bitkeep[.]com e l'azienda è operativa da cinque anni con oltre 8 milioni di utenti.[40] Flutter è il toolkit dell'interfaccia utente (UI) portatile di Google per la creazione di applicazioni compilate in modo nativo per dispositivi mobili, web e desktop da un'unica base di codice. Il dominio ufficiale di Flutter è flutter[.]dev.[41]

Entrambi i domini legittimi ospitano contenuti web nel dominio principale, ma nessuno dei domini lookalike lo fa. Al momento della registrazione, entrambi i domini fungevano da nameserver per un altro dominio, get-flutter[.]com, che è un altro lookalike di Flutter. A quel tempo, i domini erano ospitati sul provider di hosting offshore svizzero Private Layer. Questa rete ospitava anche flutter[.]vision. Anche se non possiamo attribuire in modo definitivo questi domini a un'attività dannosa, dimostrano un modello di sfruttamento dei domini lookalike per scopi non tradizionali. Si rivelano piuttosto difficili da analizzare anche per ricercatori esperti e hanno poche probabilità di attivare la maggior parte degli algoritmi di threat intelligence.

MAIL SERVER

Oltre ai nameserver, abbiamo visto dei lookalike utilizzati come mail server. I domini whirlpoolmxonline[.]com e whirlpoolservicesmx[.]com prendono di mira il principale marchio di elettrodomestici Whirlpool e condividono un'infrastruttura comune. Sono ospitati sullo stesso indirizzo IP, di proprietà di Lyra Hosting, un provider di hosting e VPS di bassa qualità con sede alle Seychelles, e condividono nameserver comuni.

Sebbene prendano di mira direttamente Whirlpool con il nome di dominio di secondo livello (SLD, Second Level Domain), abbiamo anche identificato delle caratteristiche all'interno di ogni dominio che dimostrano che prendono di mira anche altri importanti marchi di elettrodomestici. L'SLD whirlpoolmxonline[.]com ha tre sottodomini: mabe-onlinemx[.]whirlpoolmxonline[.]com, samsung-onlinemx[.]whirlpoolmxonline[.]com e lg-onlinemx[.]whirlpoolmxonline[.]com. Mabe è un'azienda messicana di elettrodomestici. L'SLD whirlpoolservicesmx[.]com non ha sottodomini, ma la catena storica di certificati SSL associata al dominio indica il targeting di marchi di elettrodomestici simili a whirlpoolmxonline[.]com: www[.]lgservicesmx[.]mabeservice[.]com e *.lgservicesmx[.]com.

L'utilizzo di lookalike come mail server offre un'ulteriore sfida per il rilevamento delle e-mail di phishing su un endpoint, a causa dell'apparenza di legittimità a una prima occhiata alle intestazioni delle e-mail.

MALWARE C2

Nella precedente paragrafo sulla distribuzione delle e-mail, abbiamo menzionato come una campagna di malspam che abbiamo identificato e che stava rilasciando il loader del ransomware Zmutzy utilizzava il dominio lookalike acrobat-adobe[.]com come malware C2. I lookalike sono perfetti per i malware C2, perché possono facilmente nascondersi nel traffico di rete insieme ai domini legittimi.I ricercatori di ESET, un'azienda slovacca di software per la sicurezza, hanno identificato un malware C2 per FatalRAT (trojan di accesso remoto) che si presentava come Telegram, l'applicazione di messaggistica, nel febbraio 2023.[42]

Tabella 8. Lookalike di Telegram che funzionano come C2 del malware.

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

I domini che ospitano i file .exe dannosi erano anche lookalike di Telegram, così come WhatsApp, Skype, Google Chrome e Firefox.

REINDIRIZZAMENTI

I lookalike possono anche essere utilizzati come reindirizzamenti. Abbiamo identificato un'ampia rete di domini typosquat che reindirizzano i visitatori a choto[.]xyz, un dominio C2 che reindirizza condizionatamente le vittime al dominio di destinazione lotto60[.]com. L'attore utilizza servizi di reverse proxy e la protezione bot di Cloudflare su choto[.]xyz, presumibilmente per impedire il rilevamento e l'esplorazione da parte dei ricercatori di sicurezza. Il dominio di destinazione sembra gestire un programma di marketing di affiliazione fraudolento. Analizzando il DOM (Document Object Model), possiamo vedere che l'HTML contiene una funzione gtag() inline che invia i dati dei visitatori a Google Analytics con l'ID di analisi G-DT4YWT5VP8. Oltre a gonfiare i numeri del marketing di affiliazione dell'attore, abbi amo osservato che lotto60[.]com viene richiesto via HTTP da file potenzialmente dannosi che corrispondono a signatures di file confermate come il trojan di accesso remoto Nighthawk.[43]

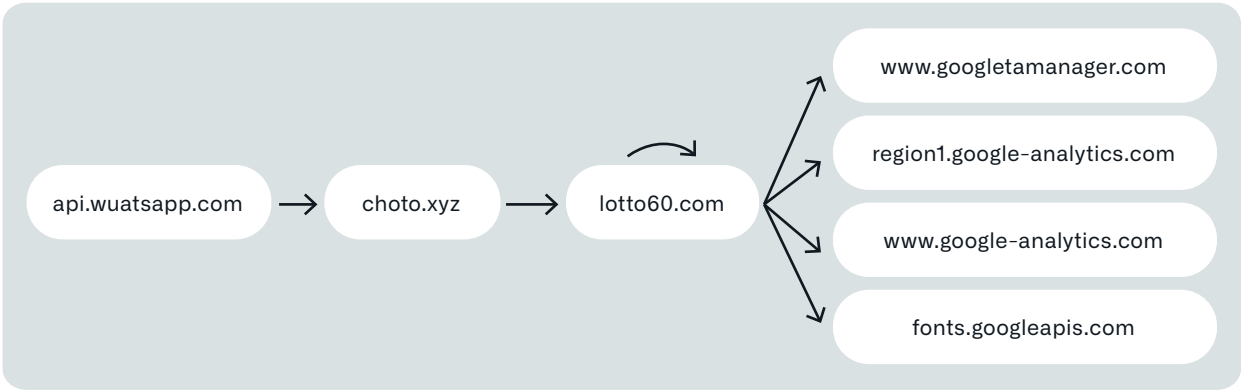


Figura 21. Esempio di catena di reindirizzamento da un dominio typosquat a Google Analytics. Credito immagine: URLQuery.[44]

I domini typosquat di prima fase imitano una varietà di aziende. Alcuni esempi includono →

Tabella 9. I lookalike funzionano come reindirizzamenti in una campagna di marketing di affiliazione.

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

Questi typosquat vengono in genere parcheggiati da uno a tre mesi prima di essere utilizzati come reindirizzamenti. L'attore ha dimostrato grande cura nella creazione di questi domini typosquat. Ogni carattere errato è direttamente adiacente al carattere corretto su una tastiera QWERTY inglese (Stati Uniti). Si tratta di errori che un utente medio potrebbe commettere più volte in un solo giorno, a parte gli utenti che guardano la tastiera mentre digitano.

PERCHÉ SONO EFFICACI?

Hai notato le 19 parole lookalike che abbiamo disseminato finora in questo documento? Alcuni di questi lookalike sono molto difficili da notare!

Suggerimento: ce ne sono altri 6. Vedi se riesci a trovarli.

Finora abbiamo trattato alcuni bersagli specifici ed il metodo di deployement delle infrastrutture che servono i domini lookalike. Ma perché sono così efficaci? Cosa li rende una minaccia così persistente?

La risposta è complicata e coinvolge aspetti di psicologia, implementazioni tecniche e semplici errori umani:
è questo che ci rende umani, dopotutto!

PSICOLINGUISTICA

Psicologicamente, il cervello umano va in cortocircuito (in questo caso, intendiamo la definizione letterale di una corrente che prende un percorso involontario di minor resistenza) durante la lettura. Probabilmente hai già visto un meme che recita qualcosa come:

> ***Sceodno una rcireca dell'Uinervtisà di Cmabrigde, non ipmtroa in che odirne snoo le ltteere in una praloa, la csoa iprmoatnte è che la pmria e l'utlmia ltteera sinao al psoto guitso. Le atlre psosono esrese in dsoidrnie e poui cmnouque lgegre snzea porbelma. Qeutso è prehcé la metne uanma non lgege una ltteera alla vltoa ma la praloa nel suo isneime.***

Sebbene l'affermazione sia infondata nel senso che nessuna ricerca del genere è mai stata pubblicata a Cambridge, il concetto di fondo sembra avere valore. Ad esempio, una recente ricerca suggerisce che "vedere una parola confusa attiva una rappresentazione visiva che viene confrontata con parole conosciute".[45] Anche se provare o confutare questioni fondamentali della psicolinguistica va oltre lo scopo di questo documento, vogliamo mostrare come la psicolinguistica giochi un ruolo importante nell'efficacia dei lookɑlike.

Nello specifico, i cortocircuiti del cervello umano giocano un ruolo quando si tratta di omograFi ed errori di battitura. Quando vedi un dominio come lnfoblox[.]com, il tuo cervello non analizza necessariamente ogni singola lettera in quel nome di dominio, quindi potresti non notare mai che il primo carattere è in realtà una "L" minuscola e non una "i" maiuscola.

Per ragioni simili, quando vedi il dominio goooogle[.]com, il tuo cervello potrebbe non fermarsi a riconoscere che ci sono tre lettere "o" piuttosto che le due corrette... Almeno, non fino a quando non è troppo tardi e hai già fatto clic su di esso.

SUPPORTO PUNYCODE: SUCCESSI ED ERRORI

I browser web dispongono di modi per difendere gli utenti dagli attacchi di om0grafi di nomi di dominio internazionalizzati (IDN). La prima e più importante linea di difesa è quella di "tradurre" il dominio Unicode in Punycode, che può essere riconosciuto dal suo "xn--" iniziale e sembra essere incomprensibile ad occhio nudo. Ciò è dovuto al fatto che Punycode esegue il mapping dei caratteri Unicode al sottoinsieme molto più limitato di caratteri ASCII (American Standard Code for Information Interchange) contenenti solo lettere, cifre e trattini. Tutti i principali browser supportano i domini Punycode. Google fornisce una descrizione dettagliata dell'euristica coinvolta nell'algoritmo che determina se mostrare la versione internazionalizzata o Punycode di un dominio in Chromium.[46] Mozilla fornisce una descrizione simile.[47]

Mozilla offre anche questo testo stimolante nella descrizione del suo algoritmo di visualizzazione IDN:

> ***La nostra risposta a questo problema è che, in ultima analisi, spetta ai registri assicurarsi che i loro clienti non possano truffarsi a vicenda. I browser possono mettere in atto alcune restrizioni tecniche, ma noi non siamo in grado di fare questo lavoro al posto loro, pur continuando a mantenere condizioni di parità per gli script non latini sul web. I registri sono gli unici in grado di implementare un controllo adeguato. Da parte nostra, vogliamo assicurarci di non trattare le scritture non latine come cittadini di seconda classe.***

Nel 2017, il ricercatore di sicurezza Xudong Zheng ha registrato un dominio già in Punycode, xn--80ak6aa92e[.]com, che si traduce in "apple[.]com", contenente caratteri cirillici che imitano l'aspetto dei caratteri latini in "apple".[48] In quel periodo, i browser Web Internet Explorer, Microsoft Edge, Safari, Brave e Vivaldi non erano vulnerabili, ma Chrome, Firefox e Opera lo erano. Al momento solo Firefox continua a tradurre Punycode, lasciando gli utenti vulnerabili all'attacco (di recente non abbiamo testato il dominio su Internet Explorer o Microsoft Edge).

COS'È PUNYCODE?

Punycode è una codifica speciale usata per convertire i caratteri Unicode in ASCII, che è un set di caratteri più piccolo e limitato. Punycode viene utilizzato per codificare i nomi di dominio internazionalizzati (IDN).

SMISHING IN iMESSAGE CON OMOGRAFI IDN

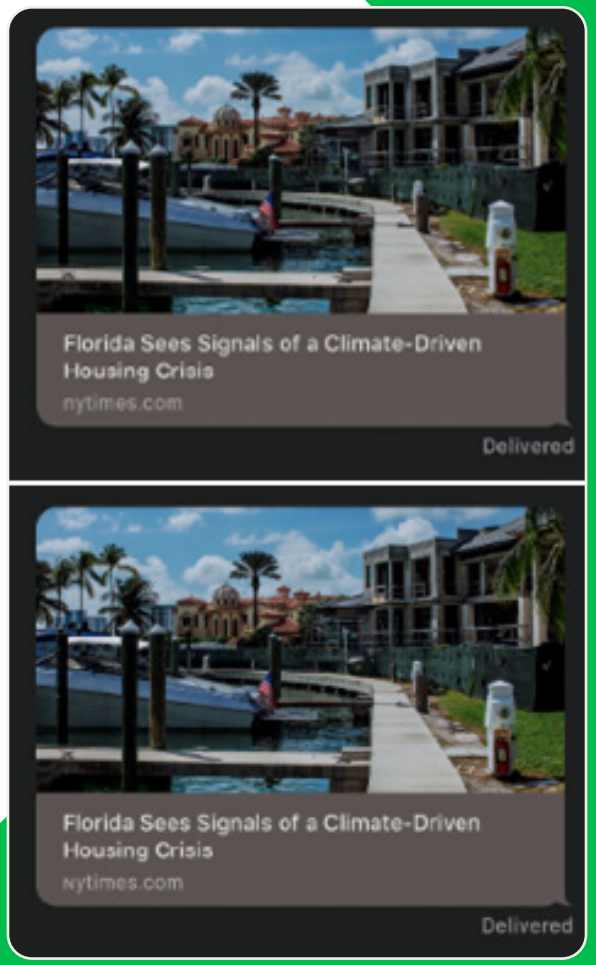


Figura 22. In alto, immagine proveniente da Tyler Butler che mostra un vero articolo del New York Times inviato tramite iMessage. In basso, immagine proveniente da Tyler Butler che mostra un articolo falsificato del NYT su un dominio omografo IDN.
Credito immagine: Tyler Butler.

Hu et al. hanno eseguito un'analisi longitudinale e quantitativa sull'efficacia delle difese basate su browser contro gli attacchi omografici IDN.[49]

Hanno deciso di rispondere a tre domande:

1. Quali politiche implementano i principali browser e in che misura le applicano?
2. Esistono modi per aggirare sistematicamente le politiche esistenti?
3. Quanto gli internauti sono in grado di riconoscere gli omografi IDN e gli omografi IDN che aggirano le politiche del browser sono più o meno ingannevoli?

Per rispondere alle domande, gli autori hanno esaminato cinque browser tradizionali (Chrome, Firefox, Safari, Microsoft Edge e Internet Explorer) nell'arco di cinque anni (da gennaio 2015 ad aprile 2020). Hanno generato 9.000 casi di test per rispondere alle prime due domande e hanno condotto uno studio sugli utenti per rispondere alla terza. Chrome ed Edge hanno avuto molto successo nel visualizzare Punycode invece dei corrispondenti omografi IDN; entrambi i browser hanno avuto un tasso di errore complessivo (in cui veniva mostrata la versione IDN anziché Punycode) del 20,62%. Safari e Firefox hanno ottenuto risultati molto peggiori, con un tasso di errore complessivo rispettivamente del 42,91% e del 44,46%. Ogni browser presentava tassi di errore diversi a seconda della categoria di IDN. Inoltre, gli autori hanno scoperto che gli internauti faticano a identificare gli IDN omografi e stabilire l'autenticità di quelli bloccati dai browser si è rivelato particolarmente complicato: il 48,8% degli utenti pensava che fossero autentici, il 48,5% degli utenti pensava che non lo fossero e il 2,7% non sapeva dirlo.

Finora ci siamo concentrati solo sui browser desktop. Ma come abbiamo visto con gli attacchi di smishing con lookalike descritti in precedenza in questo documento, i domini omografi IDN sono utilizzati comunemente anche sui dispositivi mobili, dove potrebbero persino essere più dannosi. Dimensioni dello schermo più piccole, barre degli indirizzi più piccole e una generale mancanza di anteprima dei link possono portare ad attacchi lookalike più efficaci. Anche quando è presente l'anteprima dei link, gli omografi IDN possono comunque essere efficaci sui dispositivi mobili. Nel 2021, il ricercatore di sicurezza Tyler Butler ha pubblicato un articolo sulla plausibilità dello smishing utilizzando gli omografi IDN in iMessage.[50] iMessage offre anteprime dettagliate dei link, ma un utente malintenzionato esperto può aggirare questo problema abbastanza facilmente con un dominio lookalike abbastanza buono e un po' di lavoro di stile per la pagina web stessa. Come osserva Butler, questa forma di attacco può essere utilizzata per diffondere disinformazione, rubare credenziali o distribuire malware o spyware mirati.

Butler spiega che Apple ha affermato che non affronterà la vulnerabilità a causa del fatto che gli omoɡrɑfi sono "visivamente distinguibili". Considerando la Figura 22, cosa ne pensi? Riesci a individuare la differenza?

ERRARE È UMANO, PERDONARE È DIVINO... MA AUTOMATIZZARE È SAGGIO

Sul World Wide Web, alcuni esseri umani non sono così indulgenti nei confronti degli errori degli altri. Come abbiamo accennato, gli attori utilizzano domini typosquat per sfruttare gli errori di ortografia naturali di altri. Tutto ciò che un utente malintenzionato deve fare affinché un typosquat sia efficace è registrare un dominio plausibile e attendere. Questo è tutto. Prima o poi, un essere umano commetterà quell'errore di ortografia e finirà su un dominio che non aveva intenzione di visitare. Naturalmente, i malintenzionati non si limitano ad aspettare, ma invogliano in modo proattivo le persone a fare clic. E nel nostro mondo in rapida evoluzione, molte volte non ci rendiamo nemmeno conto di aver commesso un errore in primo luogo.

In fin dei conti, i lookalike si chiamano così per un motivo: assomigliano a domini noti con l'intento di ingannare un essere umano. Come abbiamo visto, alcuni lookalike sono più efficaci di altri, ma la scelta del nome di dominio è solo una parte dell'efficacia di un lookalike. Anche il modo in cui viene distribuito un dominio lookalike può avere un impatto significativo sul successo complessivo della campagna. Prendiamo, ad esempio, un lookalike Okta o MFA come okta[.] Infoblox[.]com, o okta-Infoblox[.]com. Una persona attenta che controlla tre volte ogni nome di dominio prima di visitarlo (buona fortuna a trovare una di queste persone) potrebbe notare che la "i" nel dominio di secondo livello (SLD) è in realtà una "L" minuscola. Ma quel lookalike, abbinato a un messaggio SMS ben fatto al numero di telefono che hanno nel profilo online del loro datore di lavoro, ad esempio, potrebbe fare la differenza. Se si aggiunge all'equazione una telefonata con un invito urgente all'azione, il gioco è fatto. Naturalmente, questo è un esempio fittizio (con l'utilizzo di tutti i componenti) di spear phishing, e non una campagna generale che impiega i lookalike, ma il punto è lo stesso: le tecniche di lookalike possono essere applicate efficacemente ai domini in diversi modi e a diverse parti dell'infrastruttura DNS.

Tutto questo per dire che ai lookalike non si applica il modo di dire: "La prima volta che mi freghi è colpa tua, la seconda è colpa mia". Anche le persone più attente e consapevoli della sicurezza possono cadere in balia di un lookalike, e farlo di nuovo, e di nuovo ancora. I malintenzionati hanno il sopravvento in questa guerra, ma non è ancora persa. Infoblox ha soluzioni a livello di DNS per garantire che le organizzazioni abbiano la capacità di reagire e difendersi efficacemente.

IOCs

L'elenco completo per questo documento è disponibile su GitHub all'indirizzo https://github.com/infobloxopen/threat-intelligence

SOLUZIONI INFOBLOX

I domini lookalike rimangono popolari tra gli aggressori grazie alla loro efficacia e alla difficoltà di rilevarli su larga scala. La sfida è aggravata dalla difficoltà di identificare automaticamente un dominio sospetto destinato a imitare un bersaglio legittimo. Ciò ha portato le aziende e gli enti governativi a preoccuparsi sempre più dei domini lookalike che impersonano i loro domini aziendali o la catena di approvvigionamento.

Infoblox BloxOne Threat Defense (B1TD) Advanced offre una soluzione unica, ampia e completa contro le minacce lookalike. Sfruttando DNS su larga scala, Infoblox è in grado di applicare una serie di analisi a centinaia di migliaia di nuovi SLD ogni giorno. Ciò include più analisi per il rilevamento di lookalike, ad esempio una valutazione automatica delle somiglianze visive negli omografi IDN.

I clienti possono scegliere tra i domini comunemente presi di mira o creare un elenco personalizzato per il monitoraggio e l'analisi specializzati dei lookalike. I risultati di questa analisi approfondita sono accessibili attraverso l' interfaccia utente di segnalazione dei lookalike, che segnala anche i casi in cui il lookalike rilevato è associato ad attività sospette o di phishing. In generale, le politiche possono essere personalizzate per soddisfare le esigenze dell'ambiente specifico di un cliente e il suo livello di tolleranza al rischio. Inoltre, i dati dettagliati del dominio includono preziose annotazioni accessibili attraverso le interfacce utente e le API di B1TD Advanced, fornendo ai clienti un contesto che può accelerare le indagini sulle minacce e rendere più efficaci le risposte agli incidenti.

Queste funzionalità di rilevamento delle minacce lookalike sono solo uno dei tanti servizi offerti da BloxOne Threat Defense che consente di vedere le minacce che altre soluzioni non vedono e di bloccare gli attacchi nelle prime fasi del ciclo di vita della minaccia. Attraverso un'automazione e un'integrazione nell'ecosistema pervasive, può favorire una maggiore efficienza nelle SecOps, aumentare l'efficacia dello stack di sicurezza esistente, proteggere gli sforzi digitali e di lavoro da qualsiasi luogo e ridurre il costo totale per la sicurezza informatica.

PER ULTERIORI INFORMAZIONI

Visita infoblox.com

Seguici su LinkedIn

Seguici su Twitter

RIFERIMENTI

[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.

Infoblox unisce networking e sicurezza per offrire prestazioni e protezione senza pari. Scelti dalle aziende Fortune 100 e dagli innovatori emergenti, forniamo visibilità e controllo in tempo reale su chi e cosa si connette alla tua rete, in modo che la tua organizzazione funzioni più velocemente e blocchi le minacce prima che avvengano.

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

+1.408.986.4000
www.infoblox.com