infoblox

LOOKAL1KE-ANGRIFFE IM F0KUS

NEUE STUDIE ENTHÜLLT AKTUELLE BEDROHUNGSVEKTOREN

April 2023

LOOKALIKE-DOMAINS HABEN JEDEN IM VISIER

INHALTS-VERZEICHNIS

ZUSAMMENFASSUNG

Seit es das Internet gibt, verwenden Bedrohungsakteure ähnlich aussehende Domains, um Benutzer dazu zu verleiten, auf bösartige Websites zu klicken. Diese Domains, die so genannten Lookalike-Domains, sind ein Synonym für Phishing-Angriffe. Bei Schulungen zum Sicherheitsbewusstsein lernt man also auch, zu überprüfen, ob es sich bei einem Link um eine solche Lookalike-Domain handelt.

Trotz Sensibilisierungskampagnen und technologischen Fortschritten stellen Lookalike-Domains jedoch eine ständige Bedrohung für Verbraucher und Unternehmen dar – und die Täter passen ihre Strategien kontinuierlich an. Jeder ist ein Ziel: von Verbrauchern bis zu Regierungen, von großen Einzelhandelsmarken bis zu kleinen Restaurants, von weltweit bekannten Technologieunternehmen bis zu weniger bekannten wie unserem. In diesem Whitepaper zeigen wir anhand von Beispielen realer Domains und Kampagnen, dass wirklich „jeder ein Ziel ist“. Als mittelgroßes Unternehmen in einer Nischenbranche geraten sogar wir ins Visier.

Dieser Bericht beschreibt die aktuelle Bedrohungslandschaft anhand realer Beispiele aus verschiedenen Branchen und Benutzergruppen. Infoblox spürt seit Jahren Lookalike-Domains auf und analysiert täglich über 70 Milliarden Ereignisse im Zusammenhang mit dem Domain Name System (DNS), um neue und potenzielle Bedrohungen zu finden. Für diese Studie haben wir uns auf Ereignisse zwischen Januar 2022 und März 2023 konzentriert. Wir haben mehr als 300.000 LooKaliKe-Domains untersucht und eine Auswahl zusammengestellt, die die Herausforderungen und Risiken im Zusammenhang mit diesen Angriffen aufzeigen.

Lookälike-Domains werden oft mit breit angelegten, nicht zielgerichteten Angriffen auf Verbraucher durch E-Mail-Spam, Werbung, Social Media und SMS-Nachrichten in Verbindung gebracht. Jeden Tag werden Tausende von neuen Domains registriert, die beliebte Software, Finanzinstitute und Paketzustelldienste imitieren. Phishing-Angriffe, die darauf abzielen, Anmeldedaten von Benutzern zu stehlen oder Rechner mit Malware zu infizieren, sind so weit verbreitet und oft so schlicht, dass es sogar schon Memes dazu gibt, wie z. B. „Man kann nicht auf Phishing-Betrügereien hereinfallen, wenn man seine E-Mails nicht abruft“. Obwohl Phishing oft als komisch dargestellt wird, ist es eine ernste Angelegenheit. Die Anti-Phishing Working Group (APWG) berichtet, dass Phishing im dritten Quartal 2022 ein Rekordniveau erreicht hat.[1]

[ ] ***Alle Links in diesem Dokument wurden unschädlich gemacht, unabhängig davon, ob sie als bösartig oder legitim eingestuft wurden. Wir haben die Links unschädlich gemacht, indem wir eckige Klammern um die Punkte gesetzt haben [.]. So wird vermieden, dass sie angeklickt werden können.***

70+ MILLIARDEN

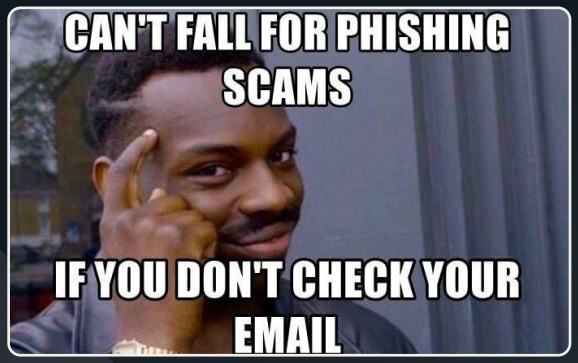
Infoblox analysiert täglich über 70 Milliarden DNS-Ereignisse, um neue Bedrohungen zu identifizieren.

ÜBER 300.000

Lookalike-Domains wurden für diesen Bericht zusammengetragen, um die Herausforderung und das Risiko dieser Angriffe zu verdeutlichen.

EIN BEISPIEL FÜR EIN PHISHING-MEME.

Ein Beispiel ist dieser Tweet aus dem Jahr 2019.[2]



Bildnachweis: Der Ursprung dieses Memes ist unbekannt.

Aber Lookalike-Domains stellen nicht nur eine Bedrohung für Verbraucher dar – sie werden auch verwendet, um sich Zugang zu Unternehmensnetzwerken zu verschaffen.

Jüngste Enthüllungen haben gezielte Angriffe aufgedeckt, bei denen böswillige Akteure Mitarbeiter dazu verleiteten, ihre MFA-Anmeldeinformationen (Multi-Faktor-Authentifizierung) bereitzustellen. In den meisten Fällen imitierten die Lookalike-Domains nicht nur das Unternehmen, sondern enthielten auch MFA-Keywords, was für die Mitarbeiter die Illusion einer sicheren Verbindung noch verstärkte. Wir haben herausgefunden, dass die Akteure es auf große und kleine Unternehmen in vielen Branchen abgesehen haben, darunter Internetanbieter, Banken und Kryptowährungen, Software und Dienstleistungen sowie Versicherungsunternehmen auf der ganzen Welt. Diese Angriffe begannen Anfang 2022 und haben im Laufe der Zeit deutlich zugenommen.

Der Einsatz von L00kalike-Domains ist profitabel, weil es sich um einen asymmetrischen Angriff handelt. Die Benutzer müssen stets wachsam sein, um ihre persönlichen Finanzen und die Informationen ihrer Arbeitgeber zu schützen. Die günstigen Preise für Domainregistrierungen und die Möglichkeit, Angriffe im großen Stil zu verbreiten, verschaffen den Akteuren einen Vorsprung. Die Angreifer haben den Vorteil der Skalierung, und auch wenn sich die Techniken zur Erkennung bösartiger Aktivitäten in den letzten Jahren verbessert haben, haben die Betroffenen Mühe, damit Schritt zu halten.

Lookalike-Phishing ist nicht nur auf dem Vormarsch, sondern die Verwendung von Lookalikes ist in einer Weise komplexer geworden, die sich am deutlichsten in DNS-Einträgen erkennen lässt. Unsere Untersuchungen haben ergeben, dass Lookalike-Domains über die traditionellen Phishing- und Typosquatting-Zwecke hinaus ausgenutzt werden. Sie werden auch auf eine Art und Weise eingesetzt, über die bisher nicht berichtet wurde: zum Beispiel als Nameserver und für die Verbreitung von Spear-Phishing-Mails. Es gibt große widerstandsfähige Netzwerke, die nur Lookalike-Domains bereitstellen und sowohl auf Verbraucher als auch auf Regierungsmitarbeiter abzielen.

Infoblox verfügt über mehrere Algorithmen zur Identifizierung von Lookalike-Domains. Wir verwenden eine Kombination aus verschiedenen Methoden, darunter die Suche nach Varianten gängiger Ziele in den Bereichen Shopping, Banken, Software und Finanzen, die Suche nach Varianten spezieller Domains und die Suche nach DNS-Infrastruktur-Akteuren, die sich auf Lookalike-Domains spezialisiert haben. Durch diesen vielseitigen Ansatz können wir ein breites Feld der Bedrohungslandschaft abdecken.

> ***WICHTIGER HINWEIS: Dieser Bericht enthält eine Reihe von Beispielen, die den Umfang und die Bandbreite von Lookalike-Domains in der Praxis veranschaulichen. Sie sind nicht dazu gedacht, erfolgreiche Angriffe oder Verstöße gegen die Vorschriften zu implizieren.***

HINTERGRUND

Wie bei allen guten Forschungsartikeln beginnen wir mit einigen Hintergrundinformationen. Dabei handelt es sich hauptsächlich um ein paar Begrifflichkeiten. Wir wissen, dass die meisten Leserinnen und Leser diesen Abschnitt überspringen, deshalb haben wir ihn kurz gehalten.

Bösartige Lookalike-Domains – also von Angreifern registrierte Domains, die einer bekannten Domain scheinbar gleichen oder sehr ähnlich sehen – sind eine bekannte, anhaltende Bedrohung in der Cyberlandschaft. Im Allgemeinen können Lookalikes sowohl offensiv als auch defensiv verwendet werden. Im offensiven Sinne werden Lookalike-Domains überall dort eingesetzt, wo man Menschen täuschen kann. Akteure nutzen Lookalike-Domains, um Geld zu stehlen, sich Zugriff auf Anmeldeinformationen zu verschaffen, persönlich identifizierbare Informationen abzugreifen, Malware zu verbreiten oder Werbeeinnahmen zu erzielen. Sie werden auch für politische Zwecke und zur Schädigung der Markenreputation eingesetzt. Kurz gesagt: Sie sind für Cyberkriminelle ein Mittel zum Zweck. Im defensiven Sinne registrieren viele Unternehmen proaktiv Domains, die ihren eigenen ähneln, um Angreifer daran zu hindern, sie zu übernehmen und zu nutzen.

Es gibt verschiedene Formen von Lookalike-Domains. Im DNS-Bereich lassen sich die folgenden Arten von Lookalike-Domains beobachten:

- **Homographen**
- **Typosquats**
- **Combosquats**
- **Soundsquats**

Sie können von der ursprünglichen Zieldomain kaum zu unterscheiden sein oder objektiv ganz anders aussehen. Ein großer Teil des Erfolgs von Lookalike-Domains als Angriffsvektor ist darauf zurückzuführen, dass Einzelpersonen damit konfrontiert werden.

Wie wir noch sehen werden, finden sich Lookalike-Domains in jedem Element eines Angriffs, von E-Mail-Absenderadressen über Phishing-URLs bis hin zu Malware Command and Control (C2). Obwohl sie normalerweise mit Adresseinträgen (A/AAAA) in Verbindung gebracht werden, haben wir auch Lookalike-Domains gefunden, die für Nameserver- (NS), Pointer- (PTR) und kanonische Namenseinträge (CNAME) verwendet werden. Sie können über E-Mails, SMS oder Textnachrichten, kompromittierte Websites, Malvertising-Netzwerke und Telefonanrufe verbreitet werden. Im folgenden Abschnitt beschreiben wir kurz die verschiedenen Formen von Lookalike-Domains und geben jeweils Beispiele dafür an.

SCHULD IST DIE SCHREIBMASCHINE

Tatsächlich lässt sich dieses moderne Problem bis in die Anfangszeit der Schreibmaschinen zurückverfolgen. Auf vielen älteren Schreibmaschinen gab es keine 0- oder 1-Tasten, da von den Schreibkräften erwartet wurde, dass sie für diese Ziffern ein großes „O“ und ein kleines „L“ verwenden.[4]

HOMOGRAPHEN (EIGENTLICH HOMOGLYPHEN)

Obwohl das Wort Homograph im Deutschen bedeutet, dass „zwei Wörter die gleiche Schreibweise, aber unterschiedliche Bedeutungen haben“, wird der Begriff Homograph in der Sicherheitsforschung seit vielen Jahren verwendet, um „zwei Domains, die visuell gleich aussehen“ zu bezeichnen.[3] Ein genauerer Begriff ist Homoglyph. Diese Domains sehen einander ähnlich und sind in manchen Fällen kaum voneinander zu unterscheiden. *Im Einklang mit der einschlägigen Literatur im Sicherheitsbereich werden wir in diesem Whitepaper den nicht korrekten Begriff Homograph verwenden.*

Diese Form der Lookalike-Domains macht sich die Tatsache zunutze, dass viele Zeichen desselben Zeichensatzes oder Alphabets einander ähnlich sehen. Zum Beispiel 0 (die Ziffer Null) und O (Großbuchstabe „o“), oder „l“ (Kleinbuchstabe „L“) und „I“ (Großbuchstabe „i“). Einige Schriftarten verstärken dieses Problem noch. Klassische Beispiele hierfür sind g0ogle.com und lnfoblox.com, in denen das „o“ in Google durch eine Null (0) und das „i“ in lnfoblox durch ein kleines „L“ ersetzt wurde.

Als sich das Internet immer weiter entwickelte und sich immer mehr Menschen, die nicht Englisch sprechen, ebenfalls im World Wide Web anmeldeten, wuchs der Bedarf an internationalisierten Domainnamen (IDNs). Ein IDN ist eine Domain, die mindestens ein Zeichen in nicht-lateinischer Schrift enthält. Die Einführung von Unicode ermöglichte die Verbreitung solcher Domains. Mit IDNs kam eine neue Form von Lookalike-Domains auf: das IDN-Homogramm. Es ist immer noch ein Homograph, aber eines, das Zeichen aus anderen Zeichensätzen oder Alphabeten verwendet, die ähnlich aussehen. Gabrilovich und Gontmakher zeigten die Fähigkeiten der IDN-Hoɱographen in ihrer 2002 veröffentlichten Arbeit „The Homograph Attack“. Die Autoren registrierten eine Lookalike-Domain der authentischen Microsoft-Domain microsoft[.]com, die die kyrillischen Buchstaben „c“ und „o“ enthielt.[5] Das Endergebnis ist eine Domain www.microsoft[.]com, die visuell nicht von der echten Microsoft-Domain zu unterscheiden ist.

Das Unicode Consortium hat ein Tool veröffentlicht, das die enorme Anzahl verwechselbarer Zeichen für eine bestimmte Zeichenfolge ausgibt.[6] Die Zeichenfolge „hi“ hat beispielsweise 684 Variationen mit Unicode-Zeichen. Für eine Zeichenfolge wie „infoblox“ steigt die Zahl auf über 2,2 Billionen Variationen an. Einige Variationen sind für eine Lookalike-Domain weniger effektiv als andere. Zum Beispiel listet das Unicode-Konsortium „۵“ (erweiterte arabisch-indische Ziffer fünf) als potenziell verwechselbares Zeichen für „o“ (lateinischer Kleinbuchstabe „O“) auf.

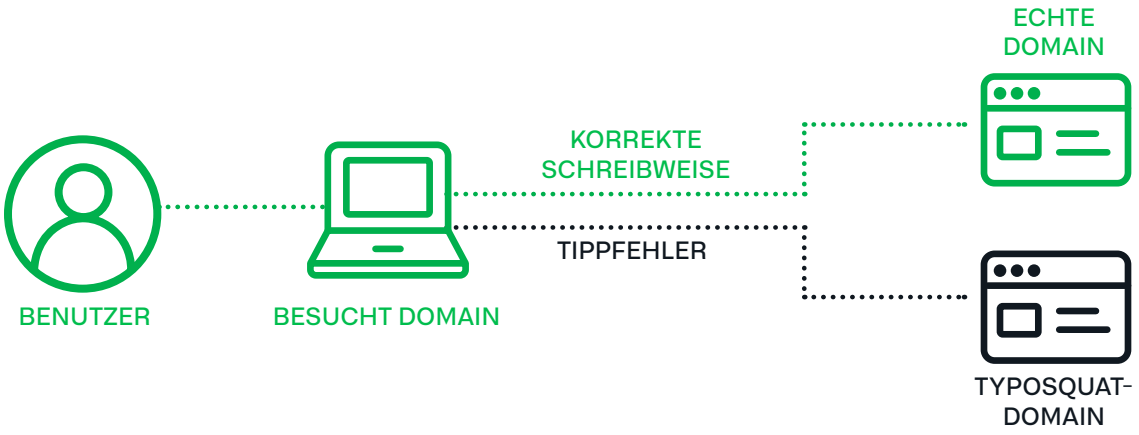
Offensichtlich ist inf۵bl۵x[.]com keine sehr effektive Lookalike-Domain. Aber können Sie in der gängigen Schriftart Arial den Unterschied zwischen der richtigen Domain {infoblox[.]com} und {infoblox[.]com} (mit einem weißrussischen oder ukrainischen kleingeschriebenen „i“ und einem armenischen kleingeschriebenen „vo“, geschrieben als „n“) erkennen, wenn sie angezeigt wird? Wir auch nicht.

TYPOSQUATS

Typosquat-Domains machen sich beliebte Domainnamen und Tippfehler zunutze, die Benutzer machen oder die durch das Tippen auf kaputten Tastaturen verursacht werden. Dieser Begriff wird in der Regel mit Domains in Verbindung gebracht, die registriert, aber ungenutzt gelassen werden, um Werbeeinnahmen zu kassieren. Einer der Autoren hat zum Beispiel kürzlich versucht, seine Miete über das Online-Portal seiner Wohnung zu bezahlen, das von appfolio[.]com gehostet wird (einem bekannten Softwareunternehmen, das SaaS-Lösungen für Hausverwaltungen und Vermieter anbietet). Er hat sich aber vertippt und beinahe appfollio[.]com besucht, eine Domain, die 2013 registriert wurde, aber derzeit nur geparkt wird.

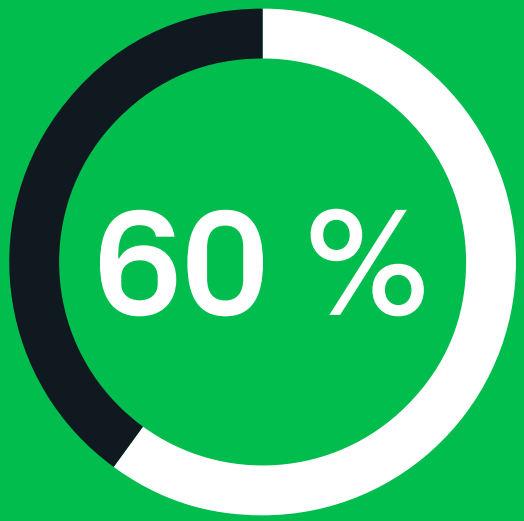
Interessanterweise scheint eine weitere offensichtliche Typosquat-Domain für Appfolio, apfolio[.]com, im Besitz von Appfolio zu sein. Klickt man darauf, wird man nämlich auf die richtige Domain weitergeleitet. Sie hat denselben Domaininhaber, dieselbe Registrierungsorganisation und denselben Registrar und wurde nur einen Monat nach der legitimen Domain appfolio[.]com registriert. Dies ist ein Beispiel für den defensiven Einsatz von Lookalike-Domains. Leider haben böse Akteure die Oberhand, weil es einfach zu viele potenzielle Lookalike-Domains gibt, die alle von Unternehmen registriert werden müssten.

Typosquats werden in erster Linie als Einnahmequelle angesehen, aber sie können auch zu einem schädlichen Zweck verwendet werden. Sie werden zwar zum Verkauf von Werbung Dritter oder zum Verkauf an den rechtmäßigen Domain-Besitzer verwendet, können aber auch für „Black Hat"-Affiliate-Marketing-Programme und als Malware-C2-Domains genutzt werden, worauf wir später noch eingehen werden. Marken und Unternehmen sind durch den Anticybersquatting Consumer Protection Act zivilrechtlich gegen Typosquatting geschützt. Aufgrund dieser Androhung rechtlicher Schritte wird Typosquatting in der Domain-Flipping-/Parking-Community als „Black Hat"-Form der Monetarisierung angesehen, und seriöse Domain-Flipper wie iGoldrush raten von Typosquatting zu Profitzwecken ab.[7]



TYPOSQUAT-BEISPIELE

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



der missbräuchlichen Combosquatting-Domains

der missbräuchlichen Combosquatting-Domains erscheinen 100 Tage nach den ersten Auflösungen auf mindestens einer öffentlichen Blockliste

COMBOSQUATTING

Combosquatting ist eine Form von Lookalike-Domains, bei der beliebte Marken- oder Firmennamen mit anderen Keywords kombiniert werden. Begriffe wie „Support“, „Help“, „Security“ und „Mail“ kommen dabei üblicherweise zum Einsatz. Nehmen wir zum Beispiel wordpresssupport[.]ru, wordpresssupport[.]store und wordpress-security[.] cloud. Diese Domains werden alle unter der gleichen, in Russland ansässigen IP-Adresse gehostet und sehen aus wie WordPress, die beliebte Software für Webinhalte. Durch die Verwendung von „Support“ und „Security“ im Domainnamen wird signalisiert, dass diese Domains für WordPress-Benutzer gedacht sind. Sie könnten dazu verwendet werden, Anmeldeinformationen abzugreifen, um WordPress-Websites zu übernehmen oder Zahlungs- und personenbezogene Daten (PII) zu erfassen.

Zusätzlich zur Generierung von Combosquat-Domains können Akteure auch Wörterbuchalgorithmen zur Generierung von Domains (Dictionary Domain Generation Algorithms, DDGAs) verwenden, um Lookalike-Domains zu erstellen. In Sekundenschnelle lassen sich damit Tausende von Domain-Kandidaten für eine Vielzahl von Marken oder Unternehmen generieren. Durch reines Glück kann der Algorithmus Kandidaten-Domains mit genau den richtigen Keywords erstellen, damit die Domain wirksam ist. Die Benutzer-Community von Steam, einer führenden Spieleplattform, ist ein häufiges Ziel für Akteure, die Combosquat-DDGAs verwenden. Einige Beispiele für Domains, die kürzlich beobachtet wurden, sind: steamcommiunity[.]com[.]ru, steamcommucnity[.]com[.]ru, steamcommunityjp[.]top und steamcommunityiq[.]top. Beachten Sie die Überschneidung zwischen Typosquatting und Combosquatting in diesen Domains.

Kitsin et al. führten 2017 eine Längsschnittstudie zum Combosquatting durch, bei der sie etwa 468 Milliarden DNS-Einträge (aus aktiven und passiven Datensätzen) analysierten. Die Ergebnisse dieser Studie waren beunruhigend:

- **Combosquat-Domains treten 100-mal häufiger auf als Typosquatting-Domains**
- **60 % der missbräuchlichen Combosquatting-Domains sind seit mehr als 1.000 Tagen aktiv**
- **20 % der missbräuchlichen Combosquatting-Domains erscheinen 100 Tage nach der ersten Auflösung auf mindestens einer öffentlichen Blockliste**
- **Die Auflösung von Combosquat-Domains ist im Vergleich zum Vorjahr gestiegen[8]**

Wir stimmen mit der Feststellung der Autoren überein, dass Combosquat-Domains weit verbreitet sind. Im Rahmen unserer Analysen haben wir mehr Combosquat-Domains gefunden als reine Typosquats oder reine HomoGraphen (IDN oder andere).

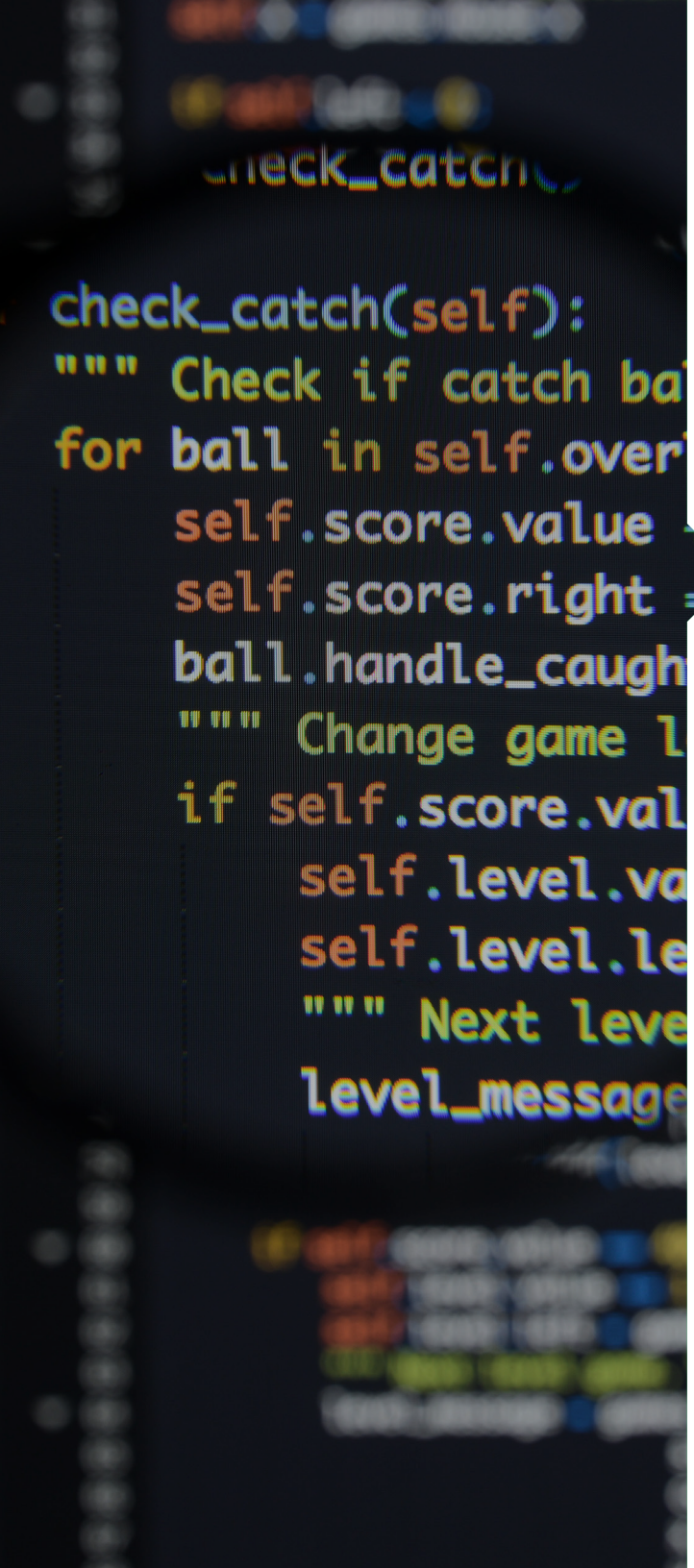
SOUNDSQUATTING

Soundsquat-Domains nutzen Homophone, also Wörter, die gleich klingen, aber anders geschrieben werden. Soundsquatting ist die jüngste Form von Lookalike-Domains und tauchte erstmals 2014 in der Literatur auf.[9] Soundsquatting hat in letzter Zeit aufgrund der Verbreitung von Smart Speakern wie Alexa, Siri und Google Voice mehr Aufmerksamkeit von Forschern erhalten.[10] Soundsquat-Domains überschneiden sich mit anderen Lookalike-Domains, da sie sowohl ähnlich klingen als auch ähnlich aussehen können. Wir haben festgestellt, dass reine Soundsquatting-Domains, d. h. solche, die nicht visuell ähnlich aussehen, aber ähnlich klingen, selten sind; im Allgemeinen können diese Domains auch durch textbasierte Vergleichstechniken gefunden werden.

Es ist wichtig zu wissen, dass Lookalike-Domains in der Praxis oft nicht so einfach zuzuordnen sind, wie wir es hier getan haben. Um die Effektivität einer Lookalikę-Domain zu maximieren, wird eine Kombination aus verschiedenen Formen verwendet. Viele der von uns beobachteten Combosquat-Domains enthalten Elemente von Typosquats und Homographen (IDN oder andere). Typosquats nutzen Elemente von Homographen, Soundsquats nutzen Elemente von Typosquats und so weiter. Das Endergebnis ist eine asymmetrische Bedrohungslandschaft, in der Verteidiger den Angreifern kaum noch hinterherkommen.

SOUND DER ANGRIFF

Die Verbreitung von Soundsquatting hat mit dem Aufkommen von sprachaktivierten Technologien wie Alexa, Siri und Google Voice zugenommen.



ANDERE FORMEN VON LOOKALIKE-DOMAINS

Auch wenn der Schwerpunkt dieses Whitepapers auf Lookalike-Domains und ihrer Rolle in der aktuellen Bedrohungslandschaft liegt, gibt es noch andere Arten von Lookalikes, die gefährdeten Benutzern Schaden zufügen können. Ein bemerkenswertes Beispiel hierfür wurde kürzlich in Python-PyPi-Paketen gefunden.

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

Paketmanager für beliebte Programmiersprachen wie Python haben die gleichen Schwachstellen wie Domains. Jeder kann ein Paket mit einem beliebigen Namen hochladen (solange dieser Name nicht bereits vergeben ist), das Code enthält, der Sicherheitsrisiken enthalten kann oder auch nicht. Im Jahr 2016 nutzte der Sicherheitsforscher Nikolai Tschacher Typosquatting auf diese Weise, um mehr als 17.000 verschiedene Hosts zur Ausführung von beliebigem Code zu zwingen.[11] Im Jahr 2021 griff der Sicherheitsforscher Alex Birsan Tschachers Idee auf und entwickelte sie weiter, indem er den Begriff „Abhängigkeitsverwirrung“ prägte.[12]

Birsan fand die privaten, internen Paketnamen von großen Unternehmen über verschiedene offene Quellen. Dazu gehörte die Untersuchung des Quellcodes auf Websites, die Suche nach Paketen auf GitHub oder sogar die Suche nach Paketnamen in öffentlichen Foren. Dann lud er Pakete mit demselben Namen wie die privaten, internen Pakete in öffentliche Paketmanager hoch. Schließlich nutzte Birsan automatisierte CI/CD-Pipelines, wodurch die öffentlichen Pakete mit den privaten, internen Paketen „verwechselt“ wurden. Anstatt die privaten Pakete zu importieren und zu installieren, fanden und importierten die automatisierten Pipelines stattdessen die öffentlichen Pakete von Birsan. Birsan nutzte dann die DNS-Exfiltration, um sich benachrichtigen zu lassen, dass sein willkürlicher Code und nicht das beabsichtigte private Paket ausgeführt worden war. Die Lookalike-Domains von Birsan ermöglichten es ihm, in 35 Unternehmen einzudringen, manchmal innerhalb weniger Stunden nach dem Hochladen seiner Pakete.

Unabhängig von der Art der Lookalike-Domain oder dem Bereich, in dem eine Lookalike-Domain verwendet wird, stellen Lookalikes eine ständige Bedrohung dar. Ein Teil der Herausforderung bei der Untersuchung von Lookalike-Domains besteht darin, dass sie undefiniert sind – es gibt mehr Möglichkeiten, als berechnet werden können, und alles ist ein Ziel. In den folgenden Abschnitten zeigen wir konkrete Beispiele für diese verschiedenen Formen von Lookalike-Domains in der Praxis, einschließlich der Ziele, der Verbreitungsmethoden, der Infrastruktur, der Gründe für ihre Wirksamkeit, der Herausforderungen und der Lösungen von Infoblox für dieses Problem.

JEDER IST EIN ZIEL

Wir glauben, dass Sie in unseren Beispielen mindestens ein überraschendes Ziel finden werden.

Eine der wichtigsten Erkenntnisse unserer Untersuchung von Lookalike-Domains im DNS war, dass jeder ein Ziel ist: Wir fanden Lookalikes für alle erwarteten Ziele, aber auch für kleinere Unternehmen und Services. Diese Domains werden von bösartigen Akteuren genutzt, um Einzelpersonen bei der Arbeit und zu Hause anzugreifen.

Wie Akamai kürzlich feststellte, werden die meisten Lookalike-Kampagnen erst veröffentlicht, wenn ein großes Ziel betroffen ist.[13] Unser Ziel ist es, Licht ins Dunkel zu bringen, und neben den „typischen" Zielen auch die zu wenig beachteten und übersehenen Ziele zu beleuchten. Um dies zu verdeutlichen, werden hier einige ausgewählte Beispiele angeführt. Wir werden aber auch die Auswirkungen auf verschiedene Branchen und die Verwendung verschiedener Methoden später ausführlicher behandeln.

SIE HABEN UNS IM VISIER!

Infoblox ist ein mittelgroßes Unternehmen mit weniger als 2.000 Beschäftigten weltweit.

Wir haben zwar einen großen Anteil am Markt für DNS, Dynamic Host Configuration Protocol (DHCP) und IP Address Management (IPAM) – zusammenfassend als DDI bekannt –, aber diese Branche ist ziemlich spezifisch, und Infoblox ist nicht gerade ein bekannter Name. Es überrascht fast schon, dass böswillige Akteure überhaupt von uns wissen, geschweige denn, dass sie uns aktiv mit Lookalike-Domains ins Visier nehmen. Dennoch haben wir viele Domains gefunden, die sowohl unsere Mitarbeiter als auch unsere Kunden täuschen sollen. Im vergangenen Jahr wurden Lookalike-Domains für interne Services, einschließlich unseres Leistungsportals, sowie für unsere Produktnamen registriert.

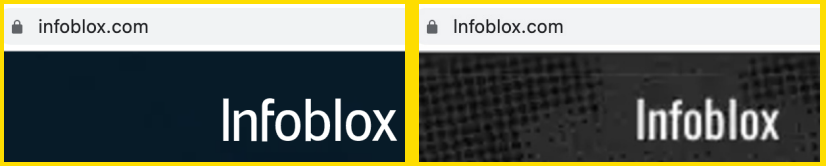


Abbildung2. Ein Vergleich der Logos der offiziellen infoblox[.]com Website (L) und der Lookalike-Domain Infoblox[.]com (R)

Zu den registrierten Domains, die nicht im Besitz von Infoblox sind, gehören:

Homograph **Infoblox[.]com**	Die Verwendung eines kleingeschriebenen „L“, um ein großes „i“ zu imitieren. Die Domain wurde im Juli 2022 registriert, und obwohl sie zum Verkauf angeboten wird, zeigt die Website in der oberen linken Ecke ein Rendering, das von dem auf unserer Unternehmenswebsite kaum zu unterscheiden ist. *Schauen Sie sich zum Vergleich Abbildung 2 an.*
Typosquat **infobloxbenifits[.]com**	Diese Domain wurde im April 2022 in China registriert und enthält einen kleinen Tippfehler unseres Portals für Mitarbeiterleistungen. Diese Domain ist derzeit bei Bodis geparkt.
TLD Squat **infoblox[.]info**	Eine andere Top Level Domain (kurz: TLD) wurde im August 2022 über den stark missbräuchlich genutzten Registrar Sav[.]com registriert. Sie ist auf dan[.]com geparkt, wo Nutzer Domains verkaufen können.
Combosquat **infobloxgrid[.]com**	Eine Lookalike-Domain unseres lokalen Flaggschiffprodukts, das von Tausenden von Kunden auf der ganzen Welt genutzt wird. Unsere patentierte Grid™ technology ermöglicht es Netzwerkadministratoren, verschiedene Netzwerkanwendungen in einem einzigen System zu kombinieren. Diese Domain ist ebenfalls auf dan[.]com verfügbar und wurde im April 2022 registriert.
Combosquat **infoblox-updater[.]com**	Ein Beispiel für die Technik, gängige Software-Begriffe innerhalb der Domain wie „Update“ oder „Support“ zu verwenden. In diesem Fall könnte ein Kunde dazu verleitet werden, sich mit einem falschen System zu verbinden, weil er denkt, dass es sich um System-Updates von Infoblox handelt. Namen oder Produkte von Technologieunternehmen werden häufig für diese Art von Combosquat-Domain genutzt, die als Phishing-Domain oder als Malware C2 verwendet werden kann. Weitere Beispiele sind dev[.]gitlabs[.]me und jira[.] atlas-sian[.]net, die beide von dem APT (Advanced Persistent Threat)-Akteur Iron Tiger in seiner SysUpdate-Malware verwendet werden.[14]

Aber nicht nur kleine Technologieunternehmen wie unser eigenes geraten ins Visier. Wir haben auch eine Vielzahl von Lookalike-Domains gefunden, bei denen es sich um betrügerische Varianten von Restaurants, Anwaltskanzleien und anderen kleinen Unternehmen handelt.

Außerdem kann ein einzelner Akteur sowohl bekannte Marken als auch kleine Unternehmen als Köder verwenden. Ein Akteur, den Infoblox seit einiger Zeit verfolgt, hat Lookalike-Domains für das New Yorker Restaurant Cotenna erstellt und dessen Website kopiert, vermutlich um Besucher dazu zu verleiten, auf der Seite Online-Reservierungen mit ihren Kreditkarten vorzunehmen.[15] Die Website cotenna[.]nyc wurde im April 2022 registriert und ist eine Lookalike-Domain der echten Restaurant-Website cotenna[.]com. Derselbe Akteur hat Lookalike-Domains, die auf große Social-Media-Unternehmen wie Twitter abzielen.

In den folgenden Abschnitten gehen wir näher auf die Branchen ein, die heutzutage am häufigsten ins Visier geraten, sowie auf einige der vielen Möglichkeiten, wie Domains für einen erfolgreichen Angriff genutzt werden können. Da jeder ein Ziel ist, werden wir die Bereiche hervorheben, in denen wir die meisten bösartigen Aktivitäten beobachtet haben, basierend auf einer Überprüfung von 300.000 Lookalike-Domains.

LOOKALIKE-DOMAINS HABEN JEDEN IM VISIER

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

SIE HABEN MITARBEITER IM VISIER

Bis vor kurzem waren viele Unternehmen der Meinung, dass die Verwendung von Multi-Faktor-Authentifizierung (MFA) ihre internen Netzwerke vor Phishing-Angriffen schützt.

Doch Anfang 2023 wurde bekannt, dass die Mitarbeiter von Coinbase Ziel von Spear-Phishing-Angriffen waren, die lookalike-Domains zum internen MFA-Login des Unternehmens verwendeten. Auf diese Enthüllung folgten schnell bestätigende Berichte von anderen Unternehmen, die von ähnlichen Angriffen betroffen waren. Aus den Berichten der Opfer wissen wir, dass böswillige Akteure den Mitarbeitern SMS-Nachrichten und E-Mails geschickt hatten, in denen sie aufgefordert wurden, sich in interne Systeme einzuloggen. In einigen Fällen waren auch Telefongespräche im Spiel, bei denen der Angreifer einen Domainnamen angab, den der Mitarbeiter in seinem Webbrowser aufrufen sollte. Die Angreifer nutzten Adversary-in-the-Middle (AitM)-Techniken, um den Mitarbeitern vorzugaukeln, sie würden mit dem echten Netzwerk des Unternehmens interagieren. Die Mitarbeiter wurden zur Eingabe eines MFA-Codes aufgefordert, den der Angreifer dann abfing und nutzte, um sich Zugang zu internen Systemen zu verschaffen.

Microsoft hatte im Juli 2022 davor gewarnt, dass mehr als 10.000 Unternehmen Ziel von AitM-Angriffen waren, die zum Diebstahl von MFA-Anmeldeinformationen von Benutzern in Echtzeit entwickelt worden waren.[16] Diese Angriffe bezogen sich speziell auf die Verwendung der Outlook 365-Authentifizierung, aber Microsoft berichtete im Februar 2023 außerdem, dass ein Phishing-Kit, das MFA-Angriffe ermöglichte, im Juli 2022 zum Verkauf stand und vielfach verwendet wurde.[17] Andere Unternehmen, darunter Twilio, hatten im Sommer 2022 über ähnliche Angriffe berichtet, aber das Ausmaß der Angriffe wurde erst durch die Enthüllungen von Coinbase bekannt.[18]

Zur Untersuchung dieses Vorfalls haben wir eine retrospektive Analyse von Lookalike-Domains durchgeführt, die MFA durch die Verwendung von Keywords wie „MFA“, „Okta“ und „2FA“ imitierten. Unsere Untersuchungen ergaben eine breite Palette von Zielen und einen deutlichen Anstieg der Aktivitäten ab Juli 2022, obwohl eine beträchtliche Anzahl von Lookalike-Domains bereits zu Beginn des Jahres für diese Angriffe genutzt wurde. Über 1.600 Domains enthielten eine Kombination aus Unternehmens- und MFA-Lookalike-Merkmalen. Die Ziele reichten von den gemeldeten großen Unternehmen wie Coinbase, Reddit und Twilio bis hin zu großen Banken, Software-Unternehmen, Internet-Service-Anbietern, staatlichen Stellen und Spieleplattformen weltweit. Weitere Ziele waren kleinere Technologieunternehmen, Lebensmittelgeschäfte und Einzelhändler, über die jedoch nicht berichtet wurde.

10.000+
UNTERNEHMEN

Im Juli 2022 warnte Microsoft, dass über 10.000 Unternehmen Ziel von AitM-Angriffen waren, die darauf abzielten, MFA-Anmeldedaten von Benutzern in Echtzeit zu stehlen.

1.600+

Unsere Recherche ergab, dass über 1.600 Domains eine Kombination aus Unternehmens- und MFA-Lookalike-Merkmalen enthielten.

Ein Beispiel für weniger bekannte Ziele sind mehrere Lookalike-Domains der MFA, die den Western Electricity Coordinating Council (WECC) imitierten.
Der WECC sorgt für die Zuverlässigkeit des Stromnetzes in einem großen Teil des Westens der Vereinigten Staaten. Zu den Lookalike-Domains gehörten wecc-okta[.]org, wecc-oktc[.]org und wecc-okta[.]com. Alle wurden im Februar 2023 registriert und verwenden dieselbe IP-Adresse.

Ein weiteres überraschendes Beispiel ist die Feldman Auto Group, zu der mehrere Autohäuser in den Vereinigten Staaten gehören.
Auch wenn das Unternehmen zu Werbezwecken mit dem US-amerikanischen Schauspieler Mark Wahlberg zusammenarbeitet, ist es ansonsten ein eher moderates Unternehmen mit 18 Standorten im Mittleren Westen.[19] Eine MFA Lookalike-Domain zu dieser Domain, feldmanauto-okta[.]com, wurde Ende Januar 2023 registriert.

Bei einigen Lookalike-Domains für MFA ist nicht klar ersichtlich, auf welche Unternehmen sie abzielen.
Die Domain frb-okta[.]com zeigt eine Anmeldeaufforderung mit einem unscheinbaren FRBOkta-Logo, bei dem es sich um die Federal Reserve Bank, die First Reserve Bank oder eine Lookalike-Domain wie die des polnischen Bekleidungsunternehmens Farbokta handeln könnte.[20] In vielen Fällen können wir nicht sicher sein, was das Ziel war, und das Phishing-Paket war möglicherweise nur für kurze Zeit aktiv. *Wir haben in Abbildung 3 einen Screenshot des Anmeldebildschirms eingefügt, damit Sie selbst mitraten können.*

Diese AitM-Angriffe richteten sich im Jahr 2022 auch gegen Verbraucher, insbesondere gegen Gamer, die MFA zum Schutz ihrer In-Game-Käufe verwenden.
In einem den Autoren bekannten Fall wurde das Opfer über einen Twitch-Livestream eines beliebten Online-Spiels auf eine Website gelockt. Nachdem das Opfer seine MFA-Zugangsdaten eingegeben hatte, kam es zu einem kurzen Denial-of-Service (DoS)-Angriff auf sein Heimnetzwerk, der zu einem mehrminütigen Internet-Ausfall führte. Als der Benutzer wieder Zugang zu seinem Gaming-Konto hatte, waren alle seine Einkäufe gestohlen worden. *Man könnte meinen, dass Gamer Teenager sind, die im Keller ihrer Eltern leben, aber die Menge an Geld, die für In-App-Käufe ausgegeben wird, macht Spiele und ihre Gamer, von Roblox bis Counter-Strike, zu einer lukrativen Zielscheibe.*

MFA-LOOKALIKE FRBOKTA.COM

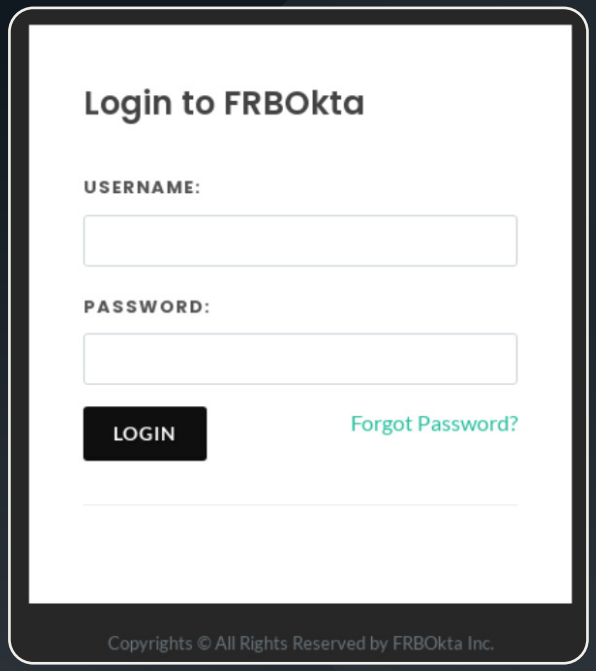


Abbildung 3. Die Website unter frb-okta[.]com zeigt eine Anmeldeseite ohne Skript mit einem Verweis auf FRBOkta. Bildnachweis: URLScan.[21]

TURKISH MINISTRY LOOKALIKE PAGE

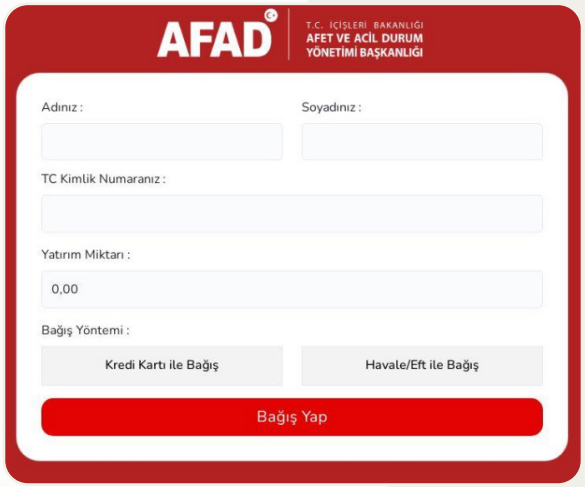


Figure 4. AFAD lookalike afadestek[.]net
Image credit: DomainTools.

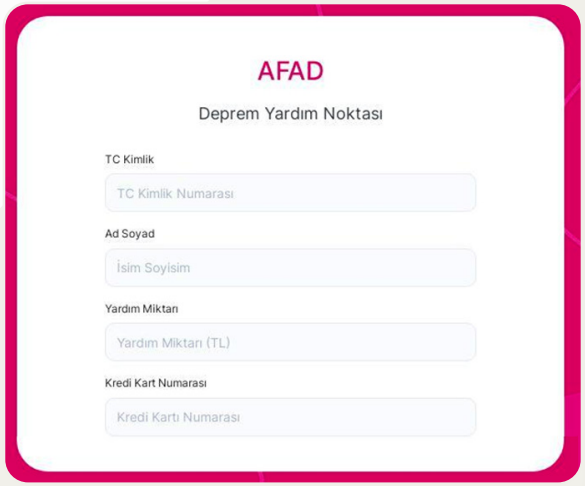


Figure 5. AFAD lookalike domain afadbagislari[.]net
Image credit: DomainTools.

SIE HABEN WELTVERBESSERER IM VISIER

Scammer, die Geld stehlen wollen, sind oft als „Ersthelfer“ zur Stelle, wenn es darum geht, Weltereignisse und Katastrophen für ihre unrechtmäßige Bereicherung zu nutzen.

Infoblox hat festgestellt, dass Scammer jedes Ereignis in den Nachrichten schnell ausnutzen, z. B. Gesundheitskrisen wie COVID-19 oder die Invasion Russlands in der Ukraine. Leider begann das Jahr 2023 mit dem Erdbeben in der Türkei und in Syrien Anfang Februar mit einer humanitären Krise.[22] Nach dem ersten Erdbeben am 6. Februar versuchten mehrere betrügerische Domains, Websites der Behörde für Katastrophen- und Notfallmanagement des türkischen Innenministeriums (AFAD) zu imitieren. Diese Domains nutzten „AFAD“ im vollqualifizierten Domainnamen und versuchten, wie die legitime Domain afad[.]gov[.]tr auszusehen. Bei den folgenden Beispielen handelt es sich um neu registrierte Domains, die zwar einen langen vollqualifizierten Domainnamen (Fully Qualified Domain Name, FQDN) haben, aber alle mit „AFAD“ beginnen.

Die Verwendung längerer FQDNs bietet Betrügern mehr Permutationen der legitimen Domain, die sie für mehrere AFAD-Kampagnen verwenden können:

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

Zusätzlich zum Combosquatting verwenden einige dieser Websites das legitime AFAD-Logo, um Besucher dazu zu bringen, auf diesen Websites zu spenden. Die betrügerische Website afadestek[.]net wurde beispielsweise am 7. Februar registriert und zeigte ein ähnliches Webdesign wie die echte türkische AFAD-Website, wie in *Abbildung 4* dargestellt. Laut der maschinellen Übersetzung scheint die Seite Spenden per Kreditkarte oder Überweisung zu sammeln und auch personenbezogene Daten wie Vor- und Nachnamen und nationale Identitätsnummern zu erfassen.

Andere betrügerische Domains haben sich nicht einmal die Mühe gemacht, das offizielle AFAD-Logo zu verwenden, und wurden schnell zusammengeschustert, um so viel Geld wie möglich von den Spendern abzugreifen. Zwei Beispiele sind afadbagislari[.]net und afadyardimyap[.]net, die beide unter der gleichen IP-Adresse gehostet werden. Dedizierte Infrastrukturen für Lookalike-Domains sind weit verbreitet und werden später noch ausführlicher behandelt. Beide Websites weisen das gleiche Layout und die gleichen Inhalte auf, wie in *Abbildung 5* dargestellt, und bitten um Spenden für die Erdbebenhilfe per Kreditkartenzahlung.

SIE HABEN KRYPTO IM VISIER

Neben Scammern, die auf das schnelle Geld aus sind, werden Lookalike-Domains häufig zum Diebstahl von Anmeldedaten verwendet.

Eine Lookalike-Domain ist wahrscheinlich das, woran die meisten Laien denken, wenn sie an eine typische „Phishing"-Website denken, die versucht, Zugriff auf die Anmeldedaten von Benutzern zu erhalten. Mit der zunehmenden Beliebtheit von Kryptowährungen haben es Angreifer auf diese Finanzdienste abgesehen, darunter Marktplätze, Wallets und Handelsplattformen. Wir haben eine Reihe von sehr überzeugenden Lookalike-Domains für die beliebte US-Handelsplattform Coinbase gefunden. Eine solche Website ist in *Abbildung 6* dargestellt.[23]

Die Domains in der folgenden Tabelle wurden beispielsweise im Januar 2023 registriert:

Tabelle 1. Beispiele für Lookalike-Domains der Handelsplattform für Kryptowährungen 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

Mit der zunehmenden Verbreitung von NFTs (Non-Fungible Tokens) – deren Handelsvolumen im Februar 2023 mehr als 2 Mrd. Dollar erreichte – haben die Akteure ihre Bemühungen, Geld von Anlegern zu stehlen, schnell auf andere Bereiche als traditionelle Kryptowährungen ausgeweitet.[24] So wurde beispielsweise der Blur-Marktplatz im Oktober 2022 eröffnet und der Blur-Token einige Monate später eingeführt, was zu einer Rekordinvestition in NFTs seit Mai 2022 führte.[25] Schon kurz nach der Produkteinführung konnten wir Lookalike-Domains von Blur beobachten, und mit der zunehmenden Popularität der Plattform stieg die Zahl der Lookalikes erheblich an.

COINBASE-LOOKALIKE

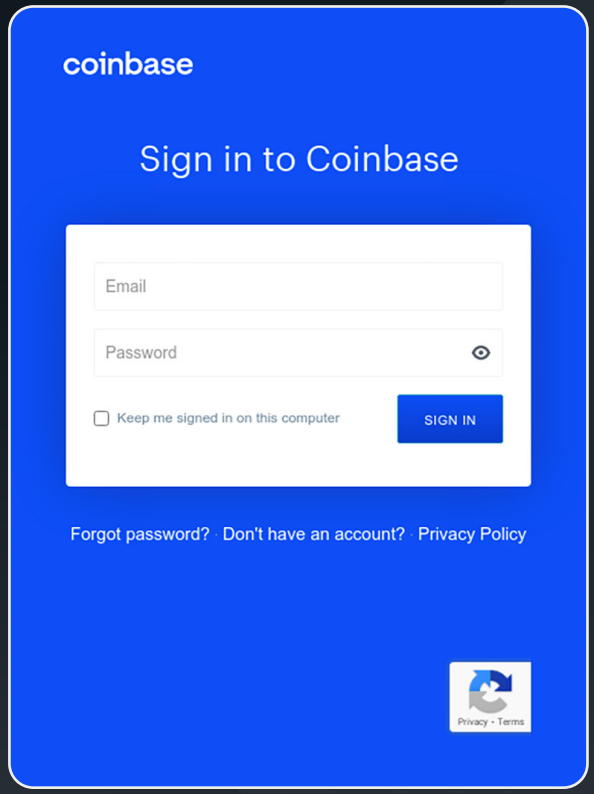


Abbildung 6. Coinbase-Lookalike click-coinbase[.]com
Bildnachweis: DomainTools.

LOOKALIKE VON BLUR NFT

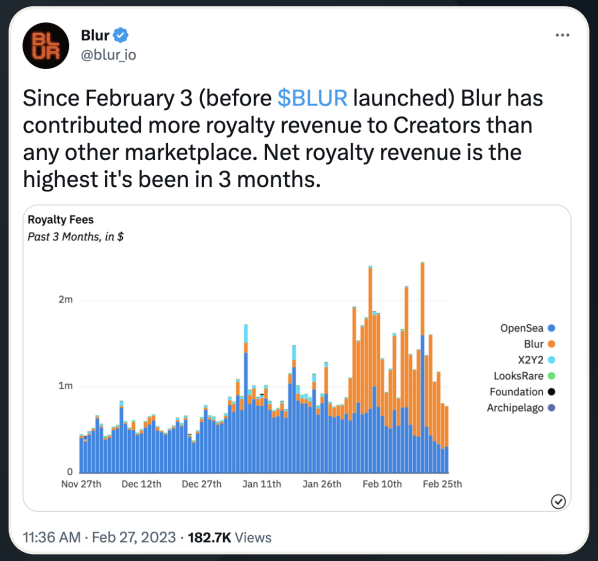


Abbildung 7. Der Blur NFT-Marktplatz ist einer der wichtigsten Wachstumstreiber für das 2-Milliarden-Dollar-Volumen im NFT-Handel im Februar 2023.[26] Bildnachweis: Infoblox

Im Vorfeld der Veröffentlichung des Blur-Tokens am 14. Februar 2023 hat sich die Zahl der Lookalike-Domains von Blur verfünffacht bis versechsfacht. Auch wenn die Zahl im März 2023 etwas zurückging, zeigt dieses Muster die Bereitschaft der Akteure, mit den Trends in der Kryptowelt Schritt zu halten, um schnelles Geld zu erbeuten.

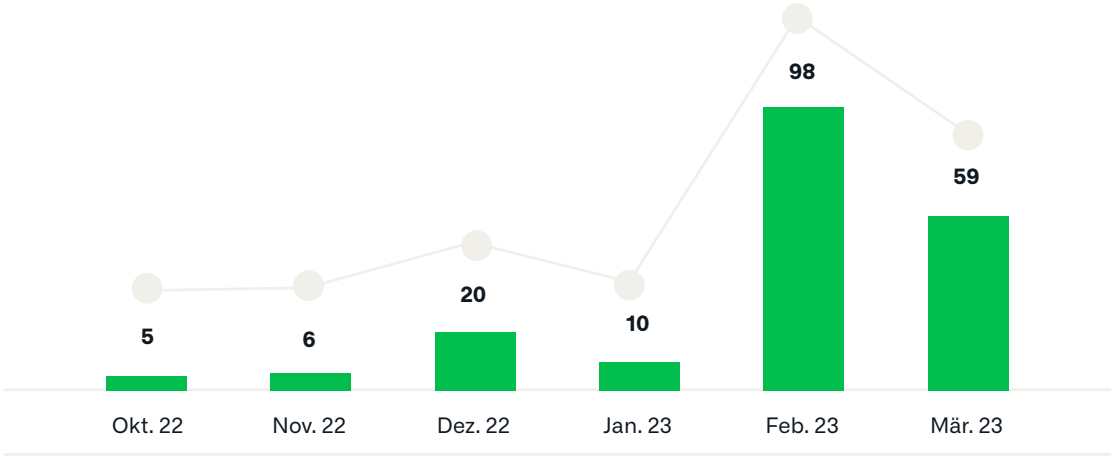


Abbildung 8. Drastischer Anstieg von Lookalike-Domains im Zusammenhang mit Blur seit der Ankündigung des Marktplatzes im Oktober 2022.

Infoblox verfolgt mehrere Akteure, die sich auf Lookalike-Domains für Kryptowährungen spezialisiert haben. Diese Akteure haben es auf alle wichtigen Unternehmen auf dem Markt abgesehen, darunter Blur und sein Konkurrent Yuga Labs, der Eigentümer von ApeCoin und der beliebten NFT Bored Ape Collection. In der folgenden Tabelle finden Sie eine kleine Auswahl dieser Domains. Zu den von diesen Akteuren verwendeten Techniken gehören einfache Änderungen der Top-Level-Domain (TLD), das Hinzufügen eines einzigen Buchstabens und Unicode-Domainnamen, deren Erkennung besonders schwierig sein kann. Beachten Sie, dass in der Tabelle unten ein Akzent über dem „i“ in apecoíns[.]com steht. Im DNS sieht diese Domain aus wie xn--apecons-cza[.]com, was etwas schwierig als Lookalike-Domain zu erkennen ist, aber in einem Webbrowser wäre sie praktisch nicht vom Original zu unterscheiden.

Tabelle 2. Beispiele für Lookalike-Domains des Blur-Token und von Yuga Labs

Lookalike-Domains von Blur [blur.io]	**Lookalike-Domains von 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

Es gibt auch weniger traditionelle Lookalike-Domains für Kryptowährungen, die YouTube als Vektor nutzen, um Ziele auf ihre Domains zu locken.

Diese Methoden beginnen damit, dass Bedrohungsakteure beliebte YouTube-Creators mit gefälschten Sponsoring-Angeboten kontaktieren, die scheinbar mit legitimen Produkten in Verbindung stehen.[27]
In den E-Mails wird der Creator aufgefordert, eine Datei herunterzuladen und zu öffnen, die angeblich mit dem Sponsoring-Angebot in Verbindung steht, z. B. eine Kopie der beworbenen Software oder eine PDF-Datei mit einem Sponsoring-Vertrag.[28] In Wirklichkeit handelt es sich bei diesen Dateien um Malware-Payloads, die, wenn sie geöffnet werden, Sitzungscookies aus dem Browser des Opfers stehlen. Die gestohlenen Cookies ermöglichen es dem Angreifer, sich Zugang zum YouTube-Konto des Opfers zu verschaffen, selbst wenn die Multi-Faktor-Authentifizierung aktiviert ist

Sobald der Angreifer Zugriff auf das YouTube-Konto des Creators hat, versucht er die Tatsache zu verschleiern, dass der Kanal gehackt wurde, indem er den Namen und das Profilfoto so ändert, dass sie zum Thema des Angriffs passen. Oft hat es etwas mit Elon Musk oder einem seiner Unternehmen zu tun.[29]
Manchmal löscht oder versteckt der Angreifer auch die vorhandenen Videos des Kanals, um seine Spuren zu verwischen. Der Angreifer beginnt dann mit dem Streaming einer bearbeiteten Version eines Videos, das mit Kryptowährungen zu tun hat, wie z. B. die Rede von Elon Musk bei Ark Invest, um die bestehenden Abonnenten des Kanals anzulocken.

Diese bearbeiteten Videos enthalten ein Text-Overlay, das die Nutzer auf die |ooKa|ike-Domain des Angreifers verweist, die mit der Kryptowährung zu tun hat, und ein Link zu dieser Domain ist auch in der Beschreibung des Streams zu finden.
Bei den Domains selbst handelt es sich um die üblichen „Verdoppeln Sie Ihr Geld“-Scams, bei denen die Opfer aufgefordert werden, einen bestimmten Betrag an Kryptowährung an eine bestimmte Wallet-Adresse zu senden, mit dem Versprechen, dass sie im Gegenzug den doppelten Betrag zurückerhalten. Bei diesen Angriffen besteht der Zweck der Lookalike-Domain darin, die Glaubwürdigkeit des Angebots zu erhöhen, indem das Thema mit dem bearbeiteten Video und dem umbenannten YouTube-Kanal übereinstimmt.

TESLA-LOOKALIKE

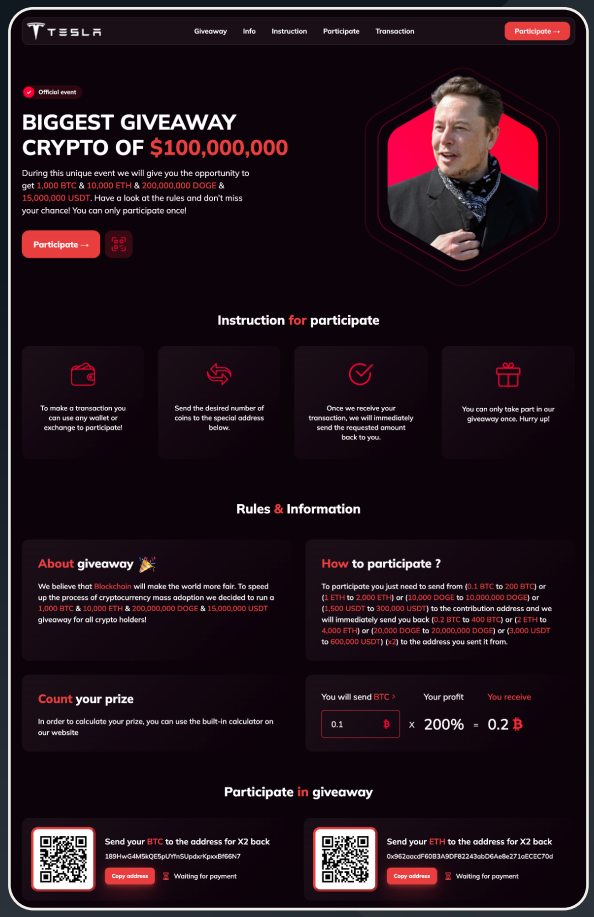


Abbildung 9. Eine Lookalike-Domain von Tesla mit Bezug zu Kryptowährungen, tesla-online[.]net, die Nutzer dazu auffordert, Kryptowährungen an bestimmte Adressen zu senden, um dafür doppelt so viel zurückzuerhalten. Bildnachweis: Infoblox.

SIE HABEN SOCIAL-MEDIA- UND MOBILGERÄTENUTZER IM VISIER

Social Media-Plattformen wie Instagram und Twitter sind neben großen Marken wie Apple ebenfalls beliebte Ziele für Phishing-Lookalikes.

Jede beliebte Marke und jeder beliebte Service ist ständig Ziel dieser Angriffe, aber wir werden nur ein paar Beispiele dieser drei Marken zur Veranschaulichung der aktuellen Bedrohung verwenden. Das Sammeln von Zugangsdaten ist nichts Neues. Bevor es Social-Media- und universelle ID-Plattformen wie Apple ID gab, versuchten die Angreifer, sich Zugang zu Ihrem E-Mail-Konto zu verschaffen. Da jedoch Social-Media- und universelle ID-Plattformen heute so eng mit unserem Leben verwoben sind, stellen diese Lookalike-Domains eine ständige Bedrohung dar.

Bedrohungsakteure haben es auf die Social-Media-Konten von jeder Person abgesehen, nicht nur auf die Accounts von Influencern und Prominenten. Es gibt viele Lookalike-Domains für Instagram, einige sind Combosquats, andere Homographen. Oft tauchen solche Domains in Clustern von gleichzeitig registrierten Domains auf, was darauf hindeutet, dass sie Teil einer koordinierten Kampagne sind, die mit Hilfe einer DDGA erstellt wurde. Die folgenden Beispiele sind alle Teil eines Instagram-Sets, das die Marke mit Wörtern wie „Help“ und „Feedback“ kombiniert.

Tabelle 3. Beispiele für Lookalike-Domains, die den Instagram-Support imitieren.

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

Auf diesen Domains wird behauptet, der Nutzer habe gegen die Urheberrechtsbestimmungen von Instagram verstoßen. Er wird dann dazu aufgefordert, seinen Benutzernamen einzugeben, um die Behauptung anzufechten; *sehen Sie sich dazu die Abbildungen 10 und 11 an.*

INSTAGRAM LOOKALIKE

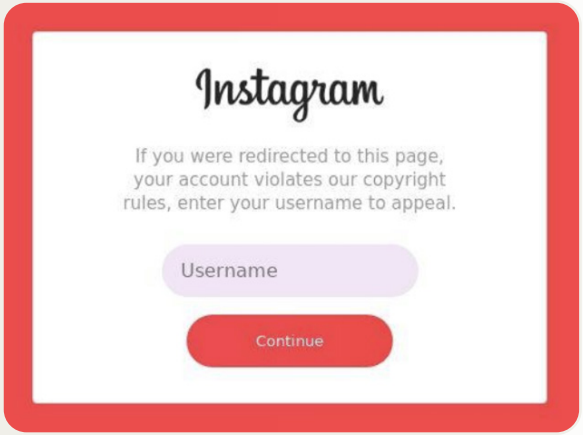


Abbildung 10. Die Instagram Lookalike-Domain help-Instagram-notice[.]com zeigt eine Urheberrechtsverletzung mit.[30]

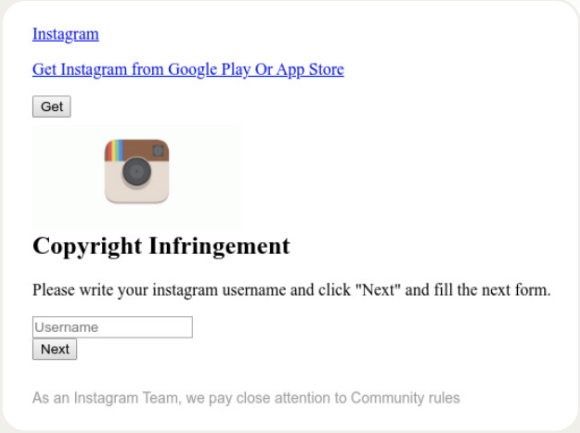


Abbildung 11. Die Lookalike-Domain help-instagram-about[.] com zeigt eine weitere Urheberrechtsverletzung mit einer Handlungsaufforderung.
Bildnachweis: URLScan.[31]

TWITTER-LOOKALIKE

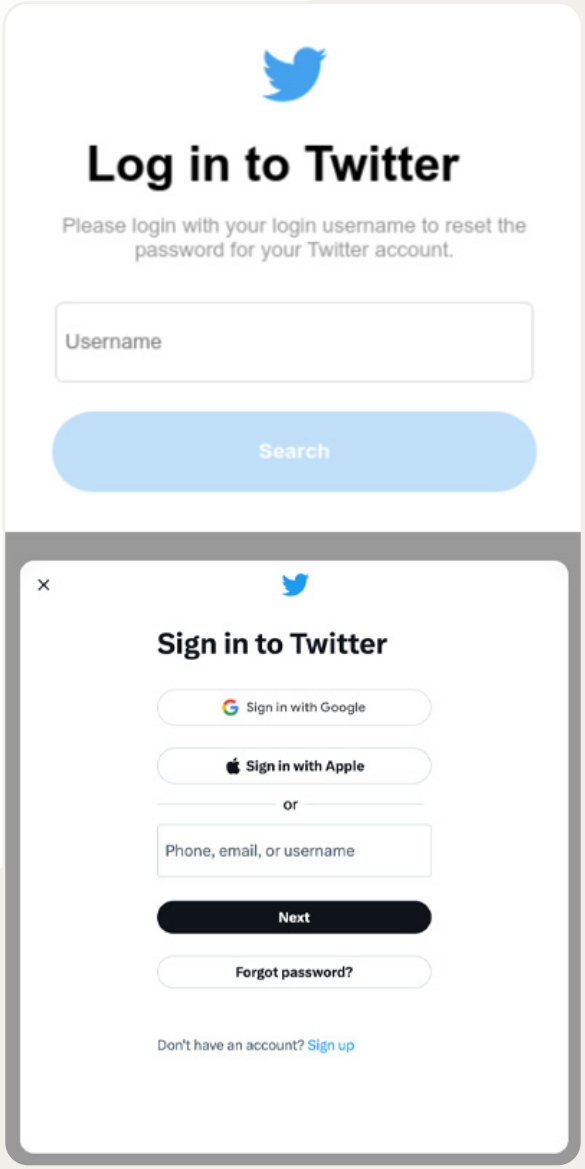


Abbildung 12. Überzeugendes Portal zum Zurücksetzen von Passwörtern auf einer Lookalike-Domain von Twitter: help-twitter-centre[.]net. Das Phishing-Bild ist oben, das legitime Bild unten. Bildnachweis: DomainTools.[32]

Andere Lookalike-Domains von Instagram zielen auf das begehrte „blaue Häkchen" ab (Instagrams Methode zur Verifizierung als öffentliche Person), indem sie ein kleines „L" anstelle eines großen „i" verwenden.
Ironischerweise hat Instagram das blaue Häkchen für bekannte Persönlichkeiten oder Unternehmen eingeführt, um Nachahmer zu bekämpfen. *So verrückt es auch klingt: Es ist durchaus denkbar, dass bösartige Akteure Lookalikes verwenden, um Anti-Lookalike-Lösungen ins Visier zu nehmen.*

Einige Beispiele sind:

Tabelle 4. Beispiele für Lookalike-Domains zur Verifizierung bei Instagram.	
Instagram-blueticket-form[.]ml	Instagram-contactbluebadge[.]ga
Instagram-verification-badges-service[.]com	Instagrambluetickverifcation[.]cf
Instagramverifybadge-contact[.]cf	Instagram-badgecentre[.]gq

Beim Aufspüren von Lookalike-Domains von Instagram haben wir festgestellt, dass die Akteure bei Social-Media-Plattformen nicht alles auf eine Karte setzen.

Neben den Lookalike-Domains für Instagram, die Meldungen zu einem Verstoß gegen das Urheberrecht enthalten, wurden auch Looka1ike-Domains für Twitter gehostet. Bei diesen Twitter-Lookalikes handelte es sich um Combosquat-Domains, die es auf die Anmeldedaten der Benutzer abgesehen haben. Die Landing Pages sehen aus wie ein legitimes Portal zum Zurücksetzen von Passwörtern; *siehe Abbildung 12.*

Zusätzlich zu den Lookalike-Domains für Social-Media-Plattformen fanden wir bei unseren Recherchen häufig Lookalike-Domains für iCloud, den Cloud-Service von Apple, der einen Cloud-Speicher bereitstellt und die Synchronisierung zwischen Apple-Geräten ermöglicht. Diese Domains nutzten eine relativ kleine Anzahl von Keywords; am häufigsten beobachteten wir „Apple", „Findmy", „ID" und „iCloud". Es gab eine ganze Reihe von Lookalike-Domains mit Apple-Bezug.

Nachfolgend finden Sie ein paar Beispiele, darunter auch einige, die sich offenbar an spanischsprachige Nutzer richten:

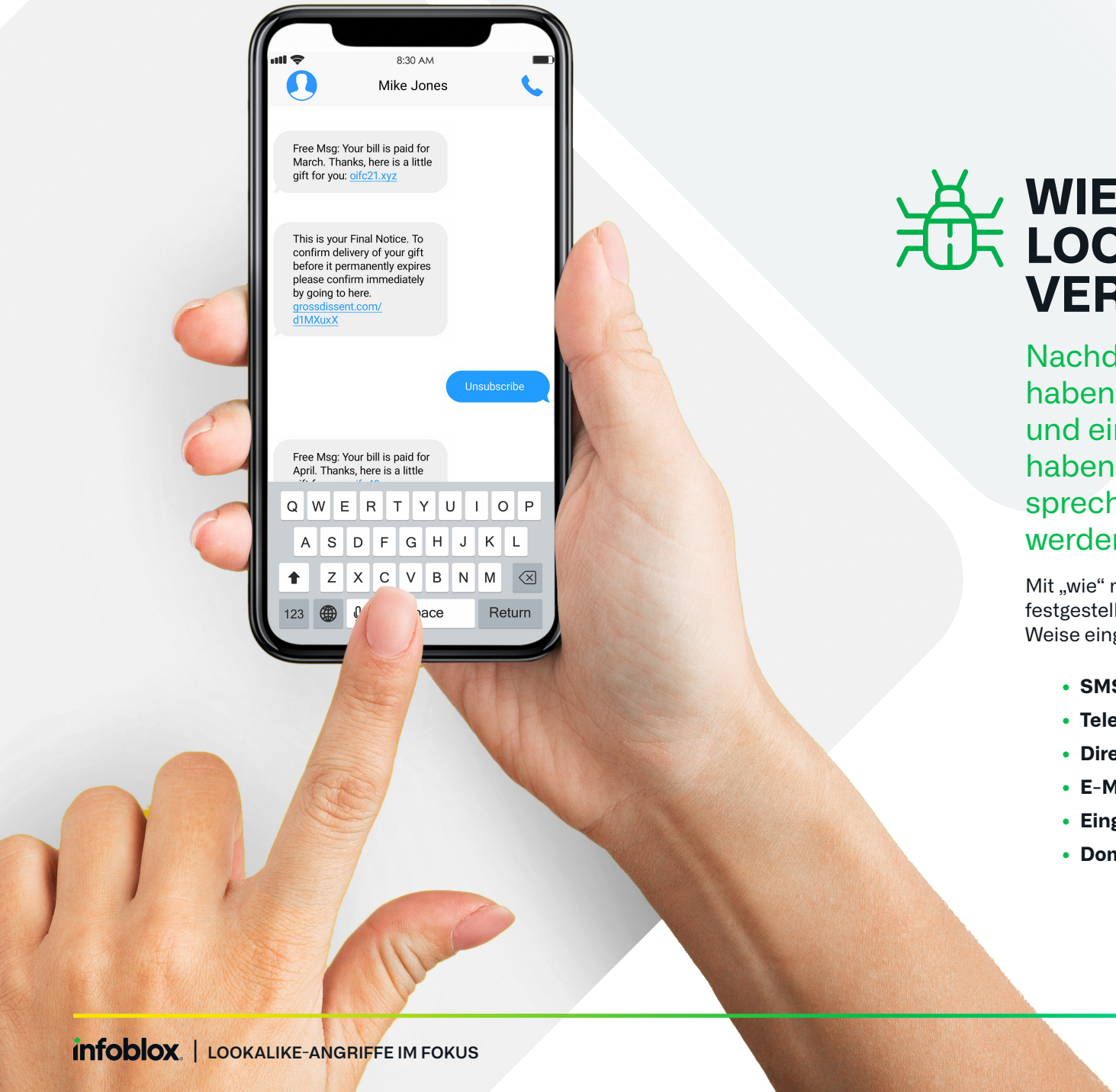
Tabelle 5. Lookalike-Domains, die auf Apple-bezogene Dienste abzielen.	
supportid-apple[.]com	sopport-apple[.]com
soporte-latam[.]us	soporte-appleid[.]com
lcloud-web-app[.]com	icloud-fndmy[.]com

SIE HABEN JEDEN IM VISIER

Unsere Erkennungsalgorithmen identifizieren jeden Tag Tausende neuer Lookalike-Domains. Jedes Unternehmen oder jeder Service, ob groß oder klein, bei dem böswillige Akteure Geld oder Identitäten stehlen können, ist ein potenzielles Ziel. Wir schließen diesen Abschnitt mit einer Auswahl von Lookalike-Domains, die wir in der Praxis beobachtet haben, und ihren Zielen ab.

Tabelle 6. Lookalike-Domains und ihre Ziele.

Lookalike-Domains	Lookalike-Ziel
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	Australische Steuerbehörde
checkscam22[.]com, checkscams[.]online, checkscammer[.]xyz	Websites zur Überprüfung von Betrug
xpressvpn[.]business, expressvpn-app[.]com, expressvpn-okta[.]com	Express VPN
anpost-paymentduty[.]com, ups-pay-deliveryfee[.]info, caddeliverypostca[.]com	Post- und Zustelldienste
crarebate-info[.]com	Kanadische Steuerermäßigung
ebl-ch[.]com	Schweizer Energieunternehmen EBL
op-fi-palvelut[.]co, op-fi-io[.]in	Op[.]fi, finnischer digitaler Bank- und Versicherungsservice
boatairbuds[.]in, boatbudsmusc[.]in, boatflashsale[.]in, boatmusicairbud[.]in	Indisches Technologieunternehmen BoAt
pumauaeshoes[.]com, pumanzsale[.]com, pumaireland[.]com, vejaoutletcanada[.]ca	Schuhhersteller
secure1-scotiabank[.]com,r-scotiabank[.]com, chasebank-jpm[.]com, thetrustnationalbank[.]com, amėricafirst[.]com	Banken
sprint-ldg[.]com, tds-telecom[.]com, teistra[.]ne, 1111systems-okta[.]com, t-mobile-okta[.]us, vzw-sso[.]com	Internet- und Cloud-Service-Anbieter
sso-authentication[.]de, sso-securelogin[.]com, service-sys-2fa[.]com	Multi-Faktor-Authentifizierung und Single-Sign-On-Domains



WIE WERDEN LOOKALIKES VERWENDET?

Nachdem wir uns damit beschäftigt haben, was Lookalike-Domains sind und einige Beispielziele genannt haben, lassen Sie uns nun darüber sprechen, wie sie verwendet werden.

Mit „wie“ meinen wir ihre Einsatzmethoden. Infoblox hat festgestellt, dass Lookalike-Domains auf verschiedene Weise eingesetzt werden, z. B:

- **SMS-Nachrichten**
- **Telefonanrufe**
- **Direktnachrichten auf Social-Media-Websites**
- **E-Mails**
- **Eingebettet in QR-Codes**
- **Domains im World Wide Web**

SIE SENDEN TEXTNACHRICHTEN

Trotz der Verbesserungen bei den Spam-Filtern für SMS-Nachrichten nimmt die Nutzung von SMS für Phishing-Nachrichten, auch Smishing genannt, weiter zu.

Die Akteure können schnell eine große Anzahl von Nachrichten verbreiten und einige der Sicherheitsmechanismen umgehen, die zum Schutz vor E-Mail-Phishing-Angriffen eingerichtet wurden. SMS werden sowohl für breit angelegte Angriffe auf Verbraucher als auch für gezielte Spear-Phishing-Angriffe auf Mitarbeiter von Unternehmen eingesetzt. In diesem Abschnitt beschreiben wir zwei Bedrohungsakteure, die SMS und Lookalike-Domains für Angriffe auf Verbraucher und Regierungsmitarbeiter verwendet haben.

Seit fast einem Jahr beobachtet Infoblox einen hartnäckigen Smishing-Akteur, der mit Lookalike-Domains arbeitet und den wir OpenTangle nennen. Unseres Wissens nach wurde über diesen Akteur noch nirgendwo anders berichtet. OpenTangle hatte es zunächst auf westliche Verbraucher abgesehen, indem er Lookalike-Domains von Finanzinstituten, Internetanbietern und Online-Händlern benutzte. Seit Kurzem nimmt der Akteur auch Angestellte und Auftragnehmer von Regierungen ins Visier. Uns sind über 1.500 Lookalike-Domains bekannt, die von OpenTangle kontrolliert werden, seit der Akteur vor etwa zwei Jahren erstmals in Erscheinung trat. Zu den Domains von OpenTangle gehören mtbsuportz0610[.]com, americafirst0nline[.]com und mygov03-ato[.]com.

Sie können sehen, dass verschiedene Lookalike-Domains verwendet werden.

Einer der Autoren dieses Artikels hat mehrere SMS von OpenTangle erhalten, darunter auch Lookalike-Domains der M&T Bank, mit der der Autor nichts zu tun hat. Zu Beginn seiner Kampagnen hat OpenTangle verkürzte URL-Links in seine Smishing-SMS eingebaut, vielleicht in der Hoffnung, dass die Verschleierung erfolgreich sein würde. Im Mai 2022 stellte der Akteur jedoch auf Lookalike-Domains um. *Abbildung 13* zeigt ein Beispiel für eine der Bankenkampagnen, in der die Anmeldedaten des Benutzers abgefragt wurden.

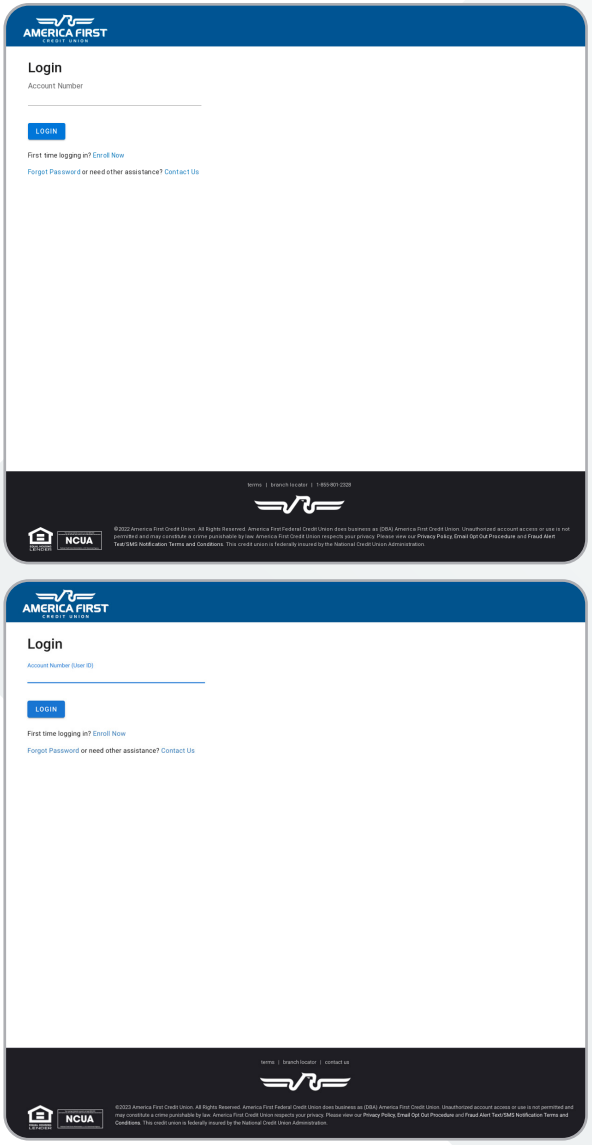


Abbildung 13. Eine Phishing-Seite auf der Domain americafirst0nline[.]com, die auf Kontoinhaber der America First Credit Union abzielt. Das Bild oben ist die Phishing-Seite, das Bild unten ist die legitime Seite. Bildnachweis: URLScan.[33]

OpenTangle hat im letzten Jahr damit begonnen, MFA mit AitM-Phishing-Kits auszunutzen. Während bei früheren Kampagnen Standard-Phishing-Anmeldeseiten verwendet wurden und diese im Allgemeinen auf Verbraucher abzielten, zeigt *Abbildung 14* ein Beispiel dafür, wie der Akteur seine Kampagnen weiterentwickelt hat. In diesem Fall zielen die Angreifer auf myGov-Kontoinhaber der australischen Regierung ab und verlangen einen MFA-Code anstelle einer einfachen Anmeldung. Sie haben auch einen Link eingefügt, um den Helpdesk anzurufen, eine weitere Technik, die im Jahr 2022 aufkam, um Benutzer zum Besuch bösartiger Websites zu bewegen.

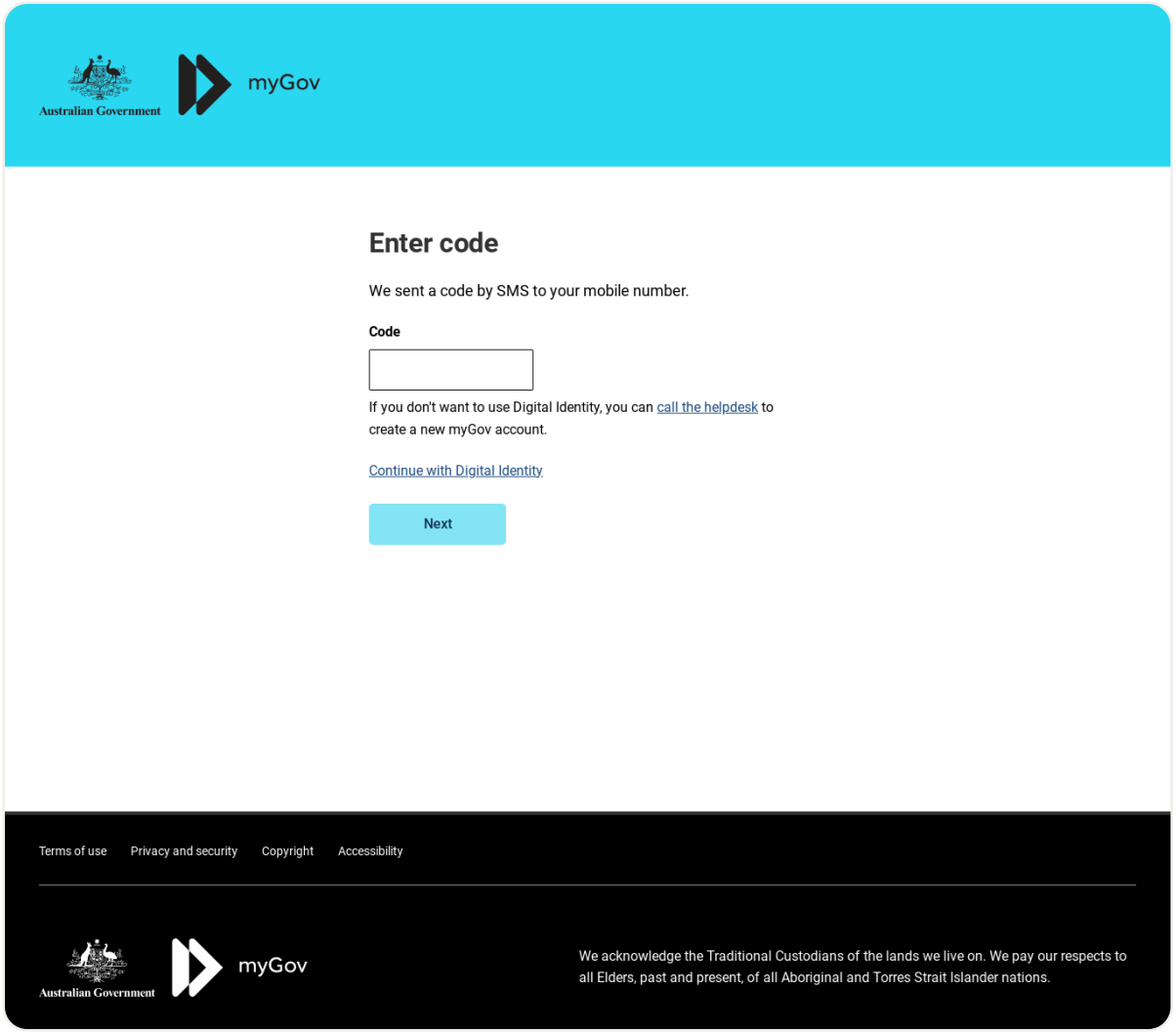


Abbildung 14. Lookalike-Domain www.mygovsupport-ato[.]com von OpenTangle, die myGov, das Online-Portal der australischen Regierung für die Regierungs-Cloud, imitiert. Bildnachweis: URLScan.[34]

Scamélie is another example of an actor using smishing messages to spread lookalikes.

Der Akteur, den wir Scamélie nennen, ist eine Gemeinschaft von lose verbundenen Gruppen und Einzelpersonen, die an einer langen Liste von Scams beteiligt sind, die aus französischsprachigen Ländern kommen und hauptsächlich auf diese abzielen. Wir haben auch festgestellt, dass sie allgemein auch Ziele in Europa und den Vereinigten Arabischen Emiraten ins Visier genommen haben. Die Lookalike-Domains von Scamélie geben sich in erster Linie als Internetanbieter, Banken, staatliche Dienste und Lieferfirmen aus. Aufgrund der lockeren Verbindung der Gruppe haben wir auch Betrugsversuche für Unternehmen beobachtet, von denen man es nicht erwartet, wie z. B. Reiseunternehmen, Sportbekleidungsfirmen und Lebensmittelgeschäfte.

Die Lookalïke-Domains von Scamélie werden oft bei großen Cloud-Providern oder sogenannten „Bulletproof"-Hosting-Anbietern gehostet. In einigen Fällen haben die Scammer ihre eigenen Hosting-Provider eingerichtet oder nutzen Hosting-Provider, die von anderen, nicht mit ihnen verbundenen Scammern eingerichtet wurden. Wir haben sowohl gezielte Domains als auch Allzweck-Domains (my-account, resolve-an-issue usw.) gefunden, die mit gestohlenen Identitäten registriert und mit virtuellen Kreditkarten oder Kryptowährungen bezahlt wurden.

Sobald die Akteure Kreditkarteninformationen gesammelt haben, rufen sie das Opfer an und geben sich als Mitarbeiter der Bank oder des Kreditkartenausstellers des Opfers aus.
Sie erklären, dass die Kreditkartendaten des Opfers gestohlen wurden, dass sie aber helfen werden, das Problem zu beheben. Der Anrufer sagt dann, dass das Opfer zwei MFA-Codes erhalten wird, die dem Anrufer zur Sicherheit des Kontos vorgelesen werden müssen.
In Wirklichkeit benötigt der Angreifer die MFA-Codes, um das Geld des Opfers in Echtzeit zu stehlen. Der erste MFA-Code erhöht den Überweisungsbetrag und der zweite ermöglicht die Durchführung der Transaktion. Damit die Anrufe noch effektiver werden, werden als Anrufer idealerweise junge Frauen und/oder Personen eingesetzt, die so Französisch sprechen, dass ein Muttersprachler keinen Verdacht schöpft.

Als unorganisierte Gruppe ist Scamélie schwer zu verfolgen und zu analysieren. Sie schlagen oft nachts zu und schalten ihre Domains schon nach ein paar Stunden oder Tagen wieder ab. Sie verwenden Anti-Bot- und Anti-Scraping-Skripte, um Sicherheitsforschern die Arbeit zu erschweren.

SCAMÉLIE BEISPIELE FÜR LOOKALIKE-DOMAINS

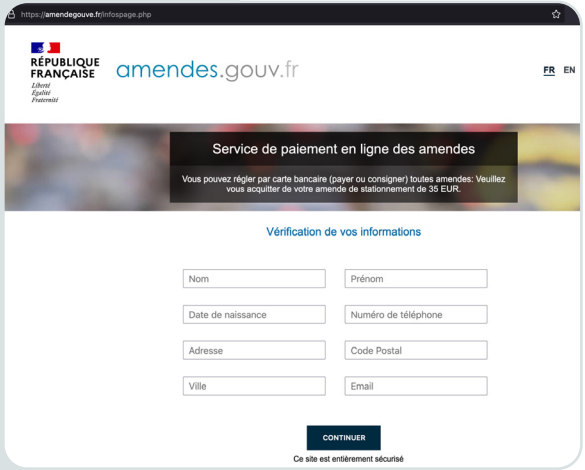


Abbildung 15. Eine Lookalike-Domain von Scamélie namens amendegouve[.]fr imitiert ein Service-Portal der französischen Regierung.

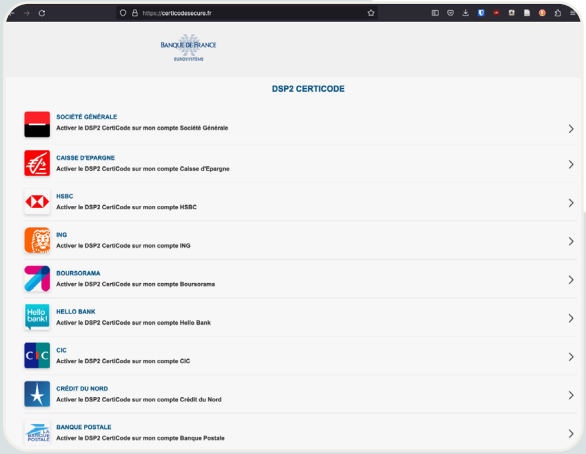


Abbildung 16. Eine Lookalike-Domain von Scamélie namens certicodesecure[.]fr imitiert einen französischen Banking-Service und verleitet Opfer dazu, ihre Kontodaten zu verknüpfen.
Bildnachweis: Infoblox.

SIE VERWENDEN ALTMODISCHE TELEFONANRUFE

Die Cybersecurity and Infrastructure Security Agency (CISA) veröffentlichte am 26. Januar 2023 ein Cybersecurity Advisory (CSA) über die böswillige Nutzung von Fernüberwachungs- und -verwaltungssoftware (Remote Monitoring and Management, RMM).[35]

Die CISA hat im Oktober 2022 eine Kampagne enttarnt, bei der bösartige Akteure Phishing-E-Mails mit einer Telefonnummer verschickten, in der die Benutzer aufgefordert wurden, diese anzurufen. Die E-Mail war so gestaltet, dass sie als Kundensupport-Nachricht durchging, und wenn die Benutzer die Telefonnummer anriefen, forderten die Akteure sie auf, eine bösartige Domain zu besuchen. Wenn ein Benutzer dieser Aufforderung nachkam, wurde eine ausführbare Datei heruntergeladen und anschließend eine zweite bösartige Domain kontaktiert, von der zusätzliche RMM-Software heruntergeladen wurde. Diese Software – AnyDesk und ScreenConnect – war legitim, aber so vorkonfiguriert, dass sie eine Verbindung zum RMM-Server des Täters herstellte, um dort zu bleiben.

Bei den verwendeten Domains handelt es sich um Lookalike-Domains bekannter Services. Die Wahrscheinlichkeit, die Domain zu akzeptieren, ist bei den Opfern, die sie am Telefon erhalten haben, sogar noch höher, da zusätzlich Social Engineering eingesetzt wird, um die Skripte und die Personas der Anrufer zu erstellen. Wir haben unsere Daten rückwirkend überprüft und Hinweise darauf gefunden, dass der Akteur schon länger aktiv ist, als die CSA angibt.[36] Diese Kampagnen sind mindestens seit Frühjahr 2021 aktiv, also über ein Jahr vor den Vorfällen, die CISA und Silent Push in einem separaten Artikel beschrieben haben. Wir konnten auch eine Wiederverwendung von Domains feststellen. Zum Beispiel war die Domain amzsupport[.]live, eine Lookalike-Domain von Amazon, Teil einer aktiven Kampagne im April 2020 und wurde dann im Oktober 2021 erneut verwendet.

Als Anfang 2023 Angriffe auf den MFA-Schutz interner Unternehmenssysteme bekannt wurden, stellte sich heraus, dass die Akteure in einigen Fällen das Opfer anriefen und sich als dessen IT-Abteilung ausgaben. Dies geschah, nachdem das Opfer auf die anfängliche Aufforderung nicht reagiert hatte, und diente dazu, die Notwendigkeit für den Benutzer, die Lookalike-Domain zu besuchen, weiter zu legitimieren. Benutzer, die der Aufforderung nachkamen, ermöglichten es dem Täter, ihre Unternehmensdaten zu stehlen.

SIE VERSCHICKEN SPAM

Wir haben zwar schon gesehen, wie gerissene Akteure Smishing und Telefonanrufe nutzen, um Lookalike-Domains zu verbreiten und ihre Opfer zu täuschen, aber die Phishing-E-Mail ist trotzdem nie ganz aus der Mode gekommen.

Infoblox analysiert jeden Tag Zehntausende von Malspam-E-Mails und stellt dabei einen scheinbar nicht enden wollenden Strom von Kampagnen fest, die Lookalike-Domains verbreiten. Wir werden auf einige dieser Kampagnen näher eingehen, möchten aber auch betonen, wie wichtig es ist, dass Unternehmen sorgfältig auf Phishing-E-Mails achten.

Eine dieser Kampagnen betrifft Xfinity, ein großes amerikanisches Telekommunikationsunternehmen. Diese Lookalike-Domains weisen DGA-ähnliche Merkmale und das folgende Format auf: xfnity.com. Beachten Sie, dass „Xfinity“ falsch geschrieben ist, weil das erste „i“ fehlt. Der Akteur sorgte auch dafür, dass der Absendername legitim erschien und als „Xfinity Mobile“ angezeigt wurde, was ein kyrillisches groß geschriebenes „X“ verwendet. Die Absender-E-Mails verwendeten ihre eigenen Domains und schienen auch im Benutzernamen DGA-ähnliche Merkmale aufzuweisen, die aus dem Muster noreply-<keyword> bestanden, wie zum Beispiel noreply-corporate@xfnitycard[.]com. Die Akteure haben nicht für jede E-Mail eine eigene Domain verwendet. In einigen Fällen wiederholten sich die Domains, aber das Keyword wurde geändert, wie z. B.: noreply-corporate@xfnitycard[.]com und noreply-active@xfnitycard[.]com.

Tabelle 7. Lookalike-Domains von Xfinity.

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

Die in der Kampagne identifizierten Domains nutzen eine Technik, die wir als Decoy-Parking bezeichnet haben: Wenn eine Domain direkt besucht wird und es so aussieht, als sei sie geparkt, aber in Wirklichkeit ist der Mailserver der Domain aktiv und versendet bösartige E-Mails. Wir haben festgestellt, dass Decoy-Parking recht häufig vorkommt und von anderen Anbietern nicht gemeldet wird. *In Abbildung 17 sehen Sie ein Beispiel für eine Seite, die Decoy-Parking verwendet*

XFINITY LOOKALIKE

Abbildung 17. Eine Decoy-Parking-Seite von der Lookalike-Domain xfnityrayton[.]com, die Xfinity imitiert. Bildnachweis: URLScan.[37]

LOOKALIKE-DOMAIN VON 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.

Abbildung 18. Hauptteil einer Malspam-Kampagne mit Wedo Machinery als Lockmittel und der Lookalike-Domain acrobat-adobe[.]com als Malware C2. Bildnachweis: Infoblox

Bei unserer Analyse haben wir diese Lookalike-Domains von Xfinity in verbreiteten schädlichen Word-Dokumenten gefunden.

Die Betreffzeilen der Kampagne dienten als CTA (Call to Action) und bezogen sich auf fehlgeschlagene Zahlungen oder die Androhung der Beendigung des Service, wie z. B. „[Ankündigung] Ihr Service wird möglicherweise gekündigt“ oder „[Maßnahme erforderlich] Ihre Karte funktioniert nicht, beheben Sie diesen Fehler“. Der Text dieser E-Mails gab vor, vom Kundendienst zu stammen, und wies die Empfänger darauf hin, dass sie „Details zum Fall im Anhang finden“.

Another campaign Infoblox identified used a Chinese recycling company, Wedo Machinery, to drop a ransomware loader. Wir haben 176 E-Mails in dieser Kampagne identifiziert, jede mit einer .zip-Datei, die eine einzige ausführbare Datei mit dem Namen Zmutzy enthält. *In Abbildung 18 sehen Sie ein Beispiel für eine E-Mail aus der Kampagne.* Wir haben zwei Dateinamen innerhalb der Kampagne gefunden: PO-0097(1).zip und PO-29862K.zip. Der Zmutzy-Loader verwendet die Lookalike-Domain acrobat-adobe[.]com, um weitere Payloads herunterzuladen.

SIE VERWENDEN QR-CODES

INeben direkten Lookalikes von Kryptowährungen haben wir auch die Verwendung von QR-Phishing beobachtet. Hierbei wird ein QR-Code verwendet, um ein URL-Ziel zu verfälschen und schädliche Inhalte zu verbreiten, und zwar in Verbindung mit Lookalike-Domains, die erstellt wurden, um Benutzer dazu zu verleiten, kostenlose Preise zu erhalten und Kontodaten für Krypto-Wallets anzugeben.

IIn einem Beispiel leitete der QR-Code das Opfer auf den Link bridge[.]walletconnect[.]com um, ein Mechanismus, mit dem Geld gestohlen werden kann. Bei diesem Betrug richteten die Täter ein Twitter-Konto ein, @adidas_weare, um Glaubwürdigkeit zu demonstrieren und ihre Lookalike-Domains zu teilen; *siehe Abbildung 19*. Das Konto hatte bis zum 21. Februar 2023 16.000 Follower. Glücklicherweise wurde es inzwischen gelöscht oder von der Plattform genommen.

Die Akteure machten Werbung für gefälschte Giveaways für verschiedene Artikel, darunter Porsches und Adidas-Kleidung oder -Schuhe. Bei den Domains handelt es sich überwiegend um Combosquats mit den Keywords „adidas“ oder „Porsche“. Beim Besuch der Lookalike-Domains, wie unten in *Abbildung 20* gezeigt, wurden die Nutzer aufgefordert, einen QR-Code zu scannen, der es ihnen ermöglicht, den verschenkten Artikel zu beanspruchen. Sie wurden dann zur dezentralen Anwendung WalletConnect umgeleitet, die dem Akteur Zugriff auf die Finanzmittel eines Nutzers gewährt.

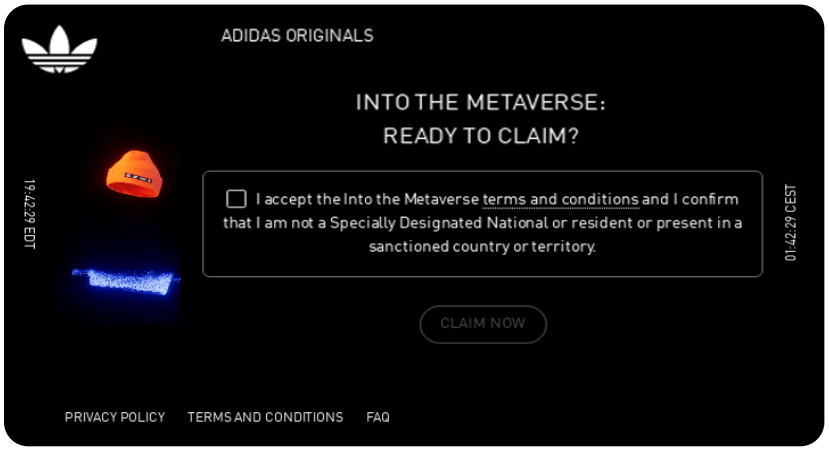


Abbildung 20. Lookalike-Domain von Adidas adidas-go[.]com, die Nutzer dazu verleitet, auf einen Link zu klicken, um einen Gratisartikel zu erhalten. Bildnachweis: URLScan.[39]

Wenn Benutzer den QR-Code scannen und ihre Kryptowährungs-Wallets mit der dezentralen Anwendung verknüpfen, sind die Akteure in der Lage, Kryptowährungen von den Benutzern zu erpressen. Diese Domains verwenden gemeinsam genutzte Nameserver und werden auf einer russischen IP-Adresse gehostet, 185[.]149[.]120[.]83, die vollständig von den Akteuren kontrolliert wird und weitere Lookalike-Domains zu Blur sowie Arbitum enthält, einer Lösung zur Verbesserung der Geschwindigkeit und Skalierbarkeit von Ethereum-Smart-Contracts.

ADIDAS LOOKALIKE

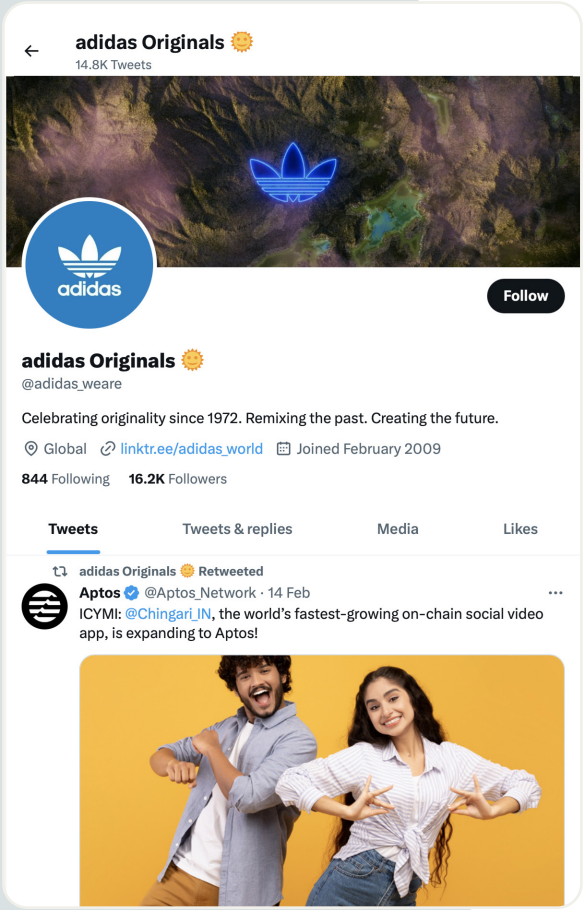


Abbildung 19. Das Lookalike-Twitter-Konto @adidas_weare von Adidas Originals @adidasoriginals. Bildnachweis: Infoblox.

SIE VERWENDEN DNS

Lookalikes kommen nicht nur als Website-Domains vor.

Wir haben festgestellt, dass sie in verschiedenen DNS-Funktionen verwendet werden, darunter:

- **Nameserver**
- **Mail server**
- **CNAME-Einträge**
- **PTR-Einträge**

In den meisten Fällen verfügen diese Domains nicht über einen typischen A-Eintrag oder eine Website-Präsenz und erscheinen oft geparkt. Dabei handelt es sich um eine Form des Decoy-Parking, die wir in einem früheren Abschnitt beschrieben haben. Angreifer verwenden Lookalike-Domains auch zur Umleitung und C2-Kommunikation im DNS.

NAMESERVER

Ein Beispiel für Lookalike-Nameserver sind die Domains bitkeep[.]dev und flutter[.]direct, die im November 2022 registriert wurden. Beide sind Lookalike-Domains für verschiedene Domains, aber sie teilen sich eine Infrastruktur. BitKeep ist ein dezentralisiertes Multi-Chain-Krypto-Wallet, das als zentrale Drehscheibe für alle Kryptowährungstransaktionen dienen soll. Die offizielle Domain von BitKeep ist bitkeep[.]com. Das Unternehmen besteht seit fünf Jahren und hat mehr als 8 Millionen Nutzer.[40] Flutter ist Googles portables Toolkit für die Benutzeroberfläche (UI), mit dem sich aus einer einzigen Codebasis nativ kompilierte Anwendungen für Mobilgeräte, das Web und den Desktop erstellen lassen. Die offizielle Domain für Flutter ist flutter[.]dev.[41]

Beide legitimen Domains hosten Webinhalte auf der primären Domain, aber keine der Lookalike-Domains tut dies. Bei der ursprünglichen Registrierung fungierten beide Domains als Nameserver für eine andere Domain, get-flutter[.]com, die eine weitere Lookalike-Domain von Flutter ist. Zu diesem Zeitpunkt wurden die Domains bei dem Schweizer Offshore-Hosting-Anbieter Private Layer gehostet. Dieses Netzwerk hostete auch flutter[.]vision. Wir können diese Domains zwar nicht eindeutig bösartigen Aktivitäten zuordnen, aber sie zeigen ein Muster der Nutzung von Lookalike-Domains für ungewöhnliche Zwecke. Ihre Analyse ist selbst für erfahrene Forscher recht schwierig und es ist unwahrscheinlich, dass viele Algorithmen zur Erkennung von Bedrohungen darauf anspringen.

MAILSERVER

Neben Nameservern haben wir auch Lookalike-Domains gefunden, die als Mailserver verwendet werden. Die Domains whirlpoolmxonline[.]com und whirlpoolservicesmx[.]com zielen auf die große Haushaltsgerätemarke Whirlpool ab und nutzen eine gemeinsame Infrastruktur. Sie werden auf derselben IP-Adresse gehostet, die Lyra Hosting gehört, einem nicht besonders guten VPS- und Hosting-Anbieter mit Sitz auf den Seychellen, und sie teilen sich gemeinsame Nameserver.

Whirlpool wird mit dem SLD (Second Level Domain)-Namen zwar direkt angegriffen, aber wir haben auch Merkmale innerhalb jeder Domain identifiziert, die zeigen, dass andere große Haushaltsgerätemarken ebenfalls zum Ziel werden. Die SLD whirlpoolmxonline[.] com hat drei Subdomains: mabe-onlinemx[.]whirlpoolmxonline[.]com, samsung-onlinemx[.] whirlpoolmxonline[.] com, und lg-onlinemx[.]whirlpoolmxonline[.]com. Mabe ist ein mexikanischer Haushaltsgerätehersteller. Die SLD whirlpoolservicesmx[.]com hat keine Subdomains, aber die historische Kette von SSL-Zertifikaten, die mit der Domain verknüpft sind, deutet darauf hin, dass ähnliche Haushaltsgerätemarken wie whirlpoolmxonline[.]com angesprochen werden: www[.] lgservicesmx[.]mabeservice[.]com und *.lgservicesmx[.]com.

Die Verwendung von Lookalike-Domains als Mailserver stellt eine zusätzliche Herausforderung für die Erkennung von Phishing-E-Mails auf einem Endgerät dar, da die E-Mail-Header auf den ersten Blick legitim erscheinen.

MALWARE C2s

Im Abschnitt über den Einsatz von E-Mails haben wir bereits erwähnt, dass eine von uns identifizierte Malspam-Kampagne, die den Ransomware-Loader Zmutzy enthielt, die Lookalike-Domain acrobat-adobe[.] com als Malware-C2-Server verwendete. Lookalike-Domains eignen sich perfekt für Malware C2s, da sie sich leicht neben legitimen Domains in den Netzwerkverkehr einfügen können. Analysten von ESET, einem slowakischen Unternehmen für Sicherheitssoftware, identifizierten im Februar 2023 Malware C2s für FatalRAT (Remote Access Trojaner), die sich als die Messaging-Anwendung Telegram ausgaben.[42]

Tabelle 8. Telegram-Lookalikes fungieren als Malware C2s.

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

Die Domains, auf denen die schädlichen .exe-Dateien gehostet wurden, waren auch Lookalike-Domains von Telegram, WhatsApp, Skype, Google Chrome und Firefox.

WEITERLEITUNGEN

Lookalikes können auch als Weiterleitungen verwendet werden. Wir haben ein großes Netzwerk von Typosquat-Domains identifiziert, die Besucher auf choto[.]xyz umleiten, eine C2-Domain, die die Opfer unter bestimmten Umständen auf die Landing-Domain lotto60[.]com umleitet. Der Akteur nutzt Reverse-Proxy-Services und den Bot-Schutz von Cloudflare auf choto[.]xyz, vermutlich um zu verhindern, dass der Angriff von Sicherheitsexperten entdeckt und untersucht wird. Die Landing-Domain scheint ein betrügerisches Affiliate-Marketing-Programm zu betreiben. Durch Analyse des Document Object Model (DOM) können wir feststellen, dass der HTML-Code eine Inline-Funktion gtag() enthält, die Besucherdaten an Google Analytics mit der Analyse-ID G-DT4YWT5VP8 sendet. Das hat nicht nur zur Folge, dass die Affiliate-Marketing-Zahlen des Akteurs aufgebläht werden, sondern wir haben auch festgestellt, dass lotto60[.]com über HTTP von potenziell bösartigen Dateien aufgerufen wird, die mit Dateisignaturen übereinstimmen, bei denen es sich nachweislich um den Remote-Access-Trojaner Nighthawk handelt.[43]

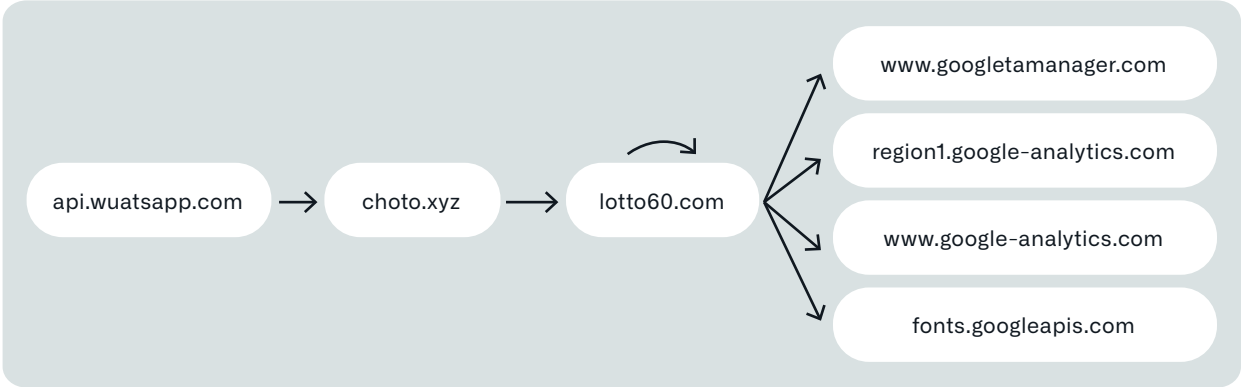


Abbildung 21. Beispiel einer Weiterleitungskette von einer Typosquat-Domain zu Google Analytics. Bildnachweis: URLQuery.[44]

Die Typosquat-Domains der ersten Stufe imitieren eine Vielzahl von Unternehmen. Einige Beispiele sind: →

Tabelle 9. Lookalike-Domains, die als Weiterleitungen in einer betrügerischen Affiliate-Marketing-Kampagne verwendet werden.

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

Diese Typosquats werden in der Regel für ein bis drei Monate geparkt, bevor sie als Weiterleitungen verwendet werden. Der Akteur hat bei der Erstellung dieser Typosquat-Domains große Sorgfalt walten lassen. Jedes falsche Zeichen befindet sich direkt neben dem richtigen Zeichen auf einer US-englischen QWERTY-Tastatur. Es handelt sich um Fehler, die jeder normale Benutzer beim Tippen an einem einzigen Tag mehrfach machen könnte – abgesehen von den Benutzern, die immer noch das „Adlersuchsystem“ verwenden.

WARUM FUNKTIONIEREN SIE?

Liebe Leserin, lieber Leser, sind Ihnen die 19 Lookalike-Wörter aufgefallen, die wir bisher in diesem Whitepaper versteckt haben? Einige davon sind sehr schwierig zu erkennen!

Tipp: Es gibt noch 6 weitere. Mal schauen, ob Sie sie finden!

Bisher haben wir uns mit einigen spezifischen Zielen sowie mit der Infrastruktur von Lookalike-Domains beschäftigt. Aber warum sind sie so effektiv? Was macht sie zu einer so hartnäckigen Bedrohung?

Die Antwort ist kompliziert und umfasst Aspekte der Psychologie, der technischen Umsetzung und einfacher menschlicher Fehler — **schließlich ist es das, was uns zu Menschen macht!**

PSYCHOLINGUISTICS

Psychologisch gesehen hat das menschliche Gehirn beim Lesen einen Kurzschluss (in diesem Fall meinen wir die wörtliche Definition eines Stroms, der unbeabsichtigt den Weg des geringsten Widerstands nimmt). Sie haben wahrscheinlich schon einmal ein Meme in dieser Art gesehen:

> ***Luat eneir Sutide der Uvinisterät Cbrmadgie ist es nchit witihcg, in wlecehr Rneflogheie die Bstachuebn in eneim Wrot sheten, das ezniige was wcthiig ist, ist dass der estre und der leztte Bstabchue an der ritihcegn Pstoiion snid. Der Rset knan ttoaelr Bsinöldn sien, tedztorm knan man ihn onhe Pemoblre lseen. Das ist so, wiel wir nciht jeedn Bstachuebn enzelin leesn, snderon das Wrot als gseatems.***

Zwar ist diese Behauptung nicht fundiert, weil es in Cambridge nie eine derartige Studie gab, aber das Konzept, das ihr zugrunde liegt, scheint durchaus stichhaltig zu sein. Jüngste Forschungsergebnisse deuten zum Beispiel darauf hin, dass „das Betrachten eines zusammengewürfelten Wortes eine visuelle Darstellung aktiviert, die mit bekannten Wörtern verglichen wird“.[45] Obwohl der Nachweis oder die Widerlegung grundlegender Fragen der Psycholinguistik den Rahmen dieses Whitepapers sprengen würde, möchten wir doch zeigen, wie die Psycholinguistik eine wichtige Rolle bei der Wirksamkeit von Lookαlikes spielt.

Die Kurzschlüsse im menschlichen Gehirn spielen insbesondere dann eine Rolle, wenn es um Homographєn und Typosquats geht. Wenn Sie eine Domain wie Infoblox[.]com sehen, analysiert Ihr Gehirn nicht unbedingt jeden einzelnen Buchstaben in diesem Domainnamen und so fällt Ihnen vielleicht nicht auf, dass das erste Zeichen eigentlich ein kleines „L“ und kein großes „i“ ist.

Aus ähnlichen Gründen wird Ihr Gehirn, wenn Sie die Domain goooogle[.]com sehen, vielleicht nicht erkennen, dass sie drei statt der richtigen zwei Buchstaben „o“ enthält … zumindest nicht, bis es zu spät ist und Sie bereits darauf geklickt haben.

PUNYCODE SUPPORT: HITS AND MISSES

Webbrowser bieten Möglichkeiten, um Benutzer vor Hom0graph-Angriffen mittels internationalisierter Domainnamen (IDN) zu schützen. Die erste und bekannteste Verteidigungslinie besteht darin, die Unicode-Domain in Punycode zu „übersetzen". Punycode ist an seinem führenden „xn--" zu erkennen und erscheint dem bloßen Auge als Kauderwelsch. Das liegt daran, dass Punycode die Unicode-Zeichen auf die weitaus begrenztere Untergruppe des American Standard Code for Information Interchange (ASCII) überträgt, die nur Buchstaben, Ziffern und Bindestriche enthält. Jeder gängige Browser unterstützt Punycode-Domains. Google beschreibt ausführlich die Heuristik des Algorithmus, der entscheidet, ob die internationalisierte oder die Punycode-Version einer Domain in Chromium angezeigt wird.[46] Mozilla stellt eine ähnliche Beschreibung zur Verfügung.[47]

Mozilla veröffentlicht in der Beschreibung seines IDN-Anzeigealgorithmus auch diesen inspirierenden Text:

> ***Unsere Antwort auf diese Frage ist, dass es letztendlich an den Registrierungsstellen liegt, dafür zu sorgen, dass ihre Kunden sich nicht gegenseitig betrügen. Browser können zwar einige technische Beschränkungen einführen, aber wir sind nicht in der Lage, diese Aufgabe für sie zu übernehmen und gleichzeitig dieselben Bedingungen für nicht-lateinische Schriften im Internet zu schaffen. Die Registrierungsstellen sind die einzigen, die in der Lage sind, hier ordnungsgemäße Prüfungen durchzuführen. Wir möchten von unserer Seite aus sicherstellen, dass wir nicht-lateinische Schriften nicht als zweitklassig behandeln.***

Im Jahr 2017 registrierte der Sicherheitsforscher Xudong Zheng bereits eine Domain in Punycode, xn--80ak6aa92e[.]com, die mit „apple[.]com" übersetzt wird und kyrillische Zeichen enthält, die das Aussehen der lateinischen Zeichen in „Apple" imitieren.[48] Zu dieser Zeit waren die Webbrowser Internet Explorer, Microsoft Edge, Safari, Brave und Vivaldi nicht anfällig, Chrome, Firefox und Opera hingegen schon. Derzeit übersetzt nur Firefox den Punycode, sodass die Benutzer gefährdet sind (wir haben die Domain in letzter Zeit nicht mit Internet Explorer oder Microsoft Edge getestet).

WAS IST PUNYCODE?

Punycode ist eine spezielle Kodierung, die verwendet wird, um Unicode-Zeichen in ASCII zu konvertieren, einen kleineren, eingeschränkten Zeichensatz. Punycode wird zur Kodierung internationalisierter Domainnamen (IDNs) verwendet.

IMESSAGE-SMISHING MIT IDN-HOMOGRAPHEN

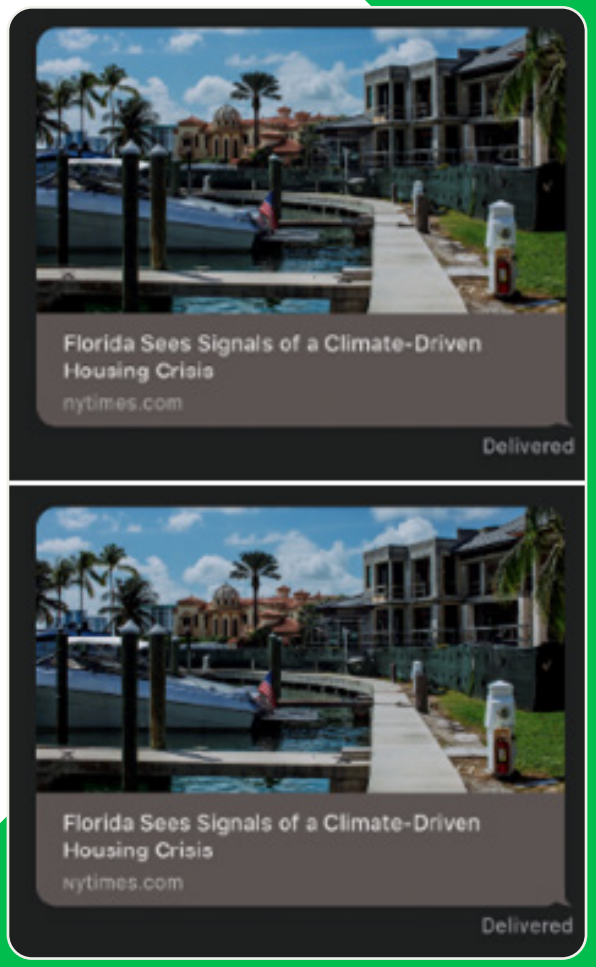


Abbildung 22. Das obere Bild stammt von Tyler Butler und zeigt einen echten Artikel der New York Times, der per iMessage verschickt wurde. Das untere Bild stammt von Tyler Butler und zeigt einen gefälschten NYT-Artikel über eine IDN-Homograph-Domain.
Bildnachweis: Tyler Butler.

Hu et al. führten eine Längsschnitt- und quantitative Analyse der Wirksamkeit von browserbasierten Abwehrmaßnahmen gegen IDN-Homograph-Angriffe durch.[49]

Dabei wollten sie Antworten auf drei Fragen finden:

1. Welche Richtlinien implementieren die gängigsten Browser und wie gut setzen sie diese Richtlinien durch?
2. Gibt es Möglichkeiten, die bestehenden Richtlinien systematisch zu umgehen?
3. Wie gut können Websurfer IDN-Homographen erkennen und haben IDN-Homographen, die die Browserrichtlinien umgehen, ein höheres oder niedrigeres Täuschungspotenzial?

Um diese Fragen zu beantworten, untersuchten die Autoren fünf Mainstream-Browser (Chrome, Firefox, Safari, Microsoft Edge und Internet Explorer) über einen Zeitraum von fünf Jahren (von Januar 2015 bis April 2020). Sie erstellten 9.000 Testfälle, um die ersten beiden Fragen zu beantworten, und führten für die dritte Frage eine Nutzerstudie durch. Chrome und Edge waren bei der Anzeige von Punycode anstelle der entsprechenden IDN-Homographen am erfolgreichsten; beide Browser hatten eine Gesamtfehlerquote von 20,62 % (d. h. sie zeigten die IDN-Version anstelle von Punycode). Safari und Firefox waren mit einer Gesamtfehlerquote von 42,91 % bzw. 44,46 % deutlich schlechter. Jeder Browser wies je nach IDN-Kategorie unterschiedliche Fehlerquoten auf. Darüber hinaus fanden die Autoren heraus, dass Websurfer Schwierigkeiten haben, homographische IDNs zu identifizieren. Die IDNs, die von den Browsern blockiert wurden, bereiteten bei der Bestimmung der Echtheit die größten Schwierigkeiten: 48,8 % der Nutzer glaubten, dass sie echt waren, 48,5 % der Nutzer glaubten, dass sie nicht echt waren, und 2,7 % konnten es nicht erkennen.

Bislang haben wir uns nur auf Desktop-Browser konzentriert. Aber wie wir bei den Lookalike-Smishing-Angriffen gesehen haben, die weiter oben in diesem Dokument beschrieben wurden, sind IDN-Homograph-Domains auch auf mobilen Geräten sehr verbreitet. Sie sind möglicherweise sogar noch bösartiger. Kleinere Bildschirme, kleinere Adressleisten und ein allgemeines Fehlen einer Link-Vorschau können dazu führen, dass Lookalike-Domains noch effektiver für Angriffe eingesetzt werden. Selbst wenn es eine Link-Vorschau gibt, können IDN-Homographen auf mobilen Geräten immer noch wirksam sein. Im Jahr 2021 veröffentlichte der Sicherheitsforscher Tyler Butler einen Artikel über die Plausibilität von Smishing mit IDN-Homographen in iMessage.[50] iMessage bietet zwar eine umfangreiche Link-Vorschau, aber ein geschickter Angreifer kann dies mit einer entsprechenden Lookalike-Domain und ein wenig Styling auf der Webseite selbst recht einfach umgehen. Wie Butler anmerkt, kann diese Form des Angriffs genutzt werden, um Fehlinformationen zu verbreiten, Zugangsdaten zu stehlen oder gezielt Malware oder Spyware zu installieren.

Butler beschreibt auch, dass Apple behauptet, sie würden die Schwachstelle nicht beheben, weil die Homogr̨aphen „visuell unterscheidbar“ seien. *Was denken Sie angesichts von Abbildung 22? Können Sie den Unterschied erkennen?*

IRREN IST MENSCHLICH, VERGEBEN IST GÖTTLICH ... ABER AUTOMATISIEREN IST KLUG

On the World Wide Web, some other humans aren't so forgiving of others' mistakes. Wie wir bereits erwähnt haben, nutzen Akteure Typosquat-Domains, um die natürlichen Rechtschreibfehler anderer auszunutzen. Alles, was ein Angreifer für einen Typosquat tun muss, ist, eine plausible Domain zu registrieren und abzuwarten. Das war's. Früher oder später wird ein Mensch diesen Rechtschreibfehler machen und auf einer Domain landen, die er nie besuchen wollte. Natürlich warten die Betrüger nicht nur ab, sondern verleiten die Menschen auch aktiv zum Klicken. Und in unserer schnelllebigen Welt merken wir das oft gar nicht.

Letztendlich werden Lookalike-Domains nicht ohne Grund so genannt: Sie sehen (Englisch „look") bekannten Domains ähnlich (Englisch „alike") und zielen darauf ab, Menschen zu täuschen. Wie wir gesehen haben, sind einige Lookalike-Domains effektiver als andere, aber die Wahl des Domainnamens ist nur ein Teil der Effektivität einer Lookalike-Domain. Auch die Art und Weise, wie eine Lookalike-Domain eingesetzt wird, kann einen erheblichen Einfluss auf den Gesamterfolg der Kampagne haben. Nehmen wir zum Beispiel eine Okta- oder MFA-Lookalike-Domain wie okta[.] Infoblox[.]com, oder okta-Infoblox[.]com. Eine aufmerksame Person, die jeden Domainnamen dreifach überprüft, bevor sie ihn besucht (viel Glück bei der Suche nach solchen Leuten), kann vielleicht feststellen, dass das „i" in der Second Level Domain (SLD) in Wirklichkeit ein kleines „L" ist. Aber diese Lookalike-Domains, gepaart mit einer gut formulierten SMS-Nachricht an die Telefonnummer, die jemand z. B. im Online-Profil seines Arbeitgebers hat, könnten den entscheidenden Ausschlag geben. Wenn dann noch ein Anruf mit einer dringenden Aufforderung zum Handeln hinzukommt, ist es zu spät. Natürlich handelt es sich hier um ein fiktives Beispiel für Spear-Phishing (bei dem alle Komponenten verwendet werden) und nicht um eine allgemeine Kampagne, bei der Lookalikes zum Einsatz kommen, aber es gilt nach wie vor: Lookalike-Domains können auf verschiedene Weise und in verschiedenen Teilen der DNS-Infrastruktur effektiv eingesetzt werden.

Das oft zitierte Sprichwort „Wer zweimal auf den gleichen Trick hereinfällt, ist selber schuld!" trifft auf Lookalike-Domains nicht zu. Selbst die wachsamsten und sicherheitsbewusstesten Personen können einer Lookalike-Domain zum Opfer fallen – und zwar immer und immer wieder. Böswillige Akteure haben in diesem Kampf die Oberhand, aber er ist noch nicht verloren. Infoblox bietet Lösungen auf DNS-Ebene an, um sicherzustellen, dass Unternehmen in der Lage sind, sich zu wehren und sich effektiv zu schützen.

IOCs ***Die vollständige Liste für dieses Whitepaper finden Sie auf GitHub unter https://github.com/infobloxopen/threat-intelligence***

INFOBLOX-LÖSUNGEN

Lookalike-Domains sind bei Angreifern nach wie vor sehr beliebt, da sie sehr effektiv sind und es schwierig ist, sie auf breiter Ebene zu erkennen. Hinzu kommt die Schwierigkeit, eine verdächtige Domain, die ein legitimes Ziel imitieren soll, automatisch zu identifizieren. Dies hat dazu geführt, dass Unternehmen und Regierungsbehörden sich zunehmend Sorgen über Lookalike-Domains machen, die ihre Unternehmensdomains oder ihre Lieferkette imitieren.

Infoblox BloxOne Threat Defense (B1TD) Advanced bietet eine einzigartige, umfassende Lösung für Lookalike-Bedrohungen. Durch die Nutzung des DNS im großen Stil ist Infoblox in der Lage, jeden Tag eine Reihe von Analysen auf Hunderttausende neuer SLDs anzuwenden. Dazu gehören mehrere Analysen zur Erkennung von Lookalike-Domains, wie z. B. eine automatische Bewertung der visuellen Ähnlichkeiten in IDN-Homographen.

CKunden können aus den gängigen Domains auswählen oder eine benutzerdefinierte Liste für die spezielle Überwachung und Analyse von Lookalike-Domains erstellen. Die Ergebnisse dieser tiefgreifenden Analyse können über die lookalike Reporting UI abgerufen werden, die auch die Fälle kennzeichnet, in denen die erkannten Lookalike-Domains mit verdächtigen oder Phishing-Aktivitäten in Verbindung gebracht werden. Insgesamt lassen sich die Richtlinien an die Bedürfnisse der spezifischen Umgebung und Risikotoleranz eines Kunden anpassen. Die detaillierten Domain-Daten enthalten wertvolle Anmerkungen, die über die B1TD Advanced UIs und APIs zugänglich sind und den Kunden Kontext bieten, wodurch die Untersuchung von Bedrohungen beschleunigt und die Reaktion auf Vorfälle effektiver wird.

Diese Funktionen zur Erkennung von Lookalike-Domains sind nur einer von vielen Services, die BloxOne Threat Defense anbietet und die es ermöglichen, Bedrohungen zu identifizieren, die andere Lösungen nicht erkennen, und Angriffe früher im Lebenszyklus der Bedrohung zu stoppen. Durch die umfassende Automatisierung und die Integration von Ökosystemen kann die Software die Effizienz von SecOps steigern, die Effektivität des bestehenden Sicherheitsstacks erhöhen, digitale und ortsunabhängige Prozesse schützen und die Gesamtkosten für Cybersicherheit senken.

FOR MORE INFORMATION

Visit infoblox.com

Follow-us on LinkedIn

Follow-us on Twitter

REFERENCES

[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 vereint Netzwerk- und Sicherheitslösungen für ein unübertroffenes Maß an Leistung und Schutz. Wir bieten Echtzeit-Transparenz und Kontrolle darüber, wer und was sich mit Ihrem Netzwerk verbindet, damit Ihr Unternehmen schneller arbeiten und Bedrohungen früher stoppen kann. Darauf vertrauen Fortune-100-Unternehmen und aufstrebende Innovatoren.

Hauptsitz der Gesellschaft
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com