infoblox

2025 BERICHT ZUR DNS-BEDROHUNGS-LANDSCHAFT

Der Nebel der Cyberbedrohung:

Wie böswillige Akteure DNS nutzen, um zu täuschen und auszuweichen

Im vergangenen Jahr haben Bedrohungsakteure ihren Einsatz von Täuschung rasch vorangetrieben – sie haben ihre Operationen skaliert und KI genutzt, um Einzelpersonen und Organisationen anzugreifen und der Bedrohungsforschung zu entgehen. Infoblox Threat Intel hat ein neues Maß an Professionalität und Geschwindigkeit bei der Durchführung von Cyberangriffen über das Domain Name System (DNS) beobachtet, die Verbraucher, Unternehmen und Behörden gleichermaßen betreffen.

Um sich effektiv zu verteidigen, müssen Sicherheitsteams die Bedrohungen verstehen, denen sie ausgesetzt sind. Einblicke in gegnerische DNS-Techniken, die Akteure dahinter und die Risiken, die sie darstellen, sind unerlässlich, um Verteidigungsstrategien zu stärken.

Dieser Bericht stützt sich auf umfangreiche Echtzeit-DNS-Telemetriedaten, modernste Analysen und jahrzehntelange Bedrohungsexpertise, um eine einzigartige Perspektive darauf zu bieten, wie Angreifer DNS ausnutzen. Es skizziert auch die geschäftlichen Auswirkungen und hebt DNS-basierte Intelligenz als kritische Schicht der modernen Cyberabwehr hervor.

INHALTSVERZEICHNIS

DAS UNGENUTZTE POTENZIAL VON DNS-INTELLIGENCE

DNS wird oft als das Telefonbuch des Internets bezeichnet, weil es Domainnamen in IP-Adressen übersetzt. Jede digitale Interaktion beginnt mit einer DNS-Anfrage, was sie zu einer hochpräzisen Quelle für Telemetriedaten im Netzwerkbetrieb macht, da sie tiefgehende Einblicke in die digitalen Assets bietet, die Verbindungen über das Internet initiieren.

DNS wird auch von böswilligen Akteuren beim Phishing, Betrug, zur Umgehung von Erkennung und bei der Datenextraktion genutzt. Folglich ist die Analyse des DNS-Verkehrs und der Domainnutzung grundlegend für Sicherheitsanalysten. DNS-Daten können in vorausschauende Bedrohungsinformationen umgewandelt werden, indem Telemetriedaten vor Angriffen ganzheitlich erfasst, die Daten angereichert, gegen Baselines analysiert und umfassende Bedrohungssuchen durchgeführt werden. Diese Erkenntnisse bieten Verteidigern einen umfassenden Überblick über die Infrastrukturen der Angreifer, die angegriffenen Opfer und die verwendeten Taktiken – noch bevor der Angreifer zuschlägt.

„DNS eröffnet einen einzigartigen Einblick in vergangene Bedrohungsaktivitäten, der wiederum als Kristallkugel dient und die Vorläufer zukünftiger Cyberbedrohungen enthüllt."

– **Dr. Renée Burton**
Head of Infoblox Threat Intel

Infolgedessen bietet DNS weit mehr als nur Namensauflösung und ist sowohl ein Durchsetzungspunkt für die Unternehmenssicherheitsrichtlinie als auch ein Indikator für potenzielle bösartige Aktivitäten in einem Netzwerk geworden. Organisationen wie das National Institute of Standards and Technology (NIST) und die Cybersecurity & Infrastructure Security Agency (CISA) haben diese kritische – und frühe – Rolle, die DNS in der Cybersicherheit spielt, erkannt und sein vorbeugendes Sicherheitspotenzial in der kürzlich vorgeschlagenen NIST Special Publication (SP) 800-81 Rev. 3 hervorgehoben.[1]

Dieser Bericht behandelt vier Schlüsselfragen:

Was sind die wichtigsten DNS-Beobachtungen der letzten 12 Monate?

Wer sind die DNS-Bedrohungsakteure und welche aktuellen Aktivitäten wurden entdeckt?

Welche bösartigen Taktiken stecken hinter DNS-Techniken und warum sind sie gefährlich?

Was sind die wichtigsten Herausforderungen für Verteidiger, und welche Möglichkeiten bietet die DNS-basierte Bedrohungsaufklärung?

1 Secure Domain Name System (DNS) Deployment Guide, National Institute of Standards and Technology (NIST), 10. April 10 2025.

ABSCHNITT 1: BEOBACHTUNGEN ZU DEN WICHTIGSTEN DNS-BEDROHUNGEN

100.8
million newly observed domains in one year

25.1%
of newly observed domains are malicious or suspicious

Vergängliche Natur von Domains

Ende Mai 2025 verarbeitete und analysierte Infoblox täglich 70 Milliarden DNS-Abfragen aus über 13.000 Infoblox-Umgebungen, die Millionen von IP-Adressen auf allen Arten von Geräten abdeckten.

Die vollständig anonymisierten Daten von über 1.300 Infoblox Threat Defense™-Kunden bieten sowohl global als auch detailliert Einblick in Millionen von Internetinteraktionen, die sich über verschiedene Kundentypen, Regionen und Branchen erstrecken. Im Jahresvergleich stieg dieses DNS-Telemetrievolumen um 21 %.

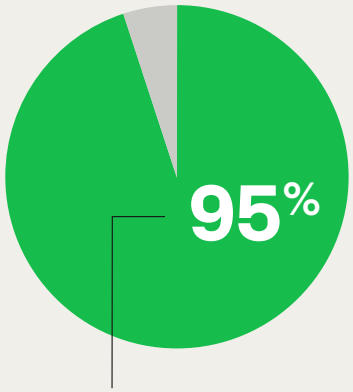
Innerhalb aller gesammelten Daten hat Infoblox Threat Intel **100,8 Millionen neu beobachtete Domains (Second-Level-Domains) in den letzten 12 Monaten identifiziert**. Dieses hohe Volumen neuer Domains ist oft das Ergebnis von sich schnell ändernden Infrastrukturen, kurzfristigen Werbekampagnen und Branding-Initiativen.

Kontrollumgehung über Einmal-Domains

Mehr als ein Viertel der neu beobachteten Domains (über 25 Millionen) wurden von Infoblox als bösartig oder verdächtig eingestuft. Bedrohungsakteure registrieren, aktivieren und setzen kontinuierlich eine große Anzahl neuer Domains ein, um Erkennungskontrollen zu umgehen. Da es schwierig ist, derart große Mengen an Domains zu identifizieren und zu klassifizieren, können Angreifer unentdeckt bleiben, Blockierungsmechanismen umgehen und nur minimale forensische Spuren hinterlassen.

Die isolierte Nutzung identifizierter bedrohungsbezogener Domains – sowohl bösartiger als auch verdächtiger – ist ebenfalls signifikant. Infoblox Threat Intel stellte fest, dass 95 % aller bedrohungsbezogenen Domains innerhalb einer einzigen Netzwerkumgebung beobachtet wurden.

Das Ziel dieser Taktik ist einfach: forensische Abwehrmaßnahmen, die auf „Patient Zero“-Daten basieren, zu umgehen, indem Wegwerf-Domains genutzt werden, von denen Angreifer unbegrenzt viele haben.



of threat-related domains were observed in only one customer environment.

Bösartige versus verdächtige Domains

- **Bösartige Domains** sind bestätigte Bedrohungen, die durch starke Beweise gestützt werden. Sie veralten nicht und machen 1,6 % der über 100 Millionen neu beobachteten Domains aus.
- **Verdächtige Domains** sind potenzielle Bedrohungen ohne schlüssige Beweise und machen 23,5 % aller neu beobachteten Domains aus. Wenn sie nicht bestätigt werden, verfallen diese Indikatoren nach einigen Monaten. Die Analysten von Infoblox Threat Intel überwachen diese Domains kontinuierlich auf neue Beweise. Wenn zusätzliche Indikatoren entdeckt werden, werden die Bewertungen aktualisiert, und verdächtige Domains können als bösartig eingestuft werden.

Cloaking Via Domains sind Teil von Traffic Distribution Systems

Adtech (kurz für Advertising Technology) bezeichnet die Tools, Software und Plattformen, die zur Automatisierung, Verwaltung, Ausrichtung, Bereitstellung und Analyse digitaler Werbung verwendet werden. Traffic Distribution Systems (TDS) sind die Plattformen oder Mechanismen, die – legitim oder böswillig – dazu verwendet werden, eingehenden Internetverkehr anhand vordefinierter Regeln an verschiedene Ziele umzuleiten. Auch Bedrohungsakteure haben diese Technologie übernommen, die oft als **bösartige Adtech** bezeichnet wird.

82%

of customers queried a domain part of a traffic distribution system.

In den letzten 12 Monaten **haben 82 % aller Kundenumgebungen** Domains abgefragt, die Teil von TDS waren, von denen ein Großteil von böswilligen Adtech-Betreibern betrieben wird, die dafür bekannt sind, schädliche Inhalte wie maßgeschneiderte Phishing-Seiten, Scareware, Betrugsversuche und Infostealer zu verbergen.

Diese TDSs bestehen häufig aus Zehntausenden von Domains, die schnell rotiert werden, um einer Erkennung zu entgehen, und liefern gezielte schädliche Inhalte an die idealen Opfer, während sie diese Inhalte vor Bedrohungsforschern verbergen.

Im Laufe der Zeit entdeckte Infoblox Threat Intel über **eine Million Domains, die von 168 bösartigen Adtech-Betreibern** innerhalb ihrer TDS-Infrastruktur verwendet wurden. Diese Indikatoren umfassen verschiedene DNS-Techniken, wie gekaperte Domains, Lookalikes, Weiterleitungen und algorithmisch vorregistrierte Domain-Sets (Registered Domain Name Algorithms, RDGAs). Mehr zu TDSs, ihrer Funktionsweise und warum sie gefährlich sind, finden Sie in Abschnitt 3.

Domains, die mit verschiedenen Bedrohungstypen verknüpft sind

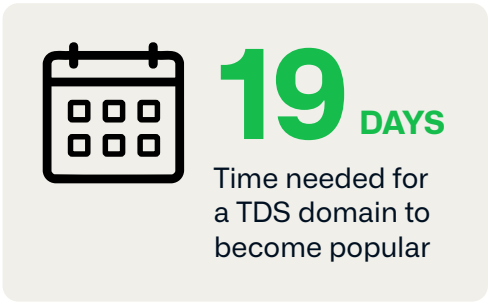
Wenn neue bedrohungsbezogene Domains entdeckt werden, untersuchen die Bedrohungsforscher von Infoblox die Akteure dahinter und ihre zugrunde liegenden Absichten. Die Tabelle auf der nächsten Seite enthält eine nach Prioritäten geordnete Liste, wie Akteure ihre Domains für verschiedene böswillige Zwecke nutzen.

Top-7-Liste: Wie Bedrohungsakteure neue Domains nutzen	
1	**Beteiligung an betrügerischen Aktivitäten und Betrügereien**, wie z. B. gefälschten Kryptowährungs-Investitionsseiten.
2	**Hosten illegaler Inhalte**, einschließlich Glücksspiel (insbesondere in Regionen wie China) und pornografisches Material.
3	**Erstellen von Phishing-Seiten**, die darauf abzielen, persönliche Informationen oder Kreditkartendaten zu stehlen.
4	**Bereitstellen von Malware.** Häufige Beispiele sind Infostealer (z. B. Lumma Stealer), Loader über Drive-by-Downloads (z. B. SocGholish), Botnets und Ransomware (z. B. BlackBasta).
5	**Tarnen ihrer Aktivitäten** über TDS und Liefern verschiedener Nutzlasten oder Benutzer dazu verleiten, unerwünschte Browser-Benachrichtigungen zuzulassen.
6	**Verteilen potenziell unerwünschter Programme** (**PUPs**), wie Scareware oder unnötige Browsererweiterungen.
7	**Durchführen von Spam-Kampagnen und Verbreiten bösartiger E-Mails**.

Tabelle 1. Zweck der Akteure für neu beobachtete Domains.

Domain-Popularität

Die DNS-Telemetrie von Infoblox bietet auch Einblicke in die Nutzung von Domaintypen und liefert Hinweise auf die Beliebtheit von Anwendungen sowie die Geschwindigkeit, mit der Bedrohungsakteure erfolgreich große Mengen an manipulierten Domains vor ihren Opfern platzieren.



Wichtige Beobachtungen:

- Acht Domainkategorien – wie Content Delivery Networks (CDNs), Technologieanbieter, Sicherheitsanbieter, Tools zur Unternehmensproduktivität, Suchmaschinen, Speicher, Cloud-Dienste und Net Conferencing – machen den Großteil (an einem bestimmten Tag etwa 70 %) aller Domains in DNS-Abfragen von Kunden aus.
- Im Mai 2025 erreichten Domain-Anfragen im Zusammenhang mit der privaten Internetnutzung – wie Online-Shopping, Gaming und soziale Medien (z. B. TikTok und Facebook) – die gleiche Häufigkeit wie Anfragen im Zusammenhang mit professionellen Kollaborationsplattformen (z. B. Microsoft Teams, Slack). Dies verdeutlicht die **zunehmende Überschneidung zwischen beruflicher und privater Internetnutzung** – eine Überschneidung, der sich Bedrohungsakteure sehr bewusst sind.
- Angreifer suchen kontinuierlich nach schwachen Angriffsflächen, wie Bring-Your-Own-Device (BYOD) und mobile Geräte, und täuschen Benutzer, um sie zu riskanten Handlungen zu verleiten, die darauf abzielen, geschäftsbezogene Daten, einschließlich Anmeldedaten, zu extrahieren. Dieser Trend wurde auch im 2025 Data Breach Investigations Report von Verizon hervorgehoben.[2] in dem bestätigt wird, dass kein Gerät vor Angriffen sicher ist, und darauf hingewiesen wird, dass **46 % der gestohlenen Unternehmenszugangsdaten** von nicht verwalteten oder privaten Geräten stammen.

2 2025 Data Breach Investigations Report, Verizon.

- Infoblox Threat Intel beobachtete, dass Domains, die Teil von TDSs sind, immer beliebter werden.[3] in nur 19 Tagen, **2,35-mal schneller als im Jahr 2024 und 39-mal schneller als im Jahr 2020.** Die Geschwindigkeit, mit der TDS-Domains an Popularität gewinnen – vergleichbar mit legitimen Websites wie `panerabread[.]com` oder `draftkings[.]com` – veranschaulicht, wie effektiv bewaffnete Domains verbreitet und von Opfern genutzt werden. Bedrohungsakteure setzen schnell große Mengen dieser Domains vor ihren Zielen ein, um die Wirkung ihrer Kampagnen zu maximieren und gleichzeitig langsamere Intelligence-Quellen wie Open-Source-Intelligence (OSINT) und forensische Analysen zu übertreffen.

ABSCHNITT 2: BEDROHUNGSAKTEURE UND FORSCHUNG

204K
total identified suspicious domain clusters

662
total identified DNS threat actors

10
new actors publicly disclosed in the past 12 months

Die 100 Millionen neuen Domains, die im vergangenen Jahr entdeckt wurden, sind keine Naturgewalten – sie werden immer durch menschliches Handeln verursacht und für bestimmte Zwecke initiiert. Infoblox Threat Intel analysiert und untersucht kontinuierlich die Akteure hinter bedrohungsbezogenen Domains, indem gesammelte Telemetriedaten angereichert und gemeinsame Muster korreliert werden.

Seit Beginn seiner Untersuchungen hat Infoblox Threat Intel insgesamt 204.000 verdächtige Domain-Cluster entdeckt, die alle gemeinsame Bedrohungselemente aufweisen, und 662 einzigartige Bedrohungsakteure identifiziert. Allein in den letzten 12 Monaten haben die Forscher von Infoblox in verschiedenen Forschungsberichten und Blogbeiträgen 10 neue Akteure öffentlich bekannt gegeben.

3 Eine Domain gilt als populär, wenn sie zu der Untergruppe von Domains gehört, die in einem bestimmten Zeitraum den Großteil des Kundenverkehrs ausmachen. An einem bestimmten Tag können es zwischen 6.000 und 10.000 Domains sein. Weitere Informationen finden Sie unter https://blogs.infoblox.com/wp-content/uploads/infoblox-whitelists-that-work.pdf.

In der folgenden Liste sind die wichtigsten Bedrohungsakteure aufgeführt, die von Infoblox Threat Intel zwischen dem 1. Juli 2024 und dem 1. Juli 2025 identifiziert und öffentlich bekannt gegeben wurden.

Akteure	Beschreibung
	Dieser Akteur betreibt ein bösartiges TDS, das legitimen Web-Traffic – hauptsächlich von kompromittierten WordPress-Websites – kapert und ihn auf Betrugs-, Malware- und Phishing-Inhalte umleitet. VexTrio gilt als einer der am weitesten verbreiteten und ausweichendsten Akteure in der Bedrohungslandschaft. In den letzten 12 Monaten wurde der Akteur in mehreren Berichten aufgrund seiner Beziehung zu Affiliate-Hackern genannt und ist dafür bekannt, Domains zu kapern, um ihre Angriffsinfrastruktur zu versorgen. **Kürzlich veröffentlichte Berichte:** • The Vexing and Vicious: Die unheimliche Beziehung zwischen WordPress-Hackern und einer Adtech-Kabale • In den Kaninchenbau gestoßen
	Diese hochentwickelte DNS-Bedrohungsgruppe ist darauf spezialisiert, verlassene Cloud-Ressourcen – wie Amazon S3-Buckets und Azure-Endpunkte – zu kapern, indem sie falsch konfigurierte oder vergessene DNS-Einträge ausnutzt, insbesondere schwebende kanonische Namen (CNAME)-Einträge. Sobald Hazy Hawk die Kontrolle über diese Sub-Domains erlangt, nutzt es das inhärente Vertrauen legitimer Domains, um schädliche Inhalte zu hosten. Seine Operationen beinhalten oft die Umleitung von Benutzern durch TDSs, um Betrug, Malware und irreführende Push-Benachrichtigungen zu verbreiten. **Kürzlich veröffentlichte Berichte:** • Bewölkt mit der Möglichkeit, vergessene DNS-Einträge zu kapern, um Scam-Akteure zu aktivieren
	Dieser finanziell motivierte Bedrohungsakteur nutzt seit Februar 2023 gekaperte Domains für Investitionsbetrug. Sie betten diese Domains in kurzlebige Facebook-Anzeigen auf mehreren Kontinenten ein und richten sich an Opfer in über 30 Sprachen, darunter Englisch, Italienisch, Polnisch, Türkisch und Spanisch. Der Angreifer nutzt den Angriffsvektor „Sitting Ducks“, um seriöse Domains zu kapern, mit denen er seine betrügerischen Websites vor Sicherheitsforschern schützt. Bis Oktober 2024 hat Infoblox fast 5.000 entführte Domains identifiziert, die mit diesem Akteur in Verbindung stehen. **Kürzlich veröffentlichte Berichte:** • Aufdeckung von TTP-Mustern von Akteuren und der Rolle von DNS bei Anlagebetrug • DNS-Räuber kapern Domains zur Versorgung ihrer Angriffsinfrastruktur

	Reckless Rabbit ist ein Investment-Betrüger, der Opfer über bösartige Facebook-Anzeigen anlockt. Es verwendet wörterbuchbasierte RDGAs und zielt auf Einzelpersonen in mehreren Ländern ab, darunter Österreich, Belgien, Dänemark, Frankreich, Polen, Schweden, das Vereinigte Königreich und andere. Der Akteur verwendet RDGAs und gefälschte Empfehlungen. **Kürzlich veröffentlichte Berichte:** • Aufdeckung von TTP-Mustern von Akteuren und der Rolle von DNS bei Anlagebetrug
	Dieser Phishing-Akteur führt Investitionsbetrugskampagnen durch, die auf Wörterbuch-basierten RDGAs beruhen und beliebte Dienste nachahmen. Der Akteur betreibt einen eigenen Domain-Cloaking-Dienst, um Benutzerüberprüfungen durchzuführen, und zielt auf osteuropäische Länder wie Rumänien, Russland, Polen und andere ab. **Kürzlich veröffentlichte Berichte:** • Aufdeckung von TTP-Mustern von Akteuren und der Rolle von DNS bei Anlagebetrug
	Dieser Akteur identifiziert verlassene Cloud-Ressourcen und nutzt sie für verschiedene bösartige Aktivitäten. Hasty Hawk ist dafür bekannt, Domains zu kapern, die in wohltätigkeitsbezogenen und DHL-bezogenen Kampagnen verwendet werden, die über Google-Anzeigen verbreitet werden. Hasty Hawk verwendet in erster Linie „bulletproof“ Hosting-Netzwerke wie Proton66 in Verbindung mit einem TDS, um Nutzer zu den Inhalten weiterzuleiten. **Kürzlich veröffentlichte Berichte:** • DNS-Räuber kapern Domains zur Versorgung ihrer Angriffsinfrastruktur
	Vacant Viper betreibt das 404TDS und nutzt es, um Malware und andere schädliche Inhalte zu verbreiten. Vacant Viper kapert Domains, die aufgrund falsch konfigurierter DNS-Nameserver anfällig sind – ein Fehler, den die Forscher von Infoblox „Sitting Ducks“ nennen – und integriert sie in seine bösartige TDS-Infrastruktur. **Kürzlich veröffentlichte Berichte:** • Wer hätte das gedacht? Domain-Hijacking ist so einfach
	Dieser böswillige Adtech-Akteur nutzt WordPress-Sicherheitslücken aus und verbreitet Malware, Phishing-Seiten, gefälschte Apps und unerwünschte Inhalte. Sie betreiben ein umfangreiches TDS, das Push-Benachrichtigungen, Pop-ups und Weiterleitungen innerhalb eines Browsers umfasst und auch dann noch Anzeigen schaltet, wenn der Nutzer die ursprüngliche Seite bereits verlassen hat. **Kürzlich veröffentlichte Berichte:** • The Vexing and Vicious: Die unheimliche Beziehung zwischen WordPress-Hackern und einer Adtech-Kabale

MORPHING MEERKAT

Morphing Meerkat ist ein globaler Spam-Akteur hinter einer fortschrittlichen Phishing-as-a-Service-Plattform (PhaaS). Dieser Akteur verwendet DNS-MX-Einträge, um den E-Mail-Dienstanbieter des Opfers zu identifizieren und dynamisch gefälschte Anmeldeseiten bereitzustellen. Morphing Meerkat nutzt kompromittierte WordPress-Websites sowie offene Weiterleitungsschwachstellen auf Adtech-Servern aus.

Kürzlich veröffentlichte Berichte:

- Eine Phishing-Erzählung über DOH- und DNS-MX-Missbrauch

FALLSTUDIE: KOORDINATION ZWISCHEN WORDPRESS-HACKERN UND DER VEXTRIO VIPER CABAL

Infoblox hat kürzlich eine komplexe Allianz zwischen **WordPress-Hackern und einem Netzwerk bösartiger Adtech-Unternehmen** aufgedeckt, insbesondere VexTrio's TDS.

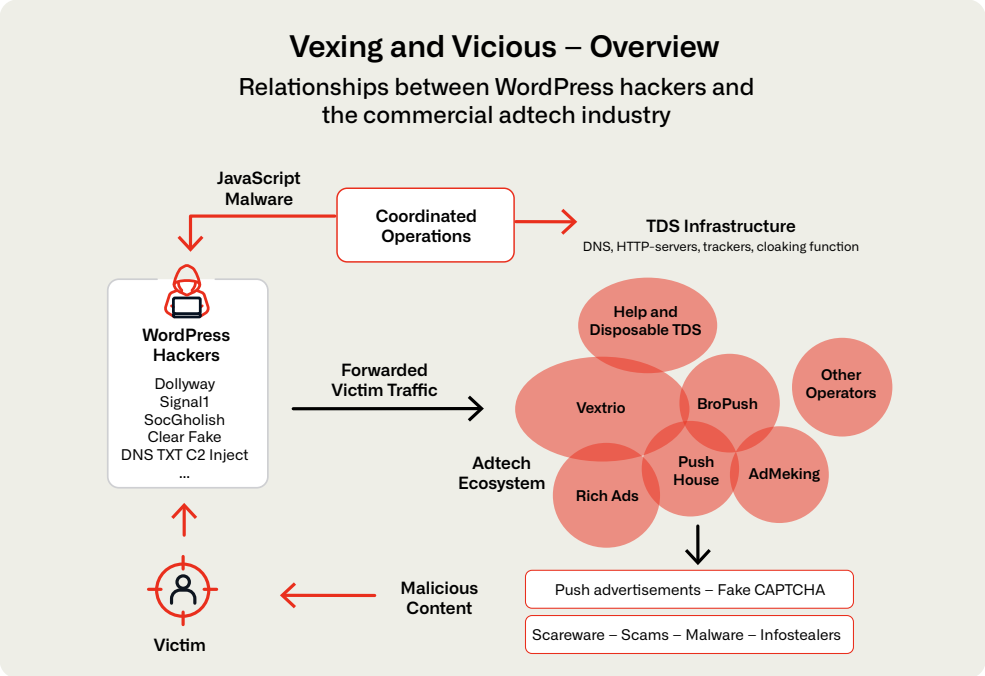


Abbildung 1. Beziehung zwischen WordPress-Hackern und der kommerziellen Adtech-Branche

Was ist passiert?

- **Schnelle Migration:** Als VexTrios TDS im Herbst 2024 ausfiel, wechselten mehrere Malware-Akteure gleichzeitig zu einem scheinbar neuen TDS namens „Help TDS“. Weitere Analysen ergaben, dass Help TDS nicht unabhängig, sondern eng mit VexTrio verknüpft ist und Infrastruktur- und Softwarekomponenten gemeinsam nutzt.
- **Koordinierte Operation:** Infoblox analysierte 4,5 Millionen DNS TXT-Eintragsantworten von kompromittierten Websites über sechs Monate. Dies enthüllte zwei unterschiedliche Command-and-Control-Server (C2), die beide auf russisch verbundener Infrastruktur gehostet werden, was auf eine koordinierte Operation zwischen WordPress-Hackern und der VexTrio-Kabale hindeutet.

- **Beteiligung kommerzieller Adtech-Unternehmen:** Mehrere Adtech-Unternehmen, darunter Los Pollos, Partners House, BroPush und RichAds, wurden als mit den Operationen von VexTrio verflochten identifiziert. Diese Unternehmen erleichterten die Verbreitung von schädlichen Inhalten über Smartlinks und Push-Benachrichtigungen.

Die Untersuchung hebt die ausgeklügelte und anpassungsfähige Natur von Cyberkriminellen-Netzwerken hervor, die kompromittierte WordPress-Seiten und kommerzielle Adtech-Infrastrukturen nutzen. Sie unterstreicht die Bedeutung von DNS-Telemetrie und gemeinschaftlichen Anstrengungen bei der Aufdeckung und Minderung solcher Bedrohungen.

ABSCHNITT 3: BÖSARTIGE DNS-TECHNIKEN

Die in Abschnitt 2 genannten Bedrohungsakteure verwenden DNS auf verschiedene Weise und mit bestimmten Zielen. Sobald Infoblox eine bedrohungsbezogene Domain entdeckt, ordnen Analyseprozesse und Expertenprüfungen der Domain bekannte bösartige Techniken zu. Die folgende Tabelle bietet einen Überblick über die gängigsten DNS-Techniken, die von Infoblox Threat Intel bedrohungsrelevanten Domains zugewiesen werden.

DNS-Techniken und bedrohungsbezogene Domains Zeitraum: Januar 2025 bis Juni 2025	
Von Maschinenalgorithmen generierte Domains (RDGA, DDGA und DGA)	54,7 %
Domains, die zur Umleitung des Datenverkehrs verwendet werden	11%
CNAME- oder Alias-Domains	5,8 %
Lookalikes	5,1 %
Gekaperte Domains	5,1 %
Domains, die in bösartigen SMS verwendet werden	4,2 %
Domains, die im Rahmen eines TDS erstellt wurden	1,8 %
Domains, die für C2 und Exfiltration verwendet werden	< 0,4 %

Tabelle 2. DNS-Techniken, die bedrohungsrelevanten Domains zugewiesen sind

Viele dieser Techniken überschneiden sich während einer Bedrohungskampagne und werden Teil umfassenderer Taktiken der Akteure, um ihre Ziele zu erreichen. In diesem Bericht gehen wir näher auf vier gängige DNS-Techniken ein, erläutern ihre Verwendung und warum sie gefährlich sind:

- Verwendung von Domains innerhalb von TDSs
- Hijacking von Domains, um Vertrauen zu stehlen.
- Lookalike-Domains, um Opfer zu täuschen
- DNS-Tunneling für C2 und Exfiltration

TRAFFIC-VERTEILUNGSSYSTEME BIETEN EIN GEFÄHRLICHES MASS AN UMGEHUNG

DNS spielt eine zentrale Rolle bei TDS, indem es Benutzer basierend auf verschiedenen Attributen wie Geolokalisierung, Gerätetyp oder Sicherheitslage verdeckt durch mehrere Zwischenebenen umleitet – oft ohne ihr Wissen. DNS spielt eine grundlegende Rolle bei der Bestimmung, wie und wohin der Netzwerkverkehr geleitet wird. Seriöse Anbieter von TDS sind meist in den Bereichen digitale Werbung oder Adtech zu finden. Der Name Adtech (kurz für Advertising Technology) bezieht sich auf die Tools, Plattformen und Software, die zur Verwaltung, Durchführung und Analyse digitaler Werbekampagnen verwendet werden.

Genau wie bekannte legale Werbetechnologien (z. B. Google AdSense) liefert bösartige Adtech die richtigen Inhalte zur richtigen Zeit an die richtige Zielgruppe, um die Effektivität ihrer Kampagnen zu steigern. Diese Art von Cyberbedrohung wird von spezialisierten Organisationen mit zahlreichen Partnern und umfangreichen finanziellen Mitteln durchgeführt.

Top-TDS-Betreiber nach Verbindungsanteil	
Name des Schauspielers	**Teilen von Verbindungen**
Vextrio Viper	72,8 %
VANE VIPER	68,4 %
Venal Viper	72,5 %
Unbekannter Akteur	64,8 %
Vero Viper	60,5 %
Tiano Gambling	50,9 %

Tabelle 3: TDS-Betreiber und der Prozentsatz der Kundenverbindungsversuche, die sie erhielten

Im Mittelpunkt dieser Aktivitäten steht ein TDS, das Opfer profiliert und sie an bösartige Werbetreibende weiterleitet, während Bedrohungsforscher auf eine Scheinwebsite umgeleitet werden.

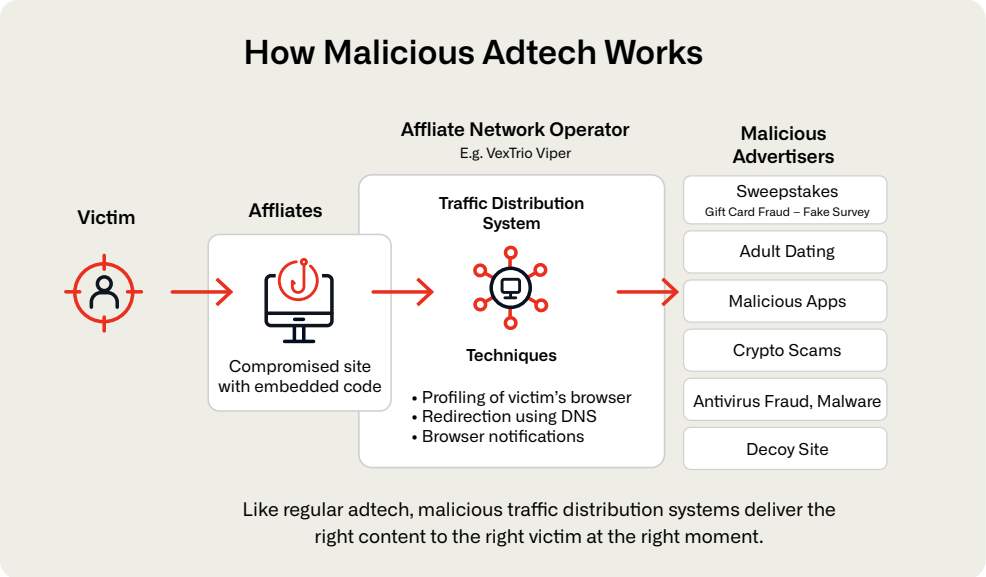


Abbildung 2: Ein Überblick über die drei Akteure im Bereich bösartige Adtech: Affiliates, Betreiber und bösartige Werbetreibende.

Es gibt mehrere Gründe, warum bösartige Adtech-Technologien schädlich sind und ein wichtiger Schwerpunkt für Sicherheitsabteilungen in Unternehmen sein sollten:

Bösartige Adtech ist ein schnell wachsender, aber wenig beachteter Bedrohungsvektor

Angreifer nutzen zunehmend bösartige Werbenetzwerke als kostengünstigen Dienst, um Malware und andere schädliche Inhalte zu verbreiten. Diese Anzeigen können zu verschiedenen Arten von Angriffen führen, darunter Drive-by-Downloads, Phishing-Websites, Datendiebstahl und Exploit-Kits (siehe Tabelle 4: TDS-Betreiber und bereitgestellte bösartige Inhalte).

Da der größte Teil der Sicherheitsbranche auf einen „Patient-Zero"-Ansatz setzt – das Sammeln von Telemetriedaten während (z. B. Sandboxing) oder nach (z. B. forensischer Intelligenz) einem Angriff – sind die daraus resultierenden Gegenmaßnahmen auf Artefakte beschränkt, die von diesem anfänglichen Kompromittierungspunkt entdeckt wurden. Diese Einschränkung macht TDSs zu effektiven Werkzeugen zur Umgehung der Erkennung, da Akteure kontinuierlich die bösartigen Inhalte, die sie bereitstellen, ändern und Bedrohungsforscher auf Köder-Websites umleiten. Folglich sind TDSs zu einer der am wenigsten gemeldeten Bedrohungen in der Cybersicherheitsbranche geworden.

Groß angelegte Infrastrukturen, die schwer zu stören sind

Organisationen, die bösartige Adtech einsetzen, bauen häufig eine Infrastruktur in beträchtlichem Umfang auf, darunter Zehntausende schnell wechselnde Domains, die darauf ausgelegt sind, Nutzer umzuleiten und sie dazu zu verleiten, Browser-Push-Benachrichtigungen zu akzeptieren. Diese Vorgänge werden häufig in mehrere Einheiten aufgeteilt, um Cyberkriminalität zu begehen und gleichzeitig rechtliche Untersuchungen zu vermeiden. Einige Betreiber, wie beispielsweise VexTrio Viper, sind seit Jahren erfolgreich und hochprofitabel – und ihre Aktivitäten zeigen keine Anzeichen einer Abschwächung.

Bösartige Adtech-Technologien bergen Risiken für Unternehmen

Bösartige Adtech-Technologie täuscht Opfer, indem sie beliebte Marken imitiert oder Inhalte anbietet, auf die sie gerne zugreifen möchten, und sie so dazu verleitet, ihre Wachsamkeit zu verringern und riskante Interaktionen einzugehen. Obwohl diese Bedrohungen in der Regel von Websites mit Kundenkontakt ausgehen, können sie leicht in Unternehmensumgebungen eindringen und die persönlichen Geräte der Mitarbeiter gefährlichen Inhalten aussetzen. Dadurch können Angreifer Erkundungen durchführen oder sich als Unternehmensbenachrichtigungen ausgeben, was das Risiko für Unternehmensnetzwerke erhöht.

DNS-Operatoren	Malware	Betrug	Phishing	Gekaperte Domain
Vacant Viper	X	X		X
VANE VIPER	X	X	X	
Vextrio Viper	X	X	X	X
Hasty Hawk			X	X
Sophisticated Chickens			X	X
Black TDS	X		X	
Parrot TDS	X			
R0bl0ch0n TDS		X		

Tabelle 4. TDS-Betreiber und bereitgestellte bösartige Inhalte

Beispiel für TDS bei der Arbeit:

Wenn ein Opfer eine kompromittierte Website von einem mobilen Gerät oder Endpunkt aus besucht, kann der Betreiber ein gefälschtes CAPTCHA anzeigen, um das Opfer dazu zu verleiten, Browser-Push-Benachrichtigungen von einem bösartigen Werbetreibenden zu akzeptieren. Diese Benachrichtigungen können dann weitere betrügerische Inhalte liefern, wie Aufforderungen zum Herunterladen nicht verifizierter Software, zur Weitergabe persönlicher Informationen oder zur Eingabe von Organisationsanmeldeinformationen.

Da das TDS Profile eingehender Opfer erstellt, können SOC-Analysten oder Bedrohungsforscher, die gängige Sicherheitstools verwenden, diese Benachrichtigungen oder schädlichen Inhalte möglicherweise nicht erkennen. Stattdessen werden sie möglicherweise auf eine Schein-Site umgeleitet, auf der legitimes Material angezeigt wird.

Aufgrund der Überschneidungen zwischen beruflicher und privater Internetnutzung hat sich bösartige Werbetechnologie zu einem wesentlichen Faktor für Cyberkriminalität entwickelt, insbesondere auf Mobilgeräten, Tablets, BYOD-Geräten und ungeschützten Ressourcen.

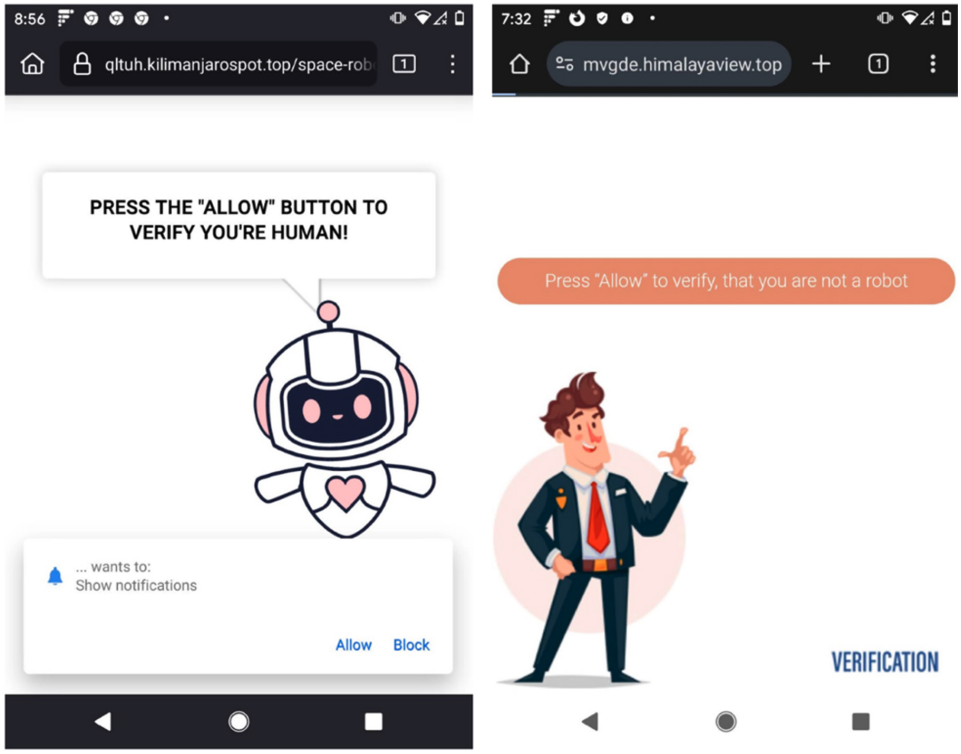


Abbildung 3: Beispiele für die Landingpage von VexTrio Viper, die den Benutzer dazu bringt, Push-Benachrichtigungen auf seinem Gerät zu akzeptieren; beide wurden beim Surfen auf `germannautica[.]com`

Von Traffic Distribution Systems genutzte Domains

In den letzten 12 Monaten hat Infoblox Threat Intel über 1 Million Indikatoren entdeckt, die von 168 böswilligen Adtech-Betreibern in ihrem TDS verwendet wurden. Diese Indikatoren umfassen mehrere Techniken, darunter RDGAs, Weiterleitungen, gekaperte Domains, Lookalikes und andere.

Von böswilligen Adtech-Betreibern verwendete TDSs können ziemlich groß sein. Viele umfassen über 10.000 Domains, einige sogar über 100.000. Die Größe eines TDS korreliert jedoch nicht unbedingt mit seiner Verbreitung oder seinem Bedrohungsgrad. Vigorish Viper betreibt ein riesiges und wachsendes Netzwerk von 170.000 aktiven Domains, zielt aber hauptsächlich auf Opfer in China, Hongkong und Macau ab. Venal Viper gehört zwar nicht zu den fünf größten Domains, ist aber eine der am häufigsten in Kundennetzwerken abgefragten Domains – 65 % aller Infoblox-Kunden haben in den letzten 12 Monaten eine Venal Viper-Domain abgefragt.

Störung von TDS

Schädliche Adtech-Technologien, die TDSs verwenden, sind erfolgreich, weil sie sich als legitime Werbung tarnen, Opfer täuschen und der Erkennung durch Sicherheitstools entgehen, die auf der Identifizierung bekannter bösartiger Verhaltensweisen durch Simulationen oder Patient-Zero-Daten beruhen. Im Gegensatz dazu können DNS-Einträge Aufschluss darüber geben, wann und wie eine neue bösartige Infrastruktur konfiguriert wird.

Forscher, die Echtzeit- und historische DNS-Daten in Verbindung mit innovativer Datenwissenschaft nutzen, können verdächtige oder bösartige Domains identifizieren, bevor eine Nutzlast übermittelt wird, einschließlich solcher, die in bösartiger Adtech verwendet werden.

DNS-basierte Informationen geben Aufschluss über die Infrastruktur hinter der Bedrohung, beispielsweise darüber, wie das TDS funktioniert und den Datenverkehr umleitet. Im Gegensatz zu anderen Sicherheitsmethoden können DNS-basierte Sicherheitsimplementierungen bösartige Adtech proaktiv aufdecken und verhindern, dass mit dem Internet verbundene Endgeräte damit interagieren.

Einfach ausgedrückt, bricht der DNS-basierte Schutz durch Fokussierung auf die Angreiferinfrastruktur die Versorgungskette zwischen bösartigen Werbetreibenden und Opfern – und bietet langfristigen Schutz, anstatt nur auf die neuesten Nutzdaten zu reagieren.

DOMAIN-HIJACKING ZUM VERTRAUENSDIEBSTAHL

Bedrohungsakteure kapern bestehende Domains in erster Linie, um die Glaubwürdigkeit und das Vertrauen legitimer Domains auszunutzen. Sobald der Widersacher die Kontrolle hat, können gekaperte Domains verwendet werden, um überzeugende Phishing-Websites zu erstellen, von Suchmaschinen priorisiert zu werden, Spam-Filter zu umgehen oder Betrug auszuführen.

Infoblox Threat Intel entdeckte mehrere Methoden, wie Akteure Domains kapern, und die Instrumente, die sie verwenden, um Benutzer zu täuschen.

Sitting-Duck-Angriffe

Sitting Ducks-Angriffe haben in den letzten Jahren an Prävalenz gewonnen. Im Jahr 2024 schätzte Infoblox Threat Intel, dass mehr als **1 Million Domains für diesen Angriff anfällig** sind. Während einer gründlichen Recherche in der zweiten Jahreshälfte 2024, **wurden 70.000 Domains entdeckt, die aus einem Pool von 800.000** anfälligen Domains entführt wurden. Dies unterstreicht das Ausmaß des Problems und die Notwendigkeit robuster Sicherheitsmaßnahmen.

Mehrere Bedrohungsakteure setzen diese Techniken systematisch ein. Die Leichtigkeit, mit der diese Angriffe ausgeführt werden können – kombiniert mit den Schwierigkeiten, mit denen Sicherheitsteams konfrontiert sind, sie zu erkennen – macht sie besonders gefährlich.

Zu den Akteuren, die diesen Angriff bekanntermaßen ausnutzen, gehören VexTrio Viper, Vigorish Viper, Horrid Hawk und Hasty Hawk. Diese Gruppen haben die Wirksamkeit von Sitting-Ducks-Angriffen unter Beweis gestellt und damit die Notwendigkeit einer erhöhten Wachsamkeit und verbesserter Sicherheitsmaßnahmen zur Abwehr dieser Bedrohungen deutlich gemacht.

Dangling CNAMES

Anfang 2025 nutzten Bedrohungsakteure Weiterleitungskonfigurationen auf renommierten Domains wie `cdc[.]gov` und mehreren Universitäten in den USA aus. Das war möglich, weil Organisationen Cloud-Anwendungen (z. B. CDNs), die von Drittanbietern (wie Microsoft Azure) gehostet wurden, außer Betrieb genommen hatten, während ihre DNS-Aliase (CNAME-Einträge) aktiv blieben.

Böswillige Akteure wie Hazy Hawk nutzten diese Lücke in der DNS-Hygiene aus, indem sie neue Inhalte auf demselben CDN erstellten. Das Motiv war einfach: Durch die Nutzung des guten Rufs des ursprünglichen Domain-Alias konnten sie Google und andere Suchmaschinen dazu bringen, die schädlichen Inhalte zu indexieren und in die Suchergebnisse aufzunehmen.

LOOKALIKE- UND TYPOSQUATTED-DOMAINS TÄUSCHEN BENUTZER

Lookalike-Domains sind leicht veränderte Domainnamen, die registriert wurden, um Benutzer zu täuschen. Sie geben sich häufig als legitime Marken, Mitarbeiterkommunikation, Lieferketten oder andere vertrauenswürdige Partner aus und verursachen dadurch erhebliche Probleme.

Angreifer verwendeten Lookalike-Domains in SMS-Nachrichten, Telefonanrufen, Direktnachrichten in sozialen Medien, E-Mails und QR-Codes. Kürzlich haben sie die Multi-Faktor-Authentifizierung (MFA) ins Visier genommen, da diese von Spielern bis hin zu Marktplätzen für digitale Währungen immer häufiger genutzt wird. Weitere Beispiele umfassen das Umgehen von Enterprise-MFA oder den Missbrauch von Domainnamen von beliebten Identitätszugriffsplattformen.

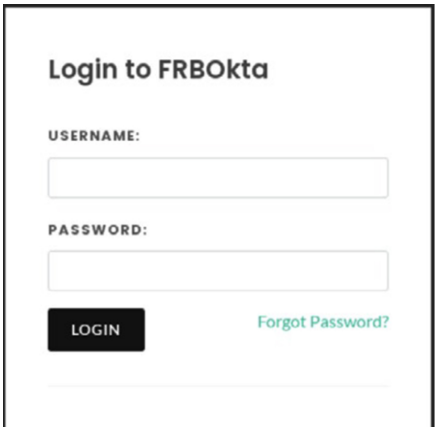


Abbildung 4. MFA-Nachricht von einer Lookalike-Domain

Lookalike-Domains sind zu einem deutlich größeren Problem geworden, da es über **1.500 Top-Level-Domains gibt, was für die meisten Unternehmen die Kosten für die Überwachung aller Variationen erhöht.**

Darüber hinaus können in Unternehmen mehrere Gruppen Domains registrieren, ohne dass eine Übersicht darüber besteht, wer was tut. Sicherheitsteams könnten annehmen, dass eine ähnlich aussehende Domain vom Helpdesk- oder Cloud-Anwendungsteam erstellt wurde, jedoch könnte die neue Domain tatsächlich von einem Angreifer konfiguriert worden sein, um Kunden zu phishen.

Mangelnde Fachkenntnisse in Sicherheitsteams führen häufig zu einem Bedarf an schnellen Lösungen durch Managed Services. Leider sind Lookalike-Domains kein leicht zu lösendes Problem. Selbst erfahrene Sicherheitsteams sind weiterhin mit ihnen konfrontiert, und eine effektive Überwachung erfordert erhebliche Sorgfalt.

Infoblox: Ähnliche Techniken identifiziert	
	**Homografen oder Homoglyphen** verwenden visuell ähnliche Zeichen aus verschiedenen Zeichensätzen, wie kyrillisch oder griechisch (z. B. das Ersetzen von „o“ durch „0“). Die Technik ist effektiv, weil die eingefügten Zeichen nicht immer klar unterscheidbar sind.
	**Typosquats** beinhalten hinterhältige Tippfehler durch die Registrierung von Domains, die beliebten Websites sehr ähnlich sind (z. B. Ersetzen von „amazonn[.]ϕ fi < “ durch „amazon[.]com“), um Benutzer auf eine betrügerische Website zu leiten.
	**Combosquats** kombinieren bekannte Marken- oder Firmennamen mit anderen Schlüsselwörtern, wie „Mail“, „Sicherheit“ oder „Support“. Combosquatting ist etwa 100-mal häufiger als Typosquatting.
	**Soundsquats** sind die neueste Form von Lookalike-Bedrohungen, bei denen Domainnamen verwendet werden, die laut ausgesprochen ähnlich klingen (z. B. „hsbsee[.]com“ statt „hsbc[.]com“). Dadurch werden Benutzer bei der Verwendung von Smart-Geräten wie Google Home, Siri und Alexa getäuscht.

DNS-TUNNELING WIRD VON BEDROHUNGSAKTEUREN, PENTESTERN UND LEGITIMEN SICHERHEITSTOOLS VERWENDET.

DNS-Tunneling kodiert Daten in DNS-Abfragen und -Antworten und ermöglicht verdeckte Kommunikation, die oft für C2-Operationen und Datenexfiltration ausgenutzt wird.

Während Infoblox in einigen Monaten über 480 einzigartige DNS-Tunneling-Domains beobachtete, wurden zwischen Juni 2024 und Juni 2025 durchschnittlich mehr als 100 einzigartige Domains im Zusammenhang mit DNS-Tunneling pro Monat entdeckt. Neben der Nutzung durch Cyberkriminelle wird DNS-Tunneling auch bei legitimen Penetrationstests und Sicherheitstools eingesetzt. Die folgende Liste bietet einen Überblick über verbreitete DNS-Tunneling-Tools mit C2-Funktionen.

+100

unique DNS tunneling domains found monthly—benign and malicious

- **Cobalt Strike** ist ein weit verbreitetes Pentest-Tool mit einem DNS-C2-Modul. Es wird von Red Teams und Bedrohungsakteuren eingesetzt und verwendet Hex-codierte Abfragen mit optional anpassbaren Präfixen wie „post“, „api“ oder „dx“.
- **Dnscat2** ist ein Tool zum Erstellen verschlüsselter DNS-Tunnel. Es ist in METASPLOIT enthalten, einem Open-Source-Tool für Penetrationstests.
- **DNS Exfiltrator** ist ein Tool, das Daten in DNS-Abfragen für die Exfiltration kodiert und den potenziellen Missbrauch von DNS in praktischen Szenarien veranschaulicht. Es verwendet TXT-Einträge, erlaubt nur eine unidirektionale Kommunikation und wird über die Befehlszeile initiiert. Infoblox hat die Nutzung durch einen Bedrohungsakteur nicht beobachtet und hält sie aufgrund des unidirektionalen Mechanismus für unpraktisch.
- **Sliver** ist ein plattformübergreifendes C2-Framework mit DNS-Tunneling-Funktionen, das häufig in Gegnersimulationen und bösartigen Kampagnen eingesetzt wird.
- **Weasel** ist ein weniger dokumentiertes DNS-Tunneling-Tool, das vom Red Team von Facebook entwickelt wurde. Es unterstützt heimliche Datenexfiltration und C2 und wird typischerweise in speziellen Red-Teaming-Aktivitäten eingesetzt. Es verwendet A- und AAAA-Einträge für die Kommunikation.
- **Pupy** ist ein Open-Source-, plattformübergreifendes Remote-Access-Tool mit DNS-Tunneling-Unterstützung, das historisch in Spionagekampagnen gegen staatliche und Unternehmensorganisationen eingesetzt wurde. Es verwendet A-Records für die Kommunikation.
- **Iodine** ist ein bekanntes Tool zum Tunneln von IPv4-Verkehr über DNS, das in Penetrationstests eingesetzt und manchmal auch für Angriffe missbraucht wird, beispielsweise von staatlichen Akteuren für C2-Zwecke. Iodine verwendet A-, TXT-, CNAME- und MX-Einträge zur Kommunikation.
- In letzter Zeit sind **mehrere automatisierte Penetrationstest-Tools** von Anbietern wie Cymulate und AttackIQ auf den Markt gekommen. Infoblox hat in Kundennetzwerken Domains entdeckt, die mit diesen Anbietern in Verbindung stehen.
- **Antiviren- und Antispam-Tools** verwenden auch DNS als Mechanismus, um nachzuschlagen, ob ein Domain- oder Datei-Hash bösartig sein könnte. Eine Anfrage kann das Format haben: „<domain>.<guid>.<avdomain>“ oder „<file hash>.<guid>.<avdomain>“ mit der Antwort NXDOMAIN, wenn der Domain- oder Datei-Hash nicht in einer bekannten Malware- oder Spam-Liste enthalten ist, oder 127.0.0.X, wenn er in einer solchen Liste steht.

Sicherheitsteams benötigen ein Skalpell, um DNS-Tunneling zu stoppen.

Das Verständnis und die Eindämmung von DNS-Tunneling sind für den Schutz von Unternehmen vor Cyberbedrohungen und die Gewährleistung der Einhaltung gesetzlicher Anforderungen wie dem Payment Card Industry Data Security Standard (PCI DSS), dem Health Insurance Portability and Accountability Act (HIPAA) und der Datenschutz-Grundverordnung (DSGVO) von entscheidender Bedeutung. Aufgrund der weit verbreiteten Verwendung von DNS-Tunneling-Tools haben viele Sicherheitsteams Schwierigkeiten, den DNS-Verkehr effektiv zu überwachen und zu kontrollieren.

Infoblox erkennt oft DNS-Tunneling in Netzwerken, auch in solchen mit Firewalls der nächsten Generation oder Technologien vom Typ Secure Access Service Edge (SASE). Obwohl sich die Erkennung von DNS-Tunneling durch diese Technologien verbessert hat, bleiben einige Komplexitäten bestehen. CDNs, die Verwendung neuer Lookalike-Domains und die Erweiterung legitimer DNS-C2-Tools erschweren die Erkennung und Blockierung aller C2-Aktivitäten.

Aus diesem Grund benötigen Sicherheitsteams präzise, zielgerichtete Tools anstelle von umfassenden, allgemeinen Maßnahmen. Um dieser Herausforderung zu begegnen, sind DNS-Schutzlösungen unerlässlich, die aktive Bedrohungsakteure verfolgen und kontinuierlich aktualisierte maschinelle Lerntechniken einsetzen.

ABSCHNITT 4: HERAUSFORDERUNGEN FÜR VERTEIDIGER

Zusätzlich zu den herkömmlichen gegnerischen DNS-Techniken wie TDSs, Domain-Hijacking, Lookalike-Domains und DNS-Tunneling stehen Verteidiger – seien es SOC-Analysten, Risikomanager oder CISOs – vor einer wachsenden Zahl von Herausforderungen.

Dieser Abschnitt bietet einen Überblick über wichtige Trends wie den Einsatz von adversarialer KI, Markenschutz und den zunehmenden Druck durch neue Compliance-Vorgaben. Vor allem werden die Möglichkeiten hervorgehoben, die DNS-basierte Bedrohungsinformationen zur Bewältigung dieser Herausforderungen bieten.

88%

of AI-generated malware evades detections[4]

ADVERSARIAL AI UMGEHT BESTEHENDE SICHERHEITSKONTROLLEN

Generative KI (GenAI) – insbesondere große Sprachmodelle (LLMs) – treibt einen Wandel in der Cybersicherheit voran. Angreifer werden zunehmend von GenAI angezogen, weil es die Hürde für die Erstellung irreführender und überzeugender Inhalte senkt. Sie nutzen es, um die Effektivität von Eindringungstechniken wie Social Engineering und der Umgehung von Erkennungssystemen zu verbessern.

Um diese neuen Herausforderungen durch KI zu bewältigen, benötigen Sicherheitsteams ein neues Maß an Verlässlichkeit – beispielsweise DNS-basierte Telemetrie – das nicht durch KI verändert oder verschleiert werden kann und ausreichende Transparenz in der Kontrollkette gewährleistet.

Aktuelle Beispiele für bösartige KI: Deepfake-Betrügereien

Ende 2024 warnte das FBI, dass Kriminelle generative KI verwenden, um in großem Umfang Betrug zu begehen und ihre Machenschaften glaubwürdiger zu gestalten.[5] GenAI-Tools wie das Klonen von Stimmen reduzieren erheblich den Zeit- und Arbeitsaufwand, der erforderlich ist, um Zielpersonen mit scheinbar vertrauenswürdigen Audiobotschaften zu täuschen. Besonders besorgniserregend ist die Leichtigkeit, mit der Cyberkriminelle auf diese Tools zugreifen können, kombiniert mit den fehlenden Sicherheitsvorkehrungen. Das Klonen von Stimmen wurde in verschiedenen Szenarien eingesetzt, darunter groß angelegte Deepfake-Videos für Kryptowährungsbetrug und die Nachahmung von Stimmen bei gezielten Telefonaten.

Fallstudie: Reckless Rabbit's unverantwortliche Verwendung von Deepfakes, um japanischsprachige Opfer zu erreichen

Infoblox Threat Intel berichtete im September 2024 über eine Kampagne zur Entführung von YouTube-Konten, bei der Deepfake-Videos von Elon Musk für Krypto-Betrug verwendet wurden. Eine ähnliche Technik wurde nun von einem verfolgten Akteur namens **Reckless Rabbit** übernommen, der Deepfakes direkt in betrügerische Websites einbettet.

Reckless Rabbit richtete seinen Fokus kürzlich auf **japanischsprachige Nutzer**, indem es gefälschte Investitionsprogramme über KI-generierte Nachrichtenartikel bewarb. Diese Websites enthalten Deepfake-Videos von Persönlichkeiten des öffentlichen Lebens wie **Elon Musk** und **Masayoshi Son** sowie erfundene positive Bewertungen, um die Glaubwürdigkeit zu steigern.

---

4 Kriminelle nutzen generative künstliche Intelligenz, um Finanzbetrug zu erleichtern. FBI-Warnnummer: I-120324-PSA, 3. Dezember 2024

5 KI könnte 10.000 Malware-Varianten generieren und in 88 % der Fälle der Erkennung entgehen, Lakshmanan, Ravie, The Hacker News, 23. Dezember 2024.

Zuvor hatte der Akteur **osteuropäische Nutzer** mit RDGA-basierten Domains und Facebook-Anzeigen ins Visier genommen, um sie auf gefälschte Nachrichten zu locken, die aus einfachem Text und Bildern bestanden.

Abbildung 5. Kürzlich entdeckte Deepfake-Seite

Reckless Rabbit verwendet gefälschte Artikel mit **Deepfake-Videos und japanischen Untertiteln**, indem er sich als große Medien wie Yomiuri Shimbun ausgibt. Diese Artikel bewerben eine gefälschte Investmentplattform namens **„Finance Legend“** mit einem Registrierungsbutton, der auf ein Kontaktformular weiterleitet. Der Akteur kontaktiert die Opfer wahrscheinlich, um mit dem Versprechen hoher Renditen Einzahlungen zu erbitten.

KI-gestützte Chatbots

Akteure wählen ihre Opfer oft sorgfältig aus, indem sie Informationen über deren Interessen sammeln, um sie für hochgradig personalisierte Betrugsmaschen vorzubereiten. Nach einer ersten Erkundung erstellen sie Smishing-Nachrichten, die die Opfer in von Chatbots gesteuerte Unterhaltungen führen. Diese Gespräche können sich über Wochen hinziehen und ungewöhnliche Schritte beinhalten, wie beispielsweise die Bitte um ein „Daumen hoch“ auf YouTube oder ein Repost in den sozialen Medien – Taktiken, die darauf abzielen, die Anfälligkeit des Opfers einzuschätzen. Mit jeder positiven Interaktion manipuliert der Akteur einen fiktiven „Kontostand“, um ihn zu erhöhen. Wenn das Opfer versucht, Geld abzuheben, fordert der Akteur Zugriff auf sein Kryptowährungskonto an und missbraucht dabei das im Laufe der Zeit aufgebaute Vertrauen, um die Gelder des Opfers zu stehlen. KI-gestützte Chatbots ermöglichen es Akteuren, diese Gespräche zu automatisieren und ihre Abläufe effizient zu skalieren.

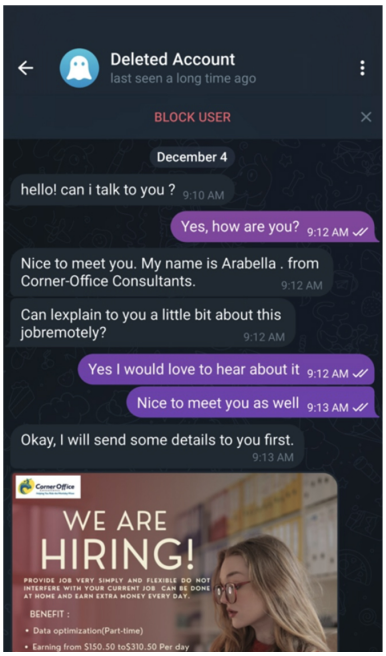


Abbildung 6. Beispiel für feindselige Chat-Nachrichten, bei denen eine Kombination aus KI/LLMs und halbautomatisierten Chatbot-Interaktionen zum Einsatz kommt.

Code-Verschleierung und Umgehung

Bedrohungsakteure setzen zunehmend GenAI ein, um Malware auf neue Weise zu verschleiern, umzufunktionieren und zusammenzustellen, um der Erkennung zu entgehen. Dieser Ansatz beschleunigt die Erstellung von Bedrohungskampagnen und reduziert die technischen Fähigkeiten, die zum Aufbau effektiver Infektionsketten erforderlich sind. Laut einer Untersuchung von HP Wolf Security hat die Umgehung von Bedrohungen über E-Mails um etwa 11 % zugenommen.[6] Unterdessen berichtete ein renommierter Sicherheitsanbieter kürzlich, dass ein unangemessener LLM-Algorithmus in **88 %** der Fälle die Einstufung seines eigenen Malware-Klassifizierungsmodells von „bösartig“ in „harmlos“ geändert hat.[7] – ein wichtiger Indikator dafür, wie effektiv gegnerische KI aktuelle Erkennungsmodelle ausnutzen kann.

SCHUTZ DES MARKEN- UND UNTERNEHMENSRUFS

Marken und der Ruf einer Organisation sind strategische Vermögenswerte. Ein guter Ruf schafft Vertrauen bei den Kunden, erhöht die Glaubwürdigkeit auf dem Markt, zieht Partner und Investoren an und fördert den langfristigen Markenwert. Laut Forbes wird „die Reputation von Unternehmensführern durchweg als ihr wertvollstes Kapital eingestuft.“[8] Der Schutz einer Marke innerhalb des DNS ist jedoch mit mehreren Herausforderungen verbunden:

- **Eingeschränkte Sichtbarkeit außerhalb des Perimeters:** Die Überwachung von Domains erfordert nicht nur die Verfolgung der eigenen Domains, sondern auch die von Tausenden potenzieller Lookalikes oder Imitationen. So hat Infoblox im Mai 2025 beispielsweise 28.331 Lookalike-Domains entdeckt.
- **Von Menschen erstellte Lookalikes sind nach wie vor schwer zu erkennen:** Lookalike-Domains werden von Menschen sorgfältig ausgewählt und imitiert, wobei sie oft die Erkennungsfähigkeiten automatisierter Systeme übertreffen.
- **Manuelles Domain-Monitoring belastet die Ressourcen:** Sicherheitsteams fehlen oft die Ressourcen, um Warnungen manuell zu überwachen und effektiv zu reagieren. Ohne Automatisierung wird die Domainüberwachung zu einer Aufgabe mit hohem Aufwand und geringer Effizienz.
- **Jurisdiktionale Barrieren behindern die Durchsetzung:** 87 % der entdeckten Hochrisiko-Domains sind bei Unternehmen registriert, die vom Office of Foreign Assets Control (OFAC) sanktioniert wurden, wo die Gesetze der USA oder der Europäischen Union (EU) nicht gelten. Infolgedessen sind Domain- und Website-Takedowns oft ineffektiv.

28,331
lookalike domains detected by Infoblox in May 2025

Um diese Hindernisse zu überwinden, müssen Sicherheits- und Marketingteams mit DNS-Experten zusammenarbeiten, die über tiefgehende Einblicke in die globale DNS-Nutzung verfügen und DNS-basierte Intelligenz nutzen können. Diese Zusammenarbeit ermöglicht es ihnen, Bedrohungen für digitale Assets, die den Ruf oder die Marke des Unternehmens widerspiegeln, zu überwachen, zu erkennen und zu beheben.

COMPLIANCE-DRUCK UND DNS-HERAUSFORDERUNGEN FÜR SICHERHEITSTEAMS

Netzwerk- und Sicherheitsteams stehen unter zunehmendem Druck durch die Weiterentwicklung bewährter Verfahren und neuer Mandate wie **EU NIS2** und **NIST SP 800-81 Rev. 3**, die branchenübergreifend gelten und eine umfassendere Aufsicht erfordern – einschließlich der DNS-Infrastruktur.

6 Hacker nutzen bildbasierte Malware und GenAI, um die E-Mail-Sicherheit zu umgehen, Coker, James, Infosecurity Magazine, 16. Januar 2024.

7 KI könnte 10.000 Malware-Varianten generieren und in 88 % der Fälle der Erkennung entgehen, Lakshmanan, Ravie, The Hacker News, 23. Dezember 2024.

8 Die Bedeutung der Markenreputation: 20 Jahre bis zum Aufbau, fünf Minuten bis zum Ruin, Blanchard, Paul, Forbes, 27. Dezember 2019.

Diese Frameworks stellen mehrere Herausforderungen dar:

- **Betriebliche Komplexität:** NIS2 schreibt Risikobewertungen, 24-Stunden-Vorfallberichterstattung und kontinuierliche Überwachung vor – Anforderungen, die für Teams ohne zentralisierte Transparenz oder Automatisierung schwierig sind. NIST SP 800-81 Rev. 3 erfordert außerdem die Bereitstellung dedizierter DNS-Server und die Verschlüsselung des internen und externen DNS-Datenverkehrs.
- **Fragmentierte Tools:** Vorhandene Tools sind häufig über lokale, Cloud- und Remote-Umgebungen hinweg fragmentiert, was zu Richtlinienkonflikten und Transparenzlücken führt. DNS-Richtlinien (z. B. Antwortrichtlinienzonen oder RPZs) müssen konsistent angewendet werden, um Unterbrechungen zu vermeiden.
- **Begrenzte Ressourcen:** SOC-Teams sind mit dem Alarmaufkommen überfordert und verfügen nicht über kontextbezogene Einblicke. Der Schwerpunkt von NIS2 auf Früherkennung und schnelle Reaktion stellt eine zusätzliche Belastung für bereits überlastete Teams dar – insbesondere für diejenigen, denen es an Transparenz auf DNS-Ebene mangelt.
- **Budgetbeschränkungen:** Die Einhaltung der Vorschriften erfordert Investitionen in Tools, Schulungen und DNS-Protokollierung. Dennoch müssen Organisationen diese Kosten angesichts engerer Budgets rechtfertigen, auch wenn die DNS-Protokollierung für die Forensik und die Reaktion auf Vorfälle von entscheidender Bedeutung ist.

Sicherheitsteams benötigen einen unkomplizierten Ansatz, um neue Compliance-Anforderungen zu erfüllen. Die Aktivierung prädiktiver Bedrohungsinformationen und die Implementierung von Kontrollen auf DNS-Ebene vereinfachen nicht nur die Einhaltung von NIST SP 800-81 Rev.3 und NIS2, sondern stehen auch im Einklang mit umfassenderen Sicherheitsrahmen wie dem NIST Cybersecurity Framework (CSF) und Zero Trust. Vor allem verbessert es die globale Bedrohungsprävention, Transparenz und die Reduzierung des Aufwands für Sicherheitsmaßnahmen.

NÄCHSTE SCHRITTE

Infoblox bietet Sicherheitsexperten zahlreiche Möglichkeiten, unsere von Experten erstellten Bedrohungsinformationen zu erkunden und ihre Umgebung mit prädiktiver Intelligenz zu schützen.

Für Bedrohungsforscher:

- Weitere Informationen zur Threat Intel-Forschung von Infoblox finden Sie unter https://www.infoblox.com/de/threat-intel/.
- Sprechen Sie mit uns auf Mastodon unter infobloxthreatintel@infosec.exchange.
- Greifen Sie auf unsere Forschungsergebnisse und Indikatoren auf GitHub zu: https://github.com/infobloxopen/threat-intelligence/.

Für Sicherheitsteams:

- Fordern Sie einen DNS-Sicherheitsworkshop an: https://insights.infoblox.com/de-resources/der/infoblox-workshop-security-workshop-de.
- Weitere Informationen zu Infoblox Threat Defense finden Sie unter https://www.infoblox.com/de/products/threat-defense/.

VERWENDETE TERMINOLOGIE

Adtech: Abkürzung für **Advertising Technology,** bezieht sich auf die **Software, Tools und Plattformen,** die von Marken, Agenturen, Verlagen und Plattformen zur Planung, Durchführung, Verwaltung und Analyse **digitaler Werbekampagnen** verwendet werden. Es ist das Backbone des Online-Werbe-Ökosystems.

BYOD: Bringen Sie Ihr eigenes Gerät mit

C2: Command and Control

CDN: Ein Content Delivery Network ist ein **Netzwerk aus geografisch verteilten Servern** , die zusammenarbeiten, um digitale Inhalte (wie Websites, Videos, Bilder und Skripte) **schnell, zuverlässig und sicher** an Benutzer je nach ihrem Standort zu liefern.

CNAME: Canonical Name-Eintrag ist eine Art von **DNS** (**Domain Name System**)-Eintrag, der **einen Domainnamen** (**ein Alias**) **auf einen anderen Domainnamen** (**den kanonischen Namen**) **abbildet.** Er wird verwendet, um eine Domain oder Subdomain auf eine andere Domain zu verweisen, anstatt direkt auf eine IP-Adresse zu verweisen.

DDGA: Dictionary Domain Generation Algorithm (Algorithmus zur Generierung von Wörterbuch-Domains)

DDI: **DNS, DHCP und IP-Adressmanagement** (**IPAM**) – drei kritische Netzwerkdienste, die zusammenarbeiten, um die **automatisierte und zentralisierte Verwaltung von IP-Adressräumen und Namensauflösung** in Unternehmensnetzwerken zu ermöglichen.

DGA: Domain Generation Algorithm (Algorithmus zur Domain-Generierung)

DNS: Domain Name System

DNS-Abfragen: Eine **DNS-Abfrage** (Domain Name System Query) ist eine Anfrage eines Geräts (in der Regel ein Computer oder Handy), um einen **menschenlesbaren Domainnamen** (wie www.google.com) in eine **maschinenlesbare IP-Adresse** (wie 142.250.190.68) zu übersetzen, damit es eine Verbindung zum richtigen Server im Internet herstellen kann.

DSGVO: Datenschutz-Grundverordnung

HIPAA: Health Insurance Portability and Accountability Act

LLM: Großes Sprachmodell

MFA: Multi-Faktor-Authentifizierung

MX-Missbrauch: Hierbei handelt es sich um böswillige Aktivitäten, die MX-Einträge (Mail Exchange) ausnutzen oder missbrauchen.

NIST: National Institute of Standards and Technology (Nationales Institut für Standards und Technologie)

NOD: neu beobachtete Domains

OFAC: **Office of Foreign Assets Control**, eine Abteilung des **US-Finanzministeriums.** Es verwaltet und erzwingt **Wirtschafts- und Handelssanktionen** auf der Grundlage der US-Außenpolitik und der nationalen Sicherheitsziele.

OSINT: Open-Source-Intelligence

PCI DSS: Payment Card Industry Data Security Standard (Datensicherheitsstandard für die Zahlungskartenbranche)

PhaaS: Phishing-as-a-Service

RDGA: Registered Domain Generation Algorithm (Algorithmus zur Generierung registrierter Domains)

SASE: Secure Access Service Edge

TDS: Traffic Distribution System (Traffic-Verteilungssystem)

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.

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

+1 408 986 4000
www.infoblox.com/de

Version: 20250730