

Fehlerbehebung bei häufigen DNS-Anforderungstypen, die in Umbrella Reports verfügbar sind

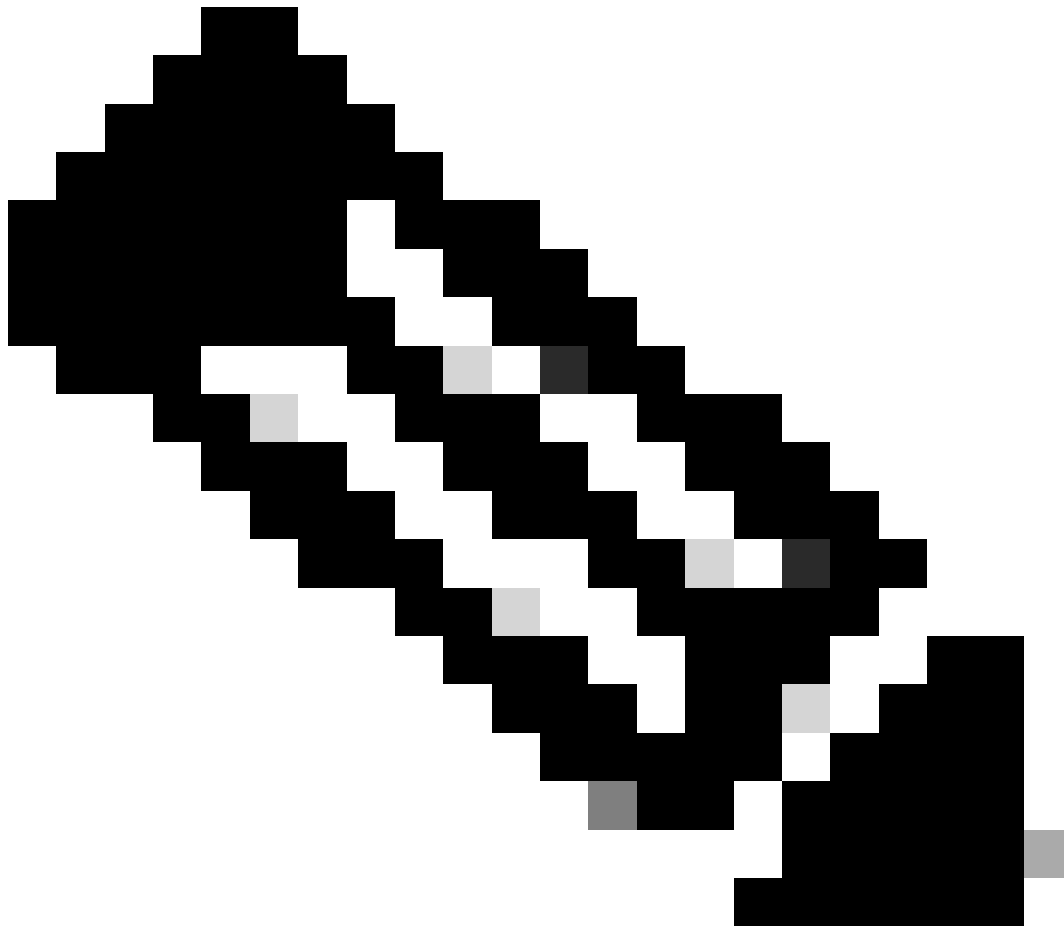
Inhalt

[Einleitung](#)

[Zulässige Sicherheitskategorien in übergeordneten Berichten](#)

Einleitung

In diesem Dokument werden die DNS-Anforderungstypen beschrieben, die erfasst und in einem Bericht aufgeführt werden können. Jeder Datensatztyp hat seinen eigenen Zweck in der DNS-Infrastruktur. Beim Denken an DNS ist der erste Eintragstyp, der einem einfällt, der A-Eintrag, bei dem es sich um die IPv4-IP-Adresse handelt, die zum Hostnamen der Domäne gehört.



Anmerkung: Diese Liste ist keineswegs erschöpfend. Eine vollständigere Liste mit den jeweiligen RFC für jeden Datensatztyp finden Sie hier:
https://en.wikipedia.org/wiki/List_of_DNS_record_types

Bezüglich blockierter Sicherheitsdomänen beachten Sie, dass Cisco Umbrella die Datensätze A, AAAA, ANY, CNAME, PTR, SRV, PRIVATE, SPF/DNS, NULL, SIG, HTTPS (Type65) und TXT blockiert, sodass Abfragen nach anderen Datensatztypen (MX, SOA und NS) zulässig sind, obwohl die Kategorie blockiert ist. Anfragen nach MX-Datensätzen von Domänen, die als "DNS Tunneling VPN" kategorisiert wurden, werden jedoch abgelehnt.

Zulässige Sicherheitskategorien in übergeordneten Berichten

Cisco Umbrella hat sich der DNS-Sicherheit verpflichtet. Es wurde festgestellt, dass DNS-Eintragstypen schädliche Verbindungen (z. B. A/AAAA) oder Tunneling-Datenverkehr (TXT, SRF usw.) unterstützen oder die Umgehung von Standard-DNS (Typ 65 usw.) ermöglichen. Einige Datensatztypen, bei denen es sich um Referenzdatensätze wie MX, SOA, NS handelt, sind auch

dann zulässig, wenn sie in einer Sicherheitskategorie gekennzeichnet sind. Wenn Sie glauben, dass ein nicht gesperrter Datensatztyp gesperrt werden sollte, kontaktieren Sie uns unter umbrella-support@cisco.com auf Anfrage. Wir überwachen auf neue Bedrohungstypen, um sicherzustellen, dass alle Datensätze durchgesetzt werden, die eine schädliche Verbindung herstellen können - ohne Anforderungstypen zu blockieren, die Informationsanforderungen an den Eigentümer der Domäne oder an Mail-Server behindern.

Um zu überprüfen, ob eine Anfrage für eine "zulässige" Malware auf eine alternative Anfrage für einen Datensatztyp zurückzuführen ist, öffnen Sie die Aktivitätssuche, und fügen Sie die Spalte für den DNS-Datensatztyp hinzu. Dies wird für die Berichterstellung transparent dargestellt - und deutet nicht auf einen Schutzausfall oder eine Abdeckungslücke hin.

Für Content-Filterkategorien werden andere Typen als AAAA, A-Datensätze nicht blockiert. Ziellisten blockieren auch nicht alle Datensatztypen, NS ist beispielsweise nicht blockiert.

Um den Datensatztyp einer Anforderung in der Aktivitätssuche anzuzeigen, wechseln Sie in die Spalte "DNS-Typen".

Wenn eine Domäne "blockiert" wird, werden die Adresssatztypen A und AAAA abgefragt. Diese geben IP-Adressen zurück, die zu den Umbrella-Blockseiten gehören. Abfragen der DNS-Eintragstypen ANY, CNAME, PTR, SRV, SIG oder TXT geben "REFUSED" zurück. (Hinweis: Bei der Abfrage nach Domänen, die als dynamischer DNS klassifiziert sind, werden die Adresseintragstypen A und AAAA blockiert, aber Abfragen nach anderen DNS-Eintragstypen geben nicht "VERWEIGERT" zurück.) Die vollständige Liste der Typen, für die wir "VERWEIGERT" zurückgeben, lautet wie folgt: 3-5,7-10, 12, 16, 30, 33, 38, 64, 65, 99, 245, 253, 255, 65280-65534.

Ausnahmen:

- DNS-Tunneling-Domänen "blockieren" alle Eintragstypen.
- Dynamische DNS-Kategorie: Es werden nur A-/AAAA-Einträge blockiert.

DNS-Suchtypen und -funktionen

DNS-Suchtyp	Beschreibung	Funktion
A	IPv4-Adressdatensatz	Gibt eine 32-Bit-IP-Adresse zurück, die normalerweise den Hostnamen einer Domäne einer IP-Adresse zuordnet, aber auch für DNSBLs und zum Speichern von Subnetzmasken verwendet wird.
AAAA	IPv6-Adressdatensatz	Gibt eine 128-Bit-IP-Adresse zurück, die den Hostnamen einer Domäne einer IP-Adresse zuordnet

DNS-Suchtyp	Beschreibung	Funktion
BELIEBIGER	Alle zwischengespeicherten Datensätze	Wenn die Domäne nicht blockiert wird, gibt Umbrella NOTIMP für Anforderungen dieses Typs zurück.
CNAME	Kanonischer Namensdatensatz	Alias eines Namens für einen anderen: Die DNS-Suche wird fortgesetzt, indem die Suche mit dem neuen Namen wiederholt wird.
MX	Mail Exchange Record	Ordnet einen Domänennamen einer Liste von Nachrichtenübertragungsagenten für diese Domäne zu
NS	Name Server-Datensatz	Delegiert eine DNS-Zone zur Verwendung der angegebenen autoritativen Namenserver
PTR	Zeigerdatensatz	Zeiger auf einen kanonischen Namen, der nur den Namen zurückgibt und zum Implementieren umgekehrter DNS-Suchvorgänge verwendet wird
SIGNIEREN	Unterschrift	Signaturdatensatz
SOA	Beginn des Zulassungsdokuments	Gibt autoritative Informationen über eine DNS-Zone an, einschließlich des primären Namensservers, der E-Mail-Adresse des Domänenadministrators, der Seriennummer der Domäne und mehrerer Zeitgeber zum Aktualisieren der Zone
SRV	Service Locator	Generalisierter Servicestandortdatensatz, der für neuere Protokolle verwendet wird, anstatt protokollspezifische Datensätze wie MX zu erstellen
TXT	Textdatensatz	Enthält zusätzliche Daten, manchmal von Menschen lesbar, die meiste Zeit maschinenlesbar sind, wie opportunistische Verschlüsselung, DomainKeys, DNS-SD usw.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.