infoblox

Threat Intel

LÖSUNGSHINWEIS

DNS-BASIERTE BEDROHUNGSJAGD ZUR FRÜHZEITIGEN ENTDECKUNG VON BEDROHUNGEN, BEVOR SIE ZUSCHLAGEN

ZAHLEN UND FAKTEN

- Der Umfang von DNS ist enorm. Mittlerweile gibt es 1.589 Top-Level-Domains, wobei jeden Tag rund 200.000 neue Domains erstellt werden.
- 81 % der Unternehmen haben in den letzten 12 Monaten einen oder mehrere Phishing-Angriffe erlebt (CRA 2023 Global State of Cybersecurity Study)
- 75 % der Unternehmen waren laut dem „State of Phish"-Bericht von Proofpoint aus dem Jahr 2024 bereits mit Smishing-Angriffen (SMS-Phishing) konfrontiert
- Lookalike-Domains werden häufig bei Phishing- und Spear-Phishing-Angriffen verwendet. Laut Hacker News haben chinesische Hacker im Jahr 2022 im Rahmen eines massiven Phishing-Angriffs 42.000 gefälschte Domains verwendet.
- Es sind aber nicht nur Lookalike-Domains. Angreifer registrieren Domains oft mehrere Monate im Voraus, um sie für eine breite Palette von Angriffen zu nutzen. Ein Beispiel ist das Toolkit „Decoy Dog", das von Infoblox Threat Intel entdeckt wurde. Viele der russischen C2-Domains, die von Decoy Dog verwendet werden, wurden im Voraus eingerichtet und bereits im Herbst 2022 von Infoblox entdeckt.
- Infoblox findet und blockiert jede Woche etwa 25.000 neue Lookalike-Domains.
- **Fazit:** Es besteht ein entscheidender Bedarf an Threat Intelligence, die proaktiv diese neu entstehenden Domains identifiziert, die für zukünftige Angriffe genutzt werden könnten

HERAUSFORDERUNGEN

Angreifer bevorzugen Phishing, weil es günstig ist und sie nur eine Person brauchen, die einen Fehler macht und auf den Link klickt. SMS-Phishing-Angriffe, die gemeinhin als Smishing bezeichnet werden, haben in letzter Zeit an Häufigkeit zugenommen. Die Angreifer betreiben mittlerweile massive, ausgefeilte Smishing-Operationen. Lookalike Domains werden häufig für Phishing- und Spear-Phishing-Angriffe verwendet. So setzten im Jahr 2022 chinesische Hacker 42.000 gefälschte Domains für eine massive Phishing-Kampagne ein.

Während Phishing und Lookalike-Domains ein wachsendes Problem darstellen, gibt es andere Fälle, in denen Domains bereits Monate im Voraus registriert wurden, bevor sie für eine Vielzahl von Angriffen verwendet wurden. Ein solches Beispiel ist das kürzlich entdeckte Toolkit „Decoy Dog", bei dem es sich um eine Reihe von Beacons handelt, die DNS zur Kommunikation mit der C&C-Infrastruktur ausnutzen. Das Toolkit verwendet das Pupy RAT, das in der Vergangenheit häufig mit nationalstaatlichen Akteuren in Verbindung gebracht wurde. Viele der Domains, die mit Decoy Dog in Verbindung gebracht werden, sind seit April 2022 aktiv und waren langlebig und unauffällig, sodass sie mit herkömmlichen Sicherheitstools schwer zu entdecken waren.

Zur Erkennung solcher Angriffe, bei denen die Domains lange vor dem Start der Angriffe eingerichtet werden, ist ein anderer Ansatz erforderlich.

DNS-BASIERTE BEDROHUNGSJAGD

Die DNS-basierte Bedrohungsjagd nutzt groß angelegte DNS- und Analyseverfahren, um die Infrastruktur des Gegners aufzuspüren, bevor ein tatsächlicher Angriff beginnt. Genauer gesagt kann darüber Folgendes geleistet werden:

- Auffinden von Domains, die für Kunden neu sind, und Einstufung als neu oder verdächtig anhand von Metadaten wie Registrar, TLD-Domains, SSL-Zertifikate, Name Server, Registrierungsverhalten usw.
- Verwendung von veröffentlichten Hinweisen Dritter (z. B. CISA-Hinweisen) und deren Erweiterung, um mithilfe von DNS-Metadaten weitere Indikatoren zu finden. In einer kürzlich veröffentlichten CISA-Ankündigung hat Infoblox beispielsweise 13 zusätzliche Domains gefunden, die nicht in der Bekanntmachung enthalten waren, und zwar allein durch die Einbeziehung von DNS-Metadaten. Dies hat erheblich zur Reduzierung eines potenziellen Bedrohungsvektors beigetragen.

DNS-basierte Bedrohungssuche schützt vor verdächtigen Domains, und das Wochen oder Monate, bevor sie als bösartig bestätigt und für Angriffe genutzt werden.

PROAKTIVER SCHUTZ MIT BLOXONE THREAT DEFENSE

Aufgrund der einzigartigen Position von Infoblox im Abfragepfad kann die Lösung die Kommunikationsabsicht beobachten, analysieren und blockieren, um so einen proaktiven Schutz zu bieten. Infoblox, der Marktführer und Experte für DNS, verfolgt die Infrastruktur von Angreifern und prüft DNS-Protokolle, um verdächtige Aktivitäten in einem frühen Stadium des Bedrohungslebenszyklus zu erkennen, wenn eine „Kompromittierungsabsicht“ besteht und bevor der eigentliche Angriff beginnt. Dadurch kann Infoblox Threat Intel neue Domains und Lookalike-Domains, die für eine böswillige Nutzung vorgesehen sind, in der Vorbereitungsphase identifizieren und sie mehrere Wochen oder Monate lang als verdächtig einstufen, bevor andere Sicherheitsorganisationen/Anbieter sie als bösartig identifizieren können. Der Hauptgrund für diese Verzögerung zwischen der proaktiven Einstufung verdächtiger Domains durch Infoblox und der Erkennung durch andere Sicherheitslösungen ist, dass diese Lösungen das Traffic-Verhalten oder den Inhalt dieser Domains bewerten. Und das ist in der Regel erst relevant, wenn die Bedrohung bereits aktiviert ist.

Hochrisiko-Domains

Sobald das Team bestimmte Domains als verdächtig einstuft, nimmt Infoblox sie in einen Feed namens „Infoblox High Risk“ (also Infoblox Hochrisiko) auf, der mit BloxOne Threat Defense verfügbar ist. So können sich unsere Kunden präventiv vor neuen und aufkommenden Bedrohungen schützen. Es handelt sich dabei um Feeds mit Indikatoren für hochgradig verdächtige Domains, für die noch keine bösartigen Aktivitäten bestätigt wurden, die aber Anzeichen dafür aufweisen, dass sie von Bedrohungsakteuren im Rahmen ihrer Bewaffnungsphase erworben wurden und in Zukunft für eine bösartige Nutzung aktiviert werden könnten. Die Feeds werden in drei Kategorien eingeteilt:

- **Verdächtige Lookalikes** – Eine Art verdächtige Domain, die legitimen Domains ähnelt und möglicherweise für zukünftige Phishing-Aktivitäten genutzt werden könnte.
- **Verdächtige NOED** – Steht für „Newly Observed Emergent Domains“ (neu beobachtete aufkommende Domains); eine Art hochriskante, verdächtige Domain, die erst kürzlich im Traffic der Kunden beobachtet wurde. (Daher auch der Ausdruck „Emergent“)
- **Verdächtige Domains** – Dies sind andere Domains, die verdächtig erscheinen, aber nicht dem Profil einer verdächtigen Lookalike oder NOED entsprechen.

Infoblox hat die Daten zu verdächtigen aufkommenden Domains Anfang November 2022 eingeführt und im Jahr 2023 ganze 19,4 Millionen aktive verdächtige Indikatoren entdeckt und kategorisiert. Die Zahl der aktiven verdächtigen Domains steigt mit der Zeit immer weiter an. Neben diesem hohen Volumen ist ein weiteres wichtiges Kriterium die Qualität der Verdachtseinstufung: Von den Millionen als verdächtig eingestuften Domains wurden nur 0,0002 % als falsch positiv gekennzeichnet.

Dank dieses Konzepts zum Blockieren verdächtiger Domains konnten Infoblox-Kunden bereits frühzeitig auf der Grundlage spezifischer Sicherheitshinweise reagieren, darunter Decoy Dog und MFA-Angriffe wie Oktapus. Viele der Domains, die mit dem Decoy Dog-Toolkit in Verbindung stehen, wurden bereits im Herbst 2022 entdeckt und in die Feeds für verdächtige Domains in BloxOne Threat Defense aufgenommen. Kunden von BloxOne Threat Defense Advanced, die ihre Richtlinie zum Blockieren der Feeds für verdächtige Domains eingestellt hatten, waren also schon damals vor vielen der C2-Domains geschützt.

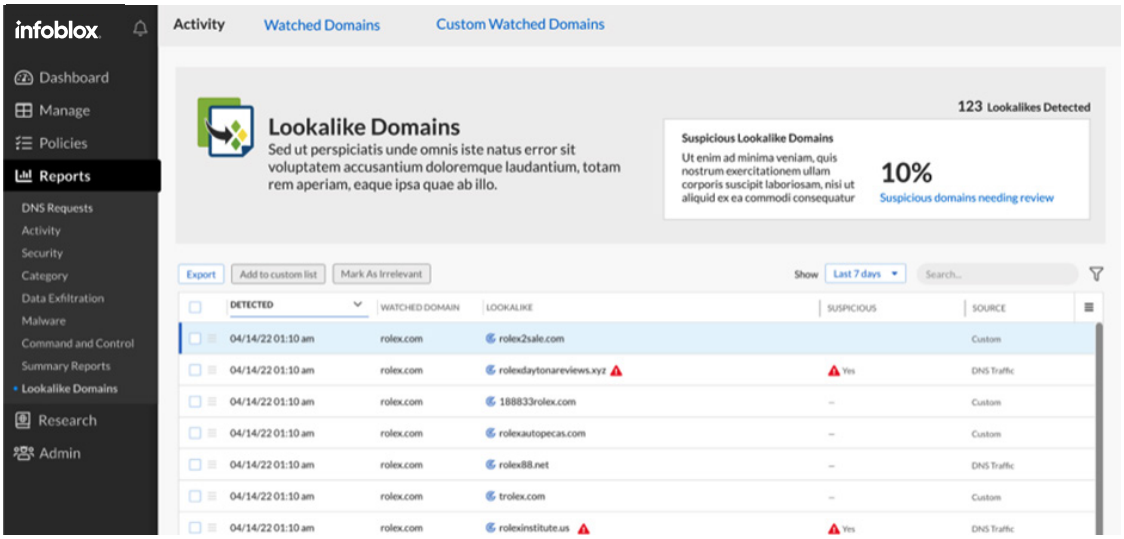
Infoblox hat im Jahr 2023 insgesamt 19,4 Millionen Domains in die Feeds für verdächtige Domains aufgenommen und damit das Risiko künftiger Angriffe erheblich reduziert.

Lookalike-Domains

Zusätzlich zu verdächtigen Feeds können Infoblox-Kunden die in BloxOne Threat Defense integrierte Sicherheitsfunktion für Lookalike-Domains nutzen, um proaktiv auf Social Engineering basierende Bedrohungen zu identifizieren und zu stoppen. Hierbei werden oft Lookalike-Domains für fortgeschrittene gezielte Angriffe genutzt, die darauf abzielen, in das Unternehmen einzudringen, Kunden zu gefährden oder Ihre wertvolle Marke zu schädigen.

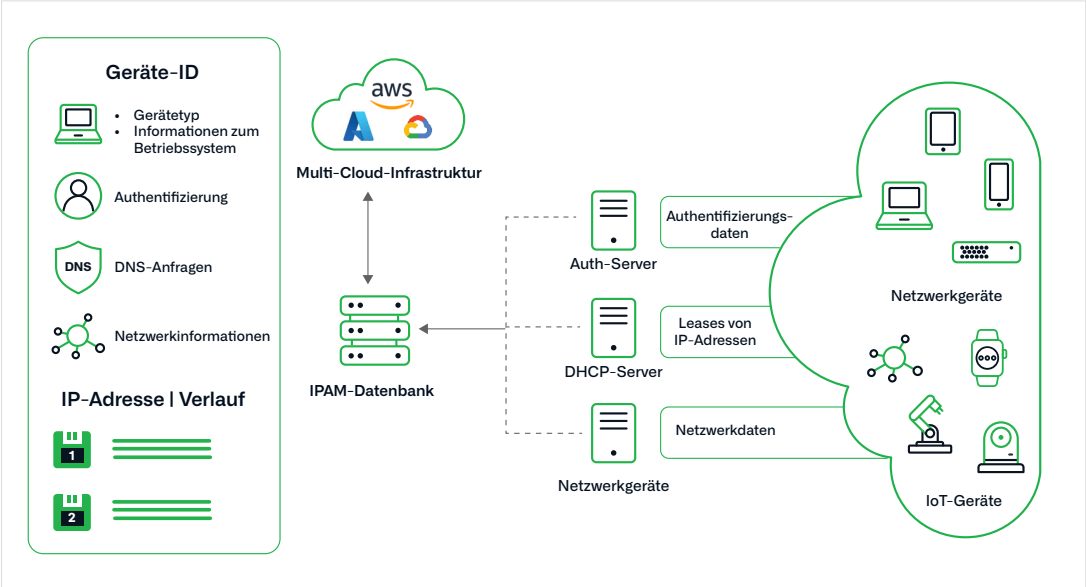
Kunden können die von ihrem eigenen Unternehmen oder von Partnern in der Lieferkette verwendeten Domains sowie andere Domains melden, die im Rahmen eines Cyberangriffs zur Täuschung von Benutzern, Partnern oder Kunden nachgeahmt werden könnten. Daraufhin beginnt Infoblox einen kontinuierlichen Überwachungsprozess für potenzielle Lookalike-Domains und analysiert die Registrierung, die Aktivitäten, den Verlauf und vieles mehr, um den Grad des Risikos zu bewerten. Diese Ergebnisse werden in einem interaktiven Dashboard dargestellt, damit Kunden schnell fundierte Entscheidungen für die nächsten Schritte treffen können. Und diese Informationen werden ständig aktualisiert, um neue Lookalike-Domains oder Aktivitäten im Zusammenhang mit aktuell identifizierten Lookalike-Domains zu berücksichtigen.

Es ist ein separater „Take-Down"-Service verfügbar, der sich auf die engen, vertrauensvollen Beziehungen von Infoblox und unsere einzigartige Position in der globalen IT-Umgebung stützt. Dieser Service ermöglicht bedrohten Unternehmen eine angemessene Reaktion, um ihr finanzielles und markenbezogenes Risiko zu begrenzen. Die Infoblox Domain Mitigation Services umfassen Validierungsdienste, um zu bestätigen, dass ein Vorfall tatsächlich stattgefunden hat; Schadensbegrenzung durch Koordination mit wichtigen ISPs und Regulierungsbehörde sowie die Überwachung mit Berichterstattung, um die Bedrohungslandschaft besser zu verstehen und Ihre Sicherheit zu stärken. Aufgrund unseres guten Rufs in Bezug auf die Sorgfalt und Qualität der Untersuchungen beträgt die durchschnittliche Beseitigungszeit in einigen Regionen nur 24 Stunden. So können unsere Kunden viele Bedrohungen bereits im Vorfeld beseitigen und schnell wieder zum normalen Geschäftsbetrieb übergehen.



Einfache Benutzer- und Gerätezuordnung

Das Blockieren der Kommunikation zu diesen Domains ist der erste Schritt. Es ist jedoch ebenso wichtig, schnell herauszufinden, welche Geräte/Assets an dieser Kommunikation beteiligt sind. Die Synchronisierung von IPAM-Metadaten mit DNS bietet die dringend benötigte Transparenz, um festzustellen, woher die bösartigen Anfragen im Netzwerk stammen. Mithilfe von IPAM-Daten lässt sich leicht feststellen, ob die anomale DNS-Aktivität von Netzwerkgeräten wie Firewalls, Benutzergeräten oder jeder anderen Art von mit dem Netzwerk verbundenen Geräten stammt. Mit Infoblox lassen sich sogar Sicherheitsrichtlinien auf der Grundlage von IPAM-Metadaten einfach definieren.



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

+1 408 986 4000
www.infoblox.com

Version: 20240411v1