So verhindern Sie, dass Angreifer DNS gegen Sie nutzen

Das Domain Name System (DNS) ist für sämtliche digitalen Geschäftsprozesse unerlässlich, unabhängig von Branche, Standort, Größe und Produktpalette des jeweiligen Unternehmens. Mithilfe des DNS-Protokolls lassen sich benutzerfreundliche Domainnamen wie www.paloaltonetworks.com in maschinenlesbare IP-Adressen übersetzen – in diesem Fall 199.167.52.137. Ohne DNS müssten wir uns also für das Surfen im Internet lange Zahlenkombinationen merken, was die meisten wohl überfordern würde. Daher ist DNS für alle Unternehmen weltweit von fundamentaler Bedeutung. Netzwerkbetreiber können DNS-Datenverkehr nicht blockieren, sondern müssen ihn passieren lassen. Denn Netzwerke funktionieren ohne DNS nicht richtig.

Allerdings sind sich viele Sicherheitsexperten nicht darüber im Klaren, wie leicht und wie häufig DNS von Angreifern missbraucht wird. Im Gegenteil: Zahlreiche Sicherheitsteams untersuchen den DNS-Traffic nicht auf Bedrohungen, weil sie stillschweigend annehmen, dass von DNS-Abfragen über Port 53 keine Gefahr ausgeht. In anderen Unternehmen wird der DNS-Datenverkehr nicht analysiert, weil sein Volumen die internen Kapazitäten übersteigt und die Suche nach Anzeichen für DNS-basierte Bedrohungen angesichts des hierfür erforderlichen Zeit- und Personalaufwands der sprichwörtlichen Suche nach der Nadel im Heuhaufen gleicht.

Diese Praxis ist riskant, da DNS eine breite Angriffsfläche bietet und vielfach für die Einschleusung von Malware, die Kommunikation mit Command-and-Control-Servern (C2) und die Datenausschleusung verwendet wird. Hacker nutzen die Tatsache aus, dass DNS in der IT-Infrastruktur omnipräsent ist, und missbrauchen das System in verschiedenen Angriffsphasen. Wie Untersuchungen unseres Bedrohungsforschungsteams Unit 42 gezeigt haben, werden die C2-Aktivitäten von fast 80 % der Malware-Varianten über DNS initiiert. So können Angreifer zuverlässige Kommunikationskanäle einrichten, die sich nur mit Schwierigkeiten identifizieren und blockieren lassen. Dieses Problem wird noch dadurch verschärft, dass viele DNS-basierte Angriffe mittlerweile automatisch ablaufen.

Hier erweist es sich als erheblicher Nachteil, dass viele Sicherheitsteams keinen Einblick in den DNS-Traffic haben und somit nicht erkennen können, über welche Kanäle Hacker die Kontrolle über infizierte Geräte behalten. Da es Millionen von schädlichen Domains und raffinierte neue Methoden für die C2-Kommunikation wie beispielsweise das DNS-Tunneling gibt, wird der lückenlose Schutz des Unternehmens zu einer wahren Herkulesaufgabe. Außerdem wächst die Zahl der schädlichen Domains mit atemberaubender Geschwindigkeit, was zur Folge hat, dass statische Signaturen zur Bedrohungsabwehr nicht schnell genug erstellt oder aktualisiert werden können. Unter diesen Bedingungen haben Netzwerk- und Sicherheitsexperten größte Mühe, infizierte Systeme zu identifizieren und auf die Infektion zu reagieren. Und wenn dies schließlich gelingt, ist es möglicherweise schon zu spät, um die Ausbreitung der Malware oder den Diebstahl von Daten noch zu verhindern.

80 %

aller Malware nutzt DNS, um C2-Server ausfindig zu machen und dadurch den Diebstahl von Daten sowie die Einschleusung weiterer Schadprogramme zu ermöglichen.

Abbildung 1: Forschungsergebnis von Unit 42 zur DNS-Nutzung durch Angreifer

Die drei häufigsten Arten von DNS-Missbrauch

Um Angriffe auf Ihr Netzwerk abwehren und Ihr Sicherheitsrisiko minimieren zu können, müssen Sie zunächst darüber informiert sein, wie Cyberkriminelle DNS missbrauchen. Deshalb stellen wir Ihnen hier die drei häufigsten Varianten des DNS-Missbrauchs durch Angreifer vor. Dabei geht es vor allem um die Tarnung von C2-Aktivitäten, damit weitere Schadprogramme eingeschleust oder Daten unbemerkt ausgeschleust werden können.

Der Missbrauch von DNS für die C2-Kommunikation

Hierbei handelt es sich um die gängigste Form des Missbrauchs von DNS. Die Angreifer nutzen zunächst gängige Netzwerkprotokolle (darunter auch DNS), um ihre Malware zu verbreiten. Als Infektionsvektoren können dabei unter anderem Online-Werbeanzeigen oder in E-Mails eingebettete Links zu schädlichen URLs dienen. Nachdem das Gerät eines Benutzers auf diese Weise infiziert wurde, sendet die eingeschleuste Malware eine DNS-Anfrage an den Command-and-Control-Server des Angreifers. Auf diese Weise wird der infizierte Computer zu einem Bot unter der Kontrolle des Angreifers. Über die hergestellte Verbindung kann der Hacker dann mithilfe der Malware Kontodaten und andere vertrauliche Informationen stehlen oder einen Netzwerkscan durchführen, um andere anfällige Geräte zu identifizieren.

Vor Kurzem hat die Hackergruppe WINDSHIFT einen Cyberangriff auf Regierungsbehörden und kritische Infrastruktur im Nahen Osten durchgeführt, bei dem DNS für die C2-Kommunikation genutzt wurde. Technische Details und nähere Informationen zum Ablauf des WINDSHIFT-Angriffs finden sich in der einschlägigen Studie von Unit 42.

Malware mit Domain-Generation-Algorithmen (DGAs)

Die Zahl der Malware-Varianten mit DGAs wächst rasant. Schadprogamme dieser Art können nach dem Zufallsprinzip Listen mit leicht variierenden Domainnamen erzeugen. So lässt sich beispielsweise mithilfe eines DGA eine Liste mit Tausenden von Domainnamen erzeugen, bei denen es sich jeweils um eine leichte Abwandlung von www.bigbadguys.com handelt. Diese Algorithmen wurden von Angreifern entwickelt, um Malware in die Lage zu versetzen, eigenständig nach neuen Kanälen für die C2-Kommunikation zu suchen. Wie Unit 42 ermittelt hat, beinhalten 18 Prozent der beobachteten Malware-Varianten DGAs, die täglich Tausende von potenziellen C2-Domainnamen erzeugen. Diese große Zahl hindert Sicherheitsteams daran, die C2-Kommunikation effektiv zu unterbinden, da die Angreifer jeden beliebigen der vom DGA generierten Domainnamen registrieren und dann für den Datenaustausch mit ihrer Malware nutzen können. Infizierte Computer versuchen, Kontakt mit einigen der Domains auf der erzeugten Liste herzustellen, und erhalten im Erfolgsfall Befehle und Updates der Angreifer. Da bei diesen Angriffen in rascher Folge immer neue Domains für die C2-Kommunikation verwendet werden, sind herkömmliche Sicherheitsmaßnahmen wie schwarze Listen oder Reputationsfilter weitgehend wirkungslos.

DGAs versetzen Angreifer in die Lage, die Standorte ihrer C2-Server geheim zu halten und ihre Infrastruktur für kriminelle Aktivitäten wie Finanzbetrug und Identitätsdiebstahl zu nutzen. Weitere Informationen zu diesem Thema finden Sie in der DGA-Kurzinfo von Unit 42.

DNS-basierte Angriffe sind effektiv und werden immer zahlreicher. Bei den Malware-Varianten mit Domain-Generation-Algorithmen (DGAs) ist ein jährliches Wachstum von **124 %** zu verzeichnen.

Abbildung 2: Forschungsergebnisse von Unit 42 zum Einsatz von Domain-Generation-Algorithmen

DNS-Tunneling

Diese Methode wird von einer wachsenden Zahl von APT-Gruppen (Advanced Persistent Threats) eingesetzt. Um bestehende Sicherheitssysteme zu umgehen, zerlegen die Angreifer ihre schädlichen Inhalte in kleine Bruchstücke, die dann in DNS-Anfragen eingebettet werden. Mit dieser Methode lassen sich Datendiebstähle und C2-Kommunikation im normalen DNS-Datenverkehr tarnen. Sobald ein Gerät des anvisierten Unternehmens infiziert worden ist, veranlasst die Malware eine DNS-Anfrage. Der DNS-Server wird instruiert, eine Verbindung zum Server der Kriminellen herzustellen, wodurch ein Kanal für die Übertragung gestohlener Daten und die Übermittlung von Befehlen entsteht. Das Perfide an dieser Methode ist, dass die gesamte Kommunikation über vermeintlich harmlose DNS-Anfragen an DNS-Server innerhalb und außerhalb der Firewall des Unternehmens läuft. Die in den DNS-Anfragen verborgenen Daten bleiben unbemerkt. Hackergruppen wie OilRig haben DNS-Tunnel in den vergangenen Jahren in großem Umfang bei ihren Angriffen eingesetzt.

Die Defizite konventioneller Sicherheitsansätze

Zahlreiche gängige Maßnahmen zur Malware-Abwehr erweisen sich bei DNS-basierten Angriffen als unzureichend. Das liegt in den meisten Fällen vor allem daran, dass die diversen DNS-basierten Angriffsvektoren nicht ausreichend überwacht und gesichert werden. Viele Unternehmen kümmern sich nur um das reibungslose Funktionieren ihrer DNS-Infrastruktur, damit Nutzer jederzeit zuverlässigen Zugang zum Internet haben. Dabei vernachlässigen sie die Bedrohung durch Cyberkriminelle, die DNS zur Einschleusung von Malware oder für den Diebstahl von Daten missbrauchen. Ohne Lösungen und Prozesse zur DNS-Sicherung und -Überwachung sind diese Unternehmen DNS-basierten Angriffen schutzlos ausgeliefert.

Andere Sicherheitsteams setzen bei der Abwehr DNS-basierter Angriffe auf das Blacklisting von bekannten schädlichen Domains, basierend auf relativ statischen Bedrohungsdatenfeeds. Allerdings ist dieser Ansatz gegen die zunehmende Zahl von Malware-Varianten mit DGAs nur von begrenzter Effektivität. Wenn ständig neue, zufällig generierte Domains für die C2-Kommunikation genutzt werden, können konventionelle, signaturbasierte Cyberabwehr-Tools meist nicht Schritt halten. Eine begrenzte Signaturdatenbank bietet einfach nicht das nötige Maß an Skalierbarkeit, das zur Unterbindung DNS-basierter Angriffe erforderlich ist.

Auch wenn Bedrohungsdatenbanken täglich oder sogar stündlich um Bedrohungsindikatoren oder Artefakte aus externen Quellen erweitert werden, bietet dies kein ausreichendes Maß an DNS-Sicherheit. Erschwerend kommt hinzu, dass herkömmliche statische Sicherheitslösungen nicht genug Kontextinformationen über Bedrohungen im Netzwerk bereitstellen. Unter diesen Bedingungen verfügen Sicherheitsteams nicht über die nötigen Einblicke und ausreichende Ressourcen, um das enorme Volumen des DNS-Datenverkehrs effektiv auf Bedrohungen zu untersuchen.

Forschungsergebnisse von Unit 42 zur Hackergruppe OilRig

Bei OilRig handelt es sich um eine aktive, organisierte Angreifergruppe, deren Aktivitäten zuerst von Unit 42 aufgedeckt wurden. Die sorgfältig geplanten Operationen von OilRig dienen der Realisierung strategischer Zielsetzungen in verschiedenen Branchen und richten sich überwiegend gegen Unternehmen und Institutionen im Nahen Osten. Dabei wurden in einigen Fällen speziell die Lieferketten ins Visier genommen. Bedrohungsanalysen haben ergeben, dass die Gruppe ausgeklügelte Methoden für das DNS-Tunneling entwickelt hat und diese sowohl für die C2-Kommunikation als auch für die Ausschleusung von Daten nutzt. In diesem Zusammenhang sind besonders die beiden folgenden Malware-Varianten hervorzuheben:

- Der Trojaner ALMA Communicator nutzt ausschließlich DNS-Tunneling, um Befehle von den Angreifern zu empfangen und Daten auszuschleusen. Die Datenübertragung von der Malware zum C2-Server erfolgt über DNS-Anfragen zur Auflösung speziell codierter Subdomainnamen. Umgekehrt erfolgt die Übermittlung von Anweisungen vom C2-Server an den Trojaner über spezifische IPv4-Adressen, die als Antwort auf DNS-Anfragen der Malware ausgegeben werden.
- Der PowerShell-basierte Trojaner Helminth kann Dateien von einem C2-Server empfangen, indem er im Abstand von 50 Millisekunden DNS-TXT-Records abfragt. Auf diese Weise können über DNS kleinste, kaum zu identifizierende Teile weiterer Schadprogramme auf das Zielsystem übertragen werden.

Durch den Einsatz von DNS-Tunneling kann OilRig die Sicherheitssysteme betroffener Unternehmen umgehen und kann über zuverlässige C2-Kommunikationskanäle weitere Angriffsphasen einleiten. Ausführliche Informationen über OilRig finden Sie in den entsprechenden Blogbeiträgen von Unit 42 sowie im interaktiven Playbook Viewer.

Um diese Defizite konventioneller Ansätze auszugleichen und für proaktiven, skalierbaren DNS-Schutz zu sorgen, implementieren manche Unternehmen Punktlösungen zur Abwehr DNS-basierter Bedrohungen. Damit lässt sich zwar die DNS-Sicherheit in bestimmten Bereichen verbessern, doch bringen auch die angeblich branchenführenden Lösungen gewisse entscheidende Nachteile mit sich. Beispielsweise funktionieren viele dieser Produkte nur dann effektiv, wenn vor der Implementierung Änderungen an der DNS-Infrastruktur vorgenommen werden. Zudem entstehen durch den Einsatz isolierter Tools Datensilos, die möglicherweise nicht in andere Komponenten der Sicherheitsinfrastruktur eingespeist werden können. Das hat zur Folge, dass ohnehin schon überlastete Mitarbeiter noch mehr Zeit auf die Zusammenführung von Daten und die Verwaltung der einzelnen Sicherheitssysteme verwenden müssen.

Wie Sie verhindern, dass Angreifer DNS gegen Sie nutzen

Das bisher Dargelegte wirft die Frage auf, wie Sie die Kontrolle über Ihren DNS-Datenverkehr wiedererlangen und zugleich verhindern können, dass Angreifer das DNS Ihres Unternehmens ausnutzen. Um Sie bei der Bewältigung dieser Herausforderungen zu unterstützen, haben wir hier eine Liste mit konkreten Maßnahmen für Sie zusammengestellt.

- **Sicherheitsdaten – je mehr, desto besser:** Sie benötigen enorme Mengen praxisnaher Sicherheitsdaten, die sie entweder selbst sammeln oder über den Datenfeed einer CTA-Gruppe (Cyber Threat Alliance) erhalten. Je weiter das Netz ihrer Sicherheitspartner gespannt ist, desto schneller erreichen Sie starken Schutz für Ihr Unternehmen.
- **Analysen und maschinelles Lernen:** Ihr Sicherheitsteam muss in der Lage sein, die zur Verfügung stehenden Daten zu analysieren. Um DNS-Tunneling oder Malware mit dynamisch variierenden C2-Domains in den Griff zu bekommen, sind auf maschinellem Lernen basierende Lösungen erforderlich, die schädliche Domains identifizieren und Verlagerungen der C2-Kommunikation prognostizieren. Ergänzend können Sie mithilfe von Verhaltensanalysen ein Profil des Normalzustands erstellen, vor dem sich Anomalien deutlich abheben. Und schließlich unterstützen Analysetools Sicherheitsteams bei der Identifizierung der sicherheitsrelevanten Ereignisse, der Priorisierung von Bedrohungen und der Einleitung von

manuellen oder automatisierten Gegenmaßnahmen. Das spart Zeit und Arbeitsaufwand.

- **Automatisierte Sicherheitsprozesse und Integration einer Next-Generation Firewall:** Viele DNS-basierte Angriffe laufen so schnell ab, dass Sicherheitsteams nur eine Chance haben, wenn sie von manuellen zu automatisierten Abwehrmaßnahmen übergehen. Mit automatisierten Prozessen können infizierte Geräte schnell identifiziert und Bedrohungen vor einer weiteren Ausbreitung im Netzwerk rechtzeitig eingedämmt werden. Außerdem sollten innovative Lösungen für die Integration alter und neuer Komponenten der Sicherheitsinfrastruktur implementiert werden, damit die Sicherheitsexperten die Nutzung bestehender Investitionen ohne Komplikationen fortsetzen können.
- **Cloudbasierter Schutz:** Cloudbasierte Schutzmechanismen sind stets auf dem neuesten Stand, lassen sich unbegrenzt skalieren und bieten Ihnen die Möglichkeit, DNS-basierte Angriffe auf Ihr Unternehmen mithilfe zentralisierter Kontrollmaßnahmen zu stoppen. In der Cloud stehen Ihren Sicherheitsexperten jederzeit die neuesten Erkennungstechnologien und andere Innovationen zum sofortigen Einsatz zur Verfügung. Außerdem erfolgt die Aktualisierung cloudbasierter Schutzmechanismen instantan, ohne dass Sie Änderungen an der Software durchführen müssen. Dadurch wird das Team Ihres Security Operations Center (SOC) entlastet.
- **Vermeidung isolierter Punktlösungen:** Grundsätzlich sollten Sie von der Implementierung von Einzellösungen mit mangelnden Integrationsmöglichkeiten absehen, vor allem, wenn hierfür Änderungen am DNS-Routing erforderlich sind. Viele dieser Tools sind nicht für automatisierte, holistische Sicherheitsprozesse ausgelegt, sodass Ihre Analysten zunächst manuell Daten aus verschiedenen Quellen zusammenführen müssen, bevor sie handeln können. Das verzögert die Reaktion auf identifizierte Bedrohungen – ein Effekt, der noch dadurch verstärkt wird, dass diese Produkte nicht die Konsolidierung von Warnmeldungen aus der gesamten Sicherheitsinfrastruktur unterstützen.

Umsetzung von Best Practices

Neben den richtigen Technologien kann Ihr Unternehmen auch die folgenden Best Practices implementieren, um das eigene Netzwerk vor DNS-basierten Bedrohungen zu schützen:

- Entwickeln und starten Sie ein Schulungsprogramm zur Stärkung des Sicherheitsbewusstseins Ihrer Mitarbeiter, das diese über die wichtigsten Identifizierungsmerkmale verdächtiger E-Mails und einfache Vorsichtsmaßnahmen zur Malware-Prävention aufklärt. Wenn Sie spezielle Anti-Phishing-Trainings durchführen, senken Sie das Risiko eines erfolgreichen E-Mail-basierten Angriffs.
- Informieren Sie sich über die aktuelle Bedrohungslage und rufen Sie ein Threat-Intelligence-Programm ins Leben, damit Sie stets über die neuesten Bedrohungen und Angriffsmethoden Bescheid wissen. Nutzen Sie Ihr erworbenes Wissen um sicherzustellen, dass die passenden Technologien zur Absicherung des Unternehmensnetzwerks vorhanden sind.
- Ziehen Sie aussagekräftige Erkenntnisse aus den verfügbaren Daten zum DNS-Traffic. Die bloße Sammlung von DNS-Protokollen hat an sich noch keinen Nutzen. Erst durch eine genaue Analyse können Sie relevante Schlüsse aus Ihren Daten ziehen und diese als Grundlage für neue Maßnahmen zum Schutz Ihres Netzwerks vor DNS-basierten Angriffen nutzen.
- Vertrauen Sie nicht blind auf DNS-Resolver. Wenn Hacker die Kontrolle über einen DNS-Server übernehmen, werden bei DNS-Anfragen möglicherweise falsche Antworten ausgegeben, die Ihren Datenverkehr auf infizierte Systeme umleiten oder Man-in-die-Middle-Angriffe ermöglichen.
- Entwickeln Sie eine Sicherheitsstrategie für die mobilen Mitarbeiter Ihres Unternehmens. Fahrlässiges Verhalten bei der Telearbeit setzt enorme Mengen an Unternehmensdaten beträchtlichen Risiken aus. Beispielsweise sollten Sie mobile Mitarbeiter unbedingt vor der Nutzung kostenloser, öffentlich zugänglicher WLANs warnen, da hier die Gefahr besteht, dass Angreifer den Datenverkehr zwischen Endgerät und Zugangspunkt abfangen. Außerdem bietet sich die Implementierung von Zugangsverfahren mit Multi-Faktor-Authentifizierung an. Auf diese Weise können Sie das Risiko von Schäden und Datenlecks infolge des Verlustes oder Diebstahls eines geschäftlich genutzten Mobilgeräts minimieren.
- Verlassen Sie sich nicht darauf, dass ein einzelnes Produkt die Lösung für sämtliche Sicherheitsherausforderungen bietet. Setzen Sie stattdessen auf einen holistischen Ansatz und sorgen Sie dafür, dass sämtliche für die Bekämpfung aktueller Bedrohungen nötigen Lösungen vorhanden sind. Dabei sollten Sie auch darauf achten, dass die verwendeten Tools miteinander integriert werden können. Denn letztlich benötigt Ihr Unternehmen eine funktionsreiche Sicherheitsinfrastruktur, die verschiedenste Bedrohungsvektoren abdeckt. Besonders wichtig sind Intrusion-Prevention-Systeme sowie Lösungen für URL Filtering und die Blockierung schädlicher Dateien.
- Implementieren Sie Lösungen, die nicht nur automatisch Warnmeldungen ausgeben, sondern im Ernstfall auch automatisch Gegenmaßnahmen einleiten. Viele aktuelle Bedrohungen treffen Unternehmen mit solcher Geschwindigkeit, dass ein ausgelöster Alarm oder eine versendete Warnmeldung wenig hilfreich ist. Bis ein Analyst den Alarm überprüft, die Echtheit der Bedrohung bestätigt und ihre Quelle ermittelt hat, ist es meistens schon zu spät, um den Diebstahl von Daten oder die Infektion mit Malware noch zu verhindern. Deshalb müssen Ihre Sicherheitssysteme in der Lage sein, Bedrohungen automatisch zu erkennen und potenziell infizierte Systeme zu isolieren, bevor weiterer Schaden entsteht.

Setzt Ihr Unternehmen die Best Practices für DNS-Sicherheit erfolgreich um? Mit unserem Best Practice Assessment können Sie sich Gewissheit verschaffen.

Oval Tower, De Entrée 99 -179
1101HE Amsterdam, Niederlande
Telefon: +31 20 888 1883
Vertrieb: 0800 7239771
Support: +31 20 808 4600

www.paloaltonetworks.de

© 2019 Palo Alto Networks, Inc. Palo Alto Networks ist eine eingetragene Marke von Palo Alto Networks. Eine Liste unserer Marken finden Sie unter https://www.paloaltonetworks.com/company/trademarks.html.
Alle anderen hier erwähnten Marken können Markenzeichen der jeweiligen Unternehmen sein.
stop-attackers-from-using-dns-against-you-wp-040219-de