Studie über das Gefahrenpotential und Gegenmaßnahmen zu Angriffen auf das DNS Protokoll durch IP-Fragmentierung

Carsten Strotmann[1], Patrick Ben Koetter[2], Roland van Rijswijk-Deij[3], Markus de Brün[4], Anders Kölligan[5]

Abstract: Caches von DNS-Resolvern können mit fragmentierten IP-Paketen kompromittiert werden. Die BSI-Studie „IP Fragmentation and Measures against DNS Cache Poisoning (Frag-DNS)“ ist der Frage nachgegangen ob und wie häufig IP-Fragmentierung auf „natürliche Weise“ im Internet vorkommt. Sie hat mögliche Gegenmaßnahmen getestet und empfiehlt einige, die mit wenig Veränderung Abhilfe schaffen. Die Studie wird unter `https://bsi.bund.de/dok/frag-dns` publiziert.

Keywords: IP-Fragmentierung, DNS Cache Poisoning, DNS-Resolver, DNSSEC

1 Inhaltsbeschreibung

Das Domain Name System (DNS) ist eines der wichtigsten Protokolle des Internets. Nahezu jede Aktion im Internet beginnt mit einer DNS-Anfrage. Kernaufgabe des DNS ist es, Domain-Namen an IP-Adressen zu binden. Inzwischen wird es jedoch auch verwendet, um Konfigurations- und Authentifizierungsanweisungen sowie Policies auszugeben.

Aufgrund seiner zentralen und kritischen Bedeutung für das Internet ist DNS zu einem lohnenswerten Ziel für Angreifer geworden. Zahlreiche auf das DNS gerichtete Angriffsmethoden existieren und für die meisten dieser Angriffe sind Gegenmaßnahmen bekannt und wurden umgesetzt. Eine relativ neue Angriffsmethode, die durch Shulman et al [6] vorgestellt wurde, nutzt die IP-Fragmentierung zur Umgehung einiger jener Sicherheitsfunktionen, die derzeit in die DNS-Software eingebaut sind.

Frühere Studien[7] konnten zeigen, dass es möglich ist, fragmentierte DNS-Antworten zu verwenden, um gefälschte oder manipulierte Daten in den Cache eines DNS-Resolvers einzuschleusen. Dieser Prozess wird als „Cache Poisoning“ bezeichnet. Im Rahmen der, von sys4 und NLnet Labs, durchgeführten BSI-Studie „IP Fragmentation and Measures

[1] sys4 AG cs@sys4.de
[2] sys4 AG p@sys4.de
[3] NLnet Labs
[4] Bundesamt für Sicherheit in der Informationstechnik (BSI)
[5] Bundesamt für Sicherheit in der Informationstechnik (BSI)
[6] Fragmentation Considered Poisonous, Amir Herzberg, Haya Shulman, `https://arxiv.org/abs/1205.4011`
[7] IP fragmentation attack on DNS, Tomas Hlavacek, RIPE 67, 16.10.2013, `https://ripe67.ripe.net/presentations/240-ipfragattack.pdf`

doi:10.18420/sicherheit2022_15

against DNS Cache Poisoning (Frag-DNS)“ wurde untersucht, ob und wenn wie häufig die notwendigen Voraussetzungen für Cache Poisoning im Internet tatsächlich gegeben sind. Somit wurde festgestellt, ob dieser Angriffsvektor überhaupt eine reale und relevante Bedrohung darstellt. Zudem wurde untersucht, wie effektiv etwaige Gegenmaßnahmen sind und welche Nebenwirkungen diese gegebenenfalls auf den DNS Betrieb hätten.

Die in diesem Beitrag vorgestellten Forschungsarbeiten untersuchten die Voraussetzungen aus zwei Gesichtspunkten:

- Aus der Perspektive des autoritativen DNS-Servers: In der Studie wurden Millionen von autoritativen DNS-Servern im Internet getestet, um festzustellen, ob diese Server relativ große DNS-Antwort-Pakete senden, welche tendenziell fragmentiert werden. Die Domänen, von denen fragmentierte Antworten eingingen, wurden mit der Tranco Liste[8] der beliebtesten 1 Million Domänen im Internet abgeglichen. Diese Messung ergab, dass es im Internet in seltenen Fällen natürlich auftretende Fragmentierung von DNS-Verkehr gibt. Obwohl sie selten auftreten, sind diese Fälle dennoch relevant, denn sie betreffen auch Domains sehr populärer Internet-Dienste.
- Aus der Sicht des DNS-Resolvers: Der DNS-Verkehr eines großen Internet Service Providers (ISP) in Deutschland wurde über einen Zeitraum von 24 Stunden beobachtet, um festzustellen, wie viele fragmentierte DNS-Antworten im realen Internetverkehr auftreten. Diese Messung bestätigt, dass DNS-Fragmentierung tatsächlich in produktiven Umgebungen vorkommt.

Da Fragmentierungs-Angriffe meist auf DNS-Verkehr abzielen, der über das zustandslose UDP-Protokoll gesendet wird, besteht eine der vorgeschlagene Gegenmaßnahmen darin, die DNS-Auflösung von UDP auf TCP umzustellen. Zur Bewertung des Potenzials dieser Gegenmaßnahme untersuchte die Studie die Anzahl autoritativer DNS-Servern im Internet, welche DNS über TCP unterstützen. Während DNS über TCP bereits seit mehr als 10 Jahren von den Internet Protocol Standards vorgeschrieben ist (siehe RFC 5966 und RFC 7766), zeigen die Messungen, dass eine beträchtliche Anzahl von DNS-Servern immer noch keine TCP Verbindungen für DNS anbietet.

Als Nebenprodukt haben die oben erwähnten Messungen ergeben, dass eine beträchtliche Anzahl autoritativer DNS-Server im Internet auf vergleichsweise alten Linux-Betriebssystemen läuft. “Long Term Support” Linux-Systeme werden zwar offiziell von ihren Herstellern gewartet und so werden Sicherheits-Patches angeboten, aber diese Updates ändern nicht notwendigerweise Standardeinstellungen in den Linux-Kerneln. Diese Standardeinstellungen könnten einige erfolgreich DNS-Fragmentierungs-Angriffe verhindern. Die Analyse ergab somit, dass der Betrieb von “Enterprise”-Linux-Systemen das Risiko von Sicherheitsproblemen erhöhen kann, selbst wenn diese Systeme vollständig gepatcht werden.

[8] https://tranco-list.eu/

Da DNS-Fragmentierungs-Angriffe eine reale Bedrohung im Internet darstellen, wurden in der Studie weitere mögliche Abhilfemaßnahmen geprüft. Da diese Maßnahmen negative Auswirkungen auf den Betrieb des DNS oder die Leistung der DNS- Namensauflösung haben könnten, wurde eine mit der DNS-Infrastruktur des Internet vergleichbare Laborumgebung aufgebaut und die Gegenmaßnahmen in dieser Umgebung getestet.

In der Studie wurden die folgenden Gegenmaßnahmen getestet und bewertet:

- **Der Betrieb eines reinen DNS-over-TCP Resolver-Dienstes:** 40-44% Performance Verlust gegenüber DNS-over-UDP
- **DNS über TLSv1.3 zwischen DNS Resolver und autoritativen DNS Servern:** Vergleichbarer Performance-Verlust wie bei DNS-over-TCP. Die TLS Verschlüsselung selbst erzeugt nur einen geringen Performance-Verlust (ca. 4%)
- **"opportunistisches TCP" (TCP bevorzugen, Rückfall auf UDP wenn notwendig):** Bei Benutzung von TCP der Performance-Verlust wie bei DNS-over-TCP, jedoch über 70% Performance-Verlust (brutto) bei Servern, welche kein DNS-over-TCP unterstützen
- **Vermeidung von DNS Fragmentierung durch Verringerung der erlaubten Antwortgröße durch EDNS:** Bei Verringerung der möglichen DNS-Antwort-Grösse auf 1232 Byte (Minimum IPv6 MTU von 1280 Byte abzüglich IP-Header und UDP-Header) geringe Performance Verluste (~ 5%) bis leichte Performance-Gewinne (3.2%) je nach DNS-Resolver-Software
- **Verwerfen alle fragmentierter UDP Pakete durch eine Firewall vor dem DNS Resolver:** Nur geringe Performance Verluste oder leichte Performance Gewinne, je nach eingesetzter DNS-Resolver-Software, da die Software bei ausbleibenden Antworten dynamisch die EDNS Antwort-Grösse anpasst (wie vorherige Gegenmassnahme)
- textbfVerwerfen von fragmentierten UDP Paketen, welche unter der durch EDNS signalisierten Antwortgröße fällt: DNS-Performance vergleichbar mit vorheriger Gegenmassnahme, jedoch komplexere Firewall-Regeln, welche mehr Last auf dem System erzeugen
- **Ignorieren der "Additional Section" in DNS Antworten:** Nicht umsetzbar, da die "Additional Section" für DNS-Delegations-Verweise benötigt werden
- **Absicherung der Kommunikation zwischen DNS Resolver und autoritativen Servern durch Transaction Signatures (TSIG):** Performance Vergleichbar mit klassischem DNS-over-UDP, muss jedoch sowohl auf DNS-Resolvern als auch auf autoritativen Servern aktiviert sein und ist bisher nicht in allen populären DNS-Resolvern implementiert

Das Ausschalten von MTU-Path-Discovery hilft gegen ICMP-Spoofing-Angriffe welche IP-Fragmentierung von DNS Paketen durch künstliches Absenken der Path-MTU erzeugen.

In der Studie haben wir jedoch auch eine Reihe von DNS-Anworten von populären Domains gefunden, welche die Ethernet-MTU von 1.500 Byte überschreiten. Daher würde die Gegenmassnahme in diesen Fällen nicht helfen.

Auf der Grundlage der Messungen und Tests zu den möglichen Abhilfestrategien empfehlen wir eine Kombination aus zwei effizienten Maßnahmen zur Abschwächung von DNS-Fragmentierungs-Angriffen:

- Verhinderung der DNS-Fragmentierung durch Herabsetzung der maximalen EDNS-Nachrichtengröße auf 1.232 Bytes. Diese Gegenmassnahme kann unilateral von Betreibern von DNS-Resolvern und autoritativen DNS-Servern konfiguriert werden und hat nur sehr geringen Einfluss auf die Performance.
- Blockieren bzw. Verwerfen aller fragmentierten DNS-Nachrichten auf der Firewall-Ebene. Wird die DNS-Antwort-Grösse auf 1.232 Byte eingeschränkt dann kann es keine “natürlichen” DNS-Anworten mit IP-Fragmentierung geben.

Zusätzlich zu diesen beiden Hauptempfehlungen führen wir weitere Konfigurationsänderungen und bewährte Verfahren zur Verhinderung von DNS- Fragmentierung auf, welche das Risiko erfolgreicher DNS-Fragmentierungs-Angriffe verringern.

Die empfohlenen Änderungen in der Konfiguration von DNS-Servern mildern zwar die Auswirkungen des Cache-Poisoning Angriffes ab, beseitigen die Ursache jedoch nicht. Zur Behebung des DNS-Cache-Poisoning Problems - und vieler anderer Angriffe auf die DNS Infrastruktur - muss die DNSSEC-Signierung und -Validierung flächendeckend eingesetzt werden.