Technologic Papers

# עלייתם של שרותי ה-DNS האלטרנטיביים

מאת אירנה דמסקי

## הקדמה

בראשון לאפריל Cloudflare וארגון APNIC יצאו בהכרזה על שרות צרכנים חדש בתחום ה-DNS: שרת ה-DNS האלטרנטיבי בכתובת 1.1.1.1 אשר מבטיח יותר מהירות ופרטיות ביחד לשרתי ה-DNS אשר ניתנים מספק האינטרנט שלכם או (לטענתם) השירותים הפומביים האחרים הקיימים היום.

1.1.1.1 מצטרף לקבוצה של שרתי DNS פומביים "מפורסמים", אשר מאפשרים לשנות את ההגדרות ברירת המחדל של ספקית האינטרנט, ולהפנות את הדפדפן / מערכת ההפעלה / הנתב / ה-VPN או האפליקציה שלכם, לשרות DNS שונה מאשר זה של הספקית אשר מבטיח הבטחות לפיצ'רים אשר לא קיימים בשרות של הספקית. במאמר זה ננסה לסרוק את האופציות השונות אשר מוצעות ע"י השירותים הללו ונראה מה אנחנו מרוויחים ו/או מפסידים כאשר אנחנו משתמשים בהם.

## RECAP - אז מהו בעצם ה-DNS?

מערכת ה-DNS נמצאת עימנו מאז שנות השמונים המוקדמות והינה אחת מאבני הביניין של האינטרנט. ההצעה המקורית לפרוטוקול נכתבה ע"י פול מוקפיטרס[1] בשנת 1983 (RFC 882[2], 883[3]) והפכה בעצם לפרוטוקול המקובל בשנת 1985 כאשר פורסם המימוש הראשון של BIND ע"י מספר סטודנטים באוניברסיטת Berkeley. מספר עדכונים ל-RFC פורסמו מאז, העיקרי שבהם, RFC 1034[4], 1035[5] פורסם בשנת 1987 והינו הלכה למעשה ההגדרה הרשמית של הפרוטוקול (RFC 7719[6]) אשר פורסם ב-2015

[1] https://en.wikipedia.org/wiki/Paul_Mockapetris
[2] https://www.ietf.org/rfc/rfc882.txt
[3] https://www.ietf.org/rfc/rfc883.txt
[4] https://www.ietf.org/rfc/rfc1034.txt
[5] https://www.ietf.org/rfc/rfc1035.txt
[6] https://www.ietf.org/rfc/rfc7719.txt

ומנסה לעשות סדר ולנקות מעט את הטרמינולוגיה אשר חלקה השתנה מאז ההגדרה המקורית בשנת 1987, אך בגדול אינו משנה את ההגדרה כלל).

ה-DNS (Domain Name System) הינו פרוטוקול היררכי ומבוזר להגדרת שמות לכתובות אינטרנט. למה צריך אותו? כי אנחנו לא רוצים לזכור כתובות IP (וגם אילו היינו רוצים, דבר זה נהיה כמעט בלתי אפשרי עם הכניסה של IPv6) ומעדיפים לזכור כתובות יותר נוחות כגון damsky.tech או digitalwhisper.co.il.

המערכת בנויה בצורה היררכית וכך, כל שרת מכיל מידע (resource records) על אזור מסוים באינטרנט (zone) וכן, כאשר תשלח בקשה לשרת ה-DNS הוא יבדוק את השאילתה ויפנה את המבקש אל השרת הבא בתור אשר מכיל את המידע הרלוונטי עבור אותה בקשה.

**מספר נקודות שכדאי לזכור לגבי DNS:**

- הפרוטוקול מוגדר ברמה 5 של מודל חמש השכבות (האפליקציה) ויושב מעל UDP (למרות שישנם מקרים בהם התשובה תחזור מעל TCP - זה קורה כאשר התשובה לשאילתה הינה יותר מ-4096 בתים, למשל במקרה של חתימות ה-DNSSEC)
- ישנם 13 שרתים המוגדרים root servers[7] ומהם מתחילה כמעט כל שרשרת הפענוח. שרתים אלו מנוהלים ע"י 12 ארגונים (Verisign שולטים על 2 מהם - שרתי ה-a וה-j) וניתן להתנדב לארח עותק של אחד מהשרתים.
- רוב השאילתות שאתם מבצעים חוזרות על עצמן ולכן המחשב, הנתב וה-firewall שלכם שומרים הרבה מאוד מהרזולוציות אצלם ב-cache. יש גם הרבה מאוד רזולוציות שנשמרות ב-cache אשר בשרת ה-DNS של הספקית שלכם - כל זאת בשביל לחסוך בתעבורה (וגם latency).

תהליך התרגום מ-domain name לכתובת IP הינו תהליך המתרחש כל פעם שאתם ניגשים לכתובת כלשהי, השרת הראשון שינסה לענות על שאלת תרגום זו יהיה השרת אשר מוגדר ע"י הספקית שלכם (אם אתם משתמש בייתי / סלולרי) או ע"י מנהל הרשת שלכם (אם אתם ברשת ארגונית) - הגדרה זו בדרך כלל מתרחשת באמצעות פרוטוקול ה-DHCP, אבל שיחה עליו זה נושא למאמר אחר לגמרי.

[7] http://www.root-servers.org/

## אז מה בעצם הבעיה בשרתים מוגדרים ע"י הספקית?

תארו לעצמכם שאתם שרת DNS שקיבל כרגע שאילתה על כתובת מסוימת, יש מספר דברים שאתם יכולים לעשות בתגובה:

- אתם יכולים לעשות את הצפוי ולהחזיר את התשובה הנכונה למיפוי אשר שאלו עליו - ז"א את הכתובת של האתר אותו ביקשו מכם.
- אתם יכולים לעשות משהו פחות צפוי ולשלוח את השואל לכתובת אחרת לחלוטין - למה שתעשו את זה?
  - אולי אתם רוצים להגן על המשתמש ולחסום לו גישה לאתרים מזיקים
  - אולי אתם רוצים למנוע מהעובדים שלכם גישה לרשתות חברתיות בשעות העבודה מהמחשבים של המשרד
  - אולי אתם ספקית אינטרנט כשר אשר רוצה למנוע מהמשתמשים גישה לאתרי פורנו וכו'
  - או אולי אתם ממשלת רוסיה שרוצה לחסום את טלגרם לאזרחים
- אתם יכולים לעשות את הצפוי אך לא הרצוי (על רוב) המשתמשים - אתם יכולים לאסוף מידע על לאן ומתי גלשתי, מה הרגלי השימוש שלי באינטרנט, תחומי העניין שלי וכולי. את המידע הזה תוכלו לחקור ולהסיק ממנו מסקנות (למשל, בתור ספקית, אם לקוחות שלי גולשים לאתרים של ספקיות מתחרות, אולי אני רוצה להעביר את הרשימה של הלקוחות האלה למחלקת שימור לקוחות שינסו למנוע מהם מלעבור למתחרה?) או למכור למי שיציע לכם על זה תמורה משתלמת (קיימבריג' אנליטיקס מזכיר לכם משהו דומה?)

**אז מה אפשר לעשות בשביל למנוע את זה?**

אז כפי שיכולתם לנחש עד כה, אפשר לא להשתמש בשרתים אשר מוגדרים לנו ע"י הספקית ולהגדיר שימוש בשרת אלטרנטיבי כלשהו אשר מתיימר לפתור חלק, אם לא את כל הבעית שהמוזכרות לעיל.

אז מי הם אותם השרתים האלטרנטיביים שקיימים כיום? בכתבה בו נסקור שלושה מהשירותים ה"חדשים" והמוכרים ביותר (בעיקר בגלל שיש להם כתובות מגניבות) ונראה מה כל אחד מהם מציע. לטובת הסדר הטוב, נזכיר גם כמה שירותים אחרים אשר מציעים שירות דומה, אך פחות נכנס לפרטים לגביהם.

## Google Public DNS - 8.8.8.8

השרות של גוגל אינו חדש, נמצא עמנו כבר כמה שנים טובות ובתקווה אינו הולך לשומקום בזמן הקרוב.

**מה הם מבטיחים?**

- מהירות
- פרטיות
- שיפור האבטחה
- ביטול הפניות למקורות לא ברורים

**ומה הם באמת נותנים?**

**פרטיות -** גוגל מבטיחה[8] שמירה של הלוגים משרתי ה-DNS שלה למשך 48 שעות בלבד בהן **רק** אנשי אבטחת המידע ומניעת ה-DDoS שלהם יוכלו להשתמש במידע לטובת חקירת אירועים ותמיכה בהגנה של הרשת. לאחר 48 שעות הפרטים המזהים שנשמרו בלוג (למשל הכתובת IP של השואל) נמחקים ונשארים רק לוגים שעברו תהליך אנונימיזציה במערכת.

חשוב לציין שגוגל מבטיחים שהם לא משתמשים במידע - לא המלא ולא האנונימי לטובת קורולציות עם מידע אחר ו/או קומבינציות עם שירותים אחרים - ז"א, הלוגים שלכם לא משמשים לפרסומות (שזו הנחת המוצא של כולנו בכל מה שקשור למידע שמגיע לגוגל).

**מהירות -** כן, גוגל מהירים. מהירים מאוד אפילו, אבל כפי שניתן לראות בהשוואה של ניקולס בבלוג[9] שהוא פרסם לאחרונה, הם **בממוצע** פחות מהירים מהשני שרתים של Cloudflare או Quad9.

**שיפור האבטחה -** גוגל מספקים אופציה לתקשר עם השרתים שלהם מעל פרוטוקולי ה-TLS וה-HTTPs ובכך מאפשרים לתקשורת בטוחה יותר.

**ביטול הפניות -** גוגל אוספים את המידע שלהם מה-root zones של שרתי ה-root בלבד ואינם משנים את המידע בשום צורה.

ניתן לקרוא עוד על השרות של גוגל באתר שלהם.

[8] https://developers.google.com/speed/public-dns/privacy
[9] https://medium.com/@nykolas.z/dns-resolvers-performance-compared-cloudflare-x-google-x-quad9-x-opendns-149e803734e5

## Quad9 - 9.9.9.9

השרות הנ"ל הוכרז בחודש אוקטובר 2017 והינו תוצר של שיתוף פעולה בין ה-Global Cyber Alliance, IBM ו-Packet Clearing House (חשוב לציין, שאלה לא ה-Vendor-ים היחידים אשר משתפים פעולה עם הפרויקט ונכון להיום, הארגונים הבאים מספקים לפרויקט מידע מודיעיני הכרחי לטובת השרות אשר הפרויקט מציע. הארגונים הינם: abuse.ch, APWG, Bambenek Consulting, Cisco, F-Secure, Mnemonic, Netlab 360, Payload security, Proofpoint, RiskIQ, ThreatSTOP)

**מה הם מבטיחים?**

- מהירות
- פרטיות
- הגנה מפני רושעות למיניהן

**ומה הם באמת נותנים?**

**מהירות -** שוב, ע"י ההשוואה מהבלוג של ניקולס[10], אנחנו רואים שהבטחה זו קיימת והמהירות היא באופן אובייקטיבי מספיק טובה (כן, גם אם יש שירותים אחרים שיחזירו לכם תשובות לשאילתות שלכם ב-18.25 מילישניות יותר מהר, אני בספק שתמצאו מה לעשות עם הזמן שהרווחתם).

**פרטיות -** להבדיל מגוגל, שרות זה כלל אינו שומר את כתובת ה-IP של שואל השאילתה ולכן, הפרטיות שלכם מובטחת בצורה הרבה יותר הרמטיות מזו שמוצעות בכל שרות אחר. את המידע האנונימי והסטטיסטי אשר הם שומרים הם חולקים עם ה-Vendor-ים אשר משתפים פעולה עם הפרויקט - סה"כ נשמע הוגן. (אגב, ה-Vendor-ים מקבלים מידע רק ביחס למודיעין שהם ספקו - ז"א, אם Vendor א' דיווח על כך שכתובת כלשהי צריכה להיחסם, הם יכולים לקבל על הכתובת הזו מידע אנונימי סטטיסטי - כל ונדור אחר אשר לא דיווח על הכתובת הזו לא יקבל מידע לגביה - בצורה זו הם גם שומרים על הפרטיות של המידע המודיעיני של ה-Vendor-ים - שגם את זה צריך להעריך)

**הגנה מפני רושעות למיניהן -** שרות ה-DNS של Quad9 בעצם ממש תצורה של מוצר הנקרא DNS Firewall אשר מאפשרת להם להשתמש בטכנולוגיה בשם DNSRPZ ע"מ לשנות את ההתנהגות (התשובות) אשר תקבלו משרת ה-DNS שלעם במקרה ואתם מנסים לגשת ל-domain שיודע בתור בעייתי.

**חשוב לציין**

א. למרות ש-Quad9 לא מציינים זאת בתור פיצ'ר ספציפי, הם כן מספקים אפשרות לשרות מאובטח ע"י מימוש של DNSoverTLS.

[10] https://medium.com/@nykolas.z/dns-resolvers-performance-compared-cloudflare-x-google-x-quad9-x-opendns-149e803734e5

ב. למרות שההבטחה הגדולה של השרות היא הגנה מפני רושעות, ישנה גרסה של השרת אשר אפשר להפנות אליה את התעבורה שלכם אשר מספקת רק מהירות ולא מסננת עבורכם את התעבורה כלל.

ניתן לקרוא עוד על השרות של Quad9 באתר שלהם.

## Cloudflare & APNIC - 1dot1dot1dot1 - 1.1.1.1

השרות האחרון שהוכרז, כמו שכבר ציינו הינו שיתוף פעולה של Cloudflare[11] עם APNIC[12] והוא הוכרז בראשון לאפריל. חלק גדול מהאינטרנט חשב שזו בדיחה, כי בכל זאת הראשון לאפריל ידוע כיום שבו חברות טכנולוגיות רבות מחליטות לשחרר מוצרים פיקטיביים ע"מ לראות מי ייפול בפח (אישית, האהוב עלי היה ההודעה של גוגל לפני כמה שנים שבעקבות ההצלחה של ג'ימייל הם מכריזים על שרות snail mail בו תוכלו לשלוח מכתבים אמיתיים במקום אלקטרוניים). השחרור של השרות מסתבר לא היה בדיחה אלא החלטה מודעת של מנכ"ל Cloudflare, ובעצם משחק על התאריך והכתובת של השרת כי 1.1.1.1 זה בעצם 1/4 - מה גם, הוא השתמש בתירוץ שבזמנו, גם גוגל שחררו את ג'ימייל בראשון לאפריל וזו לא הייתה בדיחה כלל.

**אז מה הם מבטיחים?**

- מהירות
- פרטיות

**אז מה הם באמת נותנים?**

**מהירות -** חדשות טובות קודם כל. זה נראה ש-Cloudflare באמת מספקים את המהירות הגבוהה ביותר מבין השירותים השונים וצריך לתת להם מעט קרדיט על כך כי לא תמיד מה שהמרקטינג אומרים מתקיים במציאות.

**פרטיות -** אז פה זה נהיה טיפה יותר טריקי. דבר ראשון, ההבטחה היא לא רק לפרטיות אלא ל- ultimate privacy, וכבר פה אנחנו רואים שאנשי המרקטינג נכנסו לתמונה, וגם אם לא אומרים זאת באופן מודע הם מנסים לומר שהשירותים האחרים לא מספקים את הפרטיות אשר הם מבטיחים (מה שלפחות בשני השירותים שבחנו עד כה אינו נכון). הציטוט המדויק מהאתר של הפרויקט הינו **"We will never sell your data or use it to target ads. Period."** שזאת הבטחה לא רעה, אבל בואו ננתח אותה ואת שאר ההבטחות לגבי פרטיות שהשירות מבטיח.

[11] https://blog.cloudflare.com/announcing-1111/
[12] https://labs.apnic.net/?p=1127

המידע שהשירות הנ"ל אוסף הינו מידע מלא על השאילתות שלנו, כולל כתובת ה-IP של השואל (מה שכבר הופך אותו לפחות פרטי מלמשל Quad9) וקיימת הבטחה של אנונימיזציה של המידע תוך 48 שעות מאיסופו. חשוב לציין, שלהבדיל מגוגל אשר התחייבו לנו שהם אינם הולכים להשתמש במידע המלא או החלקי לטובת מוצרים, אין הבטחה כזו מהשרות הנ"ל. כמו כן, זה שהם מבטיחים לא להשתמש במידע שלנו לטובת פרסומות לא מבטיח שהם לא ישתמשו בו לטובת דברים אחרים, למשל שיפור ופיתוח מוצרים אחרים / חדשים שאינם בתחום הפרסומות.

זה שהם מבטיחים לא למכור את המידע שלנו זה גם לא רע, אבל מצד שני הם מצהירים בצורה הכי גלויה בעולם שהם מעבירים עותק שלו ל-APNIC אשר משתמשים בו לטובת מחקרים שונים ומעבירים אותו את תהליך האנונימיזציה באופן בלתי תלוי מהתהליך שהמידע עובד ב-Cloudflare תוך 48 שעות ממתי שהם מקבלים אותו. מה שאני שומעת פה זה שבעצם ישנם שני מסדי נתונים שמכילים את המידע שלנו וישנן שתי נקודות כשל בהן המידע המלא יכול לזלוג.

**מעניין לציין**

א. גם פה, ישנה אפשרות של התקשורת מול HTTPs וגם מעל TLS.

ב. הכתובת שמשמשת את השרת - 1.1.1.1 הושאלה ל-Cloudflare לתקופה של חמש שנים בלבד - מה יקרה בעוד חמש שנים עם השרות במידה ו-APNIC יחליטו שהם לא מעוניינים בו יותר?

ניתן לקרוא עוד על השרות של Cloudflare ו- APNIC באתר שלהם.

## שירותים נוספים

כמו שאמרנו, למרות שאלה שלושת הגדולים (ולא, אנחנו לא באמת יודעים לקבוע מה אחוז השימוש שלהם באינטרנט, אלא מניחים שהם יחסית גדולים כי יש להם שמות מגניבים) חשוב מאוד לציין שהם ממש לא השירותים היחידים הקיימים בתחום. שירותים נוספים שקיימים וכדאי להזכיר הינם:

- OpenDNS - שרות שנרכש לפני מספר שנים ע"י סיסקו והיה בעצם ה-DNS FW הביתי הראשון. הם עדין מאפשרים שימוש בייתי וחינמי היום ומספקים בעיקר הגנה מפני רושעות.
- Norton ConnectSafe - מספק שרות סינון תוכן בעיקר לחסימת של אתרי פורנו ואלימות.
- CleanBrowsing - מספק שרות סינון תוכן בעיקר לחסימת אתרי פורנו ואלימות.
- FoolDNS - מספק שרות חסימה לכלים אשר משמשים למעקב ברשת כגון tracking, profiling ופרסומות למיניהן
- Green Team Internet - אשר מספק חסימות לרושעות וגם סינון אתרים
- Yandex DNS - אשר מגן בעיקר מפני וירוסים והונאות. חשוב לציין שזהו שרות המכוון בעיקר לקהל הרוסי ולכן רוב החסימות שלו הן על תוכן בשפה הרוסית ופחות בינלאומי.

## לסיכום - אז איך בעצם בוחרים מה לעשות?

בגדול - זאת שאלה של מה אתם מחפשים. (שוב, ההמלצות פה הן על שלושת ה"גדולים" אבל יש שירותים אחרים שכדאי לשקול גם כן)

- אם המטרה שלכם היא בעיקר להימנע מהשרתים של ספקית או הארגון שלכם ולא באמת אכפת לכם משום דבר אחר - הייתי ממליצה להשתמש בשרת יציב אשר מספק מהירות ולכן האופציות הטובות היותר יהיו 8.8.8.8 או 1.1.1.1. הרבה פעמים שימוש בשרת של הספקית שלכם לא יפגע כלל בביצועים של הרשת שלכם (אלא דווקא עקב הימצאותו הפיזית הקרובה אליכם עשוי לגרום למהירויות טובות יותר) ולכן, אלא אם חוששים ממנו מסיבות אלו או אחרות, אפשר גם להישאר עמו.
- אם המטרה היא פרטיות - שתי האופציות הטבות ביותר יהיו 8.8.8.8 או 9.9.9.9. לא הייתי מייחסת חשיבות לתחושת הבטן הרגילה של רובנו שגוגל אוספים עלינו מידע ומשתמשים בו לטובת התאמת הפרסומות אשר הם שולחים לנו אלא סומכת על האמירות של עורכי הדין שלהם... הפתרון של 9.9.9.9 הינו הפרטי ביותר כי בשום שלב המידע עליכם לא נשמר בשרתים שלהם.
- אם המטרה היא הגנה מפני רושעות - גוגל ו-Cloudflare כלל לא רלוונטיות והפתרון הינו 9.9.9.9. אפשר להשתמש גם בפתרון של סיסקו - OpenDNS אבל אישית נראה לי שעדיף להשתמש בפתרון לא מסחרי (מה גם, סיסקו הם אחד מספקי התוכן של Quad9 ולכן החסימות שלהם אמורות להיכלל בחסימות המאופשרות ע"י השרות של Quad9)
- אגב - אם אתם משתמשים בשירותים של גוגל או Quad9 לא הייתי טורחת לשנות ל-1.1.1.1. ההבדל במהירות של 20 מילישניות לא שווה את הכמה דקות שייקח לכם לעשות את השינוי ולוודא שלא הרסתם לעצמכם את הרשת

## על המחברת

אירנה דמסקי הינה המקימה והמנכ"לית של חברת Damsky.tech החברה הינה חברה עצמאית למחקר, הכשרות וייעוץ בתחומי מודיעין הסייבר. אירנה עצמה הינה חוקרת, מדריכה, מנטורית ויועצת בתחומי המודיעין סייבר טכנולוגי מזה שנים רבות ובין השאר משמשת כחברת ועדת הייעוץ הטכנולוגית של ה-Global Cyber Alliance. תוכלו לעקוב אחריה בטוויטר ב-@DamskyIrena או להירשם לרשימת התפוצה לעדכונים מהאתר והבלוג שלה ב-https://damsky.tech.