מיתוס אבטחת הסייבר

מָבוֹא

למרות שהאינטרנט עשה התקדמות פנומנלית במהלך העשורים האחרונים, הוא נותר שברירי ופגיע להתקפות גדולות כקטנות עד היום. משתמשים מבולבלים לגבי פעולתו המורכבת ולעתים קרובות אינם מסוגלים להבחין בין פריצה על ידי פורץ לבין פריצה לתוכנת ההגנה.

אירוע אחד כזה התרחש לאחרונה ב-18 בנובמבר 2025, כאשר Cloudflare סבלה מהפסקת הפעלה עולמית שגרמה לרגע לפגוע ברשת האינטרנט[1].
זה לא היה מקרה בודד. הקודם התרחש רק שמונה חודשים קודם לכן, והיו עוד כאלה לפני כן. באופן דומה, שירותי האינטרנט של אמזון (AWS) חוו שיבושים תכופים[2].
הפסקות אינטרנט מסוג זה הפכו לכמעט שבשגרה ואמינותם של שירותים אלה שנועדו להגן מפני חדירות סייבר הועמדה בספק.

הבעיה

הפגיעות של האינטרנט הייתה בעיה מזה עשרות שנים. בשנה שעברה פרסמה ועדת התקשורת הפדרלית (FCC) הודעה על קביעת כללים מוצעים (NPRM)[3] שזיהתה את פרוטוקול שער הגבול (BGP)[4] כיעד להפחתת הסיכון. מועצת ארכיטקטורת האינטרנט (IAB), המייצגת את קהילת האינטרנט, הגיבה בתגובה והביעה חששות[5]. אף על פי כן, הבית הלבן פרסם מפת דרכים[6] שהתמקדה בשלמות ה-BGP כאמצעי לשיפור אבטחת ניתוב האינטרנט.

בהקשר זה, חשוב לזכור כי ה-BGP נדרש להעברת חבילות בין מערכות אוטונומיות (ASes)[7] שנבחרו על ידי שרת שמות המתחם (DNS)[8], בהתבסס על כתובות IPv4 שהוקצו למנויים על ידי פרוטוקול בקרת מארח דינמי (DHCP)[9], אשר נוצר כדי להתמודד עם מחסור בכתובות IPv4. מחסנית רוטוקול זו הביאה לארכיטקטורת מערכת מורכבת הפגיעה להתקפה מכיוונים רבים, שכל אחת מהן דורשת תיקון נוסף בתגובה.

הפתרון

מערכת פגומה מזמינה סדרה בלתי נגמרת של פריצות ותיקונים. אינטרנט חזק הרבה יותר יכול לנבוע מארכיטקטורה פשוטה ויעילה שמבטלת את שורש הבעיה של מחסור בכתובות IPv4, ובכך מבטלת את הצורך בכל אחד מארבעת הפרוטוקולים שהוזכרו לעיל. זוהי תוצאה של מערכת דטרמיניסטית המכונה EzIP[10].

התפתחות הטכנולוגיה והאדריכלות

כאשר האינטרנט החל לפעול, בלוקי כתובות IPv4 גדולים ומוגדרים היטב הוקצו לחמשת מרשמי האינטרנט האזוריים (RIRs). לדוגמה, עקומות הילברט[11] המתארות הקצאות קודמות של AFRINIC (אפריקה), APNIC (אסיה-פסיפיק), ARIN (צפון אמריקה), LACNIC (אמריקה הלטינית והקריביים) ו-RIPE (אירופה, המזרח התיכון ומרכז אסיה) היו ניתנות להבחנה[12] בקלות.

למרות שכל RIR הקצה את הכתובות שהוקצו לו לספקי גישה לאינטרנט (IAPs) באזור שלו, ה-IAPs עצמם לא נדרשו לציית לאותה הגבלה. זה פתח את שער הצפה של פיצול כתובות IP, שאפשר למיקומו הפיזי של מנוי לא להיות משויך גיאוגרפית לאזור שאליו הוקצתה במקור כתובת ה-IP שהוקצתה.

כאשר מאגר כתובות ה-IPv4 החל להתדלדל, DHCP קיים את פעולות ה-IAP על ידי שימוש חוזר דינמי בכתובות IPv4 ציבוריות זמינות. לאחר מכן הוצג DNS כדי להקל על הנטל על המנויים עקב סביבה כזו בשינוי מתמיד. מכיוון שצמד פרוטוקולים זה נראה כמענה לצרכים הדחופים באותה תקופה, הוא הפך לאבן הבניין של האינטרנט המוגדרת כברירת מחדל. (ראה הערת שוליים להשלכות של זיווג ייחודי זה.)

לאחר שמוסדות שאימצו את הטכנולוגיה מוקדם הסכימו לשחרר בלוקי כתובות IPv4 עודפים למכירה פומבית כדי להפחית את לחץ התשישות של מאגר כתובות ה-IPv4, לא היה עוד מעשי לצפות שכתובת IPv4 תישא מידע מיקום פיזי משמעותי, שלא לדבר על אפשרות לאתר גיאוגרפי של מנוי. ענף נפרד של התעשייה נולד כדי לשרת צורך זה. עם זאת, הרזולוציה והדיוק של הדוחות היו לעתים קרובות מוטלים בספק במקרה הטוב[13].

לאורך הדרך, IAPs (אינטרנט אלחוטי נקודתי) בעלי בלוק כתובת IPv4 אחד או יותר פיתחו את תוכניות מסירת חבילות ה-IP שלהם. בלוקי כתובות שחולקים את אותה מדיניות תעבורה מקובצים יחד ליצירת AS אחד. מכיוון שהטווח של כל AS משתנה ולעתים קרובות מוגבל, ה-BGP שימש להעברת חבילות IP על פני גבולות ה-AS. ככל שמספר ה-AS גדל, כך גדלה המורכבות של ה-BGP האחראי לחבילות החוצות מרחק ניכר כלשהו, לעתים קרובות רק באופן מקומי, שלא לדבר על אלו המיועדות לכתובות גלובליות שצריכות לחצות גבולות AS מרובים.

למרות שכל אחד מהפרוטוקולים הללו מבוזר מטבעו, פעולותיהם דורשות תיאום משמעותי המסתמך על מאמצים מרכזיים, מה שמוביל לדומיננטיות של מספר מוגבל של עסקים בעלי משאבים, כגון מפעילי רשת אספקת תוכן (CDN)[14] הכוללים את Cloudflare, AWS וכו'. אלה הופכים לתשתית הליבה של מתקן הובלת האינטרנט.

סתירות

ישנן לא מעט שיטות אינטרנט שהופכות את עקרונותיה ופעולותיה למבלבלות:

האינטרנט מקדם השוואת תנאים. אבל קריית הוותיקן מקבלת הקצאת כתובות IPv4 של 21.4 לנפש, בעוד שיותר מתריסר ישויות לא מקבלות כלום, בעוד שמדינות אחרות מקבלות את כל האפשרויות שביניהם[15]. (הערה: העובדה שלסיישל יש הקצאה של 58.4 היא מוזרה, כתוצאה מכך שעסקים מנצלים את הסביבה הפוליטית המקומית להזדמנויות גלובליות.)

קישוריות מקצה לקצה הובטחה על ידי האינטרנט. עם זאת, מודל הפעולה השולט הנוכחי שלו, CDN, מעכב מטרה זו, אפילו בתוך קהילה מקומית.

האינטרנט התעמת עם מונופול התקשורת והרגולציה הממשלתית על רשת הטלפונים הציבורית (PSTN). עם זאת, האינטרנט נשלט כיום על ידי קונגלומרטים רב-לאומיים, אשר למעשה שולטים במגזרים עסקיים, בהתאמה, עד כדי התעלמות מאחריות והתחמקות מרגולציות. האם סוג זה של ריכוזיות אינו מנוגד בדיוק לחזון האינטרנט המבוזר?

כמו כן, הפוטנציאל של כ-200 תחומי שיפוט גלובליים המפצלים את האינטרנט ולהפוך אותו לרשת מפוצלת גיאופוליטית[16] סופג ביקורת מצד קהילת האינטרנט, בעוד שרשתות ה-AS כבר הפכו את האינטרנט לרשת בצל עם לפחות 77,000 שכבות[7]. יתר על כן, מכיוון שרוב רשתות ה-AS משרתות באופן סלקטיבי רק חלקים מהעולם, כל שכבה של קליפות הבצל דומה יותר לרשת דגים חלקית עם חורים בתוכה!

העובדה המדהימה ביותר היא שהאינטרנט מגן בתוקף על עקרון חוסר הגבולות שלו, בעוד שמנגנון הניתוב העיקרי שלו התפתח ל-BGP, כאשר האות "B" מייצגת את הגבולות סביב כל ASe!

בסך הכל, בשל האופי הדינמי והמבוזר מאוד של פרוטוקולים אלה, האינטרנט הופך לפגיע למגוון רחב של פרצות אבטחה זדוניות, החל מהטרדה יומיומית ועד תוכנות כופר.

אולי נכון לציין בנקודה זו שאיכשהו IPv6, מבלי לנצל את מאגר הכתובות העצום שלו, אימץ את פרקטיקות ה-IPv4 הללו שהתפתחו בעקבות צרכים זמניים. כעת, נראה כי חשיבותו של IPv6 דועכת בשקט[17], בעוד שאין עוד אזכור של תאריך סיום ההדרגה של IPv4. מכיוון ש-IPv6 אינו מפרסם יתרונות בולטים על פני IPv4, רוב הדיונים המתמשכים באינטרנט כבר אינם מבחינים בין השניים

הפנ י ות

1. Cloudflare היסטוריית הפסקות (2019-2025)
   https://controld.com/blothe/biggest-cloudflare-outages/

2. היסטוריה של הפסקות פעילות בענן ובמרכזי נתונים של AWS
   https://www.datacenterknowledge.com/outages/a-history-of-aws-cloud-and-data-center-outages

3. דיווח על התקדמות בהפחתת סיכוני פרוטוקול שער הגבול; ניתוב אינטרנט מאובטח
   https://www.federalregister.gov/documents/2024/06/17/2024-13048/reporting-on-border-gateway-protocol-risk-mitigation-progress-secure-internet-routing

4. פרוטוקול שער הגבול
   https://en.wikipedia.org/wiki/Border_Gateway_Protocol

5. הערות אגודת האינטרנט, מועצת ארכיטקטורת האינטרנט ותאגיד האינטרנט עבור שמות ומספרים שהוקצו בנושא "דיווח על התקדמות בהפחתת סיכוני פרוטוקול שער הגבול"
   https://datatracker.ietf.org/doc/statement-iab-comments-of-the-internet-society-internet-architecture-board-and-internet-corporation-for-assigned-names-and-numbers-in-the-matter-of-reporting-on-border-gateway-protocol-risk-mitigation-progress/

6. מפת דרכים לשיפור אבטחת ניתוב האינטרנט
   https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/09/Roadmap-to-Enhancing-Internet-Routing-Security.pdf

7. מערכת אוטונומית (אינטרנט)
   https://en.wikipedia.org/wiki/Autonomous_system_(Internet)

8. מערכת שמות מתחם
   https://en.wikipedia.org/wiki/Domain_Name_System

9. פרוטוקול תצורת מארח דינמי
   https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

10. אינטרנט דטרמיניסטי
    https://avinta.com/gallery/DeterministicInternet-SPKR.pdf

11. הילברטCurve
    https://en.wikipedia.org/wiki/Hilbert_curve

12. באמצעות עקומות הילברטויזואליזציה של מרחב IPv4
    https://thebayesianobserver.wordpress.com/2011/10/23/121/

13. מיקום גיאוגרפי באינטרנט

https://en.wikipedia.org/wiki/Internet_geolocation

14. רשת אספקת תוכן
    https://en.wikipedia.org/wiki/Content_delivery_network

15. רשימת מדינות לפי הקצאת כתובות IPv4
    https://en.wikipedia.org/wiki/List_of_countries_by_IPv4_address_allocation

16. ספלינטרנט
    https://en.wikipedia.org/wiki/Splinternet

17. ף' יוסטון: העבר, ההווה והעתיד של האינטרנט
    (TM: 1:08:18, "IPv6"רלוונטי פחות –)
    https://cloudflare.tv/this-week-in-net/geoff-huston-the-internet-s-past-present-and-future/dg78lmvO

הערת שוליים

DHCP ו-DNS הם צמד טכנולוגיות האינטרנט המדהים ביותר שעף על פני כולם במשך כל השנים הללו. כלומר, DHCP מבטיח פרטיות אישית על ידי הקצאת כתובות IP למנויים באופן דינמי לפי הצורך, רק כדי להישלל באופן מיידי ולחלוטין על ידי DNS שמציג, לפי בקשה, את כתובת ה-IP האחרונה שהוקצתה לצד מסוים, בהתבסס אך ורק על זהות אותו אדם! אלה הופכים מנויים רגילים ליענים עם אמונה כוזבת שהם מוגנים, תוך שהם שומרים על הרבה מהנדסי IT מועסקים ברווח. זוהי דוגמה מושלמת לפתגם הסיני "חנית מול מגן" (矛盾).

אף על פי כן, שכבות נוספות של פרוטוקולים המבוססים על תוכנית זו המשיכו להיבנות דרך BGP, AS ועד להקמת CDN שאפשרו את הדומיננטיות של קונגלומרט רב-לאומי, ועד שירותים גדולים כמו Cloudflare ו-AWS שהבטיחו לספק הובלת חבילות אמינה עם אבטחה משופרת. עם זאת, חוסנם של שירותים אלה היה באור הזרקורים לעתים קרובות. וכאשר האינטרנט נפרץ, איש לא נראה מוכן לקחת על עצמו את האחריות ולחפש חלופות להפחתת הפגיעות. אולי היה קשה להטיל אשמים, משום שכל האינטרנט היה כה מבוזר?

מצד שני, תצורת האינטרנט הנוכחית היא מתקן אידיאלי עבור עבריין שיכול פשוט להניח כל כתובת IP פיקטיבית שרירותית כמנוי אינטרנט רגיל ותוקף כדי להתחיל את ההתקפה, ואז לנטוש אותה לאחר מכן, וכמעט ולא להשאיר רשומות קבועות עם זהות תקפה למעקב משפטי.