לייעל את האינטרנט

1. רקע:

האימוץ המהיר והפריסה הרחבה של האינטרנט כדי להפוך לשדרת התקשורת העולמית דה פקטו לוו בבעיות הנעות בחומרה, מהטרדות סייבר ועד לפרצות אבטחה ועד לתוכנות כופר, ייתכן שהמקור של רבות מהבעיות הללו נמצא במאגר הכתובות של IPv4 מָחְסוֹר.

שדה משחק שווה לכולם הוא כבר מזמן חלק גדול מהצעת הערך של האינטרנט עם זאת, זה לא מציאות אפילו בפרקטיקה הבסיסית של הקצאת כתובות בהתבסס על אוכלוסיית העולם [1] והקצאת IPv4 הנוכחית. בארה"ב יש 4.91 כתובות לנפש, בעוד שחלקה של זמביה הוא רק 0.01, יחס העולה על שניים וחצי סדרי גודל של ותיקן 21.44 לנפש, בעוד שלמעלה מתריסר ישויות בעולם אין כאלה פערים מבהירים שעדיין נותר לעשות הרבה כדי להשיג את המטרה.

מאמצים להתגבר על מגבלות מאגר כתובות IPv4 הובילו לשימוש בכתובת דינמית, שהיא ביסודו הרבה יותר מעורבת מאשר המקבילה הסטטית שלו מסיבה כלשהי, מנגנונים דינמיים ממשיכים להיות בשימוש עם IPv6 בהיעדר מגבלות כאלה, ולא נראה שאיש. להטיל ספק ברציונל, אולי בגלל האמונה הנאיבית הרווחת שטיפול דינמי מגן על הפרטיות והביטחון. במציאות זה נכון רק עם פולשים מתחילים. מצד שני, כאשר מכוונים לגורמים ספציפיים כמו בתי ספר, בתי חולים, עסקים, ממשלות וכו', רוב כתובות ה-IP שלהם זמינות בקלות דרך שירות ה-DNS (מערכת שמות הדומיין) כדי להקל על מבצעים רציניים מנצלים את החולשות ב מערכת על ידי הסתתרות מאחורי כתובות פיקטיביות שניתן לשנות באופן שרירותי כאשר הם פותחים בהתקפות שלהם.

גרוע מכך, שיטת הכתובת הדינמית הקשה כל כך על ביצוע ניתוחים משפטיים של תעבורת אינטרנט, עד שהיא הצדיקה מעקב המוני ללא הבחנה על ידי רשויות אכיפת

החוק למען מניעת פשיעה מאחר שאין דבר שיעצור אף גורם אחר מלעשות את אותו הדבר. אם מצויד כך, בניתוח הסופי, אם בכלל, נותרה מעט פרטיות לאנשים רגילים זה הפך לנושא די שנוי במחלוקת ומפותל [3] .

זה נועד כתחליף לשיפור IPv4, זה הפתיע מאוד שהתברר שה-IPv6 לא תואם לאחור, מה שגרם למעבר מאתגר ויקר זה הצריך את יצירת פרוטוקול Dual-Stack הזמני [4] שהעלה את העלות תוך כדי לא ממש משחרר הרבה מהנכות המקורית.

קישוריות מקצה לקצה תמיד נכפתה כקריטריון ראשון לכל שיפורי אינטרנט מוצעים, אך ההשפעה המצטברת של האתגרים לעיל הובילה ל-CDN (רשת מסירת תוכן - מודל פעולת האינטרנט השולט כיום) המאופיינת ב-master-ארכיטקטורת עבדים שלמעשה מונעת תקשורת עמית לעמית ישירה בין משתמשי קצה, אפילו בתוך קהילה מקומית.

חלק נוסף בהצעת הערך המקורית של האינטרנט היה לשחרר את מערכות התקשורת הציבוריות מלהיות מונופול על ידי כמה ספקי טלקומוניקציה גדולים ומרגולציה על ידי סוכנויות ממשלתיות, עם זאת, שירות האינטרנט מחולק כעת למספר מגזרים עסקיים, כאשר כל אחד מהם מוגש על ידי קונגלומרט רב-לאומי דומיננטי יחיד (וכמה מתחרים קטנים יותר) שהוא כל כך חזק ומשפיע שהוא מסוגל להתחמק מהתקנות תוך הקטנת אחריות לבעיות שהוא יוצר.

יחד עם זאת, יש ביקורת רבה על המעורבות הגוברת של ממשלות ריבוניות ברחבי העולם בפעולות האינטרנט היומיומיות כמובילה לפיצול האינטרנט ל- Splinternet [5] העובדה היא ש-IAP (ספקי גישה לאינטרנט) חילקו את האינטרנט ארכיטקטורה ל-ASes רבים (מערכות אוטונומיות) [6] הדורשות BGP (Border Gateway Protocol) [7] כדי לחבר ביניהם.], בעוד ה-ASes כבר יצרו שכבות (כיום בסביבות K76 והולכות) [9] של רשתות כדוריות, כל אחת עוטפת את כל הגלובוס כמו שכבה אחת שלמה של קליפות בצל במובן מסוים, מספר ה"בצל-נטו" הללו. שכבות גדולות כמעט בסדרי גודל של שניים וחצי מזה של קטעי Splinternet פוטנציאליים, הניגוד הזה באמת מעורר מחשבה, אפילו לפני שמכירים בכך שמספר ה-ASes האפשרי

זהה למאגר הכתובות של 32 סיביות. 10] אולי ביקורת על Splinternet היא טקטיקה להסיח את תשומת הלב מהתמקדות ברשת הבצל.

כאשר כל האמור לעיל נלקח יחד, אין זה מפתיע שנדרש כל כך הרבה זמן כדי לאבחן ולהבין את היקף אירוע חירום באינטרנט, ועוד יותר מכך במקרה של פריצה זדונית – ימים, שבועות, חודשים או אפילו יותר זמן – פשוט להתחיל להעלות השערות לגבי הצד מאחורי מתקפת סייבר גדולה לשם השוואה, ה-PSTN המסורתי (Public Switched Telephone Network) מסוגל לאתר את המתקשר עוד לפני שמענה לשיחה.

לסיכום, חוסר היכולת של עיצוב האינטרנט המקורי, המבוסס על IPv4, לזהות באופן מפורש וייחודי כל אדם בעולם, הובילה לתרופות דינמיות שונות למרבה הצער, תרופות אלו גם סיפקו את ההסוואה המושלמת עבור עבריינים זדוניים שנועדו לתקוף משתמשים לגיטימיים אך פגיעים לגרסה החדשה ל-IPv6 יש די והותר כתובות לזהות את כל IoT (Internet of Things), תוכניות הביניים של IPv4 ממשיכות להיות מונצחות יתר על כן, מתקן ה-IPv6, שנאלץ להשתמש בסכימת Dual-Stack בגלל היעדר תאימות לאחור. מסובך ויקר יותר מ-IPv4 טהור, וכתוצאה מכך אזורים מתפתחים נלחצים לאמץ את ה-IPv6. לא בא בחשבון.

2. דרישות:

כדי לעקוף את הקיפאון הזה, פתרון מציאותי חייב להיות מסוגל להתקיים יחד עם הסביבה הנוכחית תוך התפתחות לעבר מערכת ארוכת טווח הגישה האידיאלית תהיה להציג תוכנית שמתנהגת כמו חלק מהמערכת הקיימת – ללא הפרעה לפעילות השוטפת. – אך יש לו את היכולת להתפתח לרשת שכבת-על שמתפקדת ללא תלות במתקן הבסיס, תוך שמירה על ממשקים באורך זרוע בין השניים למען יכולת פעולה הדדית ושלמות השירות הכוללת. אלה יתפתחו בהדרגה לשתי מערכות הפועלות במקביל, תוך שימוש באותה טכנולוגיה , אך הקפדה על דיסציפלינות תפעוליות שונות כדי לספק שירותים דומים. זה יאפשר למשתמשי הקצה להתנסות אישית ולהשוות את היתרונות והחסרונות של

שניהם כדי לבחור מושכלת עבור התצורה המועדפת לטווח ארוך.

3. פתרון:

למרבה המזל, זוהתה תכנית קומפקטית [11] שיכולה להתמודד עם רוב הנושאים שנדונו עד כה. הגישה הבסיסית של תכנית זו היא להשתמש ב-240/4 נטו בלוק הקיים ב- CDN, CG-NAT. (Carrier Grade - Network Address Translation) להקמת מתקן חדש, הנקרא SPR (Semi-Public Router), לכיסוי תשתית האינטרנט הנוכחית לא נדרשת טכנולוגיה חדשה בתהליך של פריסה כזו לאורך זמן.

עם מספיק כתובות סטטיות לזיהוי כל משתמש, SPR אינו זקוק ל-DHCP (פרוטוקול תצורת מארח דינמי) מה שמותיר ל-IAP לא כתובות שהוקצו לה. אינם נחוצים עוד, סביבת האינטרנט החדשה הזו פשוטה בהרבה.

כדי להשתמש בבלוק ה-240/4 שנמצא בסטטוס "שמור" כל כך הרבה זמן, ייתכן שיהיה קשה למצוא ציוד זמין לבדיקת יכולת המכשיר ואימות ביצועי הרשת. כמו כן, מתקן כזה חייב להיות תמציתי, נמוך עלות ומינימלית בעקומת הלמידה שלה על מנת לעודד כמה שיותר מתעניינים להתחיל את המעבר המוצע הזה.

להלן מתאר את הציוד והתהליך הבסיסיים להקמת מיטת מבחן לניסויים והדגמות לאחר מכן ניתן ליישם את המיומנויות והניסיון שנרכשו מהאחרונים כדי לסייע בפריסה בפועל של SPR.

. מכשיר מסוף:

Xubuntu [12] V18.04.1 זוהה כמועמדת מערכת ההפעלה הנוחה ביותר מכיוון שהיא יכולה לקבל כתובות IP כפולות בו-זמנית באותו מחשב נייד מארח (מחשב אישי, כלומר, כל מחשב מצויד כזה מתנהג כמו שני IoTs). חולקים את אותה יציאת רשת חומרה, כלומר, לקוח משותף עם כתובת DHCP לצד לקוח סטטי. שניהם יכולים לקבל את הכתובת המוכרת של IPv4 או 240/4 תהליך הרשת המקובל לאחר מכן, ה-IoT הכתובים הסטטיים באותו זוג מחשבים יכולים לאמת את

מאפייני השידור בסביבת 240/4 ללא שינויים בהגדרות החומרה או אתחול מחדש של המחשבים מבטיח שהמדיום מוכן לשינוע מנות עם כל כתובת IPv4 בכל אחת מהקטגוריות בנוסף, ניתן להשתמש במחשבים אלה עם IoT חדש דרך המדיום הזה כדי לאמת את תאימותו לפני פריסתו לשטח.

. סימולטור רשת:

מיטת בדיקה תואמת 240/4 משמשת כבד הבסיסי למכשירים תואמים מתאימים ולבדיקת ביצועי השידור שלהם.

ת. לנקודת התחלה סופית, RG (Routing/Residential Gateway) צריך להיות בעל יכולת מלאה ל-240/4 על ידי התקנת קושחה של OpenWrt [13] V19.07.3, ומעלה, שתומכת ברשימה ארוכה של RGs מסחריים רשתות LAN מקומיות (רשתות מקומיות) ו-HANs (רשתות אזוריות ביתיות) המשרתות הן IoTs מסורתיות והן אלה המניחות כתובות 240/4, תוך שהם מתנהגים כמו לקוחות DHCP 240/4 לאינטרנט.

ב. כדי לספק מארג שידור בסיסי בין הנחות (המיוצגות על ידי ה-RGs לעיל) הפועלות כ-SPR, מתג D-Link מנוהל חכם 14] DGS-1210 Series] תומך ב-OpenWrt הם מועמדים טובים.

בזמן ש-SPR נבנה, הוא יוצר רשת שכבת-על המשרתת למעשה את אותם הנחות עם אותן פונקציות כמו מארג ה--CG NAT הקיים, מלבד שסכימת הניתוב המוגדרת כברירת מחדל הופכת להיראכית כדי בסופו של דבר לשכפל CG-. לאחר מכן, ניתן להגיש מספר CG-NAT אשכולות מ-SPR אחד על ידי ניצול מלא של גודל Netblock 240/4 שהוא פי 64 מזה של Netblock 100.64/10 אשר קובע את הגבול על הקיבולת של CG-. אשכול NAT ללא הקצאה דינמית מחדש בהתאם לגודל האוכלוסייה שיש לשרת, RAN (Regional Area Network) 15]] עשוי להיות מורכב מ-SPR אחד או יותר.

4. מסקנה:

מאז שה-240/4 הרשת הוגדרה באופן רשמי כ"שמור לשימוש עתידי" או "ניסיוני" במשך כל כך הרבה שנים, התעוררו באופן טבעי שאלות לגבי האם ניתן להשתמש בו בקונגלומרטים עסקיים רב-לאומיים שמשתמשים בפועל ב-240 /4 netblock למטרות שונות ללא הכרזות [16] העובדה שנדרש מאמץ כדי לגלות פעילויות כאלה מעידה על כך שהשימוש ב-240/4 netblock אינו משבש ולא ישבש את פעולות האינטרנט הקיימות רכב אידיאלי לפריסת ה-SPR המוצע.

באמצעות כתובות סטטיות, ה-RAN ייעל את פעולת האינטרנט באמצעות ניתוב היררכי המאפשר לציבור הרחב ליהנות מתקשורת עמית לעמית, ללא דומיננטיות של קונגלומרטים עסקיים רב-לאומיים האופי הסטטי של תכנית הכתובת מאפשר ל-RAN להיות יותר דטרמיניסטית מהאינטרנט הקיים מבוסס CDN, ולפיכך חזק יותר מפני פריצות סייבר.

למידע נוסף, קיים ספר לבן מקוון [17] המנתח הצעה זו מנקודת מבט מכוונת יותר לעסק.

הפניות:

[1] מדינות בעולם לפי אוכלוסיה;
https://www.worldometers.info/world-/population/population-by-country

[2] רשימת מדינות לפי הקצאת כתובות IPv4:
https://en.wikipedia.org/wiki/List_of_countries_by_IPv4_address_allocation

[3] מצב פגיעות אבטחת סייבר
https://blog.apnic.net/2021/02/03/the-internet-of-/trash

[4] IPv6:
https://en.wikipedia.org/wiki/IPv6

[5] ספלינטרנט
https://en.wikipedia.org/wiki/Splinternet#:~:text=The%20splinternet%20(also%20referred%20to,religion%2C%20and%20divergent%20national%20interests.

[6] מערכת אוטונומית
https://en.wikipedia.org/wiki/Autonomous_system_(Internet)

[7] פרוטוקול שער הגבול
https://en.wikipedia.org/wiki/Border_Gateway_Protocol

[8] מדינות בעולם
https://www.worldometers.info/geography/how-many-countries-are-there-in-the-world/#:~:text=There%20are%20195%20countries%20in,and%20the%20State%20of%20Palestine

[9] מספר ASes נוכחיים
https://thyme.apnic.net/current/data-summary

[10] מספרי מערכת אוטונומית
https://www.arin.net/resources/guide/asn/

[11] פטנט אמריקאי מס' 11,159,425
https://image-ppubs.uspto.gov/dirsearch-public/print/downloadPdf/11159425

[12] Xubuntu
https://xubuntu.org/

[13] OpenWrt
https://openwrt.org/toh/start?toh.filter.supportedcurrentrel=22.03%7C23.05

[14] מתגים חכמים מסדרת D-Link DGS-1210
https://www.dlink.com/us/en/products/dgs-1210-series-gigabit-smart-plus-switches

[15] סימולטור רשת אזורית
https://www.avinta.com/gallery/RegionalAreaNetworkSimulator.pdf

[16] שימוש 240/4 ללא הודעה מוקדמת
https://labs.ripe.net/author/qasim-lone/2404-as-/seen-by-ripe-atlas

[17] חידוש האינטרנט:
https://www.avinta.com/gallery/RevampTheInternet.pdf

טרמינולוגיה, קיצור וראשי תיבות:

AS: מערכת אוטונומית

BGP: Border Gateway Protocol

CDN: רשת אספקת תוכן .

CG-NAT: תרגום כתובות רשת מסוג Carrier

DHCP: פרוטוקול תצורת מארח דינמי.

DNS: מערכת שמות מתחם.

Dual-Stack: סביבת רשת התומכת בשימוש בו-זמני של כתובות IPv4 ו-IPv6.

HAN: רשת ביתית (רשת מקומית למסיבות פרטיות/מגורים)

IAP: ספק גישה לאינטרנט .

IoT: האינטרנט של הדברים.

IPv4: פרוטוקול אינטרנט גרסה 4 .

IPv6: פרוטוקול אינטרנט גרסה 6 .

LAN: רשת מקומית (רשת מקומית המשמשת מוסדות)

מערכת הפעלה: מערכת הפעלה

PC: מחשב אישי

PSTN: רשת טלפונים ציבורית

RAN: רשת אזורית

RG: ניתוב/שערים למגורים

SPR: נתב חצי ציבורי

Netblock 4/240.: מאגר כתובות IPv4 הנע בין 240.0.0.0 ל-255.255.255.255, בהיקף של כ-256 מיליון (256 מיליון) או רבע מיליארד (B0.256) כתובות שלא היו בשימוש רשמי מאז 1981-09 סומנו כ"ניסיוני" או "שמור" עבור "שימוש עתידי".

https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml