לחדש את האינטרנט

1. רקע: למרות האימוץ המהיר והפריסה הרחבה של האינטרנט כדי להפוך לתשתית התקשורת העולמית דה פקטו, תמיד הייתה דאגה מציקה לגבי פגיעותה לפריצת אבטחה. כלומר, בהשוואה ל-PSTN המסורתי המסוגל לאתר את המתקשר עוד לפני שמענה לשיחה, מדוע לאינטרנט לוקח כל כך הרבה זמן, ימים, חודשים או אפילו יותר, עד שפשוט מתחילים לשער מי מבצע מתקפת סייבר גדולה?

הסיבה לבעיה זו נעוצה בעובדה שלעיצוב האינטרנט המקורי מבוסס 4IPv לא היה מאגר כתובות גדול מספיק כדי לזהות באופן מפורש וייחודי את כל IoTs שנמצאים בשימוש. פותחו תוכניות ביניים שונות כדי להתמודד באופן דינמי עם מוגבלות זו. למרבה הצער, הם גם סיפקו את ההסוואה המושלמת עבור העבריינים, בעוד המשתמשים הרגילים ישבו ברווזים בשטח הפתוח. למרות שלגרסה החדשה, ל-6IPv יש יותר ממספיק כתובות לזהות את כל IoT, איכשהו השימוש בסכימות הביניים נמשך. יתר על כן, 6IPv מסובך ויקר יותר מ-4IPv, מה שגורם לאזורים פחות ברי מזל לאמץ את 6IPv. החלפה מלאה לכל מערכת גדולה בשימוש מתמשך כמו האינטרנט אינה באה בחשבון. כדי לעקוף את הקיפאון הזה, תוכנית שיכולה להתקיים יחד עם הפרקטיקות הנוכחיות תוך שיפורן לעבר מערכת ארוכת טווח היא המקום הריאלי היחיד.

2. פתרון: למרבה המזל, התגלה שחלק ניכר (שש עשרה, ליתר דיוק) ממאגר הכתובות של 4IPv, הנקרא 4/240, netblock, "שמור" ל"שימוש עתידי" מאז הימים הראשונים. כתוצאה מכך, אף אחד מציוד האינטרנט הנוכחי אינו מסוגל להשתמש בו. זה מציע הזדמנות ייחודית לסוג חדש של נתבים להשתמש בו לזיהוי עד 256 מיליון IoT מכל כתובת 4IPv קיימת. מנוהלת כהלכה, מערכת תקשורת עולמית ניתנת להתייחסות מלאה מקצה לקצה, לא רק מספקת את כל השירותים הרצויים באופן אחיד לכל מנוי, אלא גם מפחיתה את הגורם השורשי של פגיעות אבטחת הסייבר, הכל במסגרת טכנולוגיית ה-4IPv הקיימת.

3. פריסה מדורגת: כדי להשתלב במצב הפעולה הנוכחי של שרת-לקוח אינטרנט, ניתן לפרוס את הגישה שלעיל באופן מיידי עם פורמט מנוון, לפיו נעשה שימוש ב-4/240 netblock כאילו היה מאגר כתובות הרשת הפרטיות הרביעי, ב תוספת ל-16/192.168, 12/172.16 ו-8/10. שלב ההיכרות הזה דורש רק את הפעלת ה- 4/240netblock, מבלי לשנות שום דבר אחר בעיצובי 4IPv קיימים.

4. יישום: גישה זו כמעט ולא דורשת מאמץ הנדסי כלשהו. עלות הפריסה זהה לציוד ה-4IPv הנוכחי המקביל. בנוסף, הוצאות התפעול יופחתו בשל שיטות העבודה היעילות המפחיתות את ההפרעות כגון התקפות סייבר:

א. פיתוח מוצר (ProDev): פשוט השבת את קודי התוכנה הקיימים שהשביתו את השימוש ב-4/240 netblock.

ב. הוצאות הון (CapEx): זהה לציוד 4IPv הנוכחי עבור אותה יכולת שירות, על ידי שימוש באותה חומרה.

ג. הוצאות תפעול (OpEx): מופחתות על ידי שיטות יעילות שאינן מסתמכות על תוכניות דינמיות.

ד. אבטחת סייבר: משופרת על ידי ניהול זיהוי (כתובת) IoT דטרמיניסטי.

5. פעולות מוצעות:

א. עם המאפיינים הטבועים של התחלת שירותי אינטרנט מרשת פרטית ללא מאמצי פיתוח, המערכת המוצעת הזו עשויה להיפרס על ידי כל גורם מעוניין (סוכנויות ממשלתיות, עסקים, יזמים וכו') מכתובת 4IPv תקפה זמינה תוך שימוש בציוד 4IPv קיים.

ב. מאחר שגישה זו היא גנרית במהותה, מומלץ להיבדק על ידי D-ITU על התאמתה בפריסה אוניברסלית לחידוש האינטרנט.

הפניות:

א. מצב פגיעות אבטחת סייבר

https://blog.apnic.net/2021/03/02/the-state-of-internet-security/trash/

II. הדגמת היתכנות שניתן לשכפל בקלות של הצעה זו.

https://www.avinta.com/phoenix-RegionalAreaNetworkArchitecture/home/1.pdf

III. הערה לבלוג של IAB: הצעת תכנית זו כדי להקל על השתתפות משתמש הקצה בפיתוחי פרוטוקול/מוצר.

https://blog.apnic.net/2020/08/31/rfc-8890-the-internet-is-for-end-users/

IV. טיוטת IETF: פרטים טכניים של הצעה זו

https://datatracker.ietf.org/doc/html/draft-chen-ati-adaptive-4ipv-address-space

V. קניין רוחני: מס' פטנט אמריקאי: 11,159,425

טרמינולוגיה, קיצור וראשי תיבות:

. NAT-CG: Carrier Grade Network Address Translation

. DHCP: פרוטוקול תצורת מארח דינמי

. DNS: מערכת שמות מתחם

. IAB: מועצת אדריכלות האינטרנט

. IETF: כוח המשימה להנדסת אינטרנט

. IoTs: האינטרנט של הדברים

. IPv4: פרוטוקול אינטרנט גרסה 4

. IPv6: פרוטוקול אינטרנט גרסה 6

. D-ITU: איגוד התקשורת הבינלאומי – מגזר הפיתוח

. PSTN: רשת טלפונים ציבורית

. Netblock 4/240: מאגר כתובות 4IPv הנע בין
240.0.0.0 ל-255.255.255.255, בהיקף של בערך 256
מיליון (256 מיליון) או רבע מיליארד (B0.25) כתובות

https://www.iana.org/assignments/ipv4-address-space
xhtml.space-address-4ipv/space