BGP Hijacking - או עד כמה קל להפיל את האינטרנט?

מאת דן פייגין

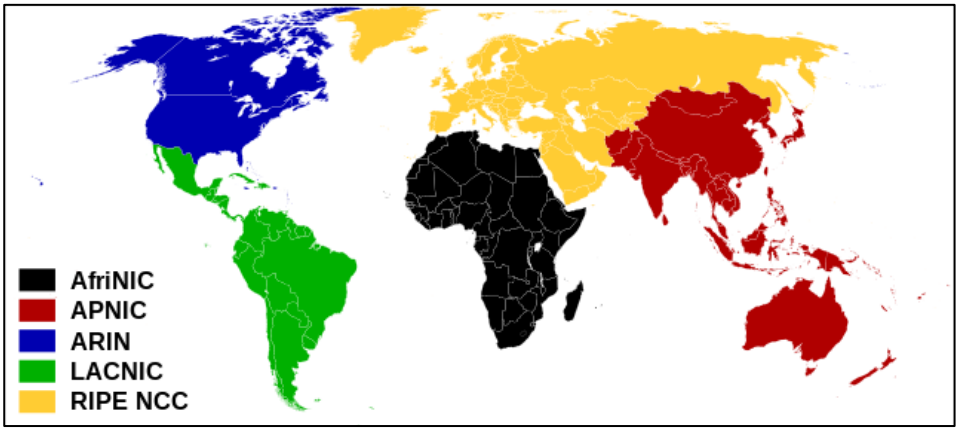
הקדמה

רבים מקוראי המגזין מכירים כיצד פועלות רשתות ביתיות, איך עובדים רכיבים כמו Router או Switch, וכנראה אף מכירים מספר סוגי תקיפות אשר רשתות כאלה והפרוטוקולים המנחים אותן מאפשרים. חבילת מידע אשר נשלחת ממחשב אל עבר הרשת אליה הוא מחובר, מועברת דרכה לספקית האינטרנט (ISP), נדרשת להגיע איכשהו למחשב אחר אשר נמצא ב-ISP אחר. על ניתוב החבילות הללו בין ה-ISPs, אשר חוצה מדינות ויבשות, מושל פרוטוקול ה-BGP (Border Gateway Protocol).

במאמר זה נכיר את הפרוטוקול ואת אופן הפעולה שלו, את מידת האבטחה שלו, ואף נראה סוג מתקפות לדוגמא ודוגמאות אמיתיות למתקפות BGP אשר תועדו בעבר.

IP Addresses and ASes

במישור ניהול האינטרנט, העולם מחולק לחמישה אזורים, ובכל אחד מהם קיים גוף אשר אחראי לניהול והקצאת כתובות IP (RIR - Regional Internet Registry). מרחב כתובות ה-IP העולמי מנוהל ע"י גוף בינלאומי בשם IANA (Internet Assigned Numbers Authority). גוף זה אחראי על הקצאת כתובות IP ל-RIRs השונים.



[מקור - ויקיפדיה:RIR]

היחידה הבסיסית לתיאור רשת אשר מחזיקה ברשותה טווח כתובות IP היא Autonomous System (AS). AS יכולה להיות ISP או כל ארגון גדול אחר אשר מחובר ישירות לאינטרנט, כאשר לכל AS מסופק מספר ייחודי (AS Number - ASN). ברשת האינטרנט, כל AS כזו מוגדרת כצומת ניתוב, כאשר בתוך הרשת הפנימית שלה, הניתוב יכול להתבצע כראות עיניה, אך על מנת להתממשק מול העולם החיצון, על ה-AS להחזיק נתבי BGP.

ניתן דוגמא: כאן בתל אביב, מוקצה לי IP (חיצוני) מספקית האינטרנט שלי, Primo Communications LTD, לצורך העניין - 185.120.125.5. ה-IP הזה הוא חלק ממרחב כתובות גדול יותר - 185.120.125.0/24 (על CIDR notation ניתן לקרוא כאן). טווח זה מכונה Prefix. Prefix זה הינו בבעלות Primo, והוא מוכרז כחלק מ-AS8948. Primo מכריזה על prefixes נוספים, כאשר 185.120.125.0/24 הוא רק אחד מהם. כעת, נניח ואני רוצה לשלוח חבילת מידע לצידו השני של העולם. בסופו של דבר החבילה תעזוב את הרשת של ה-ISP שלי, ועל כן יש צורך בניתובה ל-ISP אחר. כאן BGP נכנס לתמונה.

Border Gateway Protocol

BGP בגרסתו הנוכחית (BGP4) נמצא בשימוש באינטרנט מאז 1994, ובבסיסו מורכב משני פרוטוקולים:

- **Interior BGP / iBGP**: פרוטוקול בין שני נתבי BGP בתוך AS, שמטרתו ללמד את הנתבים הפנימיים לגבי כתובות IP מחוץ ל-AS.
- **Exterior BGP / eBGP**: פרוטוקול בין שני נתבי BGP של ASes שכנים (BGP Peers). זה הפרוטוקול בו נתמקד על מנת להבין את הניתוב ברמת האינטרנט העולמי.

מכיוון שכל AS מחזיקה טווח כתובות IP, מטרת פרוטוקול ה-BGP היא כפולה:

1. לאפשר ל-AS להבין, בהינתן כתובת IP, לאיזה AS שייכת כתובת ה-IP, ומהו ה-path של ASes שדרכו על התעבורה לעבור על מנת שבסופו של דבר התעבורה תגיע ל-AS הנכונה.
2. לאפשר ל-AS להכריז בפני שכניה (BGP Speaker) אילו כתובות IP נמצאות ברשותה (origin), על מנת לקבל תעבורה המיועדת לכתובות IP אלו.

וכעת נצלול לפרוטוקול

כאשר AS כלשהי, למשל AS x, רוצה להכריז בפני שכניה, y ו-z, שיש ברשותה את טווח כתובות ה-IP a.b.c.d/16, היא שולחת חבילת BGP Announcement אשר מכילה את ה-prefix ואת ה-ASN שלה ל-peers שלה. כעת ה-peers של AS x יודעים שכדי לשלוח תעבורה לכתובת IP תחת ה-prefix a.b.c.d/16, עליהם להעביר תעבורה ישירות ל-AS x. כעת AS y ו-AS z יכולים לחלחל את הידע הזה הלאה לשכניהם, ע"י שרשור ה-ASN שלהם להודעה. כך ה-peers שלהם ידעו שכדי להגיע לכתובת ה-IP תחת ה-prefix הנ"ל יש להעביר תעבורה ל-y/z. על מנת להימנע ממעגלים, ASes מפילות BGP Announcements שמכילות את ה-ASN שלהן עצמן.

BGP Policies

מה קורה כאשר BGP peer מקבל שתי הצעות ניתוב לאותו prefix? התשובה כאן היא שבאופן עקרוני - אין לדעת. לכל AS יש policy משלה לגבי איזה BGP Announcement היא מעדיפה לקבל ואיך היא מעדיפה לנתב את התעבורה שלה. ה-policies האלה מהוות סוד מסחרי של ה-AS, אך באופן אמפירי נראה שיש העדפה למסלולים קצרים ולכאלה שמיטיבים באופן כלכלי עם ה-AS (בין ASes יכולים להיות יחסי Provider-Customer, בהם תעבורה עוברת בתשלום, או יחסי Peer-Peer, בהם התעבורה אינה עוברת בתשלום).

BGP Sessions

BGP הוא פרוטוקול בשכבת האפליקציה בין שני BGP-enabled routers, כאשר מתחת לכובע הוא ממומש מעל TCP Session בפורט 179, כאשר כל BGP Speaker שולח הודעת Keep-Alive של 19 בתים מדי 60 שניות על מנת לשמור על חיבור.

כיצד ניתן להתחזות לנתב BGP? ובכן, ראשית יש לאתר שני נתבי BGP אשר קיים ביניהם session פעיל. כאמור, BGP רץ מעל TCP, ולכן יש צורך לבצע TCP Hijacking. לא נרחיב כיצד מבצעים TCP Hijacking על מנת שלא להיכנס ליותר פרטים. רק נציין שכדי לבצע זאת יש לשלוח חבילה עם פרמטרים נכונים, ובפרט sequence number נכון, אחרת החבילה תיפול (להרחבה ניתן לקרוא כאן). לכן אם ניתן להסניף את התעבורה של ה-Session או אם יש יכולת להיות MITM, זה הרבה יותר קל. לאחר מכן, כדי להכריז הודעת BGP כוזבת, ניתן להכין payload בינארי של BGP Update בעזרת כלים פומביים להרכבת חבילות (IPsend, Spoof), ולצרף אותו כ-payload לחבילת ה-TCP.

הנ"ל כמובן מתייחס למצב שבו התוקף אינו AS אלא מתפרץ ל-Session קיים. כאשר התוקף (במזיד או בטעות) הוא AS, אזי מעבר ליכולות פילטור עצמאיות ומשתנות של ASes אחרות, אין דבר המונע מ-AS להכריז הודעה כוזבת ולשבש תעבורה (דוגמאות בהמשך).

Prefix Hijacking

BGP הוא פרוטוקול מבוזר, כלומר, אין בסיס מידע ראשי שממנו שואבים כל ה-AS את מסלולי הניתוב האופטימאליים, והחלטות הניתוב יכולות להשתנות באופן דינאמי על בסיס המידע הנתון לכל AS באותו רגע.

Prefix Hijacking הוא שיטת השתלטות על קבוצת IPs במזיד או בטעות, אשר יכולה להיגרם מכל אחד מהתרחישים הבאים:

- BGP Speaker מכריז שהוא המקור של קבוצת IPs שאינה באמת ברשותו.
- BGP Speaker מכריז על prefix יותר ספציפי מה-prefix שהוכרז ע"י AS אחרת (prefix A מוגדר להיות יותר ספציפי מ-prefix B אם כל כתובות ה-IP של A מוכלות ב-prefix B. למשל, 8.8.8.8/20 יותר ספציפי מאשר 8.8.8.8/12). עבור כתובת IP ששייכת הן ל-prefix A והן ל-prefix B, העדפת הניתוב הדיפולטית היא ל-AS שהכריז על prefix יותר ספציפי.
- BGP Speaker מכריז על path המוביל ל-AS אשר יותר קצר (אינו בהכרח כזה שקיים) מכל ה-paths הזמינים.

בכל המקרים הללו, נתב eBGP יוסיף באופן דיפולטיבי את הכללים הנ"ל ל-routing table של ה-AS, ויחלחל באופן דיפולטיבי את מירב ההודעות שקיבל הלאה לנתבי eBGP אחרים.

באופן כזה, ניתן להשתלט על כלל התעבורה המיועדת לטווח כתובות IP מסוים. ניתן להעלות את השאלה : מדוע לתקוף בשיטה הזו? לכך יש מספר סיבות נפוצות:

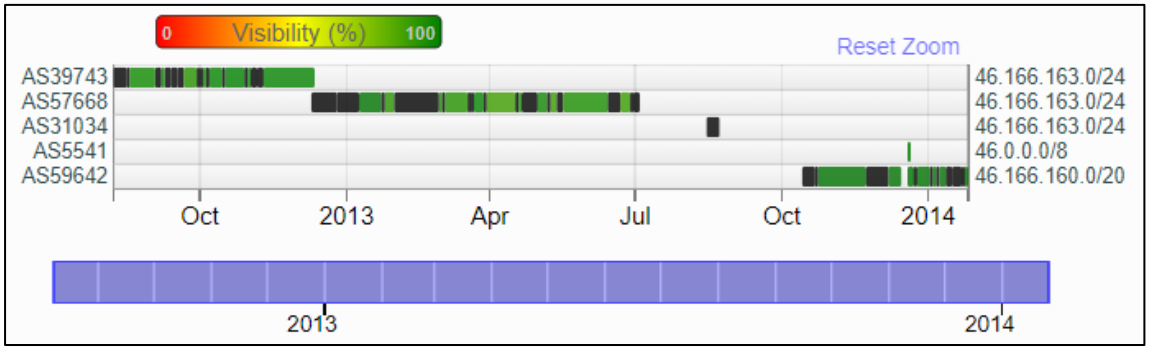
- גניבת כתובות IP "נקיות" לשם Spam או DDOS.
- לעיתים קשה לשחזר היסטוריה ולהבין מה היה ה-state של טבלת הניתוב וקשה למצוא תוקפים.
- MITM בוטה ופשוט - ניתן לכוון כנגד prefix, AS (ארגון) או קבוצת ASes (מדינה).

דוגמאות אמיתיות

1. עפ"י נתונים שנחשפו ע"י Wikileaks, ארגון ROS (ארגון בממשלת איטליה הנלחם בארגוני פשע) משתמש בתוכנת RAT (Remote Access Tool), תוכנה המאפשרת שליטה מרוחקת על מחשב, על מנת לעקוב אחר ארגוני הפשיעה במדינה. התוכנה מורכבת מ-client ו-server. ביולי 2013, נתקל הארגון בבעיה - ה-Prefix בו ישב ה-server אליו התחברו ה-clients, 46.166.163.0/24, הפך unreachable. על מנת לפתור את הבעיה במהירות, ולאפשר ל-clients להתחבר ל-IP תקין, ROS עבדה ביחד עם ספקית האינטרנט האיטלקית Aruba S.p.A (AS31034), ושתיהן הרימו server חדש עם כתובת ה-IP שאליה היו אמורים להתחבר ה-clients.

הן השיגו זאת ע"י כך ש-AS31034 הכריזה על BGP Announcement ומכילה את ה-Prefix שבו ישב ה-server, ומשכה אליה תעבורה שהייתה מיועדת ל-46.166.163.0/24 (לא כל התעבורה הגיעה אליה, שכן היו ASes שפילטרו את ההכרזות בהבנה שמדובר בהכרזות פיקטיביות). עם זאת, הפעולה עדיין הצליחה, וה-clients התחברו ל-server החדש, והיה ניתן לקנפג אותם להתחבר ל-IP חדש.

נקודה למחשבה - כיצד ניתן לאמת את הנתונים של המקרה? למזלנו, קיימים מאגריים עולמיים אשר מסניפים תעבורת BGP. מאגרים אלו מכונים collectors והם פזורים ברחבי העולם. בעזרת שירותי ויזואליזציה של מאגרי ניתוב שונים (ThousandEyes, BGPlay, וכו') ניתן לבחון היסטורית מה היה הסטטוס של כל prefix. אכן, ניתן לראות כי עבור תקופת הזמן הרלוונטית - קיץ 2013, ועבור ה-prefix הרלוונטי, קיימת קפיצה חדה בכמות ה-peers שחושבים שה-origin שלו הוא AS31034.



[מקור-ripestat.ripe.net]

2. בשנת 2008, ממשלת פקיסטן מחליטה לחסום את הגישה לאתר YouTube במדינה. אופן יישום ההחלטה הוא ע"י Prefix Hijacking. ה-IPs שפקסיטן רצתה לחסום היו: 208.65.153.238, 208.65.153.251, ו-208.65.153.23. על מנת לממש את החסימה, הספקית Pakistan Telecom (AS17557) הכריזה את ה-prefix 208.65.153.0/24 (כל הכתובות בטווח 208.65.153.255-208.65.153.0). עם זאת, באותה תקופה היה בבעלות YouTube (AS36561) ה-prefix 208.65.152.0/22, כלומר כל הכתובות בטווח 208.65.152.0-208.65.155.255. עם זאת, ה-prefix 208.65.153.0/24 הכיל את כל שרתי ה-DNS ושרתי ה-Web של החברה. מובן ש-/24 הוא יותר ספציפי מ-/22, וכאמור, נתבים מעדיפים באופן דיפולטי prefixes שהם יותר ספציפיים, ולכן ה-BGP Announcement חלחל הלאה, וכלל תעבורת YouTube הגיעה ל-Pakistan Telecom. גם כש-YouTube הכריזה על 208.65.153.0/24 זה לא עזר לפתרון הבעיה, שכן היא עדיין התחרתה עם Pakistan Telecom, ומי שזכה בתחרות הניתוב היה זה בעל הנתיב הקצר ביותר. התעבורה חזרה ל-YouTube רק כאשר היא הכריזה על ה-prefix 208.65.153.128/25, שהוא ספציפי יותר, וכך הנתיב אליה היה מועדף. בסה"כ YouTube הייתה ב-downtime של למעלה משעתיים. ניתן לשים לב ממקרה זה שתוקף יכול להרוג valid paths ע"י יצירה של bogus paths מתאימים.

קיימות דוגמאות רבות נוספות, החל ממעקב וצנזורה כנ"ל (חסימת Telegram ביולי 2018 ופורנוגרפיה בינואר 2017 ע"י איראן), עבור בגניבה של מטבעות וירטואליים (ע"י ישיבה כ-MITM על תעבורה רחבה - גניבת תעבורה של שרתי DNS של Amazon באפריל 2018 ושל ISPs קנדיים בפברואר 2014), וכלה בהשבתה המונית של חלקים נרחבים מהאינטרנט (ע"י סין ב-2010) והן מתרחשות באופן תדיר, חלקן במכוון וחלקן בטעות.

RPKI ו-BGPsec

מתקפות המנצלות את פרוטוקול ה-BGP קשות למניעה, בעיקר בגלל האופן שבו הפרוטוקול תוכנן, תכנון אשר אינו מאפשר את אימות דיוק נתוני הניתוב. על כן, קיימים מאמצים לשפר את BGP. שיפור משמעותי לכך מגיע בדמותה של BGPsec. הרחבה לפרוטוקול הכוללת מספר הגנות שנועדו להגדיל את רמת האבטחה של BGP, בעיקר ע"י שילוב יכולות קריפטוגרפיות. כל AS תחזיק רשימה חתומה דיגיטלית אשר מכילה מיפוי של IP prefixes ל-origin AS (פיצ'ר זה מכונה RPKI - Resource Public Key Infrastructure). בנוסף, כל AS תחזיק certificate על מנת לאפשר חתימה על paths, כך שבכל קפיצה בשרשרת הניתוב ה-AS תחתום על ה-path. בנוסף, BGPsec דורש את הוספת ה-ASN של ה-peer שההודעה מיועדת אליו, וגם חלק זה חתום דיגיטלית. כלומר, בכל פעם ש-AS תקבל BGP Announcement, היא תוכל לוודא שה-path נכון וההודעה אכן מיודעת אליה, ע"י וידוא החתימה ע"י כל ה-ASes הרשומות ב-path, וכשתרצה לשלוח BGP Announcement חדש, היא תשרשר את ה-ASN שלה ושל ה-ASN של ה-peer אליו היא רוצה לשלוח את ההודעה, ותחתום על ה-path החדש עם המפתח פרטי שלה.

עם זאת, שיעור האימוץ של BGPsec די נמוך. BGP הוא פרוטוקול דינאמי שמנצל משאבי ריצה רבים, ועל כן תוכנן להיות יעיל. הודעות BGP updates מאובטחות הן בהכרח גדולות יותר, בגלל המידע הנלווה ובגלל תוספת החתימות. בנוסף, זמן עיבוד כל הודעה יגדל, בגלל שהוא דורש וידוא של מספר חתימות (כאורך ה-path), וזאת בכל hop בדרך. רק לשם המחשה, עם טבלת ניתוב גלובאלית בגודל של יותר מחצי מיליון IPv4 prefixes ועם path באורך ממוצע של 4 AS hops, מדובר בוידוא של יותר מ-2 מיליון חתימות באתחול של נתב BGP. על כן, ASes תדרשנה בחומרה מתאימה יותר לחישובים קריפטוגרפיים מהירים.

בנוסף, שימוש ביכולת אבטחתית כזו מתאפשר רק ב-deployment שבו קיימת שרשרת מקצה לקצה של ASes שאימצו את השיטה, אחרת לא ניתן יהיה לוודא את נכונות ה-path. רק החלפת החומרה לבדה מהווה הבטחה ל-deployment איטי של שדרוגי אבטחה מסוג זה, כך שנוסף על הצורך בהשקעה משותפת של ASes, זה לא מפתיע ש-ASes גדולים ומרכזיים לא ששים להחליף את כל נתביהם ברחבי

העולם. משום כך גם אימוצו של BGPsec ע"י ASes קטנים יותר אינו כדאי מבחינה כלכלית, ועל כן סך שיעור האימוץ נשאר קטן.

ובכל זאת - מה ניתן לעשות?

ב-BGP4 יש כשלים אבטחתיים חמורים, ולא ניתן לראות את אימוץ הפתרונות להם באופק הקרוב. על כן, כפתרון ביניים, חברות מאמצות מנגוני פיקוח - זיהוי אנומליות וזיהוי הסטת תעבורה, ניטור Sessions, כל זאת על מנת שבהינתן מתקפת BGP, יהיה ניתן לזהותה בזמן אמת ולתקנה (ע"י קנפוג ידני של הנתבים) לפני שהשפעתה על החברה ועל הלקוחות תורגש.

סיכום

BGP מאפשר לחבר בין רשתות שונות ברחבי העולם, והוא זה ששם את המילה Inter ב-Internet. עם זאת, הפרוטוקול תוקנן כשהמודעות לאבטחה הייתה בחיתוליה. על כן המצב כיום הוא שרוב תשתיות הניתוב העולמי מיושנות ובעלות כשלים אבטחתיים חמורים בשל השימוש ב-BGP. מכיוון שהפרוטוקול שזור בתשתית האינטרנט העולמי וקיים במספר רב של רשתות אשר מתופעלות ומתוחזקות ע"י מספר רב של ארגונים, אימוץ תיקונים אבטחתיים הוא מאתגר הן ברמה הטכנית והן ברמה האבטחתית.

קישורים

1. פירוט ה-prefix תחת כל AS:

https://www.dan.me.uk/bgplookup

2. ניתוח מקרה חטיפת BGP ע"י ראוטר מספקית קנדית לטובת מעקב / אחר כורי ביטקויין:

https://www.secureworks.com/research/bgp-hijacking-for-cryptocurrency-profit

3. ניתוח מקרה חיטפת BGP ע"י ספקית סינית לטובת גניבת וציטוט תעבורה מערבית:
https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1050&context=mca

4. רשימת ה-ASes:

http://bgp.potaroo.net/cidr/autnums.html

5. אתר לתשאול מאגרי ניתוב ולמידע חדשותי בנושאי תקיפות BGP:

https://stat.ripe.net