Technologic Papers

פוטנציאל מתקפות ה-DDoS במרחב האינטרנט הישראלי

מאת יורי סלובודיאניוק

מבוא

מה שגרם לי לכתוב את המאמר הבא, היה גל התקפות ה-DDoS הקשה של חודש יולי האחרון, גל זה הפתיע אותנו (לא לטובה) בכמה מובנים, שאותם אציג במאמר זה. מקווה שתראו בפסקאות הבאות לא רק "למידת לקחים", משהו שאנחנו ישראלים חזקים לעשות, אלא גם כקריאה לפעולה למען לצפות להתקפות הבאות ולהתכונן אליהם מראש ולא בדיעבד. להגן מפני מתקפות DDoS זה לא הדבר הכי סקסי, ולמרות כל הרעש התקשורתי - 90% מהן פשוטות בתכן, מרעישות וקלות לזיהוי מיידי ומצליחות תודות לרשלנות / חוסר מיומנות / טעויות אנוש של אנשים אשר מאפשרים לציוד שלהם להשתתף בהתקפות האלה. לא נוכל כמובן לשנות את העולם אבל גם מעט שכן ביכולתנו לעשות ישנה את המצב לטובתנו. חשוב לציין שכל הנאמר מטה הם דעות ומסקנות שלי בלבד ולא משקפים את דעת המעסיק שלי.

ממצאים

ובכן חודש יולי. על קשר בין מלחמה בעזה להסלמה באינטרנט כתבו לא מעט, למשל כאן:
http://www.arbornetworks.com/asert/2014/08/ddos-and-geopolitics-attack-analysis-in-the-context-of-the-israeli-hamas-conflict/

אז אגש ישר לכמה מאפיינים של התקפות בתקופה הזאת:

התקפות על שרתי DNS של ספקי אינטרנט בישראל. ההתקפות היו לא מקריות אלא מכוונות ומושקעות. נוכחתי לראות התקפה על DNS שעברה 60 Gbit/sec. ההתקפות נמשכו זמן ארוך - כל אחת מספר שעות לפחות. כתוצאה מכך הושבתו שני שירותים:

1. הדומיינים שעבורם שרתי DNS המותקפים הם Authoritative (במילים אחרות מחזיקים zonefile של הדומיין) לא היו זמינים כי לא נענו שאילתות של resolving לגבי כל רשומה של הדומיין.

2. לקוחות בארץ שמשתמשים באותם שרתי DNS כ-Recursive DNS Server לא יכלו לקבל Resolving עבור דומיינים שרצו לגשת אליהם אם לא היו כבר ב-DNS cache של תחנות שלהם. ועקב כך לא יכלו לגלוש באינטרנט, לשלוח מיילים וכו'.

האמת די הפתיע אותי שרק עכשיו, כעבור כמה שנים של התקפות נפל לתוקפים האסימון לעשות זאת. הרי למה להתפזר ולתקוף אחד אחד אתרי בנקים\משרדים ממשלתיים\עיתונים , שגם לאורך שנים האלה מגבירים מנגנוני אבטחה שלהם, כאשר אפשרי להתמקד בשרתי DNS של ספקים ובכך (בשאיפה) להשבית את כל האתרים האלה במכה אחת ?

- **אחוז גדול של התקפות שמקורן בישראל**. שוב הוכחה לכך שתוקפים אמנם בפיגור אבל לומדים דברים. בשנים הקודמות רוב ההתקפות היו מגיעות מחו"ל וזה עדיין ככה, אבל בהתאם גם חברות הנתקפות וספקי אינטרנט עושים הרבה בנידון ומצליחים יותר ויותר לחסום התקפות מחו"ל. אז למה לעבוד קשה אם ניתן לעקוף את ההגנות האלה כשתוקפים מתוך ישראל ? וזה מה שקרה.

- **מרבית ההתקפות היו מסוג UDP reflection/ UDP flood**. שזה דווקא לא מפתיע כי משקף מה שקורה בעולם (תראו למשל כאן - http://news.techworld.com/security/3501968/monster-ntp-ddos-attack-was-too-easy-complains-cloudflare-ceo). בפרט DNS/NTP reflection והצפה UDP flood לפורטים אקראיים (לרוב לפורט 80) המגיע מ- botnets.

נוכח הממצאים האלה שאלתי את עצמי שתי שאלות:

- כמה שרתים היום זמינים במרחב כתובות ישראל שאפשר להשתמש בהם בהתקפה ?
- מה ניתן לעשות כדי לצמצם את כמותם ?

נתחיל עם שאלה הראשונה - כמה שרתים היום יכול התוקף לנצל בהתקפת DDOS שלו.

Open DNS resolvers

בכמה מלים מדובר בשרתי DNS שמוכנים לענות לשאילתות DNS מכל כתובת IP בעולם עבור כל דומיין. בגלל ש-DNS לרוב עובד על UDP, פרוטוקול שאין בו שום מנגנון בדיקה האם פקט באמת הגיע מכתובת שמופיעה כמקור או לא, התוקף שולח לשרת שאילתה כאשר מחליף כתובת מקור לזאת של הקורבן. השרת DNS כזה מקבל שאילתה ושולח תשובה לכתובת של הקורבן, עקב כך שהתשובה היא יותר גדולה מהשאילתה מקבלים אפקט הגברה: amplification).

בהתאם לכך לכל פרוטוקול שאדבר עליו כאן יש מקדם הגברה: amplification factor) שאומר לנו בכמה תשובה היא גדולה מהשאילתה. עבור DNS הוא נע בטווח 28-54 לפי https://www.us-cert.gov/ncas/alerts/TA14-017A.

נכון לחודש אוגוסט הצלחתי לאתר **3628** open DNS resolvers במרחב כתובות ישראל. ההערכה היא די שמרנית כי נכללו רק שרתים שענו תשובת אמת ולא סתם שגיאה או תשובה ריקה, רק שרתים שענו בפחות מ-500 ms (שזה השאיר בחוץ רוב הלקוחות עם מודם סלולרי - עד לכניסת LTE הם לא מהווים מטרה מושכת בכל מקרה), הסריקה נעשתה מחו"ל. לעומת זאת לפי סריקה של פרויקט shadowserver.org ישנם 4378 שרתי DNS פתוחים בישראל https://dnsscan.shadowserver.org/stats/.

כדי להבין איך אנחנו נראים בעולם חיברתי טבלה פשטנית המתארת יחס בין כמות שרתי DNS פתוחים לפי shadowserver.org לכמות משתמשי אינטרנט במדינות שונות (לקחתי כאן http://en.wikipedia.org/wiki/List_of_countries_by_number_of_Internet_users). זה לא חישוב מדעי או מתיימר להיות מדויק במשהו אבל מספיק טוב להבין פרופורציות:

מדינה	כמות משתמשי אינטרנט	כמות שרתי DNS פתוחים	יחס כמות שרתי DNS פתוחים (%)
סין	568,192,066	2,692,989	0.47
ארה"ב	254,295,536	670,540	0.26
*דרום קוראה	41,091,681	578,506	1.4
ברזיל	99,357,737	347,972	0.35
רוסיה	75,926,004	297,753	0.39
אירן	20,504,000	84,214	0.41
ישראל (לפי Shadow)	5,568,961	4378	0.078
ישראל (לפי סריקה שלי)	5,568,961	3628	0.06

* לא כדאי לקחת קוריאה כדוגמה כי מתוך ניסיון אישי עם קוראנים יכול להגיד שמצב אבטחת מידע שם פשוט זוועתי.

כמו שרואים מצבנו בעולם לא כל כך רע, אבל... אם ניקח בחשבון מיקום גאוגרפי מיוחד שלנו ושאנחנו מחוברים לאינטרנט העולמי וגם פנים ארצית לא בקיבולות מטורפות כמו קוראנים\אמריקאים אז יותר מ-3000 שרתים זמינים להשתתף בהתקפה זה המון!

חשוב לציין ש-**63%** מהשרתים הפתוחים שייכים לטווחים דינאמיים של ספקי אינטרנט, במילים אחרות מדובר במשתמשים ביתיים\עסקיים קטנים עם חיבור כבלים\ADSL ומה שפתוח זה נתב הפשוט שמחבר אותם לאינטרנט. שאר השרתים הם תוצאה של הגדרות שגויות של ציוד.

Open NTP servers

כאן התקפה מבוססת על אותו עקרון כמו של open DNS resolver רק שמדובר בפרוטוקול לתשאול\סנכרון זמן דרך רשת. NTP מבוסס גם על UDP ועובד על פורט 123. פרוטוקול NTP כולל מגוון פקודות שאילתות ותשובות שאפשר לשלוח ל\לקבל מהשרת NTP.ניתן ברמת הגדרה של שרת לאפשר\לחסום שאילתות\תשובות מסוימות, לכן מקדם הגברה כאן משתנה בהתאם.

המעניינת בין כולן היא פקודה monlist - כששרת מקבל מהלקוח את הפקודה הזאת הוא שולח בתשובה רשימה של 600 כתובות אחרונות שפנו לשרת הזה, הרשימה דינאמית ומתעדכנת כשמגיע לסף של 600 כתובות. לא לכל השרת NTP פונים 600 לקוחות שונים, אבל לכאלה שכן - מקדם הגברה מגיע ל-**556.9** (בפרקטיקה מגיע רק ל-206 אבל זה בהחלט לא משנה)!

זה אומר שאם תוקף שולח מגה של שאלתיות monlist עם spoofed כתובת מקור לזאת של קורבן, הקורבן (תלוי ברוחב פס של שרת NTP) יכול לקבל 556 מגה של תשובות!

כמו שכבר הזכרתי בהתקפה http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack על cloudflare שהגיעה ל-400 גיגה לשנייה השתמשו סה"כ ב-4529 שרתי NTP עם פקודה monlist מאופשרת.

ומה מצבנו בארץ? יותר גרוע משרתי DNS הפתוחים: ישנם **57554 שרתי NTP פתוחים לעולם**! לא בדקתי אותם לגבי כל הפקודות NTP אבל כן בדקתי כמה מהם עונים לפקודה monlist: **190** אם נניח שלכל שרת כזה יש רוחב פס של 100 kbit/sec מקבלים פוטנציאל של התקפה 3.8 Gbit/sec. לא רע בכלל. כמו במקרה של DNS רובם הם נתבים ביתיים שמופעל בהם client/server NTP.

SNMP agents פתוחים לכל העולם עם "community string" public

שימוש בפרוטוקול ניהול הזה ב-DDOS זהה לכתוב למלה - נשלחת שאילתה עם כתובת מקור של קורבן, התשובה מגיעה לקורבן. לעומת פרוטוקולים שדיברנו עד פה snmp מחייב הזדהות של השולח שאילתה עם מחרוזת שנקראת community string. והבעיה לא הייתה קיימת אילו במשך עשרות שנים יצרנים בכל העולם ואחריהם גם מנהלי רשת לא היו מגדירים כברירת מחדל מחרוזת "public".

אבל זה מה שקרה. לפי חוקרי אבטחה בעולם (למשל Rapid7) snmp זה הדבר הבא בהתקפות DDOS. למרות שאני מדבר רק על DDOS אציין שלהשאיר ציוד פתוח לעולם לשאילתות snmp עם "public" אפילו כשזה גישת קריאה בלבד זה מתנה שכל פורץ יכול רק לחלום לקבל. מכיר מקרה שארגון גדול הזמין מבדק חדירה ותודות למחרוזת מאוד פשוטה ב-community הצליחו לשנות הגדרות נתב סיסקו שמוציא חוות הלקוח לאינטרנט ואפילו לחדור לרשת פנימית שלו.

שוב, כמו NTP גם SNMP הוא פרוטוקול עם מגוון שאילתות ותשובות. לכן מקדם ההגברה נע בטווח רחב שגם מאוד תלוי ביישום SNMP בכל ציוד: 5.6-650. ההגברה של 650 נשמע מדהים אבל נצפתה בפועל בציוד מסוים בלבד (http://blog.cloudflare.com/understanding-and-mitigating-ntp-based-ddos-attacks) כאשר בממוצע מקדם ההגברה הוא בסביבות 6.

עכשיו לתוצאות הסריקה (סרקתי רק read-only והשתמשתי ב-"public" בלבד ותשאלתי רק ערך של sysdescr, תוצאות הסריקה מחקתי מיד אחרי סיום): **6441** כתובות IP ענו לשאילתה. לעומת פרוטוקולים אחרים כאן קיבלתי תשובות שהוסיפו קצת מידע על ציוד עצמו ולהלן הטבלה המדגמית:

תשובה שהתקבלה מהציוד	כמות שרתים שענו	
Software Version 3.10L.01	2168	אופייני לנתבי Dlink כמו למשל ישנים DSL-2650
NDS CORE SNMP Agent	1155	לא הצלחתי לוודא אבל שייך לציוד של חברות http://en.wikipedia.org/wiki/Advanced_Digital_Broadcast http://en.wikipedia.org/wiki/Pace_plc שמייצרים רכיבים שונים ל IPTV,Streamers etc
Cisco IOS routers	674	נתבי סיסקו. ראו טבלה הבא שמפרטת סוג הנתבים
HP ETHERNET MULTI-ENVIRONMENT	232	מדפסות רשת למיניהן של HP (/ Officejet 6500 Officejet Pro 8600)
Check Point Embedded	209	חומת אש של Checkpoint, לרוב Edge/UTM-1
(Connect WAN 3G (RS232 serial	99	מודמים סלולריים. יכול להיות אלה: http://www.digi.com/products/wireless-routers-gateways/routing-gateways/digiconnectwanfamily
SofaWare Embedded NG	99	חומת אש של Checkpoint מסוג Sbox שהייה מוצר של חברת Sofaware עד ש- Checkpoint קנו אותם
802.11 n Wireless ADSL 2/2+ Router	70	נתב ביתי שלא בדקתי מהו
Brother xxx	54	מדפסות רשת של Brother , xxx מספר שמזהה דגם

		של רכיב רשת אבל לא את הדגם המדפסת המדויק
TANDBERG	45	ציוד ועידות וידאו נפוץ בחברות בארץ http://en.wikipedia.org/wiki/Tandberg
"Videoconferencing Device"	43	ציוד ועידות וידאו לא ידוע
LinkProof :Branch - 25M / (100M	32	ציוד של radware מאזן עומסים, נפוץ בחברות ברמת ENT
ZyWALL 2 Plus	26	
KYOCERA Printing System	22	מדפסות Kyocera

10 סוגי נתבי סיסקו מתוך 24 שענו ב-snmp

סוג ציוד סיסקו כמו שנראה בתשובה	כמות
1841	154
2900	112
1900	88
880	74
2800	59
870	40
Cisco Internetwork Operating System Software	23
3800	23
2801	20
2951	13

שרתי Chargen

מאוד ייתכן שלא שמעתם עליו - פרוטוקול שנוצר ב-1983 ומזמן אין שום סיבה שיהיה מופעל, אבל בכל זאת. עובד גם על TCP ו-UDP ועובד מאוד פשוט: לא משנה איזה פקטה מגיעה לפורט שלו 19 , chargen יענה לשולח עם פקטה של תוכן אקראי בגודל מ-0 עד 512 בייט. תלוי ביישום בציוד מקדם ההגברה נע בין 200 ל-100. http://en.wikipedia.org/wiki/Character_Generator_Protocol.

השירות הוא לא חלק מ-Windows אבל כן היה חלק מתוכנות של Unix ששימש כבסיס ללינוקס ולמערכות משובצות שונות, כמו למשל נתבים. מתוך כמה כתובות שגיליתי את השירות הזה ויש לי גישת ניהול לציוד כחלק מעבודה שלי בדקתי ומצאתי שכולם היו נתבי סיסקו עם הגדרה שמפעילה את השירות: service udp-small-servers / service tcp-small-servers. כמות שרתי ה-chargen הזמינים בישראל הם 96.

שלא יטעה אתכם המספר הקטן - זה לא עניין של כמות, זה עניין של איכות. לא מדובר בקווים ביתיים אלא בקווי תמסורת עם רוחב פס רציני כשהציוד הפגיע הוא ציוד חזק כמו נתבי סיסקו 29xx\39xx. אסכם בטבלה את זמינות השירותים שיכולים לשמש את התוקפים בהתקפות DDOS:

שירות הפגיע	כמות
Open DNS resolvers	3628
Open NTP servers	57554
Open NTP servers with enabled monlist cmd	190
Open SNMP agents with "public" community	6441
Chargen servers	96

מסקנות

ועכשיו הגענו לשאלה השנייה - מה ניתן לעשות כדי לצמצם את כמותם. המסכנות הן פרי של ניסיון אישי שלי ולא מהוות שום רשות או דרך היחידה להתמודד וגם לא ממצות את הנושא. חילקתי את המסכנות לפי קהל היעד כי לכל אחד ישנם אמצעים שונים.

ספקי אינטרנט

אתחיל מספקי האינטרנט בארץ כי הם הגורם המכריע בניסיון להגן על מרחב האינטרנטי הישראלי.

- תקף לכל ההתקפות שהזכרתי. כל ההתקפות UDP reflection/amplification עובדות בגלל שיש ספקים המאפשרים לבצע החלפת כתובות IP (address spoofing) על ידי לקוחות שלהם. אין לנו שליטה על מה שקורה בחו"ל אבל כן אמורה להיות שליטה לספקים בארץ על מה שקורה בחצר שלהם. אני גם יודע שנעשים מאמצים בכיוון הזה אבל אנחנו רחוקים מיעד הסופי - שאף לקוח של אף ספק בארץ לא יוכל לזייף כתובות מקור שלו.

- Open DNS resolvers. כמו שאמרתי 63% מהשרתים האלה שייכים לטווחים דינאמיים, זאת אומרת למשתמשים ביתיים\עסקיים קטנים. והדבר החשוב להבין כאן הוא שאין להם כלים להתמודד עם הבעיה.

- רוב ה"שרתים" זה לא באמת שרתים אלא נתבים ביתיים , שברגע שאתה מפעיל בו DNS client אוטומטית מופעל גם שרת DNS לכל דבר. כמה יצרנים (סיסקו\Dlink) הוציאו קושחה מעודכנת שמתקנת את החור, אבל לא לכל הדגמים ומשתמש כזה לא יידע להתעסק עם חיפושים\שדרוגים. שלא לדבר על יצרניים יותר זולים שמבחינתם It is not a bug, it is a feature. אז המסכנה היא מאוד פשוטה - הגנה על לקוחות כאלה מפני ניצולם ב-DDOS חייבת להיות אחריות של ספק האינטרנט. כמו שאין היום לא רק בישראל אלא בעולם ספקים שמאפשרים ללקוחות עם כתובת דינאמית לשלוח מיילים פורט 25 חופשי לכל האינטרנט ובכך להפיץ ספאם - הגיע זמן שגם לא תהיה לכתובות דינאמיות אפשרות לשמש כשרת DNS. ממלא לפי הגדרה של Authoritative DNS הוא לא יכול להיות עם כתובת דינאמית. ולשמש כ-recursive DNS עבור תחנות ברשת פנימית מאחורי נתב עדיין אפשרי בלי שיגיעו לנתב שאילתות DNS לפורט 53 שלו. טכנית לבצע זאת קל ופשוט וגם באופן שקוף למשתמש, לא אלמד ספקים איך לעשות זאת כי הם יודעים היטב.

- התקפה על שרתי DNS. לא אכנס לפתרונות טכניים אתם יודעים יותר טוב ממני, אציע רק על שני דברים בסיסים שניתן לעשות כדי להקל על הקוחות:
  - ✓ להפריד בין Authoritative DNS servers ו-Recursive DNS servers עבור לקוחות קצה. כי כששרת dns.netvision.net.il או ns1.bezeqint.net תחת התקפה זה לא חייב להשפיע על resolving רגיל של גולשים.
  - ✓ אם לא באיכות אז בכמות - להגדיל כמות שרתי Authoritative DNS. למשל אם תוקף עושה whois על דומיין bezeqint.net הוא יקבל 3 שרתי DNS לתקוף, עבור netvision.net.il - 2 שרתים ועבור goldenlines.net.il גם 2 שרתים. אם אני שם דומיין ב-DNS של אמזון לעומת זאת למשל, אקבל 4 שרתים ברירת מחדל. לתקוף 4 שרתים יותר קשה משניים.
  - ✓ Open NTP servers. שוב ,ראו למלה. אין שום סיבה סבירה שעל כתובת דינאמית ישב שרת NTP. ושוב רק ספקי אינטרנט יכולים למנוע מלקוח כזה להיות חלק פעיל בהתקפה. לגבי לקוחות עסקיים עם כתובות קבועות - הסברה והתראה עובדים טוב ביותר.
  - ✓ Open SNMP agents with "public" community. לגבי כתובות דינאמיות ראו למלה. לגבי כתובות קבועות שיש להן "בעל הבית" אצל לקוח אז יצירת קשר יזום והסברה עוזרים ברוב המקרים כי אם מדובר בלקוחות עסקיים זה מעורר עניין רב כשמעדכנים אותם על ציוד שלהם פתוח מכל העולם.
  - ✓ Chargen. לרוב מדובר בציוד סיסקו שהוגדר לא נכון. ציוד כזה או בשליטה ישירה של ספק או יש ללקוח מישהו אחראי לו שישמח לסגור את החור אם ספק יעדכן אותו על כך.

מנהלי רשת

- התקפה על שרתי DNS, גם אם מדובר בשרת של ספק וגם שרת שלכם שמחזיק רשומות הדומיין שלכם (zonefile) הפתרון הקל לביצוע זה להגדיל כמות Authoritative name servers עבור הדומיין. אז אם יותקף שרת אחד ויפסיק להיות זמין לקוחות יעברו אחד אחד את כל השרתים שלכם עד שאחד יחזיר תשובה.
- Open DNS resovers. כמו גם לגבי שאר שירותים ברשימה השחורה שלי - זה די פשוט לסרוק מדי חודש את טווחי הכתובות של העסק ב-nmap מבחוץ למשל משרת וירטואלי. סתם לדוגמה ב-Amazon ישנה אפשרות להקים שרת לינוקס בסיסי בחינם לשנה שיכול לעשות זאת בלי להתאמץ (חפשו free tier AWS). אחרי שמצאתם שרתים כאלה ברשת שלכם חיפוש בגוגל לגבי גרסה\יצרן של תוכנה\חומרה ו-"disable monlist" למשל יביא לכם שפע של דוגמאות איך להקשיח את השרת.
- Open NTP servers. אותו דבר - סריקה תקופתית, סגירת שירותי NTP לגישה מבחוץ לפי המלצות באינטרנט.

- Open SNMP agents with "public" community. כאן נדרשת קצת יותר עבודה אבל גם לא קשה. סריקה לגבי community public היא התחלה טובה, אבל אם קיים ציוד ברשת שלכם שמוגדרת בו מחרוזת אחרת אבל גם לא קשה לפיצוח (ראיתי ...readonly, ReadOnly,secret) אז סריקה לא תגלה אותם.

באותו nmap, קיימת גם סריקה של snmp bruteforce שמנסה לפרוץ את המחרוזת אבל גם זה לא קובע. אז הייתי ממליץ פשוט לעבור על הגדרות של כל הציוד (ממלא אתם מגבים אותם למקום מרכזי כלשהו) ולחפש פקודות שקשורות ל-snmp כדי לוודא שמחרוזת היא לא ניתנת לפריצה וגם שיש הגבלת גישה לציוד בפרוטוקול snmp רק מכתובות מאושרות. שוב בגוגל יש את כל הדוגמאות להקשחת snmp. פתרון ארוך טווח זה לעבור לעבוד עם גרסה חדשה שנתמכת ברוב הציוד כבר - snmp v3. הגרסה החדשה מצפינה את כל התעבורת snmp ומחייבת משתמש\סיסמה כחלק מהזדהות.

- Chargen. שוב או סריקה מבחוץ בכלי כמו nmap או לעבור על הגדרות של ציוד. בגלל שרוב השרתים שראיתי הם נתבי סיסקו, מבטלים את החור הזה בשתי פקודות: no service tcp-small-servers ו- no service udp-small-servers

משתמש קצה בבית

- Open DNS resolvers. הפתרון הטוב ביותר זה פשוט להגדיר שרתי DNS ידנית בכרטיס רשת במחשבים בבית ולבטל DNS בתוך הנתב. זה כן יפריע אם אתם מתחברים לספקים שונים לסירוגין. אלטרנטיבה היא לדאוג לשדרג קושחה של הנתב במידה ויצרן מציין שהבעיה טופלה שם.
- Open NTP servers. פשוט תבטלו NTP בתוך נתב שלכם - אין בו שום צורך מעשי. מערכות הפעלה חדשות כבר מגיעות עם הגדרות סנכרון מול שרתים רלוונטים ונתב כאן לא עוזר לאף אחד.

- Open SNMP agents with "public" community. שוב בהגדרות הנתב שלכם תמצאו ותשנו אם לא תבטלו מחרוזת snmp למשהו שלא קל לנחש.

- תבדקו עם ספק שלכם אם מציעים שרותי חומת אש מנוהלים שגם לא מחייבים שינוי ברמת הנתב שלכם.

- כמו שפורסם ב-2013 משרד התקשורת חייב את כל הספקים להציע שרותי סינון אתרים בחינם. לא נכון בכל המקרים ותלוי בספק שלכם אבל לעתים קרובות סינון אתרים הוא חלק מציוד שגם מבצע חומת אש. אם זה ככה אז תוכלו לקבל שרותי חומת אש בחינם על הדרך.

דברי סיום

תודה רבה שקראתם את המאמר, אני מקווה שהסקירה הקצרה שלי תשכנע אתכם לעשות את מה שאתם יכולים על מנת לתרום לביטחון האינטרנטי שלנו. שאלות / הערות אשמח לקבל למייל: yuri@yurisk.info או לצורך דיון בקבוצה:

https://www.facebook.com/home.php?sk=group_115034391898027