



מתקפות DDoS - איך מתכוננים ליום הדין?

מאת יורי סלובודיאניוק

הקדמה

במהלך השנים האחרונות, אנו עדים לכך כי התקפות Distributed Denial of Service (DDoS) תופסות מקום הולך וגדל בקרב התקשורת ובקרב קהילות אבטחת מידע בעולם. מגמה זו מתקיימת משתי סיבות עיקריות: הראשונה הינה ההיקף והכמות של התקפות מסוג זה. השנייה הינה הנזק הכספי או התדמיתי הנגרם לנתקפים. ככל שעובר הזמן הארגונים המבצעים תקיפות אלו מפתחים עוד ועוד דרכים שיטות ודרכים להגדיל את משאביהם וכך מתקפותיהם הופכות לאיכותיות יותר ויותר - נתון המגדיל את היקף הביצוע ואת הנזק הנגרם ממנו. במאמר זה אנסה לתת מידע שיעזור לכם, בתור אנשים פרטיים ובתור ארגון עסקי, להגן על עסק שלכם ולצמצם נזקים.

כל הנכתב במאמר זה, מבוסס על ההתקפות שראיתי במהלך השנה האחרונה נגד לקוחות שלנו. חשוב לי לציין שכל הנאמר מטה הם דעות ומסקנות שלי בלבד ולא משקפים את דעת המעסיק שלי. בנוסף, דברים אלו אינם מהווים שום סוג של מסמך רשמי בנושא.

כאשר באים להתמודד עם מתקפות DDoS, ניתן להתגונן באופן אפליקטיבי (ע"י הוספת קוד במערכת / אתר) ובאופן תשתיתי (ע"י ציוד יעודי, טבלאות ניתוב, ספקיות השירות וכו'), במאמר זה אסקור אך ורק את הפתרונות התשתיתיים, בעתיד אולי אפרסם מאמר מקביל הסוקר את הפתרונות האפליקטיביים.

מבוא - מה זה DDoS ואיך זה נראה

DDoS הינה התקפה **מבוזרת** שמטרתה **השביתה של המשאב הזמין** דרך האינטרנט. "מבוזרת" הכוונה היא שמקורות התקיפה הם לא אחד - אלה רבים, ובדרך כלל מפוזרים בכל העולם. בהסתכלות גסה אפשר לחלק DDoS לשני סוגים:

- **סוג ראשון:** התקפה על רוחב פס אשר מקשר את המשאב (מכאן והלאה במשאב אני כולל כל שירות שלכם הזמין דרך האינטרנט: שרת דואר, אתר אינטרנט, חומת אש, נתב, שעון נוכחות וכו') לאינטרנט (התקפה על שכבה 4 של מודל OSI). במתקפה זו, מטרתו של התוקף הינה להעמיס על הקו בתעבורת "זבל", ובכך לנצל את כל הרוחב עד שלא יישאר רוחב פנוי להעביר את תעבורת עבודה

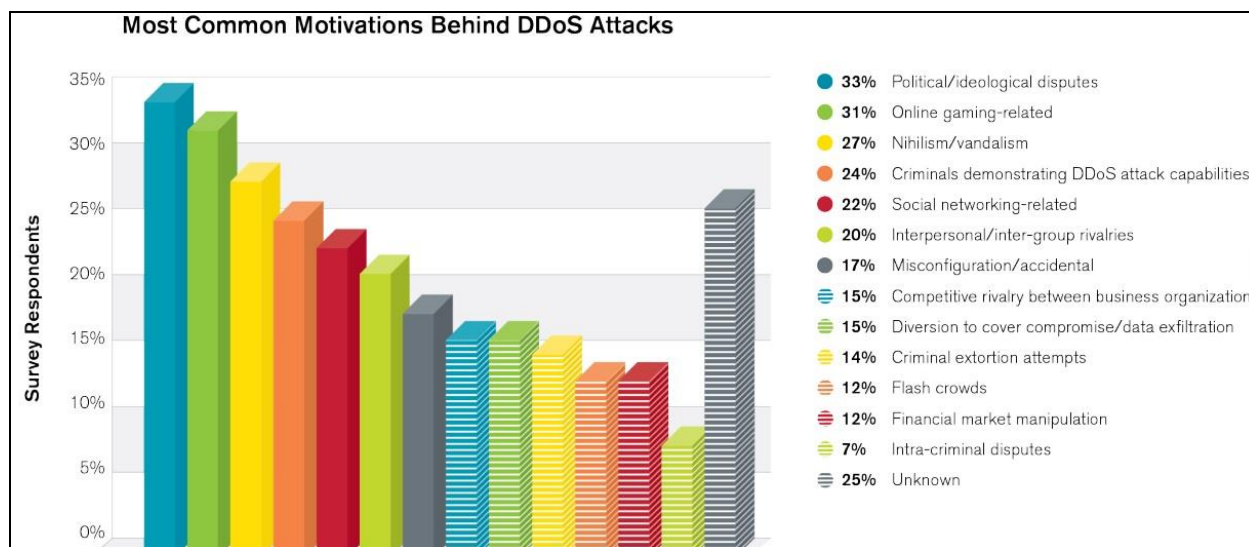
שלכם. אופייני להתקפות האלה שימוש בפרוטוקולים שמאפשרים תעבורה חד כיוונית ללא צורך בהקמת קישור מלא (למשל UDP / ICMP / IGMP / TCP SYN Flood). דבר שני שקל לעשות בהתקפה כזו IP address spoofing - זיוף או הסתרה של כתובת IP של התוקף, שמונע מהמותקף לחסום את התוקפים האמיתיים לפי כתובות IP.

- סוג שני:** התקפה של משאב יעד בעצמו שמנסים למצות את ההגבלות שלו (התקפה על שכבה 7 של מודל OSI). למשל, ביצוע SSL Renegotiation אל מול שרת שתומך ב-SSL, התוכנה התוקפת מתחברת לשרת, ואחרי שקישור הוקם מבקשת לבצע תהליך SSL Negotiation מחדש בלולאה, מדובר בתהליך הדורש לא מאט CPU, ביצוע Renegotiation בלולאה, מעמיס על ה-CPU של שרת ומנסה למצותו עד תום. **התקפות אלה בדך כלל מתוחכמות יותר ולא בהכרח דורשות רוחב פס גדול.** אמנם כאן לא ניתן להסתתר מאחורי IP Address Spoofing.

- למען האמת אפשר להוסיף סוג נוסף של DoS - פריצה למשאב ממש, השתלטות עליו - ואז השבתה שלו. למשל עקב שגיאת קונפיגורציה של נתב, תוקף מצליח לקבל גישה ניהול אליו ופשוט מכבה אותו. אך מניסיון שלי, ההתקפות כאלה לא טיפוסיות לצורכי DoS אז לא אדבר עליהן במאמר זה.

אז איך נראית התקפה בפועל?

קודם כל, סוג של התקפה בהרבה תלוי במניעים של התוקף. למטה סקירה של חברת Arbor Networks על מניעים של התקפות בשנת 2012:



[במקור: http://www.nanog.org/meetings/nanog57/presentations/Tuesday/tues.general.sockrider.2012_infra_sec_report.1.pdf]

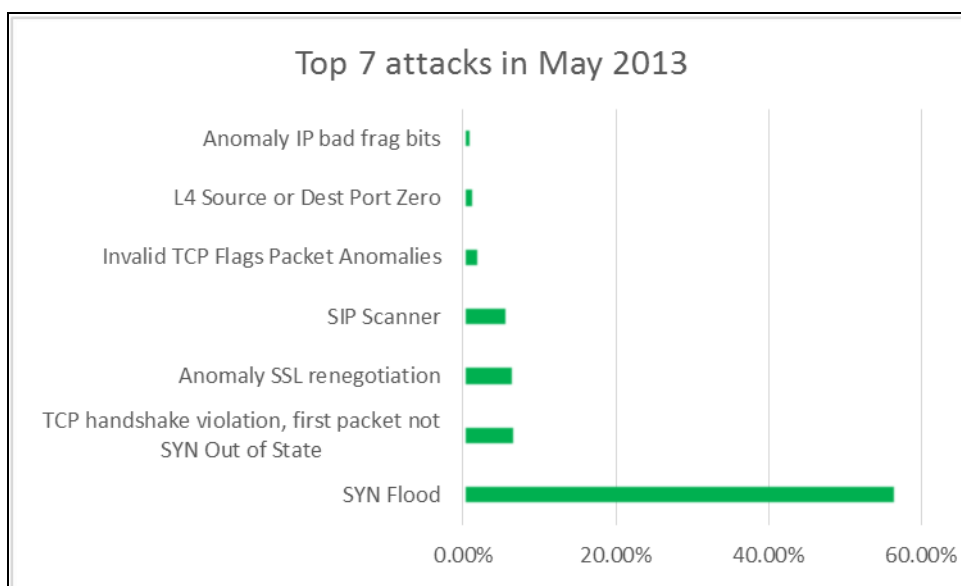
מתקפות - DDoS איך מתכננים ליום הדין?

www.DigitalWhisper.co.il

הפילוג לדעתי גם תקף לישראל, עם אחוז גבוהה יותר של תקיפות, אך מטעמים פוליטיים (קרי: שנאת ישראל / אנטי ציונות / אנטישמיות וכו').

תקיפות כאלה (כגון #OpIsrael - של 7 באפריל השנה), מתבצעות לרוב ע"י משתמשים ביתיים שקראו עליה ברשתות כגון Facebook / Twitter, אותם משתמשים מורידים כלים מוכנים כגון HOIC ו-LOIC ומטרת שלהם הם אתרי אינטרנט של ממשלת ישראל המתוחזקים ומוגנים ע"י "תהילה".

במקרה של שימוש בכלים כגון HOIC ו-LOIC, מדובר במתקפות מסוג: SYN|UDP Flood בפורט 80 וב-ICMP flood. מתקפות למטרות סחיטה או רווח בדרך אחרת כלשהי דווקא יותר משוכללות ומעניינות. כאן מבחר הכלים הרבה יותר מגוון וכולל בנוסף ניצול פריצות די חדשות (CVE-2012/2013). על מנת לתת לכם מבט מ-10000 feet view, קורה בארצנו, צירפתי למטה סיכום של התקפות שבוצעו בחודש מאי:



כמו שניתן לראות, SYN Flood הלא מתוחכמת היא המובילה. הרשימה הזאת, כמו כל רשימת ה-"top" לא משקפת את התמונה מלאה, למשל, למטה מצורף מדגם ההתקפות שבוצעו בזמן הנתון מספר ימים ספור לפני כתיבת שורות אלו:

Dst Port	Protocol	Description
0	0	IP Anomalies Invalid IP Header or Total Length
0	0	IP Anomalies Unsupported L4 Protocol
0	0	TCP Anomalies Invalid TCP Flags
0	0	TCP Anomalies L4 Source or Dest Port Zero

מתקפות - DDoS איך מתכננים ליום הדין?

www.DigitalWhisper.co.il



0	0	TCP Anomalies TTL Less Than or Equal to 1
0	ICMP	Intrusions ICMP-Frag-Needed-Storm
22	multiple	TCP DoS
23	multiple	TCP DoS
25	TCP	Intrusions Anomaly IP bad frag bits
25	TCP	Intrusions Possible-Worm
53	UDP	UDP DOS UDP Flood
80	Multiple	Multiple TCP SYN Flood
80	TCP	Intrusions Apache HTTPD mod_log_config Cookie
80	TCP	Intrusions IIS-ASN1-Overflow
80	TCP	Intrusions Web-etc/passwd Dir Traversal
443	TCP	TCP Intrusions Anomaly SSL renegotiation
443	Multiple	TCP Intrusions Anomaly TLS renegotiation
443	TCP	Intrusions Anomaly IP bad frag bits
1433	TCP	DoS General UDP
2400	Multiple	Multiple UDP Anomalies Source Address same as Dest Address (Land Attack)
2425	multiple	UDP DoS
2627	Multiple	Multiple UDP Anomalies Source Address same as Dest Address (Land Attack)
3389	multiple	TCP DoS SYN Flood
3566	multiple	Multiple TCP Anomalies Source Address same as Dest Address (Land Attack)
5060	multiple	UDP DoS
5060	UDP	Intrusions SIP-Scanner
6507	UDP	UDP DoS
6511	UDP	UDP DoS

מתקפות - DDoS איך מתכננים ליום הדין?

www.DigitalWhisper.co.il

6667	multiple	TCP DoS
6668	multiple	TCP DoS
6675	multiple	TCP DoS
8080	multiple	TCP DoS
10527	UDP	Intrusions Anomaly IP bad frag bits
14598	UDP	Intrusions Anomaly IP bad frag bits
24644	UDP	Intrusions Anomaly IP bad frag bits
26269	UDP	Intrusions Anomaly IP bad frag bits
28063	UDP	Intrusions Anomaly IP bad frag bits
31188	UDP	Intrusions Anomaly IP bad frag bits
32948	UDP	Intrusions Anomaly IP bad frag bits
33463	UDP	Intrusions Anomaly IP bad frag bits
33717	UDP	Intrusions Anomaly IP bad frag bits
56278	UDP	Intrusions Anomaly IP bad frag bits
57853	UDP	Intrusions Anomaly IP bad frag bits
58314	Multiple	Multiple UDP Anomalies Source Address same as Dest Address (Land Attack)
58410	UDP	Intrusions Anomaly IP bad frag bits

לגבי רוחב פס הנצרך בהתקפות בסגנון #OpsIsrael צפיתי ב-4-5 Gb/sec נגד כתובת בודדת (שוב של אתר ממשלתי), אך בתקיפות למטרות רוח, רוחב הפס יכול להגיע גם ליותר מגיגה.

בתקיפות שוטפות בדרך כלל, מדברים על עשרות או מאות מגה בית מקצה לקצה, רוחב זה בדרך כלל מספיק על מנת להשבית עסק ישראלי ממוצע עם קו לאינטרנט של 10 עד 20 מגה. משך ההתקפה נע בין כמה עשרות דקות לכמה ימים, תלוי במוטיבציה של התוקפים (כאשר מדובר במתקפה למטרות רוח - אורכה בדרך כלל ממושך יותר).

מתקפות - DDos איך מתכננים ליום הדין?

www.DigitalWhisper.co.il

איך מתגוננים מהתקפות DDoS?

אחרי שראינו קצת נתונים, והבנו קצת יותר את התמונה כולה - אפשר לגשת לחלק החשוב באמת שלמטרתו נכתב המאמר - מה בעל עסק / מנהל רשת יכולים לעשות בנוגע למתקפות אלו?

אולי זה יפתיע אתכם, אך האמת? די הרבה, אך לפני שאכנס לאפשרויות ולפרטים אגיד את הפרט הכי חשוב: **כאשר מדובר בתקפת מסוג DDoS, לרוב לא ניתן להתמודד לבד! ועכשיו - ניגש לעניין:**

השאיפה שלכם חייבת להיות: לא לתת להתקפה להגיע אליכם בכלל. לא משנה איזה מכשיר IPS תשימו במשרד או בחוות השרתים שלכם, אם ההצפה תגיע דרך החיבור לאינטרנט שלכם זה אומר שתישארו עם רוחב פס של 0 לתעבורה עסקית שלכם. ולא יעזור גם להגדיל אותו, כיום, עלות שכירות רשת בוטים (botnet) של כ-10,000-20,000 בוטים הינה 50-250 דולר לשעה בשוק השחור. אין רוחב פס ללקוח קצה שאי אפשר למצות.

אתם חייבים שיתוף פעולה של מי שמספק קישוריות אינטרנט למשאבים שלכם (נכון, אני עובד בספקית אינטרנט, אבל אני מבטיח לכם שאני אובייקטיבי לחלוטין). ולהלן הפתרונות:

- **הגנה מבוססת ספקית:** היום, כל הספקיות בארץ מציעות (בתשלום) שירותי הגנה נגד DDoS, שזה אומר שיש להם ציוד הגנה נגד DDoS שמנתבים דרכו את כל התעבורה המגיעה ללקוח (אליכם) דרך הספקית, ואז בזמן התקפה הציוד אמור לחסום את תעבורת התקפה בתשתית הספקית ולמנוע ממנה להגיע אליכם.

יתרונות:

- ✓ נגד התקפות על רוחב פס אין לכם ממש אלטרנטיבה - חייבים לעצור את ההתקפה לפני שהיא מגיעה אליכם.
- ✓ אתם לא צריכים לדעת כמעט כלום על DDoS, אנשי אבטחת המידע של הספקית עושים הכל.
- ✓ ההתקפה / ההתקפות לא מעסיקה אתכם שעות מרובות (במקרה שהיא נעצרת בהצלחה כמובן).

חסרונות:

- ✓ השירות הוא לטובת כלל הלקוחות המשתמשים בו, וכנובע מכך יכול להיות שלא יתואם במדויק לשירותים שאתם מספקים (לספקית אין ידע על השרת / תוכנה / משאב שלכם, ובכל מקרה ההחלטות של הספקית יהיו לטובת כל הלקוחות ביחד). כך שאם תרצו להפעיל חתימה נגד הפריצה האחרונה קשורה לשרת שלכם פרטנית - הספקית לא בהכרח תעשה זאת (ראו בסיכום לגבי מה לשאול את הספק שירות).



- **התקנת ציוד יעודי בעסק:** - התקנת ציוד אבטחה כנגד מתקפות DoS או DDoS יקנה לכם שליטה ויהווה יתרון משמעותי לאורך זמן.

יתרונות:

- ✓ הכל בשליטה שלכם. תוכלו להפעיל את החתימות וההגנות הכי חדשות ומתקדמות, כולל חתימות שאתם כתבתם ושתואמות בדיוק לשרתים ולתוכנות שלכם.
- ✓ תקבלו תובנה נוספת ממערכת לוגים שנוגעים לגביכם בלבד. נתונים אלו יוכלו לעזור בעת פנייה לספק עם שאלות ספציפיות (לדוגמא, ניתוח לוגים של מתקפה מסוימת יוכלו להסביר בקלות כיצד על הספק לפעול על מנת לחסום אותה בעתיד, או כיצד לשדרג את מערך ההגנה שלו).
- ✓ תכשירו אנשי IT שלכם לטווח ארוך - שום שירות מצד שלישי לא יכול להתחרות בידע של עובדים שלכם במערכות שלכם, הם מכירים את רשת הארגון, הדרישות והפוליטיקות הפנימיות והם צוברים ידע בעת התמודדות עם כל מתקפה ומתקפה.

חסרונות:

- ✓ עולה כסף נוסף.
- ✓ מחייב כח אדם מיומן לתפעל את הציוד.
- ✓ נקודת כשל נוספת ברשת. כמו כל ציוד (ובייחוד כזה העומד ב-Gateway) יכולים לקרות תקלות, טעויות אנוש וכו'.

- **Black Hole Routing:** לכלל הספקיות בארץ יש יכולת לבצע פעולה הנקראת "Black Hole Routing" ובדרך כלל היא מסופקת חינם (או לפחות כך אמור להיות...). עיקרון מאוד פשוט: הכתובת המותקפת (כתובתו של הלקוח) מנותבת לאיזור המכונה בשפת סיסקו: "Null0", או במילים פשוטות יותר: מושלכת לפח. הספקית מבצעת זאת רק מעבר לגבולות האינטרנטיות שלה (border routers), מה שאומר שמחוץ לתשתית של הספקית לא יהיה ניתן לגשת לכתובת הזאת, אך (תלוי בספקית) הכתובת עדיין זמינה בתוך הטווח של הספקית - ובדרך כלל, גם בכל הספקיות בארץ. פעולה זאת אומרת שלא יהיה ניתן להגיע לאתרכם מכתובות IP הממוקמות בחו"ל (ומשם הגיעו רוב ההתקפות שחווינו בזמן האחרון). בכך, כל התעבורה של התוקף מגיעה לגבול של הספקית ונזרקת שם.

יתרונות:

- ✓ לא עולה כסף.
- ✓ יעיל ביותר - ספקית יכולה להשתמש באפשרות הזו כדרך אחרונה לעצור התקפה מסיבית במיוחד.
- ✓ לא צריך שום ציוד, שום ידע מתקדם - רק שיחת טלפון לספקית האינטרנט.

חסרונות:

- ✓ במובן מסוים התוקף משיג מה שרצה - המשאב של הנתקף אנו זמין ללקוחות מחו"ל.
- ✓ לא מאפשרת לחסום תעבורה לפורטים מסוימים: או שהכל פתוח עבור אותה כתובת IP או שהכל חסום עבורה.

על מנת להשלים את התמונה, אגיד שיש שירותי Anti-DDoS מנוהלים (קרי בצד שלישי) שלא מבוססים על ספקיות האינטרנט, אלא מבוססים על טכנולוגיות ענן. הם עובדים על עקרונות זהים כמו אלו של ספקית האינטרנט (מנתבים את התעבורה של הלקוח דרכם). אך נכון לכתיבת שורות אלו, מצאתי שקיימים שירותים כאלה רק בחו"ל (אשמח אם מישהו יעיר את עיניי). כיום אין שירות ענן הממוקם בישראל, כך שבמידה ויהיה פתרון Anti-DDoS מבוסס ענן בסגנון ספקיות האינטרנט, זה אומר שיהיה צורך לנתב תעבורה מהארץ אל הענן בחו"ל (דרך פרסומי BGP או דרך סוג של GRE tunneling), מה שיוסיף חתיכת Latency (אם זיהיה אפשרי בכלל). חברות שמספקות שירותים כאלה הן: [AT&T](#), [Prolexic](#), [Verisign](#)-I.

אחסון בענן

אחת האפשרויות המתבקשות כיום היא לאחסן את האתר שלכם בענן (או לפחות להכין אחסון בענן מראש ולהעביר לשם את האתר בזמן מתקפה). אפשר ללכת על ספקיות ענן "מהשורה הראשונה" כגון: Amazon, Google, Microsoft, Softlayer, Rackspace וכו'. יש כבר "חברות מטווחות" שמוכנות להעביר את האתר שלכם לענן בעצמן ולהפעיל אותו משם. או שאפשר לפנות לספק ענן לא משורה ראשונה, כמה מהן מציעות שירותי הגנה נגד DDoS כיעוד שלהם (דוגמה Cloudflare, וחיפוש בגוגל אחר המילים: "website ddos cloud protection" יניב לא מעט תוצאות). מן הסתם מעבר לענן מחייב גם היערכות מצד מערכת ספק שירות ה-DNS שמחזיקה zone file של אתר שלכם.

יתרונות:

- ✓ יכולות של ספקי ענן גבוהות בהרבה מאשר כל לקוח קצה.
- ✓ לרוב לא מחייב שינוי בקוד של אתר האינטרנט.
- ✓ בדרך כלל, עד לגבול מסוים מקבלים הגנה נגד DDoS כערך מוסף, מבלי לשלם עליו בנפרד.



חסרונות:

- ✓ שירותי ענן הם לא בדיוק שירותים המיועדים להגנה כנגד DDoS, אם התקפה מסוימת תגיע לרמה שתשפיע על לקוחות אחרים - צפו לצעדים מצד של הספק (בסבירות גבוהה לא תגיעו לזה, אך אם נקח לדוגמא את ההתקפה שבוצעה על wikileaks, נראה שהיא אילצה את אמזון לסגור את אחסון האתר...). והנ"ל גם רלוונטי לשירותי ענן כמו cloudflare.
- ✓ המידע מאוחסן על שרתים שאין לכם שליטה עליהם. למשל מוסדות פיננסיים לא יכולים להרשאות דבר כזה מפני תקנים כגון PCI וכו'.
- ✓ עלות נוספת.
- ✓ אחסון במקומות כגון ב-Google Apps מחייב לכתוב קוד נוסף שירוך שם, ובעת מעבר לאחסון חדש - יוסיף עבודה של עיבוד הקוד מחדש.

לסיכום

- כאן אני אסיים את הסקירה על הפתרונות הקיימים כנגד DDoS, ולטובת סיכום, אציג רשימת צעדים שחשוב לבצע על מנת להתכונן להתקפה כזו:
- תשאלו את עצמכם את השאלות הבאות:
 - ✓ האם משתלם לי להגן על עסק שלי מתקיפת DDoS? כן, בעולם שוק חופשי זה מתחיל ונגמר בכסף. מה יהיה נזק כספי אם נהיה מנותקים מהאינטרנט / אתר יהיה למטה במשך שעה? חמש שעות? כמה ימים?
 - ✓ מהו התקציב שלי להגנה? ככה תדעו מה תוכלו להרשות לעצמכם.
 - ✓ מהם הנכסים ששווה להגן עליהם?
 - ✓ מי יכול לתת לי שירות שימנע מהתקפה להגיע למשאב שאני רוצה שיהיה זמין?
 - ✓ מה SLA (Service-Level Agreement) של השירות?
 - ✓ מהו גודל ההתקפה שספק השירות מתחייב לעצור?
 - ✓ מהו גודל ההתקפה שספק ייאלץ לנתק אותי משירות (אין ספק שירות שיעמוד בהתקפה לא מוגבלת, מתקפה של 150 Gb/sec יכולה להשבית אולי את כל האינטרנט של ישראל)?
 - ✓ אילו הגנות שספק יכול להפעיל? רק ברמת כתובות IP ופורטים, או שגם נגד פריצות ברמת האפליגציה?
 - ✓ מיהו איש קשר שלי בספק השירות לזמן התקפה ומה הזמנות שלו?
 - אל תאמינו לשום הבטחה של ספק שירות עד שמוצאים דרך לאשר אותה מעשית. לספק השירות שלכם יכולה להיות מערכת ההגנה המתקדמת בעולם, אך מי שקינפג אותה עשה חצי עבודה. תתאמו עם ספק שירות זמן ותבצעו דימוי DDoS יזום על מנת לבדוק הכל.

מתקפות - DDoS איך מתכוננים ליום הדין?

www.DigitalWhisper.co.il



- תארגנו לכם איך להתחבר לשרתים / משרד לא דרך קו האינטרנט שלכם, שכן, בזמן התקיפה סביר להניח שהוא לא יהיה זמין (ראיתי מקרים שלקח ללקוח כמה שעות להבין שהוא תחת התקפה, מפני שהוא לא הצליח להתחבר מהבית ורק כשהוא הגיע עבודה הוא הבין זאת).
 - תבדקו שיש לכם גישה לכל הציוד שלכם, גם כזה שמנוהל ע"י צד שלישי. גם כשהציוד מנוהל ע"י חברה אחרת.
 - תנטרו את נכסי ה-IT שלכם. לעיתים קרובות קל להתבלבל בין התקפה לבין עומס יתר לגיטימי. אתם חייבים לדעת מהו מצב רגיל ותקין על מנת להבין שמתחילה התקפה.
 - והכי חשוב: כל החלטה שתקבלו - תתרגלו אותה. כל החלטה, בין אם זה להתקשר לספק אינטרנט ולבקש לחסום כתובת שלכם ב-Null0 (למי מתקשרים? כמה זמן יקח לבצע? מי מאושר לבקש?) ובין אם זה להעביר את האתר לענן (מי מפעיל אותו שם? עם מי מדברים אם לא עובד כמו שצריך בענן? מי דואג לשנות רישומים ב-DNS?).
 - בצעו הדמיות DDoS תקופתיות על ידי חברות המספקות שירות כזה, על מנת לתרגל את צוות ה-IT ולהעמיד למבחן את מערך ההגנה שלכם.
- תודה על תשומת לבכם, מקווה שעזרתי לכם להבין כיצד ניתן להתגונן, והעיקר - אולי גרמתי לכם לרצות לעשות יותר.

על המחבר

יורי עובד 7 שנים בחברת נטויזין (כיום חלק מסלקום), מתמחה בטכנולוגיות וציוד אבטחת רשתות. בנוסף, יורי כותב בבלוג: [yurisk.info](http://www.yurisk.info). בזמנו החופשי אוהב ללמוד שפות ולתרגם לפרויקטים שונים: <http://www.ted.com>, <http://www.ossec.net>.

אשמח לקבל תגובות, הערות וכל משוב על המאמר לכתובת המייל: yuri@yurisk.info או כתגובות ב-Digital Whisper.