

מנגנוני אימות דוא"ל

מאת עוז אבנשטיין

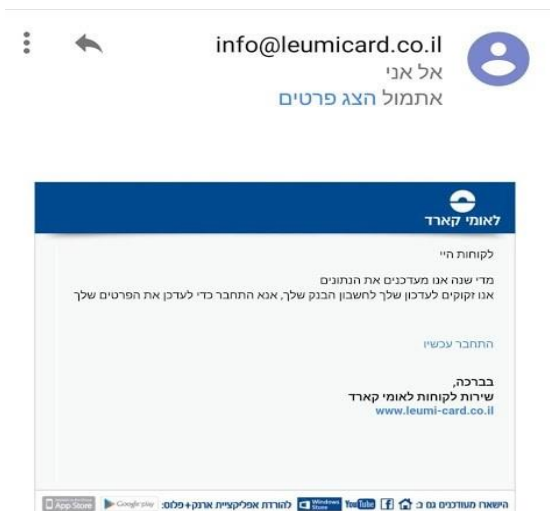
הקדמה

מערכת הדואר האלקטרוני של ימינו מבוססת על פרוטוקול האימייל SMTP (Simple Mail Transfer Protocol) שאופיין לראשונה בשנת 1982 ללא שום מנגנוני אבטחה לאימות זהות השולח.

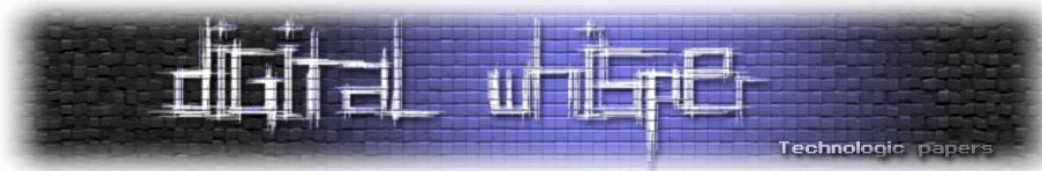
כתוצאה מזאת, תוקפים יכולים בקלות לערוך הודעת אימייל אותה הם מתכוונים לשלוח, כך שתתחזה לכזו אשר נשלחה מכתובת אימייל שרירותית לבחירתם על ידי שינוי שדה ה-"From". טכניקה זו ידועה כ-Email Spoofing והיא מיושמת בהצלחה על ידי תוקפים וספאמרים (Spammers) כבר שנים רבות מפאת החוסר במנגנוני אימות (Authentication) ראוי. בנוסף, מכיוון שטכניקה זו פשוטה ברמת המורכבות הטכנית ליישום אך עדיין אפקטיבית, השימוש בה לאורך השנים למטרות זדוניות נרחב מאוד.

כבר בתחילת שנות ה-2000 תופעת ה-Spam הייתה נפוצה מאוד, אך גם כיום מהווה חלק גדול מתעבורת האימייל העולמית (בין 50%-65%). ברוב המקרים האלו, Email Spoofing משמש על ידי הספאמרים בנסיונותיהם ליצור אמינות. כמו כן, בדומה לשימוש במקרי ה-Spam, Email Spoofing הוא חלק אינטגרלי ברוב נסיונות ה-Phishing וההונאה על ידי אימייל, בהם התוקף מתחזה ליישום אמינה בכדי להטל בקורבן.

בשנות ה-2000 המוקדמות נראו נסיונות ה-Phishing הראשונים כנגד Bank of America, ובשנת 2004 מעריכים כי 1.2 מיליון משתמשים אזרחי ארה"ב נפגעו מתקיפות Phishing שהביאו לאובדן של כמעט 930



מיליון דולר. כמה שנים לאחר מכן, ב-2011 נפגעה חברת Target מקמפיין Phishing שהביא לגניבת פרטיהם של 110 מיליון לקוחות, כולל מספרי כרטיס אשראי. בשנת 2016, פשיג (Phishing) בעזרת אימייל שומש ביותר ממחצית מפריצות אבטחת המידע שדווחו. ואפילו כיום, בשנת 2018 בזמן שמילים אלו נכתבות אנו זוכים לראות עוד נסיונות Phishing, כמו התמונה בעמוד זה.



על מנת להתמודד עם בעיית ה-Email Spoofing ששוכנת בליבו של פרוטוקול SMTP ומנוצלת באופן ישיר בדואר Spam ונסיגות Phishing ו-Social Engineering מגוונים, אופיינו מנגנונים שונים בחלוף השנים שתוכננו במטרה לספק לתשתית הדואר האלקטרוני את יכולות האימות הכל כך חשובות לתפקודה התקין והאמין. במאמר זה נסקור את המנגנונים SPF, DKIM, ו-DMARC.

חשיבותה של מערכת ה-DNS:

לפני שנתחיל בסקירת מנגנוני האבטחה האופיינו לטובת מניעת נסיגות Email Spoofing, יש להדגיש את חשיבותה הרבה של מערכת ה-DNS בכל אחד ממנגנונים אלו. בלב ליבם של כל אחד מהמנגנונים בהם נדון (SPF / DKIM / DMARC) שוכן הקונספט שאך ורק בעל דומיין כלשהו שולט ברשומות ה-DNS שלו, ואם רשומה כלשהי קיימת ב-DNS, הרי שרשומה זו הנה אותנטית ונכתבה ב-DNS על ידי יישות בעלת גישה והרשאות לבצע זאת.

SPF

SPF (Sender Policy Framework) הינו אחד המנגנונים הראשונים שאופיינו לטובת זיהוי ומניעה של נסיגות Email Spoofing.

הרעיון הראשוני למנגנון הגיע בשנות ה-2000 המוקדמות ועורר עניין רב על ידי IETF (Internet Engineering Task Force) בנושא. IETF בחרו לקחת את המושכות והקימו קבוצת מחקר בשם ASRG (Anti-Spam Research Group) לטובת אפיון ויצירה של פתרון לבעיית ה-Spam Email, שבליבה נמצאת בעיית ה-Email Spoofing. אחד מחברי רשימת התפוצה של קבוצת המחקר חיבר שני מפרטים שהוצעו (DMP ו-RMX) לאחד יחיד וקרא לו SPF - Sender Permitted Framework. בהמשך השם שונה ל-Sender Policy Framework.

המנגנון עובד בצורה המאפשרת לשרתים המקבלים (Recipient Servers) הודעת אימייל לבדוק ולאמת את אותנטיות מקור ההודעה על ידי בחינת כתובת ה-IP של השרת השולח (Sender Server). פונקציונליות זו מתאפשרת בעזרת שימוש בתשתית ה-DNS. בעל אימייל דומיין כלשהו, יפרסם TXT Record המכילה את רשימת כתובות השרתים המורשים לשלוח הודעות אימייל בשם דומיין זה. בנוסף, באותו ה-TXT Record מפורסמת מדיניות האומרת לשרת המקבל איך הוא אמור לטפל בהודעות אימייל המתקבלות לאחר בדיקת SPF אותה הוא מבצע. הדבר נעשה בשילוב של 2 סוגי דגלים שונים המחוברים יחדיו לביטוי יחיד.

סוג ראשון של דגלים הוא כתובות "שרת שולח" המורשות לשליחת הודעות אימייל בשם הדומיין, ובעצם משמש להשוואה שנעשית על ידי השרת המקבל בין כתובת שרת השולח והכתובות המורשות שפורסמו על ידי בעל הדומיין. הסוג השני מאופיין כ-Qualifier אשר מתווה לשרת המקבל איך ינהג בהודעת



האימייל שהתקבלה לאחר בדיקת הדגלים מהסוג הראשון (כתובות IP מורשות) והשוואתם כנגד כתובת השרת השולח.

ננתח את רשומת ה-SPF של הדומיין "DigitalWhisper.co.il" (יש לשים לב כי תחביר הרשומה מהווה חשיבות בבדיקת ה-SPF. הבדיקה תעשה משמאל לימין, כל זוג דגלים אשר מהווים ביטוי יחיד בתורם):

```
oz@oz-pt:~$ dig digitalwhisper.co.il txt

;<>> DiG 9.10.3-P4-Ubuntu <>> digitalwhisper.co.il txt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26151
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0005 , udp: 4000
;; QUESTION SECTION:
;digitalwhisper.co.il.      IN      TXT

;; ANSWER SECTION:
digitalwhisper.co.il.      5       IN      TXT      "v=spf1 +a +mx +ip4:5.100.248.67 ~all"
```

- **spf1** - מידע על גרסת ה-SPF. דגל זה הוא קבוע בערכו וחייב להכלל ברשומה.
- **+a** - בביטוי זה קיימת האות "a" שהנה דגל מהסוג הראשון. דגל זה אומר לשרת המקבל לבדוק האם יש לדומיין השולח רשומת DNS מסוג A. לדגל זה מתווסף דגל מהסוג השני והוא "+", האומר לשרת המקבל להעביר את את הבדיקה בהצלחה ולהעביר את הודעת האימייל לתיבה המיועדת במידה וכתובת ה-IP של השרת השולח זהה לכתובת הקיימת ברשומת A של הדומיין השולח.
- **+mx** - בביטוי השני קיים הדגל "mx" שהינו דגל מהסוג הראשון, האומר לשרת המקבל לבדוק האם יש לדומיין השולח רשומת DNS מסוג MX. לדגל זה מתווסף דגל מהסוג השני והוא "+", המתפקד בדומה לנכתב לעיל - השרת המקבל יעביר את הבדיקה בהצלחה במידה ולדומיין יש רשומת DNS מסוג MX, וכתובת ה-IP של רשומה זו זהה לכתובת ממנה שלח השרת השולח.
- **+ip4:5.100.248.67** - ביטוי שלישי מכיל דגל נוסף מהסוג הראשון והוא "ip4", האומר לשרת המקבל לבדוק האם כתובת השרת השולח היא אחת מהכתובות המצוינות (אפשרי לציין טווחים). במקרה שלנו, מצוינת רק כתובת אחת (5.100.248.67), ובדומה למקודם גם כאן דגל ה-"+" מצורף אשר מתווה לשרת המקבל להעביר את הודעת האימייל לתיבה המיועדת במידה וכתובת ה-IP של השרת השולח זהה לכתובת 5.100.248.67.
- **~all** - הביטוי האחרון הקיים ברשומת ה-SPF אותה אנחנו בוחנים מכיל דגל מהסוג הראשון והוא "all". כפי שמרומז בשם, "all" אומר לשרת המקבל איך להתייחס לכתובת IP של השרת השולח, במידה וכתובת זו אינה הותאמה באף אחת מהבדיקות הקודמות. הדגל השני המצורף לביטוי זה הוא "~" המורה על Softfail. שילוב של שני דגלים אלו לביטוי "~all" מתווה לשרת המקבל להעביר לתיבה המיועדת הודעות אימייל שהגיעו משרת שולח כלשהו בעל כתובת IP שלא נכללת ברשומת ה-SPF,

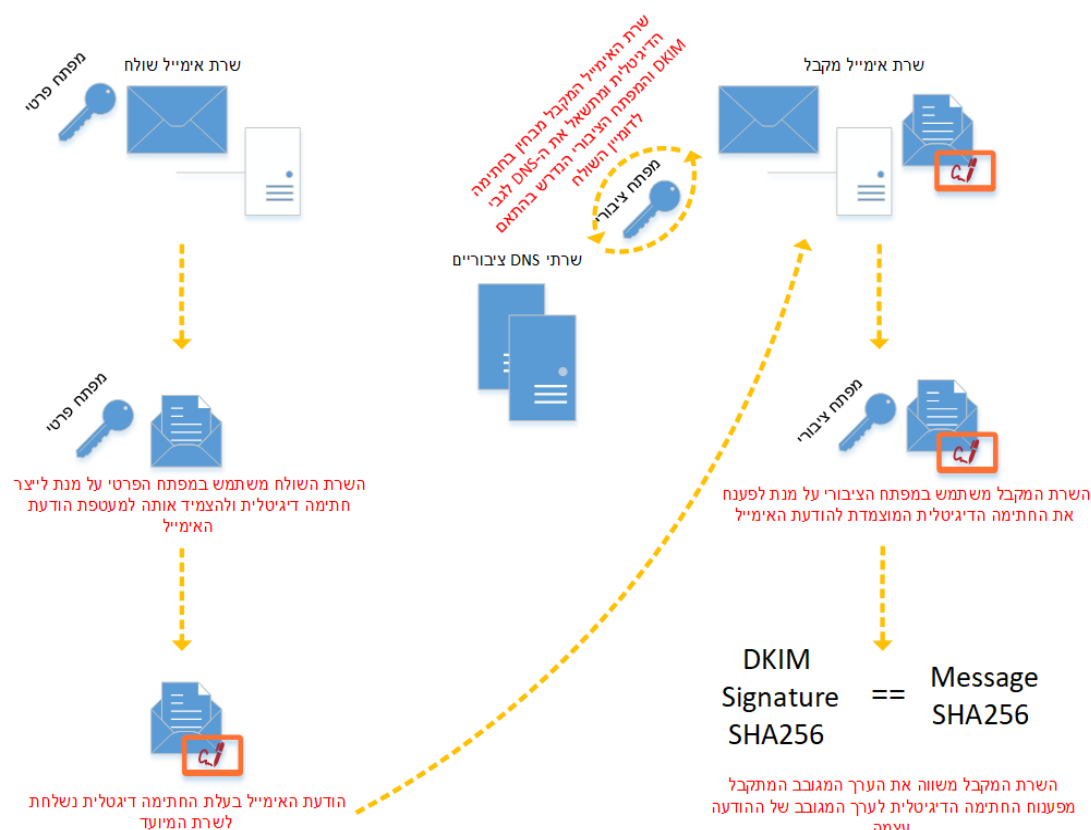
אך לתייג'לסמן אותה (רוב ספקי האימייל יעבירו הודעה התיוגה בצורה זו ל-Inbox עם אזהרה והשאר יעבירו לספאם).

DKIM

DKIM (DomainKeys Identified Mail) הוא פרוטוקול שאופיין בשנת 2004 על ידי IETF בכדי להתמודד גם הוא עם בעיית ה-Email Spoofing הנרחבת. האפיון התבצע בעזרת איחוד של שני מנגנונים שונים עליהם עבדו באותה התקופה - הראשון בהם היה "Identified Internet Mail" שעוצב על ידי Cisco, והשני עונה לשם "Enhanced DomainKeys" ועוצב על ידי Yahoo.

DKIM משתמש בקריפטוגרפיה אסימטרית על מנת לאמת את זהות המקור השולח של הודעת אימייל כלשהי. הדבר מתאפשר באמצעות חתימה דיגיטלית המתווספת (כ-Header) להודעת אימייל הנשלחת ואימותה על ידי השרת המקבל.

לטובת שימוש ב-DKIM על ידי יישות ארגון כלשהו השולח הודעות אימייל, יש ליצור זוג מפתחות אסימטריים (Public-Private Key Pair) אשר ישמשו רק למטרה זו. המפתח הפרטי ישמש לחתום דיגיטלית הודעות אימייל יוצאות על ידי השרת השולח (Sending Server), והמפתח הציבורי ישמש לאימות החתימה הדיגיטלית על ידי השרת המקבל (Recipient Server). בדומה ל-SPF גם DKIM מסתמך על תשתית ה-DNS ואמינותה, והמפתח הציבורי יפורסם בעזרת DNS TXT Record. נפשט את התהליך על ידי דיאגרמה:





לדוגמא, רשומת ה-DKIM של הדומיין "Cyberint.com", המכילה תחת tag "p" את המפתח הציבורי הדרוש לאימות החתימה הדיגיטלית:

```
oz@oz-pt:~$ dig TXT google._domainkey.cyberint.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> TXT google._domainkey.cyberint.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 19141
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;google._domainkey.cyberint.com.      IN      TXT

;; ANSWER SECTION:
google._domainkey.cyberint.com. 5 IN      TXT      "v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAld28lvj2uz1U0t+Dtg0Zwy7/u8l+ipu0jgsSP4BAZlwwKbgmTtf0RXE3kaPQvSDzDnhZ81VJeFzy38B5cPu6/I/tPzY8tN/XchgKfuIa+DtpX+6/jyJS/6Y/TtMH+ILlCax+xBuKs+/7iakBYFGvNcrkJEzJWqQjqAtfCvR5Mjikic8EeuFxrfoTP9o79" "d0qixxujSFEeMoF18BcETKnF2YEgUosLDTX5JHzzABFtxmbyvVjMEqS5Rt1bzDX4zEp691m4zTDKRm4QNVZy6HD3Ytu9iv4mKvAPKfHF2430CYVeoJ4ViDqLdxMDHlrIDV+E7iW/XtsRi5bf5N00CTwIDAQAB"
```

בנוסף, נבחן את שדה ה-DKIM Header המצורף למעטפות הודעות האימייל שנשלחות מהדומיין "Cyberint.com"

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=cyberint.com; s=google;
h=from:mime-version:thread-index:date:message-id:subject:to
:x-original-sender:x-original-authentication-results:precedence
:mailing-list:list-id:list-post:list-help:list-archive
:list-unsubscribe;
bh=yRYCEwQIAw1QmmK84IDbj6rdPQ99SxNh4Q8EVJzExoY=;
b=IxiRA7pf4b5dR7Wa8T8su/z1LQmUBQoTWMP10ixL01T4CjzgsY6KQ4jq8ZXmWIL10Z
6ffOSZ4mVbK6m6DZa5g7Z14KEknP0j1Fn1DEe12c0oRrVMP6+1VeIfzUNrgOLwVE/22aV
OkIORy1VXHJIE6zTa7wH1lDP7FqhReMXz2KeGzVzyIES/pzwmgPrAyJR4oqqLDUx4bZ
RCRCv2rbF5/h3uHsg3rRi0AUcXccr7He7S51mC0r/dmgtinPu9b4gn01bfw4iKc1GxTK
XU2JWXgip4KHWWcCYCSPovooZ1HKb+cCthW1nA91GF152r1rjxX82SosTp/m/X87g1no
dGFQ==
```

בשדה ה-Header המצורף למעטפת הודעת האימייל ניתן להבחין שנכללים דגלים שונים אשר ישמשו על ידי השרת המקבל. החשובים שבדגלים אלו הם:

- a - מכיל את סוג האלגוריתם הנדרש על מנת לייצר את החתימה שצורפה. באופן טבעי, האלגוריתם המומלץ הוא RSA-SHA256.
- b - הוא דגל שערכו הוא החתימה הדיגיטלית (DKIM Signature) שמיצרת משילוב של Headers ותוכן הודעת האימייל.
- d - מכיל את הדומיין שביצע וצירף את החתימה הדיגיטלית למעטפת הודעת האימייל.
- s - מתווסף לשם הדומיין ומשמש בכדי לבקש את המפתח הציבורי המתאים משרת ה-DNS, ומכאן שמו הוא Selector.

DMARC (Domain-based Message Authentication, Reporting and Conformance) הוא הפרוטוקול החדש ביותר אשר אופיין בכדי לתת מענה לבעיית ה-Email Spoofing ובנה על גבי שני המנגנונים שהוצגו קודם, SPF ו-DKIM.

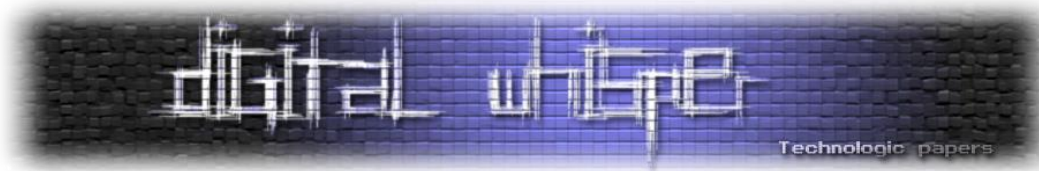
למה יש צורך בעוד מנגנון? ובכן, מספר סיבות קיימות: ראשית, לבעלי דומיין השולח אימיילים אין אינדקציה אם המנגנונים אותם הטמיע (SPF ו-DKIM) עובדים כראוי, כמה אימיילים נכשלו בבדיקת האימות וכמה עברו, או כמה נסיונות Email Spoofing נעשים על אותו הדומיין. בנוסף לכך, תשתיות האימייל הארגוניות מורכבות כיום ממערכות רבות, הכוללות מערכות של נותני שירות צד שלישי. תשתיות מורכבות אלו מקשות על הטמעה יסודית ומקיפה של SPF ו-DKIM.

כפי שנזכר לעיל, DMARC נשען על SPF ו-DKIM לטובת אימות האימייל, ומקנה לבעלי דומיין יכולת לפרסם מדיניות (Policy) הנותנת אינדקציה לשרתים המקבלים האם SPF או-DKIM מוטמעים ומשומשים, ואיך לפעול כשהודעת אימייל מתקבלת ונבדקת בעזרת מנגנונים אלו. בנוסף, מפורסמות ברשומת ה-DMARC גם כתובות אימייל בהן השרת המקבל יכול להשתמש לטובת דיווחים (Reports) לבעלי הדומיין בשמו נשלחה הודעת אימייל.

נתחיל בלפרט על מנגנון האימות ש-DMARC מקנה, ולאחר מכן נדון בדיווחים אותם הוא מאפשר.

DMARC מביא איתו את המושג יישור (Alignment), ובעצם מיישם בדיקה מחמירה יותר של אימות הודעת האימייל בעזרת ה-Headers של הודעת אימייל המתקבלת. בבדיקת ה-SPF ה-Header הנבדק הינו ה-"Envelope From" אך ברוב המקרים תוקפים\ספאמרים ישנו דווקא את ה-"Header From", ולכן DMARC עוצב כך שישווה את ה-"Envelope From" ל-"Header From". בדומה לזאת, גם במקרה של בדיקת DKIM פרוטוקול ה-DMARC לוקח צעד אחד קדימה, ומשווה את ה-"Header From" עם שם הדומיין שמצורף לחתימת ה-DKIM.

לאחר בדיקת היישור (שמבוצעת בשרת המקבל כחלק מהתהליך של DMARC לאחר בדיקות SPF ו-DKIM), השרת המקבל יישם את מדיניות ה-DMARC אותה בעל הדומיין פרסם תחת רשומת ה-DMARC, בהתאם לתוצאות היישור.



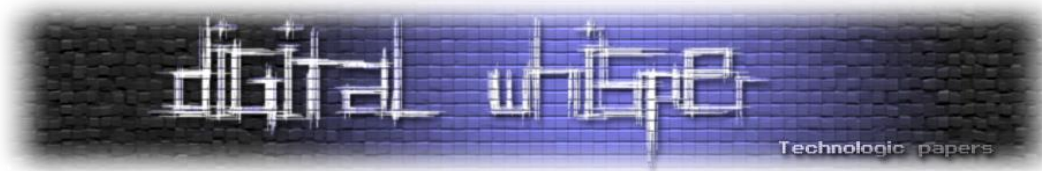
סוגי המדיניות האפשריים לפרסום הינם:

- **None** - בפרסום מדיניות זו בעל הדומיין מתווה לשרת המקבל לא לעשות שום פעולה אם בדיקת DMARC נכשלה. מדיניות זו עוזרת במעקב אחר התקדמות הטמעת DKIM ו-SPF בצורה מקיפה, באשר שהיא תתווה רק דיווח ולא שום פעולה אחרת. הודעת אימייל שנכשלה בבדיקת DMARC תגיע לתיבת האימייל המיועדת בהצלחה כשמדיניות זו מיושמת.
- **Quarantine** - מדיניות זו מתווה לשרת המקבל לסמן אימיילים שלא עברו בדיקת DMARC. שרתים מקבלים וספקי מייל שונים יייתחו למדיניות זו באופן שונה. בחלק מהמקרים הודעת האימייל תסומן כחשודה אך תגיע לתיבת המיועדת לתיקיית ה-Inbox, ובחלק מהמקרים תעבור ישירות לתיקיית הספאם או הזבל (Junk).
- **Reject** - כפי שמשמע, פרסום מדיניות Reject תתווה לשרת המקבל לחסום הודעות אימייל שנכשלו בבדיקת DMARC מלהגיע לתיבת האימייל המיועדת.

כפי שהזכרנו קודם לכן, DMARC מאפשר לבעלי דומיין לקבל דיווחים על הודעות האימייל הנשלחות בשם הדומיין שבבעלותו. סוגי הדיווחים מתחלקים לשניים RUA ו-RUF.

RUA (Reporting URI for Aggregate data) - דו"חות אלו נשלחים פעם ביום בצורה מרוכזת בפורמט XML על ידי ספק־ארגון מסוים (שקיבל אימייל־אימיילים מדומיין כלשהו אשר פרסם רשומת DMARC המכילה דגל RUA עם כתובת אימייל) אל בעל דומיין ומכילים מידע על כל הודעות האימייל שהתקבלו מכתובות המשתמשות באותו הדומיין. המידע המתקבל בדוחות מצטברים (Aggregate) מחולק ל-3 חלקים ומכיל את הפרטים הבאים:

1. מידע על הספק־ארגון ששולח את הדו"ח כגון: שם הספק־ארגון, תיבת המייל ממנה נשלח הדוח ופרטים נוספים ליצירת קשר, מספר דוח, ופרק הזמן עליו התקבל הדיווח.
2. פירוט מלא של רשומת ה-DMARC של הדומיין עליו הדוח נכתב.
3. סיכום תוצאות האימות של SPF ו-DKIM הכוללות - כתובת IP ממנה נשלחה הודעת האימייל בשם הדומיין, אינדקציה על מדיניות ה-DMARC שהוחלה, תוצאות אימות SPF, ותוצאות אימות DKIM.

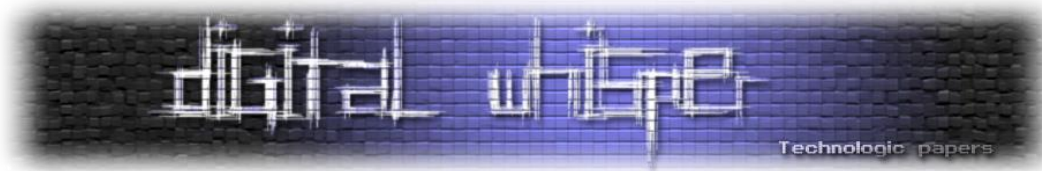


בתמונת הבאה ניתן לראות דוח מצטבר (Aggregate):

```
<?xml version="1.0" encoding="UTF-8" ?>
<feedback>
  <report_metadata>
    <org_name>google.com</org_name>
    <email>noreply-dmarc-support@google.com</email>
    <extra_contact_info>https://support.google.com/a/answer/2466580</extra_contact_info>
    <report_id>3533647987647617325</report_id>
    <date_range>
      <begin>1517011200</begin>
      <end>1517097599</end>
    </date_range>
  </report_metadata>
  <policy_published>
    <domain>cyberint.com</domain>
    <adkim>r</adkim>
    <aspf>r</aspf>
    <p>none</p>
    <sp>none</sp>
    <pct>100</pct>
  </policy_published>
  <record>
    <row>
      <source_ip>209.85.220.73</source_ip>
      <count>2</count>
      <policy_evaluated>
        <disposition>none</disposition>
        <dkim>pass</dkim>
        <spf>pass</spf>
      </policy_evaluated>
    </row>
    <identifiers>
      <header_from>cyberint.com</header_from>
    </identifiers>
    <auth_results>
      <dkim>
        <domain>google.com</domain>
        <result>pass</result>
        <selector>20161025</selector>
      </dkim>
    </auth_results>
  </record>
</feedback>
```

RUF (Reporting URI for Forensic Data) - דו"חות אלו מכילים יותר מידע מאשר דוחות מצטברים ונשלחים על ידי ספק ארגון מסוים (שקיבל אימייל מדומיין כלשהו אשר פרסם רשומת DMARC המכילה דגל RUF עם כתובת אימייל) אל בעל דומיין בהודעת אימייל בזמן אמת, בהתאם לערך שהוגדר בדגל ה-"fo" ברשומת ה-DMARC. דגל ה-"fo" מתווה לשרת המקבל באילו מקרים יישלח דוח מסוג Forensic, ויכול להכיל את הערכים:

- 0 - בהגדרת "fo=0" ברשומת ה-DMARC, השרת המקבל יותווה לשלוח דוח מסוג Forensic במקרים בהם שני המנגנונים (SPF ו-DKIM) נכשלו בבדיקת האימות.
- 1 - בהגדרת "fo=1" ברשומת ה-DMARC, השרת המקבל יותווה לשלוח דוח מסוג Forensic במקרים בהם אחד או שני המנגנונים (SPF ו-DKIM) נכשלו בבדיקת האימות.



המידע המתקבל בדוחות מסוג Forensic הוא מפורט יותר, ומכיל את הפרטים הבאים:

1. מידע על הספקלוארגון ששולח את הדוח כגון - שם הספקלוארגון, תיבת המייל ממנה נשלח הדוח ופרטים נוספים ליצירת קשר, מספר דוח, ופרק הזמן עליו התקבל הדיווח.
 2. זמן הגעת הודעת האימייל שנבדקה אל השרת המקבל.
 3. סיכום תוצאות האימות של SPF ו-DKIM הכוללות - כתובת IP ממנה נשלחה הודעת האימייל בשם הדומיין, אינדקציה על מדיניות ה-DMARC שהוחלה, תוצאות אימות SPF, ותוצאות אימות DKIM.
 4. נושא הודעת האימייל שנבדקה.
 5. מזהה הודעה (Message ID) של הודעת האימייל שנבדקה.
 6. כתובות "Sender From" ו-"Envelope From" ששומשו בהודעת האימייל שנבדקה.
 7. כתובת "Mail To" (כתובת התיבה המיועדת) אליו נשלחה הודעת האימייל שנבדקה.
 8. URLs - במידה וכאלו נכללו בגוף הודעת האימייל שנבדקה.
 9. לעיתים, גוף הודעת האימייל במלואו.
- בתמונת המסך מטה ניתן לראות דוגמא לדוח Forensic:

```
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is a spf/dkim authentication-failure report for an email message received from IP 1.2.3.4 on wed, 09 Mar
Below is some detail information about this message:
1. SPF-authenticated Identifiers: none;
2. DKIM-authenticated Identifiers: none;
3. DMARC Mechanism Check Result: Identifier non-aligned, DMARC mechanism check failures;

For more information please check Aggregate Reports or mail to abuse@participatingISP.com.
-----2276670489547100575-----
Content-Type: message/feedback-report
MIME-Version: 1.0

Feedback-Type: auth-failure
User-Agent: ParticipatingISP/1.0
Version: 1
Original-Mail-From: <xxxxx@domain.com>
Arrival-Date: wed, 09 Mar 2016 11:27:48 +0800
Source-IP: [REDACTED]
Reported-Domain: domain.com
Original-Envelope-Id: xxxxxxxxxxxxxxxx.domain
Authentication-Results: participatingISP.com; dkim=none; spf=fail smtp.mailfrom=xxxxxxx@domain.com
Delivery-Result: reject
-----2276670489547100575-----
Content-Type: text/rfc822-headers; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

Received: from xxxxx ([4.5.6.7])
    by domain.com with SMTP id 1zmYL24ZQc3vYcEd.1
    for <xxxxx@recipient.com>; wed, 09 Mar 2016 11:27:43 +0800
Date: wed, 9 Mar 2016 11:27:37 +0800
From: "Display Name" <xxxxxxx@domain.com>
To: Recipient <xxxxx@recipient.com>
Subject: Check your account!
X-Priority: 3
Mime-Version: 1.0
Message-ID: <xxxxxxxxxxxxxxxxxxxx@domain.com>
Content-Type: multipart/mixed;
```



ננתח את רשומת ה-DMARC של הדומיין "Cyberint.com" והדגלים אותם היא מכילה:

```
oz@oz-pt:~$ dig TXT _dmarc.cyberint.com

; <<>> DiG 9.10.3-P4-Ubuntu <<>> TXT _dmarc.cyberint.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38374
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

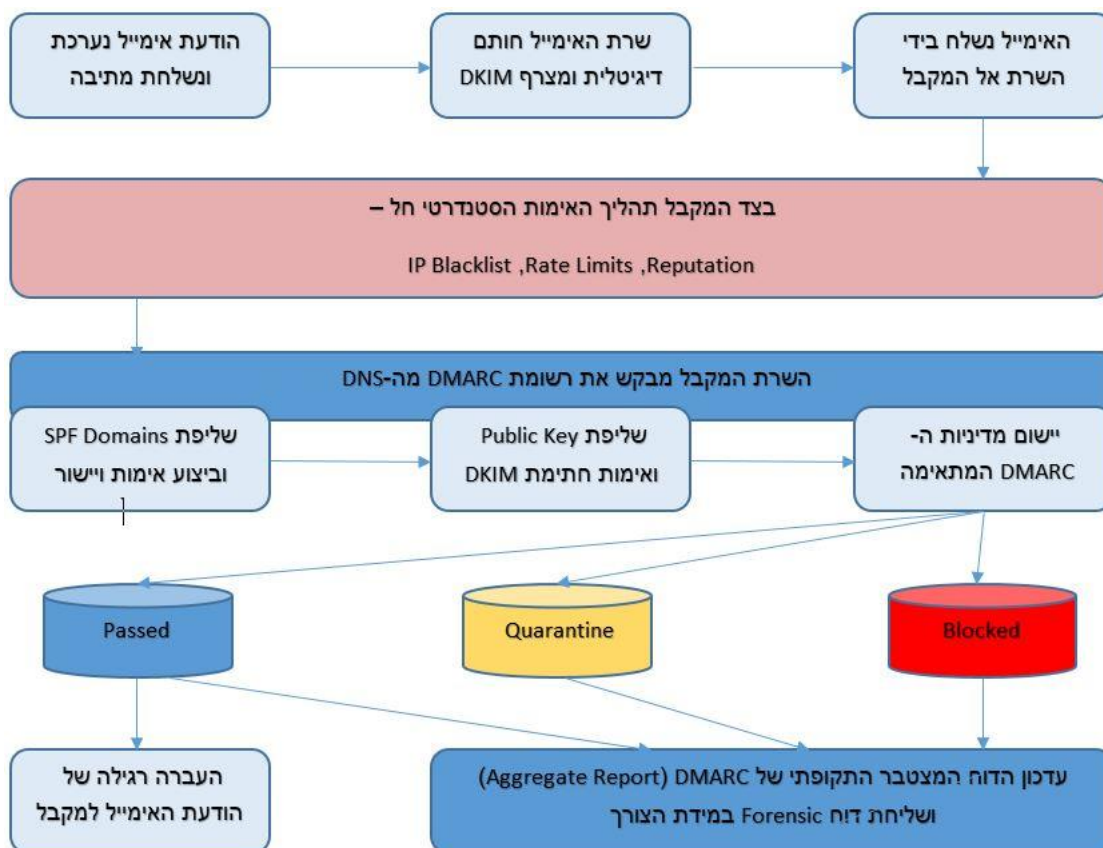
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; MBZ: 0005 , udp: 4096
;; QUESTION SECTION:
;_dmarc.cyberint.com.          IN      TXT

;; ANSWER SECTION:
_dmarc.cyberint.com.  5      IN      TXT      "v=DMARC1; rua=mailto:dmarc-repo
rts@cyberint.com; ruf=mailto:dmarc-reports@cyberint.com; p=none; sp=none; fo=1;"

;; AUTHORITY SECTION:
cyberint.com.          5      IN      NS      park2.livedns.co.il.
cyberint.com.          5      IN      NS      park1.livedns.co.il.
```

- v=DMARC1 - מידע על גרסת ה-DMARC. דגל זה הינו קבוע בערכו וחייב להכלל ברשומה.
- rua=mailto:dmarc-reports@cyberint.com - כתובת האימייל אליה יישלחו דוחות מסוג RUA (Reporting URI for Aggregate Data)
- ruf=mailto:dmarc-reports@cyberint.com - כתובת האימייל אליה יישלחו דוחות מסוג RUF (Reporting URI for Forensic Data)
- p=none - מדיניות ה-DMARC המוגדרת לדומיין זה.
- sp=none - מדיניות ה-DMARC המוגדרת לתתי-דומיין (Subdomains) של דומיין זה.
- fo=1 - דגל ה-"fo" מתווה לשרת המקבל באילו מצבים יישלח דוח Forensic. כשערכו הוא 1, על השרת המקבל לשלוח דוח Forensic אם לפחות אחת הבדיקות של המנגנונים (SPF/DKIM) לא צלחה.

הדיאגרמה הבאה מציגה את התהליך המלא שמתקיים כשהודעת אימייל נשלחת על ידי אימייל דומיין המיישם את SPF, DKIM, ו-DMARC, וגם את פעולות השרת המקבל:



סיכום

שימוש ב-Email Spoofing לטובת Spam, Phishing, הונאות מגוונות, ו-Metaphors Social Engineering, עדיין נפוץ מאוד בימינו. ההתקדמות הטכנולוגית שנעשתה לטובת מניעה של נסיונות זדוניים כאלו מגיעה בצורת המנגנונים SPF, DKIM, ו-DMARC. הטמעה מקיפה ומדויקת של המנגנונים על ידי בעל דומיין יכולה לספק מידת אבטחה גבוהה ביותר כנגד נסיונות המיישמים Email Spoofing. ניתן לראות שכיום רוב הדומיינים השולחים אימייל עדיין לא משתמשים במנגנונים אלו, וגם אם משתמשים ב-SPF באשר הוא הותיק, המוכר, והפשוט ביותר ליישום, DKIM ו-DMARC אינם משומשים, ובהחלט שכחים במידה נמוכה בנוף האינטרנטי של היום. בתור משתמשי קצה ואנשי מקצוע בתחום אבטחת המידע, נותר לנו רק לקוות שהיישומים השולחות אלינו וללקוחותינו הודעות אימייל יטמיעו את המנגנונים האלו בצורה ראויה, כך נוכל לבטוח ללא חשש בכל הודעת אימייל המגיעה לתיבה כלשהי.