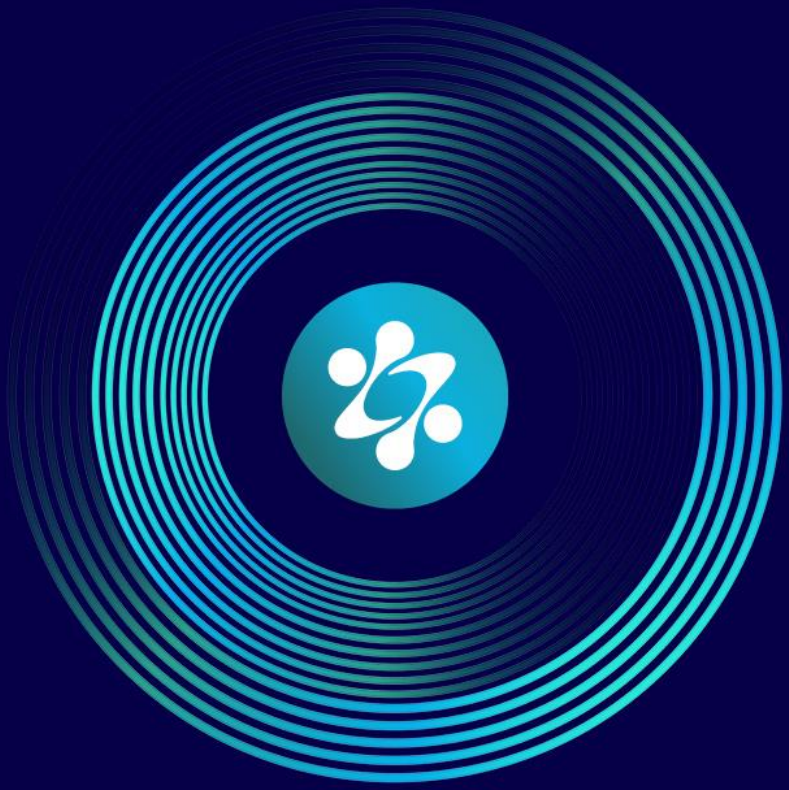

מלחמת "חרבות ברזל" במימד הסייבר: תובנות ודרכי התמודדות

מערך הסייבר הלאומי

דצמבר 2023
V1.0

מערך הסייבר הלאומי

תוכן עניינים

תקציר מנהלים

מראשית מלחמת "חרבות ברזל", מזוהה על ידי מערך הסייבר הלאומי פעילות שהתעצמה באופן הדרגתי, של תוקפים מסוגים שונים כנגד ארגונים במרחב הסייבר הישראלי.

התוקפים פועלים במנעד רחב של שיטות וטכניקות, החל ממתקפות פשוטות, לא מתוחכמות, כגון השחתת אתרים או מתקפות מניעת שירות, ועד לתקיפות ממוקדות כנגד ארגונים המהווים שרשרת אספקה לארגונים רבים במשק במטרה לייצר אפקט רחב.

במסמך זה סוקר מערך הסייבר הלאומי את פעילות הסייבר שזוהתה עד כה למול מרחב הסייבר בישראל ומצביע על מספר תובנות מן החודשיים הראשונים ללחימה.

אופי פעילות התוקפים

1. במהלך המלחמה נראה שדרוג משמעותי בפעילות התקיפה. לאורך זמן ובאופן הדרגתי. בשלב זה של המלחמה, מרבית המתקפות מכוונות למטרות נזק (CNA), בניגוד למיקוד שזוהה לפני הלחימה ובתחילתה אשר התאפיין יותר במתקפות למטרות ריגול וגניבת מידע (CNE).
2. בתקופה זו נצפה שימוש בטכניקות, טקטיקות ונהלים (TTP's) אשר נעשה בהם שימוש שכיח באירועים אחרים בעולם, כגון במלחמת אוקראינה-רוסיה. כך לדוגמה ניתן לראות קווי דמיון בין המלחמות בשני נושאים מרכזיים שעליהם נרחיב בהמשך –

- שימוש בלוחמה פסיכולוגית (תודעה) כאמצעי להדהוד מתקפות סייבר, ושימוש ברשתות החברתיות להעצמת ההשפעה.
- שימוש בכופרות ובפוגענים מסוג Wiper.

3. עיקרי פעילות התוקפים במרחב הסייבר הישראלי בעת המלחמה:

- מתווה תקיפה בולט נראה **בפעילות ריסוס רחבה (Spraying)** - במתווה זה, נעשה ניסיון לנצל לרעה פגיעויות מוכרות וטעויות אנוש בהחלת **הגדרות תצורה (Misconfiguration)**., כגון שימוש בסיסמאות חלשות והעדר אכיפה לנעילת חשבון לאחר קביעת סף לניסיונות הזדהות כושלים.
- **שימוש נרחב בתקיפות מניעת שירות מבוזרות (DDoS)** - ברמה האפליקטיבית (Layer7) וברמה התקשורתית וכן בהשחתת אתרים (Defacement).
- **ניסיונות רבים לחדירה לנכסים שונים במרחב** - לשם השגת אחיזה ומימוש דלף מידע ו/או מחיקת מידע (Wiper).
- **פעילות מול מערכות Linux** - נוסף לפעילות הנפוצה מול מערכות מבוססות Windows, במהלך המלחמה זוהתה פעילות מול מערכות Linux[1], לרבות הפעלת Wiper כחלק מתקיפה למטרת נזק[2][3]. בין היתר, תועד שימוש בטכניקות שונות להעלאת הרשאות

[1] Linux Wiper using off the land binaries
https://www.gov.il/he/departments/publications/reports/alert_1668
[2] Linux Wiper using off the land binaries
https://www.gov.il/he/departments/publications/reports/alert_1668
[3] Disk Wipe

ושימור אחיזה באמצעות מנגנוני תזמון הפעלה מובנים כגון Scheduled Tasks או Cron jobs.[4] [5].

- **מצלמות אבטחה ורשת** (CCTV) - במטרה לפגוע ביכולת השימוש בציוד זה לשם שמירה על המרחב הפיזי וכן נסיונות האויב לאיסוף מודיעין מהאזורים הנצפים על-ידי ציוד זה. כמו כן, הותקפו התקני IoT שונים.
- **מבצעי השפעה** (Influence Operations) - מצד קבוצות התקיפה בעיקר ברשתות חברתיות. כמו כן, נעשה שימוש בערוצים שונים ופרופילים מתחזים, פרסום מידע כוזב (Fake News) או דיס-אינפורמציה (Disinformation), פרסום מידע אמין ללא הקשר טכנולוגי רלוונטי, במטרה להוליך שולל, לפגוע או לנסות לבצע מניפולציה (Malinformation) תודעתית על הציבור הישראלי.
- **תקיפות דיוג** (Phishing) - באמצעות הנדסה חברתית, הן בהודעות דוא"ל והן בהודעות SMS על מנת להגביר אמינות. לעיתים אף נוסף אלמנט משלוח מידע אישי של הנמען, כדי שיפעיל את הקישור או הצרופה. אומנם מדובר בשיטת תקיפה בולטת בשיגרה, אך בתקופת המלחמה נצפתה עליה משמעותית בקמפיינים מסוג זה.
- **תקיפת יישומי Mobile** (אפליקציות לטלפון החכם) - או תשתיות של יישומים אלו, באמצעות פרסום אפליקציות מתחזות, ניצול פערי אבטחה בתשתית היישום ועוד.[6]
- **תקיפות ארגונים השייכים למגזר ה- MSP** - אשר מהווים שרשרת אספקה מהותית לארגונים רבים במשק. בקטגוריה זו ניתן למצוא חברות אירוח ואחסון אתרים וכן חברות אינטגרציה ואספקת שירותי תקשוב.

4. עד כה, במהלך הלחימה זוהו **כ-15 קבוצות תקיפה** עיקריות הפועלות במרחב הסייבר הישראלי. **קבוצות אלו מזוהות כמשויכות לאיראן, חמאס וחיזבאללה** ומרביתן משתפות ביניהן מידע מודיעיני, שיטות וכלים, לטובת מימוש מגוון סוגי תקיפות נגד הנכסים בישראל מולם הן פועלות.

---

https://attack.mitre.org/techniques/T1561/
[4] T1053 - Scheduled Task/Job
https://attack.mitre.org/techniques/T1053/
[5] TA0004 - Privilege Escalation
https://attack.mitre.org/tactics/TA0004/
[6] Mobile Techniques
https://attack.mitre.org/techniques/mobile/

5. ישנם ניסיונות לעידוד קהלי יעד שונים, כדוגמת אקטיביסטים אנטי-ישראליים, לקחת חלק בפעילות ההתקפית נגד ישראל, באמצעות הנגשת יעדים לתקיפה או כלים פשוטים לביצוע מתקפות מניעת שירות.

ארגונים ישראליים בחזית הסייבר

1. פעילות התוקפים זוהתה כנגד ארגונים בעלי המאפיינים הבאים:
   א. ארגונים המהווים נקודת ריכוז (Hub) לפעילות ארגונים נוספים, כחלק משרשרת האספקה של ארגונים שונים במשק הישראלי.
   ב. ארגונים במגזר הבריאות.
   ג. ארגונים במגזר המים.
   ד. ארגונים במגזר האקדמיה.
   ה. ארגונים במגזרי האנרגיה ואספקת דלק.
   ו. ארגונים במגזר התחבורה.
   ז. ארגונים העוסקים בשילוח ימי ועמילות מכס.
2. ארגונים אלו לעיתים מספקים שירותים כדוגמת אפליקציות משותפות חוצות מגזר. התכונה המשותפת הקיימת בעת פגיעה בארגונים אלו, היא האפשרות להשלכה נרחבת על ארגונים נוספים במגזר או כאלו הנעזרים בשירותי הארגון המותקף.

סוגי נכסים מותקפים

1. פעילות התוקפים זוהתה מול מספר רב של נכסים נפוצים בשימוש המשק:
   א. מערכות אבטחה פיזית המשרתות ארגונים שונים במשק, דוגמת מצלמות אבטחה.
   ב. ממשקי ניהול חשופים, דוגמת ממשק בקר המנוהל מרחוק.
   ג. ציוד תקשורת החושף ממשקי ניהול לרשת האינטרנט, כגון Juniper, Cisco.
   ד. מערכות ניטור ושליטה מרחוק החשופות ישירות לאינטרנט[7].
   ה. ממשקי גישה מרחוק, כגון Citrix, Fortinet.

[7] CISA Releases JCDC Remote Monitoring and Management (RMM) Cyber Defense Plan https://www.cisa.gov/news-events/alerts/2023/08/16/cisa-releases-jcdc-remote-monitoring-and-management-rmm-cyber-defense-plan

ו. שרתי Webmail, כגון Exchange OWA, Roundcube ו\או ממשקי EWS.

ז. מערכות ניהול תוכן (CMS), כגון Joomla, Drupal, WordPress.

ח. התקני IoT.

ט. ממשקי API חשופים לאינטרנט, דוגמת ממשקי REST/SOAP.

בלי תקיפה ושיטות בשימוש תוקפים

1. שימוש בשיטות תקיפה מבוססות כלים המותקנים ביעד התקיפה כחלק ממערכת ההפעלה או היישומים (LOLBAS (Living Off The Land Binaries, Scripts and Libraries.[8]
2. הנגשת כלי תקיפה לשימוש גורמים ללא ידע טכני. לדוגמה, הנגשת אתר הכולל Script לתקיפת מניעת שירות (DDoS) באשר על התוקף רק להזין את כתובת יעד התקיפה.
3. ניצול שירותים לשיתוף קבצים לטובת הפעלת כלי תקיפה או שימוש ביוזר לגיטימי לצורך גישה ראשונית לרשת הארגון, תוך מעקף אמצעי האבטחה **וכן כערוץ להדלפת מידע.** שירותים כגון Microsoft OneDrive, Google Drive, Dropbox, Discord Servers.
4. שימוש בכלי קוד-פתוח (Open Source) שהוסבו על-ידי התוקפים, דוגמת DCOMpotato[9], באשר חלק מכלים אלו עושים שימוש לרעה ב- WinAPI.[10]
5. שימוש בתשתיות Proxy ו-VPN חינמיות ומסחריות, או לחילופין עמדות קצה שהותקפו על מנת לשמש כ-Proxy ייעודי, לטובת עקיפת הגבלות בגון שימוש ב-GeoLocation למניעת גישה מחו"ל.
6. ניצול לרעה של פונקציונליות לגיטימיות של מערך הדוא"ל הארגוני, לאחר השתלטות על תיבת דואר של אחד ממשתמשי הארגון. לדוגמה, הגדרת חוקי Outlook/OWA/Office365 לשליחת העתק דוא"ל לתוקף ומחיקת ההודעה שנשלחה.
7. שימוש ב-Reverse Shell לשם יצירת קשר עם שרת הניהול (C&C) והדלפת מידע.[11]

---

[8] רשימה לדוגמה של כלי זמינה ב: Living Off The Land Binaries, Scripts and Libraries
https://lolbas-project.github.io/

[9] כלי תקיפה בשימוש בישראל
https://www.gov.il/he/departments/publications/reports/alert_1671

[10] T1106 - Native API
https://attack.mitre.org/techniques/T1106/

[11] Reverse Shell
T1059 - Command and Scripting Interpreter
https://attack.mitre.org/techniques/T1059/ש

8. שימוש בשירותי אירוח ואחסון אתרים (Hosting Services\VPS), כתשתית לביצוע תקיפות.
9. רשימה פגיעויות בשימוש קבוצות תקיפה שונות מצורפת בנספח א'.

עד כה התמקדנו במתקפות הסייבר אשר זוהו במרחב הישראלי בעת המלחמה הנובעות ממניעיי פגיעה ברציפות התפקודית של המשק.
במלחמה קיים היבט נוסף בהקשרי תקיפות המספקות רווח כלכלי או בדמות רווח כלכלי;

פשיעת סייבר

בצל המלחמה, חלה גם מגמת עלייה בשכיחות מקרי הכופרה בארץ. הבחירה בכופרה ככלי התקפי אינה מפתיעה, ואף טבעית בעת הזו, בה לוחמת התודעה היא נדבך משמעותי במערכה. אפקט ההרתעה והכאוס שמתחולל לאחר מתקפת כופרה משיג את יעדיו. מדובר בנוזקות פשוטות לתפעול, נגישות למשתמש הממוצע, ולא מצריכות ידע טכנולוגי רב למימושן. מניתוח תוכן הדיווחים אשר התקבלו במערך הסייבר הלאומי וטופלו על ידינו עולות מספר תובנות:

1. **מגמת עלייה בשימוש בכופרות מסוג Wiper** - פוגענים אשר מאופיינים במחיקת כלל המידע ברשת. לעיתים פעולה זו מלווה בהזלגת המידע החוצה (לשם קיום משא ומתן על המידע, השפלת הקורבן, התרברבות מצד התוקף) או פשוט במחיקה לשם גרימת נזק לגוף ולרציפותו התפקודית.
2. **נוזקות מסוג כופרה, המופעלות ע"י קבוצות פשיעה במודל עסקי של RaaS (כופרה-כשירות)** - מודל זה, המציע תצורת מינוי, מאפשר לכל משתמש לרכוש מוצר בעלות חודשית ולעשות בו שימוש למטרותיו ושיתוף ברווחים המושגים מתשלום דמי הכופר ע"י הקורבנות. השימוש בכופרות-כשירות נוח במיוחד, מאחר והמוצר הנרכש מגיע עם תמיכה טכנית מלאה, לא מצריך יכולת הבנה טכנית גבוהה, זורע נזק במינימום מאמץ, מבטיח הכנסה ואנונימיות למשתמש. הכופרה אינה ייחודית פר-קורבן ומקשה על שיוך למנוי מסוים ברוב המקרים.
3. **שימוש ראשוני בפוגען Wiper המטרגט שרתים מבוססי Linux** - מגמה זו מתלכדת עם הדיווחים העולמיים אודות קבוצות כופרה ופשיעה, במקביל לקבוצות תקיפה מדינתיות אשר מבצעות ריכוז מאמץ טכנולוגי לשם פיתוח נוזקות וכלים כנגד מערכות מבוססות Unix על גווניהם. ההתרחבות של שחקנים עוינים במרחב הסייבר אל עבר מערכות

הפעלה נוספות מלבד Windows מחייבת את הצד מגן להבין את הסיכונים ולספק מענה כנגד התחזקות פעולות אויב אלו (BIBI, LOLBIN[12]). האויב מודע לכך שהמרכיב האנושי במתקפת סייבר הוא החוליה החלשה. אחוז לא מבוטל מאירועי הסייבר אשר טופלו ע"י המערך, מקורם בגורם אנושי אשר פתח דוא"ל דיוג, לחץ על לינק לא מוכר או הוריד קובץ לא מוכר למערכותיו. אומנם אין מדובר במגמה ייחודית בשעת מלחמה - אך לא מן הנמנע כי מדובר בווקטור מועדף ע"י האויב בזמנים אלו.

4. **עלייה חדה בשימוש בחולשות 1-Day כווקטור חדירה לרשתות** - נראה כי קבוצות התקיפה עוקבות באופן תדיר אחר פרסום חולשות, ומאתרות השמשות לחולשות אלו בפרקי זמן קצרים מאוד. השימוש בחולשות אלו אינו ייחודי לקבוצה אחת, וניתן לראות שימוש רוחבי בחולשות אלו ע"י קבוצות תקיפה מדינתיות וקבוצות פשיעה.

סיבול כספי טרור – המערכה הכלכלית

1. מזה שנים רבות מדינת ישראל מנהלת במקביל ללחימה הפיזית ובסייבר, מערכה כלכלית עיקשת כנגד ארגוני הטרור וגורמי המימון של ארגונים אלו ברחבי העולם.
2. חמאס, בדומה לארגוני טרור נוספים בעולם, פנה לשימוש במטבעות דיגיטליים על מנת להקשות על סיכול גורמי המימון שלו, ובראשם איראן. המעבר ממטבע שאינו מגובה בסחורה (FIAT), לקריפטו, סייע לחמאס בקבלת כסף רב באופן שוטף מאיראן במהלך השנתיים שקדמו למלחמת "חרבות ברזל".
3. תחילה, חמאס עשה שימוש בקריפטו לקבלת תרומות בסכומי כסף קטנים מתומכים ברחבי העולם, אך במהרה עבר לקמפייני מימון המונים נרחבים גם באמצעות הרשתות החברתיות, הכנסות אלו הגיעו לכדי סך של מיליוני דולרים.
4. על פי המטה הלאומי ללוחמה כלכלית בטרור (מט"ל) , קריפטו נהפך לחלק חיוני מהפעילות המבצעית של חמאס. הכספים המועברים משמשים בין היתר לרכישת אמצעי לחימה ולמימון יתר פעולות הטרור.

[12] Linux Wiper using off the land binaries
https://www.gov.il/he/departments/publications/reports/alert_1668

5. במסגרת המלחמה הכלכלית בארגוני הטרור, שותפים שונים במערכת הביטחון בישראל זיהו ותפסו ארנקים דיגיטליים שהכילו עשרות מיליוני דולרים במגוון רחב של טוקנים (מטבעות קריפטוגרפים) אשר המובילים ביניהם הם: ביטקויין (BTC), איתריום (ETH) וטרון (TRX).
6. מערך הסייבר הלאומי הצטרף כשותף למערכה הכלכלית מתחילת המלחמה. במסגרת פעילות זו, פיתח המערך כלים טכנולוגיים ושיטות, אשר אפשרו איתור של עשרות רבות קמפיינים למימון טרור, **בשווי מיליוני דולרים**.
7. הכלים והשיטות שפותחו נבנו במטרה לתת מענה לאתגרי המערכת הביטחונית, כפי ששוקפו למערך על-ידי השותפים מקהיליית הביטחון. לטובת סיוע באיסוף, איתור, ועיבוד של מידע אוסינטי (OSINT) אודות קמפיינים למימון טרור. הכלים הטכנולוגיים פרוסים על מספר רחב ככל הניתן של פלטפורמות בהם פועלים מגייסי התרומות של ארגון הטרור, בדגש על פלטפורמות מימון המונים, רשתות חברתיות ועוד.

תובנות

1. בעקבות זיהוי מתווי התקיפה השונים והמגמות המתפתחות במהלך הלחימה, ניתן להצביע על מספר תובנות:
   א. **ככל שהלחימה מתארכת, תעוזה ויצירתיות התוקפים גוברת** - ניתן לראות זאת במעבר מתקיפות CNE לתקיפות CNA ובן בתקיפות "איכות", כגון תקיפת בית חולים.
   ב. **טרגוט ארגונים המשרתים ארגונים רבים** - ככל שהארגון משרת יותר ארגונים מחוצה לו, בין אם פנים-מגזרית ובין כספק נותן שירותים, הוא הופך למטרה אטרקטיבית יותר בעיני תוקף פוטנציאלי.
   ג. **ריבוי תקיפות שיבוש** - לאור ריבוי תקיפות כופרה או מחיקה הרסנית (Wiper), נדרש לתת דגש על יכולת ההתאוששות.
   ד. **קיומם של מספר גיבויים**- רצוי בטכנולוגיות שונות, אשר לפחות אחד מהם מוחזק בכל עת באופן שאינו מקוון קריטי להתאוששות.
   ה. **יכולת שחזור** - יש לוודא כי ביכולת הארגון לשחזר בהצלחה את כל נכסי הסייבר והמידע, מרמת החומרה ומעלה בסביבה חלופית, על בסיס חומרה חדשה ו/או סביבת ענן ציבורית, בפרט עבור מקרים בהם התוקף ישבש את תקינות החומרה, דוגמת שיבוש/מחיקה של ה-UEFI/BIOS.

ו. **שימוש ב-GeoLocation למניעת גישת תוקפים מחו"ל** - אינו נחשב כאמצעי הגנה הרמטי כנגד תוקף בעל גישה תקשורתית למדינת היעד. תוקפים רבים עוקפים מנגנונים אלו באמצעות שימוש בשירותים חינמיים, מסחריים או תקיפת שרתי ביניים במדינת היעד. עם זאת, מומלץ ליישם שימוש במנגנון זה ברשת הארגון לטובת צמצום חשיפת הרשת ולמניעת מתקפות מסוגים שונים ככל הניתן.

ז. **מתקפות מניעת שירות מבוזרות** (DDoS) - מחייבות היערכות מוקדמת של הארגון באמצעות הסכמים עם ספק האינטרנט ו/או שירות ייעודי לסינון התעבורה. בין היתר, מתן מענה לרמות שונות של נפחי ותדירות המתקפה בדגש על שכבת ה-Networking ושכבת ה-Application.

ח. **חשיפת מצלמות אבטחה לרשת** - מצלמות הן אמצעי אבטחה חשוב בשירות הארגון, יש להימנע מחשיפתן הישירה לרשת האינטרנט, הגדרת סיסמה חזקה (ובאם ניתן אימות MFA) והגבלת גישה אליהן למשתמשים הרלוונטיים בלבד. בזמן התקנתן יש לוודא כי אינן צופות לאזורים רגישים או למתקנים ביטחוניים מדינתיים.

ט. **כח אדם בשעת חירום** - יש להיערך מראש להיעדרותם של גורמי מפתח מקצועיים בשעת חירום, מומלץ להיערך לחלופות באמצעות חוזה שירותים/ שכירת כ"א חלופי.

י. **העלאת כוננות בחירום** - מומלץ לבחון העלאת כוננות יזומה במקרה של חירום מדינתי, לרבות נקיטת פעולות פרואקטיביות דוגמת ניתוק ממשקים מזורז מהאינטרנט, מניעת גישה לשירותים ושרתים שאינם חיוניים או הקשחת מדיניות הגלישה באינטרנט.

יא. **מודעות עובדים** - מומלץ לחדד את מודעות העובדים למתווי תקיפה שכיחים, במיוחד מתקפות דיוג, ודרכי התמודדות מקובלות, לרבות חשיבות הדיווח במקרה של חשד לאירוע סייבר.

יב. **אבטחה פיזית של חדרי שרתים** - המלחמה העלתה את חשיבות האבטחה הפיזית והסביבתית של חדרי השרתים ומתחמי העבודה, במטרה לשמר רציפות תפקודית במקרה חדירה למתקן או של פגיעה פיזית כתוצאה מירי רקטות.

דרכי התמודדות והמלצות

הקטנת משטח תקיפה |

1. מומלץ לפעול להקטנת משטח התקיפה החיצוני של הארגון (EASM), באמצעות מיפוי רציף ומעקב אחר שינויים בו, תוך כדי נקיטת פעולות להקטנת משטח התקיפה. לדוגמה, ניתן לבטל נגישות לפורטים רגישים (ממשקי ניהול) או כאלו שאינם נחוצים לפעילות העסקית והקטנה ככל האפשר של מספר ומגוון השירותים הארגוניים הנגישים מרשת האינטרנט.

עדכוני אבטחת מידע |

2. יצרנים רבים מאפשרים להירשם לרשימות תפוצה ולקבל התרעות על עדכוני אבטחת מידע ישירות לדוא"ל. מומלץ לנצל אפשרות זאת ולוודא כיצד פועלים היצרנים של הציוד המופעל על-ידי ארגונכם, ולעקוב בהתמדה אחר פרסומים אלו.
3. מומלץ לבחון התקנת העדכונים, בפרט אלו בסיווג קריטי וגבוה, תוך פרק זמן סביר ממועד פרסומם. מאחר והתוקפים מצליחים להשמיש פגיעויות תוך שעות ספורות ממועד פרסומן. ישנה חשיבות גבוהה להתקנה מהירה ככל הניתן, לנכסים החשופים ישירות לאינטרנט.

גישה לממשקי ניהול מהאינטרנט |

4. מומלץ להימנע משימוש בתווך האינטרנט לשם מתן גישה לממשקי הניהול. ניתן להשתמש בשירות כגון VPN עם הצפנה והזדהות חזקה מתאימה וכן שימוש בתשתית APN סלולרי או MPLS, ועל גביה לממש VPN.
5. הגדרת כל משתמש בגישה מרחוק, בפרט בהרשאות מנהלן, בהזדהות חזקה (MFA).
6. הטמעת מנגנון Geo-Velocity לאיתור חריגות בתהליך ההזדהות וניהול Session.
7. בחינת האפשרות להגבלת גישה מרחוק באמצעות החלת Deny List על בסיס Threat Intelligence המתעדכן באופן רציף, ובהתייחס לנתונים הבאים:
    1. כתובות IP של שירותי Proxy חינמיים ומסחריים, דוגמת: I2P, Freenet, TOR, ZeroNet, KPROXY, CroxyProxy.
    2. כתובות IP של שירותי VPN חינמיים ומסחריים.
    3. כתובות IP המשויכות למערכי תקיפה מוכרים.
    4. כתובות IP המשויכות למדינות עוינות.

הקשחת עמדות קצה ושרתים |

8. מומלץ לוודא כי לא נעשה שימוש במערכות הפעלה ואפליקציות ללא תמיכת יצרן (End of Life).

9. מומלץ לוודא כי בשגרה לא נעשה שימוש בחשבונות משתמשים בעלי הרשאות גבוהות.
10. מומלץ לבחון ולהפעיל את מנגנוני האבטחה הבאים בעמדות קצה ושרתים:

Secure Boot, Windows credential guard, Windows defender device guard, Controlled folder access, Windows sandbox, AppLocker, Windows Firewall

11. בסביבה מרובת דיירים (Multi-Tenant) מומלץ לבחון אפשרות להפעיל בו זמנית מספר מנגנונים לבידול בין סביבות לקוחות שונים, לרבות: IAM Instance ייעודי לכל לקוח, הצפנת מידע של כל לקוח באמצעות מפתח הצפנה ייעודי, שימוש בבודלים ברמת ה- Kernel דוגמת SELinux ו/או Chroot, הקצאת VXLAN\Geneve ייעודי לכל תעבורת לקוח.
12. מומלץ לוודא כי בעמדות הקצה והשרתים מותקן EDR/XDR בגרסה עדכנית, וכי הוא מתוחזק ומטויב באופן קבוע. הטמעת מוצרים מסוג זה **הוכחו כיעילים במניעה ובלימת מתקפות סייבר**.

הגנה על האתר הארגוני |

13. מומלץ לוודא כי אתר האינטרנט מוגן באמצעות WAAP[13], הכולל מימוש Allow List ברמת שדות וקלט, וביכולתו לאתר האם התעבורה מקורה באדם או מבונה, ולחסום את האחרונה.
14. מומלץ לוודא כי אתר האינטרנט מפותח ומתוחזק בהתאם לדרישות מקובלות לפיתוח מאובטח, כדוגמת OWASP ASVS[14].

הגנה על אפליקציות מובייל ארגוניות |

15. מומלץ לוודא כי אפליקציית Mobile ארגונית מפותחת ומתוחזקת בהתאם לדרישות מקובלות לפיתוח מאובטח, כדוגמת OWASP MASVS [15].

הגנה על ה"מותג" |

16. בחינת שימוש בשירות Brand Protection לשם איתור חריגות דוגמת הקמת אתר אינטרנט או הפעלת אפליקציית Mobile מתחזה.
17. בחינת ניטור אפליקציות מתחזות.

[13] WAAP - Web Application and API Protection (WAAP)
[14] OWASP Application Security Verification Standard
https://owasp.org/www-project-application-security-verification-standard/
[15] OWASP Mobile Application Security
https://mas.owasp.org/

הגנת דוא"ל |

18. מומלץ לבחון באופן עתי את הגדרות התצורה של מערך הדוא"ל ביחס ל- Baseline מאושר, דוגמת Outlook Rules, Transport Rules.
19. חסימת גישה של ממשקי Web mail מהאינטרנט. במידה וקיימת דרישה עסקית לאפשר זאת, מומלץ לממש MFA והגנה באמצעות WAF.
20. מומלץ לוודא כי מערך הדוא"ל מאפשר קבלת דוא"ל רק לאחר השלמת הבדיקות הבאות:
    1. הדוא"ל אינו Spam, לא נשלח מכתובת IP/Domain בעלת מוניטין נמוך.
    2. הדוא"ל אינו מכיל קישורים לכתובות IP IP\Domain בעלי מוניטין נמוך.
    3. הדוא"ל מכיל צרופה בהתאם לסוג שהוגדר ב- Allow List. קיימת זהות בין סיומת הקובץ, ה-Header המציין את סוגו וה- Payload.
    4. הדוא"ל אינו מכיל נוזקה – באמצעות שימוש בחתימות עדכניות ובדיקת Sandbox לאיתור התנהגות חשודה.
    5. הדוא"ל אינו מכיל קוד מובנה בשדה המלל. במקרה שקיים קיים קוד מסוג זה, על מערך אבטחת הדוא"ל להסירו או לבצע Encoding בטרם יועבר למשתמש, כך שלא ניתן יהיה להריצו.
    6. מערך הדוא"ל מסמן באופן ברור למשתמש כי מקורו של הדוא"ל מחוץ לארגון.

הגנה על גלישה מהארגון |

21. חסימת גישה לכתובות IP/Domain בעלות מוניטין נמוך (URL Filtering).
22. מומלץ ליישם אפשרות של פתיחת תעבורה מוצפנת לשם איתור וסיכול איומים.
23. מניעת גישה ישירה של המשתמש לאינטרנט באמצעות שימוש בחוצץ דוגמת RBI או טכנולוגיה דומה.
24. מומלץ לוודא כי מתאפשרת הורדת קבצים רק לאחר השלמת הבדיקות הבאות:
    1. הקובץ הינו מסוג שהוגדר ב-Allow List, וקיימת זהות בין סיומת הקובץ, ה-Header המציין את סוגו וה-Payload.
    2. הקובץ אינו מכיל נוזקה – באמצעות שימוש בחתימות עדכניות, וכן בדיקת Sandbox לאיתור התנהגות חשודה.

אבטחת שרשרת האספקה |

25. מומלץ לוודא כי ספקים בשרשרת האספקה עומדים בדרישות מתודת שרשרת האספקה של מערך הסייבר הלאומי.[16]

אבטחה פיזית |

26. היערכות למניעת פגיעה פיזית אפשרית במתקנים ולהתאוששות ממנה בשיתוף גורמי האבטחה הפיזית בארגון.
27. מומלץ לוודא כי חדרי השרתים של הארגון עומדים בדרישות תקן TIA-942 או Uptime Institute, Tier 3 ומעלה.
28. מומלץ לוודא כי חדר השרתים הארגוני והאתר החלופי (DR) ממוקמים באיזורים גיאוגרפיים שונים ואינם סמוכים זה לזה. במקרה של העדר אתר חלופי, מומלץ לבחון הקמה של אתר מסוג זה, או שימוש בסביבת ענן ציבורית כתחליף.

פרויקטים לאומיים על-ידי מערך הסייבר הלאומי

1. **פרויקט MIRROR** - Managing IR Remediation (for) Organizational Resilience - קהילה מקצועית לטובת שיתוף מידע טכני באופן מהיר והדדי.[17]
2. **תכנית VDP** – Vulnerability Disclosure Program – תכנית לגילוי ואסגרת חולשות המאגדת קהילת חוקרים מקצועיים המסיעים לחוסן המשק הישראלי והעולמי.
3. **תשתיות פישינג** – איתור ודיווח על אודות תשתיות פישינג והונאה במרחב הסייבר.
4. **מרכז לדיווח** - בכל מקרה של חשד לאירוע סייבר ניתן לפנות למרכז המבצעי הזמין 24/7 במספר 119, לדיווח וסיוע במקרה הצורך.

דיווח באמצעות טופס ממוחשב-

טופס דיווח לארגון

טופס דיווח לאזרח

[16] שאלון ספקים לחיזוק שרשרת האספקה - גרסה 1.4
https://www.gov.il/he/departments/news/querysupply

[17] פרויקט MIRROR - קול קורא להשתתפות בקבוצת שיתוף מידע מקצועית
https://www.gov.il/he/departments/publications/Call_for_bids/mirror_call

נספח א' | רשימת פגיעויות הנפוצות בשימוש קבוצות תקיפה

חלק ראשון - חולשות המנוצלות ע"י כ-15 קבוצות לתקיפות בישראל:[18]

CVE	CVSS	Vendor	Product
CVE-2023-4966	7.5	Citrix	NetScaler ADC and NetScaler Gateway
CVE-2023-47246	9.8	SysAid	SysAid Server
CVE-2023-46748	8.8	F5	BIG-IP Configuration Utility
CVE-2023-46747	9.8	F5	BIG-IP Configuration Utility
CVE-2023-43770	6.1	Roundcube	Roundcube webmail
CVE-2023-38831	7.8	RARLAB	WinRAR
CVE-2023-36851	5.3	Juniper	Junos OS
CVE-2023-36847	5.3	Juniper	Junos OS
CVE-2023-36846	5.3	Juniper	Junos OS
CVE-2023-36845	9.8	Juniper	Junos OS
CVE-2023-36844	5.3	Juniper	Junos OS
CVE-2023-34362	9.8	Progress	MOVEit Transfer
CVE-2023-29336	7.8	Microsoft	Win32k
CVE-2023-27997	9.8	Fortinet	FortiOS
CVE-2023-22518	9.8	Atlassian	Confluence Data Center and Server
CVE-2023-22515	9.8	Atlassian	Confluence Data Center and Server
CVE-2023-20198	10.0	Cisco	IOS XE Web UI
CVE-2022-47966	9.8	Zoho	ManageEngine
CVE-2022-41082	8.8	Microsoft	Exchange Server
CVE-2022-26134	9.8	Atlassian	Confluence Server/Data Center
CVE-2022-1388	9.8	F5	BIG-IP
CVE-2021-45046	9.0	Apache	Log4j2
CVE-2021-44223	9.8	WordPress	Wordpress Core
CVE-2021-34473	9.8	Microsoft	Exchange Server
CVE-2021-22986	9.8	F5	BIG-IP and BIG-IQ Centralized Management
CVE-2021-21307	9.8	Lucee Server	Lucee Server
CVE-2020-5902	9.8	F5	BIG-IP
CVE-2020-14882	9.8	Oracle	WebLogic Server
CVE-2020-0796	10.0	Microsoft	SMBv3
CVE-2019-19781	9.8	Citrix	Application Delivery Controller (ADC), Gateway, and SD-WAN WANOP Appliance
CVE-2019-1653	5.3	Cisco	Small Business RV320 and RV325 Routers

[18] פגיעויות המנוצלות לתקיפות בישראל
https://www.gov.il/he/departments/publications/reports/alert_1667

CVE-2019-11510	10.0	Ivanti	Pulse Connect Secure
CVE-2018-13379	9.8	Fortinet	FortiOS
CVE-2017-0199	7.8	Microsoft	Office and WordPad
CVE-2017-0143	8.1	Microsoft	Windows

חלק שני | חולשות בשימוש פעילות גורמי פשיעת סייבר במרחב הסייבר הישראלי:[19]

Product	Vendor	CVE	CVSS
IOX XE	Cisco	CVE-2023-20273 CVE-2023-20198	7.2 10.0
ASA, FTD	Cisco	CVE-2023-20269	9.1
Expressway Series, VCS	Cisco	CVE-2023-20209	7.2
Catalyst SD-WAN Manager	Cisco	CVE-2023-20252	9.8
NetScaler ADC NetScaler Gateway	Citrix	CVE-2023-3519 CVE-2023-4966 CVE-2023-4967	9.8 7.5 7.5
SharePoint	Microsoft	CVE-2023-29357	9.8
Webmail	Roundcube	CVE-2023-5631 CVE-2020-35730 CVE-2020-12641 CVE-2021-44026	5.4 6.1 9.8 9.8
Tomcat	Apache	CVE-2023-41080	6.1
ActiveMQ	Apache	CVE-2023-46604	9.8
SSL-VPN	Fortinet	CVE-2023-27997	9.8
vCenter	VMware	CVE-2023-34048	9.8
WS_FTP	Progress	CVE-2023-40044 CVE-2023-42657	8.8 9.6
Deep Discovery Inspector Apex One Worry-Free Business Security	Trend Micro	CVE-2023-3823 CVE-2023-3824 CVE-2023-41179	7.5 9.8 7.2
FortiProxy FortiOS FortiWeb	Fortinet	CVE-2023-29183 CVE-2023-34984	5.4 8.8
ESG	Barracuda	CVE-2023-2868	9.8
Avalanche, Sentry	Ivanti	CVE-2023-32560 CVE-2023-38035	9.8 9.8

מקורות

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.gov.il/he/departments/publications/reports/vulncatalog1401

[19] פעילות כופרה במרחב הסייבר הישראלי
https://www.gov.il/he/departments/publications/reports/alert_1662

שיתוף מידע עם ה-CERT הלאומי אינו מחליף חובת דיווח לגוף מנחה בלשהו, ככל שחלה על הגוף חובה כזו.
המידע נמסר כפי שהוא (as is), השימוש בו הוא באחריות המשתמש ומומלץ להיעזר באיש מקצוע בעל הכשרה מתאימה לצורך הטמעתו.

16