Mandiant Israel Intelligence Update (MIIU) – August 2022

על התוצר: נייר זה נכתב לטובת עדכון מנהלים על המחקרים שהתבצעו על ידי מנדיאנט ישראל וכן מוסיף את רובד התובנות המחדשות המעניות למרחב הסייבר הישראלי. התוצר מבוסס באופן בלעדי על מקורות מידע ומשאבי מחקר של חברת מנדיאנט. נייר זה לשימושכם ושימוש הארגון שלכם ואינו נועד להפצה והעברה לגורמים שאינם מורשים.

עיקרי דברים

- **סין**
  - **זיהינו קבוצה החשודה כסינית שסורקת רכיבי Pulse Secure ברחבי העולם, כולל בישראל.** הקבוצה סרקה גופים ממספר מגזרים בישראל, לרבות אנרגיה, ביומד, ביטחון, אבטחת מידע ו-NGO. אנו מעריכים שהקבוצה מנסה להתקין webshell על רכיבי Pulse Secure פגיעים – לא ידוע אם באמצעות חולשה מוכרת (1-day) או וקטור תקיפה אחר.
  - **זיהינו קשרים בין שתי קבוצות סיניות הפועלות כבכל הנראה מטעם ה-MSS (APT41 ו-APT17), ברמת תשתית ה-C2 והקוד**. הקשרים מאפשרים לנו לעקוב ולזהות תשתית וכלים נוספים של הקבוצות, ובכך לחשוף פעילות שלהן בעולם וגם בישראל אם תהיה כזו.

- **רוסיה** – **זיהינו קמפיין פישינג שלהערכתנו משויך ל-GRU ושטירגט בין היתר גוף ממשלתי בישראל**. הקמפיין טירגט בין השאר את ישראל וסעודיה כשמוקד העניין היה ביקור נשיא ארה"ב במדינות אלו. **מדובר בפעם הראשונה מזה זמן רב שאנו מזהים פעילות רוסית ישירה לטירגוט גופים בישראל**.

- **איראן**
  - **לראשונה מזה השנה זיהינו פעילות עדכנית במזרח התיכון של קבוצה אירנית המקושרת ל-APT34 (משרד המודיעין האיראני) שפעלה בעבר מול ישראל.** הקבוצה פעלה בעבר מול ממשל ישראלי, ובשנים האחרונות פועלת ברחבי המזרח התיכון, מול תשתיות קריטיות וספקיות תקשורת.
  המודיעין שהקבוצה אוספת עלול לשמש למעקב אחר אזרחים בחו"ל (בפרט במדינות ערב במזרח התיכון) ואף כמודיעין ראשוני לקראת מבצע CNA. מעקב אחר הפעילות עשוי לאפשר לחשוף פעילויות של משרד המודיעין האיראני בישראל ובעולם.
  - **שחקן איראני ביצע פעילות CNA (התקפה) מול הממשל האלבני, שכללה שימוש ב-wiper וכן פגיעה באתרים**, ככל הנראה סביב כנס האופוזיציה שהיה אמור להיערך במדינה. אנו מעריכים שהפעילות מקושרת ל-ZeroCleare, שנחשף בעבר כמבצע CNA איראני. מדובר בפעילות חריגה בפן ההתקפי, וכן מעצם התקיפה הממוקדת באלבניה.

סין

- (TLP RED) **זיהינו קבוצה החשודה כסינית שסורקת רכיבי Pulse Secure ברחבי העולם לרבות בישראל, להערכתנו במטרה להשיג נגישות לגופי מפתח.** בין השאר זיהינו שהקבוצה סרקה גופים בישראל ממספר מגזרים: אנרגיה, ביומד, ביטחון, אבטחת מידע ו-NGO.

לא ידוע לנו כיצד הקבוצה משיגה נגישות לנתקפים בפועל, ייתכן שהיא מתקינה webshell ברכיבי Pulse Secure הפגיעים לחולשות מוכרות (1-day).

יש בידינו מידע על האופן בו הקבוצה סורקת, שיאפשר לזהות פעילות סריקה נוספת מצדה. **אנו מעריכים שמעקב אחר תשתית זו וניסיון לצוד פעילות שלה עשוי להיות רכיב מפתח לזיהוי פעילות סינית בישראל.**

- (TLP RED) **זיהינו קשרים בין הקבוצות הסיניות APT41 ו-APT17, שלהערכתנו פועלות מטעם ה-MSS הסיני.** הקישורים הם ברמת דפוסי התקשורת, רישום ותפעול התשתיות, וכן ברמת תשתית הקוד שמשמשת לפיתוח הכלים.

אנו משתמשים בדפוסים אלו כדי להציף פעילות נוספת של קבוצות אלו ולמצוא מזהים נוספים שלהן – לעיתים אף לפני שנעשה בתשתיות שימוש in-the-wild. **מעקב אחר פעילות קבוצות אלו עשוי להציף פעילות סינית נוספת שלהן בעולם וכן בישראל, אם הן פועלות בארץ.**

רוסיה

- (TLP RED) **זיהינו ניסיון תקיפה של גוף ממשלתי בישראל על ידי הקבוצה הרוסית UNC4024, שלהערכתנו מקושרת ל-UNC2589 החשוד כ-GRU הרוסי.** במסגרת גל הפישינג הנוכחי זיהינו פעילות מול ישראל וסעודיה, כשלהערכתנו מוקד העניין היה סביב ביקור נשיא ארה"ב בביידן במדינות אלו. לצד ישראל וסעודיה, הקמפיין טירגט בין השאר גופי ממשל באירופה ובאוקיאניה.

במסגרת הקמפיין התוקפים שלחו מיילים זדוניים שמכילים קבצי אקסל זדוניים שבתורם מורידים לנתקפים כלי בשם ANGRYSIGN. יש בידינו מזהים של הכלי, תשתית התקשורת וחוקי YARA לזיהוי הפעילות. **מעקב אחר הפעילות והמזהים עשוי לאפשר להציף פעילות נוספת של הקמפיין בישראל ובעולם.**

איראן

- (TLP RED) **לראשונה מזה כשנה זיהינו פעילות של קבוצה המקושרת ל-APT34, שטירגטה בעבר גוף ממשל בישראל, וכיום אנו מזהים מטרגטת ברחבי המזרח התיכון, בין השאר מול סעודיה וירדן.** מדובר בקבוצה שנשארה "מתחת לרדאר" מזה מספר שנים, ללא התייחסויות פומביות, ושעשויה לטרגט פעם נוספת את ישראל.

יש בידינו מידע רב על כלים ושיטות בשימוש הקבוצה, לרבות האופן בו משיגה נגישות ראשונה באמצעות חולשת 1-day (בפרט חולשה ל-Confluence) וה-webshell-ים אותם היא מטילה. במרבית המקרים הקבוצה לא משתמשת

בתקשורת רציפה לשרתי C2 אלא בהתחברות ידנית לנתקף, ועל כן הזיהוי של פעילות הקבוצה מבוסס ברובו על זיהוי הכלים עצמם. **אנו מעריכים שניטור אחר פעילות זו עשוי להציף פעילויות נוספות של הקבוצה בישראל ובעולם.**

- (TLP RED) **זיהינו עפילות חדשה של קלאסטר ZeroCleare האיראני – הקבוצה פעלה מול ממשל אלבניה, השתמשה ב-wiper וכן תקפה אתרים אלבניים.** הפעילות כללה זריעת מסרים פרו-איראניים ונגד האופוזיציה, ככל הנראה סביב כנס האופוזיציה שהיה אמור להיערך באלבניה.

במסגרת הפעילות זיהינו וריאנט חדש של ZEROCLEAR (wiper שבשימוש הקבוצה), כלי ransomware חדש בשם ROADSWEEP, ו-backdoor חדש בשם CHIMNEYSWEEP.

מדובר בפעילות חריגה בהיבטי הטירגוט והרעש התקשורתי והתודעתי שהיא יצרה, ועל אף שלא מדובר בטירגוט של ישראל, זו הזדמנות פז ללמוד על היכולות וסל הכלים האיראני ואיך עשוי להיראות טירגוט דומה של ישראל. פרסמנו בלוג מקיף בנושא שניתן לקרוא בקישור.