מתקפות סייבר/כופרה איראניות נגד ישראל לתכלית תודעתית

בועז דולב ודוד סימן טוב | 2 בינואר, 2022

בשנתיים האחרונות היינו עדים לתקיפות סייבר – המיוחסות לאיראן – נגד חברות וארגונים עסקיים בישראל, לכאורה לתכלית כופרה, אולם למעשה לתכלית תודעתית. יצוין, כי מתקפות כופרה ככלל נפוצות מאד בשנים האחרונות ואף הוגדרו על-ידי הבית הלבן כאיום סייבר מרכזי. יחד עם זאת, השימוש במתקפות כופרה לתכלית תודעתית ולא לתכלית כלכלית הינו תופעה ייחודית במסגרת העימות בין ישראל ובין איראן ותומכיה. מאמר זה מסכם מחקר שבוצע על ידי חברת ClearSky Cyber Security **עבור המכון למחקרי ביטחון לאומי בשיתוף חוקרים מתחום התודעה ומתוכנית איראן במכון. ההבנות האסטרטגיות של התופעה גובשו על ידי צוות חוקרי המכון. המאמר מתאר את תופעת תקיפות הכופרה לתכלית תודעתית, שאירעו בשנתיים האחרונות נגד המגזר הפרטי בישראל. במסגרת המחקר מוסברים: אופן שיוך התקיפות למערך אירגוני איראני; שיטות איבחון בין מתקפת "כופרה לכאורה" למתקפת כופרה "אמיתית"; פירוט הקבוצות האיראניות וכלי העבודה בהם נעשה שימוש. בהמשך מובאות תובנות אסטרטגיות ומפורטות דרכים אפשריות להתמודדות עם התופעה.**

שנת 2020 הייתה נקודת מפנה באופי הפעילות האיראני במרחב הסייבר הישראלי. בחינת אופי הפעילות האיראני עד שנה זו, מעלה כי האיראנים הפעילו בעשור האחרון בעיקר מבצעים לצורך ריגול ומעט מבצעי השפעה (למשל, באמצעות אתרי חדשות כוזבים). מתקפות סייבר שתכליתן הרס שיוחסו לאיראן הופעלו בעיקר נגד מדינות אחרות (ביניהן ערב הסעודית). מתקפה כזו התרחשה באופן חריג גם מול ישראל בשנת 2020, נגד מתקני מים. הייתה זו השנה הראשונה שבה החלו מתקפות כופרה לתכלית תודעה. בחירת החברות המותקפות מתבססת, ככל הנראה, על ניצול הזדמנויות ואינה תוצאה של תכנית סדורה.

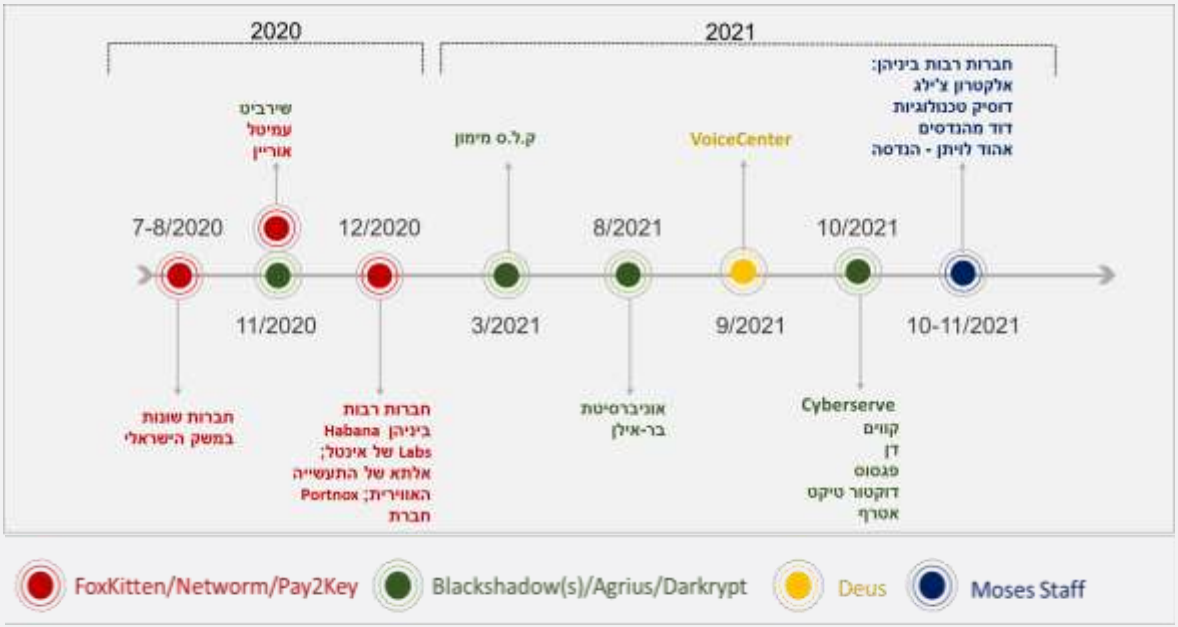
---

* בועז דולב הוא בעל למעלה מעשרים שנות ניסיון בתחום המחקר, מודיעין סייבר, בניית וניהול מערכי הגנת סייבר, וניהול פרויקטים ומערכות ממשלתיות להגנת סייבר. דולב הוא מנכ"ל חברת ClearSky, חברת מודיעין סייבר וביצוע פרויקטים לחברות וארגונים בישראל ובעולם, וכן ראש ועדת הסייבר ואבטחת המידע במכון התקנים הישראלי. בעברו שימש דולב מנהל ממשל זמין ותהיל"ה, אגף החשב הכללי, משרד האוצר.

לאחר הפרסום, ובהתאם לתגובות בתקשורת הישראלית, ממנפים האיראניים את השימוש במידע לאור ההקשר והמאפיינים הישראלים הייחודיים. למשל, מינוף ההתקפה על חברת הביטוח "שירביט" בתחום הפרטיות, בדגש על זיקה למערכת הביטחון. ניצול המרכזיות של אתר "אטרף" בתחום הפרטיות של הקהילה הלהט"בית. חברת Habana labs הקשורה לחברת "אינטל" בתחום העליונות הטכנולוגית, חברות השייכות למגזר הביטחוני ולתחום הסייבר כגון תעשייה אווירית.

להלן מובא תרשים ציר זמן בו מוצגים שמות הקבוצות התוקפות, תאריכי התקיפה ושמות הארגונים שהותקפו ופורסמו ע"י התוקפים. ניתן לראות, כי התקיפות הינן עקביות ומנוהלות בגלים. פרק הזמן שבין התקיפות מנוצל, ככל הנראה, להפקת לקחים ופיתוח כלים חדשים.

ציר הזמן - תקיפות סייבר/כופרה



השינוי האסטרטגי הוא בכך שיעדן של המתקפות הוא הפעלת לחץ על הציבור ובאמצעותו השפעה על מקבלי ההחלטות ועל העימות המתרחש בין ישראל ובין איראן בכמה הקשרים. בין אלו ניתן למנות את המערכה בין המלחמות (מב"מ) מול גורמים איראניים בסוריה, בזירה הימית, או תקיפות סייבר המיוחסות לישראל ולמערב על מגזרים ממשלתיים אזרחיים באיראן. הגידול במתקפות סייבר למטרות כופרה פוגע גם בכלכלת המדינה ובאמון של האזרחים בחברות מובילות במשק. יצוין, כי לאור פריצת ודליפת המידע מחברת הביטוח "שירביט", יו"ר רשות שוק ההון החליט להטיל קנס כספי בסך של יותר מ-10 מיליון שקלים עקב הפרות משמעותיות של הממונה בתחום ניהול סיכוני הסייבר.

דומה שאיראן איתרה "בטן רכה" בישראל – מערכי הגנת הסייבר של המגזר הפרטי/עיסקי. תקיפת ארגונים עסקיים פרטיים מאפשרת לאיראן לפעול באופן חופשי יחסית ולהשיג הישג

כפול – האחד, מול אזרחי ישראל ומקבלי ההחלטות; השני, כלפי פנים – כתגובה לתקיפות סייבר המשבשות את שגרת החיים באיראן. למרות שהרמה הטכנית של התקיפות האיראניות אינה גבוהה, הן מוצלחות בחלקן וצוברות הד תודעתי בעיקר בקרב הקברניטים המשק. הצלחתן נובעת מרמת אבטחה ומודעות נמוכה לצורך בהשקעה בהגנות סייבר של המגזר האזרחי הפרטי בישראל, כמו גם מההדהוד של תקיפות אלה בתקשורת הישראלית.

נוכח ריבוי תקיפות הכופרה, שנפוצו בשנים האחרונות בעולם, הן הוגדרו על ידי הממשל האמריקאי כאיום מרכזי המחייב מענה. הבית הלבן הכריז על הקמת צוות משימה לתיאום צעדים הגנתיים והתקפיים נגד מתקפות כופרה במימד הסייבר. הצוות שהוקם אחראי לעדכן את הבית הלבן באופן רציף על יישום קמפיין לאומי נגד מבצעי כופרה. מאמץ נוסף בהתמודדות עם התופעה הוא החלטת מחלקת המדינה האמריקאית על תשלום תגמול בסכום של עשרה מיליון דולר עבור מידע המוביל לזיהוי פשעי סייבר.

עיקרי התקיפות

בתחילת 2021 נחשף אחד ממערכי הריגול הגדולים שהוציאה לפועל קבוצת תקיפה איראנית, המכונה Fox Kitten. במתקפת סייבר, אשר נמשכה כשנתיים, הצליחו האיראנים לחדור לרשתות מחשוב של מספר רב של חברות בישראל, להתפשט ברשתות הפנימיות ולדלות מידע רגיש ברמות עניין שונות. לאחר חשיפת מערך זה שינתה קבוצה זו את פנייה בשני אופנים: תחילה ניסתה למכור ברשת האפלה את הגישה שהשיגה למותקפים בישראל ובעולם, ולאחר מכן החלה בדפוס חדש של תקיפה: תקיפת כופרה לתכלית תודעתית.

קבוצה זו חדרה בשנתיים האחרונות לעשרות חברות בישראל בתקיפת כופרה ייחודית, ופעלה במתווה תקיפה של קבוצת כופרה "קלאסית": מחשבים הוצפנו, מיילים לתכלית סחיטה נשלחו, כספים הועברו ומפתחות לפתיחת ההצפנה (שלא תמיד עבדו) סופקו. החריגה היחידה מקו ההתנהלות המצופה מקבוצת כופרה היה בשיח מתלהם שניהל התוקף עם המותקפים.

התפתחות נוספת חלה בנובמבר 2020, כשהקבוצה החלה לשלב בין תקיפות כופר ותקיפות תודעה. במהלך תקיפות אלו פרצה הקבוצה והצפינה רשתות ומחשבים בארגונים רבים, ובמקביל הדליפה בחשבונות הטוויטר והטלגרם שלה מסמכים מתקיפות ישנות ונוכחיות. הקבוצה העלתה חדשות לבקרים איומים על ישראל ברשתות החברתיות, ואף הקימה אתר ייעודי להדלפת חומרים מחברות ישראליות תוך קריאת "Winter is coming for Israel". בעקבות זאת סוקרה התקיפה בתקשורת הישראלית וזכתה להד נרחב ברשתות החברתיות.

החל מנובמבר 2020 נרשם גל תקיפות סייבר שונות, המאחדות את כל היכולות והמגמות הקודמות: מטרת התקיפה היא תודעתית, תוך שימוש בשיטת כופרה, כאשר הקבצים המודלפים מעידים לעתים על כך שהתוקפים חדרו למחשבי הארגונים המותקפים למטרות

ריגול זמן רב קודם לכן. למתקפות אלה פרופיל תקשורתי ורשתי גבוה: התקיפות מאופיינות בניסיון נחוש לזכות בכותרות בכלי התקשורת המרכזיים בישראל, שמטרתו, בין השאר, היא לזרוע פחד ומבוכה בתודעת הציבור בישראל.

התקיפות מבוצעות על ידי מספר קבוצות המסוות את עצמן כקבוצות כופרה, ומכנות את עצמן בשמות משתנים כגון: Pay2Key, BlackShadow, NetWorm. התוקפים חודרים לחברות וארגונים וגונבים מידע, זאת לאחר שהתבססו ביעדים אלה במשך חודשים רבים. אך בניגוד לעבר, התקיפות כוללות בנוסף לגניבת מידע גם הדלפות, הצפנה או מחיקה שלו וניהול משא ומתן מתוקשר ככל האפשר עם הקורבן, בדרישה לכופר תמורת שחרור ההצפנה ו/או כדי למנוע דליפה של מידע גנוב נוסף לרשת.

הדלפות המידע מנותבות בעיקרן לרשתות החברתיות טוויטר וטלגרם, ולאתרי הדלפות ברשת האפלה תחת Onion. התקיפה שזכתה לסיקור התקשורתי הנרחב ביותר בגל זה הייתה נגד חברת הביטוח שירביט, שבמסגרתה הודלפו פרטים אישיים של לקוחות רבים. התוקפים תייגו כלי תקשורת בעולם ופנו ישירות לכלי התקשורת כדי שייצרו עמם קשר. בהמשך, פרסמו התוקפים חומרים מביכים מתוך המשא ומתן שהתקיים עם הנהלת שירביט. כאמור, תקיפות אלה מתחזות לתקיפות כופרה אולם התנהלות התוקפים מעידה על כי כסף אינו כנראה בראש מעייניהם, והם מעוניינים במיוחד באפקט הפסיכולוגי.

שיוך התוקפים לאיראן

זיהוי תוקפים ושיוכם נעשה תוך בחינת הפרמטרים הבאים - התנהלות, יעדי תקיפה, כלים, תשתיות ושפה.[1]

אופן ההתנהלות:

התנהלות קבוצות ה"כופרה-לכאורה" האיראניות מבדלת אותן מקבוצות כופרה רגילות, ומצביעה על כך שהמטרה האמיתית היא תודעה ולא רווח כספי.

- שמות הישויות**:** שמות הישויות צצים, נעלמים ומשתנים כמעט בכל מבצע. לקבוצות כופרה מקצועיות חשוב מאוד לשמור על המוניטין שלהן ולכן הן שומרות על שמן כך שיהיה ידוע מה כלול ב"תיק העבודות" שלהן.

- אי שמירה על מוניטין: קבוצות כופרה כלכלית בונות ומשמרות את המוניטין שלהן בכמה ממדים - אופן ניהול המשא ומתן והגינות כלפי מי שמשלם את הכופר: מפתח הצפנה

[1] זהו עיבוד והרחבה של מודל TTP המשמש לזיהוי תוקפים ושיוכם בספרות המקצועית: ניתוח והשוואה של טקטיקות, טכניקות ופרוצדורות (Tactics, Techniques, Procedures) משמש לאפיון התנהגות תוקפים גם בעולם הפיזי וגם בתחום הסייבר.

שבאמת עובד, מחיקת הקבצים הגנובים ואי-פרסומם, תמיכה טכנית למקרה הצורך. כל אלה לא מתרחשים בעת תקיפה של קבוצה בעלת מניע תודעתי.

- היעדר דיסקרטיות**:** קבוצות כופרה מקצועיות פונות ראשית לקורבן לשם משא ומתן דיסקרטי, בדרך כלל באמצעות מכתב כופר הכולל דרכי יצירת קשר. רק במקרה של "פיצוץ" המשא ומתן או אי-יצירת קשר, הן מפרסמות את דבר הפריצה ומדליפות מסמכים גנובים. בקמפייני התודעה האיראניים מסוג כופרה-לכאורה, התוקפים מפרסמים קודם כל את דבר הפריצה ופריטים גנובים ברשת, עוד לפני שהם פונים לקורבן לשם משא ומתן כספי.

- עירוב תקשורת **:**בנוסף לתזמון הפרסום, תוקפי התודעה האיראנים מתייגים גופי תקשורת, ונראה שהם חפצים בעיקר בחשיפה כמה שיותר גבוהה. החשיפה היא המשמעותית ולא הכסף.

- גמישות במשא ומתן: התוקפים האיראניים אינם מוכנים למשא ומתן על מחירים, מציגים אולטימטומים בלתי-מתפשרים ומפרסמים חומרים גנובים בלי לחכות לכופר. זאת, בניגוד לקבוצות כופרה "מקצועיות", שמנהלות משא ומתן דיסקרטי ואמיתי עם גמישות מסוימת, כל עוד המותקף מְתַקְשֵׁר, כדי להגדיל את הסיכוי לרווח כספי.

- אמינות**:** לפחות בחלק מהמקרים בקמפיינים האיראנים, הקורבנות העבירו כספים והמידע המוצפן לא שוחזר. התנהלות זו אינה מאפיינת קבוצות כופרה מקצועיות, שכן היא פוגעת במוניטין ומחבלת בסיכויי קבלת הכופר בתקיפות עתידיות.

- סגנון דיבור: כאשר קבוצת כופרה מקצועית מנהלת משא ומתן, כל השיחה מתנהלת בנימה שירותית ואדיבה, משל היה זה שירות לקוחות (פעמים רבות התוקפים גם מכנים את עצמם support). בתקיפות הכופרה-לכאורה, המיוחסות לאיראן, טון הדיבור היה אטום, כוחני ומזלזל.

- תוקף המידע המודלף - קבוצות כופרה כלכליות תוקפות ארגון בנקודת זמן מסוימת. המסמכים שהן מדליפות אם לא משולם כופר, משויכים לאותו הזמן. קבוצות הכופרה-לכאורה האיראניות הדליפו מסמכים ישנים השייכים לעיתים למידע שנגנב עד שנתיים לפני פרסומם. משמע, נעשה שימוש בחומרים של תקיפות שמטרתן הייתה ריגול, ובעת הסבת המטרה לתודעה הם נעשו פומביים ופורסמו לשם יצירת הד תקשורתי נרחב. דוגמא לכך יכולה לשמש הדלפת מידע של התעשייה האווירית.

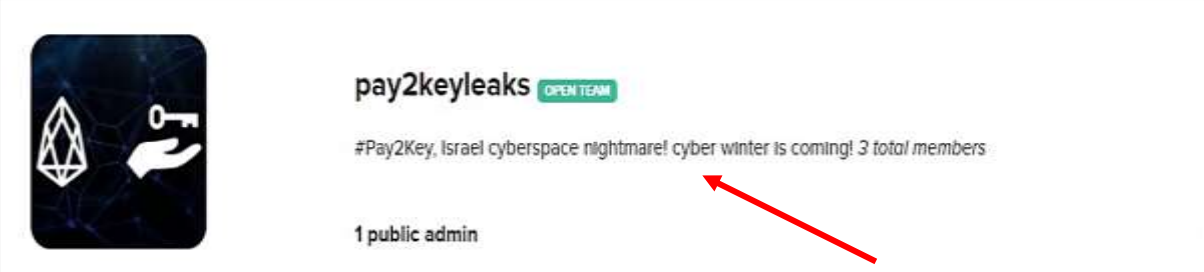
צילום מסך מתוך פרסום של קבוצת Pay2Key. השפה היא בלתי-פורמלית ולא עסקית - שפת ניהול קמפיין רשת ולא שפת עסקת כופר.

יעדי תקיפה:

קבוצות כופרה מקצועיות מתמקדות לרוב במגזר מסוים: בנקים, בתי חולים, מוסדות פיננסיים, ללא חשיבות גיאוגרפית. בקבוצות מסוימות קיימת הימנעות מפגיעה באזור גאוגרפי מסוים, למשל, קבוצות כופרה רוסיות שתוקפות רק מדינות שאינן בחבר העמים לשעבר. מבחינת יעד התקיפה, נראה כי יעדי התקיפה של קבוצות הכופרה מסומנים מראש, כך שניתן יהיה להשיג מהם רווח כספי גדול ככל שניתן.

מרבית הקורבנות שנפגעו בקמפיין התודעה הן חברות ישראליות המדורגות כבינוניות וקטנות. שיטת התקיפה המופעלת על ידי האיראנים על מנת לאתר חברות אלה ולחדור אליהן היא, בשלב ראשון, סריקה רחבה של טווח כתובות האינטרנט הישראלי לצורך איתור שרתים שלהן ושדרכם ניתן יהיה לפרוץ לרשתות של חברות אלו. בשלב הבא מחזיקים התוקפים רשימה של כתובות IP וארגונים שאליהם ניתן לחדור תוך ניצול החולשה. הם מטמינים במערכות הפגיעות כלים ("דלתות אחוריות"), שבאמצעותם ניתן יהיה לשוב ולתקוף את החברות. דפוס פעולה זה מעיד על כך שלרוב התוקפים אינם מסמנים מטרה ותוקפים

אותה, אלא מנצלים הזדמנויות. בחלק מהמקרים בוחרים התוקפים לבצע פעילות ריגול שקטה, ללא פרסום. ובמקביל, הם מסננים ותוקפים ארגונים שלפי הבנתם יסייעו לעורר הד תקשורתי נרחב. היכולת של הארגונים לשלם כופר אינה גורם מרכזי שכן הרווח שהם מייחלים לו הוא כאמור תודעתי ולא כלכלי.



דוגמא להתבטאות גלויה נגד ישראל באתר ההדלפות של קבוצת Pay2Key ברשת החברתית KeyBase.

כלים:

תוקפי סייבר משתמשים במגוון כלים לצורך חדירה לארגון, השגת דריסת רגל וביסוס אחיזה, ובהמשך להפעלת תוכנות ריגול או כופר - בהתאם למטרת התקיפה. חלק מהכלים האלה ידועים, מבוססי קוד פתוח, ציבוריים ולגיטימיים, חלקם כלים בלתי-חוקיים אך זמינים באינטרנט, וחלקם מפותחים על ידי התוקפים.

הכלים הציבוריים מבוססי קוד פתוח הם פחות ייחודיים לתוקף מסוים, אך גם כאן אפשר לראות נטייה של תוקף מסוים להשתמש יותר בכלים מסוימים מאשר באחרים. כלים ייחודיים מפיתוח עצמי משמשים כאינדיקציה חזקה לשיוך קמפיין לתוקף מסוים. כלים אלה מהווים טביעת אצבע של התוקף. מעקב אחר כלים ייחודיים מפיתוח עצמי מאפשר הקבלה בין כלים, קטעי קוד, מחרוזות טקסט ושמות ייחודיים של משתנים, שחוזרים בין קמפיינים שונים. לעתים אפשר לעקוב אחר השדרוגים של אותו כלי בין מִבְצעי תקיפה שונים וכך לשייך מספר מתקפות לתוקף אחד. בכל מתקפה קיימת האפשרות להשתמש בכלים חדשים, שונים או ייחודיים, אולם יש לזכור כי פיתוח או שימוש בכלים חדשים מצריך אימון על הכלים החדשים ולפיכך צורך משאבים גדולים יותר, הן בזמן המושקע והן בכסף. לפיכך, תוקפים חוזרים ומשתמשים באותם כלים וכך ניתן לעקוב אחריהם ולייחס להם קמפיינים בסבירות גבוהה.

בבואנו לייחס לתוקף מסוים את קמפיין התודעה שעל הפרק, נבצע מיפוי של הכלים בהם נעשה שימוש במהלך התקיפות. ניתוח הכלים במרבית התקיפות מסייע לנו להעריך כי הגורמים העומדים מאחורי התקיפות הם גורמים איראניים. מיפוי הכלים בהם נעשה שימוש ושיוכם לקבוצות תקיפה מופיע בטבלה מספר 1.

כדי להדגים כיצד נעשה השיוך באמצעות כלי תקיפה, בחרנו להתמקד בכלי אחד - נוזקה המכונה IPSecHelper, המאפשרת גישת "דלת אחורית" לשרת המותקף ובאמצעותה ניהול

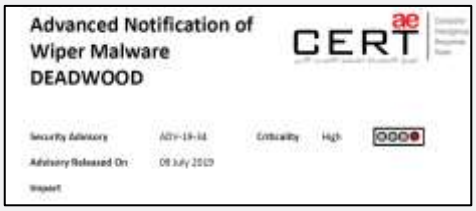
מרחוק של התקיפה. הכלי הופעל ע"י הקבוצה המכונה BlackShadows. כלים נוספים של הקבוצה נותחו במסגרת דו"חות של חברות Sentinel One ודו"ח של חברת Cyberpunkleigh בהתאמה.[2] מחקר נוסף הכולל ניתוח של הכלים והתשתיות של קבוצה אחרת שפעלה במסגרת הקמפיין המכונה Kitten Fox ניתן למצוא בבלוג אתר ClearSky.[3]

הדו"ח של חברת SentinelOne מתעד את נוזקת ה WIPER בשם DEADWOOD שנמצאה במערכות של שירביט כמו גם בחברת הדלק של איחוד האמירויות, בגרסה ישנה יותר לפני כשנה. הדו"ח סוקר את הקשר הישיר בין הנוזקות ואת השינויים שנעשו בגרסאות. הדוח של חברת SentinelOne אינו סוקר את השינויים שבוצעו בנוזקת IPSecHelper.

גרסה 1.5 של נוזקת IPSecHelper עלתה לVirusTotal באוגוסט 2019:

ה-Wiper שנמצא באיחוד האמירויות עלה ל-VirusTotal ביוני 2019:

הקובץ מופיע בדו"ח[4] של ה-CERT של איחוד האמירויות תחת השם DEADWOOD, WIPER הדוח התפרסם ביולי 2019:



בשל ההבנה כי התוקפים מפעילים את נוזקת DeadWood ביחד עם נוזקת IPSecHelper נבדקה התאמה אפשרית בין תאריכי העלאת הקבצים ל-ViruTotal ופרסומי ה-CERT של

[2] https://assets.sentinelone.com/sentinellabs/evol-agrius
https://cyberpunkleigh.wordpress.com/2021/05/27/apostle-ransomware-analysis/
[3] https://www.clearskysec.com/pay2kitten/
[4] https://www.tra.gov.ae/assets/ZTwpCOI3.pdf.aspx

איחוד האמירויות. סמיכות התאריכים מתאימה גם לעדכוני הגרסאות. מוערך בסבירות בינונית, שגרסת IPSecHelper 1.5-xml היא הגרסה הראשונה של התוקפים שהופעלה במתקפה על חברת הנפט באיחוד האמירויות. הגרסה החדשה שנצפתה בשירביט היא גרסה חדשה - עדכון לגרסה הראשונה.

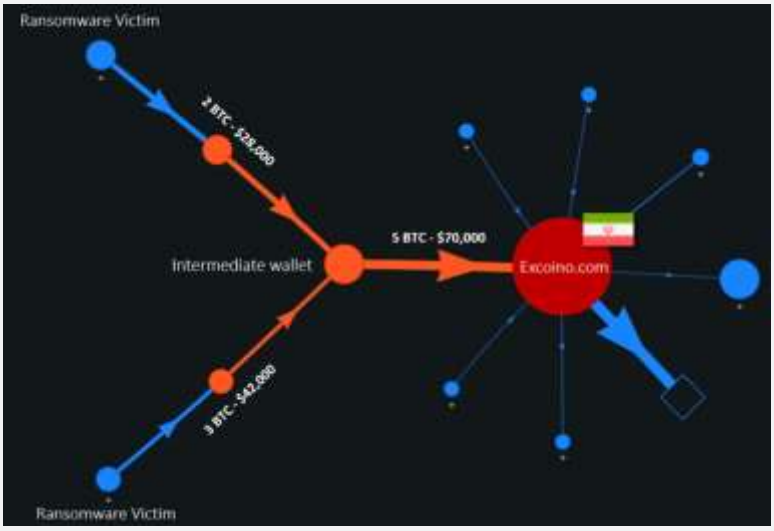
שיוך לקבוצות תקיפה ספציפיות

הטבלה שלהלן מסכמת כלים ומאפיינים נוספים המסייעים לחוקרי ClearSky לשייך מתקפות תודעה איראניות לקבוצות הידועות. יש לציין שוב שבעוד שהשיוך למערך התודעה האיראני הוא ברמת ודאות גבוהה, החלוקה הפנימית היא לנוחותנו בלבד ואינה משקפת בהכרח את המבנה הארגוני בצד השני.

תשתיות:

תשתיות בהן משתמשים התוקפים מסייעות לייחס את הקמפיינים לאותו גורם, או לפחות לראות שיתוף פעולה בין גורמים שונים. בחלק מהמקרים אפשר ממש לשייכם לאיראן: מספרי IP ושרתים המשויכים לאיראן; מספרי IP, שרתים או שירותי אחסון ורישום דומיינים מחוץ לאיראן, ששירתו מתקפות איראניות אחרות וכדומה.

במתקפת הכופרה של Pay2Key ו-NetWorm נעשתה בדיקה של חברת צ'קפוינט אחר מספר הארנק שאליו הצטוו הקורבנות להעביר את הכופר באמצעות תשלום בביטקוין. בדיקה זו הובילה לבורסת מטבעות קריפטוגרפיים איראנית, שהרישום אליו טעון הצגת תעודת זהות איראנית ומספר טלפון איראני.



גרף מתוך מחקר של חברת צ'קפוינט העוקב אחר מסלול הכסף

שפה:

השפה בה משתמשים התוקפים במסגרת משא ומתן לקבלת כופר או בתוך הודעות בערוצי תקשורת שונים יכולה להסגיר את מוצאם ולתת גושפנקה נוספת לגורם אליו ניתן ליחס את הקיפה.

במתקפות התודעה שאירעו בשנה האחרונה, כמו במתקפות כופרה אמיתיות, התוקפים משתמשים בשפה האנגלית לתקשורת עם המותקפים: בהודעות שמגיעות כקובץ Readme או בצורת רקע לשולחן עבודה, ובמשא ומתן על כופר מול נציגי הקורבן. בנוסף הם מתקשרים באנגלית באתרים במרשתת – האפלה והרגילה – ובערוצי טוויטר, טלגרם ועוד, כדי להתגאות במעשיהם ולאתר לקוחות פוטנציאליים למידע המודלף.

בחלק מהמקרים אין מספיק שגיאות באנגלית וקשה להתחקות אחר שפת האם של התוקפים, אך רוב התוקפים בקמפיינים של התודעה שוגים כך שאפשר לזהות בשיח שלהם שגיאות או "מוזרויות", אופייניות לדוברי פרסית. למשל, שגיאות ביידוע וסיתום (התוויות the ו-a בהתאמה) וביחיד-רבים, עם חוקיות שמתאימה לתחביר פרסי.[5] שימוש במילות יחס מוצרכות הוא המאפיין המסגיר ביותר של דוברים לא ילידיים, אפילו בשפות שהם דוברים היטב. מילות היחס השגויות יכולות גם הן להעיד על שפת המקור. כאשר תוקף שוגה בתחומים האופייניים האחרים אך אינו שוגה בשימוש בצורות הפועל המושלמות באנגלית (we have encrypted), זהו גם מאפיין איראני. רמת האנגלית ושיעור השגיאות (אפילו סוג השגיאות) משתנים גם בטקסטים של אותו תוקף, כנראה מכיוון שמדובר בקבוצה שחברים שונים מייצגים אותה בערוצי תקשורת שונים. אך כמעט בכולם השגיאות מצביעות על שפת-אם פרסית.

ולפעמים, אין צורך לנחש: במתקפות על חוקרי איראן באקדמיה, התוקפים כתבו לעתים בפרסית, שהייתה ברמה ילידית. ביצירת קשר אישי אפשר היה לזהות סגנון דומה בין דמויות ניתן היה לזהות גם שימוש בתעתיק עקבי, מה שמעיד על תוקף אחד שמתפעל מספר דמויות. באחד מחשבונות הג'ימייל שנחטפו והושבו, התוקפים שינו את שפת הממשק של גוגל לפרסית; במתקפת Pay2Key של FoxKitten, שהתגלתה ב-2020, נמצאו תשתיות עם שמות בפרסית, למשל citrix@kharpedar webshel. משמעות המילה kharpedar היא "בן חמור"; באחד מקטעי הקוד שנחקרו על ידי ClearSky התגלו קטעי תיעוד – הסבר בשפת אנוש לקוד של התוכנה - בפנגליש (פרסית באותיות אנגליות), ובקבצי "חלוקת עבודה" שהגענו אליהם, הופיעו שמות איראניים אופייניים, ואיותי פנגליש של שמות כמו amrica.

[5] שגיאות ביידוע אופייניות גם לדוברי רוסית ושפות מזרח אסיאתיות, האחרונים גם שוגים ביחיד-רבים. אך לכל אחד דפוס שגיאות ייחודי. שגיאות יידוע שמתאימות לתחביר פרסי כוללות, למשל, את השמטת תווית היידוע the אך שימוש נכון לרוב בתווית הסיתום a, מלבד משפטים שמניים, שבהם היא מושמטת (למשל I am professional). שימוש ביחיד במקום רבים כאשר מדובר בשם עצם קיבוצי (שמספרו אינו חשוב), או תיקון יתר - שימוש בצורת רבים במקומות שאנגלית משתמשת ביחיד במשמעות קיבוצית.

טבלה מספר 1 – פירוט התקיפות על חברות וארגונים אזרחיים בישראל

תוקף	תאריכים	מטרות (קורבנות / יעדים)	כלים מאפיינים המשמשים לשיוך	
			ציבוריים (לגיטימי או לא)	פיתוח עצמי
Blackshadow (s)/ **Agrius/** **Darkrypt**	11-12/2020	שירביט	ניצול חולשות ידועות בשרתי Exchange, VPN, חולשות אפליקטיביות בשרתי IIS, SQLI.	כופרת Apostle פוגען שליטה מרחוק IPSecHelper CryptWrapper – כלי הצפנה
	03/2021	KLS מימון רכב		
	08/2021	אוניברסיטת בר אילן		
	10-11/2021	חברות ישראליות שונות כמו: • Cyberserve • קווים • דן • פגסוס • דוקטור טיקט • אטרף		
FoxKitten/	07-08/2020	חברות שונות במשק הישראלי	Token ייחודי לקונפיגורציה	כופרת Cobalt.Client

Networm/ **Pay2Key**	11/2020	חברות הלוגיסטיקה עמיטל ואוריין ודרכן ישרות חברות נוספות	של FRPC, כולל חפיפה בכתובות שרת שליטה ובקרה בקונפיגורציה	((Pay2Key
	12/2020	חברות רבות, ביניהן Habana Labs של אינטל; אלתא של התעשייה האווירית; Portnox – חברת NAC ועוד רבות אחרות		
Deus	09/2021	Voice Center ודרכה חברות ישראליות רבות	במתקפה זו לא פורסמו הכלים, אך התנהלות התוקף ברשתות, השפה שלו והפעולה בשיטת שרשרת אספקה, מצביעים כולם על קמפיין תודעה איראני.	
Moses Staff	10-11/2021	ארגונים וחברות ישראליות ובינהן : • Gidel • אלקטרון צ'ילג • דוסיק טכנולוגיות • Epsilor • דוד מהנדסים	ניצול חולשת ProxyLogon בחברות ישראליות שמותקנים בהן שרתי Exchange שלא הותקנו להם טלאי אבטחה	כופרת DiskCryptor

		• אהוד לויתן - הנדסה • H.G.M הנדסה • ארצי, חיבה, אלמקייס, כהן פתרונות מיסוי • מתתיהו ברוכים משרד עורכי דין • חברת V-On • קורות חיים של יוצאי 8200		

סיכום

בשנתיים האחרונות אנו עדים לתקיפות סייבר – המיוחסות לאיראן – נגד חברות וארגונים עסקיים בישראל, לכאורה לתכלית כופרה, אולם למעשה לתכלית תודעתית. יצוין, כי מתקפות כופרה ככלל נפוצות מאד בשנים האחרונות ואף הוגדרו על-ידי הבית הלבן כאיום סייבר מרכזי. יחד עם זאת, השימוש במתקפות כופרה לתכלית תודעתית ולא לתכלית כלכלית הינו תופעה ייחודית לישראל ולעימות שלה עם איראן ותומכיה.

שנת 2020 הייתה נקודת מפנה באופי הפעילות האיראני במרחב הסייבר הישראלי. הייתה זו השנה הראשונה שבה החלו מתקפות כופרה לתכלית תודעה. בחירת החברות המותקפות מתבססת, ככל הנראה, על ניצול הזדמנויות ואינה תוצאה של תכנית סדורה.

לאחר הפרסום, ובהתאם לתגובות בתקשורת הישראלית, ממנפים האיראניים את השימוש במידע לאור ההקשר והמאפיינים הישראלים הייחודיים. למשל, מינוף ההתקפה על חברת הביטוח שירביט בתחום הפרטיות, בדגש על זיקה למערכת הביטחון, ניצול המרכזיות של אתר "אטרף" בתחום הפרטיות של הקהילה הלהט"בית, חברת Habana labs הקשורה לאינטל בתחום העליונות הטכנולוגית, חברות השייכות למגזר הביטחוני ולתחום הסייבר כגון תעשייה אווירית.

השינוי האסטרטגי הוא בכך שיעדן של מתקפות אלו, המשבשות את שגרת העבודה של החברות עצמן, הוא להטריד באמצעות הפעלת לחץ על הציבור ולהשפיע על מקבלי ההחלטות ועל העימות המתקיים בין ישראל לבין איראן גם בהקשרים אחרים, ביניהם המערכה בין המלחמות (מב"מ) מול גורמים איראניים בסוריה, בזירה הימית, או נוכח תקיפות סייבר המיוחסות לישראל ולמערב על מגזרים ממשלתיים אזרחיים באיראן.

דומה שאיראן איתרה "בטן רכה" בישראל – מערכי הגנת הסייבר של המגזר הפרטי/עיסקי. תקיפתה מאפשרת לאיראן לפעול באופן חופשי יחסית ולהשיג הישג כפול – האחד, מול אזרחי ישראל ומקבלי ההחלטות; השני, כלפי פנים – כתגובה לתקיפות סייבר המשבשות את שגרת החיים באיראן.

למרות שהרמה הטכנית של התקיפות האיראניות אינה גבוהה, הצלחתן נובעת מרמת אבטחה וממודעות נמוכה לצורך בהשקעה בהגנות סייבר של מגזר האזרחי הפרטי בישראל, כמו גם מההדהוד של תקיפות אלה בתקשורת הישראלית.

מסקנות והמלצות:

1. תקיפות סייבר המכוונות נגד המגזר העסקי/אזרחי מכוונות לנקודות תורפה במערכות הגנת הסייבר של ארגונים אלה. לפיכך, נדרשת חשיבה ברמה הלאומית כיצד להגביר את אבטחת הסייבר הבסיסית על המגזר העסקי/פרטי.

2. בעקבות תופעת תקיפות הכופרה לתכלית תודעה ראוי לבחון אילו תתי-מגזרים פרטיים/עסקיים עלולים לפגוע תודעתית בישראל (למשל, בסוגית הפרטיות) ולבחון כיצד לשפר את ההגנה של מגזרים אלה. במסגרת זו, ראוי לתמרץ את המגזר העסקי להקשיח את מערכי הגנת הסייבר שלו.

3. גורמים הקשורים להגנת הפרטיות – ובראשם הרשות להגנת הפרטיות – נדרשים לאכוף רגולציה קיימת בנושא הגנת סייבר בסוגיות של הגנת פרטיות, ולעדכן אותה בהתאם להתפתחות האיומים.

4. הואיל ומדובר באיום שתכליתו תודעתית, לתקשורת הישראלית תפקיד משמעותי בהתמודדות עם האיום. מוצע ליזום שיח מעמיק של הגורמים הרלוונטיים במדינה עם דוברים וכתבים לענייני ביטחון וטכנולוגיה לשם העמקת ההבנה לגבי האתגר ואופן ההתמודדות עימו במישור התקשורתי, כך שתקטין את הישגי הצד התוקף.

5. יש לבחון כיצד להשתלב במאמצי שיתוף פעולה בינלאומי, בהובלת ארצות הברית, המתמקדים במענה לתקיפות כופרה על מנת להצר את צעדי התוקפים, לחשוף אותם ולהפוך תקיפות מעין אלה לבלתי- לגיטימיות.