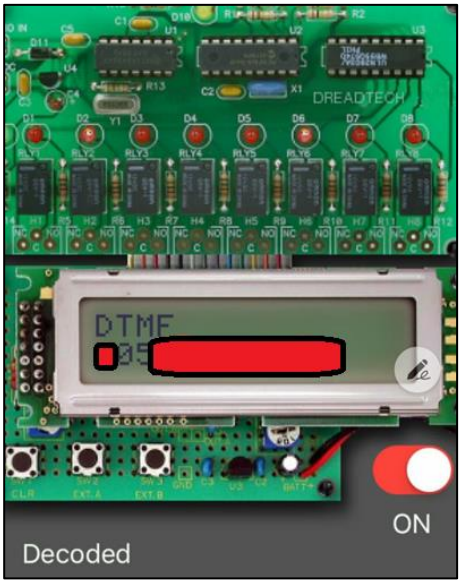
שימוש במפענח DTMF לצורך איסוף מודיעין לפני תקיפת NOC/SOC

מאת אמיתי דן

מבוא

בעבר כתבתי פה על תקיפות[1] מבוססות טלפוניה במערכת הבנקאית בישראל, שלצורך המחשה שלהן השתמשתי במפענח של צלילי הטלפון, הקרוי "DTMF Decoder- Dual Done Multi Frequency".



המאמר הזה נכתב בכדי להמחיש כיצד טכניקה דומה, מאפשרת כיום לאסוף מידע על מספרי טלפון אישיים, אימיילים ופרטים אישיים של עובדים במתקנים שבהם עובר באופן יום יומי מידע רגיש על פרצות אבטחה או אירועי חירום אחרים.

המאמר רלוונטי גם לעולם של אבטחת מידע, יצרני ומתקיני מערכות טלפוניה אך לא פחות מכך קציני ביטחון במתקנים רגישים וחברות במשק

קצת רקע

בסופי שבוע, בשעות הלילה או בחגים, מרכזי החירום כמו SOC/NOC בהקשר של אבטחת מידע וסייבר אך גם מוקדי ביטחון קריטיים אחרים פועלים לא פעם במתכונת מצומצמת, ולעיתים הם מעבירים שיחות טלפון הנכנסות למרכזיה למכשיר הנייד של הכונן.

הכונן לפעמים נמצא במתקן אבל במרוחק מחדר הבקרה, או שהוא עובד לבד וצריך לשמור על זמינות גם אם הוא לא מול המחשב או בסיור, לפעמים מדובר על נציג שבכלל נמצא בבית. המשותף לכלל המקרים

[1] https://www.digitalwhisper.co.il/0x3E/

הוא שבמידה שזה המצב, הטלפון הנייד מאפשר לו זמינות וגמישות, אבל גם הופך את המכשיר שלו לכתובת תקיפה.

מאחר שהפניית שיחה הינה שיטה שמבוססת על מערכות טלפוניה, אנשי אבטחת מידע סייבר, או קציני ביטחון רבים, לא מודעים מספיק להשלכות השליליות של מימוש לא מאובטח במצבים שבהם יש צורך תפעולי בהפניית שיחה.

מדובר על סכנה משולבת גם לביטחון האישי והפרטיות של העובדים, וגם לחשיפה של ההתנהלות במקום והשיחות אליו ממנו ובמתקן עצמו.

אישית במקרה שהניע אותי לכתוב את המאמר הצלחתי לקבל פרטים רבים על נציג בSOC רגיש אשר עבד במשמרת לילה, וזאת לאחר שהתקשרתי כדי להתריע על פרצת אבטחה.

בהקשר של מרכזי SOC/NOC, נקודת המוצא שלנו צריכה להיות, שהם מהווים מטרת איכות, חדירה מוצלחת אליהם או לאנשים שעובדים בהם תאפשר לנו לקבל מידע קריטי בין היתר על התרעות הנוגעות לפרצות שאותרו ולא תוקנו עדיין, אירועי חירום בזמן אמת ומידע רגיש אחר בהתאם לסוג המתקן ולמידע העובר בו באופן יום יומי.

אם יש לתוקף מידע על העובדים במתקן, הוא יכול לנצל זאת כדי לטרגט אותם אישית, לגנוב מחשב של העבודה, או להשתמש בסחיטה איומים ושיטות אחרות שיביאו את העובד לספק את המידע הרגיש באופן עצמאי.

לפעמים, מאוד קל לשכוח שהטלפון היה כאן קודם, להתעסק בסייבר ולשכוח שוב ושוב שהטלפון נשאר אתנו, ומהווה מטרה למתקפות ישנות וחדשות כאחת. מאחר שהמחלקות שמתחזקות את הטלפוניה בארגונים, הן לא פעם נפרדות מה IT וממחלקות אבטחת המידע או הסייבר - הדבר מזמין כשלים מערכתיים, ולפעמים מערכות הטלפוניה מיושנות וקשה להחליף אותן.

לאחרונה פורסם מאמר נוסף של Citizen Lab[2] שבו הם מתמקדים שוב בחברת NSO וסוקרים פעילות של הדבקת מכשירי טלפון ניידים ברחבי העולם. אני אוהב את המאמר הזה, כי הוא מאפשר להסביר למה מספרי טלפון הם מטרה, ולמה כשמישהו רוצה לתקוף מטרה איכותית, ידיעת מספר הטלפון ופרטים רבים על בעל המכשיר תאפשר לתוקף הדבקה קלה יותר מרחוק.

[2] https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

אז איך תוקפים?

לאחר שגורם חיצוני מתקשר בכדי להתריע על פרצות אבטחה מול ה-SOC/NOC או לצורך תקשורת מסווגת או רגישה מול מוקדי חירום אחרים, השיחה מנותבת למספר טלפון שהוזן במרכזיה, ועלול להיות לא פעם מספר נייד אישי של הכונן (מכשיר שלא פעם לא יכיל הגנות מיוחדות אם בכלל), או מכשיר נייד המשותף לכלל הכוננים ומועבר ביניהם, ונמצא פיזית במתקן באופן מתמשך.

בזמן העברת השיחה, התוקף שומע את הצלילים של המרכזייה, שהיא מצידה מזליגה את המספר שאליו מופנית השיחה.

בשלב זה התוקף משתמש במערכת לפענוח של צלילי טלפון, וממשיך לאיסוף מידע על המספר, על המכשיר, על העובד במתקן והפרטים הדיגיטליים והאישיים שלו, פרטי רכב, אימייל אישי וארגוני שיאפשר לאיסוף מידע נוסף או למטרה לפריצה, כתובת מגורים, תמונה של המטרה ועוד.

כלי עבודה בסיסיים:

- מספר הטלפון של המוקד.
- מערכת לפענוח של צלילי טלפון, ניתן למימוש בעזרת תוכנה[3] חומרה[4] או אפליקציה בטלפון נייד[5].
- שימוש בשירותי HLR Lookup שיתנו לנו מידע נוסף על מספר הטלפון[6].
- אפליקציות של ספר טלפונים שיתופי כמו TrueCaller, יש גם שירות Telegram בפיתוח ישראלי בשם "@HelpHebBO" אשר מאפשר קבלת מידע על מספרי טלפון מבלי לדרוש התקנה נוספת.
- Facebook בעבר סיפקה פרטים רבים בקלות על מספרי טלפון. בשביל למשוך ממנה כיום מידע, אפשר להתקין את האפליקציה על מכשיר פיזי או וירטואלי בעל מספר טלפון יחיד. לאחר ההתקנה ומתן הרשאות גישה לספר הטלפונים, פרטים על המספר יופיעו כאיש קשר מומלץ וזאת במקרה שהוא אכן נמצא שם.
- חיפוש המספר דרך תוכנת WhatsApp.

[3] http://www.polar-electric.com/DTMF/Index.htm
[4] http://thespystore.com/dtmf-tone-decoder-dtmf1
[5] https://play.google.com/store/apps/details?id=com.encapsystems.dtmf
[6] https://play.google.com/store/apps/details?id=srl.mobsoft.phonenumberlookup
https://phonenumber-lookup.info/
http://www.txtnation.com/mobile-messaging/hlr-number-lookup/
https://www.hlrlookup.com/validator

בהנחה ועבדתם לפי הוראות אלו, יתכן מאוד שהשגתם:

- שם פרטי
- מספר טלפון נייד
- אימייל פרטי או ארגוני
- פרופיל Facebook
- תמונות של הנציג
- כתובת מגורים שלו

עכשיו תוקף פוטנציאלי יכול לתקוף את כתובת האימייל של העובד, מכשיר הטלפון הנייד, הדבקה דרך הודעה לפרופיל ה-Facebook ועוד.

מבחינה פיזית, תוקף פוטנציאלי יכול היה להשתמש במידע שהושג בכדי לבצע חדירה לכלי הרכב וגניבת מחשב נייד, שימוש במידע לצורך סחיטה אישית, או שיטות אחרות שמתמקדות בעולם הפיזי לצורך משיכת מידע.

המעגלים החברתיים של העובד, יכללו לא פעם את העובדים שמסביבו כך שגם אם מדובר על עובד במתקן רגיש - עם סביבה ממודרת האינפורמציה שנאספה תאפשר איסוף מידע נוסף על הסביבה, ויכולת למתקפה ממוקדת מאוחר יותר.

סיכום

מרכזי SOC, NOC ו-CERT כמו גם מוקדי חירום קיימים ברחבי העולם, והשיטות של התפעול שלהם חוזרות על עצמן לא פעם.

בהקשר של אבטחת מידע, מספק לראות כיצד הנושא של הקמת מרכזים או פונקציות ארגוניות שיודעות לקבל דיווחים על פרצות נפוצים יותר משנה לשנה, בו בזמן כדאי שנבין שהקמת מרכז שכזה, הופכת אותו ואת העובדים שבו למטרה איכותית במיוחד, ולכן יש להגן על העובדים שבהם ועל התשתיות השונות בצורה המרבית.

הקשחה של שירותי הטלפוניה הארגוניות הינה רק נדבך אחד, ההבנה שמרכזי חירום מהווים מטרה הינה מטרת המאמר הזה ואני מקווה שהוא ישפיע על מקבלי החלטות בארגונים הרלוונטיים.

על המחבר

אמיתי דן חוקר אבטחת מידע, בעל רקע במודיעין עסקי, מחקרים בנושא חולשות מכשירים מחוברי אינטרנט וטלפון, חולשות במערכות טלפוניה, מחקר אקדמאי בנושא תקיפת תשתיות אסטרטגיות ועוד. ניתן ליצור קשר ע"י: Linkedin, Blog או Twitter.