

חזית חדשה במלחמת הסייבר אפליקציות מובייל

ומתקדמות. הסיבה העיקרית הינה חוסר ההבנה או הניסיון של אנשי אבטחת מידע בתחום הפיתוח וההגנות הנדרשות ברמת הקוד וזאת למרות שזו הדרך העיקרית שבה האקרים מצליחים לחדור לארגונים.

אנו רואים את הצלחתנו העיקרית בכך שהצלחנו למלא את התפר בין

ההגנה הקלאסית לבין חולשות בפיתוח על ידי ליווי, הדרכות ובדיקות חוסן בדרך ברורה ובתהליכים יעילים המבטיחים את סגירת החולשות ברמת הקוד. מסכם ארז ואומר "כי כפי הנראה פיתוחים במובייל רק ילכו ויגדלו בשנים הקרובות ואנו נהיה בחזית הלחימה ומציאת פתרונות מתאימים."

שיטת העבודה החדשה והמאוד נפוצה היום בארגונים רבים, BYOD-Bring Your Own Device, האם זהו מהלך נכון ונכון לארגונים לדעתך?

"הרצון של ארגונים לאפשר מכשירים ניידים פרטיים לעובדים מהווה סכנה ברורה ומידית לארגונים בכך שלעובד יש נגישות לנכסי הארגון על ידי המכשיר הפרטי שלו, ללא כל

בקרה, דבר המהווה סכנה. הסיבה העיקרית לסכנה זו הינה השימוש הבלתי מושכל ולא מאובטח בשימוש האישי של העובד, אשר ככל הנראה נדבק על ידי תוכנה זדונית, במקרה הטוב, או נשלט על ידי פושע סייבר אשר הצליח להטמיע אפליקציה עם חולשות או דלתות כניסה מוסתרות. ישנן שתי סיבות עיקריות לכך: האפליקציה פותחה ללא תהליכים הגנתיים ולכן יצאה לשווקים עם חולשות מובנות רבות או לחילופין, האפליקציה פותחה עם חולשות בכוונה תחילה כדי להבטיח כניסה חופשית להאקר התוקף."

שאלתנו האחרונה אל ארז מטולה הייתה מה הוביל להחלטה לקיים מסלול הכשרה מתקדם ב-Black Hat U.S.A 2013 בתחום הגנה על אפליקציות מובייל? "עקב דרישה של ארגונים מובילים ממארגני Black Hat, זהו הכנס השנתי המוביל בתחום סקוריות בעולם, המתקיים בארה"ב ולאחר חיפוש אינטנסיבי ועמידה בקריטריונים המחמירים ביותר, העברנו שלוש סדנאות בנושא Mobile Hacking למערכות הפעלה שונים בעיקר אנדרואיד של גוגל וiOS של אפל. זאת על פי דרישתם של המארגנים.

שמחנו לראות שארגונים המובילים ניצלו את האירוע ושלחו מומחי אבטחה מרחבי העולם כדי להגדיל את הידע במציאת חולשות ותהליכי הגנה במכשירים ניידים. שלושת הסדנאות היו מלאות וקיבלנו משוברים חיוביים ביותר. בעיקר על כך שהורדנו והשתמשנו באפליקציות מוגבל פליי ופאס-סטור, תוך כדי שיעור, כדי להדגים את החולשות שלהן הלכה למעשה ולא רק ברמה התאורטית או האקדמית. היה חשוב לנו להראות את הסכנות האמתיות האורבות לארגונים ודרכי אבחון וניתוח על ידי שימוש בכלים המתקדמים שפיתחנו ומתודולוגיות מתקדמות". לשמחתנו, הייתה עליה של אלפי ההורדות של אפליקציות האבחון בחודשים האחרונים.

סיכם ארז ואמר כי "בעקבות הצלחה שלנו ב-Black Hat החלטנו להעביר, לראשונה, את הסדנה בארץ ולתת לנרשמים פרטיים ולא רק לארגונים להירשם לאותה סדנה שהועברה בארה"ב. בניגוד לסדנה אשר הועברה באנגלית בעלות של אלפי דולרים למשתתף הבודד, תועבר הסדנה בארץ בשפה העברית, לנוחיות המשתתפים ובעלות סמלית. אנו מקווים שבכך נוכל להרחיב ולחזק את הידע הנדרש בארץ למומחי אבטחת מידע."

ג'ואי פלג, CISO/SecPrpf, יועץ אסטרטגי להגנת סייבר והדרכות.

מי אינו מתנהל כיום באמצעות המכשירים הניידים? כפי שאנו רואים טלפונים חכמים וטאבלטים ניידים הפכו לחלק מחיינו והצפי לחדירה לשווקים חדשים יגיע למיליארדים של משתמשים חדשים בשנים הקרובות. לצערנו, ככול שיהפכו לנפוצים וחכמים יותר, כך גם תגדלנה הסכנות הטמונות בשימוש באותם האמצעים.

בשונה ממכשירים קלאסיים כמו מחשבים שולחנים וניידים, הטלפון החכם שמלווה אותנו לכל מקום לאורך מרבית שעות היום והלילה, מתעד ושומר ולעיתים אף משדר מתוכו חלק גדול מהפעילות האישית והעסקית שלנו. מכשירים אלו מהווים ערוצי תקיפה חדשים אשר לא היו מוכרים בעבר.

תופעה נוספת הינה ההתפוצצות של אין ספור אפליקציות חדשות לכל מטרה, משחקים, משרדיים, עסקיים וכו'. והעובדה החשובה כי מרבית האפליקציות ומערכות הפעלה, אנדרואיד/iOS פותחו ללא מחשבה הנוגעת לשמירת אבטחה או פרטיות המשתמש.

על פי נתונים ידועים, מרבית התקפות הסייבר מתרחשות דרך חולשות מובנות באפליקציות ומערכות הפעלה וכפי שניתן לראות בתקשורת המקומית והעולמית, הקורבנות העיקרים למחדלי ההתקפות, הינם ארגונים בכל הגדלים בתחומים שונים, פיננסים, רפואיים, תקשורתיים וכו'. "אין יישות שהיא מוגנת מהתקפות סייבר דרך המובייל שלו". אומר **ארז מטולה**, מייסד ומנכ"ל AppSec Labs, מומחה עולמי וידוע שם בתחום אבטחה אפליקטיבית, כי מניסיונו רב השנים אשר נצבר בעקבות עבודתו ועבודת הצוותים של מומחי AppSec Labs אל מול חברות בינלאומיות ומקומיות במגזרים מגוונים כמו חברות תכנות, פיננסים, גופים צבאיים ורפואיים, כי מזה שנים מעבדות אפסכ מלוות ארגונים בינלאומיים בפיתוח מאובטח, בדיקות חוסן ברמת הקוד והכשרות אנשי פיתוח בארץ ובעולם. עוד מוסיף מטולה ומציין כי באותו אופן בדיקו נותנים פתרונות לחברות המשקיעות אמצעים רבים במוצרי מובייל כגון HP, Intel ו-Motorola. "כיוון שאנו בחזית המלחמה כתף בכתף עם חברות בינלאומיות, מחלקת המו"פ שלנו פיתחה כלים לניתוח ואבחון חולשות ברמת הקוד. כלים אלו הפכו לכלי עבודה מוכרים ומקובלים ברחבי עולם ואומצו על ידי מומחים בתחום זה". לבקשתנו, ממשיך ארז מטולה ומרחיב כי "ארגונים רבים מצאו עצמם תחת לחץ כפול של אימונים דיגיטליים נפוצים וחיוב עמידה בתקנים בינלאומיים ובשל כך, בעקבות מציאת ובניית תהליכים אלו, מצאנו את עצמנו מובילים, לא רק בארץ, אלא אף בשווקים בינלאומיים, את התחום של אבטחת אפליקציות."

לשאלתנו מהן הסכנות האפליקטיביות הנפוצות ביותר השיב ארז כי פיתוח ותפוצה של אפליקציות כל כך נפוץ ורחב, שאנשי אבטחת מידע אפליקטיבי מצאו עצמם ללא כלים ותהליכים בשלים לבדיקת חולשות ברמת הקוד ולכן פיתחנו כלים מתאימים וחשוב מכך, תהליכים מתקדמים, על מנת לאפשר ביטחון ופרטיות לארגונים בינלאומיים בתחום זה. "זאת ועוד מוסיף מטולה כי "יש להוסיף לסכנות את הקשר בין המכשירים הניידים לבין שמירת תוכן בענן כחלק מהתפעול הרגיל של האפליקציה. במצב זה יש לבדוק את בניית האפליקציה במכשיר עצמו, תקשורת עם מקום האחסון בענן, מקום האחסון עצמו וחשוב ביותר הזיהוי הוודאי של המשתמש והשרת ואבטחת כל הנקודות האלו."

בנוסף שאלנו את ארז, מהו הממצא המדאיג ביותר מניסיונו בעבודה עם ארגונים וכיצד מצא פתרון לממצאים אלו? על כך השיב כי "כפי שאנו יכולים לראות, כל ארגון ולא משנה מה גדול או חשיבותו, סובלים מחדירות על ידי פושעי סייבר, מודיעין מדינתי או על ידי פעילים חתרניים שמצליחים לחדור ולגנוב מידע או לגרום להרס תשתיות דיגיטליות בארגון וזאת למרות כל ההגנות הקלאסיות כמו חומות אש, WAF, אנטי וירוסים, IDS/IPS וטכנולוגיות הגנה חדשות



ארז מטולה

