מכשירי קצה כ"שער" למערכות מיחשוב ארגוניות

יוראי מולכו, מנהל המחקר הראשי של חברת האבטחה ESET: "אנו נתקלים יותר ויותר בניסיונות להשתמש במכשירי קצה שונים, כמו סמרטפונים או טאבלטים, כפלטפורמה שממנה אפשר להפיץ תוכנות זדוניות, לגרום הרס או גניבת מידע ממערכות מיחשוב הרבה יותר מורכבות"

אבנר פרנק

יוראי מולכו, מנהל המחקר הראשי של חברת ESET, ביקר בארץ לפני כמה ימים על מנת לערוך סיור מקצועי בקרב לקוחות נבחרים של החברה בארץ. במהלך ביקורו הקצר של מולכו הוא ערך ראיון עם כתבנו בנושא אבטחת מידע מודרנית ומה צופן לנו העתיד בתחום. כמו כן, קיבלנו את חוות דעתו המקצועית לעניין ה"האקר" הסעודי וחבר מרעיו, שמטרידים את תושבי המדינה בתקופה האחרונה.

האם תוכל לעדכן אותנו מה הם השינויים שאתם, כחברת אבטחת מידע, חשים בהם בתקופה האחרונה ?

"ראשית, התחום שלנו איננו רק אבטחת מידע, אנחנו עוסקים בתחום הרבה יותר רחב של אבטחה כוללת. אנחנו לא מדברים על אבטחה פיזית,

יוראי מולכו

"איתרנו ניסיון להשתמש בטלפון חכם כפלטפורמה שממנה התוכנה תוכל להיכנס לחשבון הבנק של הלקוחות, ומשם, אחרי שהיא כבר שתולה במערכת הבנקאית - השמים הם הגבול..."

אלא על פתרונות של אבטחה מקיפה לכל תחומי הטכנולוגיה - אנחנו עוסקים במהלך החודשים האחרונים יותר ויותר בפתרונות להגנה על מידע, נתונים, ובעיקר רכיבי קצה שלא עסקנו בהם עד כה. למשל, נושא המידע המועבר ונשמר ברכיבים כמו טלפון חכם, טאבלט, מחשבי רשת וכד' - אנחנו מאתרים עוד ועוד ניסיונות לתקוף רכיבים מעין אלה. כשאני מדבר על תקיפה אני לא מדבר אך ורק על מחיקת המידע ששמור בהם, כלומר פריצה למאגרי הנתונים שיש ברכיבים האלה - לדברים האלו נחשפנו ומצאנו פתרונות הגנה כבר לפני שנה ויותר - אני מדבר על העובדה שיותר ויותר אנחנו נתקלים בניסיונות להשתמש ברכיבים אלה כפלטפורמה שממנה אפשר להפיץ כל מיני תוכנות זדוניות שמטרתן לגרום הרס, לחדור ולאפשר גניבה של מידע מערכות הרבה יותר מורכבות. למשל, איתרנו ניסיון להשתמש בטלפון חכם כפלטפורמה שממנה התוכנה תוכל להיכנס לחשבון הבנק של הלקוחות, ומשם, אחרי שהיא כבר שתולה במערכת הבנקאית - השמים הם הגבול... יהיה קשה מאוד לעצור אותה. נכון שמדובר בינתיים בניסיונות שלא צולחים - אבל אנחנו לא יכולים להיות רגועים ולחשוב שמי משתלט לנו על הטלפון החכם - המקסימום שהוא יעשה זה כמה שיחות על חשבוננו - זה ממש לא הנושא! הנושא הוא העובדה שהטלפון שלנו עלול לשמש כל מיני משתמשים אחרים למטרות הרבה יותר זדוניות מאשר לגנוב שיחת טלפון על חשבונך.

"דבר נוסף שאנחנו בוחנים לעומק הוא מה הולך להיות הטרנד הבא של יצרני התוכנות הזדוניות. שמנו לב שבכל שנתיים מופיע פתאום משהו חדש שבעבר חששנו שהוא עלול להתפרץ. לצערנו, את המשפט "אמרנו לכם" אנחנו אומרים יותר מדי פעמים בתקופה האחרונה, וזאת בגלל שמאז שהופיע הגל הזדוני החדש שהסטוקנט בישר אותו, אנו מגלים עוד ועוד וריאציות לתוכנות שלפני שנה התכוננו אליהן והנה פתאום הן צצות כמו פטריות אצל הלקוחות שלנו".

אתה משתמש בביטוי תוכנות זדוניות כל הזמן, להיכן נעלם האנטי וירוס הוותיק? הוא כבר לא רלוונטי?

"הנושא של אנטי וירוס הוא לא משהו ארכאי או מיושן. מדובר בנושא שהוא בסיסי ומרכזי עבור כל משתמש מחשב בעבר, וכיום בסיסי גם עבור כל מחזיק טלפון ו/או טאבלט. האנטי וירוס לא נעלם, ואני חושש שהוא גם לא ייעלם בעתיד. בגלל הפשטות היחסית ליצור וירוסים, מדי כמה חודשים קם איזה "האקר" צעיר שהוריד כמה תוכנות לבניית וירוסים, הוא לומד את התוכנות הללו ומייצר מוטציות של וירוסים חדשים - אלו הם הווירוסים שאנחנו נלחמים בהם כל יום כל הזמן. התהליך הזה של יצירת וירוסים אולי לא סקסי כבר, אולי לא כל כך מעניין - אבל הוא חי וקיים, ואנשים רעים ממשיכים ליצור עוד ועוד וירוסים כל הזמן. אנחנו זהינו כבר מזמן שלא מדובר בהגנה מפני וירוסים - ההגנה שהמשתמש צריך לקבל היום היא הרבה יותר מאנטי וירוס - אנחנו מדברים על הגנה מפני חדירה למחשב לצורכי השתלטות עוינת, הגנה מפני העתקת מידע חיוני מהמחשב וגם ובעיקר הגנה מפני שימוש במחשב כעמדה התקפה למערכות אחרות מבלי שהמשתמש בכלל מודע לכך. התוכנות הזדוניות היום לא מחפשות אך ורק להרוס או להאט את עבודת המשתמש, אלא גם ובעיקר להשתמש במשאבי המחשב שהם השתלטו עליו כדי להמשיך ולהתרחב ולהגיע למטרה האמיתית, שיכולה להיות מוסד פיננסי, מוסד ממשלתי או כל ארגון אחר שליוצר התוכנה הזדונית יש כוונה לחדור אליו מבלי להשאיר עקבות".

אני החלטתי לא להשתמש יותר באנטי וירוס ובתוכנות הגנה - זה מאט