”כך נעזור לכם בגילוי מידי ותגובה מהירה אשר ימנעו נזק הרסני לארגון“

כחלק ממערך ההגנה ללקוחותיה הקימה חברת ווי אנקור שרות Sandbox ללא תשלום המבוסס על Payload Security

עליית המדרגה באיומים אליהם נחשפים כיום ארגונים דורשת שימוש במנגנוני זיהוי ותגובה השונים לחלוטין מאלו שאפיינו את מערכות אבטחת המידע בעבר. ברבים מהמקרים ארגונים מזהים את הפוגענים שחדרו לארגון רק לאחר שהנזק כבר נעשה והקוד התפשט ברחבי הארגון באופן שמקשה מאוד על הסרתו. כמענה לתופעה זו פותחה מערכת VxStream Sandbox מבית Payload Security, המהווה פלטפורמה חדשנית לניתוח פריטים חשודים המתגלים ברשת הארגון.

יתרונה הבולט של מערכת ה - VxStream, הנה השיטה הייחודית לביצוע ניתוח סטאטי, דינאמי ושילוב בין השיטות ליצירת סוג חדש של ניתוח - Hybrid Analysis. שיטה זו מסוגלת לאתר, לא רק את מה שבוצע במהלך ריצת הקוד הפוגעני בזיכרון, אלא גם את מה שלא בוצע כגון קוד ”רדום“ או ניסיון להשפעה ארוכת - טווח על מערכת ההפעלה. שיטה זו מספקת סוג של יכולת ניתוח לאחור בזמן אמיתי - Reverse engineering on-the-fly.

”בעידן של ימינו לא ניתן למנוע לחלוטין את התקיפה הבאה, במיוחד כאשר תוקף שם לו למטרה ארגון ספציפי, תוך שימוש בכלים שנבנו או הותאמו עבור תקיפת הארגון“, אומר ערן זילברמן, סמנכ”ל מכירות, בחטיבת אבטחת המידע של ווי אנקור. ”כלים אלה מתאפיינים לרוב ביכולת לעקוף כלי הגנה נפוצים, המחפשים דפוסים או חתימות מוכרות ע”י שינוי התנהגותם וחתימתם בהתאם לסביבה בה הם פועלים. בנוסף, שיטות התקיפה מתבססות כיום יותר ויותר על החוליה החלשה בשרשרת ההגנה הארגונית - העובדים עצמם, וזאת באמצעות שיטות של Phishing (דיוג) והנדסה חברתית.“

חסרונם של כלי ההגנה המסורתיים מצוי בהתבססותם על חתימות מדויקות ו/או דפוסים שנכתבו מראש. ובכך, הם עיוורים כמעט לחלוטין לתקיפות המודרניות, שאותן לא ניתן לחתום או לאפיין מראש. עם זאת, יש לזכור שעל אף שלא ניתן למנוע את התקיפה, אין זה אומר שלא ניתן לגלותה ולהגיב אליה ביעילות לפני שהנזק נעשה. שיטה יעילה להתמודדות עם האתגר הנה שימוש משולב בניתוח סטאטי ודינאמי של פריטים חשודים. באמצעות שיטה זו ניתן להבין כיצד אותו פריט עובד, להיכן תיקשר, מה הפריט עושה במערכת ההפעלה, איזה פריטי מידע הפריט מחפש וכו’ וכל זאת בזמן קצר ובאופן אוטומטי לחלוטין“.

מערכת VxStream מבית Payload Security הינה פלטפורמה חדשנית לניתוח פריטים חשודים המתגלים ברשתות הארגון. המערכת יכולה לעבוד כ- Standalone או כחלק ממערך רחב יותר באמצעות ה- API של המוצר ולהריץ קבצים חשודים על מערכות Windows מ- XP עד Windows 8.1, ותמיכה ב- VMWare ESXi או VirtualBox כתשתית.