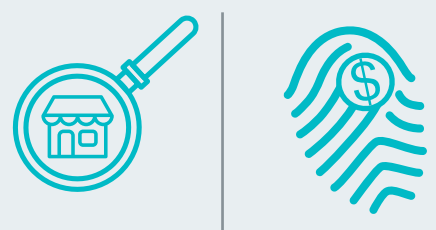
האם העסק שלך מוגן מפני מתקפות כופר?

כל ארגון זקוק להגנה מקיפה של תחנות הקצה והשרתים. ככל שיש יותר מעגלי אבטחה, כך הסיכוי למתקפות סייבר וכופר הולך וקטן.



פשיעת הסייבר צפויה עד 2020 לגלגל 170 מיליארד דולר

63% ממתקפות הסייבר מכוונות לעסקים קטנים

מעל 60% מהנוזקות המופעלות, מסתיימות במתקפת כופר

93% מהמיילים המתחזים (פישינג) מכילים נוזקת כופר

4,000 מתקפות סייבר ביום

כלכלת תוכנות הכופר, הכניסה להאקרים כ-1 מיליארד דולר ב-2016

הטכנולוגיה הרב שכבתית של ESET מספקת הגנה מקיפה ורחבה מפני מתקפות סייבר:

הגנה מפני חדירת קוד זדוני למערכות הפעלה (HIPS)
מזהה התנהגות חשודה במחשב, עוצרת את התהליך הזדוני ומונעת ממנו לבצע שינויים במערכת ההפעלה.

מאגר מידע בענן לדירוג מוניטין קבצים LIVE GRID
בודק בזמן אמת את טיב הקבצים. זמן תגובה מהיר מרגע זיהוי איום חדש עד שהתחנות מוגנות מפניו באמצעות המאגר בענן.

שימוש ב- MACHINE LEARNING
מנגנון שעושה שימוש בטכנולוגית בינה מלאכותית ומנתח התנהגות של דגימות חשודות שנאספו על ידי מאגר ה- LIVEGRID.

הגנה מפני התקפות ברשת הארגון (NETWORK ATTACK PROTECTION) רק במוצרי ה- SECURITY
שכבת אבטחה חשובה כנגד נוזקות (כמו כופר) המפיצות את עצמן ומתפשטות ברחבי הרשת הארגונית, או כנגד פרצות אבטחה שעדיין לא יצא עבורן עדכון.

מוניטין ומטמון (CHACHE AND REPUTATION)
רכיב מקומי שבודק כל אובייקט (קובץ, קישורים לאתרים זדוניים כמו אתרי פישינג) עוד בטרם מתבצעת סריקה באמצעות מאגר המידע בענן (LIVE GRID).

זיהוי על פי DNA (DNA DETECTION)
ביצוע ניתוח התנהגותי מעמיק של הקוד כדי לאתר התנהגות חשודה ואנומליות. זיהוי דגימות לא רק של נוזקות מוכרות, אלא גם של נוזקות שלא נראו מעולם (IN THE WILD).

חוסם פרצות אבטחה (EXPLOIT BLOCKER)
שכבת אבטחה ייחודית המנטרת פרצות, סורקת תהליכים המנסים לנצל אותן וחוסמת אותן. המידע עליהם מועבר לענן (LIVE GRID) לבחינה מעמיקה.

סריקת זיכרון מחשב מתקדמת (ADVANCED MEMORY SCANNER)
טכנולוגיה ייחודית שייעודה הוא זיהוי נוזקות מוסווות או מוצפנות. טכנולוגיה זו מנטרת את ההתנהגות של התהליך הזדוני כל הזמן ומאפשרת לעמוד על טיבו האמיתי של הקוד החשוד.

מערכת זיהוי מבוססת-ענן (CLOUD MALWARE PROTECTION SYSTEM)
שיתוף המידע על דגימות חשודות ב-LIVE GRID מאפשר לגלות בזמן אמת אם הקוד שהתגלה בתחנה זוהה כזדוני. זוהי שכבת אבטחה קריטית בטיפול בהתפרצויות של נוזקות חדשות ולא מוכרות.

הגנה מפני בוטנט (BOTNET PROTECTION) רק במוצרי ה-SECURITY
חלק מהנוזקות (כמו נוזקות כופר) תלויות בין השאר ביכולת של התוקפים לשדר להן פקודות מרחוק. רכיב ההגנה פועל כדי לזהות את התקשורת של הבוטנט ולעצור אותו.

פתרונות אבטחת המידע שלנו מתבלטים בזיהוי מדויק של נוזקות והתקפות סייבר בטרם נעשית פגיעה ממשית, תוך שימוש מינימלי במשאבי המערכת כדי לא להפריע לביצועים. בזכות ממשק הניהול המרכזי, ניתן לקבל תמונת מצב אמיתית על רמת המוגנות ברשת בכל רגע נתון ולטפל באירועים קריטיים בזמן אמת.

יתרונות:

ביצועים מצוינים
שלא מכבידים על המערכת ולא מאטים את המחשבים והשרתים

זיהוי מדויק
למניעת התפרצויות ועצירת איומים לפני שהם חודרים לרשת ומסכנים את המידע

ממשק ניהול מרכזי
מאפשר מבט על הלקוחות ומתריע על אירועי אבטחה קריטיים בזמן אמת

תמיכה טכנית טלפונית, ליווי ומתן פתרונות מקצועיים בעברית לכל בעיה

שמירה על מידע עסקי רגיש
מלזלוג החוצה בזכות שכבות הגנה מגוונות וקשיחות.