הטכנולוגיה הרב-שכבתית של ESET

מעבדות המחקר שלנו הפרוסות ברחבי תבל מאפשרות לנו להעמיד טכנולוגיה חדשנית ודינמית מפני איומי הסייבר המשתנים, הדורשים אבטחה רב-שכבתית. לפני קרוב ל 20 שנה התחלנו לשלב טכנולוגיה פרו-אקטיבית במנועי הסריקה שלנו ופיתחנו את הגישה הרב-שכבתית שנועדה לחסום מתקפות ונוזקות בהתאם לשלב ההפעלה שלהן – החל מהשלב שהן עדיין לא מופעלות ועד השלב שהן כבר פועלות.

הגישה הזה מאפשרת לנו להציע פתרונות שהם הרבה מעבר ליכולות אנטי וירוס בסיסיות. במסמך שלפניכן נציג לכן את גישתנו למלחמה חסרת-פשרות בנוזקות ואת הטכנולוגיה המוכחת ועטורת-הפרסים שלנו, המאפשרת לנו להיות מובילים ומצטיינים בתחום הגנת עמדות-קצה ורשתות עסקיות.

האם האנטי וירוס מת? (אמל"ק: לא)

חברת ESET נוסדה במטרה לפתור למשתמשים בעיות בתחום הנוזקות והוירוסים, והטכנולוגיה שלנו התפתחה עם השנים על מנת להתמודד עם מגוון רחב של איומים. כיום, אנטי וירוס הפך למוצר הגנה בסיסי הנדרש בכל עסק, וגם צרכנים הפנימו את חשיבותה של אבטחת המידע במחשב ובמכשיר הנייד, לא משנה מה רמת ההבנה הטכנית שלהם.

יש כיום באז נרחב בתחום אבטחת מידע של טכנולוגיות "הדור-הבא" ("Next-Gen") שלכאורה מהוות אלטרנטיבה לשיטה ה"מיושנת" של זיהוי נוזקות באופן סטטי. במסמך הזה נרחיב אודות הטכנולוגיות שבהן אנו עושים שימוש במוצרינו, משום שהטכנולוגיות שנחשבות כיום לחדשניות – מוטמעות במוצרים שלנו כבר למעלה מעשור.
בכדי לייצר טכנולוגיית זיהוי מוכחת ומדויקת, נדרשות שנים של מחקר והשקעה כלכלית, ומכאן יתרונה המובהק של ESET שקיימת מעל ל 30 שנים בתחום ה- Endpoint Security.

האנטי וירוס לא מת. מה שכן – התפיסה הישנה, של זיהוי סטטי על בסיס חתימה, אכן לא רלוונטית יותר. כדי להתמודד עם איומים מורכבים, זיהוי סטטי חייב להיות פיסה אחת קטנה מתוך מכלול רחב של טכנולוגיות ושכבות אבטחה – וזו בדיוק התפיסה שאנו מיישמים כבר למעלה מעשור.

אבטחה רב-שכבתית המתמודדת עם מגוון איומים על פני מגוון מערכות הפעלה

המלחמה באיומי הסייבר דומה למרדף בין חתול לעכבר, משום שאנו נלחמים בקבוצות האקרים מיומנות (ובדרך כלל ממומנות) עם מוטיבציה לעשות נזק, אשר משכללות את דרכי הפעולה שלהן כל הזמן ולכן על חברות האבטחה להתפתח בהתאם ואף להיות צעד אחד לפני. כל שיטת לחימה הנשענת על טכנולוגיה סטטית או הנשענת על טכנולוגיה אחת בלבד – לא מספיקה.

מערכות ההפעלה של מיקרוסופט אינן הקורבן היחיד. האקרים מנסים ללא הרף לאתר פירצות אבטחה בכל מערכת הפעלה פופולארית, בין אם של מחשבים או של מכשירים ניידים, במטרה לגבות מידע או כסף באמצעות:
(א) השתלטות מרחוק או קבלת הרשאות גישה למערכת
(ב) הרצה של קובץ הפעלה זדוני שמוחק את המידע, גונב אותו או מצפין וחוטף אותו עבור כופר.

במאמץ הזה, כל מערכות ההפעלה הפכו ליעד. ראינו תקיפות על לינוקס (לדוגמא) ועל מק OSx (אחת מרשתות הבוטנט הגדולות ביותר שנתגלו אי פעם). מכשירים סלולריים הפכו קרבן למתקפות רבות ואפילו ראוטרים ביתיים הותקפו. שימוש ברוטקיט (Rootkit) כבר מסוגל לפגוע קרוב לרמת החומרה וכעת, סביבות וירטואליות צפויות להיות הבאות בתור.

אם בעבר האקרים היו צעירים שרצו לעשות תעלול או להתפרסם, היום הסיפור אחר לגמרי - מדובר בתעשייה שמגלגלת סכומים מטורפים ופועלת מתוך בצע כסף באמצעות גניבת מידע, והשחקנים הראשיים במשחק הזה הם גופי פשיעה או גופים ממשלתיים.

יתרונות הטכנולוגיה של ESET

מטרתו של מנוע הסריקה במוצרים שלנו, הוא לזהות איומים פוטנציאליים ולקבל החלטות באופן אוטומטי לגבי עד כמה הקוד החשוד הוא אכן זדוני. המורכבות היא כפולה: מצד אחד לזהות במדויק קוד זדוני ככזה, אך לא פחות משמעותי: לא לזהות בטעות קוד תקין כזדוני (False-positive).

במשך שנים דאגה ESET לא רק ליכולות הזיהוי אלא גם לביצועי המערכת הנדרשים בתהליך, ולכן התבססה על אלגוריתמים חכמים שנכתבו בשפה הקרובה לשפת המערכת (Assembly) ועל יכולות "ארגז חול" (Sandbox) ותהליכי אמולוציה (emulation, שפירושה; בידוד והרצת הקוד החשוד בתוך סביבה וירטואלית מבודדת במחשב, כדי לבחון את התנהגותו ולסווג אותו כזדוני או נקי).

כיום, הגישה שלנו השתפרה משמעותית. כדי להשיג ביצועים מקסימלים אנו עושים שימוש ב**תרגום בינארי** לצד **יכולות האמולוציה** (emulation). שילבנו במוצרים שלנו יכולות "ארגז חול" באמצעותן אנו מבודדים רכיבים מסוימים ברמת החומרה או התוכנה ומריצים אותם כתכנית בתוך סביבה וירטואלית. בעבר היינו צריכים לבודד רכיב רכיב ולבחון כל אחד בנפרד אך עם **תרגום בינארי** אנו מסוגלים להריץ בדיקה זו על גבי יחידת העיבוד המרכזית במחשב (CPU) ולשפר משמעותית את ביצועי הסריקה ואת צריכת המשאבים. מוצרי ESET מנתחים מאות פורמטים שונים של קבצים (קבצי הרצה, קבצי ארכיון, סקריפטים, מסמכים וכו') במטרה לזהות במדויק רכיבים זדוניים המוטמעים בתוך הקוד.

ישנן דרכים רבות שהאקרים יכולים להמנע מזיהוי ולכן מערכת אבטחה המתבססת על שכבה אחת לא מספיקה. אנו מאמינים שרק הגנה בזמן האמת המבוססת על מספר שכבות אבטחה, יכולה להגיע לרמות זיהוי גבוהות ביותר.

שכבות האבטחה בטכנולוגיה של מוצרי ESET

הדיאגרמה הבאה מציגה את הבעיות שמייצרות נוזקות לאורך חייהן, ואילו משכבות האבטחה של ESET פועלות בכל שלב –

Botnet Protection	***Cloud Malware protection system***	***Reputation System***	***Exploit Blocker***	***Network Attack Protection***	***Advanced Memory Scanner***	***DNA detections***	***Scanning engine***	**הטכנולוגיה / שלב הפעולה של הנוזקה**
		■		■				החדרת הנוזקה למערכת
			■	■				ניצול פירצות אבטחה
	■				■	■	■	התקנת הנוזקה
■	■	■						ניהול מרחוק על ידי שרת בקרה ושליטה (C&C)
■	■				■	■		הרצת הנוזקה

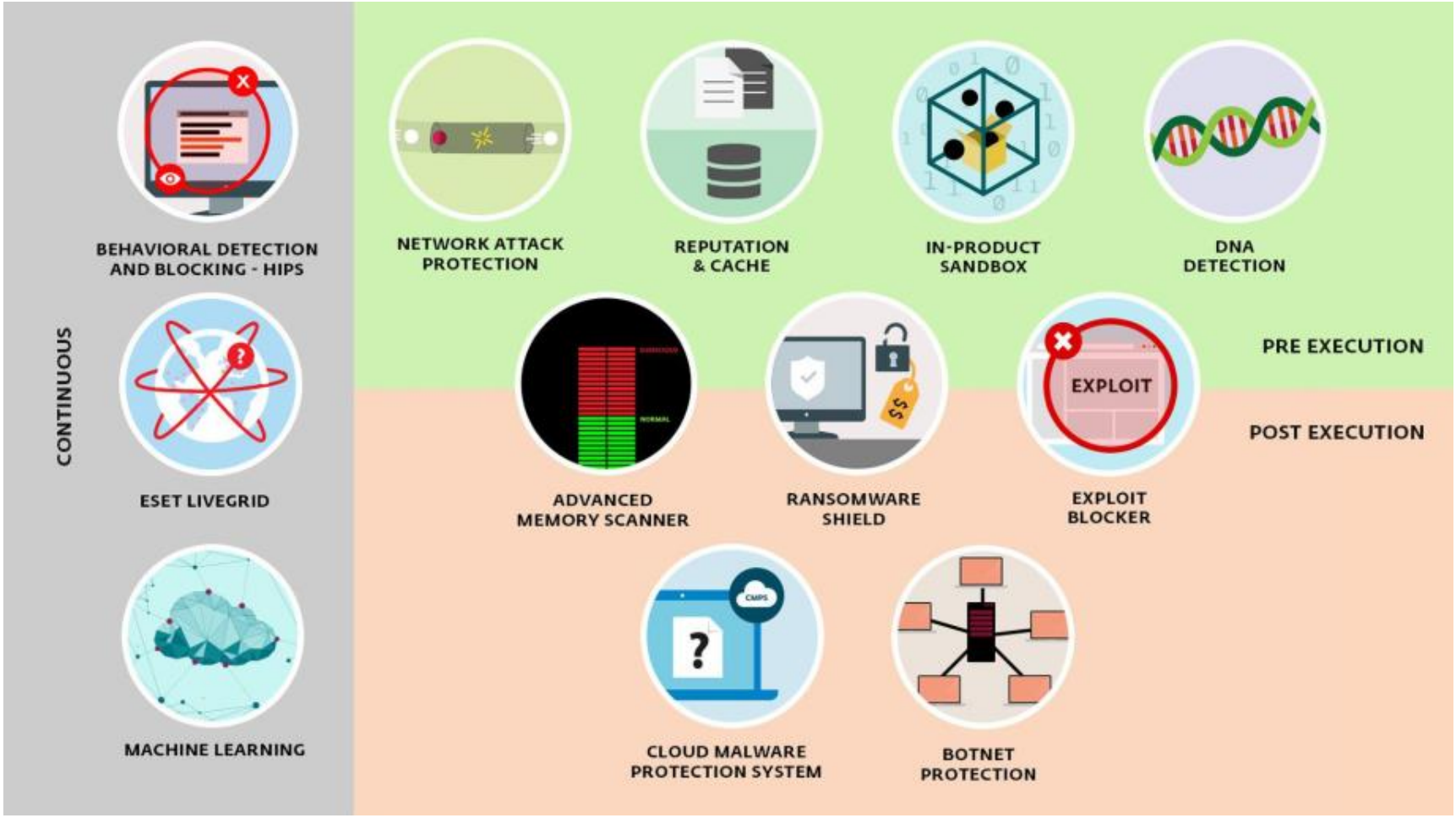
המודולים השונים במוצרי ESET על פי שלבי ההפעלה של נוזקות:

מספקים הגנה מתמשכת
- HIPS
- Live Grid
- Machine Learning

מגינים בטרם הפעלת הנוזקה
- Network Attack Protection
- Reputation & Cache
- In-Product Sandbox
- DNA Detection

מגינים בעת הפעלת הנוזקה
- Ransomware Shield
- Advanced Memory Scanner
- Exploit Blocker

מדינים לאחר הפעלת הנוזקה
- Botnet Protection
- Cloud Malware Protection System



כעת נפרט על שכבות האבטחה:

הגנה מפני התקפות ברשת (Network Attack Protection)

רכיב זו מרחיב את יכולות חומת האש המקומית ומאפשר זיהוי של פירצות אבטחה ברמת התקשורת על ידי סריקת הפרוטוקולים הנפוצים, כגון SMB, RPC ו- RDP. זוהי שכבת אבטחה חשובה כנגד נוזקות המפיצות את עצמן ומתפשטות ברחבי הרשת הארגונית, או כנגד פירצות אבטחה שעדיין לא יצא עבורן עדכון.

במתקפה הנרחבת של נוזקת הכופר WannaCry שהתרחשה ב 12 במאי 2017 נחסמה ההתקפה על ידי חסימת הפירצה בפרוטוקול SMB באמצעות רכיב הגנה זה (הנמצא במוצרי ה Security שלנו), כך שהקוד הזדוני נחסם עוד לפני שהריץ את עצמו.

סרטון הסבר קצר על המודול

מוניטין & מטמון (Reputation & Cache)

כאשר בוחנים אובייקט כגון קובץ או קישור, עוד בטרם מתבצעת הסריקה, המוצרים שלנו בודקים ב- Local Cache (ע"י רכיב ה- *ESET Shared-local cache* שקיים במוצרי ה Endpoint Security שלנו) אחר נוזקות ידועות או לחילופין קבצים שסווגו כנקיים. פעולה זו משפרת את הביצועים על ידי חסכון במשאבי סריקה.

ה-*ESET Live Grid* (מערכת-ענן לדירוג מוניטין קבצים) פונה למאגר הנוזקות שלנו בענן ובודק האם האובייקט כבר נצפה וסווג כזדוני בקרב 100 מיליון המשתמשים שלנו. פירוש הדבר הוא שאנו מסוגלים

להפיץ ולשתף מידע אודות נוזקות בקרב כל המשתמשים שלנו במהירות גבוהה (עד 20 דקות מהרגע ההתפרצות של נוזקה חדשה ולא-מוכרת!).
אובייקטים כגון קישורים נסרקים לבדיקת מוניטין ונבדקים אל מול כתובות זדוניות ידועות, כך שהמשתמשים לא ייכנסו לאתרים מפוקפקים כגון אתרי פישינג שמנסים לגנוב מידע בדרכי מרמה.

אובייקטים כגון קישורים נסרקים לבדיקת מוניטין ונבדקים אל מול כתובות זדוניות ידועות, כך שהמשתמשים לא ייכנסו לאתרים מפוקפקים כגון אתרי פישינג שמנסים לגנוב מידע בדרכי מרמה.

סרטון הסבר קצר על המודול

זיהוי על פי DNA (DNA Detection)

קוד זדוני ניתן לשינוי על ידי האקרים, אך ההתנהגות שלו לא משתנה. הטכנולוגיה של מוצרי אנטי וירוס בסיסיים תוכנתה על מנת לסרוק ולאתר בקוד תבניות זדוניות שמוכרות מהעבר (ומופצות על ידי חתימות), אך התוצאה הייתה שכל שינוי בתבנית או כל שימוש בטכניקות הסוואה, איפשר לנוזקה לחמוק מתחת לרדאר הזיהוי.

ה-זיהוי על-פי DNA אשר קיים במוצרי ESET שונה מהותית. הוא תוכנת לנצל את אותו עקרון (קוד משתנה, התנהגות לא): לכן, המוצרים שלנו מבצעים ניתוח מעמיק של הקוד כדי לגלות את ה"גנים" שאחראים להתנהגות. הניתוח ההתנהגותי של ESET המאפשר לה לייצר זיהוי ע"פ DNA, מסוגל לאתר קוד זדוני גם כשהוא רץ במחשב וגם כשהוא רץ בזכרון. אנו מבחינים בין גנים שונים ומזהים אנומליות: למעשה כל קוד שאינו מאומת, מיד נחשד כזדוני ומאובחן לעומק.

אנו עושים שימוש בתהליך סיווג אוטומטי ומיישמים אלגוריתמים של Machine Learning כדי לזהות לא רק דגימות של נוזקות מוכרות, ואת הוריאנטים שלהן, אלא גם נוזקות שלא נראו מעולם (In-the-wild),

המכילות קוד עם התנהגות זדונית. ובכדי למנוע זיהוי-שווא (False-Positive), אותם גנים של התנהגות שנסרקים על ידי המוצרים שלנו ומשווים אותם לתבניות מוכרות שכבר סווגו כנקיות.

סרטון הסבר קצר על המודול

חוסם פירצות (Exploit Blocker)

זוהי שכבת אבטחה ייחודית ושונה מטכניקות הזיהוי שמתבססות על ניתוח קוד זדוני. בטכנולוגיה שלנו יש מספר יכולות להתגונן מפני פירצות אבטחה במספר רמות: מנוע הסריקה מאתר פירצות ברמת קבצי מסמכים; רכיב ההגנה מפני פירצות רשת חוסם פירצות ברמת התקשורת;
ואילו *חוסם הפירצות* שלנו, **עוצר את התהליך שבאמצעותו מנוצלות הפירצות**. רכיב זה מנטר דרך קבע אפליקציות שבדרך כלל מתגלות בהן פירצות – דפדפנים, קוראי מסמכים, תוכנות לדואר אלקטרוני, Java ועוד – ובמקום להתבסס רק על מה שכבר ידוע (כלומר פירצות מדווחות), הוא סורק תהליכים שרצים במחשב המנסים לנצל את אותן פירצות. כל תהליך כזה מייצר אנומליה בשלב ההרצה שלו ואנו מאתרים את אותן אנומליות, ודרכן מאתרים את הפירצה. כאשר איתרנו תהליך כזה, אנו בוחנים ומנתחים אותו ואם הוא חשוד כתהליך אנו חוסמים אותו במיידי ומעבירים את המידע לענן (ESET Live Grid), במטרה לבחון אותו לעומק ולקשר אותו לאיומים מוכרים. מודיעין זה מאפשר לנו להתמודד ביעילות גבוהה עם איומים לא מוכרים שזה עתה התפרצו (Zero Day Attacks).

סרטון הסבר קצר על המודול

סריקת זכרון-מחשב מתקדמת (Advanced Memory Scanner)

סריקת זכרון-מחשב מתקדמת היא טכנולוגיה ייחודית ל-ESET המציעה פתרון אפקטיבי לבעיה רווחת בעידן הנוזקות המודרני: נוזקות המסוות עצמן או עוברות הצפנה בכדי לחמוק מזיהוי. בעבר, הטכניקות הקבועות לטפל בנוזקות מסוות הייתה להריץ ולבדוק את התנהגותן בתוך סביבה וירטואלית מבודדת (Sandbox), אך אין בכך כל ערבות שבמהלך הבדיקה הנוזקה אכן תחשוף אופיה האמיתי של התנהגותה הזדונית, וזאת משום ש(א) לעיתים הקוד הזדוני כתוב באופן כזה שלא כל תהליכי ההרצה שלו ניתנים לניתוח (ב) לעיתים הקוד כולל תנאי הפעלה (לדוגמא טריגר של זמן מי להריץ את הפעולה הזדונית) שלא ניתן לבצע עליהם מניפולציה. (ג) הנוזקה עצמה מבצע עדכון רכיבים במהלך החיים שלה ולעיתים בעת הסריקה היא כלל לא חושפת שום תוכן זדוני, אך עדכון דרך פירצת אבטחה יכול להפוך את הקוד הקיים, לזדוני.

כנגד כל האפשרויות האלה, קיימת *סריקת זכרון-המחשב המתקדמת* שלנו. היא בודקת את ההתנהגות של תהליך זדוני בזכרון, ברגע שההסוואה יורדת. במצב זו יותר סביר שנוכל לעמוד על טיבו האמיתי של הקוד החשוד, כאשר הוא בתוך הסביבה בה הוא מתוכנן לפעול.

ניתוח חד פעמי לא יכול לעזור לאתר נוזקות ברמת הזכרון, בגלל הפוטנציאל שלהן להשתנות לאורך חייהן. לכן יש צורך בניטור תמידי של התנהגויות חשודות בזכרון המחשב: בכל פעם שתהליך רץ כלשהו פונה למערכת, רכיב ה-*סריקת זכרון-מחשב מתקדמת* מבצע ניתוח התנהגותי של הקוד (בשילוב מנוע הסריקה המבוסס על זיהוי ע"פ DNA).
רכיב זה הונדס בחכמה כדי לא להאט או להשפיע על אף אחד מהתהליכים החשובית שרצים במחשב, מה שגם שהוא סורק לא רק על הזכרון הסטנדרטי אלא גם את קוד .NET MSIL (Microsoft Intermediate Language) שנעשה בו שימוש רב על ידי האקרים במטרה לשבש את פעולת הזיהוי.

סריקת זכרון-המחשב המתקדמת פועלת בשילוב ובתאימות עם *חוסם הפירצות* שלנו, על אף שהיא נכנסת

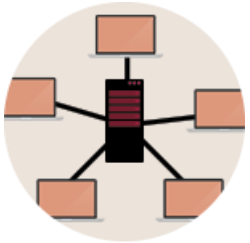
לפעולה רק לאחר שהקוד הזדוני כבר רץ. לכן צריך להבין שמדובר בשכבת אבטחה מאוחרת (מבחינה כרונולוגית) המעניקה רשת בטחון למקרה וההאקר הצליח לעקוף את השכבות האבטחה הקודמות. כמו כן , בטרנד הנוכחי, נוזקות רבות פועלות רק ברמת הזכרון (ידועות גם כ Fileless Malware), מבלי להזדקק לרכיבים ברמת המערכת (אותם פשוט יותר לזהות באופן יחסי). נוזקות מסוג זה מופיעות לרוב על גבי שרתים, בגלל שמדובר במערכות שמוחלפות לעיתים רחוקות ולכן הנוזקה יכולה להמצא בזכרון מבלי שהיא זקוקה לאתחול כדי לשרוד, אך מגמה זו מתרחבת כעת גם לתחום עמודת-הקצה. כך או כך, בזכות שכבת אבטחה זו (ואחרות) משתמשי ESET ערוכים גם לדור הבא של מתקפות חכמות אלה.

סרטון הסבר קצר על המודול

מערכת זיהוי מבוססת-ענן (Cloud Malware protection system)

מערכת הזיהוי מבוססת הענן של ESET היא רק אחת מני כמה טכנולוגיות של ESET המבוססות על ESET Live Grid. קבצים חשודים עם פונטציאל לחולל נזק נשלחים למערכת הענן דרך ה ESET Live Grid הקיים בתחנה או בשרת. אותן דגימות עוברות תהליך סריקה אוטומטי באמצעות ניתוח התנהגותי בשילוב תהליכי אמולציה ("ארגז חול"). יכולת זו היא למעשה Machine Learning שמתקיים בטכנולוגיה שלנו, משום שהיכולת להתמודד עם מאסה אדירה של דגימות חייבת להתבצע על ידי אלגוריתמים חכמים ואוטומטיים. כל משתמשי ESET "מרוויחים" בזכות יכולת עננית זו, משום שה Live Grid כולל מערכת מוניטין שמאפשרת לכל משתמש לגלות בזמן-אפסי האם הקוד החשוד שנתגלה במחשב שלו, זוהה אצל אחד המשתמשים האחרים של ESET (מבין 100 מיליון המשתמשים) – וזאת, כאמור מבלי להיות תלויים בחתימות או בעדכון מנועי הסריקה. זמן האיתור הממוצע מרגע שקוד זדוני מתפרץ אי שם עד הרגע שמערכת הענן של ESET מזהה אותו הוא כ 20 דקות (!) – הרבה לפני שעדכוני החתימות השוטפים מגיעים לכלל המשתמשים. לכן זוהי שכבת אבטחה קריטית בטיפול בהתפרצויות של נוזקות חדשות ולא מוכרות.

סרטון הסבר קצר על המודול



הגנה מפני בוטנט (Botnet Protection)

נוזקה תלויה בין השאר ביכולת של התוקפים לשדר לה פקודות מרחוק: לשם כך מוגדרת בקוד היכולת לתקשר עם שרת הבקרה והשליטה (C&C), שהיא אמנם פרוצדורה יקרה עבור ההאקרים, אך כזו שעדיין לא נמצאה לה אלטרנטיבה זולה יותר. רכיב ה*הגנה מפני בוטנטים* פועל כדי לנטר ולזהות בהצלחה את התקשורת של בוטנטים עם שרת הבקרה והשליטה וגם כדי לאתר את התהליך עצמו שאחראי על התקשורת.
מכאן החשיבות הכפולה של רכיב זה: הוא מאפשר באופן ייחודי לאתר חולשות ברשת או ערכות פריצה קיימות, אשר באמצעותן מתבצעת התקשורת. כמו כן הוא מאפשר לזהות במדויק את התהליכים הזדוניים ולעצור אותם ואף לעיתים מסוימות לעקוף את פעולת ההצפנה של התקשורת עצמה.

סרטון הסבר קצר על המודול

ההתפתחות הכרונולוגית של הטכנולוגיה הרב שכבתית של ESET -

1987
- 30 years ago… NOD was born

1995
- Heuristic Detection
- Behavioral Detection

2002
- Advanced Heuristics

2005
- DNA Detections
- ESET ThreatSense.NET

2007
- Automated detection based on DNA

2011
- Cloud base reputation system – LiveGrid
- Utilizing Machine Learning for DNA detections

2012
- Exploit Blocker
- Network Attack Protection

2013
- CMPS/DNA Hash
- Advanced Memory Scanner

2014
- Botnet Protection
- Shared Local Cache

2015
- Network Detections