אתגר זמינות ואבטחת הרשת בעידן ה-LTE

דוד בכר

הקדמה - מ"גן מוגן" לתוהו ובוהו

התנועה ברשתות המובייל גדלה בקצב מסחרר: המפעילות מדווחות על הכפלת ואף שילוש התנועה ברשת במהלך שנה קלנדרית, בעוד שחברות הסלולר מצביעות על ירידה מתמשכת בממוצע ההכנסות מכל משתמש קצה (ARPU). נתונים אלה מאיצים במפעילים לממש פתרונות אשר יספקו יעילות רשת מקסימאלית תוך הפחתת עלויות מתמשכת - פריסת רשתות LTE.

הגידול בתעבורה אינו האתגר היחיד המדיר שינה מעיני המפעילים: גידול בכמות החיבורים בו-זמנית לרשתות (connection growth) ופרצי בקשות התחברות לרשת מהווים איום אמיתי לזמינות הרשתות.

העלייה בכמות החיבורים בו-זמנית לרשת נובעת ממספר סיבות; הראשונה שבהן היא הגידול בכמות ציודי הקצה החכמים, המריצים אפליקציות הדורשות חיבור קבוע לרשת (always on connection), והעובדה כי לכל משתמש קצה יש יותר ממכשיר סלולרי בודד: טלפון אישי, טאבלט ולעיתים מודם סלולרי. השימוש באפליקציות מכונה למכונה (M2M) גם הוא מגדיל משמעותית את כמות החיבורים לרשת. אשם נוסף ומרכזי ניתן למצוא באפליקציות החינם - חיבור לשרתי פרסומות מתחלפות היוצרים עומס חיבורים על הרשתות.

התמודדות עם השלכות גידול התעבורה ברשת מהווה רק חלק מהאתגר העומד בפני המפעילים. קישור קבוע לרשת הסלולרית, גישה רחבת סרט וציוד קצה המאובזר בכוח עיבוד מאסיבי - כל אלה מזמנים אתגר חדש: אבטחת הרשת. עד היום מרכיבי ליבת הרשת של המפעיל היו חשופים להתקפות זדוניות מהאינטרנט. כיום, עם שינוי "סביבת העבודה", הם חשופים גם להתקפות מצד משתמשי הקצה.

יתרה מזו, איפיון רשתות LTE כרשתות תקשורת שטוחות מבוססות IP, היכולת האינהרנטית להתממשק לרשתות גישה שונות, שימוש באתרי רדיו ביתיים FEMTO (הידועים בקלות הפריצה אליהם), ריבוי התוכנות הזדוניות הניתנות להתקנה בקלות על ציודי קצה חכמים והעדר תקינת אבטחת מידע ברשת - הופכים את רשתות ה- LTE לפגיעות יותר ויותר.

איומים מתוחכמים דורשים אבטחת רשת יצירתית

שוק ציודי הקצה החכמים הפך לשוק המוביל את תרבות הצריכה בעולם. בהתאם לתחזיות informa, מספר ציודי הקצה החכמים יגיע לכ-870 מיליון עד שנת 2016. שוק האפליקציות גדל גם הוא, וכבר היום צרכנים מבלים יותר זמן בשימוש באפליקציות מאשר בגלישה רגילה ברחבי האינטרנט.

תוכנות זדוניות כגון malware ו-Bot "מתלבשות" כיום על מספר עצום של אפליקציות המותקנות בציוד הקצה של המשתמש, ושמות להן למטרה לפגוע במספר יעדים:

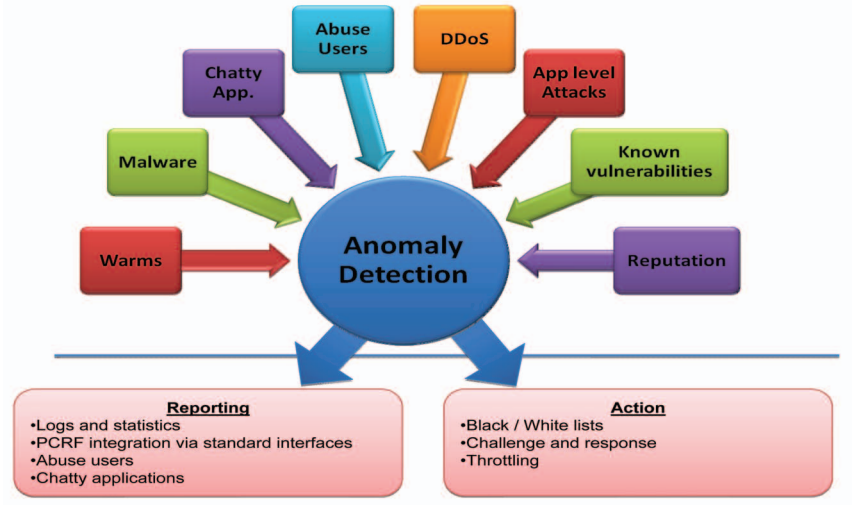
- המשתמשים: גניבת זהות (גישה לספר הטלפונים, פריצת חשבונות אימייל ומדיה חברתית), איכון לקוחות, ריקון סוללה, שימוש וגבייה יתר בחשבון ה-data של הלקוח ועוד.
- המפעילים: התקפות DDoS, התקפות שירותי רשת קריטיים כגון שרתי DNS, התקפות אפליקציות שירותי ערך מוסף והתקפות הפוגעות בציוד הליבה והרדיו של הרשת.
- אתרי אינטרנט: ציודי קצה המחומשים בכוח עיבוד חזק, רשת גישה רחבה ואפליקציות התקפה ייעודיות (כדוגמת mobile LOIC) יכולים בקלות לפגוע באתר תוכן בעוצמה הזהה לכל מחשב PC המחובר לרשת גישה קווית.

אבטחת הרשתות הופכת למסובכת ומצריכה חשיבה יצירתית על דרכים להגן על משאבי הרשת היקרים. יש צורך במנוע אבטחה אשר ידע לזהות התנהגות רשת חריגה (אנומליה).

מוצרי האבטחה של רדוור מצויידים במנוע fuzzy logic המתחשב בגורמים משתנים כמו זמן והסתברות, ויכולים לזהות שינוי קיצוני בהתנהגות צרכנים ורשת להתריע ולחסום תנועה זדונית שעלולה להעמיס את רשת המפעיל ואף לגרום לקריסתה המוחלטת.

מערכת האבטחה של רדוור AMS - Attack Mitigation System, בודקת ונותנת ציון לכל חיבור רשת. הציון מצביע עד כמה החיבור הרגעי חשוד כהתקפה על סמך אנליזה עמוקה של כלל שכבות התנועה, מרמת החיבור הפיזי ועד לרמת האפליקציה.

מערכת האבטחה משווה את נתוני הרשת לנתונים סטטיסטיים היסטוריים ומנסה לזהות האם ישנה התנהגות רגעית החשודה כהתקפה. איסוף המידע ההיסטורי וקביעת ספי ההתקפה מתחשבים במספר רב של משתנים, כגון: מספר ממוצע של חיבורי רשת ללקוח, גישה בו-זמנית ליעדים שונים ופורטים ברשת, מספר ממוצע של חיבורי רשת פר אפליקציה (קיימות אפליקציות שתוכננו לייצר מספר רב של חיבורי רשת), סטטיסטיקות ברמת ציודי הקצה השונים, משך זמן ממוצע של חיבור רשת, ממוצע שגיאות התחברות למשתמש ועוד.

ניראות הרשת הנה מעלה נוספת במערכת האבטחה של רדוור. היכולת לדווח בזמן אמת על התנהגות אנומלית ברשת ולהתממשק למערכות ניהול חיצוניות מסייעות למפעיל להגן על משאבי הרשת היקרים שלו כנגד התקפות עומס, ירידה בחוויית המשתמש של לקוחותיו, מניעת מצבי Billing shocks בהם הלקוח נדרש לשלם על תנועת data שלא ביצע במתכוון, ובעיקר למנוע פגיעה בשמו הטוב ובמוניטין של המפעיל.

למידע נוסף בקרו באתר רדוור
www.radware.com