



אבי צ'סלה

אם התוקפים נכשלים במלאכתם והמתקפה לא צולחת, הם מגבירים את חומרת המתקפה או משנים את הסוג שלה. במקרים מתקדמים של ההתקפות, צוות ה-ERT שלנו נדרש בזמן אמת ליצור הגנות חדשות ולעדכן את תצורת ה-AMS בהתאם - הצוות מתאמן ונבחן על הצלחתו במשימות אלו.

הלהיט: מתקפת נגד

"ייחודו של צוות התמיכה ERT, אמר צ'סלה, הוא ביכולתו לא רק לעצור את המתקפה, אלא גם לבצע מתקפת נגד, תחום בו יש לרדוור פטנטים רשומים. אנשי הצוות מתבוננים על התוקפים, מזהים את הכלים ושיטות ההתקפה, מנתחים את חולשותיהם ומתקיפים בחזרה בהתאם." "כך לדוגמה", הוא אומר, "כאשר נחסם במהלך תקיפה, הפעולה הטבעית לעשותה היא לחסום, או לסגור, את החיבור שלו (connection). במקרה כזה, התוקף יוצר חיבור חדש. במסגרת הפעילות של מתקפת הנגד, אנשי צוות ה-ERT עשויים לשקול ולבחור להשאיר את החיבור פתוח, ולגרום לתוקף לפתוח עוד ועוד חיבורים, על מנת לבזבז את משאבי המיחשוב שלו, מבלי שאנשי רדוור והארגון המותקף מבזבזים את משאבי המיחשוב שלהם".

"כך", מספר צ'סלה, "לרדוור היה לקוח ארגוני גדול הפועל בעולם המסחר המקוון. חברת אנונימוס התקיפה את מערך המיחשוב שלו במשך שבוע". "יישמנו את תהליך מתקפת הנגד", הוא מספר, "צוות התמיכה ERT של רדוור עקב אחר התוקפים בחדרי הצטיים שלהם והבחין כי הם מתלוננים על כך שהמחשבים שלהם עובדים באופן אטי ולעתים אף קורסים. משאבי הזיכרון והעיבוד של המחשבים שלהם הלכו וכלו, עד שבוע לאחר המתקפה הם התייאשו ועברו לתקוף אתר אחר". הוא מסכם כי "זוהי עדות חשובה להצלחת התפיסה של מתקפת הנגד".

"לרדוור", אמר צ'סלה, "יש גוף תמיכה נגד מתקפות סייבר, אנשיו מתמחים בפעילות תמיכה ERT (Emergency Response Team). בזמן אמת באנשי אבטחת המידע של הארגון המותקף הם מוודאים כי המערכות הותקנו עם התצורה המתאימה, ומחכים למתקפה". "עם בואה של המתקפה", הוא אומר, "המערכות שלנו מתחילות להגן באופן אוטומטי מפניה. במקביל, נפתח 'חדר מלחמה', שבמסגרתו אנשי רדוור מתחברים למערכות ה-IT של הלקוח הארגוני המותקף. הם מוודאים כי המערכת של רדוור חוסמת את ההתקפות בצורה יעילה, והם מנתחים ומזהים את הסוגים השונים של המתקפות. פעילות נוספת הנעשית אף היא במקביל, היא ברמה המודיעינית. אנשי רדוור נכנסים לפורומים ולצ'טים של האקרים, מנסים לגלות את זהותם ולברר מהי הפעולה המתקפתית הבאה שבכוונתם לערוך, או מיהו יעד המתקפה הבא. פעילות מודיעינית זו מטרתה להשיג מידע בזמן אמת ולהקדים מבחינת לוחות זמנים את התוקפים".

על פי צ'סלה, "ברוב ההתקפות,

"עם בואה של המתקפה המערכות שלנו מתחילות להגן באופן אוטומטי מפניה. במקביל נפתח 'חדר מלחמה' שבמסגרתו אנשי רדוור מתחברים למערכות ה-IT של הלקוח הארגוני המותקף"