

מתקפת הנגד בהאקטיביסטים

אבי צ'סלה, CTO רדוור, מסביר לאנשים ומחשבים את החשיבות של הגנה על רשתות התקשורת הארגוניות גם במהלך מתקפה, ולא רק לפני ואחרי ♦ צ'סלה שולף את הנשק הסודי שלו: מתקפת נגד בהאקטיביסטים ♦ לידיעת הקוראים חברי אנונימוס ודומיהם

יוסי הטוני

מתקפת מניעת שירות מבוזרת. התוקפים הפילו את אתר החברה למשך יומיים שלושה, ובדיעבד, לאחר כמה ימים התברר כי הפלת האתר הייתה פעילות הסחה, שנועדה להסתיר את העובדה שבעצם הם גונבים מידע מבסיס הנתונים של החברה המותקפת.

"מדובר בפעולת הסחה קלאסית", אמר צ'סלה, "מנהלי הזו היו עסוקים בהחזרת השרתים לפעילות ולא שמו לב לכך שהתוקפים גונבים מידע בזמן זה. מנהלי המידע בארגונים אינם ערוכים לסוג כזה של מתקפות. בכלל יש ריבוי מתקפות, ובתוך שלל המתקפות, קל יותר לבצע את פעילות ההסחה לטובת גניבת מידע, כי מנהלי התשתיות, מנהלי התקשורת, ומנהלי אבטחת המידע טרודים בעלייה חזרה לאוויר." "מערכי ההגנה בארגונים", הסביר צ'סלה, "בנויים בצורה כזו שיש להם טכנולוגיות הגנה שונות לטובת סוגים שונים של איומים. פעמים רבות אין סינכרון טוב בין מוצרי האבטחה השונים, דבר היוצר פערים ביניהם ופוגע בצורך ליצור מעטפת הגנה מוכללת."

פעילות תוך כדי המתקפה

"ככלל", אמר צ'סלה, "ארגונים משקיעים בשני מקומות: האחד, היערכות בטרם מתקפה - ניטור, בקרה, מציאת חולשות, ועל בסיסן בניית מנגנוני הגנה פנימיים. המקום השני בעולם האבטחה שארגונים משקיעים בו הוא לאחר המתקפה. אז הם יודעים לערוך ניתוח פורנוזי, ומפיקים בעקבותיו לקחים ונערכים לקראת המתקפה הבאה."

"הבעיה המרכזית של ארגונים", אמר צ'סלה, "היא שהם אינם ערוכים לפעול בזמן אמת, בעת שהמתקפה מתרחשת, אין להם את הניסיון הדרוש לפעילות בזמן זה. נדרש להם צוות של אנשים עם טכנולוגיות מתאימות, על מנת לנתח את ההתקפה, להגן מפניה באופן אוטומטי, וליצור התקפות נגד מתאימות בזמן אמת. כיוון שהמתקפה המבוצעת

ארגונים אינם ערוכים למלחמה מול ההאקטיביסטים (שילוב המילים האקרים ואקטיביסטים, פעילים חברתיים). מדי חודש יש כמה וכמה מתקפות כאלה. רדוור היא החברה היחידה המציעה פתרון מלא לטיפול בנושא זה, המבוסס על טכנולוגיה בשילוב מתודולוגיה", כך אומר **אבי צ'סלה**, CTO רדוור, בראיון מיוחד לאנשים ומחשבים.

לדבריו, "בשנתיים האחרונות היינו עדים ליותר מדי מקרים שבהם חברות ענק, דוגמת לוקהיד-מרטין, סוני, RSA, הבורסה לניירות ערך בניו-יורק ואחרות, הותקפו, נפרצו, נגנב מהם מידע והאתרים שלהן הופלו".

צ'סלה שימש כ-CTO ב-VSecure, חברת סטארט-אפ בעולם אבטחת המידע, שעסקה בחיפוש וניתוח דפוסי התנהגות של רשתות בוט המשתלטות על מחשבים ותוקפות שירותים. ב-2005 רכשה רדוור את VSecure, ועל בסיסה הרחיבה את פעילותה בעולם אבטחת רשתות תקשורת.

לדבריו, "ההאקטיביסטים תוקפים כיום בצורה חדשה יחסית: הם מנתחים את ארגון היעד אותו הם מתכננים לתקוף, בדרך כלל הם גם מבצעים 'ניסוי-כלים', ואז תוקפים כמה נקודות ברשת, באופן בו-זמני, בשיטה המכונה Multi-vector Attack, התקפות הנמשכות בדרך כלל יומיים-שלושה בממוצע. המתקפות מבוצעות בשיטות שונות ומטרתן משולשת - הפלת האתר, השחתתו וגניבת מידע. ההאקטיביסטים תוקפים שוב ושוב, במגוון אופנים, עד שהם מצליחים להגיע לאחת משכבות המיחשוב הארגוני ומשם חודרים הלאה, פנימה."

מתקפה לצורך הסחה

לדברי צ'סלה, מרכיב מפתח בעת המתקפות הוא פעולת ההסחה. כך, הסביר, במקרה המתקפה על סוני פלייסטיישן, היא החלה כ-DDoS,

