דו"ח מעבדה - תרחיש מס' 2

# פרטים:

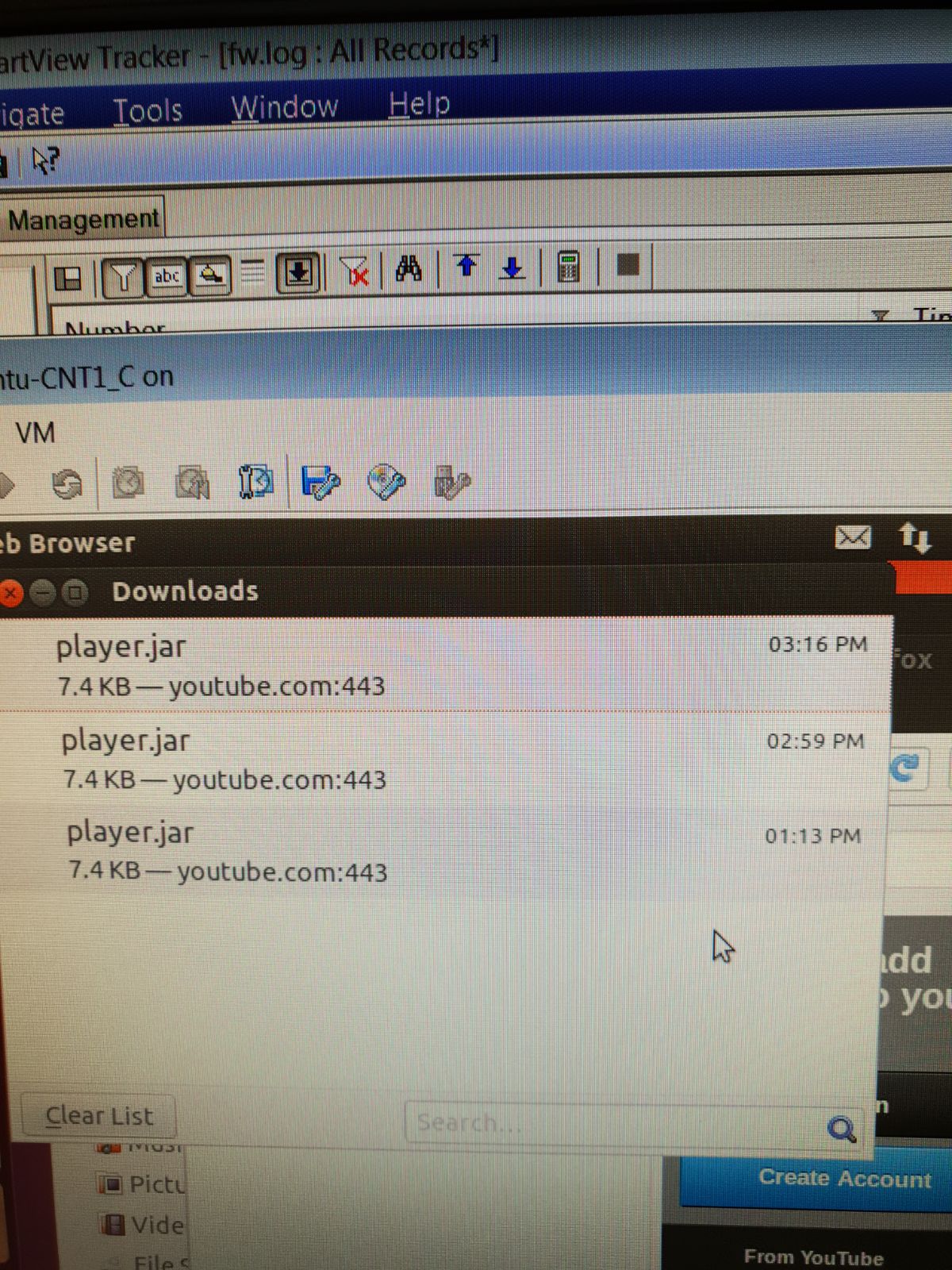
מגיש: דביר ברזילי

תאריך: 22.4.2018

שם התרחיש: חדירה לחברה מתחנת קצה

# תהליך ההתקפה:

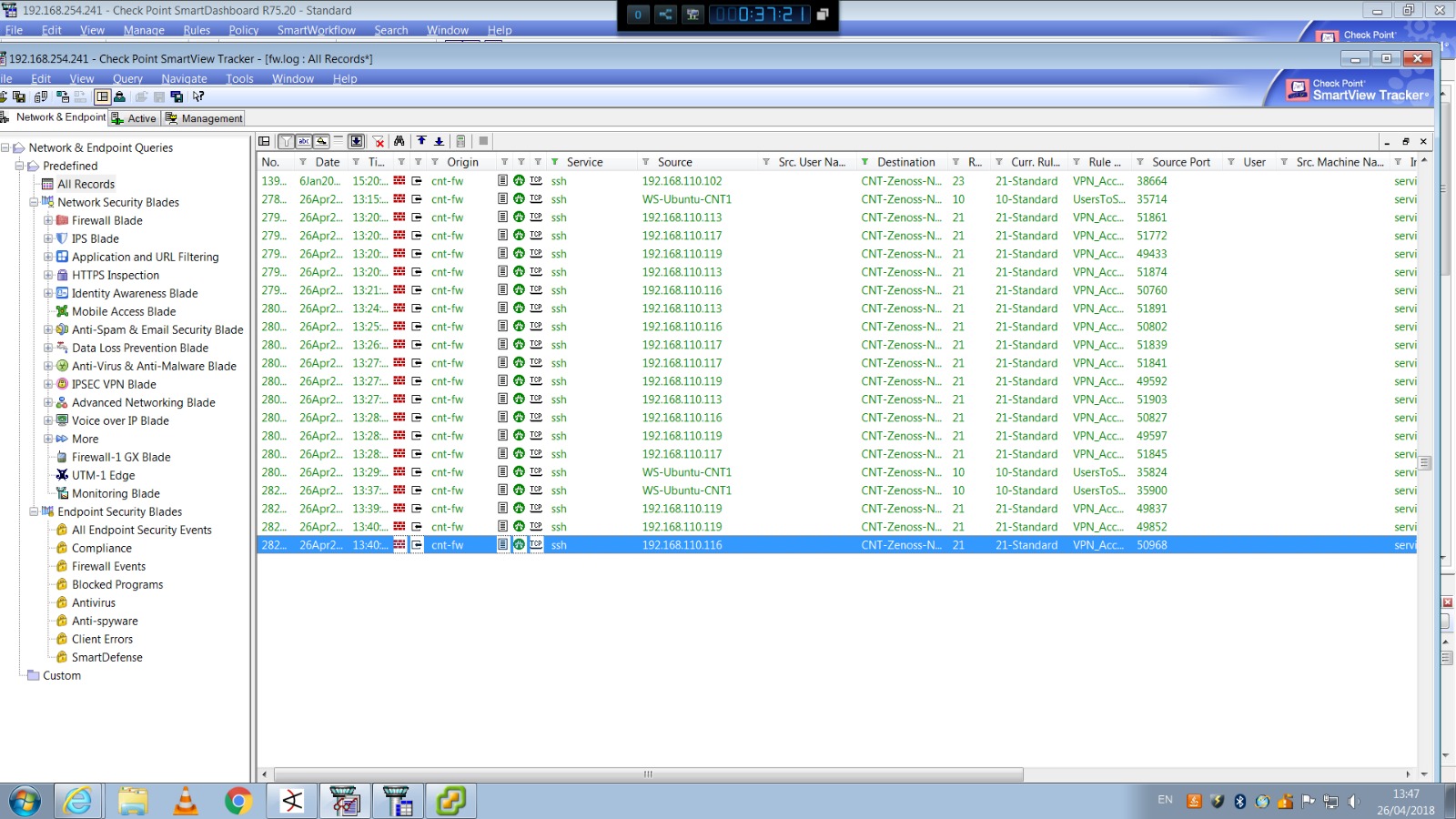
עובד בחברה הוריד לתחנת הקצה שלו קובץ player.jar מתוך האתר youtube. הקובץ הכיל נוזקה שהפילה את שרתי החברה. בנוסף, ע"מ להקשות עלינו באיתור הנוזקה בתחנת הקצה התוקף שיבש תאריכים ובכך גרם לנו לסווג קבצים כלא רלוונטים לתחקיר.



הורדו קבצים חשודים לתחנת הקצה

# תהליך הזיהוי:

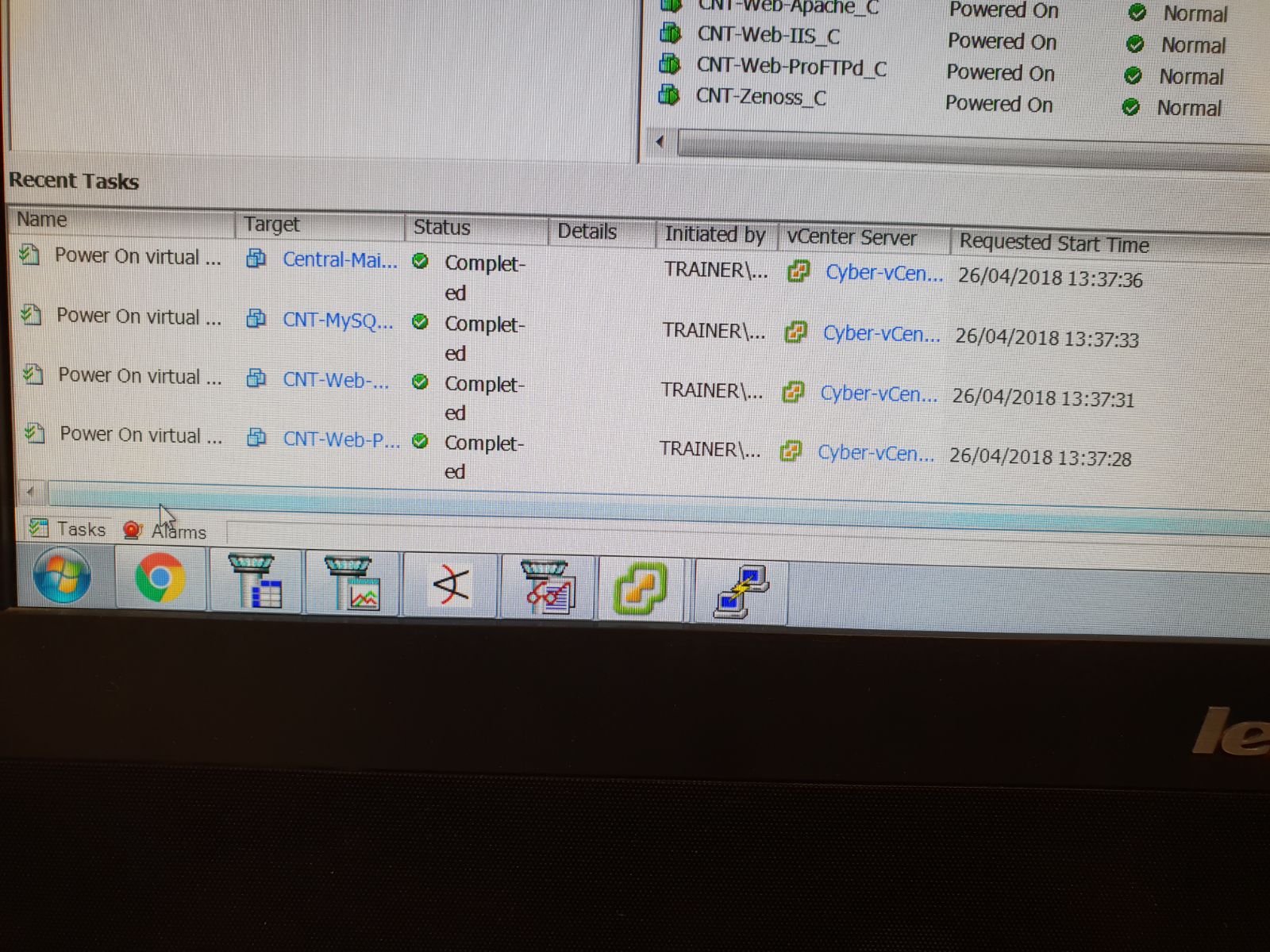
שמנו לב ששרת ה-Zenoss נפל. השתמשנו בכלי VMware כדי להרים את השרת חזרה, ומייד ראינו בו שיש עוד הרבה שרתים שנפלו. התחלנו לחקור את התחנות ומצאנו ב-SmartView Tracker שתחנת קצה מבצעת תקשורת חשודה עם השרתים וכנראה היא זו שגורמת לנפילת השרתים. חיפשנו בתחנת הקצה את הנוזקה שמפילה את השרתים. מצאנו בדפדפן שהמשתמש הוריד קובץ player.jar מיוטיוב שהכילה תקייה עם שמות של קבצים חשודים (כמו metasploit). אכן התברר שזו הייתה הנוזקה.



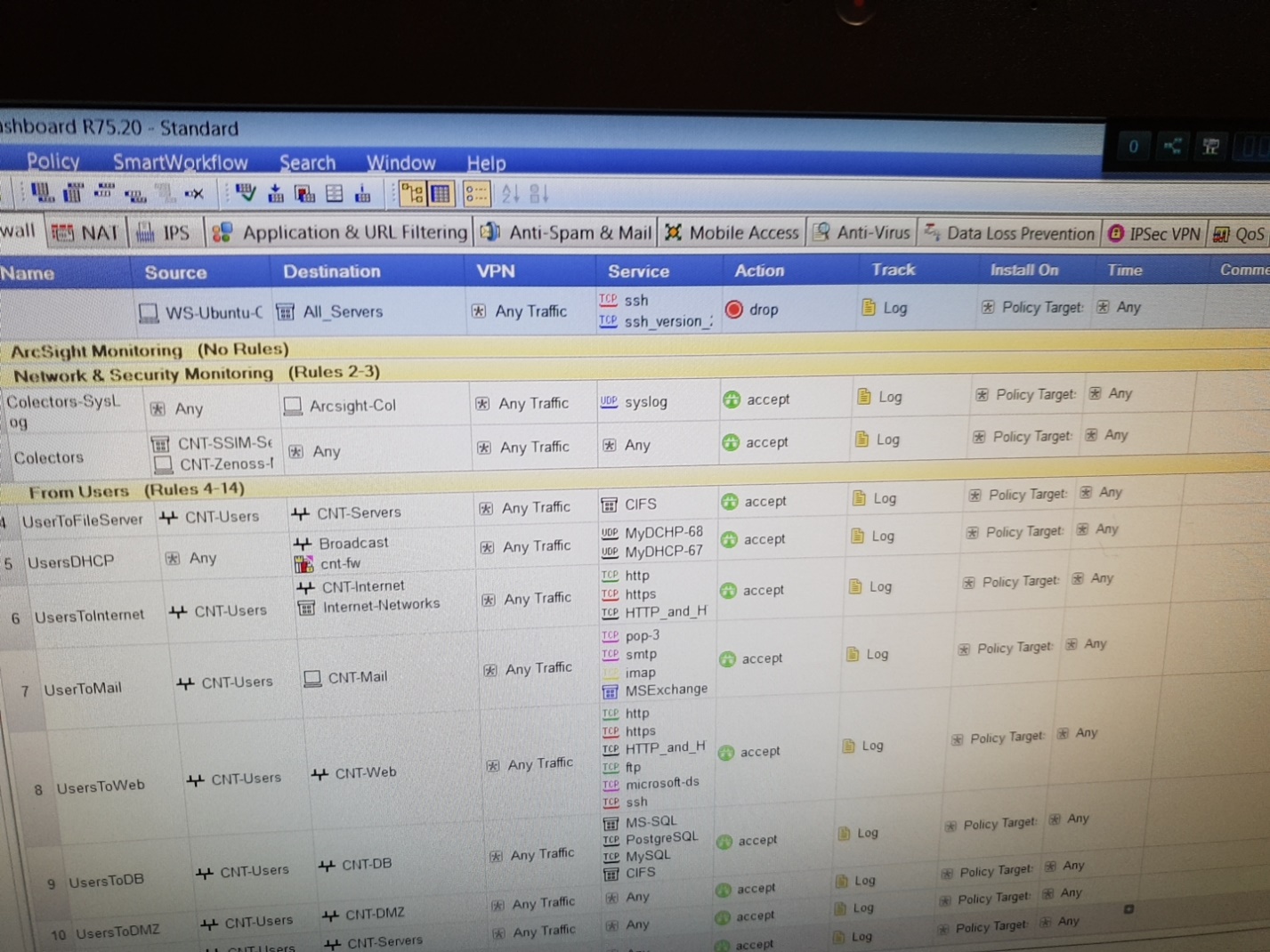
תחנת הקצה מתקשרת עם השרתים ברשת

# תהליך הגנה:

לאחר שזיהינו שהשרתים נפלו ניסינו להרים אותם חזרה, אולם הם נפלו כל פעם מחדש. כשהבנו בעזרת המעקב על התקשורת ברשת דרך ה-FireWall שתחנת הקצה היא זו שמפילה את השרתים חסמנו את התקשורת של התחנה עם הרשת. השרתים הפסיקו ליפול וכך אושר לנו שאכן זו הייתה התחנה הבעייתית. כך יכלנו לתחקר את תחנת הקצה ולבדוק אותה offline. בנוסף שינינו את הסיסמאות לשרתים להגנה נוספת.



מרימים את השרתים



חוסמים תקשורת של תחנת הקצה עם מחשבי הרשת

# תהליך הגנה מונעת:

* שינוי סיסמאות לשרתים לסיסמאות חזקות יותר.
* סגירת פורט 22.
* ניהול חוקים ב-FireWall כך שתחנות קצה לא יוכלו לגשת חופשי לשרתים.
* התקנת תוכנת אנטי וירוס על המחשבים.

# הפרצות באבטחת הארגון

סיסמאות חלשות. גישה לשרתי הארגון דרך תחנות קצה ללא צורך. המחשבים לא מוגנים ע"י תוכנות אנטי וירוס ולכן חשופים לתקיפות סייבר.

# אופן עבודת הצוות

תחילה חילקנו ביננו משימות ע"מ להיות יעילים ולהשגיח על החברה דרך הכלים השונים. כשהתחיל התרחיש היה מי שאחראי על הרמת השרתים והיה מי שאחראי לנסות לזהות את הבעייה. כשהיה חשד לבעייה כלשהי ניסינו לנטרל את המשך פעילותה. לאחר שחסמנו את התקשורת של תחנת הקצה עם הרשת נרתמנו כולנו לאיתור הנוזקה בתחנת הקצה.

# חוסרים/קשיים

היה קושי באיתור הנוזקה במחשב הקצה. איתור הנוזקה דרש זמן רב של חיפוש ועיון בקבצים השונים של משתמשים שונים בתחנת הקצה.