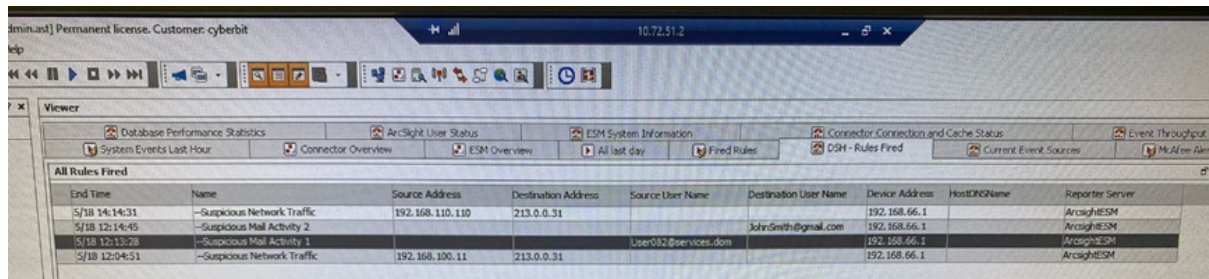


5/18 בשעה 12:13 אחד ממשתמשי הרשת שלנו 192.168.100.11 ניסה להיכנס לכתובת 213.0.0.31

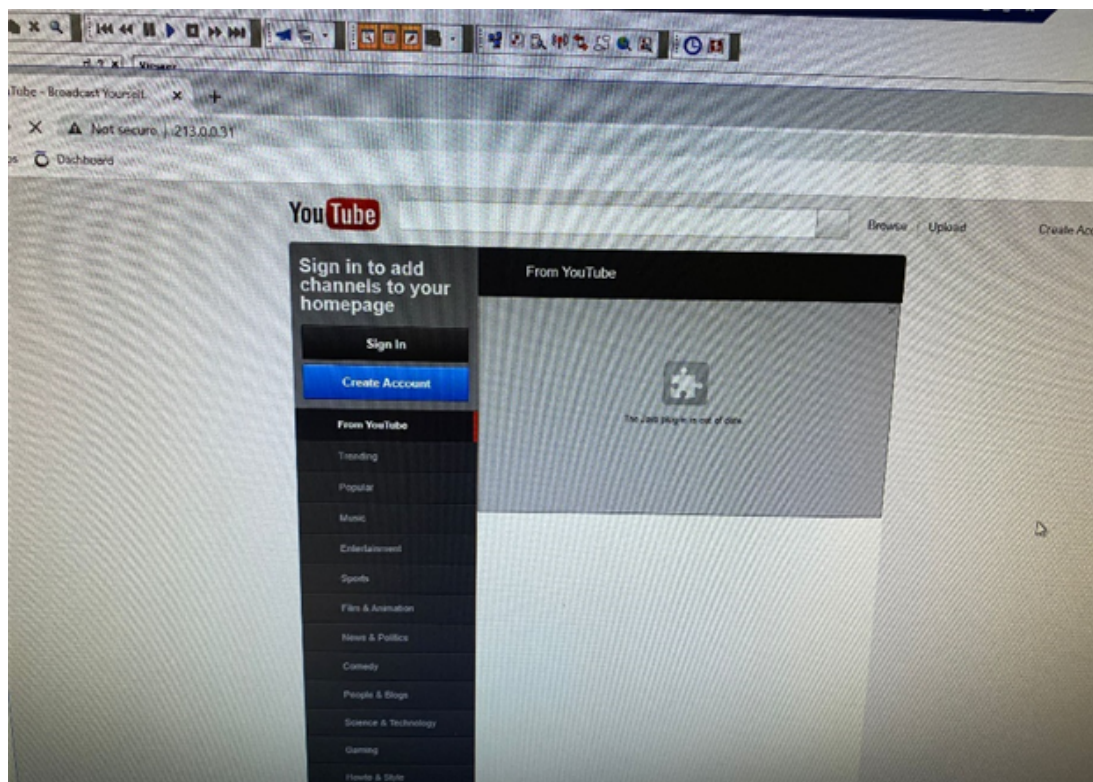


The screenshot shows the ArcSight console interface. At the top, there's a navigation bar with various tabs like 'Database Performance Statistics', 'ArcSight User Status', 'ESM System Information', etc. Below this, a table titled 'All Rules Fired' displays the following data:

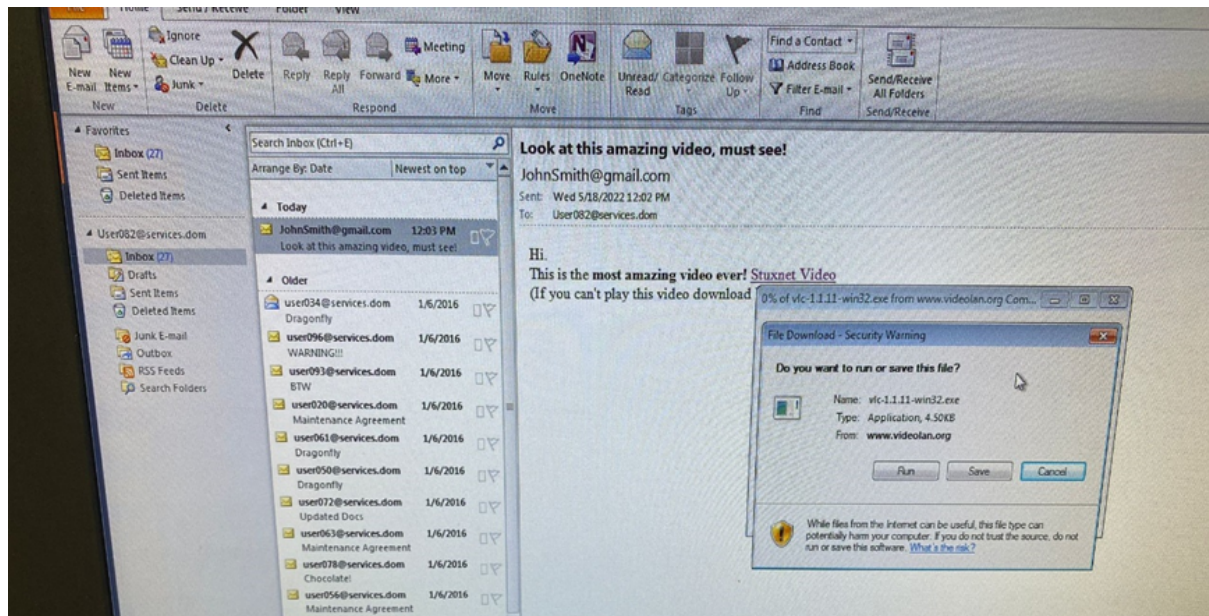
End Time	Name	Source Address	Destination Address	Source User Name	Destination User Name	Device Address	Host/DNS Name	Reporter Server
5/18 14:14:31	-Suspicious Network Traffic	192.168.110.110	213.0.0.31			192.168.66.1		ArcsightESM
5/18 12:14:45	-Suspicious Mail Activity 2				JohnSmith@gmail.com	192.168.66.1		ArcsightESM
5/18 12:13:28	-Suspicious Mail Activity 1			User082@services.dom		192.168.66.1		ArcsightESM
5/18 12:04:51	-Suspicious Network Traffic	192.168.100.11	213.0.0.31			192.168.66.1		ArcsightESM



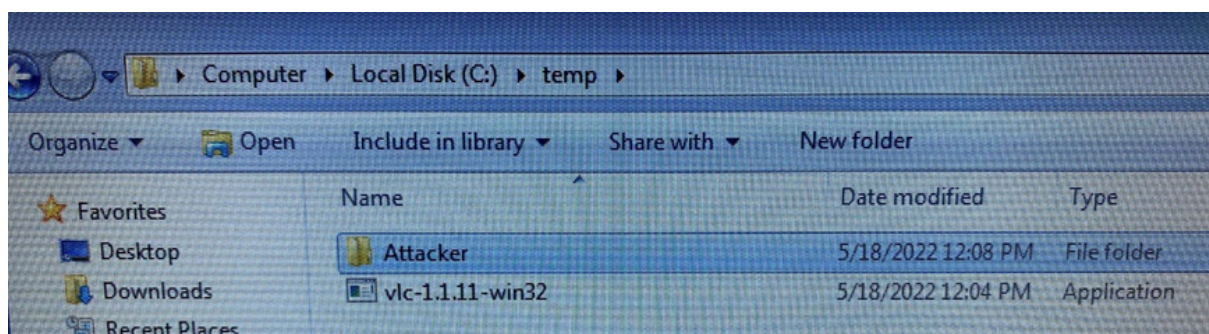
הלכנו לכתובת 213.0.0.31 דרך הדפדפן. היה אתר שנראה כמו אתר יוטיוב, אבל לא היה לו חיבור מאובטח ולא היה DNS של יוטיוב



נכנסנו למחשב של user082.
 היה לו מכתב בתיבת הדואר שלו מאיש מסוים JohnSmits@gmail.com.
 האימייל הזה כלל קישור לסרטון וקישור נוסף לנגן וידאו.



בקבצים זמניים בתיקיית Temp, מצאנו את קובץ ההתקנה של הנגן ואת תיקיית ה-
 Attacker



נכנסנו לתיקיית Attacker, מצאנו את הקובץ SendFile.vbe
 הקובץ הזה הכיל סקריפט ששלח מידע מהמחשב שלנו

לאחר מכן מחקנו את כל הקבצים ש-user082 הוריד והרץ

כיצד להגן על עצמך מפני סוסים טרויאנים
נוכחות של חבילת אנטי וירוס איכותית על המחשב.

מערכת ההפעלה צריכה להיות מעודכנת כל הזמן.

עליך להשתמש רק במשאבי אינטרנט מהימנים. אתה צריך להיות זהיר בעת לחיצה
על קישורים ובאנרים שונים, שנמצאים במספרים עצומים באינטרנט המודרני. אם
קישור או באנר נראים חשודים, אז עדיף לא ללחוץ עליהם.
עליך להשתמש בסיסמאות מאובטחות. סיסמאות לא צריכות להיות קלות לניחוש
ואיכשהו להיות משויכות לבעלים של חשבון. אין לאחסן סיסמאות במקום אחד, וגם לא
להיות זהות. כמו כן, רצוי "להכניס סיסמא" לחשבון המנהל.