דוח אירוע - 4

מגיש: עוז מעתוק 305181158

שם התרחיש: Trojan Data Leakage

תהליך התקפה: התקפה מסוג זה בנוייה בכדי לפגוע ברשתי ה Mail של ברשת שלנו. פעולתו הראשונה של התוקף התבצעה מתוך הרשת שלנו ע"י משתמשים פנימיים שכנראה נדבקו בתוכנה זדונית בזמן עבודתם.ההדבקה התבצעה באמצעות הודעות דוא"ל שיקריות עם קישורים לאתרים אשר בכניסתם המשתמש נדבק (כמו קישור להורדת תוכנה לניגון ווידאו). ההתקפה בוצעה על שרת הדוא"ל שלנו 213.0.0.46 זאת בכדי להפיץ את ההתקפה ע"י שירותי דוא"ל פנימיים של הרשת. לאחר הדבקת המשתמשים וניסיון הגישה לשרת הדוא"ל התחילו להישלח בצורה אוטומטים מיילים ברחבי הרשת (ללא ספציפיות במשתמש היעד) בעלי תוכן זדוני שהתבטא בקובץ PDF הכיל תוכנה זדונית מסוג הסוס הטרויאני אשר מדליף בצורה אוטומטים מידע / קבצים מתוך המשתמש הספציפי בעזרת הודעות דוא"ל.

תהליך הזיהוי: תחילה העמדנות תצפית בכל כלי שיכולנו, כאשר הכלים האפקטיבים היו ה – ArcSight, CheckPoint Dashboard, וה – Zenoss. הסיבה לכך שדווקא כלים אלו היו רלוונטים לתרחיש היא מפני שה ArcSight מאפשר לנו לזהות תרחישים שאינם עומדים בחוקיות המוטמעת במערכת, CheckPoint Dashboard מנטרת את תעבורת הרשמת ומתייגת מקרים לפעולות רשת מוכרות, וה – Zenoss עוקבת אחר תהליכים ושרותים אשר נמצאים בכלל הרשת. הפעולה החריגה הראשונה לה שמנו לב במערכת הייתה על תוכנת ה ArcSight, אשר הציגה לנו התראה על תעבורת רשת חשודה בתוך הרשת עצמה, ז"א ממשתמש קיים ברשת שלנו אל שרת כתובת שרת הדוא"ל. לאחר זמן קצר קפצה התרעה נוספת על שליחת דוא"ל חשוד בתוכנת CheckPoint Dashboard Tracker כאשר מצויינת כתובת הדוא"ל אשר פעלה ועברה על החוק (user082). בהמשך לשתי מקרים אלו נכנסו לקבצי הלוג של שירותי הדוא"ל על השרת ה Mail הנתקף, ובעזרת המידע שסופק לנו מתוכנת ה Tracker פנינו לתיקיית ההודעות של user082. שם ראינו את קובץ הלוג של הודעות הדוא"ל עבור המשתמש הספציפי, כאשר ניתן היה בקלות להבחין בהודעות דוא"ל שאינן שיגרתיות וחשודות ממשתמשים פנימיים ובדגש ממשתמש בשם john smith. בכדי לברר פרטים נוספים אודות התקיפה נכנסנו אל user082 אשר רץ על גבי מערכת הפעלה Windows 7, זאת נעשה ע"י תוכנת VMWare vSphare שאיפשרה לנו בממשק נוח לשלוט על המשתמש מרחוק. מתוך המשתמש user082 נכנסו לתוכנת הדוא"ל outlock וללא הפתעה ראינו את שלל הודעות הדוא"ל ע"פ קובץ הלוג שהוזכר לעילת כאשר מתוך ה outlock היה לנו הרבה יותר קל להבין את משמעות הודעות הדוא"ל אשר user082 נקשר אליהם. מבדיקת ההודעות היוצאות התגלו לנו הודעות דוא"ל אל אותו john smith בעלות גבצים מסווגים שמיקומם במערכת היה בכונן המשתמש תחת C:\\CIA. בשלב הזה היה ברצננו לפענח את משמעות הקבצים אשר עברו בדוא"ל של המשתמש אל john, לשם כך השתמשנו במגוון תוכנות כמו PEID, exeEditor, subLine ועוד בכדי לנסות להבין את משמשעות הקוד / הסקריפט אשר עובר בהודעות הדוא"ל, אך ללא הצלחה בנושא. בעקבות ההכוונה למיקום C:\\CIA גילינו בכונן הנ"ל את התיקייה \tmp\Attacker ובה נמצא סקריפט VB (דווקא VB מפני שזאת השפה הנגישה לעבודה מול Microsoft OutLock) אשר מבצע

את שליחת הדוא"ל האוטומטית מתוך user082. הגענו למסקנה כי ההתקפה כיוונה להזליג מידע בצורה אוטומטית מתוך המשתמשים ברשת, ובנוסף להדביק כמה שיותר משתמשים בפגיעה זו.

<u>תהליך ההגנה ראשוני:</u> כתגובה הראשנית להתקפה זו הזנו חסימה לכתובתו של הפורץ ע"י הגדרת חוק מתאים בחומת האש של הרשת ע"י תוכנת ה Dashboard של Checkpoint. בהמשך לחסימת התוקף, הגדרנו חסימה בתוכנת ה OutLock על קבלה ושליחה של הודעות דוא"ל לגבי המשתמש החשוד John Smith, זה נעשה ע"י עריכת קבתי ההרשאות בשרת הדוא"ל של הרשת.

<u>תהליך הגנה מונעת:</u>

- כמו שצויין בתהליך ההגנה הראשוני, חסימת כתובת ה IP של התוקף, וחסימת כתובת הדוא"ל שלו עבור קבלת ושליחת הודעות הן פעולות הגנה מונעות אשר מגינות עלינו מפני התקפות נוספות מצד התוקף הספציפי.
- מפני שההתקפה התנהלה בעיקר בתוך הרשת שלנו, מהלך נכון הוא הפעלת תוכנת אנטיווירוס + אנטיספאם על המשתמשים.
- מרגישות נושא הודעות הדוא"ל והגישה הישירה שלהם לשרת / למשתמש, יש לבצע סינון רחב יותר עבור הודעות חשודות ואפילו לעדכן הגבלה דרך השרת ותוכנת ה outlock על חסימת מוחלטת של הודעות חשודות, או לפחות חסימה אוטומטית עד לאישור ידני.
- איסוף מאפייני ההתקפה והזנתם בתוכנות המעקב שלנו (Tracker / DashBoard) בכדי שבמקרה של התקפה נוספת מסוג זהה יהיה ניתן להבחין ולספר יותר אינפורמציה.

<u>הסבר מפורט על אופן ההתקפה (התמקדות בחולשות):</u> כמו שהוסבר לעיל, ההתקפה התחילה ב"טעות אנוש" או שיתוף פעולה עם התוקף מתוך הארגון שלנו (social engineering) התבטאה בכניסה לאתר אינטרנט מזהם בעקבות הודעת מייל שהגיעה לאחד מהמשתמשים ברשת הפנימית. הודעות אלו יכולו בכלל להגיע אל המשתמש אך ורק מהסיבה כי קיימת אפשרות לשליחת הודעות דוא"ל אל חוץ ופנים הרשת שלנו, ובכלל הגישה לרשת אינטרנט. בנוסף לכך, תוכנת ה"אנטי-וירוס" אשר אמורה להגן על המשתמש מפני מפגעים מהסוג הזה, כנראה לא היית מספיק מעודכנת (אצל המשתמש או בשרתי החברה של האנטי-וירוס) או לא מספיק טובה (יש לזכור כי הקבצים המזיקים הוטמעו בתוך קבצים מסוגים אחרים שבדרך כלל לגיטמיים במהלך שימוש יום יום במחשב) בכדי לעלות על פגיעה מסוג זה. לאחר הדבקת המשתמש בסוס הטרויאני ותחילת פעולתו, היה ניתן לראות סימנים בתוכנות המעקב שלנו, אך גם שם ההתראות היו מאוד כלליות וכמובן דרשו חקירה והעמקה בנושא. עיקר החולשה שלנו מול התקפה מסוג כזה היא שממש בקלות בעקבות טעות אנוש ניתן להזיק למחשב שלך או לארגון כולו, מבלי שמישהו ירגיש! ולפעול ברקע הפעולות ללא משיכת תשומת לב מתוכנות או משתמשים.

כלים חדשים שפיתחתם/השתמשתם: פקודות לינוקס הקשורות בחיפוש מלל בקבצי השרת, פקודות עריכת קבצים, חקירת שרת Mail והכרת המבנה שלו על גבי מערכת ההפעלה Linux. במהלך התרחיש השתמשנו בפקודות כמו VIM בכדי לקרוא קבצי לוגים, ברצץ הפקודות:

cd /etc/postfix/ + vim sender_access + "appending to the file the John Smith address"

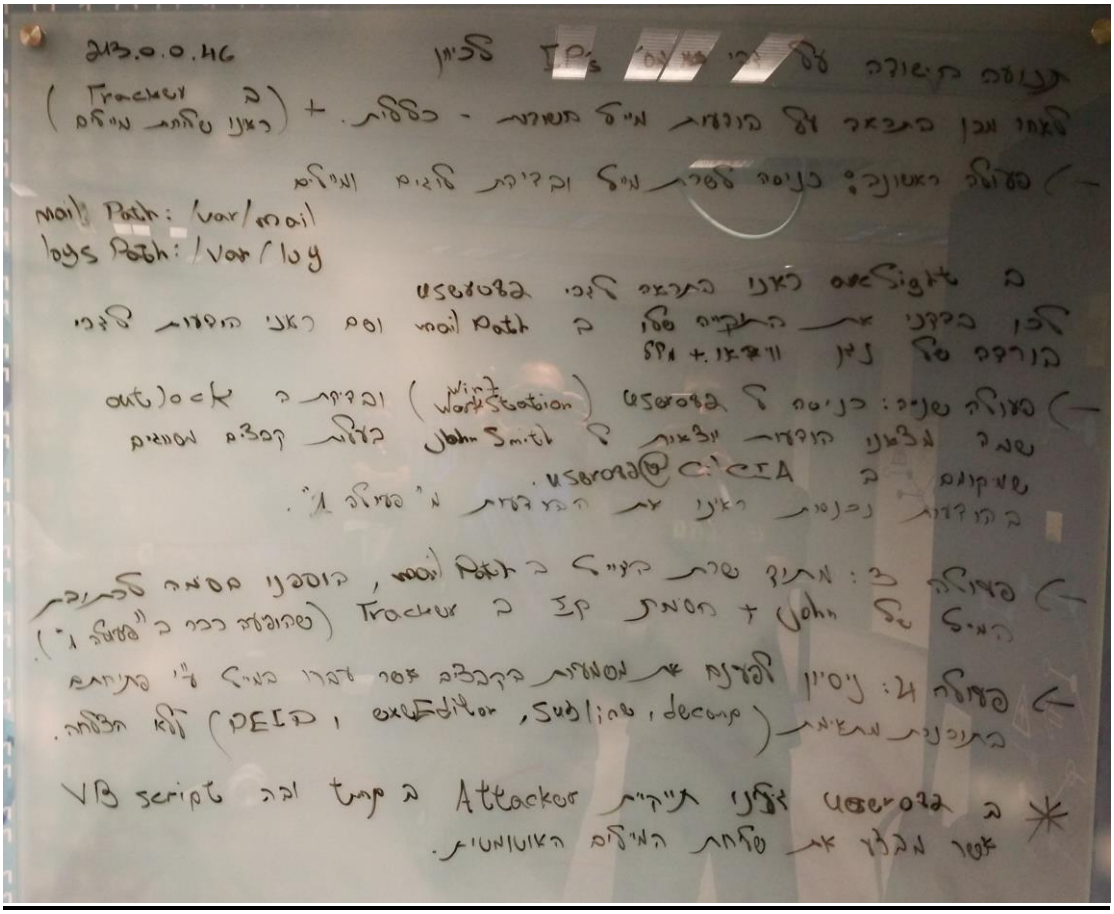
בכדי לחסום את שליחת וקבלת ההודעות מ John Smith, ופקודות נוספות המפורטות בלינקים למטה אשר כלולות בסביבת ה Bash של מערכת ה Linux. עבודה עם תוכנות כמו subLine, exeEditor, PEID על מנת לפענח קוד סקריפט זדוני.

אופן עבודת הצוות: כמו בכלל התרחישים הקודמים, עבודת הצוות התחלקה למשימה כאשר אחר מהחברים קיבל את הפיקוד לידיים, חילק את העבודה ודאג לסנכרן את חברי הצוות התוצאות ובדרישות נוספות. בתרחיש זה העבודה היית יותר ספציפית ולאחר זיהוי התרחיש החלוקה התבצעה לשתי עמדות עיקריות: שרת הדואר ומשתמש user082. רוב חברי הצוות גילו הבנה במהלך התרחיש גם אם זה לא חלק מהעמדה שלהם.

חוסרים/קשיים/בעיות: קושי ראשון אשר נדע אלינו הוא חוסר הספציפיות של תוכנת ה Tracker לספק לנו אינפורמציה מקיפה לגבי תעבורת רשת חשודה, לכן משימה זו הפכה לידנית ובוצעה על ידינו. בנוסף ההתמודדות עם התקפה שהיא פנימית בפעם הראשונה מצריכה לפעול בדרכים שונות וע"י הניסיון שצברנו פעם הראשונה נוכל להשתמש במאפייני תקיפה אלו בצורה נרחבת יותר (כמו לגשת למשתמשים המעורבים ישירות וכדומה). לבסוף נעשה מאמץ בפיענוח ההתקפה לעומק והבנת הסקריפטים אך ללא הצלחה.

<u>ציון זמנים וצעדי התקדמות של הצוות:</u>

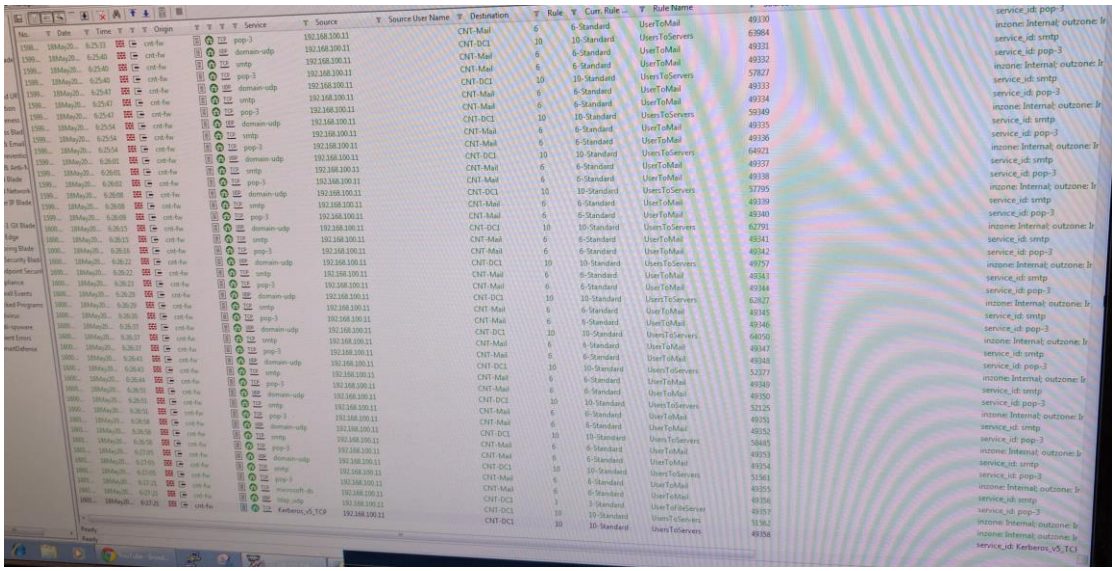
כמפורט בתמונה, ללא הגדרת זמנים אך לפי סדר ההתרחשות.



תמונות:

Notice for Suspicious Network Traffic and Suspicious Mail Activity on Arcsight

And then the wierd mails traffic on the Tracker

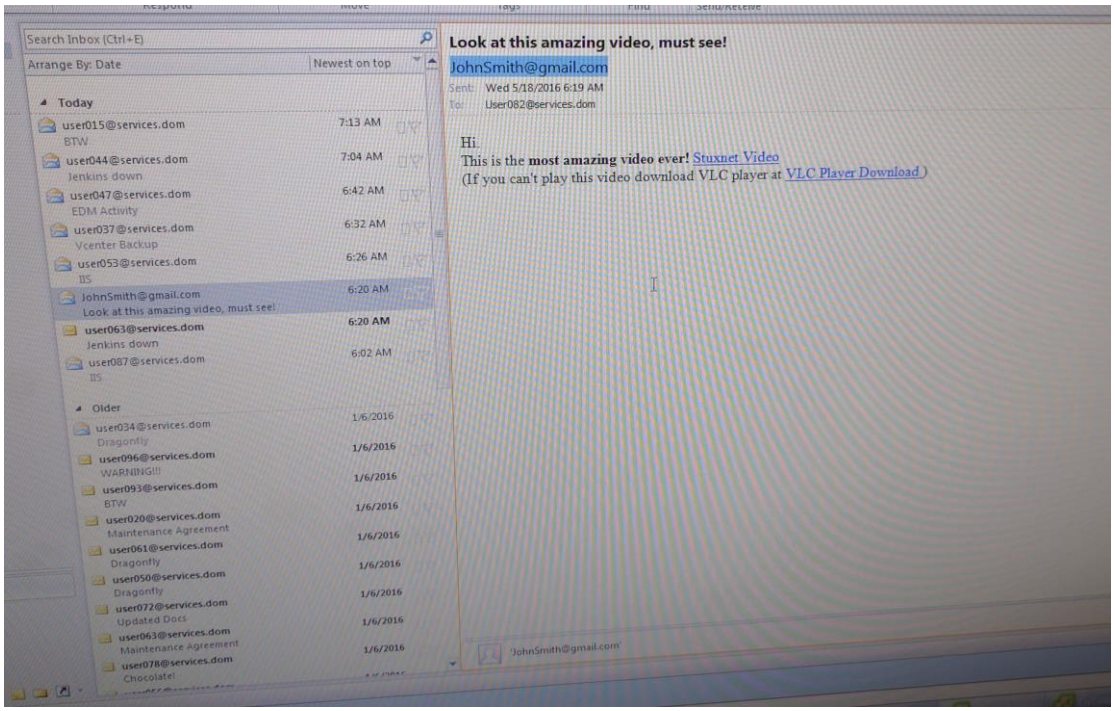


Mails log file for user082

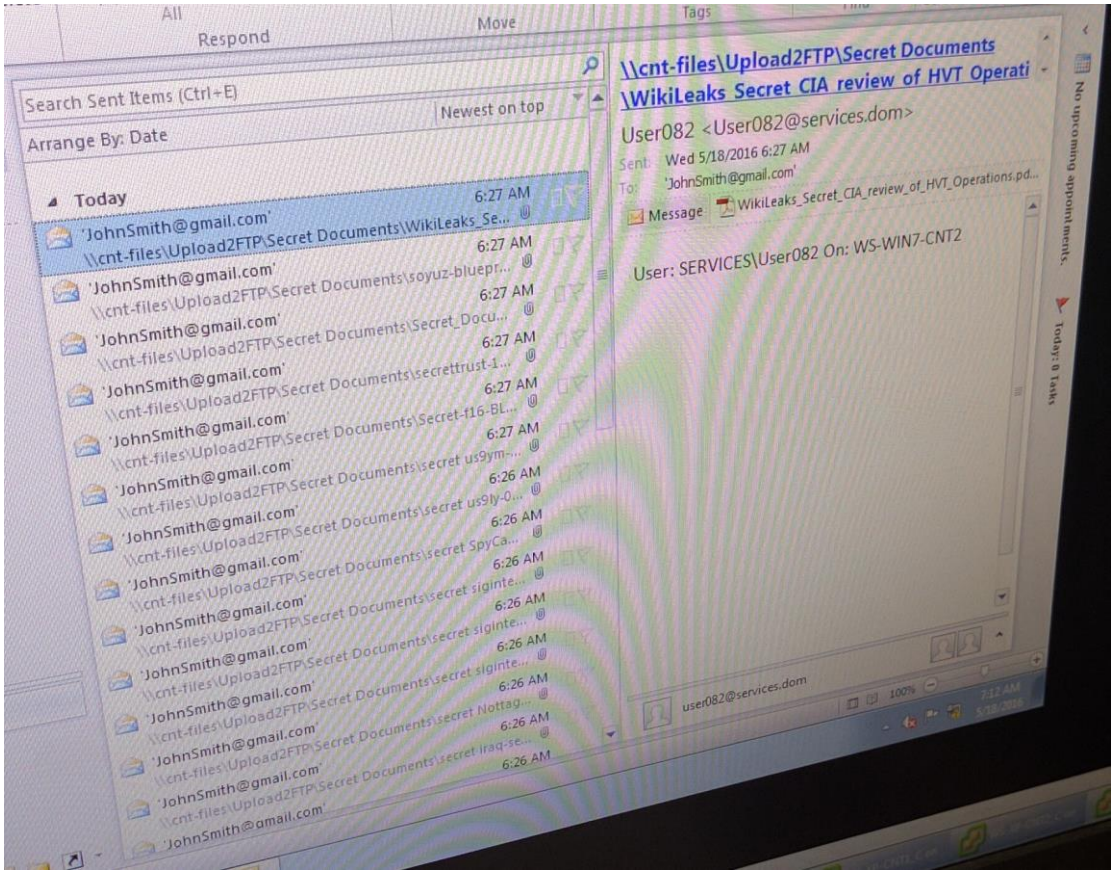
```
I lost the connection to the IIS server. Do you know who can help me out?

From user063@services.dom  Wed May 18 06:19:37 2016
Return-Path: <user063@services.dom>
Received: from services.dom ([192.168.100.115])
        by Central-Mail1.SERVICES.DOM (8.14.4/8.14.4/Debian-2ubuntu1) with SMTP id u4I6JWrt004817
        for <user082@services.dom>; Wed, 18 May 2016 06:19:37 GMT
Date: Wed, 18 May 2016 06:19:32 GMT
Message-Id: <201605180619.u4I6JWrt004817@Central-Mail1.SERVICES.DOM>
from: <user063@services.dom>
to: <user082@services.dom>
Subject: Jenkins down
X-UID: 32
Status: RO

Hey All,

Jenkins (Production) will be down for about an hour because of storage issues.

Thanks,

From JohnSmith@gmail.com  Wed May 18 06:19:48 2016
Return-Path: <JohnSmith@gmail.com>
Received: from localhost.localdomain (mailrelay.services.dom [172.16.100.7])
        by Central-Mail1.SERVICES.DOM (8.14.4/8.14.4/Debian-2ubuntu1) with ESMTP id u4I6J1Vh004850
        for <User082@services.dom>; Wed, 18 May 2016 06:19:48 GMT
Received: from Internet-Mail.gmail.com ([199.203.100.99])
        by localhost.localdomain (8.14.4/8.14.4/Debian-2ubuntu1) with ESMTP id u4I6JfwM001356
        for <User082@services.dom>; Wed, 18 May 2016 06:19:42 GMT
Received: from Ariel-TMS2 ([213.0.0.46])
        by Internet-Mail.gmail.com (8.14.4/8.14.4/Debian-2ubuntu1) with ESMTP id u4I6JFq8001399
        for <User082@services.dom>; Wed, 18 May 2016 06:19:26 GMT
Message-Id: <201605180619.u4I6JFq8001399@Internet-Mail.gmail.com>
MIME-Version: 1.0
From: JohnSmith@gmail.com
To: User082@services.dom
Date: 18 May 2016 06:19:26 +0000
Subject: Look at this amazing video, must see!
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: quoted-printable
X-UID: 33
Status: RO

Hi.<br>This is the <b>most amazing video ever!</b> <a href =3D"ht=
tp://www.bestvideonet.com/video/stuxnet.avi">Stuxnet Video</a><br=
>(If you can't play this video download VLC player at <a href=3D"=
http://www.videolan.org/download/vlc-1.1.11-win32.exe"> VLC Playe=
r Download </a>)
```

```
root@Central-Mail1: /var/mail

r malware onto systems, and running executable files on infected computers.  It is

From user054@services.dom  Wed May 18 06:36:16 2016
Return-Path: <user054@services.dom>
Received: from services.dom ([192.168.100.116])
        by Central-Mail1.SERVICES.DOM (8.14.4/8.14.4/Debian-2ubuntu1) with SMTP id u4I6aBQx008306
        for <user037@services.dom>; Wed, 18 May 2016 06:36:16 GMT
Date: Wed, 18 May 2016 06:36:11 GMT
Message-Id: <201605180636.u4I6aBQx008306@Central-Mail1.SERVICES.DOM>
from: <user054@services.dom>
to: <user037@services.dom>
Subject: WARNING!!!
X-UID: 112
Status: O

Someone is giving away infected USB devices outside the building!!! do NOT plug it in to your PC!!

From user089@services.dom  Wed May 18 06:37:07 2016
Return-Path: <user089@services.dom>
Received: from services.dom ([192.168.100.129])
        by Central-Mail1.SERVICES.DOM (8.14.4/8.14.4/Debian-2ubuntu1) with SMTP id u4I6b2Pa008456
        for <user037@services.dom>; Wed, 18 May 2016 06:37:07 GMT
Date: Wed, 18 May 2016 06:37:02 GMT
Message-Id: <201605180637.u4I6b2Pa008456@Central-Mail1.SERVICES.DOM>
from: <user089@services.dom>
to: <user037@services.dom>
Subject: Meeting
X-UID: 113
Status: O

I'm sorry but I have to reschedule our meeting for next week

From user068@services.dom  Wed May 18 06:38:45 2016
Return-Path: <user068@services.dom>
Received: from services.dom ([192.168.100.125])
        by Central-Mail1.SERVICES.DOM (8.14.4/8.14.4/Debian-2ubuntu1) with SMTP id u4I6ceMP008761
        for <user037@services.dom>; Wed, 18 May 2016 06:38:45 GMT
Date: Wed, 18 May 2016 06:38:40 GMT
Message-Id: <201605180638.u4I6ceMP008761@Central-Mail1.SERVICES.DOM>
from: <user068@services.dom>
to: <user037@services.dom>
Subject: IIS
X-UID: 114
Status: O

I lost the connection to the IIS server. Do you know who can help me out?

From user057@services.dom  Wed May 18 06:38:49 2016
Return-Path: <user057@services.dom>
Received: from services.dom ([192.168.100.130])
        by Central-Mail1.SERVICES.DOM (8.14.4/8.14.4/Debian-2ubuntu1) with SMTP id u4I6cidL008771
        for <user037@services.dom>; Wed, 18 May 2016 06:38:49 GMT
Date: Wed, 18 May 2016 06:38:44 GMT
Message-Id: <201605180638.u4I6cidL008771@Central-Mail1.SERVICES.DOM>
from: <user057@services.dom>
to: <user037@services.dom>
Subject: EDM Activity
X-UID: 115
Status: O

Hi,
I would like to come over in order to continue with the EDM activity.
Kindly let me know if tomorrow at 15:00 PM or Sunday(next week) at 10:00 AM will be a convenient time for you.
```

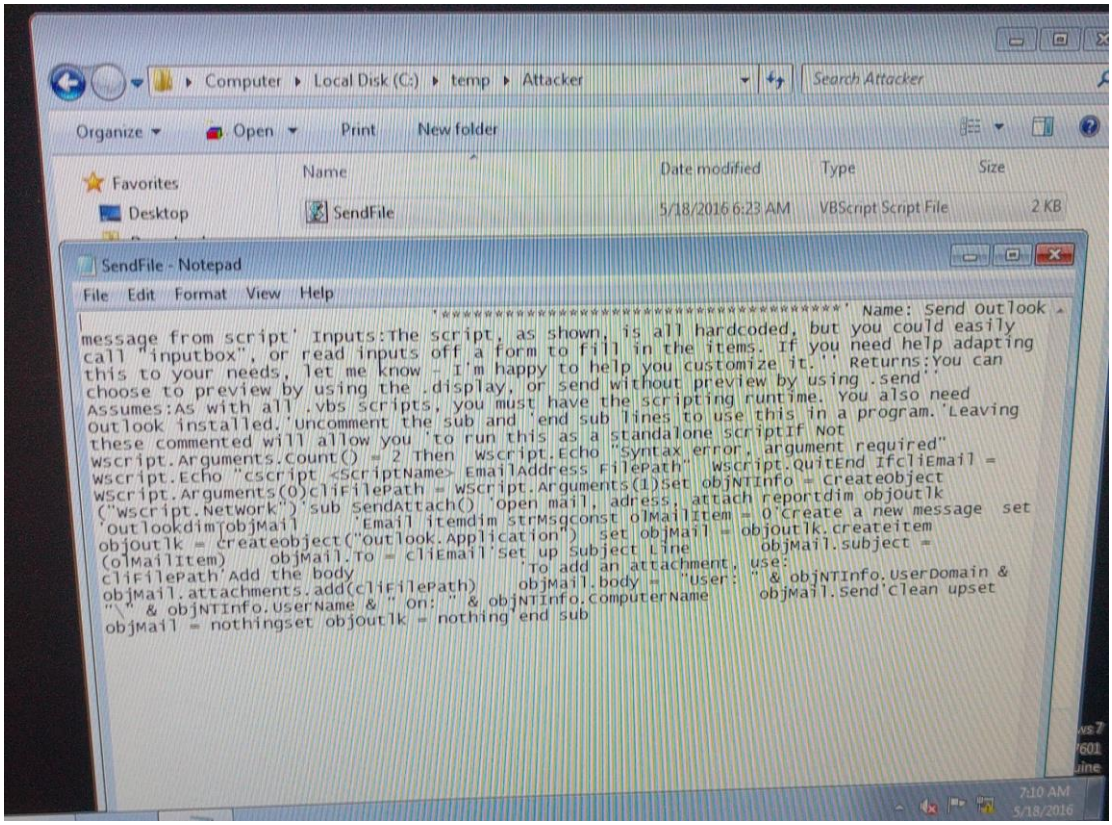
User082 outlock inbox



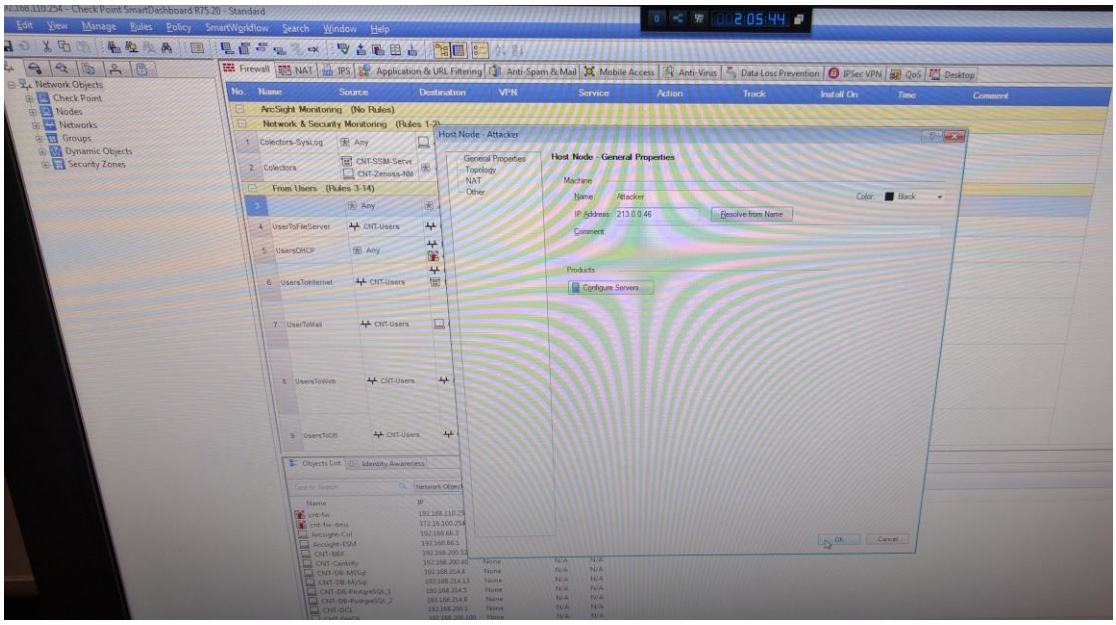
User082 outlock sent mails



VB Script for auto mails on user082



Setting new rule for blocking attacker



להרחבה / קישורים נוספים:

Linux Bash commands

Microsoft outlock guide

Infected PDF files

Linux mail servers (ubuntu ver)

Script readers / text edits / decompile apps:

- exeEdidor
- PEID
- subLime

Blocking Email address on linux mail server

ArcSight SEIM by HPE

Zenoss

Vmware vSphare

Checkpoint smartView Tracker

תוכנת בקרת רשת מבית checkpoint המספקת ממשק נוח ויעיל לאיתור אירועים ברשת. התוכנה מספקת כלים מאוד משמעותיים בסינון פעולות אשר מעניין את העוקב. התוכנה בנוסף מציגה לוגים רלוונטים לפעולות ברשת ומנתחת את תעבורת הרשת.