# דו"ח מעבדה - תרחיש מס' 4

## פרטים:

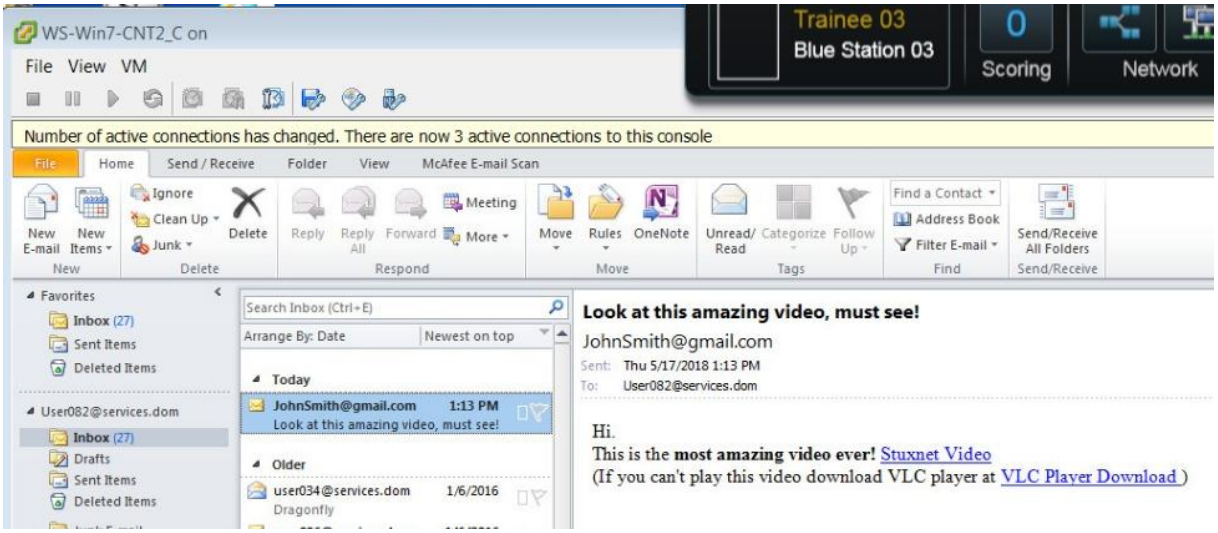
מגיש: דביר ברזילי

תאריך: 18.5.2018

שם התרחיש: Data Leakage

## תהליך ההתקפה:

התוקף החדיר נוזקה לתחנת קצה של עובד בארגון על ידי שליחת מייל. במייל היו שני קישורים, האחד לצפייה בסרטון והשני להורדת תוכנה שתאפשר צפייה בסרטון ובה הייתה הנוזקה. תפקיד הנוזקה היה לגנוב מידע על הארגון ושליחתו לתוקף.




בתמונה: המייל החשוד שבו העובד בארגון נפל למלכודת של התוקף.

## תהליך הזיהוי:

קיבלנו התראה ב ArcSight על מייל שהתקבל לאחד ממשתמשי הארגון וכנראה היה בעייתי. נכנסנו לתחתנת הקצה של המשתמש שקיבל את המייל ושרת המיילים ע"מ לאתר את המייל הנגוע. מצאנו שהתקבל מייל מ- JohnSmith@gmail.com למייל של עובד בארגון User082@services.dom

שהתוכן שלו היה נראה חשוד והיו בו קישורים להורדות. הורדנו את הקבצים לסביבה בטוחה כדי לבדוק מה הקבצים עושים. ניסינו לעשות reverse engineering לקבצים אך לא הצלחנו. כשרצינו לבדוק האם בהפעלת התוכנה מתבצעת תקשורת מהמחשב זיהינו בעזרת Wireshark שהתוכנה שולחת נתונים לתוקף.

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 1 | 0.000000 | 192.168.100.10 | 192.168.100.255 | NBNS | 92 | Name query NB WPAD<00> |
| 2 | 0.764355 | 192.168.100.10 | 192.168.100.255 | NBNS | 92 | Name query NB WPAD<00> |
| 3 | 2.798321 | Vmware_bb:4a:90 | Broadcast | ARP | 42 | who has 192.168.100.254? Tell 192.168.100.11 |
| 4 | 2.798584 | Vmware_8b:57:5a | Vmware_bb:4a:90 | ARP | 60 | 192.168.100.254 is at 00:50:56:8b:57:5a |
| 5 | 2.798594 | 192.168.100.11 | 192.168.200.3 | TCP | 66 | 49395 > pop3 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 6 | 2.798935 | 192.168.200.3 | 192.168.100.11 | TCP | 66 | pop3 > 49395 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 |
| 7 | 2.798977 | 192.168.100.11 | 192.168.200.3 | TCP | 54 | 49395 > pop3 [ACK] Seq=1 Ack=1 Win=131328 Len=0 |
| 8 | 2.799242 | 192.168.200.3 | 192.168.100.11 | POP | 74 | S: +OK Dovecot ready. |
| 9 | 2.799331 | 192.168.100.11 | 192.168.200.3 | POP | 60 | C: CAPA |
| 10 | 2.799442 | 192.168.200.3 | 192.168.100.11 | TCP | 60 | pop3 > 49395 [ACK] Seq=21 Ack=7 Win=14656 Len=0 |
| 11 | 2.799484 | 192.168.200.3 | 192.168.100.11 | POP | 127 | S: +OK |
| 12 | 2.799709 | 192.168.100.11 | 192.168.200.3 | POP | 68 | C: USER User082 |
| 13 | 2.799862 | 192.168.200.3 | 192.168.100.11 | POP | 60 | S: +OK |
| 14 | 2.799943 | 192.168.100.11 | 192.168.200.3 | POP | 69 | C: PASS P@ssw0rd |
| 15 | 2.811711 | 192.168.200.3 | 192.168.100.11 | POP | 70 | S: +OK Logged in. |
| 16 | 2.811819 | 192.168.100.11 | 192.168.200.3 | POP | 60 | C: STAT |
| 17 | 2.811960 | 192.168.200.3 | 192.168.100.11 | POP | 66 | S: +OK 1 1265 |
| 18 | 2.812021 | 192.168.100.11 | 192.168.200.3 | POP | 60 | C: UIDL |
| 19 | 2.812169 | 192.168.200.3 | 192.168.100.11 | POP | 82 | S: +OK |
| 20 | 2.812237 | 192.168.100.11 | 192.168.200.3 | POP | 60 | C: LIST |
| 21 | 2.812330 | 192.168.200.3 | 192.168.100.11 | POP | 82 | S: +OK 1 messages: |
| 22 | 2.812418 | 192.168.100.11 | 192.168.200.3 | POP | 60 | C: QUIT |
| 23 | 2.812746 | 192.168.200.3 | 192.168.100.11 | POP | 72 | S: +OK Logging out. |
| 24 | 2.812766 | 192.168.100.11 | 192.168.200.3 | TCP | 54 | 49395 > pop3 [ACK] Seq=60 Ack=202 Win=131072 Len=0 |
| 25 | 2.812845 | 192.168.100.11 | 192.168.200.3 | TCP | 54 | 49395 > pop3 [FIN, ACK] Seq=60 Ack=202 Win=131072 Len=0 |
| 26 | 2.815580 | 192.168.200.3 | 192.168.100.11 | TCP | 60 | pop3 > 49395 [ACK] Seq=202 Ack=61 Win=14656 Len=0 |
| 27 | 3.517677 | 192.168.100.11 | 213.0.0.88 | TCP | 66 | 49396 > https [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 28 | 3.518658 | 213.0.0.88 | 192.168.100.11 | TCP | 60 | https > 49396 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 29 | 4.024542 | 192.168.100.11 | 213.0.0.88 | TCP | 66 | 49396 > https [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 30 | 4.025652 | 213.0.0.88 | 192.168.100.11 | TCP | 60 | https > 49396 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 31 | 4.539382 | 192.168.100.11 | 213.0.0.88 | TCP | 62 | 49396 > https [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1 |
| 32 | 4.540517 | 213.0.0.88 | 192.168.100.11 | TCP | 60 | https > 49396 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 33 | 7.798853 | Vmware_8b:57:5a | Vmware_bb:4a:90 | ARP | 60 | who has 192.168.100.11? Tell 192.168.100.254 |
| 34 | 7.798872 | Vmware_bb:4a:90 | Vmware_8b:57:5a | ARP | 42 | 192.168.100.11 is at 00:50:56:bb:4a:90 |

```
⊞ Frame 14: 69 bytes on wire (552 bits), 69 bytes captured (552 bits)
⊞ Ethernet II, Src: Vmware_bb:4a:90 (00:50:56:bb:4a:90), Dst: Vmware_8b:57:5a (00:50:56:8b:57:5a)
⊞ Internet Protocol Version 4, Src: 192.168.100.11 (192.168.100.11), Dst: 192.168.200.3 (192.168.200.3)
⊞ Transmission Control Protocol, Src Port: 49395 (49395), Dst Port: pop3 (110), Seq: 21, Ack: 99, Len: 15
⊞ Post Office Protocol
```

בתמונה: הקלטה בעזרת התוכנה Wireshark של התקשורת שבתחנת הקצה ברגע הפעלת התוכנה החשודה.

## תהליך הגנה:

חסמנו את התקשורת מהמחשב שהותקף לתוקף בעזרת חקיקת חוק חדש ב-FireWall, ומחקנו את הנוזקה. כמו כן היה עלינו לשנות את הסיסמה למחשבי הארגון מכיוון שהתוקף כבר הצליח לגנוב אותה.

## תהליך הגנה מונעת:

על מנת למנוע מתקפה דומה על הארגון שלנו עלינו להגביר את המודעות בקרב העובדים לגבי הסכנות שעומדות בפנינו בעולם הסייבר והדכים להימנע מהן.
בנוסף לכך קיים צורך להתקין על המחשבים בארגון תוכנת אנטי וירוס.

## הפרצות באבטחת הארגון

הפרצות באבטחת הארגון הינם עובדי הארגון (משתמשי תחנות הקצה). העובדים בארגון הם דלת קלה ותמימה לתוקפים להחדיר נוזקות ולפרוץ לתוך הרשת הפנימית של הארגון.

## אופן עבודת הצוות

באופן כללי היה לנו מאוד פשוט למצוא את המייל החשוד שעליו קיבלנו התראה. משם המשכנו כולנו לחקור את הנזק שהתוכנה גורמת.

## חוסרים/קשיים

היה קשה להבין מה התוכנה שהמשתמש הוריד מהמייל עושה. בנוסף לקח זמן רב עד שמצאנו את הקובץ עם הקוד שהיה אחראי על שליחת המידע לתוקף.