דוח pen test

דוח מספר 3

מאת: יגאל נאמן 300369972

דוח מעבדה בעניין אירוע Worm Wmi

Worm Windows Management Instrumentation

תהליך התקפה: ידוע גם בשם נוסף: **WORM_AGENT.WMI**

הוא וירוס מחשב מסוג תולעת שתקף באוקטובר **2008** והתפתח בגרסאות נוספות עד לשנת ו**2017** וירוס זה תקף מספר רב של מחשבים בעולם. התולעת תוקפת את מערכת ההפעלה חלונות. היא מנצלת פרצת אבטחה הקיימת בגרסאות: **Windows 2000, Windows XP, Windows Vista, Windows Server 2003, Windows Server 2008,** ובגרסת הבטא של **Windows 7.**

התולעת תוקפת בעיקר מחשבים עם סיסמאות רשת חלשות, פרצות אבטחה של מיקרוסופט ומחשבים בעלי תוכנות אנטי-וירוס לא מעודכנות.

הווירוס פועל על תקן "פצצת זמן", כלומר שהוא תוכנן לקבל הוראה של הורדה של נתונים מהמחשב האישי הנגוע בתאריך מסוים. התולעת כוונה ל-**1** באפריל **2009.** תאריך זה גרם לתהיות רבות באשר ליוצריו. יש שחשבו שמדובר במתיחה אחת גדולה לרגל התאריך. למרות זאת, בניגוד לציפיות, התולעת לא עשתה דבר ב-**1** באפריל, אך היא עדיין עלולה **"**להתעורר**"** בהמשך ולקבל הוראות מיוצריה **(**בד**"**כ מבוסס על שרת **C&C)** בסגנון בוטנט.

אופן פעילות של התולעת:

התולעת גורמת נזק באמצעות גלישת חוצץ (buffer overflow), תקלת תכנות הגורמת לכך שתוכנית מחשב כותבת לאזור בזיכרון המחשב (החוצץ) יותר מידע מאשר אותו אזור מסוגל להכיל. כתוצאה מכך "גולש" חלק מהמידע אל מחוץ לגבולות החוצץ, ומשנה נתונים שלא היו אמורים להשתנות. התולעת משתמשת בבקשת RPC ייחודית כדי להפעיל את קוד התוכנה שלה על מחשב המטרה.

כמו כן, כחלק מהפעילות של התולעת היא תוקעת את ה-task manger בכדי להקשות על גילוי טיפול ואף סגירת הפרוסס של וירוס עצמו.(בזמן ריצה)

Remote Procedure Call

התולעת מבטלת שירותים חיוניים של מערכת ההפעלה חלונות כגון: Windows Automatic Update, Windows Security Center, Windows Defender ואף Windows Error Reporting. ביטול שירותים אלה לבדו לא גורם נזק מיידי למחשב אך הופך את המחשב לפגיע יותר וחושף אותו למתקפות שונות שאת חלקן היא עצמה עשויה ליזום בשלב השני של פעילותה.

התולעת פותחת דלת אחוריתBACKDOOR לקבלת הוראות נוספות משרת מרוחק. היא עשויה לקבל מהשרת אחת או יותר מההוראות הבאות: הוראה להתרבות ולהפיץ את עצמה, הוראה לאסוף מידע אישי על המחשב ועל המשתמש, הוראה להוריד מהשרת או ממקור אחר תוכנות זדוניות נוספות למחשב בו הופעלה[3]. כמו כן התולעת מתחברת לתהליכים[4] הבאים של מערכת ההפעלה: svchost.exe, explorer.exe וגם services.exe.

סיפטומים להזיהוי בהדבקה בתולעת: (תהליך זיהוי)

bna- Netstat

ואץ חיפשנו לפי file modify קבצים שהשתנו בעמרכת ללא הרשאה שלנו ושהם חשודים לפי תאריך ושעה (חקירה של הקבצים)

בנוסף, במקרה של הדבקה יהיה מצב שהטסקמנגר יהיה תקוע לא יהיה גישה להגיע לרשימת הפרוססים ולהרוג אותם

stack (ctrl alt delete) will be Taskmanger - יהיה תקוע... (במקרה הכי קל לזיהוי הטסקמנגר פשוט יהיה תקוע בדיוק כמו שראינו בשיעור הקודם)

דרכי הדבקה : התולעת מפיצה עצמה בעיקר דרך אתרים לא מהימנים ("זדוניים"), אך גם דרך התקנים חיצוניים, כדוגמת זיכרונות נשלפים כמו דיסק און-קי

וירוס זה היה בין הוירוסים המזיקים בתולדות המחשוב האישי. משווים את נזקיו לאלו של התולעת SQL Slammer משנת 2003, וגם כן התולעת MyDoom (המוכר גם כ-Novag) משנת 2004, ומעריכים כי התולעת גרם נזקים גבוהים מאשר גרמו .

Malware type :TROJ_WMIGHOST.A, WMIWORM.A ,a WMI script, arrives on a system bundled with BKDR_HTTBOT.EA ,a DLL malware

Aliases: Backdoor.Win32.Agent.amb (Kaspersky), W32/Autorun.worm.c (McAfee), Trojan.Panddos (Symantec), BDS/Agent.amb.15 (Avira), Mal/Heuri-D (Sophos),

וירוס זה היה בין הוירוסים המזיקים בתולדות המחשוב האישי. משווים את נזקיו לאלו של התולעת SQL Slammer משנת 2003, וגם כן התולעת MyDoom (המוכר גם כ-Novag) משנת 2004, ומעריכים כי התולעת גרמה נזקים גבוהים

- שירותים שונים של מערכת ההפעלה, כגון Automatic Updates, Background Intelligent Transfer Service (BITS), Windows Defender ו-Error Reporting Services לא יפעלו[1].
- שרתי דומיין יגיבו באיטיות לבקשות המחשב.
- עומס על הרשת.
- בגישה לאתרים המקושרים לתוכנות אנטי-וירוס שונות המאפשרות לעדכון מערכת ההפעלה תהיה חסומה[1].
- התולעת מאפשרת ליוצריה לנצל מחשבים נגועים, על ידי שליטה מרחוק (מצב המכונה "מחשב זומבי דהיינו: גישה המתקבלת דרך שרת C&C …BOTNET"), שימושים זדוניים: התקפות מניעת שירות (DDos), רישום הקשות מקשיKEYLOGGERS, שליחת דואר זבל ("SPAM") ...

תהליך הגנה + טיפול והסרה על פי סעיפים והמלצות:

בראש ובראשונה יש לוודא כי המחשב מאובטח כשורה וכי האנטי וירוס פעיל, כולל חומות האש , ושאין תוכנות שלא מוכרות רצות ברקע. (Task managers) בלינוקס `ps -aux | less`

להקשיח סיסמאות(סיסמאות ארוכות עם סימנים)

להחליף סיסמאות אחת לכמה זמן – בקופות קצרות באופן יזום אחת לחודש

לבצע עידכוני תוכנה של אנטי וירוס + MICROSOFT WINDOWS באופן שותף

תדרוך לאנשים המתפעלים מחשב לבצע תדרוך בעניין מודעות בארגון(הגורם האנושי)

ניתן לתת דוגמא: Opisrael אשר גופים גדולים כמו "מכבי -שירותי בריאות" – למשל

בימים שיש מתקפות סייבר היינו מוצאים מייל בצורה מסודרת לכל הגורמים בארגון באשר לסכנות שיש להימנע מפתיחת מיילים/ לחיצה על לינקים לא מוכרים/או פתיחת קבצים מאנשים לא מוכרים בארגון.

ושאין לאשר קבלת מיילים מגורמיים שהם לא מהארגון (גורמים חיצוניים)

יש לדווח למנהל אבטחת המידע \מערכות מידע \CISO בכל עיניין חריג.

יש להזהיר את הצוות בנוגע לכניסה למיילים לא מוכרים ולחיצה על לינקים שהם לא מאנשים מוכרים אנשים מהארגון) כיוון שמצב זה עלול לפתח מתקפה כנגד או בתוך הארגון כתוצאה מקובץ זדוני\פישינגי וכיוצא בזה..

עוד ניתן לומר כי:

עדכון תוכנה הקרוי MS08-067 המתקן את פרצת האבטחה שוחרר על ידי מיקרוסופט כבר ב-15 באוקטובר 2008, הרבה לפני שמישהו ניחש את ממדי הנזק שגרמה התולעת. עדכון התוכנה עובד רק בגרסאות הבאות: Windows XP בו מותקנת חבילת השירות השנייה או השלישית, Windows 2000 בו מותקנת חבילת השירות הרביעית, ו-Windows Vista. עדכון תוכנה עבור גרסאות מוקדמות יותר של Windows XP ו-Windows 2000 לא הופץ מכיוון שתקופת האחריות לתמיכה במוצרים אלה פגה.

כלים להסרת התולעת קיימים אצל ספקי התוכנה Microsoft, BitDefender, ESET, Symantec, Sophos, ו-Kaspersky Lab. בתוכנת אינטל סקיוריטי אפשר להסיר את התולעת בסריקה לפי בקשה. מכיוון שאחד האמצעים שדרכו עוברת התולעת הוא כונני USB, כדאי לבטל את אפשרות ה-AutoRun למדיה חיצונית בעזרת ה-Registry של חלונות

תיאור מצב ברגיסטרי:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\

[AutoRun]
open= audiodg.exe
shell\Auto\command=audiodg.exe
shellexecute= audiodg.exe

Details:

Arrival and Installation

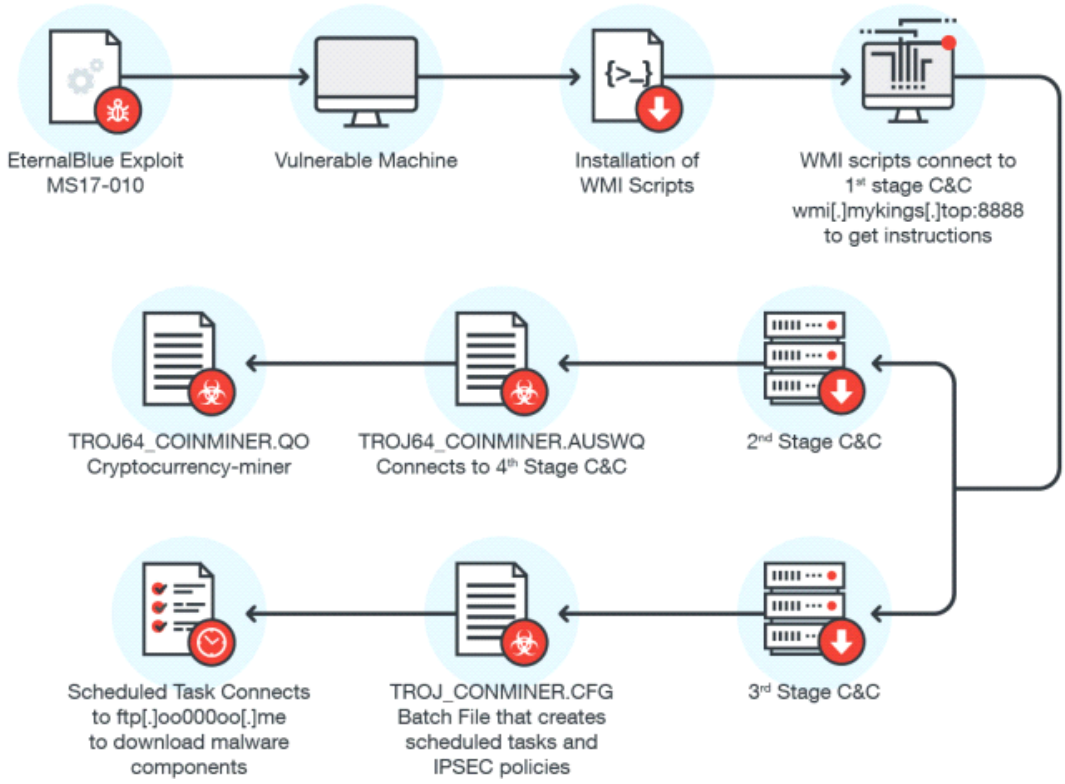
This worm may arrive as a dropped file through removable drives.

This worm drops and executes the following file:

- %System%\audiodg.exe

מצב תרשים זרימה של התולעת (תהליך הישתלשלות הדברים)

C&C , מתאר מצב בוא התועלת מחוברת לשרת COMMAND CONTROL של התוקפים (אלה שהפיצו את הוירוס)



דוגמא להמחשה למצב המתאר הפעלת הוירוס קופר, במטרה לסחות כספים מהארגונים

מה שבעצם קרה זה התקופים עשו WGET במילים אחרות DOWNLOAD דרך שרת ה C&C הם שידרגו את וירוס לוירוס קופר במטרה לסחוט כספים מארגונים כנגד הצפנת הקבצים (מטרת הוירוס הקופר ראה דוגמא WANNACRY)

דוגמאות נוספות משירותי הסרביס של מערכת ההפעלה/ תיאור מצב:

WMI Abused for Malware Operations

TROJ_WMIGHOST.A, a WMI script, arrives on a system bundled with BKDR_HTTBOT.EA, a DLL malware

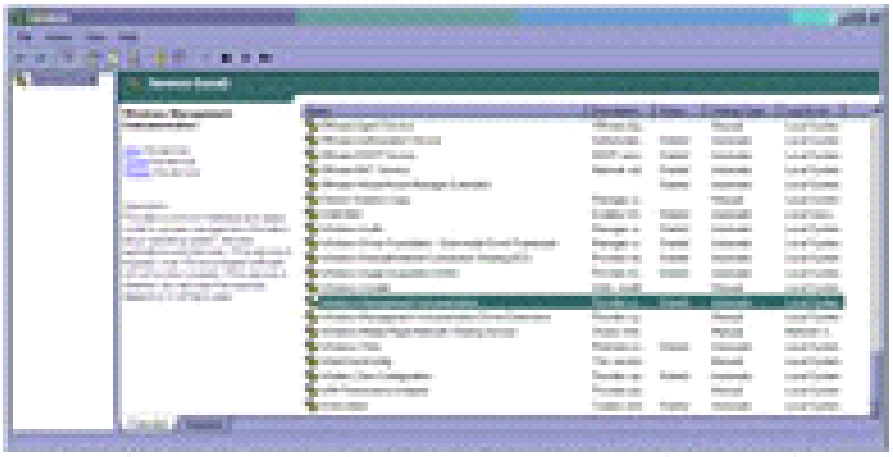


Figure 1. Screenshot of *Windows WMI*

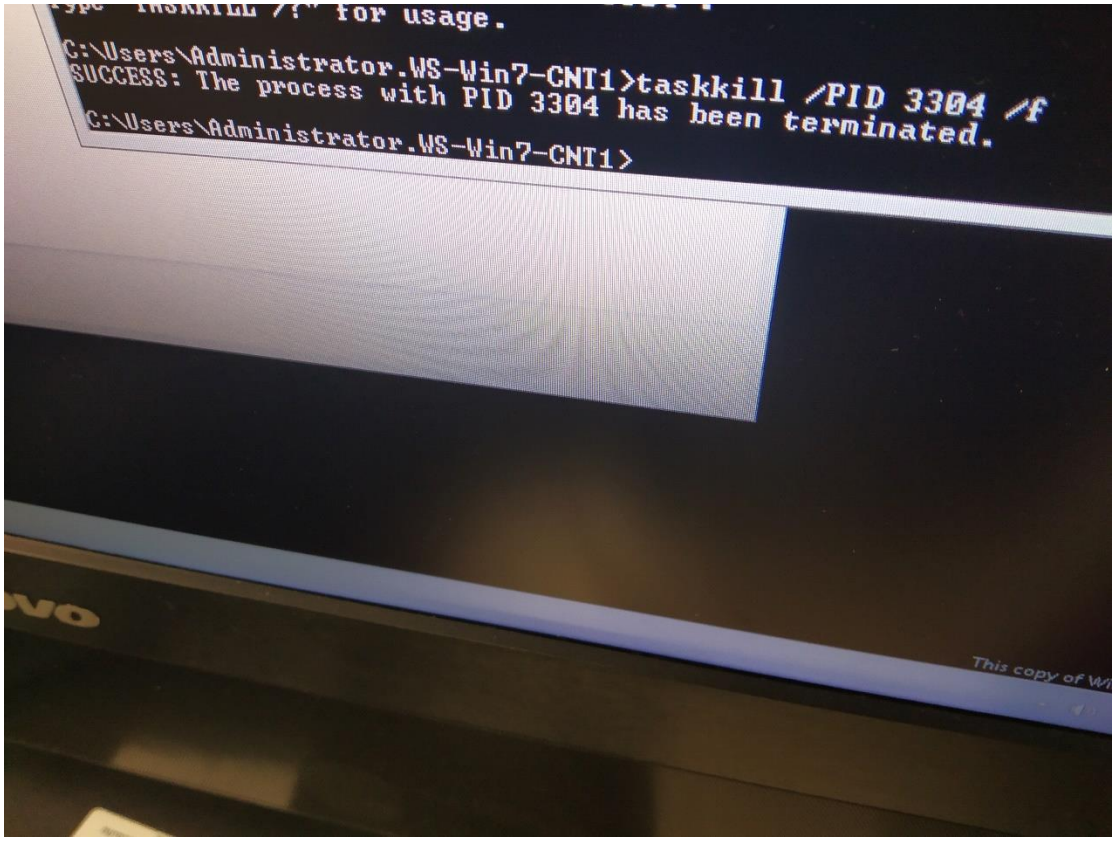
c:\users**A**dministrator\.ws-win7-cnt1> taskkill /pid 3304/f

הפעולה – חשוב לשים לב שהפעולה הצליחה (סקסס)

לגבי היוזר: בדגש על ה- Administratorהמציין את יוזר מנהל המערכת, ביצענו "הריגה" ל- מספר ה- PID

שאחראי לזה שהפרוסס רץ מאחריי הקלעים.

פירוש הדבר כיוון התולעת תוקעת את ה- MANGER TASK כמו שציינו, היינו צריכים לסגור את הפרוסס מה ה- CLI



<u>המשך תהליך זיהוי, הסברה לצורך הבנה , מה המניע של התוקפים בעצם בד"כ:</u>

לאחר זיהוי ועריכת הקוד של התולעת, ניתן להבחין כי ה- בתוך הקוד יש סיסמא להתחברות לשרת בכדי לנטרל את התולעת

הסיסמה cyber

וה- "בוט" (התולעת למעשה) מאשרת את הסיסמה בכך שהיא עונה yes master

מזכיר לנו מצב - מימיי ה-IRC העליזים (1998-2006):

מצורף כאן קישור לסרטון עורך **<u>דקה</u>** יוטיוב אשר מדגים במצב אמת מהו מתקפת DDOS למעשה:

https://www.youtube.com/watch?v=Mx836bkUd04

חשוב לציין כי כל מי שמופיע בסרטון מצד ימין למטה זה ה- "בוטים" המחשבים שנפרצו והופצה בהם התולעת, ומי שנמצא למעלה עם סימן ה- &אמפרסנט(מנהלי הסרבר), ה @ שטרודל נקראים אופרטורים,

לרוב שרתים מסוג זה רצים על שרתי לינוקס מבוסס APACHE אשר IRCD רץ מאחריי הקלעים עם פורט פתוח ל- 6667 ועד 7000 זהו פורט התחברות לשרתי ה MIRC אני נותן שירות למתקפות כמו שציינתי לעיל.

בנוסף התוקפים הם בעלי השליטה על הבוטים והם אלה שאחראים על ההפצה שלהם , הכתיבה שלהם , השדרוגים הכל הכל, זה ממש כמו "בית תוכנה קטן", בד"כ מנוהל ע"י 3-4 אנשים

(חדרי בוט מסוג זה לרוב מנוהל על ילדים בגילאי ה- 14 עד 17 , ונקראים בשפה המקצועית ScriptKiddz)

זה מתקשר גם היום לעיניין # opisrael

<u>מקווה למצוא זמן ושאדון על זה בהמשך...</u>

בעצם מה שקרה בערוצים האלה היו משתלטים על בוטים בכדי ליצור "אנרכיה" התקפות DDOS , SYN, ICMP וכיוצא בזה

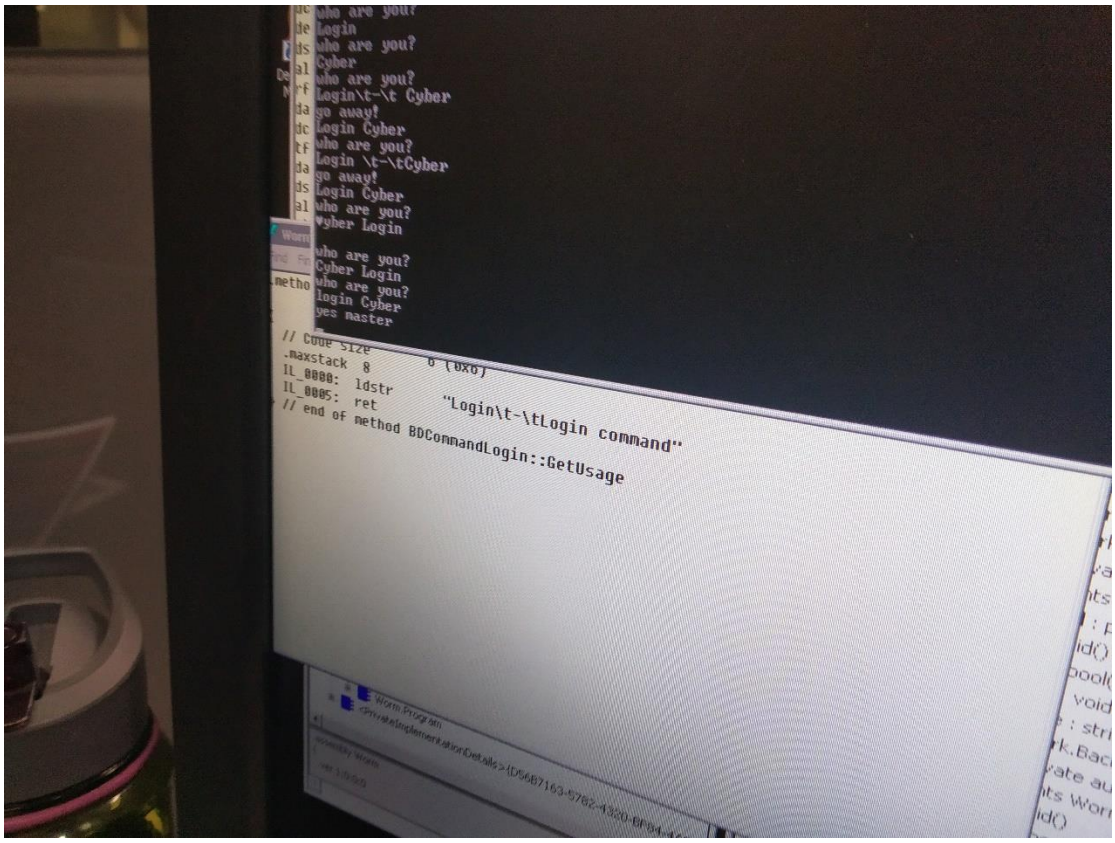
וזה מה שמצב , חוזר על עצמו כיום בדיוק כמו רוטינה רק שפעם זה היה תוקף שרתי WINDOWS

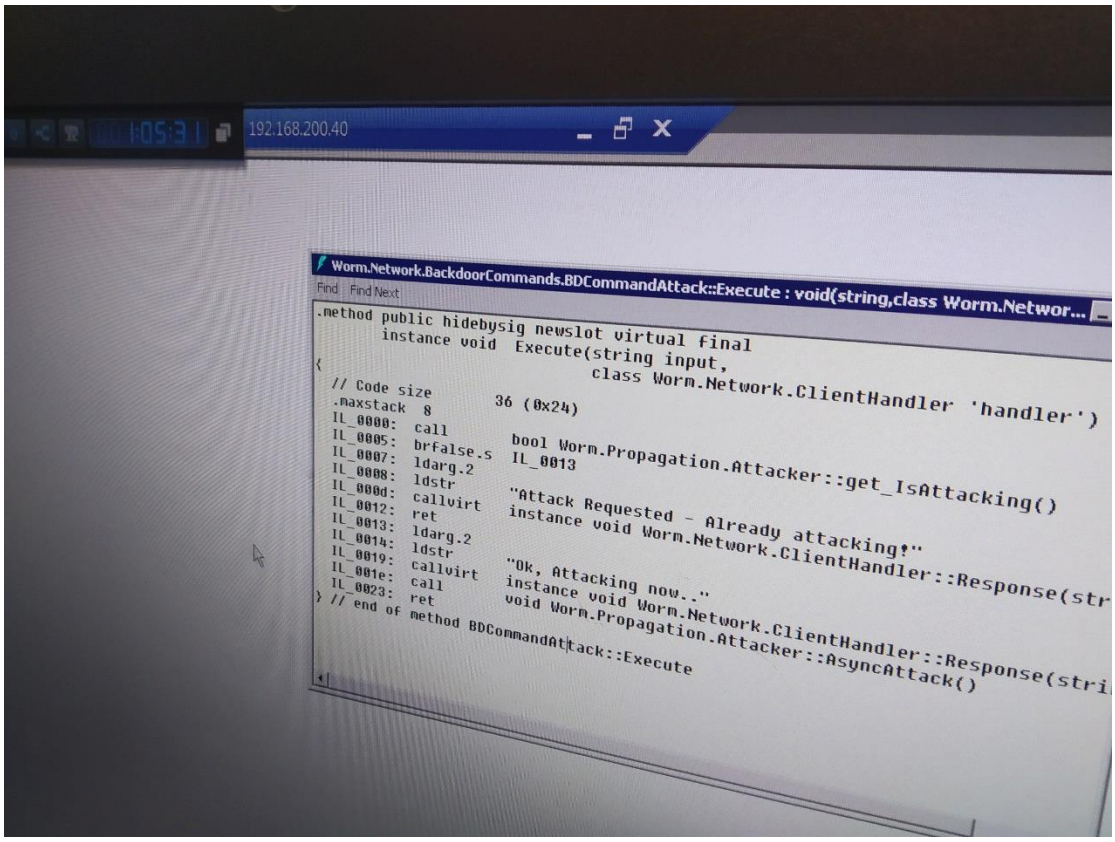
היום למעשה רוב ה- "אקספלוייטים מבוססים ו\או נכתבים ב PYTHON, מה שמביא להתקפות רבות והשתלטויות על שרתי LINUX'

ואצל ההאקרים בלעז זה נקרא: **uptime server במטרה** למצוא XDCC# #warezone \0day\

שיוכל להכיל כמה שיותר שרתי בוטנט לצורך התקפת מניעת שירותת\ואו מכירה של בוטנטים.

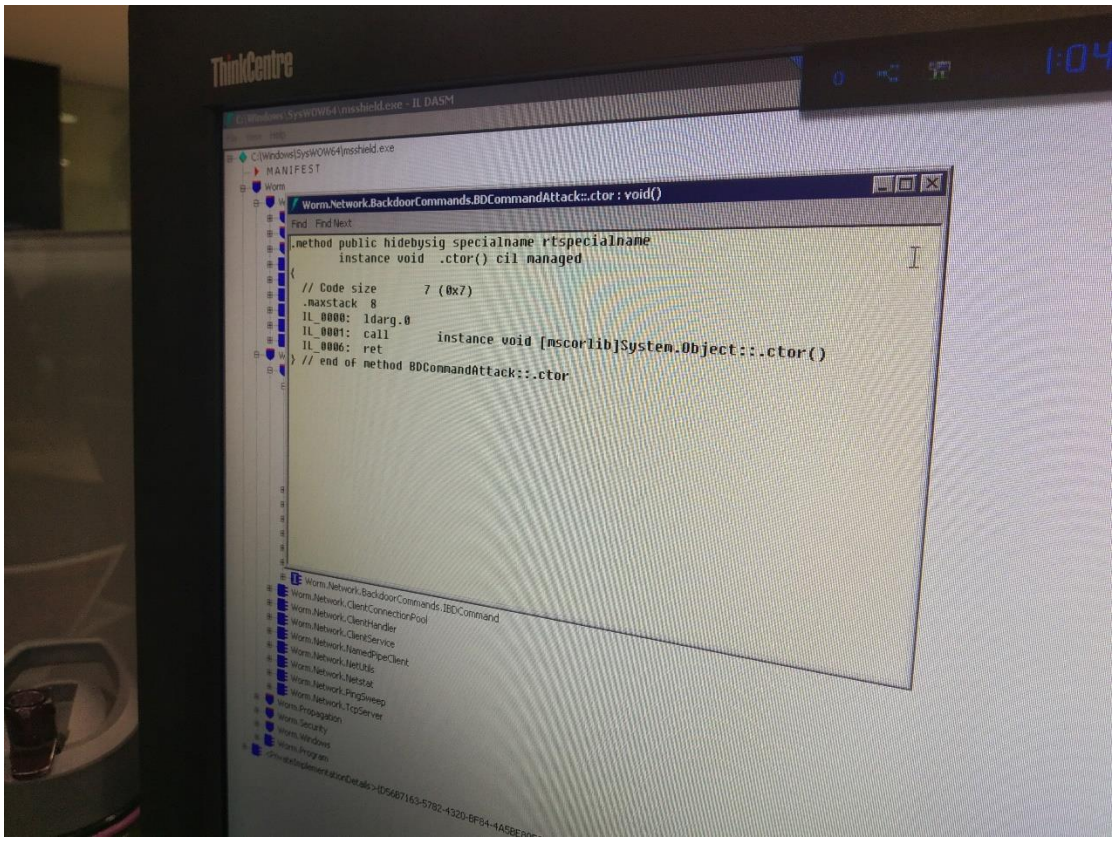
המטרה אצל האקרים בעצם זה למצוא שרתים חזקים שהחיים שלהם אורכים בכדי לשמש והישתמש בהם בתור שרתי IRCD למשל ואז ליירט דרכם גירסאות חדשת של וירוסים\תולעים.





עוד תמונות מהאירוע.

כאן ניתן להבחין בקוד של התולעת ברמה של תוכנה\קוד.(ILSDASM) דיבגר



עוד תמונות מן האירוע תמונת הצלבה בקוד באסמבלי,(לאחר קומפילציה) לצורך מימוש התולעת

לסיכום :

אי אפשר שלא להתרשם מהדרך המתוחכמת בה פועלת התולעת. כותבי התולעת השקיעו המון ידע ותכננו תולעת ברמה מאוד גבוהה, השתמשו בשיטות מתקדמות, מימשו אלגוריתמים חדשניים ה-R ב-RSA אפילו דאגו להתעדכן ולשפר את מנגנוני התולעת שאותם הצליחו לעצור

. התולעת הופעלה בראשון באפריל 2008 והייתה אמורה לטרוף את דרכה ברשת.

אבל לא קיימת הוכחה שיוצריה הפעילו אותה בצורה כלשהי. אולי עצם העובדה שהיא הופעלה ב-1 באפר נותנת את התשובה שזאת סתם הייתה מתיחה, למרות שקשה להאמין כי השקעה בתולעת מתוחכמת כל כך נעשתה לשם מתיחה...

דגשים אחרונים:

-הדרכות (הגורם האנושי) לכלל חבריי הארגון וביצוע מבדק לעובדים דרך מערכת ה CRM המבוססת שם משתמש וסיסמה יחודית לכל עובד אשר תאפשר לי לנהל שליטה ובקרה בעמיתי הארגון שמכירים בסכנות העולות מן הרשת לתוך הארגון.

פשוט לערוך מצגת הסברה ,אשר מאשר לי כי העובדים מכירים בסכנות העלות מן הרשת האינטרנט לתוך האירגון, בכדי לצמצם פגיעויות בארגון בוא אני מטפל.

- לחסום USB (דיסקאונקי ללא הרשאה בארגונים – לצורך מניעה והידבקות בוירוסים)

- להקפיד על סיסמה חזקה מאד
- החלפת סיסמה בשותף אחת לחודש תזמון אומטי באופן יזום
- עדכון מערכות הגנה כולל אנטי וירוסים

חשוב לזכרור את אבני היסוד שלנו, ובשביל זה אנחנו כאן. CIA

- **שלמות** .(integrity)הגנה מפני שינוי זדוני של המידע או השמדתו, כולל הבטחת אי התכחשות ואימות זהויות בעלי המידע.
- **סודיות** .(confidentiality)הגבלת גישה או חשיפה, כולל הגנה על פרטיות וזכויות קניניות.
- **זמינות** .(availability)שמירה על זמינות ויעילות הגישה אל המידע בכל זמן נתון.

אופן העבודה בחלק זה לרוב עבדתי עצמאית ברוב הזמן.

בחלק האחרון לקאת המשימה נתתי ממש פול גז בכדי לרדת לעומק הבעיה (היו הסתעפויות באירוע)

זה בהחלט אירוע שלא קל לזיהוי – ולחסרי ניסיון יכול להיות אף מסתכל במציאת פתרון הבעיה)

ראוי לציין כי ברוב הזמן יצרתי מגע ושבאמת נסיתי לעזור לשאר חבריי הצוות כמה שיכולתי.בסה"כ מדובר באירוע לא פשוט כלל מכוון שצריך יכולות גבוהות בכדי להבין בעצם מה מטרת המתקפה , מה היעדים שלה, ואיך היא תוקפת .