Digital Whisper
Technologic Papers

Malwares 2.0, ודרכי התמודדות בארגון

מאת אריק יונאי

הקדמה

במאמר זה לא אכנס להגדרות של מהו וירוס, תולעת, סוס טרויאני וכו'. אני משוכנע שמי שממש ירצה לדעת את ההגדרה הרשמית שלהם יוכל לפנות ל-Wikipedia הקרוב למקום מגוריו ☺. מאמר זה יעסוק בהתקפות קוד זדוני בארגון, כולל את כל משפחת "הרעים", קרי Malwares.

כולנו מבינים את חשיבותו של אנטי-וירוס בארגון. סטטיסטית, רוב האנטי-וירוסים של רוב היצרנים, יזהו את רוב ה-Malwares הנפוצים בארגון. אסביר את הבעיה בכמה משפטים:

אנטי-וירוס מגלה רק וירוסים שהוא מכיר. משמע, אנטי-וירוס (אנטי-וירוס "מסורתי"), הינו מבוסס "חתימות" (Definitions), אשר יצרני האנטי-וירוס מפיצים עדכונים אחת לכמה דקות / שעות בדר"כ. כאשר קוד זדוני (וירוס, לצורך העניין) רץ על מכונה, האנטי-וירוס אמור לזהות את הקוד הזדוני, אך ורק במידה ויצרן האנטי-וירוס **נתקל בקוד הזדוני בעבר, וייצר נגדו חתימה**. חשוב להבין, כי במידה ויצרן האנטי-וירוס לא נתקל בקוד הזדוני בעבר, וכתוצאה מכך גם לא ייצר נגדו חתימה, כנראה שהוירוס ירוץ על אותה מכונה לאורך זמן רב, ללא כל הפרעה.

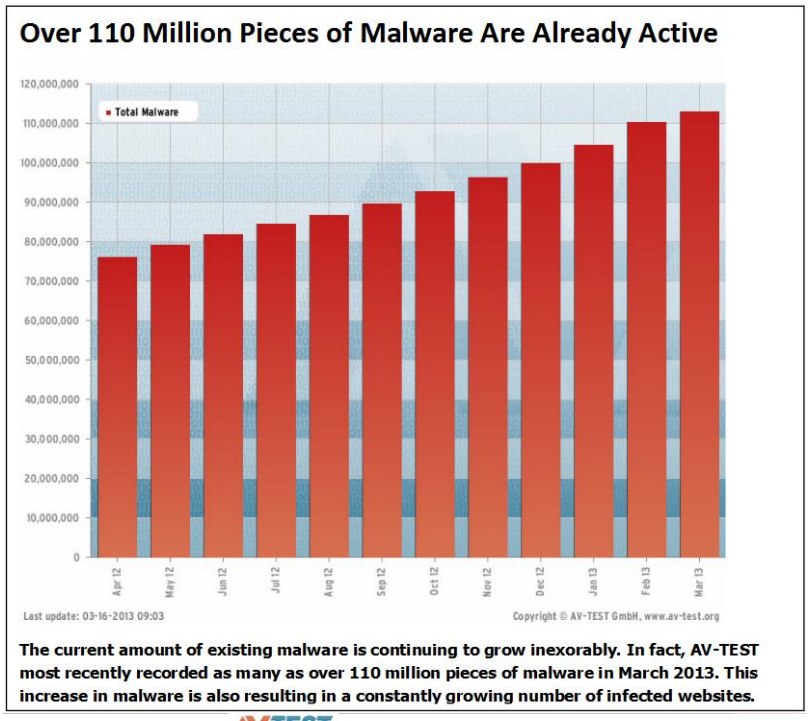
מחזור החיים של וירוס ממוצע:

1) וירוס **חדש** נכתב בעולם. הוירוס מגיע לרשת הארגון (בצורה כזו או אחרת, לא עקרוני בשלב הזה).
2) הוירוס החדש פועל ברשת. אולי הוירוס יתגלה במזל בעקבות תלונת משתמש על תופעות ליווי של הוירוס או בצורה אחרת, ואולי לא יתגלה לעולם.
הוירוס יכול להתגלות מיד, או להתגלות לאחר זמן רב, או כאמור לא להתגלות כלל, לא ע"י האנטי-וירוס (מאחר והוירוס הוא וירוס **חדש**, לאנטי-וירוס עוד אין חתימה המתריעה כנגד הוירוס), ולא ע"י אף גורם בארגון.
3) במידה ולארגון היה מזל והוא הצליח לאתר את הוירוס (לא באמצעות האנטי-וירוס), הוא משקיע מאמץ באיתור אותו קוד זדוני, ומעביר אותו ליצרן האנטי-וירוס (ברוב המקרים Process נגוע, אך לא תמיד).
4) יצרן האנטי-וירוס מייצר חתימה כנגד הוירוס, לרוב תוך שעות עד ימים.
5) חתימות היצרן מתעדכנות בשרתי האנטי-וירוס ובתחנות הארגון, והוירוס מאותר ומושמד.

הבעיה בתסריט הנ"ל (התסריט הנפוץ ברוב הארגונים), ברורה. עד שהארגון לא מעביר וירוס חדש (שאיננו מוכר ליצרני האנטי-וירוס) ליצרן האנטי-וירוס, הוירוס יכול לפעול חופשי.

בעיה נוספת היא, שגם במידה ויצרן אנטי-וירוס כתב חתימה כנגד הוירוס, פעמים רבות החתימה כנגד אותו וירוס תהיה מופצת **רק לאותם מוצרים של יצרן האנטי-וירוס**, ויצרני אנטי-וירוסים אחרים לא יוכלו לספק את החתימה לוירוס שהתגלה ע"י היצרן ה"מקורי" (במידה והם לא נתקלו בוירוס), וזאת מאחר ויצרני האנטי-וירוס לרוב אינם משתפים את החתימות שלהם עם יצרנים אחרים (ישנם גם חריגים, אך הרוב לא עושים זאת). לרוב, אנטי-וירוס הוא פשוט פתרון לא יעיל כנגד וירוסים חדשים לא מוכרים, אשר גורמים לנזק שאינו בולט או שאינו יוצר "רעש" מורגש.

וירוסים שלא מתגלים ע"י האנטי-וירוס (מאחר והפעם הראשונה שהוירוס מופיע איפשהו, הוא עדיין לא מוכר ע"י יצרני האנטי-וירוס), לרוב פועלים ללא שום הפרעה, ועשויים לגרום לנזקים כאלה ואחרים ברשת הארגון, לגנוב מידע אל מחוץ לארגון, לפגוע בזמינות המידע והשירותים וכו'. מעבר לכך, כמות ה-Malwares בעולם עולה מהר כ"כ ובאופן דרסטי כ"כ, שרוב יצרני האנטי-וירוס מפיצים קובץ חתימות כה גדול, אשר משפיע באופן דרמטי מאוד על ביצועי התחנות. **כך, נוצר מצב שבו יצרנים רבים נאלצים להסיר חתימות ישנות מקובץ החתימות, מה שגורם למצב אבסורדי ובו וירוסים ישנים ש"נעלמו" מהעולם לפני שנים רבות, פתאום חוזרים לחיים, ולא מאותרים ע"י אותו אנטי-וירוס שזיהה אותם בעבר.** בעוד זמן לא רב בכלל, בהחלט ייתכן והאנטי-וירוסים הקלאסיים יאבדו מיעילותם עקב גידול אדיר בכמות הנוזקות, וכאמור עקב העובדה שיצרני אנטי-וירוס רבים נאלצים לבחור אילו חתימות להכניס לקובץ החתימות, ואילו להשאיר בחוץ (בדומה ל"סל תרופות").



[עליה דרמטית בכמות הוירוסים. מקור: האתר AV-TEST קישור למקור.]

פתרונות יעילים לצמצום משמעותי של הבעיה

פתרון חלקי לבעיה, הינו הפעלה של **Endpoint Protection** מלא על תחנות הארגון. פתרונות Endpoint Protection, מכיל בתוכם גם את האנטי-וירוס ה"מסורתי" (מבוסס חתימות, ויודע להתמודד רק עם וירוסים שכבר הגיעו ליצרן האנטי-וירוס), אך גם רכיבים אחרים.

Endpoint Protection יכיל מספר רכיבים, כגון:

- "**0-day protection**" - רכיב שמתיימר להתמודד בדיוק עם מקרים של וירוסים חדשים שטרם נכתבה להם חתימה, לרוב ע"י רכיב אשר אמור לזהות אנומליות ו"התנהגות חריגה". נכון להיום, לצערי, הרכיב הזה חסר משמעות אצל הרבה מהיצרנים, מאחר והוא איננו מסוגל באמת לזהות ולהתמודד עם "התנהגות חריגה" של תחנה בארגון, או לחילופין יוצר False-Positive רבים (מקרים שבהם קבצים שאינם מזיקים, מזוהים כזדוניים, וזאת לרוב עקב שיטות פיתוח לא סטנדרטיות של אפליקציות).

- **Endpoint Firewall** - Firewall על תחנות הקצה, המאפשר ניטור ושליטה על התעבורה היוצאת והנכנסת בתחנות הקצה.
בכדי להפוך את רכיב זה ליעיל, יש ללמוד לעומק את סוגי התעבורה המועברת בתוך הארגון. רכיב זה עשוי ליצור "Overhead" משמעותי לאותו גורם בארגון אשר אמון על תחזוקת הרכיב באופן שוטף, וכן עשוי ליצור מקרי "False-Positive" ותקלות משתמשים מורגשות, במידה והרכיב לא ינוהל בצורה מיטבית.

- **Host-based IDS / IPS** מבוסס חתימות (דומה לאנטי-וירוס "מסורתי") רק שרכיב זה עובד בשכבות רשת התקשורת, יעיל מאוד מול תולעים (Worms) ונוזקות אחרות המתפשטות ברשת, כאמור אך ורק אם הנוזקה כבר מוכרת ליצרן.

- **הגנה על קבצי מערכת רגישים** - רכיב אשר מגן על קבצים רגישים במערכת ההפעלה, קבצים אשר לא אמורים להשתנות, לא אמורים לרוץ ע"י קבצים שאינם מתוך מערכת ההפעלה, מונע כתיבה לאזורים מסויימים ב-Registry, ועוד.

קיימים עוד מספר רכיבים כאלה ואחרים, אך לא נתעמק בהם במאמר זה.

לצערי הרב, מעטים הארגונים בארץ המפעילים את רוב הרכיבים הנ"ל בצורה יעילה. רוב הארגונים המשתמשים ב-Endpoint Protection, מתקינים אך ורק את רכיב האנטי-וירוס ה"מסורתי", ולא מתקינים או לא מגדירים נכון את רכיבי ה-IDS / IPS / Firewall או רכיבים אחרים, כך שאפילו גם אם מוצר Endpoint Protection כבר קיים בארגון, השימוש בו ברוב המקרים הוא כאילו היה אנטי-וירוס "מסורתי" בלבד.

בהחלט יתכן וכדאי לשקול בחיוב להטמיע רכיבים נוספים בפתרון ה-Endpoint Protection בתחנות הארגון. בתפעול שוטף של המערכת כדאי לשקול להפעיל הגנות קריטיות וחמורות בלבד, בכדי לצמצם "Overhead" תפעולי. בהחלט מומלץ להכין Policy מוקשח במוצר ה-Endpoint Protection, אותו יהיה ניתן להפעיל בלחיצת כפתור, ב"יום הדין" (במקרה של התפרצות תולעת או Malware אגרסיבים במיוחד).

שאלו את אותם הארגונים שנאלצו להתמודד עם Conficker ותועלים אחרות בשנים האחרונות, אשר הרשת שלהם הייתה מושבתת שבועות, ושנאלצו לעבור עם CD על כל מחשב ומחשב בארגון באופן ידני כי התולעת ניתקה את התקשורת מהתחנות לשרתים, האם הם חושבים שיש צורך ב- Endpoint Protection איכותי, והכנה של "Policy חירום".

הדובדבן שבקצפת כנגד Malwares: טכנולוגיית **Sandboxing.**

מאחר ואת הבעיה שהזכרתי כולם מכירים, התחילו יותר ויותר יצרני מוצרי אבטחת מידע לחפש פתרונות אחרים, רציניים יותר, שיהוו אלטרנטיבה טובה לפתרונות אנטי-וירוס מבוססי חתימות.

רוב מוצרי ה-Sandboxing הקיימים בשוק הם עדיין בחיתולים, אך בהחלט נותנים תמורה טובה מאוד מול איומי 0-day ווירוסים לא מוכרים.

מהי טכנולוגיית ה-Sandboxing?

טכנולוגיית ה-Sandboxing היא בעצם טכנולוגיה המדמה סביבה חיה, ומריצה מערכת הפעלה בסביבה מבוקרת וסגורה, וקבצים מכל מיני סוגים ובוחנת לעומק את התנהגותם, באופן אוטומטי כמובן.

כאשר קובץ מורץ ב-Sandbox, הוא מורץ בסביבה סגורה בה הוא לא יוכל לגרום נזק לרשת הארגון, אך בכל זאת לדמות את התנהגותו (Emulation) של קובץ, דומה ככל שניתן להתנהגותו בסביבה חיה.

מוצרי ה-Sandbox מריצים קבצים ב-Sandbox, ומנטרים מספר פרמטרים שמאפיינים נוזקות ווירוסים, כגון:

- האם נפתחת תקשורת החוצה לרשת מהקובץ המורץ (ואם כן, האם הקובץ אמור לייצר תקשורת החוצה?).
- לאילו ערכים ב-Registry הקובץ מנסה לכתוב (והאם הוא אמור לנסות לכתוב לערכים ב-Registry?).
- האם הוא מנסה לכתוב לקבצים רגישים במערכת ההפעלה, האם הקובץ אמור לשנות קבצי DLL של מערכת ההפעלה, האם הוא מנסה להחליף קבצים ב-Kernel של מערכת ההפעלה, האם הוא יוצר מוטציות לעצמו, מנסה לכשפל את עצמו, ועוד ועוד.

רוב מוצרי ה-Sandbox גם מזיזים את השעון של מערכת ההפעלה (ב-Sandbox) באופן אוטומטי, בכדי לדמות ריצה של הקובץ בזמן עתידי, ובכך מנסים לזהות התנהגות של קבצים המופעלים רק בתאריך מסויים.

יצרני פתרונות Sandbox מסויימים אף מריצים אפליקציות ייעודיות בכדי לזהות התנהגות חריגה גם של קבצים הדרושים אפליקציות אשר **אינן נמצאות Built-in במערכת ההפעלה עצמה**, כגון: Adobe Flash Player, Microsoft Office, Internet browsers, PDF readers ועוד, וזאת על מנת לזהות לא רק קבצי Executable נגועים, אלא מגוון רחב של איומים הנמצאים בקבצים שלעיתים נראים (בטעות) ככאלה שאינם יכולים להזיק (מצגות, קבצי Doc, תמונות, מסמכי PDF, "add-ons" Internet browser ואחרים).

ע"י ניתוח אוטומטי של הפרמטרים הנ"ל, מוצר ה-Sandbox יודע להעריך בצורה יחסית מדוייקת ברוב המקרים, האם הקובץ הינו זדוני או לא.

ארכיטקטורות

קיימים מספר פתרונות Sandboxing, השלושה העיקריים הם Sandbox הממוקם ב-Gateway הארגוני, Sandbox הממוקם כ-Sniffer ברשת הארגון, ו-Sandbox המותקן בתחנות הארגון. Sandbox ב-Gateway: קיימים מספר יצרנים גדולים ומוכרים המייצרים Sandbox הפועל בשכבה שניה או בשכבה שלישית למודל ה-OSI, המאפשרים Emulation אוטומטי ב-Sandbox.

כאשר משתמשי הארגון מורידים קבצים, מוצר ה-Sandbox ב-Gateway מריץ את את אותם קבצים שהורדו אצלו במכונה וירטואלית או שולח אותם לניתוח בענן היצרן, ולאחר הניתוח (שלרוב אורך דקות בודדות), המוצר מדווח למי שהוגדר לו על תוצאות הניתוח.

המשמעות היא שמשתמשי הקצה מורידים ופותחים קבצים, ובמקביל לזה, באופן שקוף למשתמשי הקצה, מתבצע ניתוח אוטומטי של הקבצים שהורדו לתחנות ולשרתים ע"י הרצה שלהם במוצר ה-Sandbox.
הפתרון מהווה מעין "תחנת הלבנה" לתעבורת רשת.

היתרון הבולט בארכיטקטורה זו, היא שהקבצים המגיעים מכיוון האינטרנט נבדקים. מנסיוני, הפתרון יעיל מאוד, ואכן מצליח לזהות קוד זדוני שיצרני האנטי-וירוס ה"מסורתי" אינם מכירים.

Sandbox כ-Sniffer: פתרון זה דומה מאוד למוצרי Sandbox ב-Gateway, אך לעומת Sandbox ב-Gateway, מוצרי Sandbox כ-Sniffer אינם יושבים ב"שערי הארגון", אלא מחוברים ל-Span port (Mirror port - המעתיק את התעבורה באותו VLAN למכונת ה-Sandbox), ומנתח את התעבורה בדומה מאוד ל-

Sandbox הממוקם ב-Gateway של הארגון. גם כאן המשתמשים מורידים קבצים ומוצר ה-Sandbox מקבל את אותם קבצים באופן השקוף למשתמש, ומבצע Emulation של אותם קבצים בכדי לגלות את טיבם האמיתי.

היתרונות בארכיטקטורה זו הם שמוצרי Sandbox הממוקמים כ-Sniffer ב-VLAN, מסוגלים גם לנתח גם תעבורה שמקורה הוא לאו דווקא מה-Gateway, לדוגמא תעבורה המועברת בין תחנות הארגון לבין עצמן, או לשרתים. יתרון נוסף הוא שהטמעה של מוצר ב-Span port לרוב היא הטמעה קלה מאוד (לעומת מיקום מוצר ה-Sandbox ב-Gateway), ובמידה והמוצר מפסיק לעבוד בעקבות תקלה או מכל סיבה אחרת, עבודת הרשת איננה מופרעת.

פתרון נוסף מעניין מאוד, שנכון לרגע זה עוד טרם הבשיל: Sandbox ב-Endpoint. על תחנות הארגון יותקנו Agents, אשר יעתיקו קבצים לא חתומים / לא מוכרים לשרת Sandboxing, או לחילופין יריצו קבצים לא מוכרים ב-Sandbox מוגן בתחנת הקצה.

נכון לרגע זה, טרם נתקלתי במוצר המבצע Sandbox אמיתי ברמת ה-Endpoint, שהגיע לרמת בשלות ו-QA כמו של פתרונות אנטי-וירוס "מסורתי", אך כבר היום יצרנים מובילים בשוק מייצרים פתרונות כאלה, ואין ספק שיצרנים רבים הולכים לכיוון זה. הטמעת מוצרי Sandbox ב"שערי הארגון", כמו כן בתחנות הקצה משפר משמעותית את היכולת הארגונית להתמודד עם איומי 0-day ונוזקות אשר אנטי-וירוס איננו מסוגל להתמודד איתן.

טכנולוגיה נוספת אשר מתגלה כיעילה מאוד, היא שימוש במוצרים אשר מחזיקים Database דינאמי של רשימות שרתי C&C (Command & Control). טכנולוגיה זו יעילה במיוחד מול סוסים טרויאנים ודומיהם.

הסבר קצר: סוסים טרויאנים רבים או "Botnet", יוצרים תקשורת מתוך הארגון לאינטרנט וממתינים לפקודות מהמפעילים. תעבורה היוצאת מתוך הרשת החוצה, היא לרוב תעבורה שקשה מאוד לנטרה, ולרוב היא מתאפשרת בפיקוח מצומצם מאוד. מפעילי הסוסים הטרויאנים, "Botnets", "Keyloggers" ואחרים, יכולים להשיג גישה לארגון, בעצם, מתוך הארגון עצמו, מאחר והנוזקות הנ"ל הן אלו שיוצרות את התקשורת לכיוון האינטרנט ו"מושכות" פקודות מהמפעיל, מבפנים החוצה.

רוב יצרני מוצרי ה-SIEM, יצרני Firewalls מסויימים, פתרונות Content filtering ואחרים, מנהלים Database של שרתי C&C מוכרים, המתעדכנים באופן שוטף. בארגונים רבים רצים Keyloggers וסוסים טרויאנים, ולא תמיד יצרן האנטי-וירוס (ואולי אף יצרן ה-Sandbox) יצליחו לגלות אותם.

המוצר עליו נמצא אותו Database של שרתי C&C, **מסוגל להתריע על תעבורה היוצאת מתוך הארגון לאותן כתובות IP החשודות / ידועות כזדוניות**, ובכך ניתן לגשת ולחקור את אותה כתובת מקור פנימית בארגון, ולנסות להבין האם אכן יש עליה Malware.

עדכון שוטף של ה-Database הוא קריטי במיוחד במוצרים מסוג זה, מאחר ולעיתים מפעילי הסוסים הטרויאנים ושאר הנוזקות מחליפים את כתובות שרתי ה-C&C כל מספר שניות.

הלבנה ו"הלבנה"

בארגון מסויימים נתקלתי בתחנות "הלבנה", אשר אינן באמת תחנות הלבנה יעילות. בארגונים אלו, קיים מחשב "הלבנה" ייעודי, לרוב מנותק מרשת הארגון, אשר מריץ מוצר אנטי-וירוס כזה או אחר, לרוב אותו מוצר אנטי-וירוס אשר מותקן בכל מקרה גם בתחנות הארגון. כאשר עובד מהארגון מעוניין לחבר אמצעי מדיה נתיקה מסוג Disk-On-Key, DVD, USB Drive וכו', לרשת הארגון, הוא מחוייב להריץ סריקה על אותו התקן חיצוני, בטרם הוא מחבר את ההתקן לתחנה ברשת הארגון.

ה"מהדרין" בתחנות "הלבנה" מסוג אלו, אף יריצו מספר פתרונות אנטי-וירוס שונים על אותה תחנת "הלבנה". מיותר לציין שהיעילות של תחנות "הלבנה" מאולתרות מסוג זה היא מוגבלת מאוד, ולא לפתרון זה מתכוונים בתחנת הלבנה "אמיתית" (כמובן שזה עדיף מכלום, אך זה רחוק מההלבנה אליה התכוון המשורר...).

תחנת הלבנה אמיתית, בנוסף לשימוש באנטי-וירוס "מסורתי", תבצע סריקה מעמיקה בקבצים הכוללת בדיקת Mime-type מול סיומת הקובץ, איתור ב-Meta-data וב-Hidden-data של הקובץ, הרצה של תחנת ההלבנה מ-CD / DVD (ובכך למנוע הדבקה אפשרית של מערכת ההפעלה), חסימת סוגי קבצים מסויימים, חסימה ואף הסרה של חלקים ספציפיים בתוך קובץ (כגון: Marco, Flash, וכו').

שימוש בפתרונות אנטי-וירוס "מסורתי", בנוסף לפתרונות הלבנה, ובנוסף לפתרונות Sandboxing, ישפרו משמעותית את התמודדות הארגון עם Malwares.

הגנה מפני וירוסים המגיעים בדואר האלקטרוני

בקצרה, אציין מספר רכיבים חשובים בהגנה מפני וירוסים המגיעים באמצעות הדוא"ל: Mail-relay ארגוני, הכולל אנטי-וירוס "מסורתי". אנטי-וירוס ייעודי לשרתי הדוא"ל. בנוסף לאנטי-וירוס המותקן על תחנות ושרתי הארגון, קיימים מוצרי אנטי-וירוס ייעודיים לפתרונות דוא"ל, לדוגמא: אנטי-וירוס ייעודי ל- Microsoft Exchange.

חשוב להתקין אנטי-וירוס ייעודי למוצרי הדוא"ל, אשר ידע לסרוק את ה-Data הנמצא בתוך מוצר הדוא"ל עצמו, ולא רק ברמת מערכת ההפעלה.

יש המהדרין המקפידים להתקין מספר יצרני אנטי-וירוס שונים לרכיבים שונים: יצרן אנטי-וירוס אחד ל-Mail-relay, יצרן אנטי-וירוס שונה לשרתי הדוא"ל הארגוניים, ויצרן נפרד לתחנות ושרתי הארגון, בכדי להעלות את הסיכוי לתפוס וירוסים מוכרים, ע"י יצרנים שונים.

פתרונות נוספים להגנה מפני Malwares שמקורם באינטרנט

- פתרון יעיל (שיסוקר בקצרה במאמר זה), הוא פתרון Secure browsing. פתרון זה נותן מענה יעיל יחסית, כנגד Malwares שמקורם בגלישת משתמשים והורדות מאינטרנט. פתרון Secure browsing יעיל, יכלול לרוב שרת ייעודי לגלישה באינטרנט, בדר"כ עם גישה מוגבלת לרשת הארגון, עליו יופעל דפדפן מוקשח ומאובטח. **המשתמשים יגלשו לאינטרנט דרך אותו שרת ודפדפן מוקשחים, לרוב ע"י דמוי-דפדפן מקומי מתחנת המשתמש**. כך, Malwares אשר יתקפו את מערכת ההפעלה או את הדפדפן, יתקפו בעצם את השרת הייעודי לגלישה באינטרנט, ולא את תחנות המשתמשים.

- שרת Proxy לאינטרנט (גם כן יסוקר בקצרה במאמר זה) – שרת Web proxy לאינטרנט, אשר רק דרכו משתמשים ושרתים יוכלו לגשת לאינטרנט. מומלץ לדרוש Authentication בשרת ה-Proxy בכדי לגשת לאינטרנט, בכדי להקשות על Malwares ליצור גישה לאינטרנט מתוך הארגון (אשר אין בידם את ה-Credentials של המשתמש). יתרון נוסף בהטמעת שרת Proxy ברשת, הינו "שבירת ה-Session", אשר מקשה על Malwares לנצל פגיעויות קיימות בדפדפן בתחנת הקצה, ויתרונות נוספים.

אירועי אבטחת מידע ארגוניים

בארגונים בהם מתגלים עשרות ומאות וירוסים מידי יום (גם אם הם מוסרים בהצלחה), תמיד עולה אצלי השאלה: כמה Malwares נכנסים לארגון ואינם מתגלים וגם לא יתגלו בעתיד, לעומת כל אלה שנכנסים וכן מתגלים?

ארגון המגלה Malwares רבים מדי יום, צריך לשמוח שהוא אכן מצליח לתפוס אותם, אך גם צריך לחשוש מהכמות, כי סביר להניח שכאשר כמות ה-Malwares שנתפסים גדולה, בהחלט יתכן וגם יש כאלו שאינם נתפסים.

כל "Script kiddy" יודע שפריצה לארגון, גניבת מידע, ביצוע DoS, או כל פעולה עויינת אחרת נגד ארגון, היא במקרים רבים תוצאה של פעילות הדורשת הכנה ארוכה ומורכבת, הכוללת שלבים רבים. במקרים רבים כאשר מושתל Keylogger בארגון, נוספת לכך עבודת הכנה ארוכה. זו טעות לנתק באופן גורף אירועי אבטחת מידע אחד מהשני:

פעמים רבות אין אנו יודעים או יכולים ליצור את הזיקה בין "Port scanning" (לדוגמא) שבוצע מהאינטרנט על כתובת ה-IP הציבורית של הארגון, לבין 50 וירוסים שהתגלו בפרק זמן של שלוש דקות בתחנות של משתמשים, לבין אירוע של זליגת סיסמאות שהתבצע חודש לאחר מכן, אך במקרים רבים קיים קשר הדוק בין האירועים, גם אם לא נדע עליו לעולם.

אירועי אבטחת מידע מורכבים לרוב לא מתחילים ונגמרים במידע סודי של הארגון שנמצא באינטרנט, ברוב המקרים קיימת עבודה הכנה מעמיקה, שהדליקה נורות אדומות רבות, הכוללת בתוכה שילוב של שיטות איסוף מידע ותקיפה רבות, אך רוב הארגונים מתקשים לראות את הקשר בין האירועים.

הפתרונות שהוצגו במאמר זה, בהחלט עשויים לצמצם חלק מאירועי אבטחת המידע בארגון ממוצע.

כמעט ולא הזכרתי במאמר זה פתרונות SIEM (Security Information and Event Management) זאת מאחר ואתייחס לפתרון זה במאמר נפרד ומעמיק, אך פתרון SIEM מלא ואיכותי, שמוגדר ומנוהל היטב (רמז: מעט מאוד ארגונים הצליחו לייצר פתרון כזה בצורה אפקטיבית), בהחלט יכול לסייע בזיהוי, תחקור, וקישור בין אירועי אבטחת מידע שונים.

הרגל מגונה

ארגונים רבים מפרסמים שמות של מוצרים בהם הם משתמשים, או לחילופין מאפשרים ליצרן לפרסם את שם הארגון, תחת רשימת "בין לקוחותינו", לצורכי PR וכו'. חשוב מאוד להבין שכאשר תוקף מתכנן תקיפה על ארגון, כנראה שהוא ינסה לגלות באילו מוצרים הארגון משתמש, ישיג את אותם מוצרים, ויעשה את הנסיונות הפריצה קודם כל אצלו בבית. לדוגמא: כאשר האקר מנסה לכתוב Keylogger או סוס טרויאני לארגון, כנראה שהוא ינסה לגלות איזה אנטי-וירוס קיים בארגון.

לאחר שהוא יגלה שהארגון משתמש באנטי-וירוס "X", הוא יתקין אצלו את אותו אנטי-וירוס, ויפתח את ה-Keylogger או הסוס הטרויאני בצורה כזו שהוא לא יתגלה ע"י אותו האנטי-וירוס.

פרסום המוצרים איתם אנו עובדים בארגון, עשוי להקל במקרים מסויימים את עבודתו של ההאקר, המעוניין להחדיר קוד זדוני לארגון.

סיכום

קיימים כלים רבים ומגוונים למלחמה ב-Malwares, הרבה מעבר לאנטי-וירוס "מסורתי". מנסיוני ולהבנתי, פתרונות Sandbox הם "גולת הכותרת" ואחת הטכנולוגיות המבטיחות בכל מה שקשור לחדשנות וליעילות נגד Malwares, אך במאמר זה נסקרו מגוון רחב של פתרונות כנגד Malwares, מעבר ל-Sandboxing.

תודה על תשומת הלב.

אריק יונאי.