וירוסים, סוסים ותולעים

במחשבי מקינטוש

מאפייני מסמך

מחבר	פולינה זסלבצ'יק, יול בהט
מספר גרסה	1.0
סטטוס	גרסה
תאריך הוצאה	ספטמבר 2010
שם קובץ אלקטרוני	

תשומות / הערות

שם/תפקיד	הערה (אופציונאלי)	תאריך	חתימה

היסטוריה

מ. גרסה	ת. הוצאה	מחבר	שינויים מרכזיים בגרסה
0.1	21/09/10	פולינה זסלבצ'יק, יול בהט	גרסת טיוטה
1.0	21/09/10	פולינה זסלבצ'יק, יול בהט	גרסה סופית

הפצה

מ. גרסה	נמענים

תוכן עניינים

1. כללי.....4

1.1 מבוא 4

1.2 רקע.....4

2. החולשות הגדולות בעולם המקינטוש 6

2.1 ארכיטקטורת החבילה (Bundle).....6

2.2 תיקיית האפליקציות.....7

2.3 ספר טלפונים יחיד 8

2.4 שאננות המשתמשים.....8

3. היסטוריית של התוכנות הזדוניות במחשבי Macintosh.....9

3.1 1982.....9

3.2 1987.....10

3.3 1988.....10

3.4 1990.....10

3.5 1995.....11

3.6 1996.....11

3.7 2004.....11

3.8 2006.....12

3.9 2007.....13

3.10 2008.....15

3.11 2009.....16

3.12 2010.....18

4. סיכום.....19

1.כללי

1.1 מבוא

אחד מהמיתוסים המפורסמים בעולם אבטחת המידע הוא שבניגוד למחשבים המבוססים על מערכת ההפעלה Windows של חברת Microsoft, מחשבים המבוססים על מערכת (או מערכות) ההפעלה של חברת Macintosh הן מוגנות לחלוטין. נושא זה עולה בשנים האחרונות שוב לאור הפופולאריות העולה וגוברת של המכשירים הניידים מבית Macintosh; ה-IPhone ובני דודו ה-iPod וה-iPad, כולם מבוססים על מערכות הפעלה מלאות לכל דבר ועניין.

אנו משתמשים במילה מיתוס, מכיוון שנראה כי על פי דעת הקהל (הלא מודע, כמובן), וירוסים ושאר זודנות ופוגענים הם מושגים שקיימים רק בעולם המייקרוסופטי, ולא בעולם ה-Mac, תפיסה אותה נפריך במסמך זה.

יש לומר כבר כאן, במבוא למסמך, כי ללא ספק אין מקום להשוואה בין כמות הפרצות הידועות, הוירוסים הפעילים והסוסים הטרויאנים הנפוצים עבור Windows ובין המקבילים ב-Mac לסוגיו השונים. עם זאת, אין הדבר אומר שאין סכנה, ואין סכנה יותר גדולה מאשר הסכנה אליה אנו לא מודעים כלל.

מסמך זה לא ינסה לטעון כי מערכת הפעלה אחת טובה או בטוחה יותר מאחרת, אלא רק יציג מעט רקע היסטורי, ובתקווה יעלה את המודעות לנושא בקרב קהל המשתמשים.

1.2 רקע

מקינטוש (באנגלית: Macintosh), או בקיצור מק, הוא במקור שמה של סדרת מחשבים אישיים המעוצבת, מיוצרת ומשווקת על ידי חברת אפל. מחשבים אלו פועלים באמצעות גרסאות שונות של מערכת ההפעלה Mac OS, אשר נרחיב עליה בהמשך. מקור השם "מקינטוש" בשמו של זן תפוחים, בעקבות שם החברה ("תפוח" בעברית). מחשב המקינטוש הראשון יצא לשווקים ב-24 בינואר 1984.

המקינטוש היה המחשב המסחרי הראשון שלו ממשק משתמש גרפי ועכבר, בניגוד לממשק שורת הפקודה שבמערכות הפעלה אחרות. במקביל למקינטוש, המשיכה אפל בייצור מחשבי Apple II שלה, שהיו עד אז מקור ההכנסה העיקרי של החברה, עד שמחשבי המקינטוש האפילו עליהם החל מ-1987.

המקינטוש המשיך לאורך השנים לעמוד בחזית הטכנולוגיה בתחום המחשוב האישי, עם חידושים כגון אפשרות פשוטה לרישות, צג צבעוני והצגת סרטים

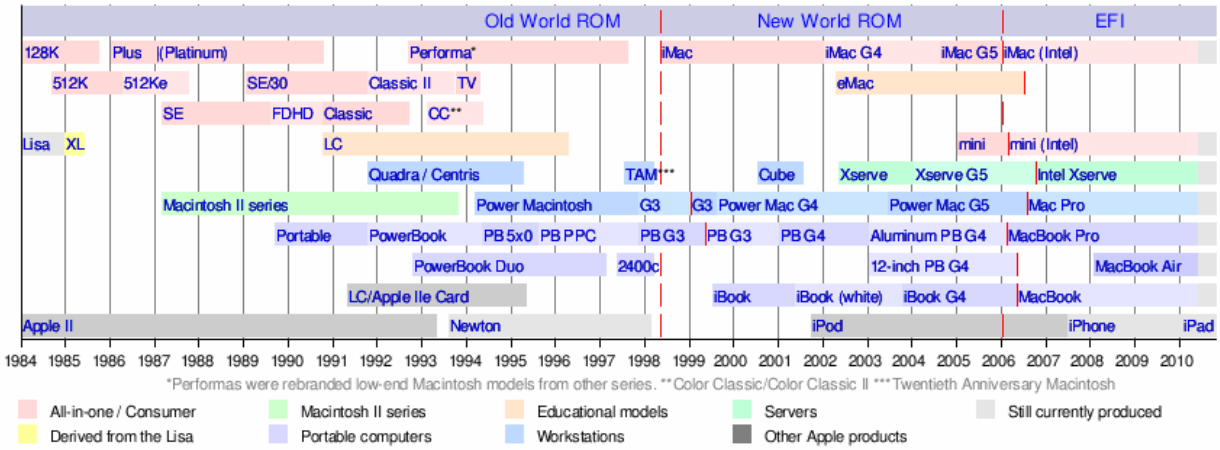
ונגינת מוזיקה. המק גם היה אחד הגורמים המרכזיים במהפכת המחשוב בתחום הגרפיקה, ההוצאה לאור, המוזיקה והוידיאו. כמובן שאין לשכוח להזכיר גם את המהפיכות שביצעה החברה בתחום המחשבים הניידים, החל מהוצאת ה-PowerBook בשנת 1991 ועד ל-MacBook Pro ו-MacBook Air של ימינו.

עד 1998 התבססו מחשבי המק ("מקים") בעיקר על טכנולוגיה וחומרה ייחודיים של אפל. באותה שנה החלה אפל לעבור בהדרגה לטכנולוגיה וחומרה סטנדרטיים, עם המעבר לשימוש ביציאות USB, שבבי זיכרון סטנדרטיים ועוד. בשנת 2005 הכריזה אפל על כוונתה להעביר את קו מחשבי מקינטוש לשימוש במעבדי אינטל, שיחליפו את מעבדי ה-PowerPC ששימשו עד אז. בתחילת 2006 יצאו הדגמים הראשונים המבוססים על מעבדי אינטל.

כמו כן, כמובן, ישנם גם מכשירי ה-iPod, ה-iPhone וה-iPad, שרבים שוכחים שהם מחשב לכל דבר, ומבוססים על מערכת ההפעלה iOS, שהיא בתורה מערכת הפעלה המבוססת על מערכת ההפעלה העדכנית של מחשבי המק - Mac OS X, שבתורה היא מערכת הפעלה מבוססת Unix.

ככל שהחומרה הופכת קטנה ויעילה יותר בצריכת אנרגיה, כך הגרסאות הניידות של OS X יהפכו לחלק הולך וגדל מקו המוצרים של אפל. האייפון המקורי, עליו הכריזה אפל בתערוכת Macworld 2007, כבש את עולם הסלולר בסערה שישה חודשים לאחר מכן, כאשר הגיע לשוק. ממשק המשתמש שלו, שכלל טכנולוגיות שהיו עד אז בלעדיות למחשבים אישיים, עשה לתעשיית הסלולר מה שהמקינטוש המקורי עשה בשעתו לתעשיית המחשבים האישיים. ועם כל עדכון נוסף של תוכנת ה-iPhone, הוא ובן-דודו ה-iPod Touch צברו עוד ועוד מאפיינים, השתפרו מבחינת ביצועים, ובסופו של דבר, עם פתיחתה של App Store על מאות היישומים הקיימים בה, הפכו הלכה למעשה לפלטפורמה אמיתית שיש לקחת בחשבון בכל המובנים, ובכללם אבטחת מידע.

להלן קו הזמן של מוצרים של דגמים של Macintosh.



2.החולשות הגדולות בעולם המקינטוש

2.1 ארכיטקטורת החבילה (Bundle)

במערכות הפעלה מקינטוש אפליקציות משתמשות בארכיטקטורה שנקראת Bundle. זוהי בעצם טכניקה בה תיקיות שלמות שמכילה קבצים שונים נראות כמו קובץ בודד. היתרון של שיטה זו הוא שמשאבים רבים נמצאים באותו המקום ומנקודת המבט של המשתמש זה קובץ אחד בודד. (ישנו גם יישום דומה לשיטה זו גם ב Microsoft; קבצי docx הם בעצם מספר קבצים מכווצים, אך שם לא מדובר בקונספט שלם עליו מבוססת מערכת ההפעלה). הדבר מקל מאוד על מפתחי התוכנה, מכיוון שהם יכולים להיות בטוחים בהימצאותם של רכיבים\קבצים בתיקיה, ולא להסתמך על קיום תיקיות מערכת מסואבות ומרכזיות. בסופו של דבר, בארכיטקטורה זו נוצר קובץ הרצה שמתאים לפלטפורמות שונות (Classic Mac OS, PowerPC או Mac OS מבוסס Intel), וכן קבצי אפליקציה בהם יש את כל הגרפיקה של הפקדים, חבילות \תיקיות של קבצי עזרה ורכיבים נוספים אחרים.

למשל כך ניראה קובץ iTunes.app

אבל "הקובץ" בעצם מכיל קבצים רבים:

ארכיטקטורה זו מסייעת לכותבי התוכנות הזדוניות על ידי כך שהם יכולים להחדיר לחבילה קוד הרצה זדוני; למשל לקחת קובץ הרצה של iTunes הנמצא בתת תיקיה MacOs ולהחליף את שמו לשם אחר ולשתול קובץ ההרצה בשם iTunes שיכיל קוד הרצה זדוני. ברגע שהמשתמש יריץ את הקובץ יורץ קוד זדוני, באיזשהו שלב הקוד הזדוני יריץ גם את הקוד המקורי בכדי שהמשתמש לא יחשוד.

2.2 תיקיית האפליקציות

במערכת הפעלה Mac, בדומה למערכות Unix, ישנה תיקיה בשם Applications\ שבה נמצאות כל האפליקציות, כולל קוד ההרצה שלהן (ראה סעיף קודם). לכל אפליקציה יש הרשאות להשתמש בתיקיה זו, כולל יצירת קבצים ותיקיות. זאת אומרת, שקוד זדוני שמותקן בתיקיה, עלול להיות מסוגל להחליף קבצים של אפליקציות אחרות או להתחזות לתוכנה תמימה מבלי להשאיר עקבות.

2.3 ספר טלפונים יחיד

משתמשי מערכת Mac נהנים מספר טלפונים אחד ויחיד. הספר כולל שמות, כתובות פיזיות, כתובות דואר אלקטרוני, טלפונים, כתובות של חברים בתוכנת המסרים המידיים וכו'. נתונים אלו זמינים עבור כל האפליקציות במערכת ההפעלה. במקרה של מחיקת רשומה כלשהי, היא לא באמת נמחקת, אלא המערכת פשוט מסמנת את הרשומה בתור רשומה מחוקה על מנת שאם המשתמש מסנכרן מספר מכשירים, מכשיר שממנו נמחק הנתון יוכל בעתיד לעדכן מכשירים אחרים על המחיקה. הדבר יכול מאוד להועיל לכותבי תוכנות זדוניות, מכיוון שהם יכולים להשיג מסד נתונים עם כתובות רבות, היכולות לשמש את התוכנה הזדונית על מנת על מנת להפיץ את עצמה.

2.4 שאננות המשתמשים

כאמור, הבעיה העיקרית בנושא אבטחת המידע במק היא לאו דווקא הטכנולוגיה שלה, אלא המיתוס, אותה גישה של משתמשי המחשבים, אשר לא שמים לב כלל לאבטחת המידע ומתייחסים אליה בקלות ראש. שוק תוכנות ההגנה (תוכנות Anti-Virus, Anti-Malware, Personal Firewall וכו') למחשבי מק קטן משמעותית מנתח השוק הכללי של המחשבים האלו בעולם.

גישה לא זהירה זו גורמת לשאננות וליקויים בקבלת החלטה בעת התמודדות עם איום תוכנות זדוניות.

3.היסטוריית של התוכנות הזדוניות במחשבי Macintosh

3.1 1982

היסטוריית הווירוסים למחשבים מתחילה כמעט מאז הופעת המחשבים הלא תעשייתיים הראשונים, אי אז בסוף שנות ה-60 ותחילת שנות ה-70. עם זאת, הווירוס הראשון אי פעם שהצליח להתפשט אל מחוץ "למעבדה" בה הוא נכתב, נועד דווקא למחשבי Apple2 של חברת Apple. הווירוס נכתב ע"י תלמיד תיכון בן 15 בשם Rich Skrenta. שמו של הווירוס היה Elk Cloner, והוא התפשט בעזרת דיסקטים. ברגע שהוכנס דיסקט שהכיל וירוס, ובוצע boot מהדיסקט, הווירוס טען את עצמו לזיכרון. כאשר הוכנס דיסקט ללא ווירוס, הווירוס הועתק לדיסקט ה"נקי" אל אזור ה-Boot Sector.

הווירוס לא ממש גרם לנזק, אלא הציג שירון כאשר בוצע Boot בפעם ה-15.
תוכן השיר היה:

Elk Cloner: The program with a personality

It will get on all your disks
It will infiltrate your chips
Yes, it's Cloner!

It will stick to you like glue
It will modify RAM too

Send in the Cloner!

כפי שעוד נראה, היסטוריית הווירוסים המיועדים לשוק המקינטושי רוויה בווירוסים ותולעים שלא נכתבו כדי לעשות נזק, אלא רק כדי להוכיח כי וירוסים במקינטוש זה דבר אפשרי.

3.2 1987

nVir זוהי בעצם משפחה של וירוסים, שנועדה לתקוף מערכות Macintosh מגרסה 4.1 עד 8. מכיוון שהקוד של הווירוס, שפורסם כקוד פתוח, מאוד נגיש, נוצרו מספר גרסאות של הווירוס. הווירוס מדביק אפליקציות במחשב, ולמעשה גורם לאפליקציה "לקפוץ" לקוד הזדוני. ברגע ההתקנה של הוירוס נותר מונה המאותחל ל-1000. בכל אתחול של המחשב יורד ערכו של המונה ב-1, ובכל הרצה של אפליקציה מודבקת ערכו יורד ב-2. כאשר ערך המונה יורד מתחת ל-0, בכל פעם שהמונה מגיע לכפולה שלילית של 8, המחשב מצפצף. אם מותקנת על המחשב התוכנה MacinTalk, אז במקום לצפצף המחשב אומר "Don't Panic"[1]. כאמור, ישנן גרסאות רבות של הווירוס, וחלקן אף שונו כך שיהיו זדוניות, ומוחקות קבצי מערכת וגורמות להפלתה.

3.3 1988

בשנת 1988 התגלו לראשונה וירוסים שנועדו לתקוף את תוכנת HyperCard. תוכנת ה-HyperCard היא בעצם פלטפורמת פיתוח למערכות Apple, וייעודה הוא עיצוב אפליקציות גרפיות בצורה נוחה (פלטפורמה זו סללה את הדרך לפלטפורמות כגון Borland Delphi או Visual Basic שהופיעו מספר שנים לאחר מכן עבור מערכת ההפעלה Windows 3.1). ה-HypeCard התבססה על רעיון של "מחסנית" (Stack) של "כרטיסיות" (Card), כאשר כל כרטיסייה ייצגה פריט כלשהו, ומחסנית ייצגה משהו בדומה לדף או ל-Form. ישנה גם כרטיסייה ראשית בשם Home. בשנת 1988 החלו לצוץ וירוסים ראשונים ל HyperCard, שהיו נצמדים לתוכנות שפותחו באמצעותה.

3.4 1990

ב-1990 נוצר וירוס בשם mdef. הווירוס שינה את המשאבים האחראים לציור של התפריטים בתוכנות שונות. לווירוס לא הייתה מטרה זדונית פרט להתפשטות, אך עקב "באג" הוא גרם לעיתים לקריסה של מערכת ההפעלה, ולמעשה נחשב לאחד הווירוסים ההרסניים ביותר במערכות מבוססות Mac.

---

[1] כמחווה לספר "המדריך לטרמפיסט בגלקסיה"

3.5 1995

בשנת 1995 חברת Microsoft יצרה, ככל הנראה בטעות, את הווירוס הראשון שהשתמש במאקרו של Word. הווירוס הופץ כחלק מתוכנת Word על גבי דיסק ההתקנה. ווירוס זה היה ייחודי מכיוון שהוא היה הווירוס הראשון שתקף הן מחשבי Mac והן מחשבי PC, ולמעשה תוקפים רבים התבססו עליו על מנת ליצור משפחה שלמה ווירוסים וקוד זדוני אשר יכול לפעול בשתי הסביבות.

3.6 1996

בשנת 1996 יצא הווירוס הראשון לתוכנת Excel. הווירוס השתמש בשיטות דומות לאלו המתוארות בסעיף הקודם, כלומר באמצעות מאקרו זדוני. הווירוסים של Excel לא פגעו במערכות Mac עד הופעתו של Excel 98, שהיה מיועד גם למחשבי Mac. בשנה זו פתאום הייתה עלייה בתקיפות מחשבי ה-Mac, ורבים מקשרים בין שני המקרים.

3.7 2004

בשנת 2004 יצאה תולעת Renepo שהכילה Script אשר ביצע מספר פעולות זדוניות, וביניהן הקלטה של הקלדת סיסמאות, פתיחת ערוץ SSH אחורי, שיתוף קבצים, סריקה של המחשב על מנת למצוא סיסמאות ובסופו של דבר שליחת נתונים דרך ftp או דואר אלקטרוני. כמובן, מכיוון שהתולעת פתחה ערוץ אחורי, ניתן גם היה להשתלט על המחשב מרחוק.

בשנה זו יצא גם סוס בשם Amphimix-A, שמטרתו הייתה הוכחת עיקרון (Proof of Concept). הסוס התחזה לקובץ mp3. הקובץ ניראה כקובץ mp3 תמים, אך ברגע שמריצים את הקובץ מוצגת הודעה :

התוכנה טענה קובץ בשם Amphimix לתוך הנגן iTunes. בתוך הקובץ היה רכיב שהכיל מנגינה בשם "Wild Laugh", שהכיל 4 שניות של צחוק. התוכנה לא גרמה לשום נזק, אלא רק הוכיחה כי אפשרי להריץ ולהציג אפליקציה כקובץ נגינה.

3.8 2006

ב2006 יצא הווירוס Leap-A שהיה הווירוס הראשון שהופץ דרך תוכנת המסרים המידיים iChat. המשתמש קיבל קובץ מכווץ בשם "latestpics.tgz". הקובץ הכיל מה שנראה כתמונה, אבל לא כך הדבר, זהו קובץ הרצה.

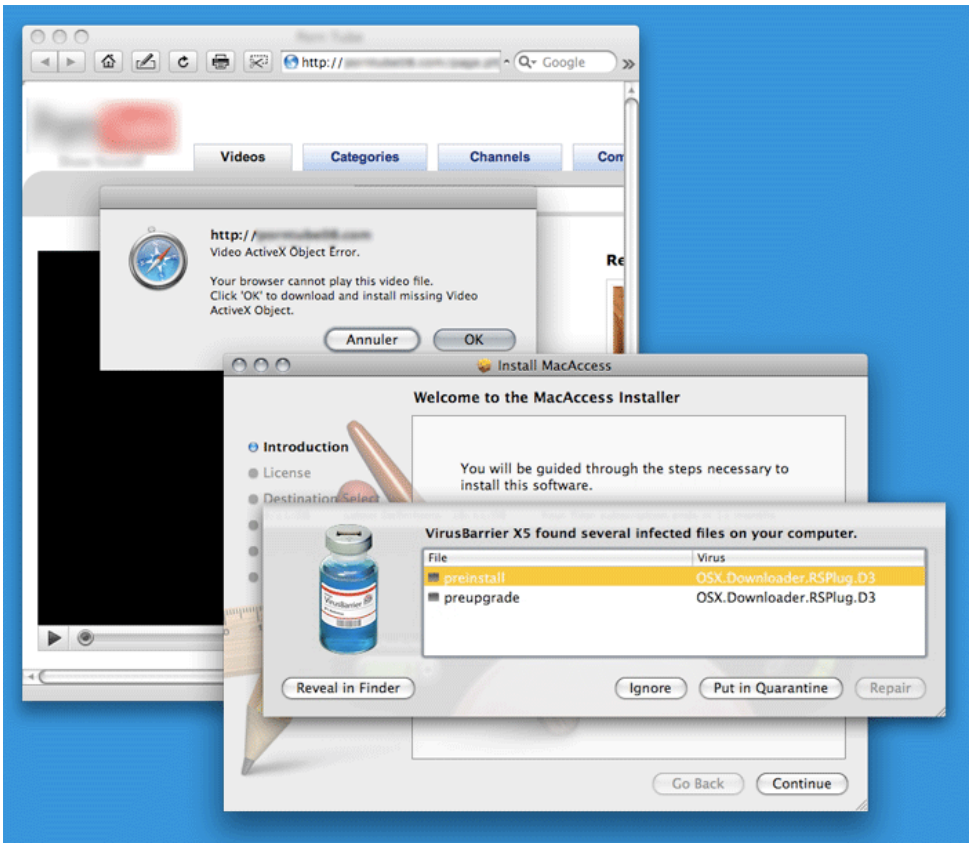
הוירוס החדיר רכיב ששלח לכל החברים (Buddies) את הקוד הזדוני. לאחר מכן הווירוס ניסה להדביק אפליקציות שנמצאות במחשב ע"י העתקה של קובץ ההרצה של האפליקציה בשם אחר, ויצר קובץ זדוני במקום קוד ההרצה. במהלך הריצה התוכנה הזדונית הריצה גם את הקוד המקורי אך היה "באג" בקוד, והוא לא הצליח להריץ את האפליקציה, ולכן היה מאוד קל לזהות את הווירוס ברגע שהמחשב היה נגוע.

Inqtana הוא גם תולעת שנוצרה באותה השנה על מנת להוכיח עיקרון. התולעת מנצלת חור אבטחתי מסוג Directory Traversal ב Bluetooth. הווירוס שלח 3 בקשות OBEX Push (פרוטוקול להעברת קבצים בינאריים). אם המשתמש מסכים לקבלת המידע, התולעת יצרה קבצים ותיקיות במחשב המודבק (תוך ניצול החור האבטחתי), וניסתה לאתר מכשירים שמחוברים למחשב באמצאות Bluetooth בכדי להדביק גם אותם.

3.9 2007

הווירוס BadBunny נכתב גם הוא על מנת להוכיח עיקרון. הווירוס הופץ ע"י מסמך OpenOffice/StarBasic בשם badbunny.odg שהכיל מאקרו. המאקרו הכיל קוד שמשפיע על מערכות הפעלה של Windows, Mac OS, ו-Unix. בכל מערכת הווירוס ביצע פעולות שונות.

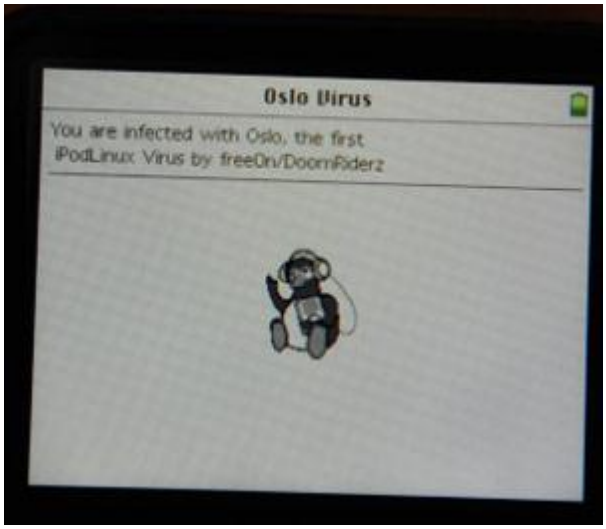
בשנה זו יצא גם סוס טרויאני השם RSPlug. הסוס הציג את עצמו כ Codec שיעזור לאנשים לצפות בסרטון. כאשר גולש תמים ניסה לצפות בסרטון, הוצגה למשתמש הודעה שהוא צריך להתקין codec על מנת לצפות בסרטון, אם המשתמש הסכים להתקין את הקובץ הוא בעצם הוריד והריץ את הסוס במחשבו. לאחר ההדבקה הסוס שינה רשומות DNS של המערכת והפנה את המשתמש לאתרים אחרים. הסוס לא ניצל שום חור אבטחתי אלא ניצל את השאננות של משתמשי mac, שחושבים שהמערכת שלהם בטוחה.



בשנה זו יצא הסוס הטרויאני הראשון ל iPhone בשם 113 prep, ובישר את פתיחת העידן החדש של וירוסים ייעודיים Smartphone. הסוס הגיע בתור תוכנה בשם 113 prep, ותקף רק מכשירים פרוצים (jailbroken). בעת ריצה רגילה הסוס לא גורם נזק, אלא פשוט מציג את ההודעה "shoes". לעומת זאת, אם מסירים את התוכנה, ההסרה מנסה למחוק את תיקיית bin/, ובמידה והצליחה הדבר פגע בתפקוד של אפליקציות רבות אחרות. מי שכתב את הסוס הוא ככל הנראה ילד בן 11.

גם ה מכשיר ה-iPod נפגע מתוכנה זדונית בשנה זו. וירוס בשם Podloso נכתב במיוחד ל-IPod שמותקן עליו Linux. במקרה זה כותב הווירוס רצה להתריע על שאננות המשתמשים, ולהראות כי במובנים מסוימים, iPod הוא מחשב לכל דבר. הווירוס לא יכול להריץ את עצמו ללא הרצה מכוונת על ידי המשתמש. ברגע ההרצה של התוכנה, הווירוס סורק את התיקיות וקבצים במכשיר, ופוגע בכל קבצי ההרצה. אם מנסים להריץ קובץ מודבק, מוצגת ההודעה:

"You are infected with Oslo, the first iPodLinux Virus"



2008 3.10

בשנה זו יצא תוכנה בשם MacSweeper, תוכנה זו יכולה להיות מותקנת בצורה נסתרת מבלי ידעה של המשתמש או כתוסף לתוכנות אחרות. לאחר התקנה, התוכנה הודיעה כי במחשב ישנם איומים אבטחתיים (שלא באמת קיימים) וקבצי זבל (שחלקם קבצי תוכנות לגיטימיות). אם ברצונו של המשתמש להיפטר מהאיום, עליו לשלם סכום של $39.99 בכדי לקבל את הגרסה המלאה של התוכנה.

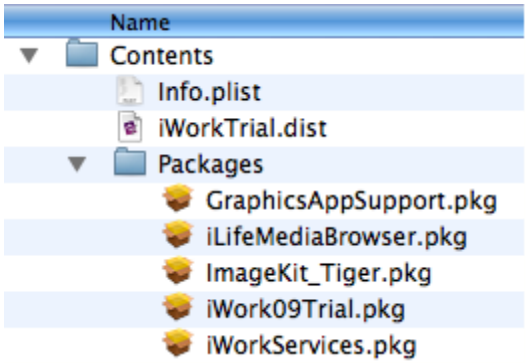
OSX/Hovdy-A הוא סוס אשר מנצל חור אבטחתי של Apple Remote Desktop Agent. מטרת הסוס היא גניבת סיסמאות. הסוס פותח פורטים ב-Firewall המקומי, מוחק קבצי לוג, מנטרל כתיבת לוגים, מבטל עדכונים של המערכת, מנטרל תוכנות אנטי וירוס ופותח סרוויסים של vnc, ssh ו-ard. הסוס בעצם משאיר את המערכת פרוצה לגמרי, כי ברגע שהמשתמש מאשר את הרצת הסוס, הוא מקבל הרשאות Root.

בשנה זו יצא גם סוס בשם Troj/RKOSX-A אשר פתח Backdoor במחשב, והעתיק את עצמו כך שבכל אתחול מחדש של מחשב הוא ירוץ.

בשנה זו התגלה גם סוס בשם OSX/Jahlav-A. צורת ההדבקות שלו הייתה דומה לצורתו של RSPlug. כאשר הקורבן ניסה לצפות בסרטון פגוע באתר כלשהו, הוא קיבל הודעה שישנה שגיאת ActiveX ובאפשרותו להוריד תיקון לבעיה. אם המשתמש היה מסכים להורדה של התוכנה מתבצעת בדיקה של סוג מערכת ההפעלה של הקורבן. אם הקורבן משתמש במערכת Windows אזי הורד למחשבו של הקורבן קובץ an.EXE ואם מערכת Mac OS אזי הורד קובץ a.DMG. לאחר ההרצה נוצר job/Corn מתוזמן שמריץ קוד Perl הפותח ערוץ תקשורת TCP בפורט 80 מול שרת שליטה ובקרה. בערוץ זה מועבר משרת השליטה קוד זדוני והלקוח שולח לשרת נתוני רגישים כגון סוג מערכת ההפעלה, סוג מעבד, וכתובת IP.

3.11 2009

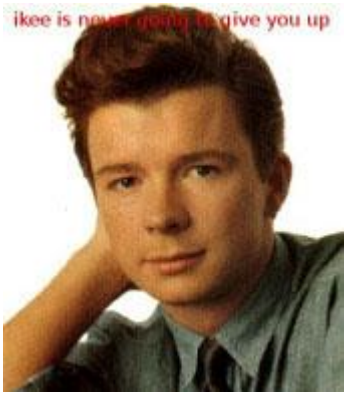
בתחילת השנה התגלה סוס בשם OSX.Trojan.iServices.A או OSX/iWorkS-A Trojan אשר הופץ כגרסה לא חוקית של תוכנת iWork, בעיקר בעזרת תוכנות שיתוף קבצים. הסוס מכיל גרסה של התוכנה וגם כולל קוד זדוני בשם iWorkServices.pkg.



מהרגע שהמשתמש מתקין את התוכנה, מתחילה לרוץ גם ההתקנה של הסוס, שבאחד השלבים גם דורשת הקלדה של סיסמאת Administrator. הדבר כמובן נותן הרשאות מלאות לסוס. הסוס רושם את עצמו בתיקיית StartUp, המאפשרת הרצה של הקוד הזדוני בכל עליה של המערכת. הסוס פותח ערוץ תקשורת מול שרת שליטה ובקרה ומשדר ב broadcast על הימצאותו.

בחודש מרץ של אותה השנה, יצאה גרסה חדשה של OSX/RSPlug אשר התחזתה לתוכנה לצפייה של סרטים הפורמט HDTV בשם MacCinema.

בשנה זו יצאה תולעת בשם iKee, שהייתה התולעת הראשונה למכשירי iPhone. התולעת תוקפת רק iPhones פרוצים (JailBroken). התולעת משתמשת בעובדה שברוב המקרים המשתמשים לא משנים את סיסמת ברירת מחדל לרכיב ה-SSH אם הם מתקינים אותו (צעד הכרחי בתהליך פריצת המכשירים). לאחר התקנה מוצלחת, התולעת מחפשת מכשירים פרוצים ברשת שהמכשיר מחובר אליה. התולעת לא גורמת נזק, היא רק מחליפה את תמונת שולחן העבודה לתמונה של ריק אסטלי עם הכיתוב " ikee is never going to give you up"[2]



היוצר של התולעת היה סטודנט אוסטרלי בשם אשלי טאוונס (Ashley Towns), שרצה להראות אנשים את הקלות שניתן להשתלט על מכשיר ה iPhone. הבחור טען שבסריקה פשוטה שהוא ביצעה הוא מצא 27 מכשירים שהתקינו SSH וב-26 לא שונתה סיסמת ברירת המחדל.

בשנה זו גם יצוא שתי גרסאות של תולעת בשם Tored, אשר גם היא, באופן מפתיע, ניסתה להוכיח עיקרון. התולעת פותחה בשפת RealBasic, והיא ניסתה ליצור רשת של מחשבים זומבים בשם Raedbot. התולעת גם ניסתה לאסוף מרכיב ה-AddressBook כתובות דואר מהמחשב המודבק ולהפיץ את עצמה. עם זאת, שגיאות בקוד ובגוף המייל המופץ גרם לבעיות רבות בהפצה, ולכן ישנו סיכוי מאוד קטן להידבקות.

הנושא של המייל הוא :

For Mac OS X ! :(If you are not on Mac please transfer this mail to a Mac and sorry for our fault :)

בתוך הקוד היה רשום :

"RESPECT about what are you talking about me (cybercriminal..) Don't say what you ignore!!!!!!!!

[2] הכיתוב נוצר בהשפעת תופעת ה-Rickrolling שהחלה באותה שנה. מידע נוסף על התופעה ניתן לקרוא כאן: http://en.wikipedia.org/wiki/Rickrolling

3.12 2010

בשנה זו הופיע Spyware בשם OSX.OpinionSpy מותקן למחשב בזמן התקנה של אפליקציות אחרות כגון אפליקציות של שומרי מסך או Video Plugins. התוכנה מותקנת עם הרשאות root. התוכנה פותחת Backdoor בפורט 8254, ואוספת נתונים של תעבורה גם באינטרנט וגם ברשת הפנימית. התוכנה סורקת את הקבצים במחשב, אוספת את כל ההתכתבויות בiChat במיילים כולל כתובות ואת כל הנתונים שולחת לשרתי שליטה ובקרה בצורה מוצפנת בפורט 80 או 443. ישנם גם מקרים של הידבקות שלאחר זמן מה של פעילות המחשבים מפסיקים לעבוד כראוי ונדרש לבצעה Reboot.

4.סיכום

ללא ספק, הסכנות הקיימות לשוק מחשבי ה-PC מבוססי מערכת ההפעלה Windows גדולים בצורה משמעותית מאלו של המכשירים מבוססי מערכות ההפעלה של Apple. עם זאת, אי אפשר להתעלם מהפוטנציאל הקיים ואף ממומש לתוכנות זדוניות מסוגים שונים ומגוונים, אשר נכתבים במטרה תחילה כדי לתקוף מערכות מבוססות Mac.

בין אם מדובר במחשבי Macintosh "רגילים", מבוססי מערכת ההפעלה MacOS לדורותיה השונים, ובין אם מדובר במכשירי iPhone, iPod, iPod Touch, iPad או כל מכשיר עתידי מבית Apple, מדובר במחשבים לכל דבר, עם מערכת הפעלה לכל דבר, וסכנות ממשיות לכל דבר.

מסמך זה נכתב כדי להעלות את המודעות בקרב המשתמשים השונים לסכנות אלו, ולבקש כי לא יניחו בקלות דעת כי הם מוגנים מפני הסכנה. המחשבים והמכשירים הניידים שלנו מכילים את כל המידע הרגיש עלינו, שבוודאי לא היינו רוצים שיגיע לידיים הלא נכונות. גם לא היינו רוצים לסייע באופן לא מודע לתקיפה של מכשירים אחרים השייכים לאנשים ברשת החברתית שלנו.

אנא, היו מודעים, התנהגו בחוכמה, והתקינו את אמצעי ההגנה הנדרשים, לפחות הבסיסיים שבהם, בדיוק כפי שהייתם עושים במחשבי ה-Windows שלכם.