קורא יקר,

וירוסים, פרצות וספאם הולכים ומתרבים מיום ליום **באופן מבהיל.** מערכות המחשוב הופכות למורכבות וסבוכות. במקביל, הפס הרחב, הוירטואליזציה, BI - מציעים **הזדמנויות חדשות ומלהיבות** וגם תפקיד מנהלי המחשוב עובר טרנספורמציה **דרמטית ומבטיחה**. כך, לנוכח שטף חידושים וגלי תמורות, שרק מתעצמים ומואצים, קשה להתמקד במה שבאמת חשוב. **למי להאמין? על מי לסמוך?**

תחקירי PCאון מספקים בכל שבוע ריכוז של החדשות החשובות ביותר בעולם המחשוב והתקשורת, יחד עם תחקיר מקצועי שמתמקד בנושא מפתח מרכזי ומשמעותי. הם משרתים חלק גדול ממנהלי המחשוב המובילים של מדינת ישראל. חלקם מנויים לשירות קרוב לשש עשרה שנים כיוון ש:

- PCאון הוא מקור מידע **אמין ותכליתי.** הוא מתמקד רק **בנושאי המפתח** החשובים ביותר בעולם המחשוב והתקשורת, והוא **מדבר בשפתך המקצועית.**
- PCאון כולל את ריכוז **החדשות החשובות** ביותר וגם **מגמות, טיפים, ידע יישומי ושימושי** נוסף. הוא מאפשר בהשקעה של **פחות מ-10 דקות** בשבוע, להיות כל הזמן **עם יד על הדופק.**
- PCאון מביא תועלת בכך שהוא **רלוונטי לבעיות הנוכחיות שלך,** בנוסף לכך, הוא מסייע לך בהערכות מוקדמת בפני **סכנות ואיומים** למערך המחשוב **ו/או ניצול הזדמנויות עסקיות** חדשות.
- ניתן **להתרשם ממנו באופן אישי** באמצעות תחקיר הדוגמא המצורף או להסתמך על למעלה ממאה חוות דעת של מנהלי מחשוב מובילים (ראה - www.pcon.co.il/v5/103.asp).

PCאון נתפס כיום כ**מפתח מוכח להצלחה מהירה,** וככזה גם אתה תוכל ליהנות ממנו בקרוב. כמו ארגונים רבים תוכל להצטרף כמנוי ארגוני ותאפשר לכל העוסקים במחשוב בארגונך, ליהנות מכל היתרונות שלמעלה.

מחירי מנוי השנתי בגין 52 תחקירים:

מספר מנויים	המחיר בדולרים + מע"מ
1	516
5	1270
10	1970
20	3270
50	5970
100	7700
200 ויותר	9700

נכון, אפשר לנסות להתמודד לבד עם כל התמורות. להתעלם או לדגום מאמר אקראי ולקוות לטוב. **תחשוב על התוצאות.** מצד שני ניתן ללכת **בדרך סלולה ובטוחה** שבה הולכים המובילים במחשוב הישראלי, שגם ימשיכו להוביל בבטחה. כדי להצטרף אליהם, ללכת יחד איתם, אפשר לקרוא על תחקירי PCאון ולהצטרף באתר ב- www.pCon.co.il/promo טלפון 03-9667939, פקס 03-9660310 או מייל - sub@pcon.co.il

קובי שפיבק
העורך הראשי של PCאון

נ.ב. על כל תחקירי PCאון חלות כל ההגנות החוקיות של זכויות יוצרים. ביחד עם זה, אנו מתירים לשכפל ולהפיץ את תחקיר זה, **מבלי לשנותו, עד 31.12.2007 ורק יחד עם דף היתר זה!** למנהלים, עמיתים ואנשי מחשוב נוספים, שעשויים לדעתך למצוא בו עניין.

מה אתה מקבל? - מפתחות להצלחה

קורא יקר,

תיזכר ב"נפילה" האחרונה של מערכת בארגון, ב"פספוס" בבחירת טכנולוגיה, בפרוייקט שלא "סיפק את הסחורה". מדמיין? עכשיו קח לך פחות מחצי דקה ותחשוב על מי שקרא תחקיר דומה, לפני כשנה. באינטואיציה פנימית חזקה הוא הבין שמצא פיתרון אמיתי לצורך אמיתי - להיות ממוקד באיומים האמיתיים וההזדמנויות המבטיחות שרלוונטיים לארגון ולתפקיד שלו, למציאות שבה הוא חי. שוב ושוב הוא נוכח מאז, שהוא מתבסס על מקור מידע שמדבר אליו בשפתו, מקור תכליתי ואמין.

כאשר חבר קרוב מתקשר ושואל לחוות דעתו על תחקירי PCאון. "מה הם נותנים לך באופן מעשי?" באופן טבעי הוא נזכר ומספר על כמה מהדוגמאות הבאות:

- **בתחקיר - ה-IT מאיץ חדשנות** - הוא גילה את הטרנספורמציה שעוברת היום כגל סוחף בעולם העסקי. ה-IT הופך מכלי שתומך בעסקים, למנוע שמאיץ חדשנות ופותח הזדמנויות חדשות. התועלת עבורו הייתה דרך הסתכלות חדשה על היבטי ה-IT, כזאת שפתחה בפניו דלת לקידום מהיר...

- **בתחקיר - חוסכים חשמל** - הוא מצא נתונים לפיהם, עלויות החשמל של דטה סנטר בשנה יכולות להיות יקרות יותר מכל עלויות החומרה שבו. הוא גם קרא כיצד השינוי בצריכת החשמל בניידים לוקחת אותנו לעידן חדש. התועלת שהפיק מהתייחסות ויישום הייתה - הרבה כסף לארגון. איך זה נשמע?

- **בתחקיר - כללי אצבע למנמ"ר** - הוא מצא נתונים, מספרים, כללי אצבע ומקורות שחיוני לכל מנהל שעוסק במחשוב להיות מצויד בהם. התועלת שהפיק הייתה קבלת החלטות מהירות יותר, מבוססות ומוצלחות יותר. התוצאות נראות בשטח. מכיר אנשים כאלה?

- **בתחקיר - וירטואליזציה בשרתים** - הוא הבין את המשמעויות המעשיות של מגמה מרכזית שסוחפות כיום את עולם המחשוב, כאשר הוא גילה **איך** וירטואליזציה יכולה להעניק יותר גמישות, חיסכון עצום, שרידות, עבודה קלה ועוד יתרונות נוספים. פתאום הכול התחבר. אתה רואה זאת?

- **בתחקיר - Rootkit - חפרפרת במחשב** - הוא קרא כי ברשת הארגונית של כל ארגון חמישי באוסטרליה (וכנראה כך גם בארץ), חבויה כיום תוכנה נסתרת, שיכולה לפתוח דלתות לתוכנות מזיקות. בדרך כלל, לא ניתן לגלות אותה! גניבת מידע, שיבוש נתונים, האזנות, ציטוטים, חדירות, נזקים. חלק מהאיומים יכולים להביא לקריסה. הוא עשה את כל שניתן לטפל בכך וישן טוב בלילה. ואתה?

הוא גם לא היחידי שחושב כך. מאה המלצות נוספות עם מסר חד וברור מדברות בעד עצמן. אחרי הכול, עם הישגים שמוכחים בשטח, קשה להתווכח...

לכן אנו ממליצים לשתף מספר רחב ככל האפשר של חברים, עובדים ומנהלים, בארגון ומחוצה לו, בשימוש בתחקירי PCאון. בדומה לטלפון ופקס, ככל שרבים יותר המשתמשים בהם, כך גם גדלה התועלת. אתה ודאי מכיר זאת.

עכשיו אתה מוזמן לקרוא את התחקיר המצורף, להתרשם באופן בלתי אמצעי ולהתקשר - דרך האתר www.pCon.co.il/promo לטלפן 03-9667939, לפקסס 03-9660310 או מייל - sub@pcon.co.il

אחרי שתצטרף ותסתכל קדימה שנה מהיום, יתכן וגם אתה תחשוב כמוהו? מה דעתך?

PCאון ©

למנהלים ומשתמשי מחשב בכירים

תדרוך מקצועי קצר ומרוכז ● בחדשות ומידע שימושי ייחודי ● למיצוי המחשוב באופן מרבי

RootKit ... והפעם - חפרפרת במחשב

מסר אישי

מה הסבירות שאוסף סוסים טרויאניים מוטמעים במערכות ההפעלה בארגון, על חלק ניכר מהמחשבים ולא ניתנים לזיהוי על ידי כלי האבטחה הרגילים? אפסי! נמוך? עיין ערך RootKit ותגלה שהתשובה הרבה פחות מרגיעה! מדובר בסוג מתוחכם במיוחד של נוזקה, המתמחה בהסתתרות. תופעה מסוכנת, שהמודעות אליה עדיין נמוכה ואמצעי ההתגוננות - מעטים ובסיסיים. היא אינה חדשה, אך לאחרונה נראה זינוק גדול מאוד בהיקפי התפשטותה ונזקיה.

מהן הסכנות שמציב איום זה? עד כמה הוא באמת נפוץ? כיצד לבדוק זאת בארגון וכיצד להתגונן? על כך ועוד, יעדכן אותך התחקיר שלפניך.

תמצית החדשות בעולם המחשוב טור

- חדשות בקצרה 3
- הכרזות 3
- חדש באבטחה 4
- מעולם הניידים 4

תוכן התדרוך השבועי טור

להתמקד בעיקר

- שורש האיום 5
- אומדן נזקים 5
- מגמות וחידושים 6

תועלות, הזדמנויות והיבטי רכש

- הגנה ללא חתימה 7
- איך הם מגיעים? 7
- על המדף 8

המיוחד ביישומי מחשב בישראל

- האנשים שבחזית 9
- אמצעי מניעה 9
- טיפול שורש 10

להעמיק בנושאי מפתח

- 7 עובדות מעניינות 11
- **סוני** וטיפול השורש 11
- קישורים מעשירים 12

ליצירת קשר אישי

עורך ראשי - **קובי שפיבק** B.Sc. ,MBA

עורך - **עמית לוי**

תחקיר וכתיבה - **משה כהן**

טלפון - **03-9667939**, פקס - **03-9660310**

דואר - **ת.ד. 2340 ראשון לציון 75121**

E-Mail - **editor@pcon.co.il**

לתשומת לבך

793.11 – חדשות בקצרה

• **שר התקשורת, אריאל אטיאס, הודיע כי בחודש הקרוב יוציא מסמך מדיניות למתן רישיונות להפעלת Voice Over Broadband (VOB), במטרה לקדם תחרות מול מפעילי הטלפוניה הקווית, ובעקבותיה הוזלת ושיפור השרותים.** זאת, לאחר עיכוב של כשנתיים בקידום הנושא, מאז פרסום מסמך ראשוני בנידון, בסוף 2004. מהלך זה מגיע בעקבות סבב שימועים וישנן הערכות כי הוא יוביל לטלפוניה זולה ב-25% מהטלפוניה הקווית הנוכחית (על פי **nrg**). לדברי השר, מדיניותו בנושא זה תאזן בין חסמים, לבין עידוד הספקים.

• מחלקות מחשוב מובילות מוציאות על מחשוב **$9,024** למשתמש, לעומת **$8,485** במחלקות בינוניות. כך מצא סקר **Hackett Group**, שבדק מדדי ביצועים ב-200 חברות בינלאומיות. במחלקות מובילות מועסקים כ-24% פחות עובדים במשרה מלאה, אך דווקא הם מרוויחים כ-24% יותר. החיסכון המשמעותי ביותר, נובע מהשקעה במחשוב, שמובילה לחיסכון בתהליכי רכש, פעילות פיננסית ומשאבי אנוש.

• "מעבר לעולם התוכנה והשירותים, מתוך כוונה לתת פיתרון מלא לאחסון ניהול ואבטחת הנתונים הארגוניים לצד **ILM - Information Lifecycle Management**", תהיה האסטרטגיה המובילה של **EMC** בשנים הקרובות, כך אמר **יוסי פיקל** המנהל האיזורי, בכנס השנתי של החברה, בשבוע שעבר. **טום הייזר**, סמנכ"ל בכיר למיזוגים ורכישות, הציג את חזון החברה, תוך שהוא מזכיר מספר חברות ישראליות שרכשה החברה. לדבריו, היתרון הבולט של **EMC**, טמון במתן מכלול פתרונות מובילים במעטפת אחת. כן הוצגו בכנס, מערכות האחסון החדשות **Symmetrix DMX3** שמאחסנת עד 1.2 פטה-בייט ו-**Clariion CX3** , שמאחסנת עד 240 טרה בייט.

793.12 – הכרזות

כמה הכרזות חדשות ומעניינות, מעולם המחשוב:

• **נובל** הודיעה על השתתפותה בפרוייקט קוד פתוח, שמטרתו לגשר בין פורמטי מסמכים שונים, לאפשר ללקוחות חבילת **OpenOffice.org** שלה לעבוד עם מסמכי **Office** של **מיקרוסופט**. בתחילת 2007 מתוכננת השלמת התאימות למעבדי התמלילים, כך שמשתמשי **OpenOffice.org** יוכלו לעבוד גם בתאימות מול מסמכי **Office 2007** החדש.

• **Dell** הודיעה על מגוון שרתים חדשים. **Dell** שילבה "טכנולוגיית אנרגיה חכמה" בדגמים **PowerEdge 1950** ו-**2950** במטרה לעזור להוריד צריכת כוח ועלויות הפעלה, עם שיפור 25% בביצועים פר וואט. דגמים אלה מגיעים עם מעבדים הצורכים רק 40 וואט, לעומת 65 וואט או 80 וואט בשרתים הסטנדרטיים. ☎ 03-7674000.

• **תדיראן טלקום** משיקה שירות ייחודי **בישראל**: ליסינג תפעולי לתקשורת **IP**. אחד היתרונות בשירות זה הוא ריכוז כל האינטראקציות מול גורם אחד, **תדיראן טלקום**. השירות מיועד בעיקר לארגונים קטנים ובינוניים, והוא מציע יישום מהיר של פתרונות תקשורת. ☎ 03-9262000.

• **TechLease**, חברת מימון המתמחה במתן מגוון פתרונות מימון להצטיידות במערכות מיחשוב, מכריזה על תוכנית מימון תפעולי לרישיונות **מיקרוסופט** ב-36 תשלומים חודשיים. ☎ 03-5390292.

• **סאן** וקהילת **NetBeans** התקדמו צעד חשוב קדימה, עם יציאת סביבת הפיתוח המשולבת לאפליקציות **ג'אווה**: **NetBeans 5.5** בקוד פתוח. ראה - www.netbeans.org

793.13 – חדש באבטחה

מה שבטוח, חשוב להתעדכן:

• על פי תחזיות **McAfee** ל-2007: היקף הספאם ייגדל ובמיוחד ספאם מבוסס תמונות (40% מהספאם, לעומת 10% לפני שנה). 80% מהנוזקות כבר מבצעות נסיון להסתיר עצמן מגילוי, דרך אמצעים כהצפנה או כיווץ. 10% בלבד מהנוזקות כעת הן "פרזיטים" - נוזקות המנסות להטמיע עצמן במערכת, אך נראה כי היקפן גדל. גניבה של זהויות ואובדן מידע ימשיכו להוות סיכון גדול, כולל גניבת מחשבים ואובדן גיבויים. לפי נתונים מ**ארה"ב**, יותר מ-10 מיליון אמריקנים נופלים קורבן לגניבת זהות כל שנה. עוד ייתחזקו התקפות ה-**Phishing** ו-**Adware**, סוסים טרוייאנים, **Keyloggers** ו-שימוש ב-**Bots**.

• **SecureWave** הכריזה על זמינות יישום חינמי לסריקת התקני קצה, המאפשר למנהלי ה-**IT** לבחון את ההיסטוריה המלאה של כל אמצעי האחסון הניידים אשר חוברו לנקודות הקצה בארגון. באמצעות היישום ניתן להעריך בקלות את הסיכון הקיים לזליגת מידע מהארגון ולחדירה של תוכנות ריגול דרך נקודות הקצה. **TrekIT** ☎ 03-9016190.

• חברת האבטחה **Protegrity**, המספקת פתרונות ניהול אבטחת נתונים לארגונים, זכתה ב**ארה"ב** לאישור פטנט על פיתוח שיטה ומערכת לזיהוי ובקרה של פעילות חריגה, בבסיסי נתונים ארגוניים.

• פרצה חדשה נמצאה ב-**Word**. מדובר בפרצה המאפשרת לתוקף להיכנס לקובצי **Word** ומשם להשתלט על המחשב כולו. התוקף יכול לעשות זאת דרך אתר האינטרנט שלו הכולל קובץ **Word** זדוני, או לשלוח אימייל עם הקובץ.

793.14 – מעולם הניידים

המחשוב הנייד צובר תנופה ומחדש:

• **טושיבה** הודיעה השבוע על הדגם החדש של הכונן הקשיח הקטן שלה המציע קיבולת של **100GB**. הכונן החדש מתאים למחשבים ניידים, אשר סבלו מאז ומתמיד מבעיית קיבולת עקב מגבלות מקום.

• **Cognos** הציגה את מערכת **Cognos 8 Go! Mobile** המיועדת ללקוחות **SAP**. המערכת היא פתרון ה-**BI** הנייד החדש המעביר למשתמשי **SAP** מידע המסייע לקבלת החלטות אל הטלפונים הסלולריים, מחשבי כף יד ומחשבים ניידים אחרים. המידע המופיע מספק למשתמשים ומנהלים תמונה שלמה של ביצועי החברה לקבלת החלטות בזמן אמת ולניהול הביצועים העסקיים. **ליבי טכנולוגיות תוכנה** ☎ 03-6129088.

• **ASUS** מציעה את **Asus R2H Ultra Mobile PC**, מחשב נייד שהוא גם **PDA**. המכשיר שוקל כ-960 גרם בלבד, ומשלב יכולות של מחשב נייד ומחשב כף יד. המחשב מבוסס על מערכת ההפעלה **Microsoft Windows Tablet PC** וכולל מסך מגע בגודל 7 אינץ', מצלמה מובנית **1.3MP**, תמיכה בתקשורת אלחוטית בתקן **802.11B/G** ובתקן **Bluetooth**, קורא כרטיסי זכרון מסוג **SD**, והגנה באמצעות קורא טביעות אצבע.

• **מיקרוסופט** ו-**Samsung Electronics** הודיעו על השקת הטלפון הסלולרי החדש: **Samsung Ultra Messaging i600**. מדובר בטלפון נייד מסוג G3 דור שלישי, הכולל לראשונה מקלדת **QWERTY** מלאה, ממש כמו במקלדת רגילה, עם גלגלת ההופכת את חוויית הניווט בין האפשרויות קלה ונוחה. טלפון זה תומך גם באפליקציות רשת כמו שידורים שונים (**Podcasting**) ו-**RSS Feeder**, ומסוגל לסרוק אתרי **אינטרנט** על מנת לקבל עדכונים.

• **מיקרוסופט** גם הביעה עניין להצטרף לפרוייקט מחשב נייד לילדים בעולם השלישי. זאת למרות ההצהרות הלגלגניות מעט, שהגיעו בעבר מכיוון **ביל גייטס** לגבי הפרוייקט.

793.21 – שורש האיום

ה-RootKit הוא איום ותיק הצובר כיום תאוצה. הוא מטריד יותר ויותר ומאתגר את המנמ"רים וחברות אבטחת המידע. מדובר בסט כלי פריצה המושתל ומוסתר בתוך ליבת מערכת ההפעלה ושוכן שם לאורך זמן, ללא ידיעת המשתמש ואמצעי ההגנה השונים. מדובר במעין סוס טרויאני בסיסי ורב-שימושי, שמומחיותו - הסתתרות בתוך מערכת ההפעלה ושימוש בה, בזמן ובדרך, עליהם יחליט מי שהתקין אותו.

תפקיד ה-**RootKit**, להוות דלת אחורית זמינה לפעילות אחרת, כהחדרת נוזקות, גניבת מידע, הסתרת מידע, הפצת ספאם וגם פעילות לגיטימית או לגיטימית למחצה (למשל במערכת הגנת זכויות יוצרים). האופי החמקמק של ה-**RootKit**, יכולתו להוות קרש קפיצה לתקיפות שונות, הפוטנציאל הפלילי הרחב שטמון בו והנזק המתגלגל, מחייבים הערכות מיוחדת ברמת האמצעים, ברמת הידע וברמה הניהולית.

RootKit נחלקים בהכללה לשני סוגים: **RootKit** ברמת המשתמש, שפועל כישום עצמאי או משעבד ישום קיים והוא הקל יחסית לאיתור. **RootKit** ברמת ליבת מערכת ההפעלה (ה-**Kernel**), פועל לעיתים בתוך מנהלי התקן או רכיבי מערכת אחרים והוא בעל פוטנציאל השפעה רחב וקשה לאיתור. העיקרון דומה בשני הזנים: הסתרת מידע של מצב המערכת מכלי הדיאגנוסטיקה וההגנה.

ההדבקה עשויה להתרחש במגוון דרכים מוכרות להפצת נוזקה, דוגמת התקנת תוכנה נגועה, לחיצה על קישור באתר נגוע או פתיחת קובץ נגוע, המקושר להודעת דואר.

ההשלכות לארגונים חמורות: ארגון החש מוגן, עשוי להיות בפועל פרוץ לתקיפות רבות. אם מתרחשת תקיפה באופן זה, היא יכולה בקלות להיות חשאית ולהתגלות רק אחרי זמן רב. הנזקים עשויים להיות רבים: דליפת מידע מהארגון, פגיעה בשמו הטוב, בעקבות הפצת ספאם או חדירה לפרטיות, בהמשכיות העסקית ומגוון נזקים כלכליים, כמו למשל שינוי נתונים כספיים, מחירי מוצרים או מידע על לקוחות.

מגמות אחרונות בתחום, מגבירות את דחיפות העלאת המודעות לקריטיות האיום: עליה בתחכום ה-**RootKits**, גידול בהיקפים, במספר הסוגים ובמגוון אופני ניצולם על ידי התוקפים.

בעוד שלרוב אין ל-**RootKits** כל נזק ישיר, ישנם נזקים כלכליים משמעותיים, עקב פתיחת פתח לפעולת נוזקות אחרות, גניבת מידע או פגיעה בפרטיות. לדוגמא: עובד ממוצע מבזבז מעל שעה בחודש על טיפול בספאם (**ITU**), שעולה 50 מיליארד דולר בשנה, לכל הארגונים בעולם ביחד (**Ferris Research**). ככלל, השיעור הממוצע של נזקי אבטחה בארגונים, הוא כ-0.23%-0.14% מתקציבם (**גרטנר**).

על פי **סימנטק**, התחזקות ה-**RootKits** היא אחת המגמות הבולטות ביותר באבטחה ב-2006. ואכן, כיום 22% מהפגיעות עליהן מדווחים מנהלי מחשוב, נובעות מ-**RootKits** ו-**KeyLoggers** (נתוני **FaceTime Communications**). לפי **McAfee Avert Labs** היקף התופעה כנראה ייתרחב ב-2007. מצד שני, צפוי שכך גם יקרה להיקף הפתרונות ויעילותם.

<u>לסיכום - חיוני להכיר את הסיכון החמקמק שמציבים יישומי ה-RootKit ולטפל בהם, באופן שגרתי, יסודי ומתודי.</u>

793.22 – אומדן נזקים

כך עלול ה-RootKit להשפיע על הארגון:

• **סייבר-פשעים -** ה-**RootKit** מהווה תשתית לגניבת מידע וריגול מסחרי. האקר יכול לאסוף או לשבש מידע ארגוני וכך לגרום לנזק עצום.

• **פרסום שלילי -** הסקנדל התקשורתי על דליפת מידע ארגוני, מזיק לרוב הרבה יותר מהדליפה עצמה.

• **קנסות, תביעות, הגבלות -** רגולטוריות, חוקיות וכלכליות, בעקבות חשיפת מידע לקוחות רגיש.

• **התפשטות נגעים -** תשתית **RootKit** בארגון, מאפשרת לתוקפים חשיפת פרצות אבטחה נוספות, עד כדי גישה רחבה בכל המערכת והחדרת נגעים נוספים.

• **קריאות שרות -** הנוזקות להן מאפשר ה-**RootKit** לפעול, ייגרמו לקריאות שרות יקרות. חשוב להזכיר, את מורכבות הנסיון לאתר ולטפל במקרים אלה.

• **האטת ביצועים -** מחשבים הנגועים ב-**RootKit** נוטים להיות איטיים מעט יותר, דבר שפוגע בפרודוקטיביות.

דגש – מחיר הסיכון

על פי נתוני McAfee, קיים שוק שחור פעיל ל-RootKits איכותיים, במחירים המגיעים עד $2,000. ברור, שמי שמשקיע סכום כזה ברכישת "מוצר איכות" מסוג זה, הם לקוחות שגם יודעים לתקוף באמצעותו, באופנים המניבים להם רווחים (ולארגונים נזקים), בסכומים גדולים מכך משמעותית.

כמו כן, נזכיר כי ישנן גם רשתות של מחשבים הנגועים ב-**RootKit**, שהאקרים רותמים כ"זומבים", לשם שימוש בהם או מכירת שירותיהם, למטרות הפצת ספאם או ביצוע התקפות **באינטרנט**.

793.23 – מגמות וחידושים

ומה התחזית? גשום - יותר RootKits, יותר מתוחכם, מסתיר מגוון רחב יותר של נוזקות:

• **גידול בהיקף הנוזקות מסוג זה** - בשלוש השנים האחרונות, נראתה צמיחה של יותר מ-600% בשימוש ב-**RootKits** (נתוני **McAfee**).

• **שימושים מתרחבים** - על פי **McAfee's Avert Labs**, טכנולוגיות ההסתרה היו עד 2005 תחום בלעדי של סוסים טרויאניים. כיום, נוזקות נוספות מצטרפות לכך בקצב גובר: תולעים, וירוסים פרסומות פופ-אפ וישומים מסחריים (ראה **ידיעה 793.53**).

• **תחכום גובר** - ניכרת עלייה במורכבות כלי ה-**RootKit** המופצים. לפי הערכות **McAfee**, מורכבותם גדלה בין 2000 ל-2005, ב-400%.

• **צמצום בנפגעים** - למרות כל זאת, נראית ירידה מסויימת במספר המחשבים הנגועים, עקב הדרכת משתמשים וכניסת כלי זיהוי והסרה.

• **תקיפת ה-BIOS** - על פי מומחי חברת האבטחה הבריטית **Next-Generation Security Software**, ישנה כבר טכניקה זמינה להחדרת **RootKits** לשבבי **BIOS** על לוחות אם. דבר זה, עלול להעלות את רף הסיכון מהתקפות **RootKit**, בעתיד הקרוב.

793.31 – הגנה ללא חתימה

מעבר לגישה הנפוצה של סריקת המערכת לגילוי נוזקה, ישנן גישות המזהות פעילות חשודה:

• **ניתוח התנהגותי** - זיהוי פעילות חשודה של יישומים פעילים, העשוי לסייע, בשלבים בהם נוזקה כלשהיא מתקינה **RootKit** או כשה-**Rootkit** מבצע פעילות חשודה. משלים לפתרונות המבוססים על סריקת קבצים. עשוי לספק התרעות שווא ובמקרה שמתריע על פעילות חשודה, הבנת המתרחש תדרוש ידע טכני מעמיק.

• **ריצה ב"ארגז חול"** - הרצת תהליכים שונים באזור שמור וסגור בזיכרון. אזור זה מהווה מעין מחשב נפרד בפני עצמו, שנוזקה הפוגעת בו לא תיפגע במחשב הראשי. החסרון המיידי הוא פגיעה בביצועים.

• **חומת אש בזיכרון** - חוצץ בין היישום לבין הזכרון, שמשווה את המתרחש מול כל מה שמותר לישום ליזום. יעיל נגד נוזקות חדשות ובמיוחד מול התקפות מבוססות זיכרון.

• **רשימה לבנה** - הרצת תהליכים מוכרים בלבד. פתרון שאינו טורדני ומעניק הגנה גבוהה מפני נוזקות חדשות, אבל רק במידה ואינן מטמיעות עצמן בתוך תהליכים מוכרים. מתאים לסביבות מחשוב אחידות יחסית. פתרון זה אינו יעיל מאוד בפני **RootKits**, מאחר ומומחיותם היא הסתתרות בתהליכים מוכרים, של מערכת ההפעלה.

793.32 – איך הם מגיעים ?

מפיצי ה-RootKit, נעזרים בכמה דרכים אופייניות לביצוע זממם:

• **התקנת תוכנה "תמימה" לכאורה** - ה**אינטרנט** מציע שפע תוכנות חינמיות, שחלקן משולבות רוגלה וכלי **RootKit**.

• **שהיה באתרים נגועים** - אתרים מסויימים מתקינים תוכנות זדוניות במחשבי המשתמשים באופן אוטומטי וסמוי במהלך הגלישה בהם. גם אתרים לגיטימיים עלולים להיות נגועים ללא ידיעתם.

• **פתיחת דואר ספאם** - חלק מדואר הספאם שנשלח, משחרר תוכנות זדוניות במהלך הפתיחת הדואר או הקובץ המצורף ובכלל זה **RootKits**.

• **תרמיות ActiveX** - החדרת תוכנות זדוניות, באמצעות הקפצת הודעה לגיטימית לכאורה במחשב ואישורה על ידי המשתמש.

• **חיבור רשת אלחוטי** - ניצול אבטחה נמוכה ברשתות אלחוטיות ואוסף הגאדג'טים שבכיסנו, החשופים להדבקה "על הדרך" ובדרך, אל הרשת הארגונית.

• **שימוש בשרותי שיתוף קבצים** - תוכנות הנעזרות בחיבור P2P ממחשב מרוחק ואנונימי - סביבה אידאלית להפצת נגעים. תוכנם של הקבצים המוצעים אינו בשליטה, אינו ידוע ולעיתים גם שמם מטעה.

• **תוכנות מוכרות** - יותר ויותר מוצרי תוכנה מסחריים מכילים **RootKits**. לרוב, הם אינם מזיקים, אך קיימת סכנה שהאקרים ינצלו אותם לרעה.

793.33 – על המדף

אלו כמה מוצרים בולטים, שיסייעו בהתמודדות:

• **מיקרוסופט** - רכשה לאחרונה את המוצר **Rootkit Revealer**, כלי זיהוי שמאתר טווח רחב של **RootKits** - www.microsoft.com/technet/sysinternals/utilities/RootkitRevealer.mspx

Malicious Software Removal Tool (MSRT) הוא כלי זיהוי נוזקה חינמי של **מיקרוסופט**, המאתר גם כמה **RootKits**. להתקנה במסגרת **Microsoft Update** או - www.microsoft.com/malwareremove

• **DiamondCS - ProcessGuard** הוא כלי המסייע במניעת הידבקות המערכת ב-**RootKits**. החל מ-**$29.95**, לשימוש ארגוני - www.diamondcs.com.au

• **F-secure** מציעה את **Internet Security Suite 2006** ואת **Blacklight**, כלי זיהוי וניקוי **RootKit** - www.f-secure.com/blacklight

• **GMER** - כלי ידוע (אם כי ממפתח לא מוכר במיוחד) לזיהוי **RootKit**, הבודק ומציג פרטים טכניים שונים על פעילות מערכת ההפעלה - www.gmer.net

• **Ice Sword** - כלי זיהוי פופולארי וחינמי, למשתמשים מתקדמים. דורש ידע והפעלה "ידנית" של אמצעי בדיקה ודיווח, על המתרחש במערכת - www.antirootkit.com/software/IceSword.htm

• **InfoProcess** - מציעה את **AntiHook**, כלי המסייע בניטור בזמן אמת, של נסיונות נוזקה (כולל **RootKits**) להיטמע במערכת. **$17** - www.infoprocess.com.au

• **McAfee - McAfee Total Protection for Enterprise** היא חבילת הגנה כוללת, המגינה גם מפני **RootKits**. **רנסאנס** ☎ 09-7645700.

• **ESET - NOD32** הוא אנטי וירוס תואם **חלונות ויסטה**, המזהה גם **RootKits**. פועל בדפוס סריקה וגם לפי זיהוי התנהגויות חשודות. **קומליין** ☎ 03-6290845.

• **Resplendence - Rootkit Hook Analyzer**, הוא כלי חינמי המנתח השתלבות קוד בפעילות מערכת ההפעלה (בגישת **Kernel hooks**) - www.resplendence.com

• **Sophos - Sophos Anti-Rootkit** - כלי לבלימת, זיהוי וניקוי **RootKits**, המוצע בחינם - sophos.com/products/free-tools/sophos-anti-rootkit.html

• **Symantec** - מציעה פתרונות כוללים, המטפלים גם ב-**RootKits**, לארגונים בגדלים שונים. מ-**Norton AntiVirus 2007** (**$39.99**) לארגונים קטנים ועד חבילת האבטחה הארגונית **Sygate Enterprise Protection**. ☎ 03-9180404.

עוד בולטים, **טרנד מיקרו** (**סקיור טרנד** ☎ 03-6383850), **Sunbelt CounterSpy** (www.sunbelt-software.com) ו-**Webroot SpySweeper** (www.webroot.com).

793.41– האנשים שבחזית

כך שמענו משני מומחים בתחום:

אבי וויסמן מנכ"ל חברת האבטחה **שיא סקיוריטי** (☎ 03-6122831), אומר שאין פתרון אחד ואין פתרון מושלם לבעיה ועדיין ההאקרים מנצחים יום יום. לשם ההתמודדות עם אתגר זה, נדרשים שני מרכיבים: הראשון הוא שימוש בכלים טכנולוגיים והשני הוא ידע - מנמר"יים צריכים לדעת איך מתנהל המאבק מול האקרים. לשם כך נדרשת גם הכרה בבורות הקיימת, מאחר וכרגע זה נראה כקרב בו המנמ"ר נאבק "בעיניים קשורות" מול אוייב מסוכן - קרב שתוצאותיו ברורות.

לדעת **טל קנדל**, מהנדס מערכת ויועץ קדם-מכירה ב**סימנטק** (☎ 03-9180404), הגנת אנטיוירוס כבר אינה מספיקה והיום יש צורך להגן גם על רכיבי הליבה. מערכת נקיה ומוגנת, הכוללת יישום מדיניות הרשאות עקבית, תהיה נגישה פחות ל-**RootKits**. **טל** אומר, כי העלאת נושא ה-**RootKit** למודעות המנמ"רים הוא צעד חיובי. בו בזמן, חברות האבטחה מודעות לצורך בפתרון, עומדות באתגר וסוגרות פערים.

793.42– אמצעי מניעה

אלו כמה עצות שימושיות למתגונן:

- **החכם לא נכנס לצרה, שהפיקח (חושב שהוא) יודע לצאת ממנה** - ניקוי מערכת הנגועה ב-**RootKit** מסובך בהרבה מניקוי מערכת נגועה בוירוס רגיל. לרוב גם לא ברור אם הנגע הוסר לחלוטין (הרי הסתתרות היא בדיוק המומחיות שלו!) ובכל מקרה, מדובר בתהליך מורכב במיוחד וגוזל זמן. לכן, מניעה חשובה כאן יותר מכל.
- **כמה כלים במקביל** - בגלל טבעו החמקמק של איום ה-**RootkIt**, אין כלי אחד שמאתר את כולם. לכן, מוטב להשתמש בכמה כלים במקביל.
- **גישת החבילה** - העדף שימוש בחבילות אבטחה מלאות, הכוללות בין היתר איתור והסרת **RootKit**. חבילות כאלה קיימות כבר היום והן מתרבות, גם כחלק ממגמת מעבר לחבילות אבטחה וגם מתוך מודעות גוברת אצל ספקים, לצורך בפתרונות לטיפול ב-**RootKit**.
- **תועלת ה-Firewall** - כל **Rootkit** מגיע יומו! הכוונה ליום בו הוא ינסה לתקשר עם מפעילו המרוחק, דרך **האינטרנט**. במצב זה, ה-**FireWall** הצנוע, עשוי להפריע לו ולספק לך אינדיקציה על פעילות חשודה. מסיבה זו, **FireWall** איכותי, עדכני ומופעל היטב, הוא בעל ברית חשוב למלחמה ב-**RootKits**.
- **Intrution Detection & Prevention** - כלי גילוי ומניעת פריצות מזהים פעילות עוינת, על בסיס התנהגותי ולכן הם בעלי ערך מוסף באיתור נוזקות חדשות.
- **התפוח הרקוב** - וודא שכל המחשבים ברשת, זוכים להגנה מתאימה ועקבית. די במחשב בודד המהווה נקודת תורפה, בכדי להדביק רשת שלמה בנוזקה, כולל **RootKit**.

דגש – סביבת המחשוב

כיום, פעילות נוזקות מסוג RootKit מתרחשת בעיקר בסביבת חלונות, אך בעבר, התופעה התחילה והתפתחה בסביבת Unix. אחרי שיא של 71% מהנוזקות בסביבת **Unix** בשנת 2001, נותרה במערכות אלה בסוף 2005 פעילות זעומה בלבד. באותה תקופה, הפעילות ב**חלונות** קפצה ב-2,300%!

תוכניות ה-**RootKit** ימשיכו ויפעלו בעיקר עבור **חלונות** בעתיד הנראה, בעיקר בשל הפופולריות הרבה של מערכת הפעלה זו. מצד שני, שיפורי האבטחה ב**חלונות ויסטה**, עשויים להחליש מגמה זו במידת מה.

793.43– טיפול שורש

צעדים אלה, יסייעו להתארגן לטיפול שיטתי במפגע זה:

1. **ללכת על בטוח** - בחירה מושכלת של כלי גילוי והגנה ייעודיים. חלק גדול מאמצעים אלה נכתבו על ידי מומחים עצמאיים. בבחירת כלי הגנה, זיהוי וניקוי **RootKits**, מוטב להעדיף כלים מחברות אבטחה מוכרות, שבמילא נכנסות גם הן לתחום זה בהדרגה.
2. **בדיקות יזומות** - מאחר ולא מדובר בוירוסים, שפעולתם "רועשת" ובדרך כלל חושפת אותם במהרה, חיוני להפעיל בדיקות יזומות. בדיקות אלה יש לבצע בקביעות.
3. **בדיקות מומחה** - יש לומר בפה מלא, שמיומנותו של המנמ"ר הממוצע בכל הנוגע ל-**RootKits**, נמצאת הרחק מאחור, ביחס למיומנות כותבי ה-**RooKit** ולרמה הטכנית של יצירי כפיהם. לכן, מומלץ להיעזר מדי פעם במומחה חיצוני המתמחה בכך, בכדי לבדוק מערכות להדבקה וגם בכדי לבצע בדיקות הדבקה יזומות. באותה הזדמנות, גם תפתח ותבסס קשרי עבודה טובים, לקראת מקרי הידבקות חמורים, בהם יהיה צורך בסיוע של מומחה חיצוני.
4. **מדיניות הרשאות הדוקה** - שימוש מושכל בהרשאות והקפדה על מינימום הרשאות נדרש. בעיקר, חשוב להמנע משימוש בהרשאת **Administrator** במחשבי הקצה, למעט לפעולות ניהול ותחזוקה.
5. **ביסוס מעטפת אבטחה** - מעטפת אבטחה איכותית, תצמצם את הסיכוי להידבקות, במרבית סוגי ה-**RootKit**. אנטיוירוס איכותי, פתרון אנטי רוגלה וחומת אש, חיוניים. במיוחד אנטיוירוס בעל מוניטין, המסופק עם שרות מהיר, אפקטיבי ועדכוני חתימות תדירים.
6. **עדכונים שוטפים** - התקנת עדכוני אבטחה חיוניים ורצוי אוטומטית. המנעות מעדכונים, עלולה להגדיל את פגיעות המחשבים לאורך זמן.
7. **שולחן עבודה אחיד** - רצוי להמנע ככל האפשר מלהכניס למערכת תוכנות אנונימיות, לא מוכרות ולא מאושרות. מדיניות המגדירה בבירור את הכלול בשולחן עבודה אחיד סטנדרטי בארגון, תסייע לכפות כלל זה.

ראה **תחקיר 791 - סטנדרט לשולחן העבודה**.

תחקיר 793 – עובדות מעניינות

כמה עובדות מעניינות על RootKits:

1. על פי **גרטנר**, RootKits מהווים איום גובר כלפי ארגונים, שהולך ונעשה מסובך למניעה ולגילוי. בחמש עד עשר השנים הקרובות, הם יהיו בין האיומים, בעלי פוטנציאל הנזק הגדול ביותר.
2. על פי ארגון National Computer Emergency Response Team האוסטרלי, אחד מתוך חמישה תאגידים **באוסטרליה**, נמצא נגוע RootKit ברשת האירגונית, בתחילת 2006.
3. 14% מהמחשבים הנגועים בנוזקה כלשהיא, נגועים גם ב-RootKits (לפי נתוני **מיקרוסופט**).
4. 20% מהמחשבים הנגועים ב-RootKits, כוללים גם טרויאני מסוג דלת אחורית (לפי נתוני **מיקרוסופט**).
5. **McAfee's Avert Labs** מדווחת על עליה של 700% בתפוצת RootKit ברבעון הראשון של השנה, בהשוואה לאותו רבעון, אשתקד.
6. RootKits עלולים לעשות שימוש באמצעי תקשורת שחברת **FaceTime** טבעה עבורו את המושג ההולם "רשתות אפורות" - מדובר ברשתות המתבססות על תוכנות **P2P**, מסרים מידיים או וועידות וידאו, שזמינות בארגונים רבים, רשמית או לא רשמית.
7. על פי **מקאפי**, הזינוק החד שנראה לאחרונה בהיקפי התופעה, נובע במידה רבה, מכך שקוד בנושא זה זמין ללימוד והעתקה באתרים רבים.

תחקיר 793.52 – סוני וטיפול השורש

מסתבר כי ה-RootKit משמשים לעיתים גם למטרות מסחריות הנחשבות לגיטימיות, כמו בתוכנות אמולציה, אבטחה והסתרה. אך לפעמים, דבר זה גובל ב"תחום האפור", מבחינת לגיטימיות. מבחינה זו, פרשה בולטת היא פרשת ה-RootKit, ששתלה חברת **Sony BMG** בשנת 2005 בתקליטורי מוזיקה, לצורך הגנה בפני העתקה. באמצעות יישום מדף של חברת **First4Internet**, הוסיפה **סוני** לכמה CD מתוצרתה מערכת ההגנה בפני העתקות לא חוקיות בשם **XCP**. תוכנה זו הסתירה עצמה מנסיונות גילוי, לא איפשרה הסרה ובשלב מסוים זוהתה והוגדרה כ-RootKit.

החל מ**אוגוסט** 2005, דיווחים מסתוריים על התרסקויות מערכת, הקשורות בקובץ מסתורי בשם **aries.sys**, דווחו ועם הזמן קושרו לתוכנה של **סוני**. מי שניסו להסיר את התוכנה ידנית, דיווחו כי פעולה זו שיבשה את הגישה לכונן ה-CDROM.

למרות כוונותיה הטובות של **סוני**, לפחות מבחינת שמירת האינטרסים שלה, תגובת הציבור הייתה חריפה ובהדרגה, חברות אנטי וירוס החלו לכלול במוצריהן יכולות זיהוי והסרה, גם לקוד זה. עוד נטען, כי RootKit זה פתח חור אבטחה במחשבי הלקוחות, אשר האקרים עלולים לנצל לרעה.

עוד על הפרשה, ראה כאן - en.wikipedia.org/wiki/Sony_rootkit

"**פרשת סוני**" העלתה למודעות הציבורית את נושא ה-RootKit בכללו ובמיוחד את הזווית המפתיעה של יישומם ה"אפור", על ידי חברות מסחריות לגיטימיות.

דגש – הגלולה הכחולה

בוועידת ההאקרים Black Hat, שהתקיימה באוגוסט השנה בלאס וגאס, הציגה מיקרוסופט שיפורי אבטחה שונים של חלונות ויסטה. מומחית האבטחה **Joanna Rutkowska** לעומת זאת, הציגה מגוון דרכים לעקיפת הגנותיה החדשות של ליבת מערכת ההפעלה. בין השאר, הציגה **Rutkowska** גישה חדשנית שהיא מכנה **Blue Pill**, לעקיפה של כל מנגנוני ההגנה של המערכת, באופן שמניב מעין "סופר RootKit", שאינו ניתן לגילוי (על פי המפתחת), למרות שהקוד שלו גלוי לציבור! השיטה מבוססת על ניצול יכולות וירטואליזציה של מעבדי AMD, באופן כזה בו מערכת ההפעלה, המשתמש ותוכנות אנטי וירוס, עובדים מול מצג שווא שמציגה הנוזקה. ראה - tinyurl.com/mhnsf

תחקיר 793.53 – קישורים מעשירים

אלו כמה אתרים בנושא RootKit:

- **RootKit.com** - אתר המתמחה ב-RootKits מנקודת מבטו של האקר. מציג מאמרים, חדשות ועדכונים. באתר שפע רב של תוכנות עזר, RootKit דמו, איבחון והסרה. מומלץ להיזהר, לגבי חומרים המוצעים בו להורדה - www.rootkit.com
- **AntiRootKit** - אתר מקיף בנושא זה, הכולל פורום, מאמרים, חדשות, רשימות RootKit, כלים, קישורים וכלים שונים לזיהוי והסרה - www.antiRootKit.com
- **Invisible Things** - אתר של חוקרת אבטחת המידע **Joanna Rutkowska**, המתמחה בנוזקות מסתתרות. מכיל מידע מגוון ומעניין בנושא זה וכלי עזר שימושיים - www.invisiblethings.org
- **Security Now** - מגזין אבטחה מקוון, המציג בפרק זה ראיון בנושא RootKits, עם המומחה **סטיב גיבסון** - www.grc.com/sn/SN-009.htm
- **Microsoft** - מידע על התפתחות פרוייקט נסיוני שלה בשם **Strider**, לגילוי RootKits, על פי התנהגות חשודה - research.microsoft.com/RootKit
- **Wikipedia** - מציגה בדף הבא מאמר כללי, אם כי ארוך, יסודי ומעניין, בנושא RootKits. ראה בתחתיתו, הפניה לקישורים נוספים בנושא זה - en.wikipedia.org/wiki/RootKits