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?

תחקיר 703 ● WWW.PCON.CO.IL ● 21 מרץ 2005

PCאון ©

למנהלים ומשתמשי מחשב בכירים

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

Spyware באיום ממשי ...והפעם

מסר אישי

הניסיון לשוד הגדול בעולם של 423 מיליון דולר, עליו דיווחו כותרות העיתונים ביום שישי האחרון, הוא רק דוגמא אחת לנזק אפשרי של תוכנות Spyware. באמצעות אחד ה"זנים" שלה - ה-**Key logger**, ניתן לעקוב אחר הקלדת סיסמאות ולעשות בהן כיד הדמיון. אבל, מעבר לדרמה, הנזק היומיומי של ה-**Spyware** בראיה כוללת, גדול הרבה יותר. תוכנות אלה מאטות את קצב העבודה וקשה להבחין בהן בגלל השינוי ההדרגתי, לכן הן גורמות להאטה משמעותית של העבודה עם **PC** ולנזק שנתי מצטבר שמגיע למיליוני שקלים לכל ארגון גדול.

כיצד למזער את נזקי ה-**Spyware** (או רוגלה בעברית)? למנוע את כניסתן? לאתרן? לנקותן? בתחקיר שלפניך.

תמצית החדשות בעולם המחשוב טור

תוכן התדרוך השבועי טור

ליצירת קשר אישי

עורך ראשי - **קובי שפיבק**, **MBA**, **B.Sc.**

עורך - **עמית לוי**

תחקיר וכתיבה - **תום שם-טוב**

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

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

E-Mail - editor@pcon.co.il

לתשומת לבך

- כל הזכויות שמורות **לקומרקטינג בע"מ** ©. אין לצלם או להפיץ את הגיליון ללא היתר ובכל צורה שהיא.
- אנו משתדלים להביא מידע אמין ומדויק אולם האחריות לתוצאות השימוש בו תחול על המשתמשים.
- שמות המוצרים והחברות המוזכרים ב-**PCאון**, הם שמות שמורים של בעליהם.
- ככלל המחירים בגיליון הם בדולרים וללא מע"מ. מחירי ספרים ניתנים בש"ח כולל מע"מ.
- לאתרים **באינטרנט** יש להוסיף הקידומת **http://**

לכבוד **קומרקטינג בע"מ**
פקס 03-9660310
ת.ד. 2340 ראשון לציון 75121

___ כן אני רוצה להיות מנוי **PCאון**, לתקופה של 3 / 6 / 12 חודשים. אני מצרף סך בשקלים של $129 / $244 / $464 + מע"מ (סמן בחירתך בעיגול), לפקודת **קומרקטינג בע"מ** ומחכה לגיליון הקרוב.

שם מלא _____

ארגון _____

תפקיד בארגון _____

כתובת _____ מיקוד _____

טלפון _____ פקס _____

תאריך _____ חתימה _____

הערות _____

PCאון© למנהלים ומשתמשי מחשב בכירים

703.11– חדשות בקצרה

• **מנוע חיפוש המיועד לרשתות סלולריות, הוצג השבוע לראשונה, על ידי חברה נורווגית בשם FAST.** המוצר כולל פורטל חיפוש, המאפשר למשתמש לחפש ברשת הפנימית של ספקית הסלולר וספקיות התוכן שלה, וגם לבצע חיפושים **באינטרנט** הסלולרי. **Vodafone** - ספקית הסלולר הגדולה **באירופה**, כבר ניסתה את הטכנולוגיה במהלך השנתיים האחרונות וכעת מרחיבה **FAST** את מעגל תפוצתה לספקיות סלולר נוספות, לספקיות תוכן ולשוק הארגוני.

• "2005 תהיה שנת תוכנות הריגול ותוכנות הפרסום", כך אמר **אריה דנון**, מנכ"ל **סימנטק איזור הים התיכון**, בכנס **Infosec 05** שהתקיים ביוזמת **אנשים ומחשבים** ביום רביעי האחרון. עוד ציין **דנון** את נזקן הרב של הרוגלות, בעיית ריבוי מוצרי האנטי-רוגלה שבשימוש, ופתרונות המספקים הקלה לטווח הקצר בלבד.

• **חוק המחשבים בישראל** חייב לעבור רפורמה, בכדי לענות כראוי על הנדרש ממנו כיום. זו המסקנה הברורה שהתגבשה, בכנס שהתקיים **במכללת שערי-משפט בהוד השרון**, לציון עשור ל**חוק המחשבים**. **ד"ר אריה רייך** מ**אונ' בר-אילן**, **פרופ' מיגל דויטש** מ**אונ' תל-אביב**, **עו"ד נעמי אסיא** ומומחים נוספים, הסכימו כי מטרתו המקורית של החוק, היתה לגשר על הפער בין העולם המחשוב לעולם המשפט, אך כיום, עידן ה**אינטרנט** משנה את פני החוק והמשפט עצמם, ו**חוק המחשבים** חייב להתעדכן ברוח הזמן (על פי **Ynet**).

703.12– רשמים מתערוכת CeBIT

בתערוכת CeBIT 2005 שהתקיימה ב-16-10 במרץ בהאנובר, גרמניה, נראתה נוכחות חזקה של הטלפוניה הסלולרית, נושא הניידות בכללו, VoIP ואבטחת מידע (עם חידוש מעניין מפוג'יטסו, בדמות פתרון זיהוי ביומטרי מבוסס זיהוי תבנית העורקים בכף היד). נושא הקוד הפתוח הפגין אף הוא נוכחות חזקה ביותר. בין ההכרזות שבלטו:

• פישוט תהליכי אחסון וניהול מידע בארגונים בינוניים וקטנים, מבטיחות **EMC**, **מיקרוסופט**, **סיסקו** ו**אינטל**. החברות הכריזו במשותף על גישת **Making Storage Simple**, שתכלול מגוון מערכות ושירותים, המיועדים לסייע בהתמודדות עם הגידול בנפח המידע.

• **נובל** חשפה את **SuSE Linux Professional suite 9.3**, הכוללת, פרט למערכת ההפעלה, גם כמאה אפליקציות קוד פתוח (ככלי פיתוח שונים, טכנולוגיית הוירטואליזציה **Xen** ותוכנה לשיחות **VoIP**). **נובל** מעריכה כי בשלב זה רק מפתחי תוכנה ומומחי **לינוקס** יתקינו אותה, אך היא מספקת לארגונים הצצה לפיתוחים וטכנולוגיות, שיוכנסו בעתיד לשימוש בארגון. זמינות - החל מאמצע **אפריל**.

• **סמסונג** הציגה את **SCH-V770**, טלפון סלולרי בעל מצלמה של 7 מגה-פיקסל ודיסק מובנה בנפח **3GB**. עוד הציגה החברה מספר טלפונים ניידים, המשמשים כמחשבי כף יד ומבוססים על מערכת ההפעלה **Windows Mobile**.

• **סימנס** הציגה מספר חידושים בתחום הטלפונים הסלולריים, כולל 5 טלפונים בטכנולוגיית הדור השלישי ובהם **M75**, המכיל מערכת הגנה מיוחדת בפני מים וחול.

• מעל טרהביט אחסון לאינץ' מרובע! זו יכולתו הפוטנציאלית של השבב הנסיוני **Millipede**, אותו הציגה **IBM** בתערוכה (להמחשה - כל שבב בגודל בול, יוכל לאחסן 600,000 תמונות דיגיטליות). פיתוח המוצר צפוי להימשך, לפחות עוד שנתיים.

703.13– הניידים זזים קדימה

מספר חידושים מעולם המחשוב הנייד:

• **אינטל** מתכננת הוזלות מחיר של עד 33.6% למעבדי **Pentium M**, בעקבות הכרזת **AMD** על **Turion 64** לניידים. ההוזלות יתמקדו במעבדים שבטווח המחירים היקר ביותר והבינוני (על פי **DigiTimes**).

• **Dell** הוסיפה להיצע המחשבים הניידים שלה את **Inspiron 2200** קל-המשקל (2.72kg), שמחירו מתחת ל-**1,000**$. למחשב מסך "14.1 ומעבד **1.4GHz Intel Celeron M 360**. **יוניטק** ☎ 1-800-732-000.

• **טושיבה** חשפה נייד חדש, בעל מערכת הגנה מיוחדת נגד נפילה, מכות או נזק מנוזלים. מערכת מיוחדת מזהה רטט פגיעה, ומעבירה את הדיסק הקשיח למצב הגנה, שנמשך עד חלוף הסכנה. **Portege S100** מוצע באתר **טושיבה** ב-**1,599**$ - www.toshibadirect.com

• **Acer** הכריזה על ניידים מבוססי **AMD Turion 64-bit**. המחשבים, מסדרות **Aspire 5000** ו-**5020**, המיועדים לעסקים קטנים עד בינוניים. הדגמים יוצגו בחודשיים הקרובים ומחירם עדיין לא נקבע.

• חוקרים ב-**MIT** מקדמים כעת פרויקט ייחודי, שמטרתו לספק מחשבים ניידים במחיר שלא יעלה על 100$. מחשבים אלה יסייעו לקידום ילדים **בקמבודיה**, ויציעו פתרון בסיסי לשימוש **באינטרנט** ומולטימדיה. אין זה הפרויקט הראשון מסוגו, אך כל יוזמה כזו מסייעת לקידום והוזלת המחשוב הנייד הבסיסי, והפיכתו שווה לכל נפש.

703.14– סקרים ומחקרים מאירים

נתוני מחקרים וסקרים חושפים תובנות חדשות:

• סקר **Forrester** חוזה עליה בהוצאות המחשוב השנה. 45% מהמנמ"רים (תושבי **צפון אמריקה**) צופים כי הוצאותיהם תהיינה גדולות מהמתוכנן, לעומת רק 25% בסקר דומה שנערך ברבעון הראשון של 2004. עיקר השינוי מגיע מארגונים של 1,000-5,000 עובדים. 57% מתארים את האקלים העסקי כחזק עד חזק מאוד (לעומת 36% ברבעון הראשון של 2004).

• שוק תוכנות האחסון הגיע לרווח של 2.2 מיליארד דולר ברבעון הרביעי של 2004, גידול של 15% לעומת השנה שעברה (**IDC**). **IDC** גם מציינת, כסיבות העיקריות לגידול, את העליה ברכישת פתרונות ניהול והגנת מידע, כמו גם הצורך בהתאמה לדרישות רגולטוריות שונות.

• מסקר שערכה **גרטנר** עולה כי 39% מהארגונים מתכוונים להגדיל השקעותיהם בתחום ה-**BI**. בנוסף, מתריעה החברה כי החסמים המרכזיים להצלחת **BI** בארגונים הם חוסר במיומנות משתמשים ובידע לגבי **Best Practices**.

• מחקר **Forrester** מצא שאמון הציבור בתוכן המועבר במדיה מכל הסוגים, ממשיך להידרדר בקרב צרכנים ב**צפון אמריקה**. הידרדרות זו נראית כבר משנת 2002 ואמצעי המדיה היחיד שזכה לעליה במידת האמון היא רשת ה**אינטרנט** (**מ-15%** ביטחון ב-2002, ל-21% ב-2004). עם זאת, שיעור האמון בדואר אלקטרוני צנח במידה הגדולה ביותר, ביחס לכל אמצעי מדיה אחר, כאשר 25% מהציבור לא בוטחים בתוכן המגיע דרך **E-Mail** מאנשים מוכרים לנשאל, לעומת 13% שענו כך ב-2002.

• 58% מהגולשים נוהגים למחוק קבצי **Cookies** מחשש לפגיעה בפרטיות, על פי מחקר **Jupiter Research**. כ-39% מוחקים אותן לפחות פעם בחודש. צעד זה מסייע לגולשים להרגיש שיפור בפרטיותם ובבטיחות הגלישה, אך הוא גם מגביל יכולת אתרים לתפקד מול משתמשיהם הקבועים.

703.21 – פצצה מתקתקת

עד לאחרונה הוכתר ה-Spyware כאיום הרביעי בגודלו על ארגונים מבחינת אבטחת מידע (IDC), אך לאור נסיון השוד שהזכרנו, ומתוך למידת התחום, נראה שדירוג זה עשוי לזנק למעלה מהר מאוד. אין ספק שמדובר במגיפה עולמית שנזקיה רבים ושונים. בין 80% ל-90% מכלל המחשבים נדבקו כבר בסוג כלשהו של רוגלה (**גרטנר**) וקיימים כ-90(!) סוגי רוגלה שונים בכל מחשב (לפי סקר **AOL**, שעסק במשתמשים ביתיים).

אחת הסיבות להתפשטות המגיפה היא חוסר המודעות של משתמשים פרטיים וארגונים לנושא. כ-92% מכלל הארגונים נגועים ברוגלה, אולם בממוצע, רק כ-6% מהמועסקים מודעים לכך (סקר **Websense**). רוב המחשבים "פרוצים" לגמרי בפני הרוגלות מאחר ומפעיליהם לא נקטו בצעדים הדרושים להגנה עליהם. דבר זה מעודד את יצרני הרוגלה (וגם יצרני ה-**Ad-Ware** שמקפיצות פרסומות ובאנרים) להמשיך ולהגביר את היקף הפעילות שלהם. ישנו כסף רב בפיתוח הרוגלות, גם ככלי מעקב לצורך מחקר התנהגותי/שיווקי וגם ככלים לוכדי סיסמאות ומידע פנימי יקר ערך. הרווח הרב של יצרני הרוגלה הוא ההפסד שלנו. 75% מכלל קריאות השירות (**Help Desk**) נגרמו על ידי רוגלות (**גרטנר**). אולם הזמן והכסף שבתיקון הנזקים מהווה עלות זניחה יחסית לעלות האמיתית הנובעת מהאטת ביצועי המחשב. חשוב להדגיש את אזהרת **גרטנר**, לפיה **Spyware** נפוץ בארגונים, בגלל שהוא נכנס דרך ערוצי כניסה לגיטימיים, שאינם מוגנים דיים. לאור זאת, לא מפתיע לגלות שרק 25% מהארגונים מתייחסים ל-**Spyware** כאל איום של ממש (**Secure Computing Corporation**).

ארגונים מתחילים להגיב לאיום החמור רק בתקופה האחרונה. כ-69% מהארגונים הגדולים מתכוונים לרכוש תוכנות אנטי-רוגלה לעומת 53% מהארגונים הקטנים עד בינוניים. אם כי לכ-80% מהארגונים כבר יש פתרונות אנטי-רוגלה (סקר **Forrester**), הם הוצגו רק כפתרון נקודתי, שהובא בשנתיים האחרונות, לטיפול במחשבים שנדבקו. ב-**IDC** צופים ששוק האנטי-רוגלה יגיע לשווי של 301 מיליון דולר בשנת 2008 כאשר בשנת 2003 שווי השוק היה רק 12 מיליון דולר.

לאחרונה נכנסה **מיקרוסופט** לתחום האנטי-רוגלה, עם רכישת חברת האבטחה **Giant** ושיווק גרסת בטא חינמית של התוכנה. כמו כן, הגרסה הבאה של דפדפן **IE**, אמורה לכלול בתוכה רכיב אינטגרלי נגד רוגלה.

<u>לסיכום - רוגלות מהוות איום חמור ורציני לארגונים שגורם לנזקים כספיים אדירים. לכן מומלץ להיאבק בהן וברצינות, ולהשקיע את הכסף והזמן הנדרש לסילוקן ומניעת חדירתן למערך המחשוב הארגוני.</u>

703.22 – סוגי המרגלים

ברשת יש מגוון רחב של איומים הנופלים תחת ההגדרה Spyware להלן פירוט הסוגים הנפוצים:

• **Ad-Ware** - תוכנה שלאחר שהתקינה עצמה, תציג פרסומות קופצות ובאנרים בפני המשתמש בעת הגלישה. דוגמא לתוכנה שכזו היא **Gator**, שלרוב חבויה בתוכנות חינמיות ברשת, התוכנה מקפיצה פרסומות ומציגה באנרים על פי הרגלי הגלישה של המשתמש, אחריו היא מרגלת.

• **תוכנות סטטיסטיקה** - תוכנה כזו עוקבת אחר הרגלי גלישה ומספקת מידע זה לתוכנות ה-**Ad-Ware** המחליטות בעזרתו אילו פרסומות כדאי להציג בפני הגולש. תוכנה שכזו היא **Transponder**, שעוקבת אחר הרגלי גלישה ומידע שהגולש מכניס לסקרים, ובהתאם לכך, שולחת ל"קורבן" מידע פרסומי של מממניה.

• **חוטפי דפדפן** - תוכנות אלו גורמות לכך שדף הבית של המשתמש יהיה אתר פרסומי כלשהו ואינן מתירות את האפשרות לשנות זו. תוכנה שכזו היא **CoolWebSearch** שמנצלת פרצות אבטחה בדפדפן ומחדירה קוד **HTML** זדוני שמאפשר לה לשנות את דף הבית של המשתמש. תוכנה זו גם מחדירה סרגל כלים לחיפוש, אשר מפנה את המשתמש בו אך ורק לחברות המשלמות ליצרניה.

• **מנטרי מקשים** - תוכנה זו תייצר קובץ שישמור בתוכו כל תו אותו יקיש המשתמש ולפי הסדר, כך התוכנה תוכל לשגר סיסמאות, מספרי אשראי ושאר מידע רגיש לשרת-האם. תוכנה שכזו היא **Perfect Keylogger** שפשוט מנתרת כל תו במקלדת או הקלקה על העכבר.

• **חייגנים** - תוכנות אלו "חוטפות" את המודם וגורמות לו להתקשר אל אתרים הגובים תשלום, ללא ידיעת המשתמש. תוכנה שכזו היא **TIBS Dialer**, המקשרת את המשתמש אל אתרי פורנוגרפיה בתשלום.

• **מנטרי מערכת** - תוכנה המנטרת את כל פעילות המערכת החל מאתרים בהם ביקר הגולש, דרך ציתות לשיחות בהודעה מיידית או צ'אט וכלה בצילומי מסך או ציתות דרך מצלמת רשת או מיקרופון. התוכנה תשלח את כל המידע הרגיש לשרת מרכזי. תוכנה שכזו היא **007 Spy Software** שפשוט לוקחת את כל המידע שהוקלד, אתרים שביקר בהם המשתמש, שיחות שערך, צילומי מסך, צילומי מצלמת רשת וציתותים בעזרת המיקרופון ושולחת אותם דרך דוא"ל, למקום מוגדר מראש.

703.23 – כך נדבקים

יצרני הרוגלות מצאו דרכים מתוחכמות להדבקת מחשבים, ובהן:

• **התקנת תוכנה "תמימה" לכאורה** - תוכנות חינמיות רבות המחולקות **באינטרנט** מכילות בתוכן רוגלה, ועל אף שהדבר מצוין ב"חוזה ההתקנה", הוא כל כך ארוך, שקל לפספס את הסעיף (ולא תמיד קוראים אותו).

• **תרמיות Active X** - מצב בו נפתח בדפדפן חלון, הנראה כהודעה לגיטימית להתקנת תוסף מסוים, שכביכול נדרש. בפועל, לחיצה על "אישור" תגרום להתקנת רוגלה.

• **פתיחת דואר "ספאם"** - הרבה מהודעות הספאם, מכילות רוגלה שמתקינה את עצמה ברגע שהדואר נפתח או ברגע שנפתח קובץ המצורף אליו.

• **שהיה באתר נגוע** - לפעמים אתרים מסוימים מסוגלים להתקין רוגלות במחשבים של משתמשים שגלשו בהם באופן אוטומטי וסמוי, צורה זו של חדירה נקראת **DriveBy Installation**.

• **תוכנות שיתוף קבצים** - תוכנות אלו המאפשרות חיבור **Peer to Peer**, נותנות למיליוני משתמשים ברחבי העולם גישה למערכת שלך, עובדה המהווה נקודת פתיחה טובה למפיצי נוזקה, כולל **Spyware**.

703.31 – היכן הנזק?

רוגלות גורמות לארגונים נזקים כלכליים, בדרכים רבות:

• **האטה בתפקוד** - לרוב ההאטה אינה דרסטית, עם זאת גם האטה קטנה יחסית תתבטא בהפסדים כספיים רציניים - האטה של 10%-20% תעלה לארגון אחוז דומה מהשכר הכולל של כל העובדים המשתמשים ברשת, מאחר ועבודתם תתעכב.

• **קריאות שירות** - כל פניה ל-Help Desk הנובעת מרוגלות, עולה לארגון בין $15 ל-$45 (מחקר **Forrester**). בנוסף לכך, בזמן תיקון המחשב המשתמש אינו פעיל. לפי תחשיב **InformationWeek.com** בהנחה שבזמן תיקון התקלה העובד אינו יעיל ושתיקון עלול לקחת אף כחצי יום עבודה (עקב ניסיונות תיקון עצמיים, כולל התעסקות לא מיומנת בקבצי ה-**Registry**), עולה כי בארגון בן 1,000 עובדים שיתקל ב-10 תקלות שכאלו ביום עבודה, עלותן של רוגלות מסתכמת ב-$512,000 בשנה.

• **פתח לנוזקות** - לרוב רוגלות משאירות אחריהן פתח לנוזקות אחרות כגון וירוסים וסוסים טרויאניים, שעלולים לגרום נזק חמור בהרבה בעצמם. יש לזכור בהקשר זה, כי **Spyware** הוא בבסיסו סוס טרויאני.

• **סייבר-פשעים** - רוגלות מאפשרות להאקרים שיצרו אותן לגנוב מידע מהארגון ואף לרגל אחר עובדיו, הנזק לארגון יכול להיות עצום במקרה ומדובר בריגול תעשייתי. הרוגלות עלולות גם לשלוח סיסמאות חשובות מהארגון להאקרים, שבעזרתן יעשו ככל העולה על רוחם ברשת הארגון.

• **חייגנים** - חייגנים נמצאים בקטגוריה בפני עצמה מאחר והם מעלים עלויות באופן ישיר ואקטיבי. מודם שמתקשר לאתרים בתשלום באופן תדיר וממושך, יכול לגמד את העלויות השנתיות של כל הנוזקות האחרות במשולב.

יש גם מי שמרוויח מהצרות שלנו. יצרן הרוגלה מוכר את המוצר שלו לחברת הפרסום/שווק, החברה משלמת ליצרנית תוכנה חינמית לגיטימית שתכלול את הרוגלה בתוך המוצר (או לבעל אתר שיחדיר אותה מאתרו), את המידע שהתקבל החברה יכולה למכור לארגונים מסחריים או להשתמש בו על מנת לפרסם בעצמן. נראה שכולם מרווחים, חוץ מאיתנו. המאבק ברוגלות יוביל ארגונים לרכישה מאסיבית של פתרונות ושוק הפתרונות יעלה מ-12 מיליון דולר בשנת 2003 ו-31 מיליון דולר ב-2004 ל-305 מיליון דולר ב-2008 (**IDC**).

703.32 – שיקולים בבחירת פיתרון

להלן מספר שיקולים לרכישת מוצר אנטי-רוגלה:

1. **פרו-אקטיביות** - העדף פתרונות המסוגלים לזהות רוגלה לפי מאפיינים כלליים ולא רק לפי "חתימה".
2. **עדכונים** - חשוב שלספקית המוצר יהיה מרכז-מעקב אחר רוגלות חדשות, שיפעל באופן מקצועי ומיומן ושיוכל לעדכן את המוצר שאצלך בהגדרות רוגלה חדשות ובמהירות מרבית.
3. **שיתוף המידע** - תן עדיפות למוצרים שיאפשרו לך להתחבר לרשת אנטי-רוגלה (מערך משתמשים שמעבירים בין מחשביהם הגדרות רוגלה ונתונים על רוגלות שנמצאו בהם). המאמץ המשותף יסייע להתגבר על האיום.
4. **חיסול מלא** - לא כל המוצרים מוחקים קבצים נגועים באופן מושלם, העדף מוצר שלא משאיר "זנבות" (תוכל לבדוק זאת על ידי הפעלת גרסת נסיון של המוצרים השונים, על מחשב הנגוע ברוגלות מוכרות).
5. **זמן אמת** - דאג שהמוצר יוכל לזהות איומים ברגע שהם חודרים למערכת או ברגע שהם מותקנים, ובכך תמזער נזקים.

לארגונים חשובים גם השיקולים הבאים:

1. **בקרה מרכזית** - מומלץ לבחור פיתרון אנטי-ספיוור, שיוכל לנהל את עצמו על גבי כל העמדות השונות בארגון, בו זמנית ובאופן אוטומטי.
2. **סיכומים ודו"חות** - העדף מוצר שיפיק דו"חות וסיכומים לגבי הרוגלות ולגבי העמדות שנדבקו, ויעזור במציאת דרכי התמודדות.

703.33 – מחסלי הרוגלות

להלן מובאים מספר פתרונות אנטי-רוגלה בולטים בשוק:

• **Aladdin eSafe Spyware** - מגן על המחשב מרוגלות בארבעה אופנים - חסימת התקנת תוכנות אוטומטית, חסימת מאפייני רוגלה ברמת ה-**ActiveX** ותוספי דפדפן בלתי מורשים, סריקה לגילוי קבצי רוגלה שכבר הותקנה במחשב ובלימת תקשורת בין רוגלה לשולחיה. ☎ 03-6362222.

• **CA - Pest Patrol**, אשר לוכד את הרוגלות בעזרת בסיס נתונים מקיף, המתעדכן אוטומטית ממרכז הפיתוח של החברה דרך **האינטרנט**. על פי החברה, הפתרון ייחודי בכך שהוא מיועד גם להפעלה מרכזית בארגון (כולל מערכת דו"חות מפורטת, המאפשרת הצלבה וחיתוכי מידע) וגם למשתמש בודד, העובד מהבית. $39.99. ☎ 09-9626000.

• **Finjan** - מציעה פתרון אבטחה מפני רוגלות ברמת היישום, שימוש ברשימת אתרי הפצת רוגלה ידועים ורכיב אופציונלי לאבטחת ניידים המתחברים לרשת. ☎ 09-8648200.

• **Intel LANDesk Security Suite** הוא פתרון אבטחה משולב, מבוסס **LANDesk Management Suite**, הכולל גם איתור והסרה אוטומטיים של **Spyware**, ברמת הארגון. מחיר מומלץ לתחנת עבודה בשנה הראשונה הוא $59 ולאחר מכן $29 כמנוי שנתי. **P2P Support** ☎ 09-7401921.

• **LavaSoft** - מספקת מוצר בשם **Ad-Aware** שעובדת בעזרת בסיס נתונים המכיל מידע על רוגלות וגם בעזרת טכנולוגית **CSI** או **Code Sequence Identification** שמגלה איומים פוטנציאליים לא מוכרים בזמן אמת. $26.95 לגרסה הפרטית ו-$39.95 לגרסה הארגונית **www.lavasoft.de**

• **McAfee** - עם מוצר בשם **AntiSpyware** לו בסיס נתונים לזיהוי הרוגלות המתעדכן אוטומטית מה**אינטרנט**. ברכישת המוצר מציעה החברה שנה ראשונה של עדכונים בחינם. ניתן להשיג אצל **E.I.M** (☎ 1700-50-20-62) או מהאתר ($29.99) - **us.mcafee.com/root/package.asp?pkgid=182**

• **Microsoft** - שיחררה לא מזמן גרסת בטא למוצר **Anti-Spyware** הפועל בעזרת בסיס נתונים לזיהוי רוגלה המתעדכן דרך **האינטרנט** עם אופציה להשתתף ברשת מקוונת לזיהוי רוגלה, חסימת רוגלות בזמן אמת, וחיסול מלא של קבצים נגועים. התוכנה מוצעת בחינם - **www.microsoft.com/athome/security/spyware/software/default.mspx**

• **Panda** - חברת אנטי-וירוס בולטת, שמתחילה אף היא להיכנס לתחום. לסקירת מוצריה השונים לשוק הארגוני, ראה - **enterprises.pandasoftware.com** לבדיקת **Spyware** מקוונת, ראה **Panda ActiveScan**, בכתובת - **www.pandasoftware.com/activescan**

• **Spybot S&D** - משווקת מוצר באותו השם, המוצר עושה שימוש בבסיס נתונים המתעדכן בצורה אוטומטית מה**אינטרנט** ומגיעה בפורמט פשוט למשתמשים חדשים וגם במצב מתקדם למביני דבר. התוכנה היא חינמית לחלוטין- **spybot.safer-networking.de/he/features/index.html**

• **Trend Micro** - מציעה מוצרי אבטחה, המזהים ומסירים גם רוגלה, כולל **OfficeScan Corporate Edition** ו- **PC-cillin Internet Security 2005** (ל-PC בודד). **חילן** ☎ 03-6383850.

• **TrustWare AntiMalware** - **$10-$40** למשתמש) הוא פתרון שמגדיר הרשאות גישה, באופן המאפשר, לטענת החברה, למנוע נזקים מכל נוזקה, גם אם היא כבר פועלת במחשב וללא עדכוני חתימה. ☎ 03-6444012.

703.41– מדברים על ריגול

דיברנו עם מספר בעלי תפקידים המעורים היטב בתוך תחום אבטחת המידע.

רמי שלום, מנהל תחום אבטחת מידע ב**מיקרוסופט ישראל** (ramis@microsoft.com) מספר כי **מיקרוסופט** נכנסה לתחום האנטי-רוגלה עם הרכישה של חברת **Giant** מאחר ורוב הרוגלות משתמשות בתשתית של החברה בכדי לפגוע במשתמשים, דבר שמפנה את האצבע המאשימה גם ל**מיקרוסופט** ופוגע בשוק שלה. לדבריו, החברה מתקדמת לעבר הגישה הפרו-אקטיבית ופועלת להכרת נקודות החולשה במערכת ולמניעת המערכת מלעבוד בתצורה שתזיק לה עצמה, לפחות עד לשחרור טלאי אבטחה חדש. **שלום** מדגיש גם שרוגלות לרוב מצליחות לחמוק מעבר לתוכנות ה-**Firewall** ובין נזקיהן הרבים, החמור ביותר הוא כנראה הפגיעה בפרטיות האישית והארגונית, דבר שנחשב בעיקרון כבלתי נסבל.

אייל ווינדלר, מנהל תחום אבטחת מידע ב-**ICT** (☎ 09-9587722) מדבר בגנות פתרונות הרוגלה הקיימים כיום, המבססים את פעולתם על בסיס נתונים שלדבריהן אמור להכיל את המידע לגבי "כל הרוגלות", זאת מאחר ולדבריו הדבר מטעה ואף בלתי אפשרי. בנוסף גם במקרה שמאגר נתונים אכן יכיל מידע על כל הרוגלות, הדבר אינו מונע את האפשרות של רוגלה חדשה ולא מוכרת שתפגע במחשב. לדעתו ספקי האנטי-רוגלה יתחילו בקרוב, בדומה לעמיתיהם יצרני האנטי-וירוס, לבסס את הפיתרון ברמת ה-**Gateway** שיעבוד בגילוי רוגלה פוטנציאלית שאינה קיימת בבסיס הנתונים. כרגע ממליץ **ווינדלר** למנמ"רים לנקוט בחסימת **URL** ואי מתן הרשאות אדמיניסטרטיביות למשתמשים, בכדי למזער את סיכון החשיפה לרוגלה.

ניר בן יוסף, יועץ לאבטחת מידע ב-**CA** (☎ 052-6626672) קורא לרוגלות "מכה עולמית" ומספר שבשנים האחרונות נרשמה עליה של עשרות אחוזים בהיקף התחום, כאשר בשנה שעברה נרשמה עליה דרסטית במיוחד. לדעתו, העלייה נובעת מהשימוש ההולך וגובר בתוכנות המסרים המיידיים ושיתוף הקבצים. עוד מוסיף **בן יוסף** כי המאבק ברוגלות הוא מלחמה יומיומית, וכי זהו צורך בלתי מתפשר לעצור אותן, זאת מאחר והנזקים שהן גורמות לארגון, אף שאינם מיידיים כמו הנזקים שגורמים הוירוסים, הם קריטיים. לשם עצירת הרוגלות קיימים מרכזי-פיתוח החוקרים רוגלות חדשות בעולם, הדבר מצריך עבודה מסביב לשעון והישארות תמידית עם האצבע על הדופק, בכדי לצמצם ככל הניתן את הזמן מרגע הופעת הרוגלה ועד לעדכון בסיס הנתונים בתוכנות ההסרה.

703.42– טיפים למתגונן

להלן מספר עצות שיעזרו למנמ"ר לשפר את ההתגוננות הארגונית בפני הרוגלות.

- **חוות דעת שנייה** - לא כדאי להסתפק בפיתרון אנטי-רוגלה יחיד. לרוב, כדאי להתקין שניים או יותר, מכיוון שתמיד יהיו רוגלות שתוכנה אחת תגלה והאחרת - לא תגלה.
- **עדכן, עדכן, עדכן!** – הקפד להוריד עדכונים לתוכנה. הדבר קריטי, מאחר ורוגלות חדשות מיוצרות לבקרים, ותוכנה לא מעודכנת, לא תגן מפניהן.
- **חבור לקהילה** - במקרה שפתרון האנטי רוגלה שלך מציע אפשרות להפוך לחלק מקהילת שיתוף מידע אנטי-רוגלות (כמו בתוכנת ה-**Anti-Spyware** של **מיקרוסופט**) הדבר יעזור להגן עליך ועל יתר המשתמשים, על ידי קיצור זמן התגובה של חברת האבטחה לרוגלה החדשה.
- **שקול קוד פתוח** - מפתחי תוכנות מסוג זה, מאפשרים לכל משתמשיהן לבדוק את קוד המקור. גם אם לא כדאי לארגון הממוצע להיכנס לבדיקה יסודית (וגוזלת משאבים) של קוד כזה, עצם חשיפתו לעיניים רבות ברחבי העולם, מצמצמת סיכוי לנוזקה המובנית בו.
- **נטרל Spyware חוזר** - לעתים, נראה כי רוגלה "חוזרת לחיים" לאחר מחיקתה, ללא הסבר. הדבר יכול לקרות תוך נסיון לשחזר מערכת למצב קודם, בעזרת תכונת **System Restore** של **חלונות**, כאשר מנגנון התקנת או הפעלת הרוגלה מותקן מחדש אף הוא, מבלי משים. יש לשקול את ה-**Trade-Off** של תועלת תכונה זו מול נזקה האפשרי (הכולל גם "שחזור" וירוסים). ביטול זמני של התכונה והפעלת המחשב מחדש, עשויים למחוק, יחד עם מצבי המערכת שנשמרו, גם את הנוזקה.
- **שים לב** - שים לב לסימנים מדאיגים בתפקוד המחשבים כגון האטה, הופעת סרגלי כלים חדשים, תנועות עכבר מוזרות, פרסומות קופצות ושינויים בדף הבית, ודאג לבצע סריקה, כל אימת שמתעורר חשד.

דגש – הסכנות שבחיבור מרחוק

במקרים רבים, ישנה סכנה משמעותית של חדירת רוגלה, באמצעות עובדים שברשותם מחשבים ניידים. לרוב המחשב הנייד נלקח הביתה לצורכי עבודה, אך הוא משמש גם את יושבי הבית, לרבות ילדיו של העובד, העלולים לאפשר חדירת רוגלה למחשב משום שאינם מודעים לסיכונים ולאמצעי הבטיחות. בנוסף מאחר וניידים לרוב מתחברים לרשת הארגונית בעזרת שם משתמש וסיסמא הם הופכים פגיעים במיוחד לרוגלה מסוג **Key Loggers** (מתעדי מקשים). במקרה בו נייד נדבק ברוגלה מסוג זה, שם המשתמש והסיסמא של העובד עוברים לרשותו של ההאקר, שיוכל לעשות בארגון כבתוך שלו. סכנה זו נשקפת גם בפני מועסקים שעובדים מביתם.

703.43– אסטרטגיית "חיסון"

להלן מספר צעדים שיעזרו למנמ"ר הזהיר ב"חיסון" הארגון, בפני חדירה אפשרית של רוגלות:

1. **הצב חוקים** - הקפד על איסור התקנה של תוכנות בלתי מורשות (דוגמת תוכנות שיתוף-קבצים) וגלישה לאתרים מפוקפקים (כאתרי פורנוגרפיה).
2. **צור מודעות** - העבר סדנת מודעות לנושא, על מנת לשתף את העובדים בסיכונים שבגלישה ובדרכי ההידבקות האפשריות ברוגלות השונות.
3. **אכוף נכון** - השתמש בתוכנות שימנעו מהעובדים לגלוש לאתרים לא מאושרים או להתקין תוכנות כלשהן מהרשת, ללא אישור.
4. **צמצם גישה למערכת** - אל תאפשר לעובדים להתחבר לעמדתם כ-**Administrator**, ובכך תצמצם אפשרויות ביצוע שינויים לא-מורשים במערכת, גם עבור הרוגלות עצמן.
5. **נקה תדיר** - השתמש בפתרונות האנטי-רוגלה באופן תדיר, סמן לתוכנה לבדוק את המחשבים בתדירות גבוהה (המינימום המומלץ הוא פעם בשבוע. רצוי בשתי תוכנות). דאג בנוסף להשתמש באופציית ה"חיסון" במידה וקיימת בפיתרון.
6. **חסום את השער** - חסום ונטר פורטים, בעזרת תוכנות כגון **Firewall**. צעדים אלה עשויים לשבש פעולת רוגלה ולספק לך אינדיקציה על נוכחותה במערכת.
7. **בדוק בעצמך** - בצע חיפוש **בגוגל** בנושא רוגלות חדשות וכל הקשור בהן (מידע על אתרים ותוכנות שנחשפו).

703.51 – "עובדים" עלינו

אייל ווינדלר מנהל תחום אבטחת מידע ב-ICT הסביר על פעולת הרוגלות מההיבט הטכני – ראשית, התוכנה חייבת לחדור לתוך המחשב, הדבר יכול להיעשות על ידי אישור התקנה דרך **Active X** או התקנה של תוכנה המכילה רוגלה. עם זאת, ישנם אתרים מסוימים המסוגלים לשלוח מידע ישירות למחשב בעזרת **JavaScript** או **JavaApplet** דרך הפורטים 80 ו-443. קשה מאוד לתוכנות האבחון (אנטי-רוגלה, אנטי-וירוס, **Firewall**) להבחין בין קוד לגיטימי לקוד מזיק העובר דרך פורטים אלה, וחסימתם תגרום לשיבושים בגלישה.

לאחר שנכנסה, מפעילה הרוגלה את עצמה, לרוב מדובר בפיסת קוד זדוני אותה קשה מאוד לגלות, זאת מאחר ובניגוד לוירוסים, הרוגלות אינן מריצות פקודות של פתיחת פורטים או העמסה על זיכרון **(buffer overflow)**.

פעולתה של הרוגלה בתוך המחשב מבוססת על שימוש לרעה בטכנולוגיה הלגיטימית של **מיקרוסופט** וספקיות דפדפנים אחרות כדוגמת **Mozilla**. **מיקרוסופט** מאפשרת לכל יצרן לכתוב תוכנות לסביבת **חלונות** כשהקוד וההסברים נגישים גם ליצרני הנוזקות למיניהן.

את המידע, הרוגלה שולחת לרוב דרך פורט 80. מאחר והשליחה מתבצעת מתוך המחשב החוצה תוכנת ה-**Firewall** לא תחסום את המידע הדולף ואילו סגירה מוחלטת של הפורט תימנע גלישה לחלוטין. בנוסף תוכנות מסוימות שולחות מידע דרך חשבון הדוא"ל של הקורבן.

שאלה מעניינת היא, האם **Cookies** מהווים רוגלה? התשובה היא לרוב לא, כאשר תוכנות אנטי-רוגלה יזהו אותן כמסוכנות, רק אם הן הותקנו על ידי יצרן הרוגלה עצמו. אם כי **Cookies** לגיטימיות עשויות להיקרא גם על ידי תוכנות צד שלישי (כרוגלה), הן עצמן לא אוספות מידע באופן אקטיבי וקל מאוד להסירן.

703.52 – פתרונות מוגבלים

להלן כמה אתגרים, המקשים על פתרונות האנטי-רוגלה בעבודתן התקינה והאפקטיבית:

• **הגורם האנושי** - לרוב הגורם האנושי אחראי על החדירה עצמה של הרוגלות בכך שלא שם לב לכללי הזהירות. בנוסף מועסקים רבים ישכחו לעדכן את הפתרונות ובכך יפגמו ביעילותם.

• **רוגלות לא מזוהות** - לא תמיד התוכנות יזהו כל רוגלה שחודרת למחשב ומתוך כך לא יאפשרו הסרתה. למעשה, מקובל השימוש בזוג תוכנות אנטי-רוגלה, ואף יותר, מאחר ופעמים רבות, כל אחת מהן תזהה גם רוגלות שהשניה לא זיהתה!

• **צעד אחד אחורה** - כמו בכל ענף האבטחה, התרופה לרוב באה רק אחרי המכה ויצרני הרוגלות נמצאים תמיד צעד אחד לפני מפתחי הפתרונות, דבר זה יוצר פרק זמן מסוים בין יציאתה של הרוגלה החדשה עד למציאת הפיתרון להסרתה וכך היא מספיקה לגרום נזק.

• **סיבוכים בהסרה** – לרוב, רוגלות משנות קבצים חיוניים למערכת והופכות אותם לתלויים בהן כך שהסרתן תפגע בתפקוד המחשב או הרשת כולה.

• **קוד חוקי** - יצרני רוגלות נעזרים לעתים בהסבת קוד של תוכנה חוקית, כפתרונות ניטור גלישה (להורים או לארגונים). מקרה דרמטי מסוג זה, אם כי יוצא דופן, היה חשיפת תוכנת המעקב **D.I.R.T** של כוחות הביטחון ב**ארה"ב** (אם כי ללא קוד-המקור), באתר פתוח לציבור.

• **פתרונות מפוקפקים** - לסיום, נזהיר מתופעה חדשה: אם מישהו ב**אינטרנט** מנסה לשכנע אותך בהפחדות לרכוש תוכנה דוגמת **Spyware Assassin**, סביר שאותה תוכנה אכן תגלה אצלך, כביכול, רוגלות רבות. אלא שאנו נגלה (ונחסוך) לך, שפעילות היצרנית **MaxTheatre** הופסקה על ידי בית-משפט ב**ארה"ב**, לאחר שהתגלה כי מדובר בהונאה.

דגש – ההיבט החוקי

נושא הרוגלות "כיכב" לאחרונה בבתי משפט רבים בארה"ב. טענתן של יצרני הרוגלות, מחד, היא שאינם עוברים על שום חוק ושזוהי זכותם החוקתית לפרסם ולהתפרנס. טענת-הנגד, היא שהדבר נעשה בפגיעה ברווחי הפרסום של אתרים **באינטרנט** וחמור מכך בפגיעה במשתמשים שנחשפו לרוגלות. לאחרונה, חלו כמה התפתחויות חיוביות בנושא החקיקה כנגד רוגלות. **בסנאט האמריקאי** אושרו שתי הצעות חוק (והשלישית בדרך) שיאפשרו לראשונה לסגור חברות המפיצות רוגלות ואף לדרוש מהן להחזיר את הכסף שהרוויחו מכך. בנוסף, במדינת **יוטה** עובדים על חוקים שימנעו מיצרני רוגלות לחדור למחשבי תושבי המדינה, כשעוד מדינות עוקבות אחר הדרך שמתווה **יוטה**. את המלחמה החוקית בספאם מבססות גם זכיות חשובות כמו במקרה של **EarthLink** שזכתה בתביעה של 2 מיליון דולר נגד "מלך הספאם", **סנפורד וואלאס**, ב**קליפורניה**.

703.53 – עשו נזק

איום הרוגלות כבר גבה מחיר משמעותי ממשתמשים וארגונים רבים, להלן תיאור חלק מהנזקים והקורבנות:

• **בעלי חשבון בנק מקוון** - ניזוקו רבות מתרמיות רוגלה שרוקנו חשבונות שלמים. ב**גרטנר** מעריכים כי התופעה פגעה ב-1.98 מיליון איש, וכי העלות השנתית של ההונאות מסתכמת ב-2.4 מיליארד דולר. לאחרונה, הגבילו הבנקים הגדולים ב**ניו-זילנד** גישה מקוונת לחשבונות בגלל התראות על **Spyware**.

• **Dell** - החברה טוענת כי בין 10% ל-12% מסך קריאות התחזוקה של מחלקת השירות שלה נגרמות על ידי רוגלות. סקר של החברה, מגלה שכמעט ארבעה מכל עשרה משתמשים, מרגישים בטוחים פחות בהפעלת המחשב מכפי שהיו לפני שנה, עקב התפשטות **Spyware**.

• **Microsoft** - טוענת כי 50% מקריסות מערכות ההפעלה שלה, נגרמות על ידי הפרעות רוגלה והדבר גורם נזק שיווקי ומעלה את עלויות מתן השירות.

• קריאות **Help Desk** - ארגונים כיום משלמים כסף רב על כל קריאת **Help Desk** (לתיקון המחשב) שנגרמה על ידי רוגלה. בנוסף, כ-50% מכלל קריאות ה-**Help Desk** מבוססות רוגלה **(Forrester)**.

• **נזקי פרסום** - 2 חברות מדינת **יוטה** תבעו את יצרנית ה-**Adware** שנקראת **WhenU.com** על סך של מיליוני דולרים, מאחר ולטענת החברות התוכנה גורמת לפרסומות של חברות מתחרות, להופיע באתרים שלהם.

703.61 – במסלול יומי

במסלול יומי של 2-5 דקות ניתן לקבל באתר www.PCON.co.il פרספקטיבה יומית, עדכנית ותמציתית, על החדש והחשוב בענף המחשוב.

- **בכותרת היום** - דיווחנו על **יאהו בכיס שלך..** - **בלקברי**, מכשירי כף היד הסלולריים, קיבלו חיזוק השבוע, כשנודע שבקרוב יגיעו עם **יאהו מסנג'ר** מותקנת עליהם.

ראה גם בארכיון - www.PCON.co.il/HeadlineArc

- **באתר הנבחר** - סקרנו את **פז בשטח - Paz Logistics** - אתר חברת **מ. פז לוגיסטיקה**, המשווקת מגוון מוצרים רחב, מערכות ומיכלולים מתקדמים, בתחומי האלקטרו-אופטיקה, ניווט, תקשורת ועוד. בחרנו להתמקד ביישומי ה-GPS ושילובם במערך המידע הארגוני.
- **בהכרזה היומית** - תמצא את **מחפש משהו?** - על השקת **EMC Centera Seek**, תוכנה לחיפוש ואחזור מהירים ויעילים בארכיבים ארגוניים הבנויים על מערכת ה-**Centera**. התוכנה מאפשרת חיפוש מתקדם ואחזור של תוכן מובנה בארכיבים מורכבים רחבי היקף, על ידי שימוש ב- **EMC Centera Chargeback Reporter** הנכלל בה. כלי זה מספק דיווחים מפורטים על המידע בארכיב למערכות **Chargeback** ארגוניות ומתעל **Metadata** מאוחסן לאספקת דיווח שימוש מותאם.
- **פיקנטי במחשוב** - כותרתנו הפעם היא **זוב'תי באמשך..** (לא טעות דפוס..), ואם תרצה להבין למה הכוונה, תלמד שם על **המילון האורבני המקוון**, המנסה לספק פירושים למונחי סלנג שונים. התוצאות לא בהכרח מדויקות (מבוסס על פירושים שמוסיפים הגולשים), אך תמיד מעניינות.

703.62 – מסרים ממוביל'י המחשוב

בכל שבוע תמצא את עיקרי החזון והניסיון של אנשי מפתח מובילים בתחומי המחשוב בישראל:

- **בחזון המנכ"ל** - מדבר **ברוך שלו**, מנכ"ל משותף ב-**IQS** על עשיית **סוף לגניבת הזהויות**: "אנחנו מאמינים, בצורך במניעת התחזות ובזיהוי ודאי, בכל מקום בו יש נגיעה לכסף, בטחון ומערכות מידע. בעיית גניבת הזהויות היא בעיה שצריך למצוא לה פתרון, וחברת **IQS** שמה לעצמה למטרה להצטרף לארגונים המחפשים פתרון לכך".

ראה גם בארכיון - www.PCON.co.il/LeaderArc

- **בניסיון המנמ"ר** - מציע **אבי אג'ימן**, מנמ"ר **מטרומרקט** **להשקיע בחומרה איכותית**: "אני מאמין בלשלם יותר על החומרה, בכדי להרגיש בטוח יותר. ...הסיסמה שלי היא: אני לא עשיר מספיק, בכדי להשקיע בחומרה זולה".

ראה גם בארכיון - www.PCON.co.il/CIOArc

703.63 – תועלת מיידית מהתחקיר

כדי לאפשר לבדוק את ישימותו המיידית של תחקיר זה, לשתף ולבקש התייחסות של אנשי מפתח בארגון, כמו גם לערוך דיון קצר בנושא, שאל עצמך:

1. האם קיים מערך הגנה כנגד רוגלות בארגון? אם כן, האם הוא עונה על צרכינו?
2. באיזו מידה מתלוננים משתמשי הארגון, על תופעות של האטת מערכות?
3. האם יישומן של שיטות ההגנה המתוארות בתחקיר יכול לשפר את מערך ההגנה הארגוני בפני רוגלות?
4. האם אני מודע להתפתחויות החדשות באיומי הרוגלה?
5. האם אני מודע לפתרונות החדשים בתחום?

ראה - www.PCON.co.il/Apply

703.64 – פוקוס על חיפוש חכם

דוגמא מעשית, תמחיש תועלת נוספת שתמצא באתר:

בתחקיר ממוצע של **PCאון**, מופיע מספר לא מבוטל של מונחים טכניים שונים, ראשי תיבות ויחידות מדידה לא מוכרות. כך גם בכל מסמך טכני אחר בתחום המחשוב - ואין אדם שמכיר את כולם. הדבר מקשה על רבים להתמצא במהירות בתחומים טכנולוגיים חדשים או לא מוכרים. "איך ניתן למצוא במהירות פירוש לראשי תיבות ומונחים טכנולוגיים?" - נשאלנו לעתים קרובות.

עבור אלה ששאלו - וגם בשבילך - הוספנו אפשרויות חיפוש מהיר, ישירות **מדף הבית של PCאון**. החיפוש יבוצע, לבחירתך, באתר **Google**, באתר **NeteX** או באתר **PCאון** עצמו, בו תקבל תוצאות רלוונטיות מתחקירי **PCאון**, מידיעות חדשותיות שפורסמו בו, מהכרזות רלוונטיות ועוד.

לניסיון, בדוק אותנו ב - www.pcon.co.il

703.65 – דקה לטיפ דקה לחיוך

במסגרת טיפ יומי קצר ושימושי ניתן בכל יום לעשות אתנחתא לרכישת תובנה או יכולת חדשה, ולהתעדכן בגימיקים המצחיקים ביותר שמסתובבים ברשת.

כך למשל הראינו במסגרת **קיצור הדרך** של יום **שני**, כיצד ניתן לתזמן שליחת אימייל, למועד הנוח לך. בכדי לתזמן שליחת מייל בתוכנת **Outlook** -

1. לאחר כתיבת ההודעה בשלמותה (כולל הנמען)..
2. הכנס לתפריט **קובץ** ולחץ על **שמור**.
3. הכנס לתיקית **טיוטות** וגרור את ההודעה אל איקון **Calendar** בתפריט קיצורי **Outlook**.
4. בחלונית שנפתחה, הגדר את זמן השליחה הרצוי.

לטיפים נוספים - www.PCON.co.il/TipArc

ולבסוף, לניקוי ראש ולהרגשה טובה בסיום כל הפסקת צהריים, תוכל לקבל גימיק משעשע עם הקדמה שמותחת ומגבירה את החוויה. למשל - בגימיק **מי חי יותר?** תגלה:

☺ כיצד פועלים בעלי חוש ספורטיבי, משחקים לגו-מלגזות (זה כבר נכנס לאולימפיאדה, לא?..).
☺ מה עושה גבר-גבר רב-תושיה, כשהסולם קצר מדי?
☺ מדוע נשים לא יודעות לנהוג (וגברים כן, כמובן..) - את ההסבר וההוכחה הניצחת, מספק נהג נועז המוביל פצצות.
☺ מדוע גבר אמיתי לא צריך חגורת בטיחות / קסדה / עזרה מאף אחד?
☺ כיצד מסתדר אדון תושיה עם עבודה שחייבים לעשות מעל המים? בוא נראה - סולם מתכת? יש. כלי עבודה ב-220 וולט? רשמנו v. אני יחף? כן. אז קדימה לעבודה! **ISO** מה?..
☺ איך מרימים אוטו בצ'יק-צ'ק, רק בלי ג'ק..?
☺ כמה גברים צריך בשביל להחליף מנורה?
☺ ולבסוף - המסקנה המצטברת מאוסף תובנות מאיר-עיניים זה או מדוע נשים חיות יותר זמן מגברים.

לגימיקים נוספים - www.PCON.co.il/GimikArc

להרשמה חינם למייל היומי של **TipPCon** - www.pcon.co.il/TIPSUB