כלכליסט

שבת 10 ינואר

טכנולוגי | אינטרנט

מכה לציר הרשע גרסת האינטרנט

מתחת לאף של כולנו צמחו ברשת ארגוני ענק של האקרים שגונבים מיליארדי דולר בשנה. חברת אבטחת מידע ישראלית פרצה לאחד ממחשביהם, ומעניקה הצצה למערכת פשיעה מתוחכמת שלא פסחה על ישראל

צמרת פרנט

24.12.08, 09:15

3 תגובות

גניבת המסמכים הסודיים של התעשייה האווירית אירעה כמעט במקרה. אחד מעובדי מערכת הביטחון נדבק בתחילת השנה בתוכנת ריגול, בעת שגלש באינטרנט. ואולי הוא קיבל דוא"ל מאדם לא מוכר, והפעיל קובץ מצורף שהשתיל במחשבו סוס טרויאני. כך או אחרת, מרגע שנדבק בתוכנת הריגול, כל הסיסמאות שהקליד אותו עובד נשלחו אל מחשב מרוחק. הסיסמאות הללו התווספו למאגר של כ־200 אלף סיסמאות ששימש את מפעילי המחשב המרוחק כמפתח גנבים ענקי לאתרי אינטרנט. תוכנות מיוחדות סרקו את הרשת, ובכל פעם שנתקלו באתר של בנק, חברת כרטיסי אשראי או סתם אתר נעול, הם ניסו במהירות להתאים לו סיסמה. כשהגיעו, במסגרת סריקת הרשת, לשרתי התעשייה האווירית, פעלה הסיסמה הגנובה, והמסמכים באתר הועתקו אל השרת, כדי להימכר מאוחר יותר בשוק השחור.

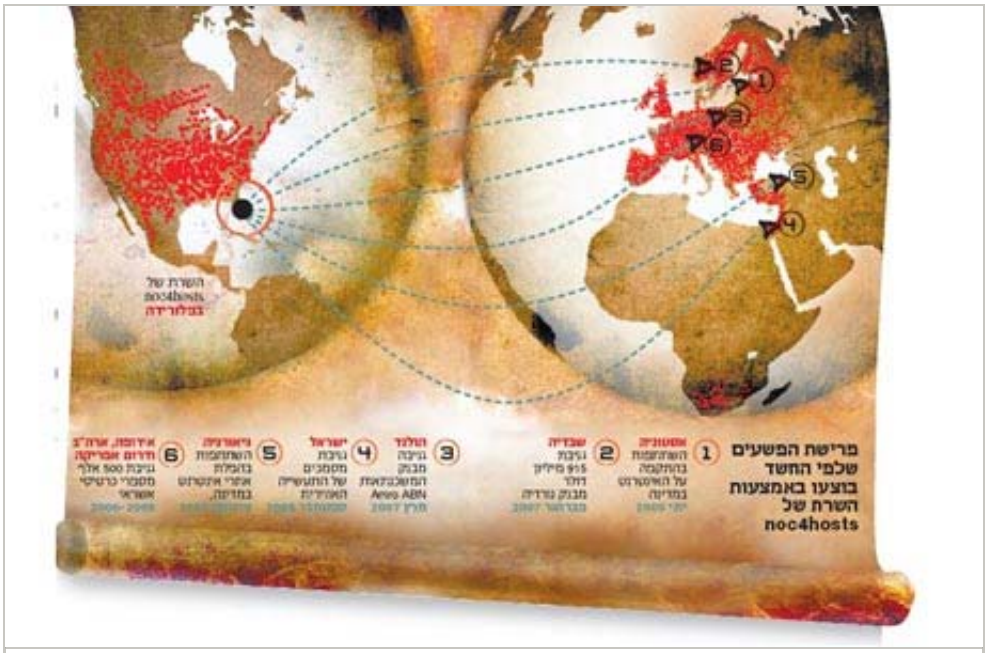
"נתקלנו בהם רק בספטמבר", אומר יפתח עמית מחברת האבטחה הישראלית אלדין, שהצליחה לחדור לאותו מחשב האקרים מרוחק, מחשב שמומחי אבטחה בעולם מתארים כ"מה שעשוי להיות אחד מהמחשבים הפיזיים הגדולים ביותר ששימשו לביצוע עבירות ברשת". "במשך הרבה זמן עקבנו אחרי פריצות של האקרים לאתרים באירופה", אומר עמית, "וגילינו שהמון פריצות מגיעות מאותו המקור. העקבות הדיגיטליים הובילו לשרת אחד מסוים שפעל מטמפה, פלורידה. הצלחנו לפרוץ אליו ומצאנו בו מערכת עסקית מסודרת עבור האקרים".

הגילוי של אנשי האבטחה של אלדין, שמפורט בדו"ח חדש של מחלקת המחקר שלהם, הוא אחד ההישגים הדרמטיים ביותר שאירעו לאחרונה בעולם אבטחת המידע, הישג שחשף את המידה שבה פשעי המחשב הפכו לתעשייה עסקית יעילה ומאורגנת. "בתוך השרת שניהל את ההתקפות מצאנו 'לוח בקרה' להפעלה מרחוק של מחשבים שהאקרים השתלטו עליהם. מצאנו דוחות סטטיסטיים ומדריכים. זה ממש שירות עסקי. מצאנו שם גם רמזים לכך שלפחות שלושה ארגונים גדולים פועלים באמצעות המחשב הזה לגניבת מידע פיננסי, ומצאנו בו עוד הרבה חומר שנגנב מאתרים בעולם". בדיקת "כלכליסט" העלתה כי בשרת נמצאו מסמכי התעשייה האווירית שהיו בסיווג "סודי ביותר", ובין השאר כללו רשימות של בכירים בתע"ש וכן תוצאות ניסוי שנערך בשטחה של מדינה זרה. "הם לא ניסו לרגל אחרי ישראל", אומר עמית, ראש צוות חטיבת המחקר eSafe באלדין, שנמנה עם מחברי הדו"ח שמתעד את החדירה לשרת ומנתח את ממצאיה. "זה פשוט ארגון עסקי, שגונב מה שהוא יכול וסוחר בזה. השרת הזה הוא ההוכחה לכברת הדרך

שעבריינות הרשת עברה בשלוש השנים האחרונות, ולכך שהיא הפכה לתעשייה כלכלית שמגלגלת מיליארדים. אני מקווה שהנזק שגרמנו להם יאט אותם קצת".

נפילת ברון הספאם

כשחברת אלדין העבירה את המידע שגילתה למשטרה ולרשויות החוק האמריקאיות, היא עדיין לא ידעה כמה חשוב הגילוי. חודשיים לאחר העברת הפרטים לארה"ב הגיעו אנשי FBI למשרדיה של ספקית אינטרנט קטנה בשם McColo, שפעלה מסן חוזה, קליפורניה, והחרימו את כל מחשבי החברה. כעבור דקות צנחה תעבורת הספאם בעולם ב־75%. "זה רק שלב בדרך לעיקר", אומר עמית. "חברת McColo, שהיתה למעשה קבלנית ספאם ענקית, היתה רק אחת מכמה ארגוני פשיעת רשת אמריקאיים גדולים. הם לא אלה שמפעילים את השרת, שעדיין פועל מפלורידה. עכשיו בארה"ב אוספים ראיות כדי להפיל את החברה שמחזיקה בשרת, חברה בשם noc4hosts".



הפשעים שבוצעו לפי החשד משרתי noc4hosts

noc4hosts היא חברה אמריקאית לאירוח אתרים. היא ידועה בתעריפים הנמוכים שלה, ולפי הארגון הישראלי למעקב אחרי התקשורת בעולם הערבי ממר"י, היא מארחת בין היתר אתרים אסלאמיים המזוהים עם אל־קאעידה. המגזין "נטוורק וורלד" של סוכנות ידיעות המחשבים IDG פרסם בתחילת השנה שהחברה מסייעת לאתרים אסלאמיים להצפין מידע ברשת, ובלוגים העוסקים באבטחת מידע ממליצים זה חודשים לחסום אתרים שפועלים משרתיה.

למה לא עוצרים אותם עכשיו?

"רשמית, הם בסך הכל מארחי אתרים. לפי מה שאני מבין, בימים אלה מחפשים ראיות ומנסים להכין להם תיק", אומר עמית. לאחר סגירת חברת McColo נשאל דובר ה־FBI האם הפעולה היא חלק מחקירה נרחבת יותר. הוא סירב להגיב.

בחברת אלדין מספרים שלאחר שניתחו את הממצאים מהשרת, הם הצליבו אותם עם מידע שנשאב מפורומים מחתרתיים של האקרים שנמצאים תחת מעקב, עם מאגרי מידע של הממשל האמריקאי ועם מידע של היחידה למניעת פשע מאורגן בהולנד, שמחזיקה במאגר המידע הגדול ביותר בתחום הפשיעה ברשת. "גילינו שהארגונים שהשתמשו בשרת הם גדולים ומאורגנים", אומר עמית. לדבריו, אחד מהארגונים השתמש בשירותי השרת כדי לגנוב כ־900 מיליון דולר מבנק נורדיה השבדי בתחילת 2007. הגניבה בוצעה

לאורך שלושה חודשים, באמצעות סיסמאותיהם של 250 מלקוחות הבנק, שנדבקו בסוס טרויאני. "הארגונים השתמשו בשרת כדי להשתיל תוכנות ריגול ביותר מ־87 אלף אתרים, והמערכת אפשרה לארגונים לשאוב סיסמאות מכל הגולשים שביקרו באתרים ונדבקו בתוכנות הללו. היא כללה אפילו ממשק נוח לשליטה במחשבים הנגועים", אומרים באלדין.

עוד פשעים שאלדין מקשרים לארגונים שפעלו באמצעות השרת של noc4hosts הם גניבת ענק מבנק המשכנתאות ההולנדי Amro ABN והשתתפות בהתקפה על אתרי אינטרנט באסטוניה בשנת 2005. בחודש נובמבר דיווחה חברת האבטחה האמריקאית RSA כי הארגונים שמשתמשים בשרת גנבו יותר מ־500 אלף מספרי כרטיסי אשראי ופרטים של חשבונות בנק ברחבי העולם, ובעיקר במערב אירופה, ארה"ב ודרום אפריקה.

פניות של מערכת "כלכליסט" לחברת noc4hosts מפלורידה לא זכו לתגובה מצדם.

ההאקינג המאורגן

"מה שהרשים אותנו היה המידה שבה הפכה הפריצה למחשבים לתעשייה מסודרת", אומר עמית. "אם פעם היה צריך לגייס האקרים כדי שיפרצו עבורך לאתרים, השרת הזה הוא דוגמה לדור הבא: הוא מציע לעבריינים שירותים בתשלום, מדריכים, השכרת שירותי תוכנות ריגול ומעקב אחרי המחשבים המודבקים. הכל באופן מאובטח, 'ידידותי למשתמש' ממש. המחירים גבוהים, ולכן הלקוחות הם כמה ארגונים גדולים מארה"ב ומאירופה, אבל החידוש הוא שהיום כל מי שיש לו כסף ומצליח ליצור קשר עם בעליו של שרת כזה, יכול להשתמש בכלים שיאפשרו לו לגנוב מידע פיננסי ולגרוף סכומים לא מבוטלים".

"עולם הפשע באינטרנט צובר תאוצה רק בשנים האחרונות, ובעיקר בשנה וחצי האחרונות", אומר עמית. "רשויות החוק בעולם עדיין לא למדו להתמודד עם הארגונים האלה, ולכן את עיקר המלחמה מנהלות חברות מסחריות. למיקרוסופט, למשל, יש מחלקה משפטית ענקית שפועלת כיחידה ללוחמה בטרור־רשת. היא לקחה את זה על עצמה בגלל שחלק מפעילות הארגונים הוא סחר בתוכנות פיראטיות".

מיהן "משפחות הפשע" של האינטרנט?

"קשה להצביע עליהן", אומר עמית. "אנחנו עוקבים אחרי שישה או שבעה ארגונים, שמשתמשים בכינויים שונים, ולפעמים קשה לנו לדעת איזה כינוי שייך למי. אבל רוב הפעילות העבריינית ברשת מתבצעת על ידם, ומדובר בנזקים של מיליארדי דולרים בשנה".

מנתחים את הצעד הבא

"השאיפה שלנו", אומר עמית, "היא לא רק לעזור לרשויות החוק להעניש האקרים, אלא גם להבין כיצד מתנהלים עסקי הפשיעה ברשת, ולצפות מראש את דפוס הפעילות העתידי. בעבר חוקרי אבטחת מידע היו מנתחים התקפות בדיעבד. כיום אנחנו מנסים לחזות אותן מראש. למשל, מצאנו בשרת תוכנה מעניינת שמשנה מדי כמה זמן את נתוני המיקום הגיאוגרפי וכתובת האינטרנט שלו. לאחר שניתחנו אותה, אנחנו יודעים מה יהיו הכתובות שלו בכל תאריך נתון בעתיד, וכך נוכל להמשיך לחסום את האתרים שפועלים ממנו. אבל מה שבטוח הוא שכל עוד המודל העסקי שלהם לא נפגע, הפעילות שלהם תמשיך", מסכם עמית, "עכשיו גם הם חושבים על המהלך הבא".