מאמרים
רשת הפצת מאמרים מקצועיים לשימוש חופשי

# מכה חדשה ישנה- גניבת שמות דומיין

מאת אורן שני [ 29/09/2008 ]

מכה חדשה ישנה - גניבת שמות דומיין
אם קיבלתם פנייה לקניית הדומיין שלכם חזרה - אתם לא לבד

אם חשבנו שמכת גניבת שמות הדומיינים (שמות מתחם) מאחורינו- טעינו. בימים אלה מקבלת חברת אבנת פניות חוזרות ונישנות של לקוחות, אשר שמות דומיין הדומים לשלהם נרכשו. לא די ששמות דומיין אלה נרכשו ע"י גורמים שאינם קשורים לארגון, הקונים מנסים למכור בחזרה ללקוח את הדומיין.

ברור שדומיין פעיל שאינו שלך, אליו יש סיכוי שלקוחותיך ייכנסו אינו מצב נוח. הנתונים המוצגים בו אינם בשליטתך, היכולת להטעות את הלקוחות קלה יחסית, קיימת אפשרות של בעל הדומיין לבצע הפנייה אוטומאטית של כל הנכנסים לכל יעד בו יחפוץ וכמובן שאפשר להשתמש בדומיין לביצוע התקפות - Phishing (גניבת נתונים תוך התחזות לאתר המקורי).

ארגונים החושבים "להיפטר מהבעיה" ע"י קניית הדומיין חייבים לקחת בחשבון כי גם אם יחליטו לקנות את הדומיין הבעיה לא תפתר שכן שמות הדומיין הקרובים הינם רבים ומגוונים, גם בצורת רישום שם הדומיין (עם קו תחתון, בלי קו תחתון, שם מלא, ראשי תיבות) וגם כמובן ברמת הסיומות (co.il, com ורבות אחרות).

ארגונים רבים ביצעו בעבר רכש מסיבי של שמות דומיין קרובים על מנת להימנע ממצבים אלה. עלות שם הדומיין זניחה יחסית (עשרות דולרים בודדים בשנה), כך שגם קנייה של דומיינים רבים מסתכמת בסכום לא גדול יחסית. ארגונים שרכשו שמות דומים ביצעו הפנייה אוטומאטית משמות הדומיין הקרובים לדומיין המוביל ובכך ניסו להימנע ממשחק החתול והעכבר.

אורן שני, מנכ"ל אבנת העוסקת בייעוץ אבטחת מערכות מידע: "בעיית גניבת שמות דומיין הינה בעיה ידועה ומוכרת ומשמשת גורמים עוינים כחלק מתקיפות Phishing, כך שלאחר שקיבל הגורם המותקף מייל מזוייף הוא יופנה לאתר בעל שם דומה אשר לא נראה חשוד. פעולה זו מבוצעת על פי רוב כחלק מהערכות התוקף להידמות ככל הניתן לגוף אותו הוא תוקף על מנת לצמצם את החשד אצל הלקוחות. כחלק משירותי אבטחת המידע שמספקת אבנת, ביכולתנו להתריע בפני כל לקוח אודות שמות דומיין הדומים לשלו אשר עלו לאוויר על בסיס יומי ובכך להתריע אודות פעולה עויינת אשר עשוייה להתרחש. כמו כן, פיתחנו כלי אשר ביכולתו לחולל שמות הדומים לשם הדומיין הקיים, כולל שינויים בשם המדוייק, שינוי הכתיב ושינוי סיומות, שמטרתו בחינה ודיווח אודות קיומם של דומיינים פעילים בשמות דומים".

מה ניתן לעשות: מבחן העבר מראה שלבעלי שמות דומיין קרובים אין עתיד מזהיר. בין אם חיוב בתי משפט להעביר לידי הלקוח החוקי את הדומיין ובין אם מאבק ארוך טווח בסופו הם מוכרים את שם הדומיין בסכום פעוט. ניתן לציין את 411 אשר ניסו לתת שירות הפוך לזה של 144 בו בסופו של יום הופסק השירות וכיום משמש להפניות ישירות לאתרים. או את הפסיקה מחודש נובמבר 2007 בה הורה שופט בית המשפט המחוזי בירושלים לשנות שם דומיין של אתר עסקי אשר הטעה לקוחות פוטנציאליים לחשוב שמדובר בעסק מתחרה ששם הדומיין שלו דומה וזאת במסגרת עוולת תיאור כוזב. ניתן כמובן להשתמש בשירות של איתור שמות דומים, כאשר במקרה זה יש לעקוב אחר תכולת האתר לאחר הקמתו ומידת הקשר בין האתר המוקם לארגון ולפעול במידת הצורך, כולל ברמה המשפטית.

הכותב הוא אורן שני,מנכ"ל אבנת אבטחת מערכות מידע וניהול סיכונים
http://www.avnet.co.il
oren@avnet.co.il

**מקור המאמר:** www.Articles.co.il - מאמרים לשימוש חופשי