

מהי הדרך לחזק סיסמה

כיום קל לפרוץ סיסמאות, גם ארוכות מאוד, באמצעות שימוש בכרטיסים גרפיים במקום במעבדים המרכזיים הרגילים - כך אמר **רועי ליפמן**, ארכיטקט תוכנה ב-AVG. לדבריו, "רוב הסיסמאות הן שמות בעלי חיים, תאריכים משמעותיים, שמות הילדים, שמות של בני משפחה אחרים ומושגים רבים מהסוג הזה. הפתרון לכך הוא הגדלת טווח התווים".

"סיסמה חזקה מאופיינת בטווח התווים שלה. שימוש בספרות מאפשר אך ורק עשר אפשרויות לכל תו, הוספה של תווי הכתב האנגלי מגדילה את האופציות ל-62, ושימוש בכל התווים שבמקלדת נותן לנו 94 אפשרויות לכל תו.

"עבור סיסמה של שמונה תווים שכולם ספרות ישנן מאה מיליון אפשרויות, ככל שנצל יותר אפשרויות, מספר האופציות יילך ויגדל. ג'ימילי, פייסבוק, אתרי הבנקים ודומיהם מבקשים פרטים מזהים

וסיסמה. המערכת מצפינה את הפרטים בבסיס נתונים, ומעבירה את הסיסמה דרך פונקציית האש (HASH), שגורמת לכך שכל הסיסמאות תהיינה בעלות אותו אורך. אין אפשרות לחשב בכיוון ההפוך".

ליפמן נתן הסבר טכני, לגבי ההבדלים בין הכרטיסים השונים בהקשר לפריצות: "בעוד ה-CPU מאפשר להריץ 250 אלף ערכי האש בשנייה, ה-GPU יכול לחשב מיליארד לשניה. כרטיסים גרפיים מגיעים עם 2,900 ליבות, שעון של 900 מגהרץ וזיכרון של 3 ג'יגה. הרעיון של הרצת קוד על המעבד הגרפי מצריך מודל חדש - מודל מקבילי. לא ניתן לקחת כל בעיה ולהשליך על ה-GPU. בעיות שכן כדאי לפתור הן בעיות שניתן לשבור אותן לתתי בעיות הרבה יותר קטנות, לקחת את כל הפתרונות הקטנים ולאחד לפתרון אחד גדול.

"כדי לכתוב על הכרטיס הגרפי - NVIDIA הציגה את CUDA שיכולה לרוץ על המעבד הגרפי. אם אדם רוצה לחשוף סיסמה של 8 תווים עם אותיות וספרות במעבד, ייקח לו 17 ימים. בכרטיס גרפי הדבר ייקח לו יומיים בלבד. אם נרצה להוסיף עוד מעבדים גרפיים, אמזון מספקת שירות שמאפשר לשכור



רועי ליפמן

מחשבים בענן, ובכך להקטין את משך זמן פיצוח הסיסמה להשעות או דקות בודדות".

ליפמן סיכם עם עצה לגבי חיזוק הסיסמה: "יש להוסיף 'מלח' - עוד כמה תווים חסרי הגיון. בנוסף, כדאי להעביר את הסיסמה דרך כמה רצות של האש וכמובן להשתמש ביותר מפונקציית האש אחת".

"מצאנו דלתות בבתי כלא שסיסמאותיהן היו פשוטות"

שחר טל, חוקר אבטחה בצ'ק פוינט, אמר, כי "ניתן להשתמש בכלי שיסרוק את כל האינטרנט בכמה שעות, והתוצאות שהוא נותן הן מחשבים שמפעיליהם השתמשו בסיסמאות היצרן או סתם סיסמאות פשוטות לשרתים שלהם. כך, ניתן להפעיל אותם כדי לחפש עוד

טובים נגד תקיפות DDOS".
דולב פירט גם על איומים מסוגים אחרים, כמו ריגול תעשייתי וגורמים מדינתיים: "גניבת IP מארגונים פרטיים ובטחוניים, עלתה למשק האמריקאי סדר גודל של 300 מיליארד דולר. מבחינת גורמים מדינתיים לא היו חשיפות רבות, מלבד השיטות של ה-NSA והסינים".

גיא מזרחי: "Prism, המערכת האמריקאית

שאמורה לרגל אחרי

אזרחים ומה שהם עושים,

יודעת לאסוף כמעט הכל

- מיילים, צ'טים, וידאו,

תמונות שעולות לרשתות

חברתיות"

דולב מנה את הכלים הפופולאריים למתקפות סייבר ב-2013: תקיפות פשינג והנדסה חברתית; ניצול חולשות כמו סיסמאות, חולשת מערכת ההפעלה; זיוף תעודות דיגיטליות; מבוססות Watering Hole - הדבקת אוכלוסיות ממוקדות על ידי שתילת קוד עויין באתר תמים שבו

מבקרת אותה אוכלוסייה; חשיפת DNS; תקיפות מבוססות חומרה - השנה ראינו מספר תקיפות מבוססות חומרה שבוצעו על ידי קבוצות פשיעה, תקיפות אלה דרשו משאבים ותכנון בעולם הסייבר אך יושמו בעולם הפיזי. בולטת שבהם היא הפגיעה במערכת המודיעין והשליטה של מערכת המכולות והתובלה בנמל אנטוורפן בבליגיה; שיטות וכלי תקיפה חשאיים של סוכנויות ביון.

"התחזית לשנת 2014: בעקבות הפיכתו של סנואודן לסוג של אליל לפושעי הסייבר - הגורם הפנימי יעלה בחשיבותו השנה. גם ההאקטיביסטים יהיו פעילים השנה, אך מערכת ההגנה היקפית תוכל למנוע את הנזקים מהם, מסכם דולב.

"תהיו מודעים לכך שכל הזמן עוקבים אחרינו"

גיא מזרחי, מנכ"ל סייבריה ובעלים של CyberHat, נדרש לשאלת היתכנותה של Prism ישראלית: "כשמדברים על ריגול חושבים על ג'יימס בונד. ברור שקיים ריגול כנגד גופים ממלכתיים, אבל גם ארגונים מפעילים ריגול עסקי ואפילו מדינות מפעילות ריגול כנגד תעשיות של מדינות אחרות. צריך לקחת בחשבון שמרגלים אחרינו כשאנחנו בעבודה, בבית, מדברים בטלפון או יושבים מול המחשב.

"Prism, המערכת האמריקאית שאמורה לרגל אחרי אזרחים ומה שהם עושים, יודעת לאסוף כמעט הכל - מיילים, צ'טים, וידאו, תמונות שעולות לרשתות חברתיות. ניתן להגיד שהיא התגלמות של אותו אח גדול שכולם מדברים עליו".



גיא מזרחי

מזרחי הביא כדוגמה תמונה שהעלתה הדוגמנית בר רפאלי לחשבון האינסטגרם שלה, והכילה גם את נתוני ה-GPS שרשם הטלפון הסלולרי, מהם היה ניתן להבין שהיא מתגוררת במגדלי יו. הוא המשיך והסביר שכל פעילות שמתבצעת ברשתות

החברתיות נרשמת ומשאירה רמזים לגבי הם עצמם, וסיכם: "תהיו מודעים לכך שכל הזמן עוקבים אחרינו, חשבו היטב מה אתם הולכים לפרסם".