



בלמיס
- 1 -

18 מאי 2017

כ"ב באייר תשע"ז

סימוכין : ב-ס-38

אתר האינטרנט שלכם הושחת? כך תתמודדו

כבעליו של אתר אינטרנט שהפיתוח ו/או ניהול שלו מתבצעים במיקור חוץ, עליך להתייעץ עם הספקים שלך כיצד אתה יכול לשתף פעולה בכדי להימנע מהשחתה (Defacement) של האתר. בכדי להשחית אתר, התוקף משנה את תוכנם של דפים קיימים או מוסיף דפים חדשים. מאות אלפי אתרי אינטרנט מושחתים בכל יום, לעתים קרובות מבלי להיות מטרה ממוקדת כלל. השארת תוכנה זדונית מאחור לאחר ההשחתה, כזו שעשויה להדביק את המבקרים באתר הופכת שכיחה מאוד בתקופה האחרונה. לכן חשוב מאוד להבין את הסיכונים ולהתגונן כראוי. אתרי אינטרנט רבים פגיעים, אולם בקלות יכולים להימנע מהשחתה. ישנם אמצעים שונים שניתן ליישם כדי להפחית באופן משמעותי את הסיכון להשחתה. מאמר זה כולל את המאפיינים המרכזיים של השחתה, מהן השלכות ומה ניתן לעשות על מנת למקסם את ההגנה נגד התקפות כאלו.

עובדות מפתח

- השחתה היא כאשר תוקף משנה את התוכן של אתר אינטרנט.
- השחתה תתרחש לעתים קרובות, ובדרך כלל אחרי התקפה על שרת CMS או שרת האינטרנט שלך.
- תוקפים משתמשים בהשחתה כדי להפיץ תוכנות זדוניות.
- ניתן להפחית את הסיכון להשחתה על ידי ניהול כראוי ואבטחת אתרים.
- תוכנית תגובה המוכנה היטב מאפשרת להתאושש מהשחתה במהירות רבה יותר.

מה היא השחתה?

כדי להשחית אתר, התוקף משנה את תוכנם של דפים קיימים או מוסיף חדשים. ההשחתה עשויה להיות מאוד ברורה או נסתרת. השחתה תתרחש לעתים קרובות, ובדרך כלל אחרי התקפה על שרת האינטרנט או מערכת ניהול התוכן (CMS) כדוגמת ג'ומלה, וורדפרס ודרופל. למשל: על ידי ניצול לרעה של חולשה במערכת או על ידי פרטי משתמש וסיסמא. השחתה יכולה להתמקד בארגון ספציפי, אבל ברוב רובם של המקרים ההשחתה אינה ממוקדת. השחתה לא ממוקדת המתבצעת אוטומטית בעזרת כלי פריצה יכולה לשנות מספר רב של אתרים בעת ובעונה אחת. השחתתם של מאות אלפי אתרים ברחבי העולם בכל יום היא עניין שבשגרה. השחתה יכולה גם להתבצע גם בדיסקרטיות. תוקף יכול להוסיף או לשנות מאמר אחד באתר חדשות, כך שייקח זמן רב בטרם מישוהו יבחין בשינוי, עד אז סביר מאוד שהמסר יועבר. כמו כן, השחתה יכולה להפוך את האתר לנקודת הפצה לתוכנה זדונית.

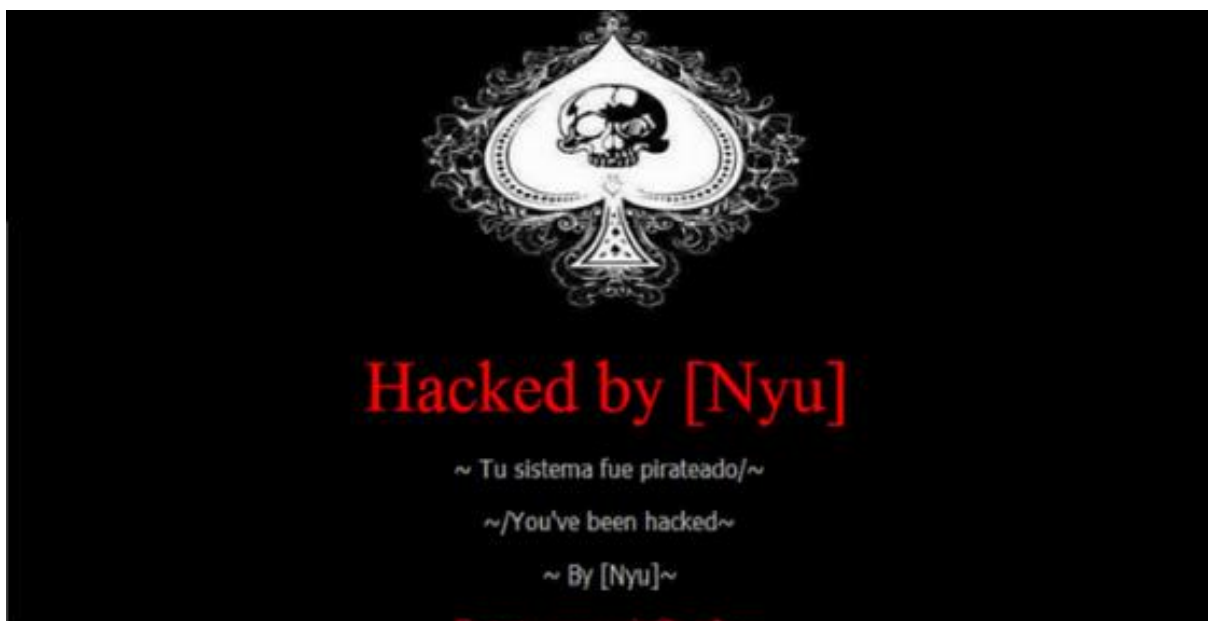


בלמיס
- 2 -

כמו כן יכולה ישנן דרכים נוספות להציג למבקר באתר מידע שגוי, למשל באמצעות חטיפת DNS. באמצעות חטיפת DNS, המשתמש המבקש לגלוש לאתר מסוים, מופנה לדף מזויף. למרות שזה לא מסווג באופן רשמי כהשחתה, יכולות להיות לכך השלכות דומות.

מי מבצע את ההשחתה ולמה?

האקרים, תוקפים לא מנוסים המכונים "סקריפט קידיס" ותוקפי סייבר יבצעו השחתה לרוב רק כי הם יכולים. הם מפעילים תוכנות לסריקה האינטרנט בחיפוש אחר אתרים פגיעים ויחליפו את דף הבית עם דף משלהם במה שמכונה "השחתה המונית". צורה זו של השחתה היא סוג של גרפיטי דיגיטלי שבו האקר משאיר מאחור את החתימה (Tag) שלו (איור 1).



איור 1. דוגמה לחתימה (Tag)

אקטיביסטים כדוגמת קבוצות אנונימוס או האקרים כמו הצבא הסורי האלקטרוני (איור 2), מבצעים השחתת אתרים במדינה מסוימת או בארגונים ממגזר מסוים כדי להפיץ את המסר האידיאולוגי שלהם או כדי לפגוע במתנגדיהם.



בלמים
- 3 -



איור 2. דוגמה להשחתת אידיאולוגית

במרדף אחר רווח כספי פושעי סייבר ישחיתו אתרים ופיצו תוכנות זדוניות על מנת לגנוב פרטים התחברות אישים או לחבר אותם לבוטנט (botnet). גם כאן, התוקפים ינסו לבצע זאת בדיסקרטיות בכדי שהאתר יישאר פרוץ זמן רב ככל האפשר מבלי להתגלות. תופעה נוספת המתרחבת כרוכה בהצבת פרסומות נגועות

בתוכנות זדוניות באתרים תמימים. לבסוף, יש מקרים שם עובדים לשעבר ממורמרים ישחיתו בזדון את האתר של המעסיק אצלו הועסקו. הם מסוגלים לעשות את זה כי יש להם עדיין את שמות המשתמשים והסיסמאות שהם צריכים כדי לשנות את אתר האינטרנט בקלות.

כמה משמעותית יכולה להיות השחתה?

השלכותיה של השחתה עשויות להיות שונות בין ארגונים שונים. כל ארגון צריך להעריך את ההשפעה הפוטנציאלית של השחתה ולנקוט באמצעים מתאימים. בדרך כלל השפעתו הראשונית של אתר שהושחת תהיה על תדמיתה של החברה ועל העלויות הכרוכות באחזור האתר. חברות התלויות באתר האינטרנט למסחר עלולות לסבול הפסדים כספיים בשל מכירות מופחתות.

השחתת אתר בדרך כלל לא תשפיע על הארגון המתבסס על מערכות מחשב, אך יכול לשמש כהסחה לצורות אחרות של פשעי אינטרנט. פושעי סייבר עשויים להשתמש בהשחתה כדרך להשגת פרטי ההתחברות של עובדים למערכת הדואר האינטרנטי של הארגון, תוך שימוש בשם הדומיין של הארגון למטרה זו.



בלמיס
- 4 -

אם השחתה משמשת להפצת תוכנות זדוניות או כדי לגרום למבקרים באתר להזין את פרטי ההתחברות האישיים שלהם לאתר או לשירותים כמו פייסבוק, גוגל וכו', הנזק גודל ועולה מעבר לפגיעה בחברה הניזוקה. במקרים כאלה מידע אישי של המבקרים או מידע של חברה עשוי להיות מנוצל לרעה.

מה הופך אתר לפגיע?

אתר הוא פגיע להשחתה אם:

- השרת (הווירטואלי) באינטרנט או ממשק השרת הווירטואלי הפרטי (VPS) אינם מוקשחים.
- משתמשים לא מורשים שיכולים לקבל גישה לשרת האינטרנט או ממשק ה-VPS יכולים להוסיף תוכן לשנותו או למחוק אותו.
- אי עדכון של מערכת ניהול התוכן (CMS). אלו מכילות נקודות תורפה רבות, ויש לעדכן את עדכוני אבטחה שספקי ה-CMS מפרסמים באופן קבוע למוצריהם.
- כאשר פרטי ההתחברות למערכת ה-CMS או שרת האינטרנט נפלו לידי התוקפים. למשל, על ידי עשיית שימוש בחשבונות סטנדרטיים וסיסמאות ברירת מחדל או סיסמאות פשוטות, באמצעות דיג ממוקד או כאשר האתר לא מוגדר לעשות שימוש בפרוטוקול מאובטח TLS להעברת המידע.
- כאשר תצורת האתר מכילה נקודות תורפה ל-XSS, שניתן לנצלן להצגת תוכן 'שיקר'.
- תוכנות זדוניות פעילות באתר באמצעות ספקי תוכן פרסומי לא אמינים.
- אתרים מסוימים כדוגמת אתרים דתיים, של ארגונים פוליטיים או של חברות תקשורת, נמצאים בסיכון מיוחד להתקפות ממוקדות. אולם השחתת אתר של ארגונים אלו אינו מצביע בהכרח על תקיפה ממוקדת, וייתכן סיכוי רב כי האתר נפל קורבן להשחתה כחלק מהשחתה המונית.

השחתה של מדיה חברתית

חשוב מאוד לארגונים המשתמשים במדיה חברתית כמו טוויטר ופייסבוק לשקול את ההשלכות של פגיעה בשירותים אלו. הודעות כוזבות בטוויטר או פרופיל פייסבוק שהוסב עשויים לפגוע בדימוי הארגון באותה מידת חומרה כמו השחתת אתר.

כמשתמש אינך יכול לעשות רבות כדי לשפר את אבטחתם של אתרי מדיה חברתיים גדולים, אולם אתה יכול להגן על עצמך בצורה יעילה ככל שניתן כנגד ניצול לרעה של חשבונות המשתמש שלך.

- השתמש באימות כפול (2-factor authentication) בכל מקום המאפשר זאת
- השתמש בסיסמאות ארוכות ומורכבות
- שנה באופן קבוע את סיסמאות שלך
- גבש תכנית תגובה והתאוששות



בלמיס
- 5 -

כיצד מבחינים בהשחתה?

רוב ההשחתות כל כך ברורות שאין ספק שהאתר הושחת ומיהו הגורם שלוקח אחריות על כך. ישנם אמצעים טכניים שונים שניתן לנקוט כדי לפקח על אתר האינטרנט לשינויים לא מורשים, כמו גם חברות שיעשו זאת תמורת תשלום.

אם לא הבחנת בהשחתה מיד, ייתכן שתזעק על ידי:

- משתמשים שמבקרים באתר ושמו לב להשחתה.
- מאגרי מידע מקוון שעוקבים אחר השחתות, ובמקרים מסוימים, שולחים הודעה למנהל האתר.
- ניטור תגובות של הציבור על אתר האינטרנט במדיות החברתיות כמו טוויטר או פייסבוק.
- ספק שירותי האינטרנט, אשר לעתים קרובות הינו הראשון להתריע כאשר האתר הושחת.

כיצד מונעים השחתה?

למרות שאף פעם לא ניתן לשלול לחלוטין את הסיכוי להשחתת האתר, ישנם אמצעי מניעה שונים שניתן לנקוט כבעליו של האתר (או באמצעות הספק) כדי להפחית את הסיכון לפגיעה באופן משמעותי.

- לוודא כי השרת מוקשח ואין בו שירותים (Services) מיותרים.
- להקפיד להתקין את התיקונים האחרונים ועדכוני אבטחה המופצים למערכת.
- לבדוק באופן קבוע שהמערכת מעודכנת לגרסה האחרונה.
- לבדוק קיומם של תוכנות זדוניות.
- לא להשתמש בחשבונות וסיסמאות סטנדרטיים למערכות ההפעלה או ה-CMS.
- למחוק מיד את חשבונות המשתמש של עובדים שעזבו את הארגון או שאינם זקוקים לגישה למערכת ניהול התוכן או שרת האינטרנט.
- להתקין חומת אש ולסנן את תעבורת הרשת לדפוסים חשודים.
- להגביל את מספר כתובות ה-IP שיכולות לקבל גישה לשרת ומערכת ניהול התוכן.
- חיבור ל CMS יעשה רק באמצעות חיבור TLS מאובטח.
- היכן שאפשרי, אבטח את הגישה לשרת האינטרנט ומערכת ניהול התוכן עם מערכת אימות כפול (2-factor authentication).
- לסרוק באופן קבוע את רמת האבטחה של האתר, באמצעות סורקים אוטומטיים. לתאם זאת מראש עם מנהל האתר או בעלים, כך שזה לא יראה כניסיון תקיפה.
- הצגת מדיניות גילוי נאות, כך שנקודות תורפה שימצאו באתר האינטרנט ידווחו בסודיות, זה יאפשר גילויים ותיקונם של חולשות טרם שינוצלו על ידי גורמים זדוניים.
- במידה והאתר מתארח אצל ספק חיצוני, חשוב להגדיר עמו מדיניות ברורה בדבר אבטחת האתר.



בלמי"ס
- 6 -

בנוסף, ובוודאי אם האתר או תדמיתו של הארגון חשובה במיוחד או שקיים סיכון גבוה מהממוצע להשחתה, ניתן לשקול ביצוע בדיקות חדירות תקופתיות לאיכות האבטחה של אתר האינטרנט ולתקן כל חולשה שזוהתה כדוגמת פגיעות XSS. בנוסף יש ליישם מערכת זיהויי חדירה (IDS) כדי לאתר פעילות חשודה מוקדם ככל האפשר.

כיצד מתכוננים ליום בו האתר הושחת?

- מכיוון שאין ערובה של 100% לביטחון, צריך להיות מוכנים תמיד להגביל את הנזק שנגרם במקרה של השחתה.
- יש לבצע באופן קבוע גיבוי של האתר. מה שיאפשר שיחזור קל יותר של האתר במקרה של פגיעה.
- יש לוודא כי יש דף אינטרנט נאה חלופי שישימש להחליף באופן מידי את האתר שהושחת.
- מומלץ לגבש תכנית תגובה למקרה שבו האתר הושחת. חשוב לשקול גם את התקשורת הפנימית וחיצונית בזמן התקרית.
- אם האתר מתארח אצל ספק חיצוני, מומלץ לסכם מראש בחוזה על מה הספק רשאי / צריך לעשות ביוזמתו ומה ראשית יש לדון עליו עם בעל האתר.

האמצעים החשובים ביותר נגד השחתה

מניעה:

1. ודאו כי שרת האינטרנט ומערכת ניהול התוכן מוגדרים באופן מאובטח ומעודכנים בכל עדכוני האבטחה האחרונים.
2. במידת האפשר השתמשו באימות כפול לגישה (2-factor authentication) לשרת האינטרנט ומערכת ניהול התוכן.

אופן ההכנה:

3. בצעו באופן קבוע גיבוי של האתר
4. גבשו תכנית תגובה מה לעשות במקרה של השחתה

תיקון:

5. הכינו דף אינטרנט חליפי שישימש להחלפת האתר המושחת בעת הצורך
6. דונו על ההשלכות האפשריות לאירוע.
7. אבטחו את תוכן האתר המושחת למטרות חקירה פליליות ולדיווח האירוע למשטרה.
8. תקנו והגדירו מחדש את אתר האינטרנט ובדקו את הגדרות האבטחה טרם החזרתו לפעילות מקוונת.
9. בדקו כיצד ניתן לשפר את התצורה או את ניהול האתר בתגובה לתקרית ויישמו את השיפורים.



בלמי"ס
- 7 -

כיצד לתקן השחתה?

תכנית התגובה שגובשה היא זו שתצא לפועל כאשר מתרחשת השחתה.

להבטחת תיקון מהיר, יש לכלול:

- הצבת דף אינטרנט חליפי.
- הערכת הנזק שנגרם על ידי ההשחתה. האם רק צורתו של האתר היא שהשתנתה, או שהתוקף גם השאיר תוכנות זדוניות או תוכן לא חוקי מאחוריו?
- יידעו את הגורמים רלוונטיים על האירוע.
- אבטחו את התוכן והלוגים של האתר המושחת למטרות חקירה פליליות.
- נסו לברר כיצד ההשחתה בוצעה, מהן החולשות שנוצלו?
- בדקו את הגיבוי האחרון של האתר לנוכחות של תוכנות זדוניות וחולשות.
- הגדירו שרת חדש עם הגרסאות העדכניות ביותר של התוכנות הדרושות ושחזרו את הגיבוי האחרון המאובטח של תוכן האתר.
- פרסמו את האתר רק לאחר שברור שכל החולשות נפתרו.

לאחר שהאתר תוקן נותר עוד רבות לעשות כדי לוודא שלא תהיה הישנות:

- לקבוע אם האתר עדיין כפוף לכשלים טכניים או נקודות תורפה. במידה וכן, לתקן אותם או להקים מחדש את האתר עם מוצרים פחות פגיעים.
- לבדוק אם ניתן לבצע שיפורים נוספים בצורת הניהול של האתר. בהקשר זה ניתן לשקול את תיזמון התקנתם של תיקונים ועדכונים, ניטור האתר ותגובת הארגון בזמן אירוע.
- אם אתם מנהלים את האתר בעצמכם או לא מרוצים מהשירותים הניתנים על ידי הספק הנוכחי שלכם, יש לשקול שינוי אירוח האתר לספק אחר.
- בדקו את תכנית התגובה. מה פועל טוב, ומה לא ודורש שיפור. האם יש לבדוק את תכנית התגובה (לעתים קרובות יותר) בעתיד? האם יש לנקוט בצעדים נוספים? או דרושים אמצעים נוספים?
- לאחר שזוהו שיפורים מבניים המבוססים על הכתוב לעיל, יש לנקוט גישה אקטיבית וליישם אותם.

לסיכום

השחתת אתרים נמצאת בשימוש יותר ויותר ככלי תעמולה לקבוצות אידיאולוגיות שונות. כמו כן, יותר ויותר כלים מופצים כדי לסרוק אתרים באופן אוטומטי וגם לשנות אותם באופן אוטומטי במידה ונמצאות חולשות.

על ידי נקיטת אמצעי אבטחה ספציפיים ניתן להפחית באופן משמעותי את הסיכון להשחתה.