

מחקר של ניוסטאר: שיקוף DNSSEC סיכון DNS חמור

הספקית של DNS ושירות מיתון DDoS חושפת פגיעויות רווחות של הגברת DNSSEC

הגברת ה-DNSSEC הממוצעת גדולה בקרוב לפי 30 מהבקשות

סטרלינג, וירג'יניה, 17 באוגוסט 2016, ([BUSINESS WIRE](#)):

Neustar, Inc. (NYSE: NSR) ניוסטאר, ספקית אמינה ניטרלית של שירותי מידע בזמן אמת, פרסמה היום את "DNSSEC: איך תוקפי DDoS מתוחכמים משתמשים בהגנות שלנו נגדנו" (DNSSEC: How Savvy DDoS Attackers Are Using Our Defenses Against Us), דוח מחקר שמפרט איך אפשר לנצל לרעה DNSSEC (תוספים להגברת האבטחה של DNS) כמגבר בהתקפות DDoS (מניעת שירות מבוזרת). ניוסטאר קבעה שבממוצע שיקוף DNSSEC יכול להפוך שאילתה של 80 בייט לתגובה של 2,313 בייט, גורם הגברה של קרוב לפי 30, שיכול בקלות לגרום להפסקת שירות ברשת בזמן התקפת DNS, והתוצאה היא הפסד הכנסות ופריצות לנתונים.

"DNSSEC התפתח ככלי למלחמה בחטיפות של DNS, אבל לרוע המזל הפצחנים הבינו שהמורכבות של החתימות האלה הופכת אותן אידיאליות להצפת רשתות בהתקפת DNS", אמר ג'ו בלס, מנהל שיווק מוצרים, שירותי אבטחה, ניוסטאר. "אם DNSSEC לא מאובטח היטב, אפשר לנצל אותו, להפוך אותו לנשק ובסופו של דבר להשתמש בו ליצירת התקפות DNS מסיביות".

DNSSEC תוכנן כדי לספק תקינות ואימות ל-DNS, והוא משיג אותן באמצעות החלפות של מפתחות וחתימות דיגיטליות מורכבות. כתוצאה מכך, כשרשומת DNS מועברת ל-DNSSEC, נוצרת כמות בלתי רגילה של מידע נוסף. בנוסף, כשנותנים את פקודת ה-ANY DNS, התשובה המוגברת מ-DNSSEC גדולה באופן מעריכי מאשר תשובת DNS רגילה.

ממצאים חשובים מהדוח "DNSSEC: איך תוקפי DDoS מתוחכמים משתמשים בהגנות שלנו נגדנו":

1. **הפגיעויות של DNSSEC רבות מאוד** – ניוסטאר בדקה ענף אחד עם 1,349 שמות מתחם וקבעה שב-1,084 מהם (80 אחוז) אפשר לעשות שימוש זדוני כמגבר בהתקפת DNS (הם נחתמו באמצעות DNSSEC והגיבו לפקודה ANY).
2. **גורם הגברת ה-DNSSEC הממוצע הוא 28.9** – ניוסטאר בדקה פגיעויות של DNSSEC באמצעות שאילתה של 80 בייט, שהחזירה תגובה ממוצעת של 2,313 בייט. תגובת ההגברה הכי גדולה הייתה 17,377 בייט, גדולה פי 217 מהשאילתה של 80 בייט.
3. **האנטומיה של התקפת שיקוף DNSSEC** – ניוסטאר מדגימה את שרתי הפקודות והבקרה שנחוצים כדי להפעיל את רובוטי הרשת והסקריפטים שמתכוונים אל שרתי שמות DNS כדי לבצע התקפות הגברת DNSSEC.
4. **פרקטיקות מיטביות לצמצום** – לארגונים שמסתמכים על DNSSEC, ניוסטאר ממליצה להבטיח שספק ה-DNS שלהם לא מגיב לשאילתות ANY או שמותקן אצלו מנגנון שמזהה ומונע שימוש לרעה.

"ניוסטאר מתמקדת בשימוש במדעים קשורים כדי לחבר בין אנשים, מקומות ודברים, ולכן אבטחת הרשת כל כך הכרחית", אמר בלס. "ככל שיותר ארגונים מאמצים את DNSSEC, יש חשיבות קריטית להבין איך לאבטח אותו. הזמן לתקן אותו הוא עכשיו".

למידע נוסף על הדוח "DNSSEC: איך תוקפי DDoS מתוחכמים משתמשים בהגנות שלנו נגדנו", בקרו בבקשה כאן:

<https://hello.neustar.biz/201608---Security-Services---Trade-Show---Black-Hat-DNSSEC-LP.html>.

אודות ניוסטאר

כל יום העולם מייצר בערך 2.5 קוודריליון ביטים של נתונים. ניוסטאר (NYSE: NSR) מבודדת אלמנטים מסוימים ומנתחת, מפשטת ועורכת אותם כדי לקבל החלטות מדויקות ורבות ערך שמביאות לתוצאות. כאחת מהחברות הבודדות שיכולות לדעת בוודאות מי נמצא בצד השני של כל אינטראקציה, המותגים הגדולים של העולם סומכים עלינו שנקבל החלטות קריטיות בערך 20 מיליארד פעמים ביום. אנחנו עוזרים לאנשי שיווק לשלוח מסרים רלבנטיים ובזמן לאנשים הנכונים. משום שאנחנו יכולים לומר ללקוח בסמכותיות בדיוק מי מתקשר או מתחבר אליו, אנחנו מאפשרים תגובות קריטיות בזמן אמת. ואותו מידע מקיף שמאפשר ללקוחותינו להפנות ולנהל הוראות גם עוצר התקפות. אנחנו יודעים כשמישהו אינו מי שהוא טוען שהוא, וזה עוזר לעצור הונאות ומניעת שירות לפני שהם הופכים לבעיה. בגלל שאנחנו גם מנהלים מנוסים של כמה ממסדי הנתונים המורכבים ביותר בעולם, אנחנו עוזרים ללקוחות לשלוט על הזהות האינטרנטית שלהם, לרשום את שמות המתחם שלהם ולהגן עליהם ולנתב תעבורה לכתובת הרשת המתאימה. על ידי חיבור בין המידע הכי חיוני ובין האנשים שתלויים בו, אנחנו מספקים ליותר מ-12,000 לקוחות בכל העולם החלטות – לא רק נתונים. מידע נוסף נמצא בכתובת <http://www.neustar.biz>

אנשי קשר

ניוסטאר

Laura Cahill

laura.cahill@axicom.com

(+44) 2083924071

מקור: ניוסטאר



צפו בהודעה לעיתונות הזאת במקור בשפה האנגלית באינטרנט בכתובת:

<http://www.businesswire.com/news/home/20160816005745/en>

*** הידיעה מופצת בעולם על ידי חברת התקשורת הבינלאומית **Business Wire**

לפרטים נוספים: נוי תקשורת 03-6026026 זהר 052-2641769