



NOxCrypt v2.3.0 – מפרט פומבי

מחבר: NOX

1. שם

NOxCrypt v2.3.0 – אלגוריתם הצפנה קנייני שפותח במיוחד עבור מערכת NOX. מטרתו היא לספק הצפנה שאי אפשר לזהות כהצפנה, כולל הסוואה לפורמטי מדיה שונים ולזרמים בינאריים אקראיים. האלגוריתם מבוסס גם על עקרונות (NOX development) Deep InCrypting.

2. מטרת ותכונות

- הסתרה לא רק של תוכן הנתונים, אלא גם של עצם קיומם.
- פלט הנתונים יכול לדמות תמונות, אודיו, וידאו או נתונים בינאריים שרירותיים.
- הסוואה לפורמטים פופולריים (לדוגמה, JPEG, MP3, PNG).
- שימוש בלעדי בתוך האקו-סיסטם של NOX.
- מפתח דינמי, עם יצירה ייחודית לכל סשן.
- שילוב של (NOX development) Deep InCrypting כמנגנון ייחודי.

3. ארכיטקטורה

הארכיטקטורה משתמשת בשלבי טרנספורמציה מדורגים, כולל החלפות, ערבוב והוספת רעש מבוקר. הסכמות המתמטיות והטבלאות הפנימיות הן מידע חסוי ואינן נחשפות בגרסה הציבורית של המפרט.

4. מפתח וסשנים

מפתח ההצפנה ארוך במיוחד ונוצר באופן דינמי באמצעות פרמטרים אקראיים ופרמטרי סשן. לכל סשן נוצרים טבלאות ייחודיות וכללי טרנספורמציה, המונעים שימוש חוזר במפתחות או תבניות הצפנה.

5. הסוואה

האלגוריתם מסוגל להפוך זרם מוצפן למראה התואם לסוגים שונים של קבצי מדיה או תעבורת רשת, מה שמקשה מאוד על זיהוי עצם העברת המידע המוצפן.

6. אבטחה

כל סשן משתמש במפתחות ייחודיים ובמערכת כללים ייחודית. גם במקרה של ירוט התעבורה, ללא גישה למפתח, פענוח אינו אפשרי. האלגוריתם כולל מנגנונים מובנים למניעת קריפטואנליזה והסוואת מבנה הנתונים.

7. יישום

NOXCrypt יכול להצפין טקסט, נתוני קול וזרמים בינאריים כלליים, ולהפוך אותם לצורה שאינה מעוררת חשד. האלגוריתם מותאם למהירות גבוהה ולעיכוב נמוך בהעברת נתונים.

8. מסקנה

NOXCrypt היא מערכת הצפנה מהדור החדש, הממוקדת בהבטחת פרטיות ואנונימיות מרבית, וכן בעמידות בפני זיהוי וניתוח. מפרט זה מציג סקירה של הטכנולוגיה ואינו חושף את פרטי האלגוריתם הפנימיים.