

## חברת קלירסקיי חשפה חולשה לא ידועה (0day) במערכות Windows המנוצלת בשטח על ידי קבוצת תקיפה רוסית CVE-2024-43451

### תקציר

במהלך חודש אוגוסט 2024 חשף צוות ClearSky חולשה לא ידועה - Zero-Day בקבצי URL במערכות ההפעלה של Windows. הפגיעות מאפשרת לקבצי URL בהם מוטמעות שורות קוד ספציפיות להפעיל סקריפט המתקשר עם שרת התוקף גם כשהמשתמש לא מפעיל את הסקריפט ישירות ומבצע פעולות שלא אמורות להפעיל את הסקריפט ובהן:

1. **לחיצה אחת בעכבר על שם הקובץ** – לחיצה אחת לא אמורה להפעיל את הקובץ שעליו לוחצים. החולשה תקפה לכל הגרסאות של Windows.
2. **לחיצה ימנית אחת בעכבר** – לחיצה אחת ימנית על העכבר לא אמורה להפעיל את הקובץ שעליו לוחצים. החולשה תקפה לכל הגרסאות של Windows.
3. **גרירת הקובץ לתיקייה אחרת** – גרירה של קובץ למחיצה לא אמורה להפעיל את הקובץ הנגרר. החולשה תקפה ל Windows 10/11 ובתצורות מסוימות של Windows 7/8/8.1.
4. **מחיקת הקובץ** – מחיקת הקובץ למחיצה לא אמורה להפעיל את הקובץ הנמחק. החולשה תקפה ל Windows 10/11 ובתצורות מסוימות של Windows 7/8/8.1.

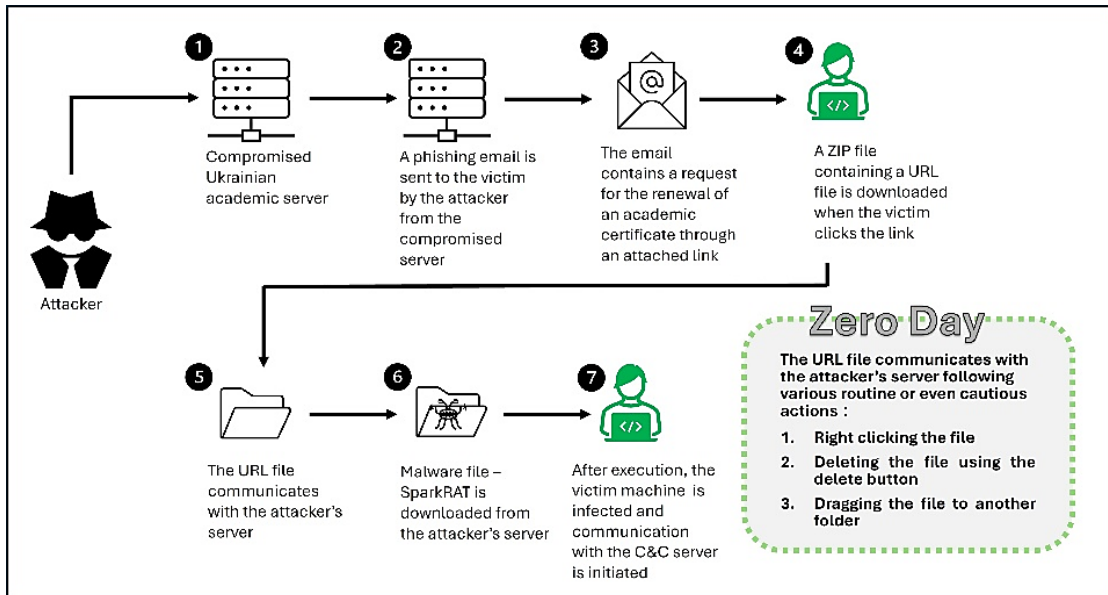
הקבצים הזדוניים והחולשה הנלווית אותרו על ידינו בקבצים שהורדו מאתר רשמי של ממשלת אוקראינה. האתר מאפשר להוריד תעודות ובהם הסמכות אקדמאיות רשמיות. התוקף שלח לקורבנות מייל מתוך מערכת המייל הממשלתי, ובו הודיע להם כי תוקף התעודה האקדמית שברשותם פג, ולפיכך עליהם לבצע תהליך של חידוש התעודה באמצעות קישור שצורף למייל. לחיצה על הקישור הפעילה שרשרת של פעולות שמטרתן הדבקת המחשב בנוזקה. המחקר שותף עם מערך הסייבר האוקראיני - CERT-UA. מערך הסייבר האוקראיני חשף כי קובץ ה-URL מופץ כחלק מקמפיין של קבוצת תקיפה רוסית המכונה UAC-0194. קבוצה הפועלת מול ארגונים ואזרחים באוקראינה.

הפגיעות דווחה לפני מספר חודשים במקביל לחברת Microsoft והיא תיקנה אותה במסגרת "Patch Tuesday" שהתפרסם הלילה - 12.11.2024 (CVE-2024-43451).

<https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-43451>

בכדי להתגונן מפני החולשה, מומלץ לעדכן את המחשב ולחסום קליטה של קבצים מצורפים למייל עם קבצי URL או קבצי ZIP המכילים קבצי URL.

להלן שרטוט מתווה הקמפיין:



פרטים מלאים על הקמפיין ניתן בבלוג החברה [www.clearskysec.com/blog](http://www.clearskysec.com/blog)

המחקר בוצע יחד עם מערך הסייבר האוקראיני וחברת Microsoft, תודה על העבודה המשותפת

[www.clearskysec.com](http://www.clearskysec.com)

[info@clearskysec.com](mailto:info@clearskysec.com)