

09 נובמבר 2020  
כ"ב חשון תשפ"א  
סימוכין: ב-ס-1192

## פוגענים בשימוש קבוצות תקיפה

### תקציר



לאחרונה פרסמו גורמי אבטחת מידע ואכיפת חוק אמריקאים פרטים לגבי פוגענים עדכניים המצויים בשימוש קבוצות תקיפה. הפוגען **ComRAT** מצוי בשימוש קבוצת התקיפה **Turla**. הפוגען **Zebrocy** מצוי בשימוש קבוצת התקיפה **APT28**. להתרעה זו מצורף קובץ מזהים. מומלץ לנטרם במערכות הארגוניות.

### פרטים



1. להלן פירוט הקבצים הכלולים בהתרעות:

פוגען	שם קובץ	מטרה
ComRAT	corrected.ps1	<b>Dropper</b> . קוד מעורפל מאד שמטרתו להתקין קוד <b>PowerShell</b> ב- <b>registry key</b> , ולשנות משימות מתוזמנות כדי להריץ קוד זה.
	Decode_PowerShell.ps1	<b>Loader</b> . קוד ה- <b>PowerShell</b> המותקן על-ידי הקוד הקודם ב- <b>registry key</b>

מטרתו לפענח ולטעון DLL זדוני.		
קובץ 32bit Windows DLL של ComRAT שזוהה כמודול של ComRAT.v4. קובץ זה נטען לתוכנת Explorer.exe באמצעות קוד ה-PowerShell.	ComRATv4.exe	
קובץ 32bit Windows DLL. קובץ זה מוזרק לדפדפן ברירת המחדל במערכת הקורבן באמצעות הקודם, ומשמש כמודול תקשורת. הוא עושה שימוש בפרוטוקול HTTP ובתשתית של אתר Gmail לטובת C2, תוך שימוש בקישורים מאובטחים.	Communication_module_32.dll	
קובץ 64bit Windows DLL. מבצע פעילות דומה לזו של הקובץ בסעיף הקודם.	Communication_module_64.dll	
Backdoors כתובים בשפת Go. מאפשרים יצירה, שינוי ומחיקת קבצים, צילום מסך, מיפוי כוננים, הרצת פקודות באמצעות cmd.exe, יצירת משימות מתוזמנות לצורך שימור אחיזה	smqft_exe sespmw_exe	Zebrocy



דרכי התמודדות



1. להתרעה זו מצורף קובץ מזהים. מומלץ לנטרם במערכות הארגוניות.

לכל מידע נוסף ניתן לפנות אלינו. במידה שעלו ממצאים בבדיקתכם, נבקש לקבל היזון חוזר.

מקורות



1. <https://us-cert.cisa.gov/ncas/analysis-reports/ar20-303a>
2. <https://us-cert.cisa.gov/ncas/analysis-reports/ar20-303b>
3. <https://www.zdnet.com/article/us-cyber-command-exposes-new-russian-malware/>
4. [https://www.virustotal.com/en/user/CYBERCOM\\_Malware\\_Alert/](https://www.virustotal.com/en/user/CYBERCOM_Malware_Alert/)

שיתוף מידע עם ה-CERT הלאומי אינו מחליף חובת דיווח לגוף מנחה כלשהו, ככל שחלה על הגוף חובה כזו. המידע נמסר כפי שהוא (as is), השימוש בו הוא באחריות המשתמש ומומלץ להיעזר באיש מקצוע בעל הכשרה מתאימה לצורך הטמעתו.



בברכה,  
CERT-IL