



05 אוגוסט 2020  
ט"ו אב תש"פ  
סימוכין:ב-ס-1134

## ארה"ב פרסמה מידע לגבי פוגען בשימוש גורמי תקיפה סיניים

### תקציר



לאחרונה פרסמו CISA, ה-FBI ו-DoD, התרעה לגבי שימוש של גורמי תקיפה סיניים בפוגען בשם Taidoor. להתרעה זו מצורף קובץ מזהים. מומלץ לנטרם במערכות הארגוניות הרלוונטיות.

### פרטים



- על פי דיווחים שונים, גרסאות של הפוגען היו בשימוש החל משנת 2008.
- הפוגען הינו כלי לגישה מרחוק (RAT - Remote Access Trojan).
- לפוגען גרסאות למערכות הפעלה 32 או 64 ביט.
- הפוגען כולל 2 קבצים. הקובץ הראשון מופעל כ-Service, טוען את הקובץ השני לזיכרון, מפענח את ההצפנה ומריץ אותו.
- ההתקנה כ-Service אינה חלק מהפוגען ובוצעה ככל הנראה באמצעים אחרים.
- התקשורת עם שרתי ה-C2 מבוצעת בפורט 443 אך בחלקה אינה בפרוטוקול TLS אלא גלויה.

### דרכי התמודדות



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



2. בנספח א' מצורף חוק YARA העשוי לסייע בזיהוי קבצים חשודים.

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

## מקורות



1. <https://us-cert.cisa.gov/ncas/analysis-reports/ar20-216a>

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.





נספח א'

```
rule CISA_10292089_01 : rat loader TAIDOOOR
{
  meta:
    Author = "CISA Code & Media Analysis"
    Incident = "10292089"
    Date = "2020-06-18"
    Last_Modified = "20200616_1530"
    Actor = "n/a"
    Category = "Trojan Loader Rat"
    Family = "TAIDOOOR"
    Description = "Detects Taidoor Rat Loader samples"
    MD5_1 = "8cf683b7d181591b91e145985f32664c"
    SHA256_1 = "363ea096a3f6d06d56dc97ff1618607d462f366139df70c88310bbf77b9f9f90"
    MD5_2 = "6627918d989bd7d15ef0724362b67edd"
    SHA256_2 = "0d0ccfe7cd476e2e2498b854cef2e6f959df817e52924b3a8bcdade7a8faaa686"
  strings:
    $s0 = { 8A 46 01 88 86 00 01 00 00 8A 46 03 88 86 01 01 00 00 8A 46 05 88 86 02 01 00 00 8A 46 07 88 86 03 01 00 00 }
    $s1 = { 88 04 30 40 3D 00 01 00 00 7C F5 }
    $s2 = { 0F BE 04 31 0F BE 4C 31 01 2B C3 2B CB C1 E0 04 0B C1 }
    $s3 = { 8A 43 01 48 8B 6C 24 60 88 83 00 01 00 00 8A 43 03 }
    $s4 = { 88 83 01 01 00 00 8A 43 05 88 83 02 01 00 00 8A 43 07 88 83 03 01 00 00 }
    $s5 = { 41 0F BE 14 7C 83 C2 80 41 0F BE 44 7C 01 83 C0 80 C1 E2 04 0B D0 }
    $s6 = { 5A 05 B2 CB E7 45 9D C2 1D 60 F0 4C 04 01 43 85 3B F9 8B 7E }
  condition:
    ($s0 and $s1 and $s2) or ($s3 and $s4 and $s5) or ($s6)
}
```