כלי ניטור וניהול מרחוק (RMM) בשימוש תקיפה פעילה בישראל

29/04/2026
י"ב אייר תשפ"ו

[תקציר]

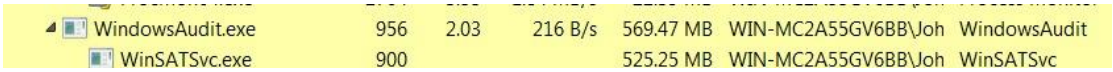
1. לאחרונה דווח למערך הסייבר הלאומי על תקיפה פעילה בישראל באמצעות כלי ניטור וניהול מרחוק (RMM) שאינו מוכר.
2. מטרת התרעה זו, הפצת מזהי הכלי והתקיפה לציבור, לצורך זיהויה ומניעת התפשטותה.

[פעולות מידיות לביצוע]

- להתרעה זו מצורף קובץ מזהים. מומלץ מאד **לחסום** מזהים אלו בכל אמצעי האבטחה הארגוניים הרלוונטיים.
- מומלץ להשתמש בפקודות ה-PowerShell המפורטות להלן, או בכלי Autoruns, לבדיקת עמדות החשודות כנגועות בפוגען.

[פרטים]

1. יכולות כלי התקיפה:
   1. הרצת פקודות מרחוק.
   2. איסוף וגניבת מידע רגיש.
   3. שימור אחיזה קבועה במערכת (Persistence) באמצעות מנגנונים כגון WMI, Registry (Run, Service).
   4. הורדת נוזקות ו-Payloads נוספים משרת התוקף ברשת האינטרנט.
2. ההדבקה הראשונית מבוצעת באמצעות 2 קבצים:



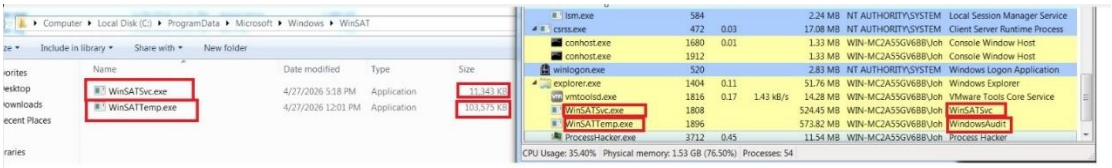
3. הנוזקה משתמשת בפלטפורמות Discord ו-HiveMQ כערוצי תקשורת דו-כיווניים (C2). קיים גם ערוץ טלגרם אופציונלי, ככל הנראה כגיבוי ל-2 האפשרויות הראשונות.
4. התקשורת עם HiveMQ מתבצעת בפרוטוקול MQTT ומוצפנת באמצעות TLS. פורט 8883.

ריכוז נתוני התחברות (MQTT)

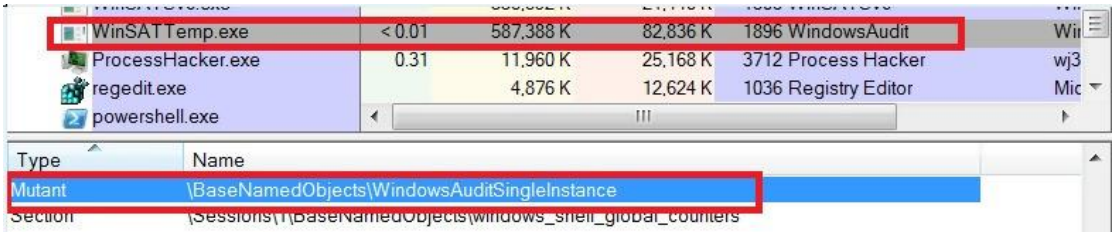
פרמטר	ערך
Broker Host	`6fce11e04d8947dcbb6141b0e01661b8.s1.eu.hivemq.cloud`
Port	`8883`
Username	[צונזר]
Password	[צונזר]
TLS Enabled	`True`
Command Topic	`/commands`
Result Topic	`/results`

5. התקשורת עם Discord מתבצעת באמצעות HTTPS.
   1. להלן פרטי הערוצים השונים ב-Discord:
      - מזהה שרת (Guild ID): 1212298596993605642
      - ערוץ ניהול (BusChannelId): 1399994586763628584
      - ערוץ אחסון (StoreChannelId): 1498233412245262436
      - קצב דגימה (PollIntervalMs): 5000 (כל 5 שניות)
      - פורמט נתונים מודלף: Compressed Chunks עם סיומת bin.gz.
      - ספריית פיתוח: Discord.Net v3.18.0
6. הנוזקה מתקינה קבצים של הפוגען בנתיבים:

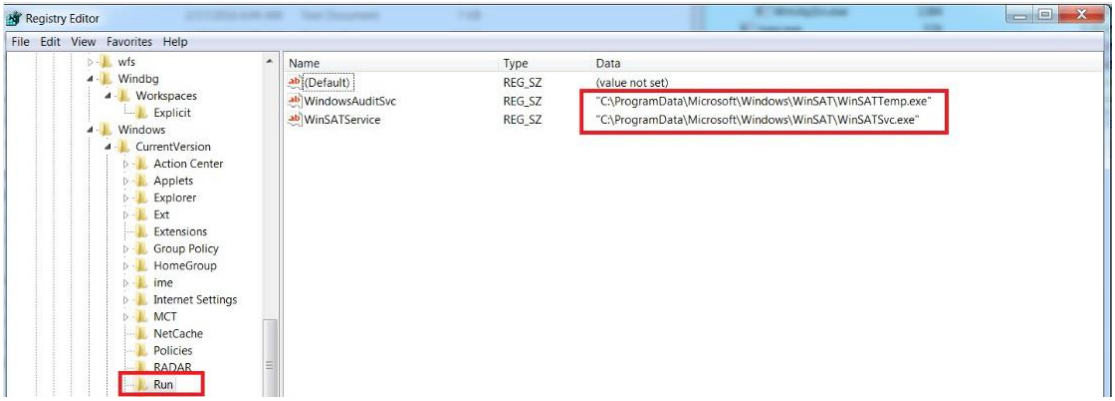
- C:\ProgramData\Microsoft\Windows\WinSAT\WinSATTemp.exe (העתק של הפוגען)
- C:\ProgramData\Microsoft\Windows\WinSAT\WinSATSvc.exe (Watchdog)



7. קבצי הפוגען גדולים יחסית (101MB ו-11MB). מנועי AV מסוימים עלולים שלא לבודקם כלל, מאחר ולעיתים כלי AV מוגדרים לדלג על קבצים בגדלים אלו.
8. הפוגען מנסה להחריג את ספריית ההתקנה שלו (C:\ProgramData\Microsoft\Windows\WinSAT) מסריקה על ידי Windows Defender (Exclusion).
9. הפוגען מגדיר Mutex בשם Global\WindowsAuditSingleInstance למניעת הדבקה חוזרת.

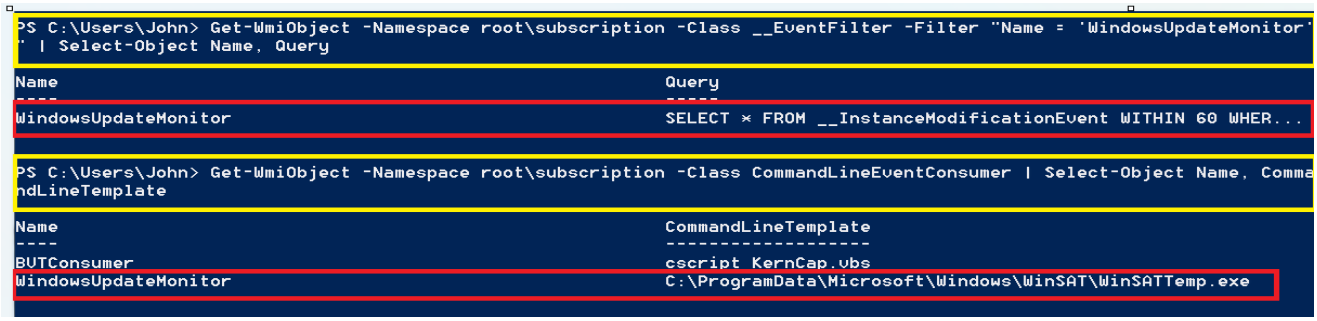


10. הפוגען מגדיר מספר Registry Keys לצורך שימור האחיזה בעמדה.



11. הפוגען מגדיר משימה מתוזמנת בשם RemoteAdminEdrCleanup.
12. זוהתה הרצה של פקודת bcdedit המגדירה את המחשב לעלות במצב בטוח (Safe Mode Minimal). פעולה זו אופיינית לתוקפים המנסים לנטרל כלי אבטחה המותקנים על העמדה.

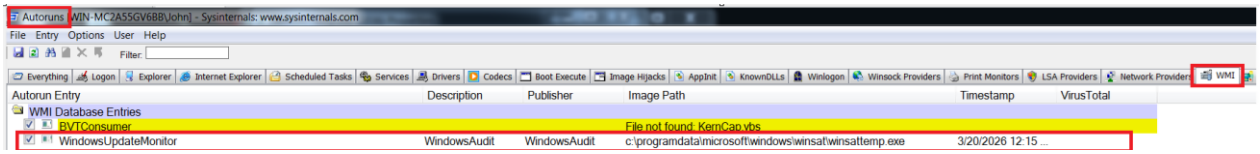
13. זוהתה יצירת שירות (Service Creation) עם שם התצוגה "Windows Audit", ותיאורו "Windows security audit and compliance monitoring service".
14. דוגמאות לפקודות PowerShell לזיהוי מנגנון אחיזה של הפוגען באמצעות אובייקטי WMI:



אם מופיע בפלט של הפקודה הראשונה WindowsUpdateMonitor, קיים חשד סביר שהעמדה הותקפה.

אם מופיע בפלט של הפקודה השנייה WindowsUpdateMonitor, וגם אחד הנתיבים המפורטים לעיל, התחנה מודבקת בנוזקה ברמת סבירות גבוהה.

15. דרך נוספת לזיהוי קיומו של הפוגען בעמדה היא באמצעות הכלי Sysinternals Autoruns:



[דרכי התמודדות]

1. להתרעה זו מצורף קובץ מזהים. מומלץ מאד **לחסום** מזהים אלו בכל אמצעי האבטחה הארגוניים הרלוונטיים.
2. מומלץ להשתמש בפקודות ה-PowerShell שתוארו לעיל, או בכלי Autoruns, לבדיקת עמדות החשודות כנגועות בפוגען.
3. מומלץ לנטר **תעבורה חריגה** מרשת ארגונכם לכתובות discord.com, gateway.discord.gg, בפרט אם נתוני התעבורה תואמים לפרטי תעבורת Discord המפורטים בסעיף "פרטים/5" לעיל, או שמקורה בשרתים, עמדות או VLANs שלא אמורים לתקשר ישירות עם Discord.
4. מומלץ לנטר **תעבורה חריגה** מרשת ארגונכם לכתובת *.hivemq.cloud . אם ארגונכם אינו משתמש בפרוטוקול MQTT, מומלץ לבחון חסימת תעבורה בפורט 8883 מתוך רשת הארגון, החוצה לרשת האינטרנט.
5. אם קיים חשד להימצאותו של הפוגען במערכות ארגונכם, נא עדכנו בהקדם האפשרי את מוקד 119 של מערך הסייבר הלאומי.