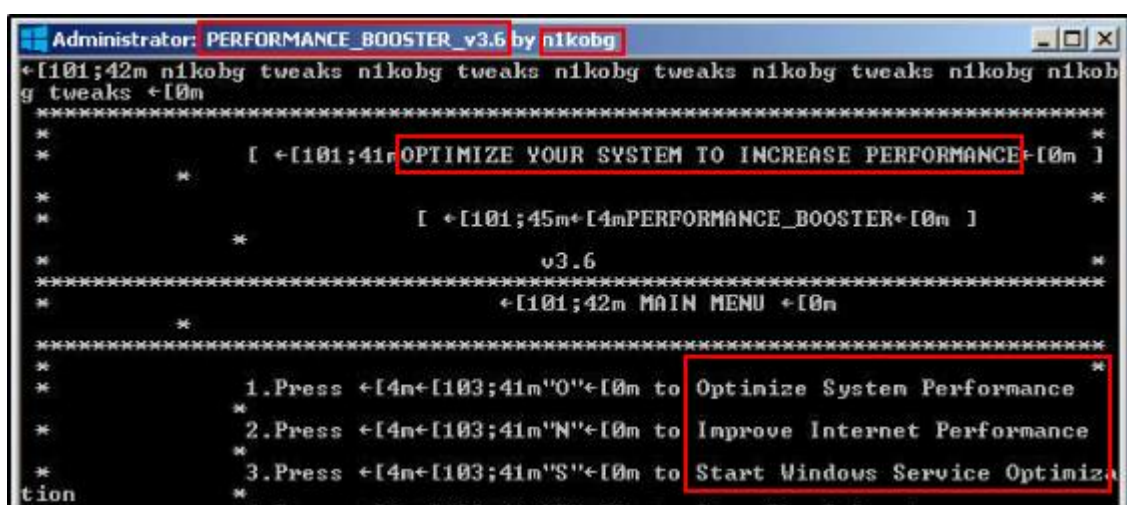


Bonus

Analizzare le seguenti segnalazioni e fare un piccolo report riguardo l'attacco spiegando com'è possibile evitarlo in futuro.

<https://app.any.run/tasks/8e6ad6d9-4d54-48e8-ad95-bfb67d47f1d7/>

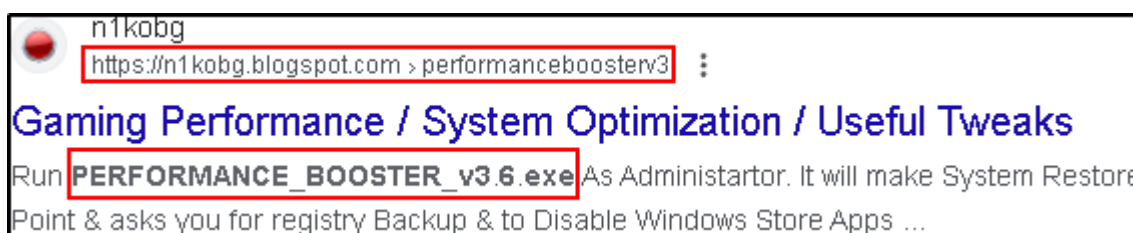
Dal nome e dalla finestra di avvio del file si suppone che il file sia un software che migliori le prestazioni del sistema. L'analisi di AnyRun rivela che il file PERFORMANCE_BOOSTER_v3.6.exe una volta avviato mostra varie attività malevole e sospette, tra cui modifiche alle politiche di esecuzione di PowerShell, il rilascio di file aggiuntivi, interazioni con il registro di sistema e potenziali connessioni di rete. Questo potrebbe portare ad una potenziale fuga di informazioni sensibili o danni al sistema.



```
Administrator: PERFORMANCE_BOOSTER_v3.6 by n1kobg
+ [101;42m n1kobg tweaks n1kobg tweaks n1kobg tweaks n1kobg tweaks n1kobg n1kobg
g tweaks + [0m

*****
*
*      [ + [101;41m OPTIMIZE YOUR SYSTEM TO INCREASE PERFORMANCE + [0m ]
*
*      [ + [101;45m + [4m PERFORMANCE_BOOSTER + [0m ]
*
*      v3.6
*
*      + [101;42m MAIN MENU + [0m
*
*****
*
*      1.Press + [4n + [103;41m "O" + [0m to Optimize System Performance
*
*      2.Press + [4n + [103;41m "N" + [0m to Improve Internet Performance
*
*      3.Press + [4n + [103;41m "S" + [0m to Start Windows Service Optimiza
tion
```

Facendo un'ulteriore ricerca incrociando nome del file e nome dell'autore troviamo un blog



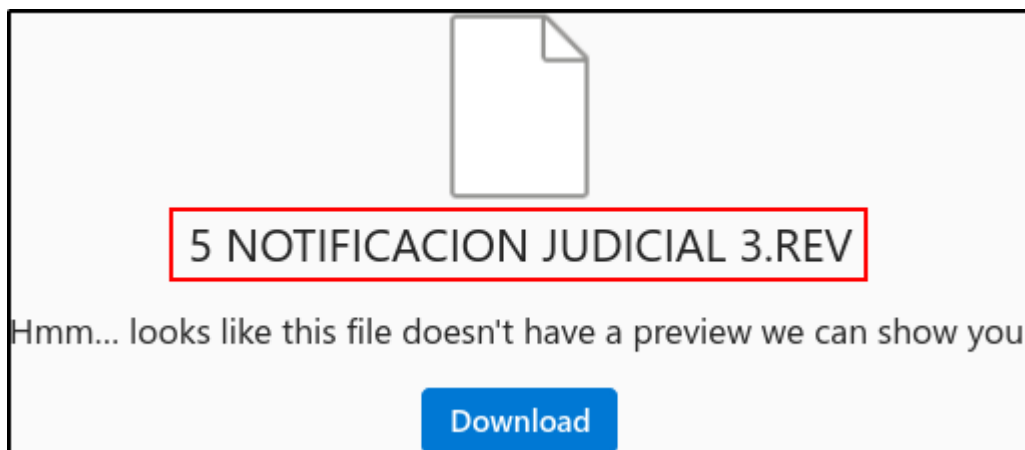
In quest'ultimo è spiegato nel dettaglio il comportamento del file. Secondo l'autore dovrebbe ottimizzare i processi del sistema eseguendo svariate modifiche, ma è sempre meglio dubitare di questo genere di software perchè possono avere scopi malevoli.

Per prevenire questo tipo di problemi è necessario:

- Non avviare file di cui si è prima verificata l'esatta provenienza
- Assicurarsi di avere un software antivirus aggiornato
- Usare un account utente senza privilegi di amministratore

<https://app.any.run/tasks/60b9570f-175b-4b03-816b-a38cc2b0255e/>

In questa situazione, il link in questione aveva come destinazione un file potenzialmente malevolo ospitato su OneDrive. Tuttavia, AnyRun non è riuscito a scaricare il file a causa dell'obsolescenza del browser utilizzato. Al posto di analizzare il comportamento del malware, AnyRun ha registrato l'avvio di una procedura di download e installazione di Microsoft Edge. Di conseguenza, il report non fornisce informazioni dettagliate sul comportamento effettivo del presunto malware, ma si concentra sulla sequenza di eventi legata all'installazione di Microsoft Edge.



Il nome del file suggerisce la possibilità che si tratti di un tentativo di phishing. L'approccio potrebbe coinvolgere l'invio di una notifica giudiziaria falsa, mirata a persuadere la vittima ad aprire il file allegato, che a sua volta comporterebbe un'eventuale infezione del sistema.

Per prevenire questo tipo di problemi è necessario:

- Usare filtri anti-phishing per prevenire l'apertura di link malevoli
- Fare particolarmente attenzione a file che creano un senso di urgenza per essere aperti, soprattutto se provenienti da fonti non confermate
- Assicurarsi di avere un software antivirus aggiornato