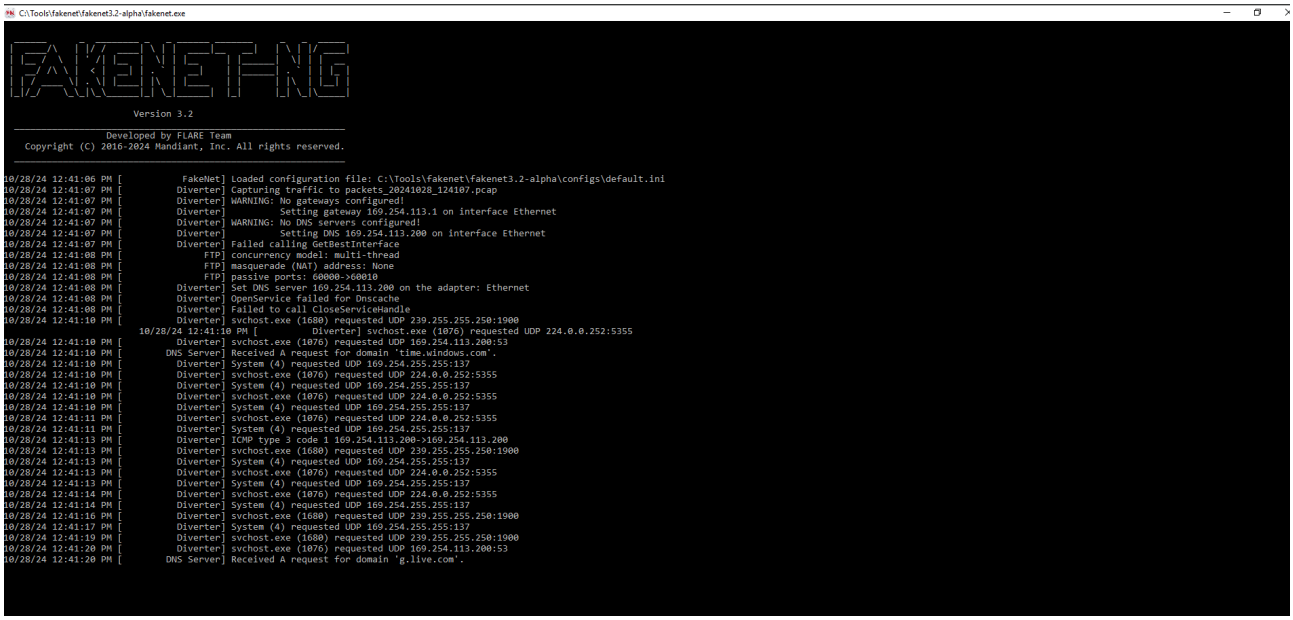
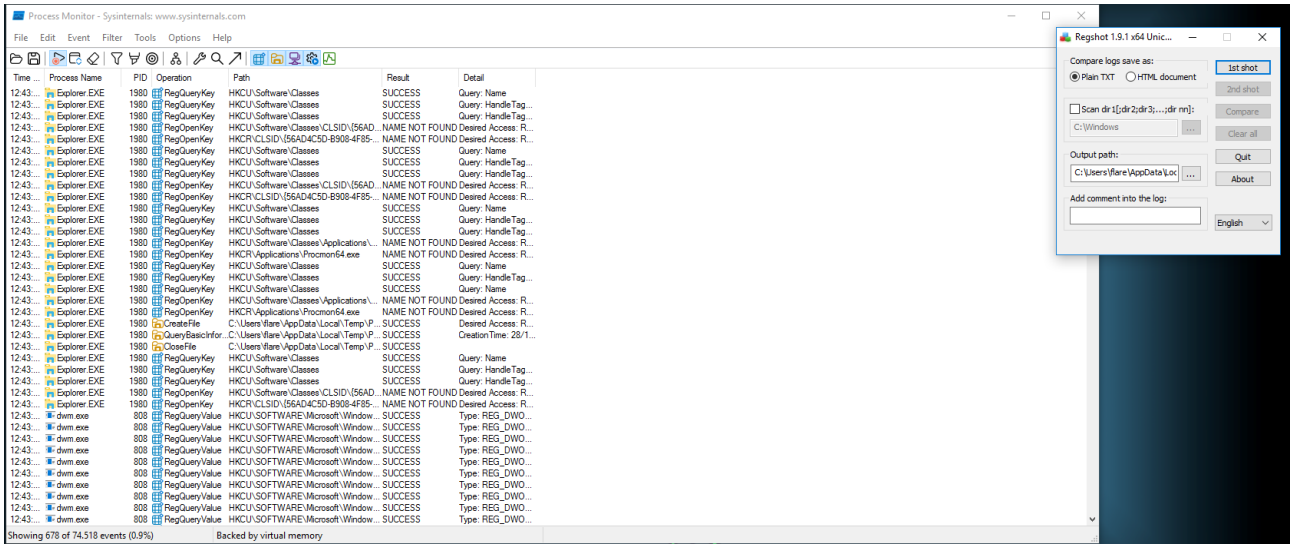
PROCEDIMENTO ANALISI DINAMICA Rogue Malware

Eseguo l’analisi dinamica in un ambiente controllato.

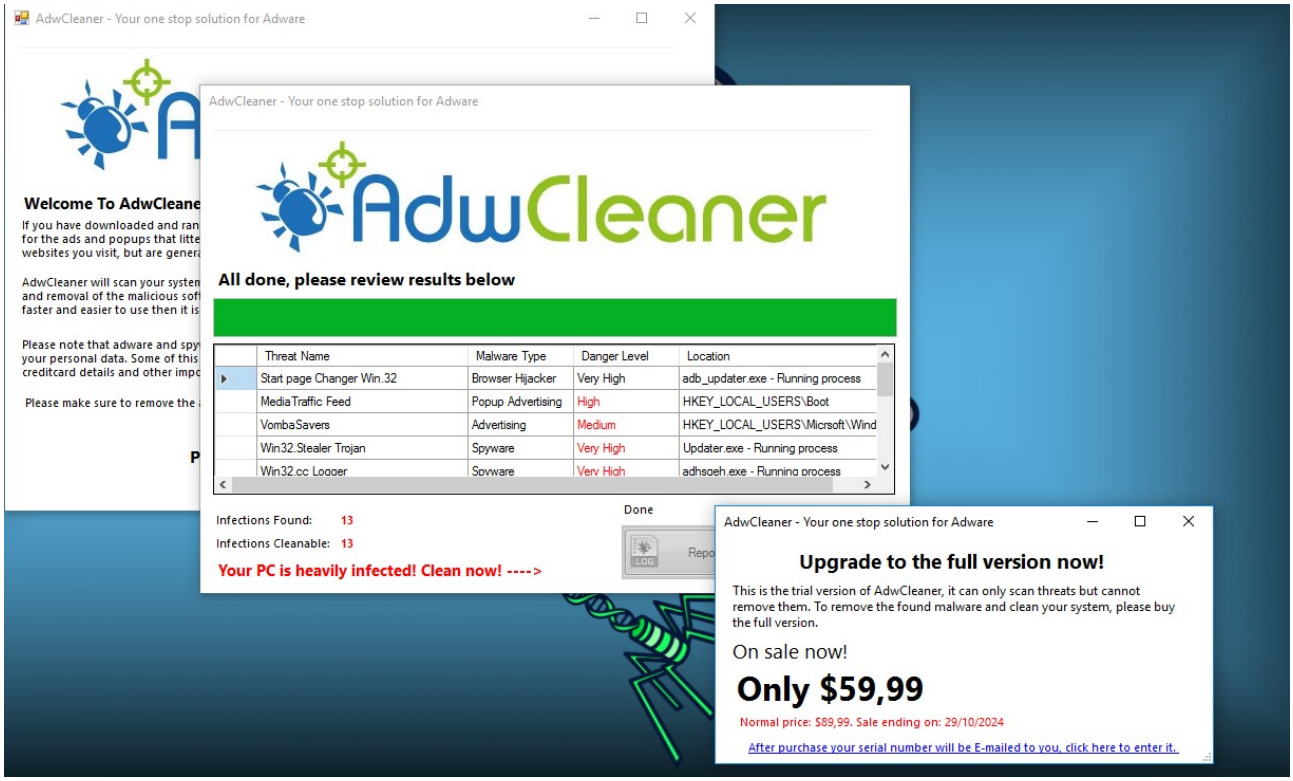
1. Avvio il programma fakenet per creare falso rumore di rete.



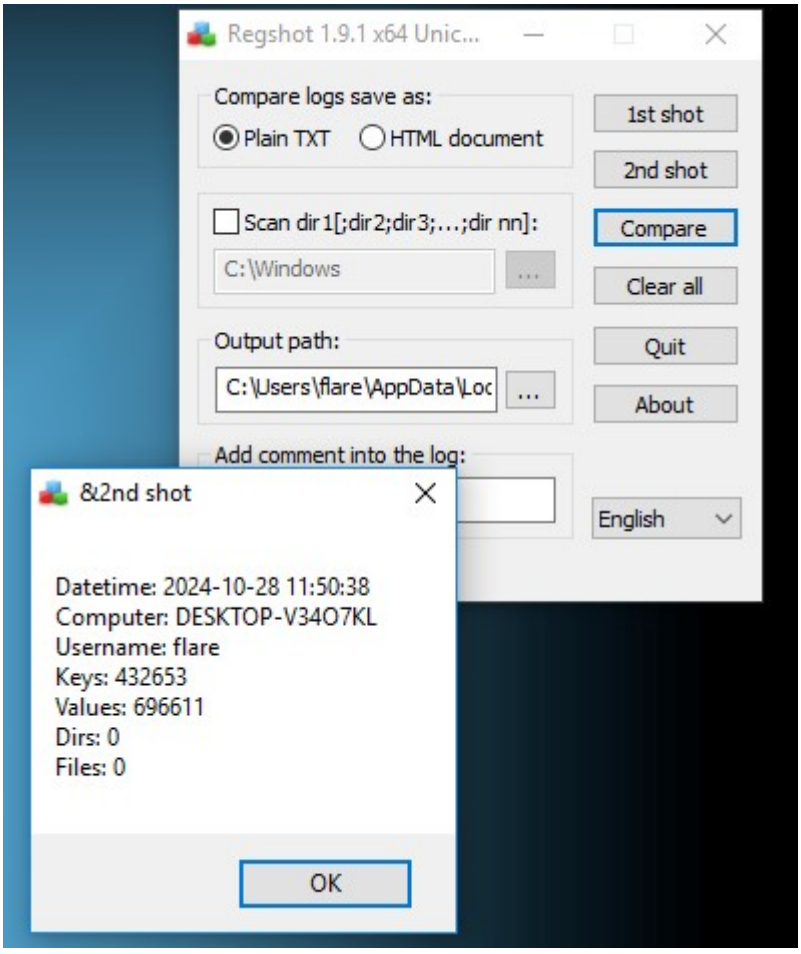
2. Avvio il programma procmon per monitorare i processi e il Programma regshot per confrontare il registro di windows e il file system in due momenti diversi.

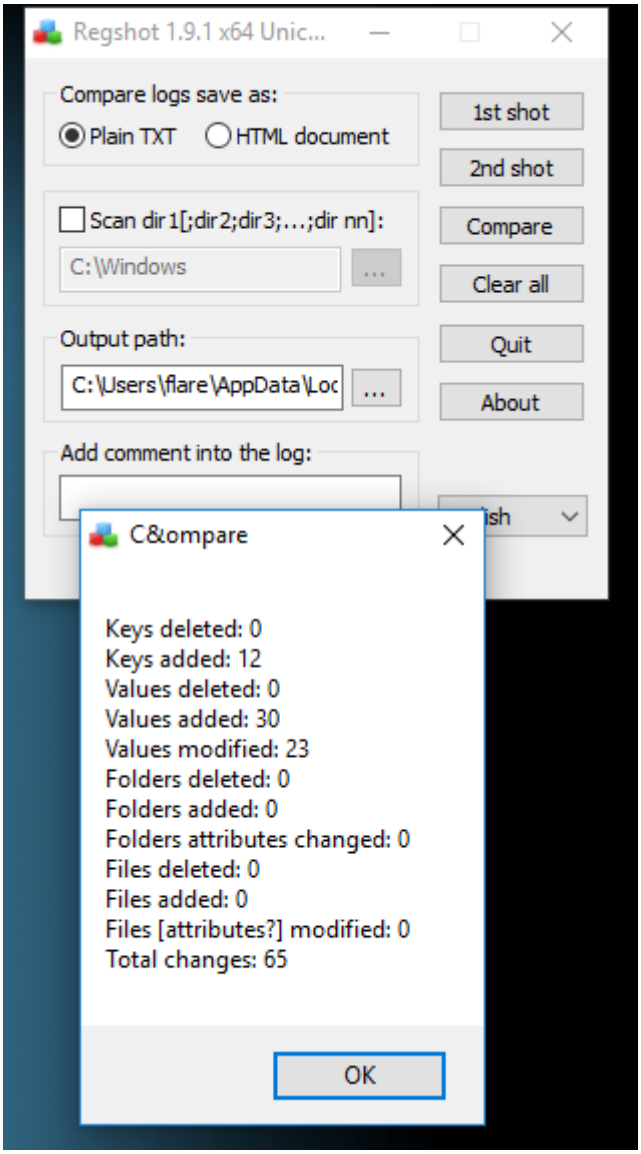


3. Eseguo quindi il first shot mediante regshot, dopodichè esegui il malware AdwCleaner.exe.



4. Effettuo il second shot mediante Regshot ed effettuo il confronto tra il primo e il secondo shot.




Regshot 1.9.1 x64 Unic...
Compare logs save as:
Plain TXT
HTML document
1st shot
2nd shot
Scan dir1[;dir2;dir3;...;dir nn]:
C:\Windows
Compare
Clear all
Output path:
C:\Users\flare\AppData\Loc
Quit
About
Add comment into the log:
C&ompare
Keys deleted: 0
Keys added: 12
Values deleted: 0
Values added: 30
Values modified: 23
Folders deleted: 0
Folders added: 0
Folders attributes changed: 0
Files deleted: 0
Files added: 0
Files [attributes?] modified: 0
Total changes: 65
OK

5. Analizzo il report generato da Regshot.

Ecco le principali modifiche:

1. Chiavi di registro aggiunte (Keys added: 12):

- Certificati di sicurezza in HKLM\SOFTWARE\Microsoft\SystemCertificates
- Chiavi relative al tracing per AdwCleaner
- Chiavi per la gestione delle finestre e delle applicazioni
- Chiave specifica di AdwCleaner sotto HKU

2. Valori modificati nel registro (Values modified: 23):

- Timestamp e configurazioni di diagnostica
- Impostazioni di interfaccia utente (posizioni finestre, etc)
- Statistiche di utilizzo delle applicazioni
- UserAssist (traccia dei programmi eseguiti)

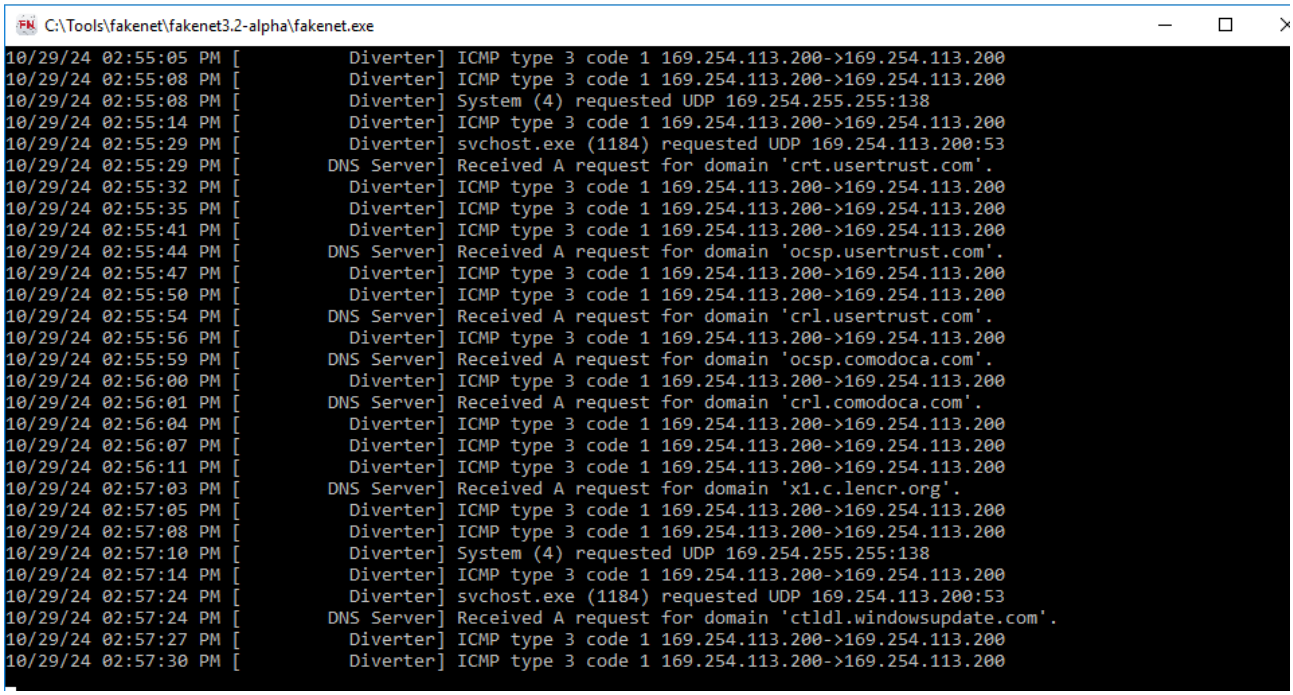
3. Valori aggiunti (Values added: 30):

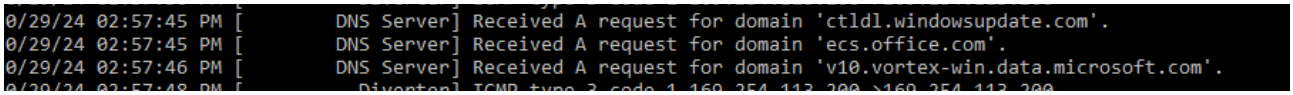
- Configurazioni per AdwCleaner
- Blob del certificato di sicurezza
- Percorsi dei file eseguiti
- Impostazioni di tracciamento
- Configurazioni finestre e UI

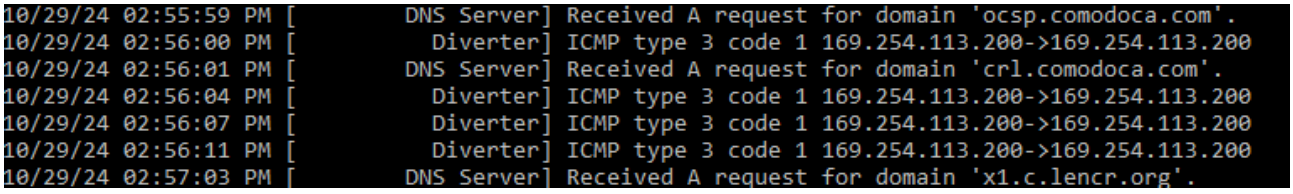
Queste modifiche mostrano:

- L'installazione di AdwCleaner e relative configurazioni
- L'aggiunta di certificati di sicurezza
- Modifiche al registro per tracciare l'esecuzione del programma
- Cambiamenti nelle impostazioni di visualizzazione delle finestre
- Log delle attività dell'utente

6. Analizzo il rumore di rete del malware mediante la fakenet.







Osservo che vengono eseguite delle richieste DNS e i domini coincidono con quelli risultanti dall’analisi statica delle stringhe del malware.