

# PROCEDIMENTO ANALISI DINAMICA Rogue Malware

## Esegui l'analisi dinamica in un ambiente controllato.

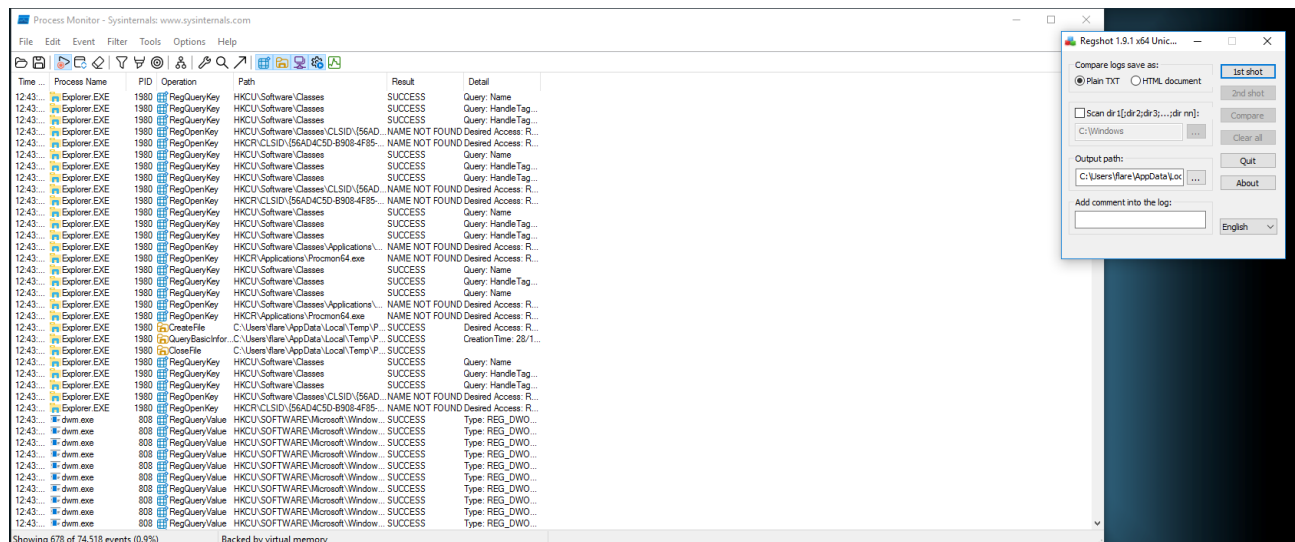
### 1. Avvio il programma fakenet per creare falso rumore di rete.

```
C:\Tools\fakenet\fakenet3.2-alpha\fakenet.exe

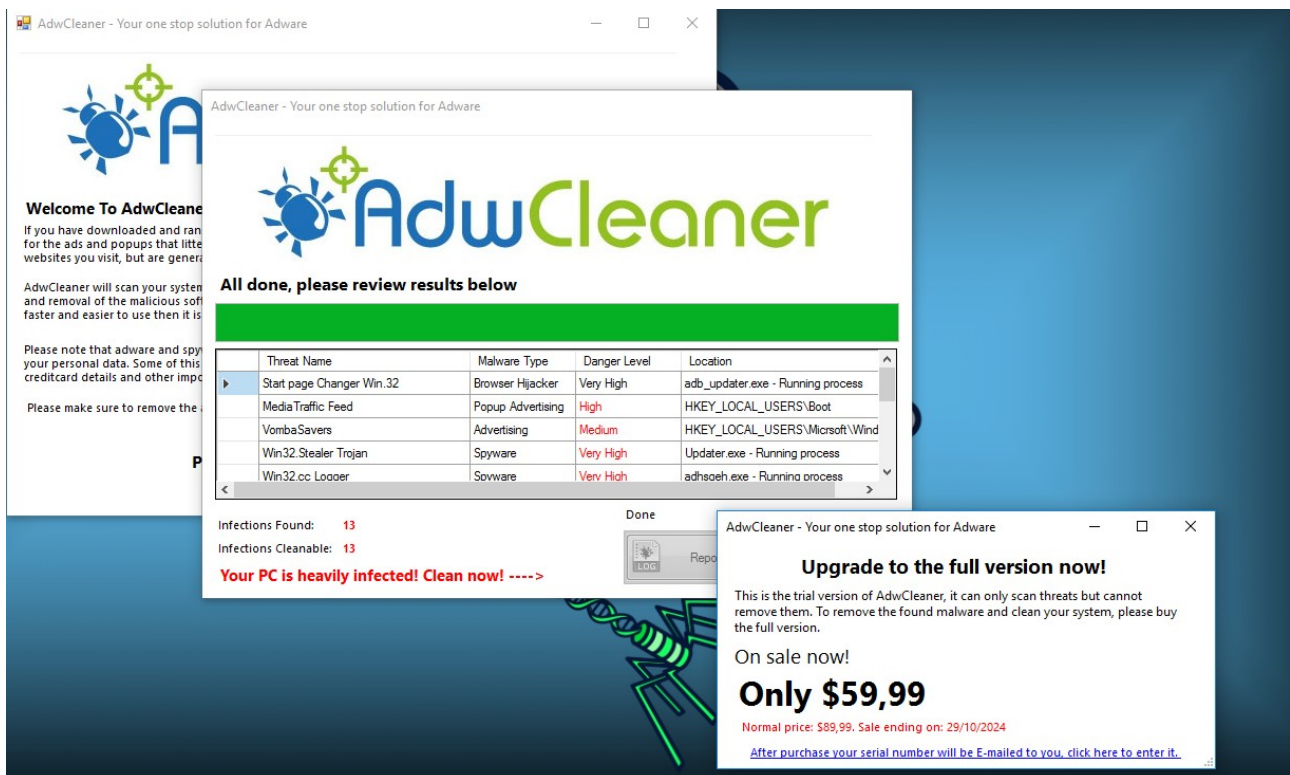
FAKENET-NG
Version 3.2
Developed by FLARE Team
Copyright (c) 2016-2024 Mandiant, Inc. All rights reserved.

10/28/24 12:41:06 PM [Fakelnet] Loaded configuration file: C:\Tools\fakenet\fakenet3.2-alpha\configs\default.ini
10/28/24 12:41:07 PM [Divertor] Capturing traffic to packets_20241028_124107.pcap
10/28/24 12:41:07 PM [Divertor] WARNING: No gateways configured!
10/28/24 12:41:07 PM [Divertor] Setting gateway 169.254.113.1 on interface Ethernet
10/28/24 12:41:07 PM [Divertor] WARNING: No DNS servers configured!
10/28/24 12:41:07 PM [Divertor] Setting DNS 169.254.113.200 on interface Ethernet
10/28/24 12:41:07 PM [Divertor] Failed calling GetBestInterface
10/28/24 12:41:08 PM [Divertor] concurrency model: multi-thread
10/28/24 12:41:08 PM [Divertor] masquerade (NAT) address: None
10/28/24 12:41:08 PM [Divertor] passive ports: 60800-60810
10/28/24 12:41:08 PM [Divertor] Set DNS server 169.254.113.200 on the adapter: Ethernet
10/28/24 12:41:08 PM [Divertor] OpenService failed for DnsCache
10/28/24 12:41:08 PM [Divertor] Failed to call CloseServiceHandle
10/28/24 12:41:10 PM [Divertor] svchost.exe (1680) requested UDP 239.255.255.250:1900
10/28/24 12:41:10 PM [Divertor] svchost.exe (1076) requested UDP 224.0.0.252:5355
10/28/24 12:41:10 PM [Divertor] svchost.exe (1076) requested UDP 169.254.113.200:53
10/28/24 12:41:10 PM [Divertor] DNS Server Received A request for domain 'time.windows.com'
10/28/24 12:41:10 PM [Divertor] System (4) requested UDP 169.254.255.255:137
10/28/24 12:41:10 PM [Divertor] svchost.exe (1076) requested UDP 224.0.0.252:5355
10/28/24 12:41:10 PM [Divertor] System (4) requested UDP 169.254.255.255:137
10/28/24 12:41:10 PM [Divertor] svchost.exe (1076) requested UDP 224.0.0.252:5355
10/28/24 12:41:10 PM [Divertor] System (4) requested UDP 169.254.255.255:137
10/28/24 12:41:11 PM [Divertor] svchost.exe (1076) requested UDP 224.0.0.252:5355
10/28/24 12:41:11 PM [Divertor] System (4) requested UDP 169.254.255.255:137
10/28/24 12:41:13 PM [Divertor] ICMP type 3 code 1 169.254.113.200->169.254.113.200
10/28/24 12:41:13 PM [Divertor] svchost.exe (1680) requested UDP 239.255.255.250:1900
10/28/24 12:41:13 PM [Divertor] System (4) requested UDP 169.254.255.255:137
10/28/24 12:41:13 PM [Divertor] svchost.exe (1076) requested UDP 224.0.0.252:5355
10/28/24 12:41:13 PM [Divertor] System (4) requested UDP 169.254.255.255:137
10/28/24 12:41:14 PM [Divertor] svchost.exe (1076) requested UDP 224.0.0.252:5355
10/28/24 12:41:14 PM [Divertor] System (4) requested UDP 169.254.255.255:137
10/28/24 12:41:16 PM [Divertor] svchost.exe (1680) requested UDP 239.255.255.250:1900
10/28/24 12:41:17 PM [Divertor] System (4) requested UDP 169.254.255.255:137
10/28/24 12:41:19 PM [Divertor] svchost.exe (1680) requested UDP 239.255.255.250:1900
10/28/24 12:41:20 PM [Divertor] svchost.exe (1076) requested UDP 169.254.113.200:53
10/28/24 12:41:20 PM [Divertor] DNS Server Received A request for domain 'g.live.com'.
```

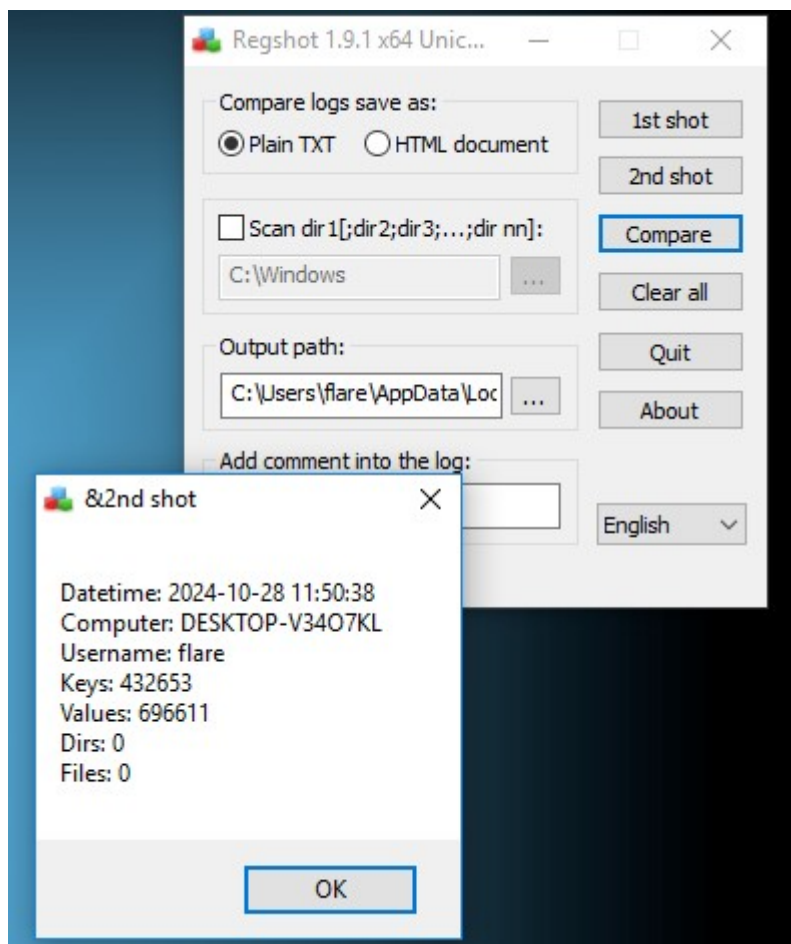
### 2. Avvio il programma procmon per monitorare i processi e il Programma regshot per confrontare il registro di windows e il file system in due momenti diversi.

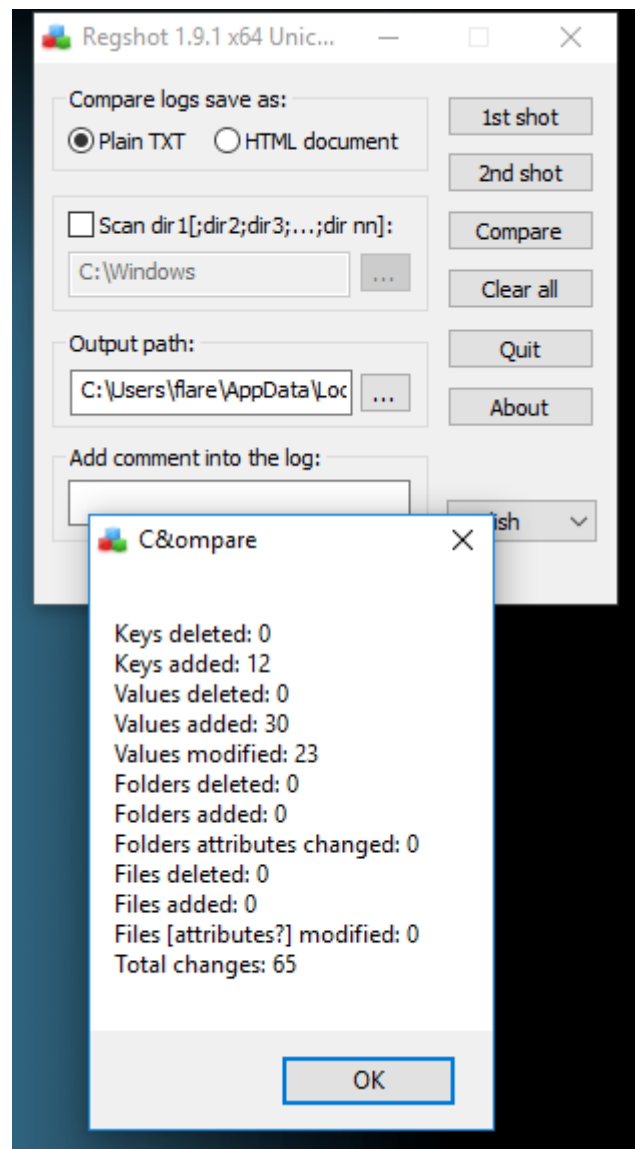


3. Eseguo quindi il first shot mediante regshot, dopodichè esegui il malware AdwCleaner.exe.



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





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.

```
C:\Tools\fakenet\fakenet3.2-alpha\fakenet.exe
10/29/24 02:55:05 PM [      Diverter] ICMP type 3 code 1 169.254.113.200->169.254.113.200
10/29/24 02:55:08 PM [      Diverter] ICMP type 3 code 1 169.254.113.200->169.254.113.200
10/29/24 02:55:08 PM [      Diverter] System (4) requested UDP 169.254.255.255:138
10/29/24 02:55:14 PM [      Diverter] ICMP type 3 code 1 169.254.113.200->169.254.113.200
10/29/24 02:55:29 PM [      Diverter] svchost.exe (1184) requested UDP 169.254.113.200:53
10/29/24 02:55:29 PM [      DNS Server] Received A request for domain 'crl.usertrust.com'.
10/29/24 02:55:32 PM [      Diverter] ICMP type 3 code 1 169.254.113.200->169.254.113.200
10/29/24 02:55:35 PM [      Diverter] ICMP type 3 code 1 169.254.113.200->169.254.113.200
10/29/24 02:55:41 PM [      Diverter] ICMP type 3 code 1 169.254.113.200->169.254.113.200
10/29/24 02:55:44 PM [      DNS Server] Received A request for domain 'ocsp.usertrust.com'.
10/29/24 02:55:47 PM [      Diverter] ICMP type 3 code 1 169.254.113.200->169.254.113.200
10/29/24 02:55:50 PM [      Diverter] ICMP type 3 code 1 169.254.113.200->169.254.113.200
10/29/24 02:55:54 PM [      DNS Server] Received A request for domain 'crl.usertrust.com'.
10/29/24 02:55:56 PM [      Diverter] ICMP type 3 code 1 169.254.113.200->169.254.113.200
10/29/24 02:55:59 PM [      DNS Server] Received A request for domain 'ocsp.comodoca.com'.
10/29/24 02:56:00 PM [      Diverter] ICMP type 3 code 1 169.254.113.200->169.254.113.200
10/29/24 02:56:01 PM [      DNS Server] Received A request for domain 'crl.comodoca.com'.
10/29/24 02:56:04 PM [      Diverter] ICMP type 3 code 1 169.254.113.200->169.254.113.200
10/29/24 02:56:07 PM [      Diverter] ICMP type 3 code 1 169.254.113.200->169.254.113.200
10/29/24 02:56:11 PM [      Diverter] ICMP type 3 code 1 169.254.113.200->169.254.113.200
10/29/24 02:57:03 PM [      DNS Server] Received A request for domain 'x1.c.lencr.org'.
10/29/24 02:57:05 PM [      Diverter] ICMP type 3 code 1 169.254.113.200->169.254.113.200
10/29/24 02:57:08 PM [      Diverter] ICMP type 3 code 1 169.254.113.200->169.254.113.200
10/29/24 02:57:10 PM [      Diverter] System (4) requested UDP 169.254.255.255:138
10/29/24 02:57:14 PM [      Diverter] ICMP type 3 code 1 169.254.113.200->169.254.113.200
10/29/24 02:57:24 PM [      Diverter] svchost.exe (1184) requested UDP 169.254.113.200:53
10/29/24 02:57:24 PM [      DNS Server] Received A request for domain 'ctldl.windowsupdate.com'.
10/29/24 02:57:27 PM [      Diverter] ICMP type 3 code 1 169.254.113.200->169.254.113.200
10/29/24 02:57:30 PM [      Diverter] ICMP type 3 code 1 169.254.113.200->169.254.113.200
```

```
10/29/24 02:57:45 PM [      DNS Server] Received A request for domain 'ctldl.windowsupdate.com'.
10/29/24 02:57:45 PM [      DNS Server] Received A request for domain 'ecs.office.com'.
10/29/24 02:57:46 PM [      DNS Server] Received A request for domain 'v10.vortex-win.data.microsoft.com'.
10/29/24 02:57:48 PM [      Diverter] ICMP type 3 code 1 169.254.113.200->169.254.113.200
```

```
10/29/24 02:55:59 PM [      DNS Server] Received A request for domain 'ocsp.comodoca.com'.
10/29/24 02:56:00 PM [      Diverter] ICMP type 3 code 1 169.254.113.200->169.254.113.200
10/29/24 02:56:01 PM [      DNS Server] Received A request for domain 'crl.comodoca.com'.
10/29/24 02:56:04 PM [      Diverter] ICMP type 3 code 1 169.254.113.200->169.254.113.200
10/29/24 02:56:07 PM [      Diverter] ICMP type 3 code 1 169.254.113.200->169.254.113.200
10/29/24 02:56:11 PM [      Diverter] ICMP type 3 code 1 169.254.113.200->169.254.113.200
10/29/24 02:57:03 PM [      DNS Server] Received A request for domain 'x1.c.lencr.org'.
```

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