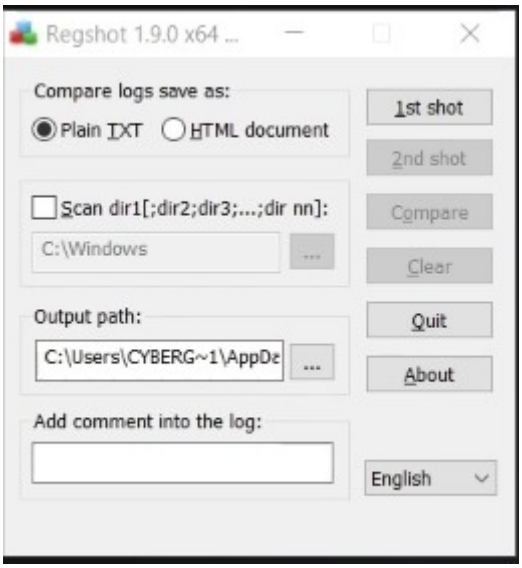
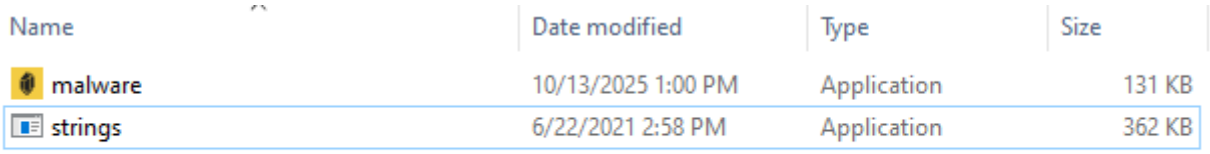
OUTPUT:

REGSHOT:

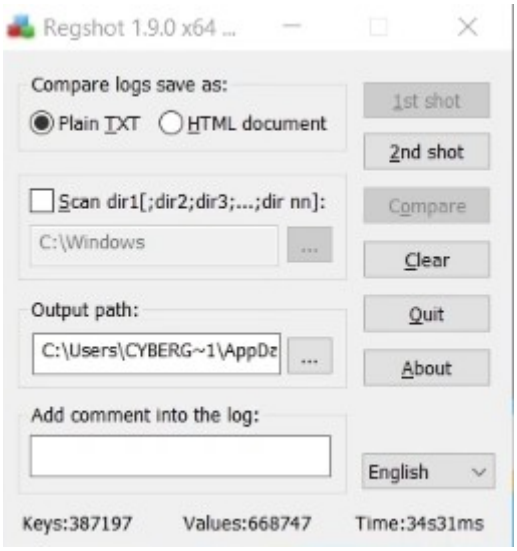
1) 1st Snapshot



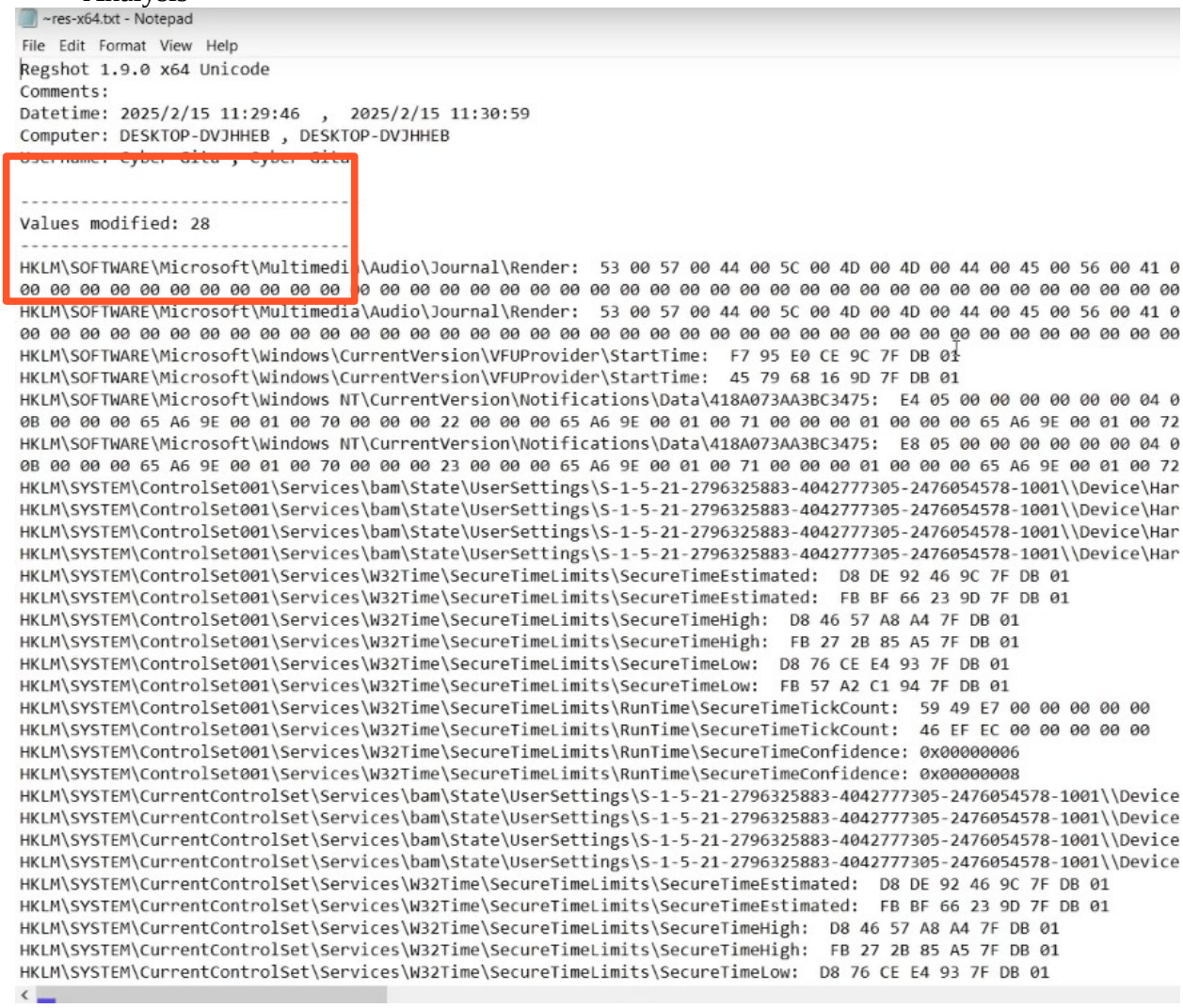
- Run that Malware



- 2nd Snapshot



- Analysis



~res-x64.txt - Notepad

File Edit Format View Help

```
Regshot 1.9.0 x64 Unicode
Comments:
Datetime: 2025/2/15 11:29:46  ,  2025/2/15 11:30:59
Computer: DESKTOP-DVJHHEB , DESKTOP-DVJHHEB
Username: Cyber Gitu , Cyber Gitu

----------------------------------
Values modified: 28
----------------------------------
HKLM\SOFTWARE\Microsoft\Multimedia\Audio\Journal\Render:  53 00 57 00 44 00 5C 00 4D 00 4D 00 44 00 45 00 56 00 41 0
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKLM\SOFTWARE\Microsoft\Multimedia\Audio\Journal\Render:  53 00 57 00 44 00 5C 00 4D 00 4D 00 44 00 45 00 56 00 41 0
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\VFUProvider\StartTime:  F7 95 E0 CE 9C 7F DB 01
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\VFUProvider\StartTime:  45 79 68 16 9D 7F DB 01
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC3475:  E4 05 00 00 00 00 00 00 04 0
0B 00 00 00 65 A6 9E 00 01 00 70 00 00 00 22 00 00 00 65 A6 9E 00 01 00 71 00 00 00 01 00 00 00 65 A6 9E 00 01 00 72
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC3475:  E8 05 00 00 00 00 00 00 04 0
0B 00 00 00 65 A6 9E 00 01 00 70 00 00 00 23 00 00 00 65 A6 9E 00 01 00 71 00 00 00 01 00 00 00 65 A6 9E 00 01 00 72
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2796325883-4042777305-2476054578-1001\\Device\Har
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2796325883-4042777305-2476054578-1001\\Device\Har
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2796325883-4042777305-2476054578-1001\\Device\Har
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2796325883-4042777305-2476054578-1001\\Device\Har
HKLM\SYSTEM\ControlSet001\Services\W32Time\SecureTimeLimits\SecureTimeEstimated:  D8 DE 92 46 9C 7F DB 01
HKLM\SYSTEM\ControlSet001\Services\W32Time\SecureTimeLimits\SecureTimeEstimated:  FB BF 66 23 9D 7F DB 01
HKLM\SYSTEM\ControlSet001\Services\W32Time\SecureTimeLimits\SecureTimeHigh:  D8 46 57 A8 A4 7F DB 01
HKLM\SYSTEM\ControlSet001\Services\W32Time\SecureTimeLimits\SecureTimeHigh:  FB 27 2B 85 A5 7F DB 01
HKLM\SYSTEM\ControlSet001\Services\W32Time\SecureTimeLimits\SecureTimeLow:  D8 76 CE E4 93 7F DB 01
HKLM\SYSTEM\ControlSet001\Services\W32Time\SecureTimeLimits\SecureTimeLow:  FB 57 A2 C1 94 7F DB 01
HKLM\SYSTEM\ControlSet001\Services\W32Time\SecureTimeLimits\RunTime\SecureTimeTickCount:  59 49 E7 00 00 00 00 00
HKLM\SYSTEM\ControlSet001\Services\W32Time\SecureTimeLimits\RunTime\SecureTimeTickCount:  46 EF EC 00 00 00 00 00
HKLM\SYSTEM\ControlSet001\Services\W32Time\SecureTimeLimits\RunTime\SecureTimeConfidence: 0x00000006
HKLM\SYSTEM\ControlSet001\Services\W32Time\SecureTimeLimits\RunTime\SecureTimeConfidence: 0x00000008
HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2796325883-4042777305-2476054578-1001\\Device
HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2796325883-4042777305-2476054578-1001\\Device
HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2796325883-4042777305-2476054578-1001\\Device
HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2796325883-4042777305-2476054578-1001\\Device
HKLM\SYSTEM\CurrentControlSet\Services\W32Time\SecureTimeLimits\SecureTimeEstimated:  D8 DE 92 46 9C 7F DB 01
HKLM\SYSTEM\CurrentControlSet\Services\W32Time\SecureTimeLimits\SecureTimeEstimated:  FB BF 66 23 9D 7F DB 01
HKLM\SYSTEM\CurrentControlSet\Services\W32Time\SecureTimeLimits\SecureTimeHigh:  D8 46 57 A8 A4 7F DB 01
HKLM\SYSTEM\CurrentControlSet\Services\W32Time\SecureTimeLimits\SecureTimeHigh:  FB 27 2B 85 A5 7F DB 01
HKLM\SYSTEM\CurrentControlSet\Services\W32Time\SecureTimeLimits\SecureTimeLow:  D8 76 CE E4 93 7F DB 01
```