Regshot 1.9.1 x64 Unicode (beta r321)
Comments:
Datetime: 2024-10-28 13:54:12, 2024-10-28 14:01:28
Computer: DESKTOP-V34O7KL, DESKTOP-V34O7KL
Username: flare, flare

Keys added: 12

HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\E12DFB4B41D7D9C32B30514BAC1D81D8385E2D46
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS
HKLM\SOFTWARE\WOW6432Node\Microsoft\SystemCertificates\AuthRoot\Certificates\E12DFB4B41D7D9C32B30514BAC1D81D8385E2D46
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000104E2
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000020234
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000204B4
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:000000000004044A
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000404B0
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000504BC
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\RecentApps\{7A3F7238-ABC4-455C-BC74-FDE20674D839}
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\AdwCleaner

---
Values added: 30

HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\E12DFB4B41D7D9C32B30514BAC1D81D8385E2D46\Blob: 03 00 00 00 01 00 00 00 14 00 00 00 E1 2D FB 4B 41 D7 D9 C3 2B 30 51 4B AC 1D 81 D8 38 5E 2D 46 68 00 00 00 01 00 00 00 08 00 00 00 00 40 91 20 D0 35 D9 01 7E 00 00 00 01 00 00 00 08 00 00 00 00 00 63 F5 89 26 D7 01 1D 00 00 00 01 00 00 00 10 00 00 00 F9 19 B9 CC CE 1E 59 C2 E7 85 F7 DC 2C CF 67 08 14 00 00 00 01 00 00 00 14 00 00 00 DA ED 64 74 14 9C 14 3C AB DD 99 A9 BD 5B 28 4D 8B 3C C9 D8 62 00 00 00 01 00 00 00 20 00 00 00 6F FF 78 E4 00 A7 0C 11 01 1C D8 59 77 C4 59 FB 5A F9 6A 3D F0 54 08 20 D0 F4 B8 60 78 75 E5 8F 09 00 00 00 01 00 00 00 22 00 00 00 30 20 06 08 2B 06 01 05 05 07 03 03 06 0A 2B 06 01 04 01 82 37 0A 03 04 06 08 2B 06 01 05 05 07 03 08 0B 00 00 00 01 00 00 00 2A 00 00 00 53 00 65 00 63 00 74 00 69 00 67 00 6F 00 20 00 28 00 55 00 54 00 4E 00 20 00 4F 00

62 00 6A 00 65 00 63 00 74 00 29 00 00 00 20 00 00 00 01 00 00 00 6A 04 00 00 30 82 04 66 30 82 03 4E
A0 03 02 01 02 02 10 44 BE 0C 8B 50 00 24 B4 11 D3 36 2D E0 B3 5F 1B 30 0D 06 09 2A 86 48 86 F7 0D 01 01 05 05 00 30 81 95 31 0B 30 09 06 03 55 04 06 13 02 55 53 31 0B 30 09 06 03 55 04 08 13 02 55 54 31 17 30 15 06 03 55 04 07 13 0E 53 61 6C 74 20 4C 61 6B 65 20 43 69 74 79 31 1E 30 1C 06 03 55 04 0A 13 15 54 68 65 20 55 53 45 52 54 52 55 53 54 20 4E 65 74 77 6F 72 6B 31 21 30 1F 06 03 55 04 0B 13 18 68 74 74 70 3A 2F 2F 77 77 77 2E 75 73 65 72 74 72 75 73 74 2E 63 6F 6D 31 1D 30 1B 06 03 55 04 03 13 14 55 54 4E 2D 55 53 45 52 46 69 72 73 74 2D 4F 62 6A 65 63 74 30 1E 17 0D 39 39 30 37 30 39 31 38 33 31 32 30 5A 17 0D 31 39 30 37 30 39 31 38 34 30 33 36 5A 30 81 95 31 0B 30 09 06 03 55 04 06 13 02 55 53 31 0B 30 09 06 03 55 04 08 13 02 55 54 31 17 30 15 06 03 55 04 07 13 0E 53 61 6C 74 20 4C 61 6B 65 20 43 69 74 79 31 1E 30 1C 06 03 55 04 0A 13 15 54 68 65 20 55 53 45 52 54 52 55 53 54 20 4E 65 74 77 6F 72 6B 31 21 30 1F 06 03 55 04 0B 13 18 68 74 74 70 3A 2F 2F 77 77 77 2E 75 73 65 7
2 74 72 75 73 74 2E 63 6F 6D 31 1D 30 1B 06 03 55 04 03 13 14 55 54 4E 2D 55 53 45 52 46 69 72 73 74 2D 4F 62 6A 65 63 74 30 82 01 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 82 01 0F 00 30 82 01 0A 02 82 01 01 00 CE AA 81 3F A3 A3 61 78 AA 31 00 55 95 11 9E 27 0F 1F 1C DF 3A 9B 82 68 30 C0 4A 61 1D F1 2F 0E FA BE 79 F7 A5 23 EF 55 51 96 84 CD DB E3 B9 6E 3E 31 D8 0A 20 67 C7 F4 D9 BF 94 EB 47 04 3E 02 CE 2A A2 5D 87 04 09 F6 30 9D 18 8A 97 B2 AA 1C FC 41 D2 A1 36 CB FB 3D 91 BA E7 D9 70 35 FA E4 E7 90 C3 9B A3 9B D3 3C F5 12 99 77 B1 B7 09 E0 68 E6 1C B8 F3 94 63 88 6A 6A FE 0B 76 C9 BE F4 22 E4 67 B9 AB 1A 5E 77 C1 85 07 DD 0D 6C BF EE 06 C7 77 6A 41 9E A7 0F D7 FB EE 94 17 B7 FC 85 BE A4 AB C4 1C 31 DD D7 B6 D1 E4 F0 EF DF 16 8F B2 52 93 D7 A1 D4 89 A1 07 2E BF E1 01 12 42 1E 1A E1 D8 95 34 DB 64 79 28 FF BA 2E 11 C2 E5 E8 5B 92 48 FB 47 0B C2 6C DA AD 32 83 41 F3 A5 E5 41 70 FD 65 90 6D FA FA 51 C4 F9 BD 96 2B 19 04 2C D3 6D A7 DC F0 7F 6F 83 65 E2 6A AB 87 86 75 02 03 01 00
01 A3 81 AF 30 81 AC 30 0B 06 03 55 1D 0F 04 04 03 02 01 C6 30 0F 06 03 55 1D 13 01 01 FF 04 05 30 03 01 01 FF 30 1D 06 03 55 1D 0E 04 16 04 14 DA ED 64 74 14 9C 14 3C AB DD 99 A9 BD 5B 28 4D 8B 3C C9 D8 30 42 06 03 55 1D 1F 04 3B 30 39 30 37 A0 35 A0 33 86 31 68 74 74 70 3A 2F 2F 63 72 6C 2E 75 73 65 72 74 72 75 73 74 2E 63 6F 6D 2F 55 54 4E 2D 55 53 45 52 46 69 72 73 74 2D 4F 62 6A 65 63 74 2E 63 72 6C 30 29 06 03 55 1D 25 04 22 30 20 06 08 2B 06 01 05 05 07 03 03 06 08 2B 06 01 05 05 07 03 08 06 0A 2B 06 01 04 01 82 37 0A 03 04 30 0D 06 09 2A 86 48 86 F7 0D 01 01 05 05 00 03 82 01 01 00 08 1F 52 B1 37 44 78 DB FD CE B9 DA 95 96 98 AA 55 64 80 B5 5A 40 DD 21 A5 C5 C1 F3 5F 2C 4C C8 47 5A 69 EA E8 F0 35 35 F4 D0 25 F3 C8 A6 A4 87 4A BD 1B B1 73 08 BD D4 C3 CA B6 35 BB 59 86 77 31 CD A7 80 14 AE 13 EF FC B1 48 F9 6B 25 25 2D 51 B6 2C 6D 45 C1 98 C8 8A 56 5D 3E EE 43 4E 3E 6B 27 8E D0 3A 4B 85 0B 5F D3 ED 6A A7 75 CB D1 5A 87 2F 39 75 13 5A 72 B0 02 81 9F BE F0 0F 84 54 20 62 6C 69 D4
E1 4D C6 0D 99 43 01 0D 12 96 8C 78 9D BF 50 A2 B1 44 AA 6A CF 17 7A CF 6F 0F D4 F8 24 55 5F F0 34 16 49 66 3E 50 46 C9 63 71 38 31 62 B8 62 B9 F3 53 AD 6C B5 2B A2 12 AA 19 4F 09 DA 5E E7 93 C6 8E 14 08 FE F0 30 80 18 A0 86 85 4D C8 7D D7 8B 03 FE 6E D5 F7 9D 16 AC 92 2C A0 23 E5 9C 91 52 1F 94 DF 17 94 73 C3 B3 C1 C1 71 05 20 00 78 BD 13 52 1D A8 3E CD 00 1F C8
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32\EnableFileTracing: 0x00000000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32\EnableAutoFileTracing: 0x00000000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32\EnableConsoleTracing: 0x00000000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32\FileTracingMask: 0xFFFF0000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32\ConsoleTracingMask: 0xFFFF0000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32\MaxFileSize: 0x00100000

HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASAPI32\FileDirectory: "%windir%\tracing"
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS\EnableFileTracing: 0x00000000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS\EnableAutoFileTracing: 0x00000000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS\EnableConsoleTracing: 0x00000000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS\FileTracingMask: 0xFFFF0000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS\ConsoleTracingMask: 0xFFFF0000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS\MaxFileSize: 0x00100000
HKLM\SOFTWARE\Microsoft\Tracing\6AdwCleaner_RASMANCS\FileDirectory: "%windir%\tracing"
HKLM\SOFTWARE\WOW6432Node\Microsoft\SystemCertificates\AuthRoot\Certificates\E12DFB4B41D7D9C32B30514BAC1D81D8385E2D46\Blob: 03 00 00 00 01 00 00 00 14 00 00 00 E1 2D FB 4B 41 D7 D9 C3 2B 30 51 4B AC 1D 81 D8 38 5E 2D 46 68 00 00 00 01 00 00 00 08 00 00 00 00 40 91 20 D0 35 D9 01 7E 00 00 00 01 00 00 00 08 00 00 00 00 00 63 F5 89 26 D7 01 1D 00 00 00 01 00 00 00 10 00 00 00 F9 19 B9 CC CE 1E 59 C2 E7 85 F7 DC 2C CF 67 08 14 00 00 00 01 00 00 00 14 00 00 00 DA ED 64 74 14 9C 14 3C AB DD 99 A9 BD 5B 28 4D 8B 3C C9 D8 62 00 00 00 01 00 00 00 20 00 00 00 6F FF 78 E4 00 A7 0C 11 01 1C D8 59 77 C4 59 FB 5A F9 6A 3D F0 54 08 20 D0 F4 B8 60 78 75 E5 8F 09 00 00 00 01 00 00 00 22 00 00 00 30 20 06 08 2B 06 01 05 05 07 03 03 06 0A 2B 06 01 04 01 82 37 0A 03 04 06 08 2B 06 01 05 05 07 03 08 0B 00 00 00 01 00 00 00 2A 00 00 00 53 00 65 00 63 00 74 00 69 00 67 00 6F 00 20 00 28 00 55 00 54 00 4E 00 20 00 4F 00 62 00 6A 00 65 00 63 00 74 00 29 00 00 00 20 00 00 00 01 00 00 00 6A 04 00 00 30 82 04 66
30 82 03 4E A0 03 02 01 02 02 10 44 BE 0C 8B 50 00 24 B4 11 D3 36 2D E0 B3 5F 1B 30 0D 06 09 2A 86 48 86 F7 0D 01 01 05 05 00 30 81 95 31 0B 30 09 06 03 55 04 06 13 02 55 53 31 0B 30 09 06 03 55 04 08 13 02 55 54 31 17 30 15 06 03 55 04 07 13 0E 53 61 6C 74 20 4C 61 6B 65 20 43 69 74 79 31 1E 30 1C 06 03 55 04 0A 13 15 54 68 65 20 55 53 45 52 54 52 55 53 54 20 4E 65 74 77 6F 72 6B 31 21 30 1F 06 03 55 04 0B 13 18 68 74 74 70 3A 2F 2F 77 77 77 2E 75 73 65 72 74 72 75 73 74 2E 63 6F 6D 31 1D 30 1B 06 03 55 04 03 13 14 55 54 4E 2D 55 53 45 52 46 69 72 73 74 2D 4F 62 6A 65 63 74 30 1E 17 0D 39 39 30 37 30 39 31 38 33 31 32 30 5A 17 0D 31 39 30 37 30 39 31 38 34 30 33 36 5A 30 81 95 31 0B 30 09 06 03 55 04 06 13 02 55 53 31 0B 30 09 06 03 55 04 08 13 02 55 54 31 17 30 15 06 03 55 04 07 13 0E 53 61 6C 74 20 4C 61 6B 65 20 43 69 74 79 31 1E 30 1C 06 03 55 04 0A 13 15 54 68 65 20 55 53 45 52 54 52 55 53 54 20 4E 65 74 77 6F 72 6B 31 21 30 1F 06 03 55 04 0B 13 18 68 74 74 70 3A 2F 2F 77 77 77 2
E 75 73 65 72 74 72 75 73 74 2E 63 6F 6D 31 1D 30 1B 06 03 55 04 03 13 14 55 54 4E 2D 55 53 45 52 46 69 72 73 74 2D 4F 62 6A 65 63 74 30 82 01 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 82 01 0F 00 30 82 01 0A 02 82 01 01 00 CE AA 81 3F A3 A3 61 78 AA 31 00 55 95 11 9E 27 0F 1F 1C DF 3A 9B 82 68 30 C0 4A 61 1D F1 2F 0E FA BE 79 F7 A5 23 EF 55 51 96 84 CD DB E3 B9 6E 3E 31 D8 0A 20 67 C7 F4 D9 BF 94 EB 47 04 3E 02 CE 2A A2 5D 87 04 09 F6 30 9D 18 8A 97 B2 AA 1C FC 41 D2 A1 36 CB FB 3D 91 BA E7 D9 70 35 FA E4 E7 90 C3 9B A3 9B D3 3C F5 12 99 77 B1 B7 09 E0 68 E6 1C B8 F3 94 63 88 6A 6A FE 0B 76 C9 BE F4 22 E4 67 B9 AB 1A 5E 77 C1 85 07 DD 0D 6C BF EE 06 C7 77 6A 41 9E A7 0F D7 FB EE 94 17 B7 FC 85 BE A4 AB C4 1C 31 DD D7 B6 D1 E4 F0 EF DF 16 8F B2 52 93 D7 A1 D4 89 A1 07 2E BF E1 01 12 42 1E 1A E1 D8 95 34 DB 64 79 28 FF BA 2E 11 C2 E5 E8 5B 92 48 FB 47 0B C2 6C DA AD 32 83 41 F3 A5 E5 41 70 FD 65 90 6D FA FA 51 C4 F9 BD 96 2B 19 04 2C D3 6D A7 DC F0 7F 6F 83 65 E2 6A AB 87 86 75
02 03 01 00 01 A3 81 AF 30 81 AC 30 0B 06 03 55 1D 0F 04 04 03 02 01 C6 30 0F 06 03 55 1D 13 01 01 FF 04 05 30 03 01 01 FF 30 1D 06 03 55 1D 0E 04 16 04 14 DA ED 64 74 14 9C 14 3C

AB DD 99 A9 BD 5B 28 4D 8B 3C C9 D8 30 42 06 03 55 1D 1F 04 3B 30 39 30 37 A0 35 A0 33 86 31 68 74 74 70 3A 2F 2F 63 72 6C 2E 75 73 65 72 74 72 75 73 74 2E 63 6F 6D 2F 55 54 4E 2D 55 53 45 52 46 69 72 73 74 2D 4F 62 6A 65 63 74 2E 63 72 6C 30 29 06 03 55 1D 25 04 22 30 20 06 08 2B 06 01 05 05 07 03 03 06 08 2B 06 01 05 05 07 03 08 06 0A 2B 06 01 04 01 82 37 0A 03 04 30 0D 06 09 2A 86 48 86 F7 0D 01 01 05 05 00 03 82 01 01 00 08 1F 52 B1 37 44 78 DB FD CE B9 DA 95 96 98 AA 55 64 80 B5 5A 40 DD 21 A5 C5 C1 F3 5F 2C 4C C8 47 5A 69 EA E8 F0 35 35 F4 D0 25 F3 C8 A6 A4 87 4A BD 1B B1 73 08 BD D4 C3 CA B6 35 BB 59 86 77 31 CD A7 80 14 AE 13 EF FC B1 48 F9 6B 25 25 2D 51 B6 2C 6D 45 C1 98 C8 8A 56 5D 3E EE 43 4E 3E 6B 27 8E D0 3A 4B 85 0B 5F D3 ED 6A A7 75 CB D1 5A 87 2F 39 75 13 5A 72 B0 02 81 9F BE F0 0F 84 54 20
62 6C 69 D4 E1 4D C6 0D 99 43 01 0D 12 96 8C 78 9D BF 50 A2 B1 44 AA 6A CF 17 7A CF 6F 0F D4 F8 24 55 5F F0 34 16 49 66 3E 50 46 C9 63 71 38 31 62 B8 62 B9 F3 53 AD 6C B5 2B A2 12 AA 19 4F 09 DA 5E E7 93 C6 8E 14 08 FE F0 30 80 18 A0 86 85 4D C8 7D D7 8B 03 FE 6E D5 F7 9D 16 AC 92 2C A0 23 E5 9C 91 52 1F 94 DF 17 94 73 C3 B3 C1 C1 71 05 20 00 78 BD 13 52 1D A8 3E CD 00 1F C8
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\syner\Qrfxgbc\Znyjner\ebthrf\NqjrerPyrnare.rkr: 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 80 CA EF 19 41 29 DB 01 00 00 00 00
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\syner\NccQngn\Ybpny\6NqjPyrnare.rkr: 00 00 00 00 00 00 00 00 03 00 00 00 3D EA 01 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000104E2\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000020234\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000204B4\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:000000000004044A\VirtualDesktop: 10 00 00 00 30 30 44 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000404B0\VirtualDesktop: 10 00 00 00 30 30 44 56 A7 E7 E4 2B D2 CB FE 44 A5 76 EC 0F 3D 89 20 5B
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000504BC\VirtualDesktop: 10 00 00 00 30 30 44 56 A7 E7 E4 2B D2 CB FE 44 A5 76 EC 0F 3D 89 20 5B

HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\AdwCleaner: ""C:\Users\flare\AppData\Local\6AdwCleaner.exe" -auto"
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\RecentApps\{7A3F7238-ABC4-455C-BC74-FDE20674D839}\LastAccessedTime: 0x01DB294119EFCA80
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\RecentApps\{7A3F7238-ABC4-455C-BC74-FDE20674D839}\AppId: "C:\Users\flare\Desktop\Malware\rogues\AdwereCleaner.exe"
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\RecentApps\{7A3F7238-ABC4-455C-BC74-FDE20674D839}\LaunchCount: 0x00000001
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\C:\Users\flare\Desktop\Malware\rogues\AdwereCleaner.exe: 53 41 43 50 01 00 00 00 00 00 00 00 07 00 00 00 28 00 00 00 48 FB 02 00 37 0F 03 00 01 00 00 00 00 00 00 00 00 00 03 06 00 01 00 00 33 50 4C 2B 57 DF D1 01 00 00 00 00 00 00 00 00
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\AdwCleaner\id: "0"

Values modified: 23

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\SettingsRequests\LastDownloadTime: 0x01DB293F3A63B3A3
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\SettingsRequests\LastDownloadTime: 0x01DB2941787EAF69
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC3475: 0F 00 00 00 00 00 00 00 01 00 04 00 01 02 01 00 98 2C 00 00 00 A2 05 06 00 01 00 99 04 00 00 00 A2 05 06 00
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC3475: 10 00 00 00 00 00 00 00 01 00 04 00 01 02 01 00 98 B3 00 00 00 A2 05 06 00 01 00 99 1F 00 00 00 A2 05 06 00
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\OneDrive\Accounts\LastUpdate: 0x00000000671F9753
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\OneDrive\Accounts\LastUpdate: 0x00000000671F97E4
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\HRZR_PGYFRFFVBA: 00 00 00 00 77 00 00 00 31 01 00 00 DC 77 5E 00 10 00 00 00 21 00 00 00 C6 3E 12 00 7B 00 31 00 41 00 43 00 31 00 34 00 45 00 37 00 37 00 2D 00 30 00 32 00 45 00 37 00 2D 00 34 00 45 00 35 00 44 00 2D 00 42 00 37 00 34 00 34 00 2D 00 32 00 45 00 42 00 31 00 41 00 45 00 35 00 31 00 39 00 38 00 42 00 37 00 7D 00 5C 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 50 00 6F 00 77 00 65 00 72 00 53 00 68 00 65 00 6C 00 6C 00 5C 00 76 00 31 00 2E 00 30 00 5C 00 70 00 6F 00 77 00 65 00 72 00 73 00 68 00 65 00 6C 00 6C 00 2E 00 65 00 78 00 65 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 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 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 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 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 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 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 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 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 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 01 00 00 00 29 00 00 00 AC EE 13 00 7B 00
31 00 41 00 43 00 31 00 34 00 45 00 37 00 37 00 2D 00 30 00 32 00 45 00 37 00 2D 00 34 00 45
00 35 00 44 00 2D 00 42 00 37 00 34 00 34 00 2
D 00 32 00 45 00 42 00 31 00 41 00 45 00 35 00 31 00 39 00 38 00 42 00 37 00 7D 00 5C 00 63 00
6D 00 64 00 2E 00 65 00 78 00 65 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 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 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 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 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 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 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 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 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 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 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 00
00 00 00 00 00 00 00 00 00 00 10 00 00 00 21 00 00 00 C6 3E 12 00 7B 00 31 00 41 00 43 00 31
00 34 00 45 00 37 00 37 00 2D 00 30 00 32 00 45 00 37 00 2D 00 34 00 45 00 35 00 44 00 2D 00
42 00 37 00 34 00 34 00 2D 00 32 00 45 00 42 00 31 00 41 00 45 00 35 00 31 00 39 00 38 00 42 00
37 00 7D 00 5C 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 50 00 6F 00 77 00 65 00 72 00 53
00 68 00 65 00 6C 00 6C 00 5C 00 76 00 31 00 2E 00 30 00 5C 00 70 00 6F 00 77 00 65 00 72 00
73 00 68 00 65 00 6C 00 6C 00 2E 00 65 00 78 00 65 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 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 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 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 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 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 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 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 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 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 0
0 00 00 00
HKU\S-1-5-21-3267748229-1519003285-2922249362-
1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-
4F4F-9178-9926F41749EA}\Count\HRZR_PGYFRFFVBA: 00 00 00 00 78 00 00 00 38 01 00 00
94 2B 64 00 10 00 00 00 21 00 00 00 C6 3E 12 00 7B 00 31 00 41 00 43 00 31 00 34 00 45 00 37
00 37 00 2D 00 30 00 32 00 45 00 37 00 2D 00 34 00 45 00 35 00 44 00 2D 00 42 00 37 00 34 00
34 00 2D 00 32 00 45 00 42 00 31 00 41 00 45 00 35 00 31 00 39 00 38 00 42 00 37 00 7D 00 5C
00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 50 00 6F 00 77 00 65 00 72 00 53 00 68 00 65 00 6C
00 6C 00 5C 00 76 00 31 00 2E 00 30 00 5C 00 70 00 6F 00 77 00 65 00 72 00 73 00 68 00 65 00
6C 00 6C 00 2E 00 65 00 78 00 65 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 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 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 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 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 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 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 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 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 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 01 00 00 00 29 00 00 00 AC EE 13 00 7B 00
31 00 41 00 43 00 31 00 34 00 45 00 37 00 37 00 2D 00 30 00 32 00 45 00 37 00 2D 00 34 00 45
00 35 00 44 00 2D 00 42 00 37 00 34 00 34 00 2
D 00 32 00 45 00 42 00 31 00 41 00 45 00 35 00 31 00 39 00 38 00 42 00 37 00 7D 00 5C 00 63 00
6D 00 64 00 2E 00 65 00 78 00 65 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 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 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 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 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 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 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 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 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 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 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 00
00 00 00 00 00 00 00 00 00 00 10 00 00 00 21 00 00 00 C6 3E 12 00 7B 00 31 00 41 00 43 00 31
00 34 00 45 00 37 00 37 00 2D 00 30 00 32 00 45 00 37 00 2D 00 34 00 45 00 35 00 44 00 2D 00
42 00 37 00 34 00 34 00 2D 00 32 00 45 00 42 00 31 00 41 00 45 00 35 00 31 00 39 00 38 00 42 00
37 00 7D 00 5C 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 50 00 6F 00 77 00 65 00 72 00 53
00 68 00 65 00 6C 00 6C 00 5C 00 76 00 31 00 2E 00 30 00 5C 00 70 00 6F 00 77 00 65 00 72 00
73 00 68 00 65 00 6C 00 6C 00 2E 00 65 00 78 00 65 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 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 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 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 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 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 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 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 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 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 0
0 00 00 00
HKU\S-1-5-21-3267748229-1519003285-2922249362-
1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-
4F4F-9178-9926F41749EA}\Count\Zvpebfbsg.Jvaqbjf.Rkcybere: 00 00 00 00 02 00 00 00 1B 00
00 00 AF 13 05 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00

00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 80 53 A6 44 EC 1D DB 01 00 00 00 00
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\Zvpebfbsg.Jvaqbjf.Rkcybere: 00 00 00 00 02 00 00 00 1D 00 00 00 DC B4 06 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 80 53 A6 44 EC 1D DB 01 00 00 00 00
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Gbbyf\Ertfubg-k64-Havpbqr\Ertfubg-k64-Havpbqr.rkr: 00 00 00 00 01 00 00 00 03 00 00 00 ED 65 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 90 8E BF C6 40 29 DB 01 00 00 00 00
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Gbbyf\Ertfubg-k64-Havpbqr\Ertfubg-k64-Havpbqr.rkr: 00 00 00 00 01 00 00 00 04 00 00 00 47 71 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 90 8E BF C6 40 29 DB 01 00 00 00 00
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\syner\NccQngn\Ybpny\Grzc\Cebpzba64.rkr: 00 00 00 00 00 00 00 00 01 00 00 00 C0 29 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\syner\NccQngn\Ybpny\Grzc\Cebpzba64.rkr: 00 00 00 00 00 00 00 00 02 00 00 00 B4 46 02 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{D0498E0A-45B7-42AE-A9AA-ABA463DBD3BF}\iexplore\Count: 0x0000000A
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{D0498E0A-45B7-42AE-A9AA-ABA463DBD3BF}\iexplore\Count: 0x0000000B
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{D0498E0A-45B7-42AE-A9AA-ABA463DBD3BF}\iexplore\Time: E8 07 0A 00 01 00 1C 00 0D 00 35 00 2B 00 89 03
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\Stats\{D0498E0A-45B7-42AE-A9AA-ABA463DBD3BF}\iexplore\Time: E8 07 0A 00 01 00 1C 00 0D 00 37 00 12 00 5C 00
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx: 03 00 00 00 04 00 00 00 02 00 00 00 01 00 00 00 00 00 00 00 FF FF FF FF
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx: 04 00 00 00 03 00 00 00 02 00 00 00 01 00 00 00 00 00 00 00 FF FF FF FF

HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MinPos1920x1014x96(1).x: 0xFFFFFFFF
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MinPos1920x1014x96(1).x: 0xFFFF8300
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MinPos1920x1014x96(1).y: 0xFFFFFFFF
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MinPos1920x1014x96(1).y: 0xFFFF8300
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x1014x96(1).left: 0x00000144
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x1014x96(1).left: 0x00000125
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x1014x96(1).top: 0x000000B9
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x1014x96(1).top: 0x000000DF
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x1014x96(1).right: 0x000005B7
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x1014x96(1).right: 0x00000598
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x1014x96(1).bottom: 0x0000033A
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x1014x96(1).bottom: 0x00000360
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx: 03 00 00 00 04 00 00 00 02 00 00 00 01 00 00 00 00 00 00 00 FF FF FF FF
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx: 04 00 00 00 03 00 00 00 02 00 00 00 01 00 00 00 00 00 00 00 FF FF FF FF
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MinPos1920x1014x96(1).x: 0xFFFFFFFF
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MinPos1920x1014x96(1).x: 0xFFFF8300
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MinPos1920x1014x96(1).y: 0xFFFFFFFF

HKU\S-1-5-21-3267748229-1519003285-2922249362-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MinPos1920x1014x96(1).y: 0xFFFF8300
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x1014x96(1).left: 0x00000144
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x1014x96(1).left: 0x00000125
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x1014x96(1).top: 0x000000B9
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x1014x96(1).top: 0x000000DF
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x1014x96(1).right: 0x000005B7
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x1014x96(1).right: 0x00000598
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x1014x96(1).bottom: 0x0000033A
HKU\S-1-5-21-3267748229-1519003285-2922249362-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1920x1014x96(1).bottom: 0x00000360

Total changes: 65
