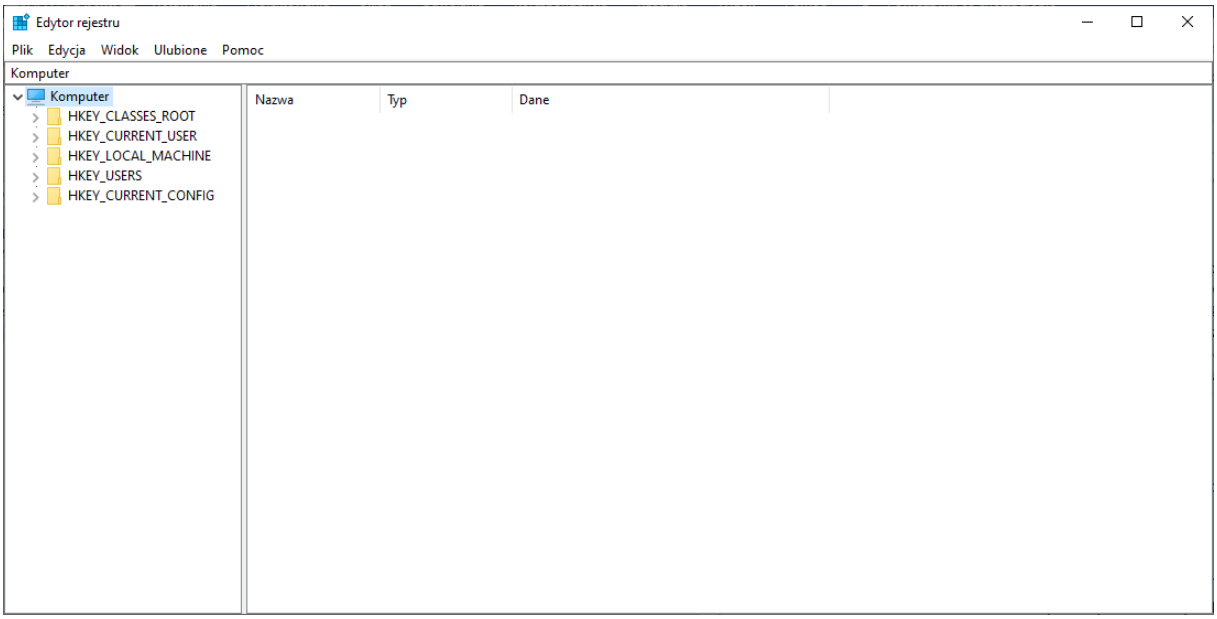
Rejestr systemu Windows

Czym jest rejestr?

Rejestr jest to baza danych zapisywana w kilku plikach w różnych częściach systemu. Baza ma strukturę hierarchiczną, czyli każda zmienna umieszczana jest w kluczu, który to znajduje się w innym kluczu i w taki sposób powstaje niezrozumiałe dla większości użytkowników, nieprzejrzyste drzewko, w którym każda gałąź może być odpowiedzialna na zupełnie różne funkcje i programy. W rejestrze przede wszystkim przechowywane są ustawienia konfiguracyjne systemu, ścieżki ważnych plików, czy tymczasowe zmienne. Klucze odpowiedzialne za działanie ogółu systemu współdzielone są z innymi użytkownikami i zapisywane w plikach bez rozszerzenia w folderze Windows\System32\config\, natomiast drzewka poszczególnych użytkowników system przechowuje w ich katalogach w plikach NTUSER.dat.

Programy do edycji rejestru

Najbardziej podstawowym i wbudowanym w system edytorem rejestru jest regedit.exe. W zupełności powinien on wystarczyć do większości zadań, ale jeśli potrzebowalibyśmy czegoś potężniejszego, zawsze można użyć takich programów jak Advanced Regedit, czy RegCool.



Obrazek 1: Program regedit

Podział rejestru

W rejestrze możemy wyróżnić 5 głównych gałęzi, z których każda służy do czegoś nieco innego.

HKEY_CLASSES_ROOT – zawiera definicje zapisanych w systemie rozszerzeń plików oraz przypisanych im programów, ikon itp.

HKEY_CURRENT_USER – zawiera konfigurację bieżącego profilu użytkownika

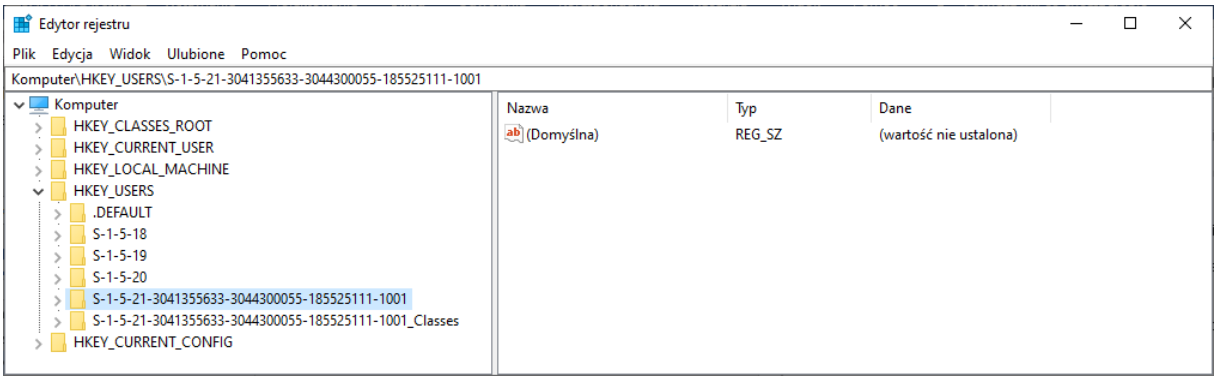
HKEY_LOCAL_MACHINE – zawiera najważniejsze informacje o konfiguracji komputera oraz niezbędne do rozruchu systemu

HKEY_USERS – zawiera informacje o każdym profilu użytkownika systemu, który kiedykolwiek zalogował się na komputerze

HKEY_CURRENT_CONFIG – inne dane konfiguracyjne systemu i programów

HKEY_USERS a HKEY_CURRENT_USER

Te dwa klucze są w zestawieniu siebie szczególnie ciekawe, gdyż HKEY_CURRENT_USER jest kopią jednego z kluczy gałęzi HKEY_USERS. Po co coś takiego? Prawdopodobnie dla kompatybilności lub ułatwienia roboty wszelakim programom aby nie musiały za każdym razem zdobywać SIDu użytkownika. No właśnie… w HKEY_USERS gałązki poszczególnych użytkowników, jak wszędzie w systemie, nie są identyfikowane po jego nazwie czy imieniu, a po specjalnym numerze SID, o którym już wspominałem. W gruncie rzeczy numer SID jest unikalny dla każdego użytkownika w systemie, jego pierwsza cyfra oznacza wersję identyfikatora, druga to identyfikator uprawnienia, kolejne kilka to ID komputera, a ostatnie 4 to numer użytkownika lub grupy.

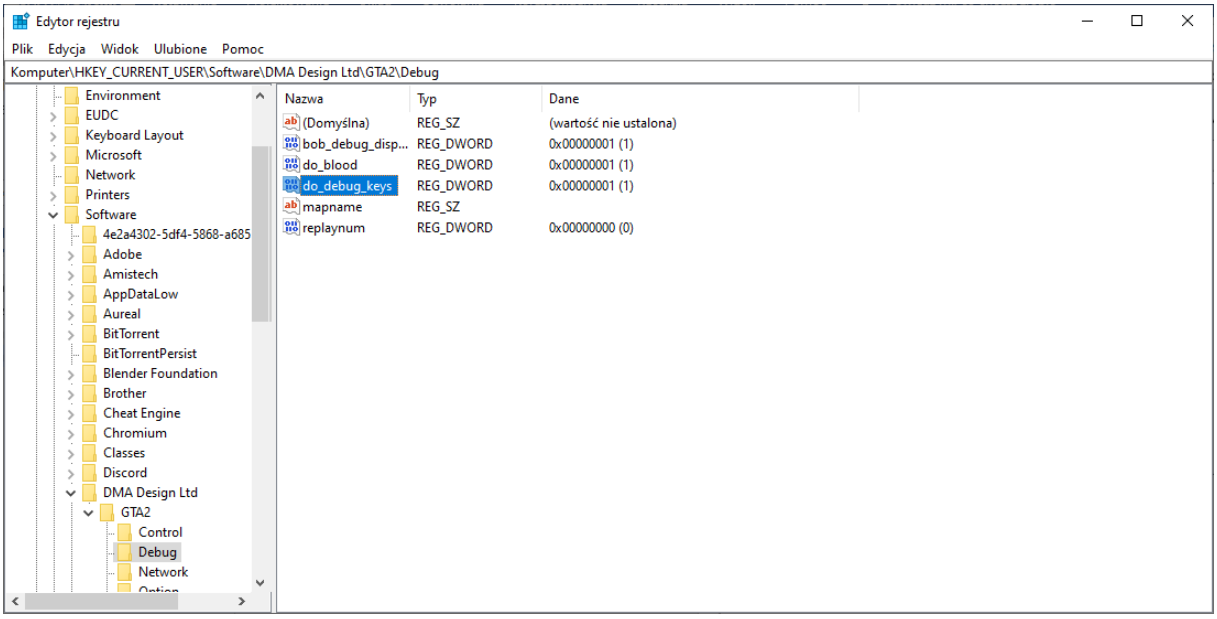


Obrazek 2: Zawartość gałązki HKEY_USERS

Swój SID możemy sprawdzić wpisując w CMD `whoami /user`.

Poruszanie się po rejestrze w regedit.exe

W programie regedit.exe klucze przedstawione są jako foldery o konkretnych nazwach, w których mogą znajdować się inne podfoldery i mamy w ten sposób ładnie pokazane drzewko kluczy. Po kliknięciu na strzałkę przy danym kluczu, zostanie on rozwinięty i ujrzymy jego podklucze. Jeśli natomiast klikniemy prosto na ikonkę lub nazwę, na panelu po prawej ukażą nam się wartości wraz z ich typem i danymi.



Obrazek 3: Przykładowy klucz wraz z jego wartościami

W systemie Windows 10 dostaliśmy też pewną funkcjonalność, która pozwala nam nieco szybciej wyszukiwać kluczy i przemieszczać się między nimi. Jest nią ten niepozorny pasek adresu u góry. Znacząco ułatwia nam on pracę z rejestrem. Możemy do niego wkleić konkretny adres w rejestrze i zostaniemy do niego przekierowani.

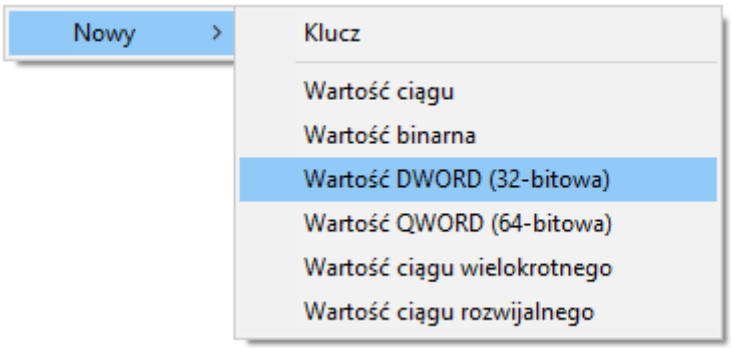
Ponad to możemy przeszukać rejestr w poszukiwaniu konkretnych kluczy, wartości, czy danych. Zrobimy to skrótem Ctrl + F3. W okienku możemy wpisać poszukiwany ciąg oraz wybrać typ informacji. Po wyświetleniu się pierwszego wyniku, możemy łatwo zmusić program do wyszukania kolejnego poprzez naciśnięcie przycisku F3. W taki sposób możemy łatwo przeklikać się do wartości, która jest nam potrzebna.

Tworzenie wartości

Po kliknięciu prawym przyciskiem myszy na dowolne puste miejsce panelu po prawej, będziemy mogli utworzyć nową wartość do obecnie zaznaczonego klucza. Wartości mają swoje typy, każdy służy do nieco innych zastosowań, a najczęściej używana jest zwykła wartość binarna.

Typ wartości możemy zdefiniować tylko podczas tworzenia zmiennej, nie może ona zostać potem w żaden sposób zedytowana.

Każda wartość w danym kluczu musi mieć swoją unikalną nazwę, którą możemy edytować klikając na nią prawym przyciskiem i wybierając opcję „Zmień nazwę” lub przy użyciu F2.



Obrazek 4: Wybieranie typu wartości

Wartość ciągu – tekst

Wartość binarna – czyste dane dla komputera wyświetlane w rejestrze dla uproszczenia w systemie szesnastkowym

DWORD – liczba 32-bitowa

QWORD – liczba 64-bitowa

Wartość ciągu wielokrotnego – kilka wartości ciągu połączonych w jedną. Poszczególne wartości oddzielane są spacją lub przecinkiem

Wartość ciągu rozwijalnego – zmienne tekstowe, które mogą łatwo zmieniać swoją długość

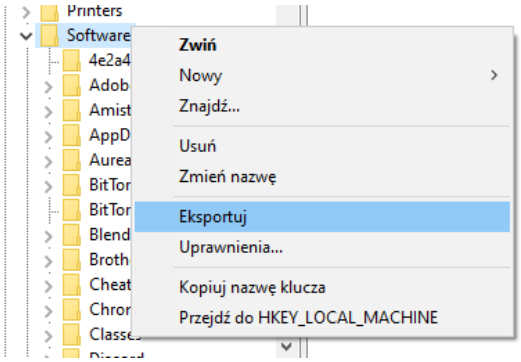
Niebezpieczeństwa przy edycji rejestru

Jak można było już zauważyć, regedit to potężne narzędzie pozwalające na zmianę przeróżnych ustawień systemu, profili, czy programów. Nie powinny mieć więc do niego dostępu osoby nieuprawnione. Edycja rejestru w systemie Windows jest więc możliwa tylko po otrzymaniu uprawnień administratora. Użytkownik bez admina nadal może jednak przeglądać rejestr o ile nie zostało mu to prawo odebrane. Jest to kolejny przykład tego, że bardzo uważnie powinniśmy rozdawać użytkownikom uprawnienia wyższe i jak jeden niezdarny bądź wredny użytkownik jest w stanie zniszczyć cały system i pracę innych.

Eksportowanie rejestru

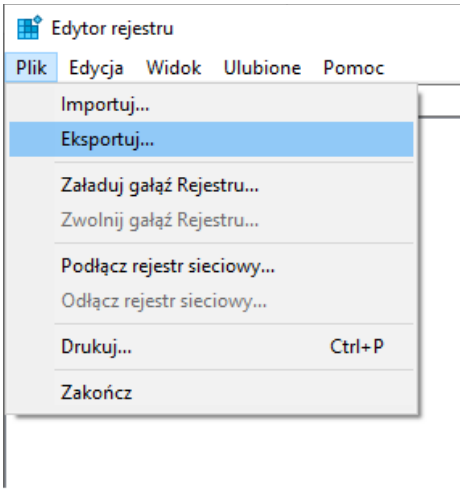
Jeśli chcemy podzielić się częścią swojego rejestru ze znajomym (nie polecam) lub po prostu zabezpieczyć się na wypadek zepsucia czegoś w nim, rejestr możemy wyeksportować do pliku .reg.

Eksportować możemy zarówno pojedynczą gałąź, jak i cały rejestr. Jeśli chcemy zrobić to pierwsze, po prostu klikamy prawym przyciskiem myszy na nią i wybieramy „Eksportuj”. Zostaniemy poproszeni o podanie ścieżki docelowej pliku i nasz kawałek rejestru zostanie zapisany.



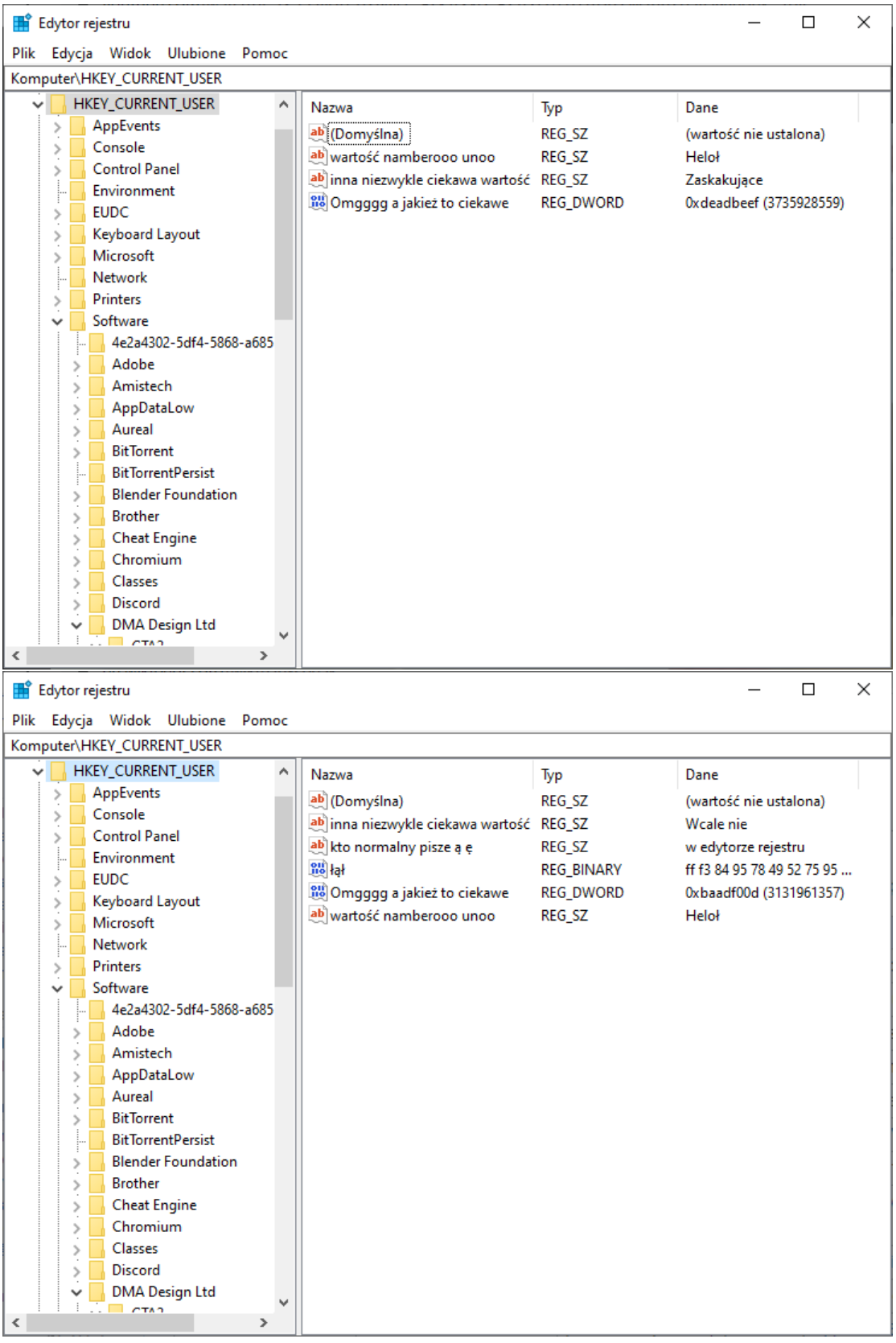
Obrazek 5: Eksportowanie danego klucza

Jeśli natomiast chcielibyśmy wyeksportować cały rejestr, wystarczy że wybierzemy z menu u góry Plik > Eksportuj… i zaznaczymy na dole „Wszystko”.



Obrazek 6: Eksportowanie całego rejestru

Plik .reg możemy później w każdej chwili otworzyć w eksploratorze i klucze zostaną nadpisane.



Obrazek 7: Przed i po imporcie klucza rejestru

Jak widać, po zaimportowaniu pliku .reg istniejące dane zostały nadpisane, a brakujące wartości utworzone.

Czyszczenie rejestru

Jak każdy element systemu, rejestr także może zostać zaśmiecony po dłuższym używaniu. Aby zapewnić szybką pracę komputera i w małym stopniu oczyścić także dysk, powinniśmy co jakiś czas skanować rejestr specjalnymi programami w poszukiwaniu nieużywanych kluczy, błędnych wartości itp. KŁAMSTWO! Dla komputera nie ma najmniejszego znaczenia, jak wiele kluczy jest w rejestrze, musiało by ich być naprawdę ogrom aby wywarło to jakikolwiek wpływ na działanie komputera co raczej nigdy się nie zdarza. Podobnie z rzekomo uszkodzonymi wartościami. Wartości takie nie istnieją, gdyby już coś miało się uszkodzić, to cały sektor lub dysk ale na tym ucierpiałby cały rejestr, a nie pojedyncze wartości. Natomiast klucze nieużywanych programów są tak małymi częściami danych, że nie są warte dogłębnych analiz rzekomo cudotwórczymi programami bo nieużywane pozostają dla systemu praktycznie niewidoczne, a na dysku zajmują tylko kilka bajtów. Swoją drogą programy takie od jakiegoś czasu wykrywane są przez sam system jako szkodliwe i blokowane są przez większość antywirusów.