Подмена базовых идентификаторов CurrentVersion

Версия 0.4

Введение

Назначение приложения - генерация системных идентификаторов, затрудняющая или в идеале делающая невозможной идентификацию пользователя и хоста.
Приложение будет иметь два режима - автоматический и экспртный, где идентификаторы выбираются вручную. Нас пока интересует только автоматический.
Алгоритм работы в общем случае следующий - приложение стартует и делает бэкап ключей реестра, которые могут быть затронуты генерацией. Пользователь выбирает, какие группы параметров нужно сгенерировать (список ниже). Приложение генерирует ряд параметров и записывает их в определенные ключи реестра. Какие-то параметры генерируются полностью рандомно, какие-то выбираются из списка, какие-то генерируются согласно алгоритма. Думаю, на первом этапе нас интересует только факт смены параметра.
Алгоритмы генерации не являются тривиальными, т.к. сгенерированные значения не должны навредить работе Windows и выглядеть “как настоящие”.
По окончании работы происходит откат к первоначальной конфигурации.
Важным моментом является поддержка x64 систем, где, как известно, есть ветка реестра для обратной совместимости с x86 приложениями. Некоторые параметры на 64-разрядных системах записываются в обе! Это надо учитывать, и я опишу ниже какие именно.
Ниже перечислены все пять групп, которые могут быть выбраны для генерации в отдельности.
Параметры, продублированные в ветках реестра WOW64_32 и WOW64_64, отмечены WOW64_32

Генерируемые параметры

Сетевые идентификаторы

Key	Value	Type
HKLM\SYSTEM\CurrentControlSet\services\Tcpip\Parameters	Hostname NV Hostname	REG_SZ
HKLM\SYSTEM\CurrentControlSet\services\Tcpip\Parameters	ComputerName	REG_SZ
HKLM\SYSTEM\CurrentControlSet\Control\ComputerName\ActiveComputerName	ComputerName	REG_SZ
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion (WOW64_32)	RegisteredOwner	REG_SZ

Идентификаторы операционной системы

Key	Value	Type
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion (WOW64_32)	BuildGUID BuildLab BuildLabEx CurrentBuild CurrentBuildNumber CurrentVersion EditionID ProductId ProductName	REG_SZ
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion	DigitalProductId DigitalProductId4	REG_BINARY
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion (WOW64_32)	InstallDate	REG_DWORD
HKLM\SOFTWARE\Microsoft\Internet Explorer (WOW64_32)	svcKBNumber	REG_SZ
HKLM\SOFTWARE\Microsoft\Internet Explorer\Registration	ProductId	REG_SZ
HKLM\SOFTWARE\Microsoft\Internet Explorer\Registration	DigitalProductId DigitalProductId4	REG_BINARY
HKLM\SOFTWARE\Microsoft\Internet Explorer\Migration (WOW64_32)	IE Installed Date	REG_BINARY

Аппаратный профиль

Key	Value	Type
HKLM\SYSTEM\CurrentControlSet\Control\IDConfigDB\Hardware Profiles\0001	HwProfileGuid	REG_SZ
HKLM\SOFTWARE\Microsoft\Cryptography	MachineGuid	REG_SZ
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate	SusClientId	REG_SZ
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate	SusClientIDValidation	REG_BINARY

Идентификаторы шрифтов

Идентификаторы шрифтов являются особым случаем, т.к. здесь мы не проверяем какое-то конкретное значение, а проверяем количество значений в ключе реестра (шрифтов в системе)

Key	Value	Type
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Fonts	-	REG_SZ

Телеметрия Windows 10

Как следует из заголовка, данные параметры присутствуют только в Windows 10

Key	Value	Type
HKLM\SOFTWARE\Microsoft\SQMClient	MachineId	REG_SZ
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Diagnostics\DiagTrack\SettingsRequests	ETagQueryParameters	REG_SZ

Формат параметров

Сетевые идентификаторы

Key	Value	Format
HKLM\SYSTEM\CurrentControlSet\services\Tcpip\Parameters	Hostname	Hostname
	NV Hostname	Hostname
	ComputerName	Hostname
HKLM\SYSTEM\CurrentControlSet\Control\ComputerName\ActiveComputerName	ComputerName	Username
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion	RegisteredOwner	Username

Идентификаторы операционной системы

Key	Value	Format
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion	BuildGUID	UUID
	BuildLab	From list
	BuildLabEx	From list
	CurrentBuild	From list
	CurrentBuildNumber	From list
	CurrentVersion	From list
	EditionID	From list
	ProductId	See format
	ProductName	From list
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion	DigitalProductId	See format
	DigitalProductId4	See format
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion	InstallDate	Unix time
HKLM\SOFTWARE\Microsoft\Internet Explorer	svcKBNumber	From list

HKLM\SOFTWARE\Microsoft\Internet Explorer\Registration	ProductId	Same as ProductID
	DigitalProductId	Same as DigitalProductId
	DigitalProductId4	Same as DigitalProductId4
HKLM\SOFTWARE\Microsoft\Internet Explorer\Migration	IE Installed Date	See format

UUID

Стандарный UUID в формате HEX:
ffffffff-ffff-ffff-ffff-ffffffffffff

BuildLab

[7601.win7sp1_ldr.170913-0600, 9600.winblue_r4.141028-1500, 16299.rs3_release.170928-1534]

BuildLabEx

[7601.23915.amd64fre.win7sp1_ldr.170913-0600, 9600.17415.amd64fre.winblue_r4.141028-1500, 16299.15.amd64fre.rs3_release.170928-1534]

CurrentBuild, CurrentBuildNumber

[7601, 9600, 16299]

CurrentVersion

[6.1, 7.1, 9.0]

BuildLabEx

[7601.23915.amd64fre.win7sp1_ldr.170913-0600, 9600.17415.amd64fre.winblue_r4.141028-1500, 16299.15.amd64fre.rs3_release.170928-1534]

EditionID

[Starter, HomeBasic, HomePremium, Professional, ProfessionalN, ProfessionalKN, Enterprise, Ultimate, Core, Pro, ProN, Enterprise, EnterpriseN, OEM, withBing, Home, ProEducation, EnterpriseLTSB, Education, IoTCore, IoTEnterprise, S]

ProductId

XXXXX-YYY-XXXXXXX-XXXXX

Где X - случайное число, YYY - случайные числа либо строка OEM

ProductName

[Windows 7, Windows 8.1, Windows 10]

DigitalProductId

Формат DigitalProductId следующий.
Это бинарный массив длиной 164 байта, изначально заполненный нулями
Диапазон [0x00:0x07] = [0xA4, 0, 0, 0, 0x3, 0, 0, 0]

Диапазон [0x08:0x19] содержит ProductID
Диапазон [0xA0:0xA3] = [0xB9, 0xEC, 0x21, 0x73]
Все остальное – нули

DigitalProductId4

Формат этого идентификатора еще сложнее.
Для этого ID сначала следует ввести понятие Dispersed String, строка, где каждый второй байт нулевой. Именно байт 0x00, а не символ “0”.
Затем - понятие Product DigitalID4 String, который представляет собой значительную часть этого идентификатора.
DigitalID4 имеет формат "{0}-{1}-{2}-{3}-{4}-{5}-{6}x0000{7}”
{0} - строка из 5 числовых символов
{1} - строка из 5 числовых символов
{2} - строка из 3 числовых символов
{3} - строка из 6 числовых символов
{4} - строка из 2 числовых символов
{5} - строка из 4 числовых символов
{6} - строка из 4 числовых символов
{7} - год установки системы, очевидно, не может быть в будущем
И эта строка является Dispersed String, то есть, каждый второй байт - нулевой, включая завершающий строку.

CamDigitalID4 представляет собой бинарный массив длиной 1272 байта, изначально заполненный нулями
Первые два байта [0xF8, 0x04]
Со смещения 0x08 начинается Product DigitalID4 String, и он имеет фиксированную длину.
Со смещения 0x88 начинается случайный UUID в виде Dispersed String, и он также имеет фиксированную длину
Со смещения 0x118 начинается System Edition, (например Education, ProfessionalN, IoTCore - сам Edition без пробелов), в формате Dispersed String. Он имеет переменную длину.
Со смещения 0x0328 начинается случайный массив размером 80 байт
Со смещения 0x0378 начинается Dispersed String в формате "{0}{1}-{2}”, где
{0} - символ в UPPERCASE
{1} - строка из 2 числовых символов
{2} - строка из 5 числовых символов
Со смещения 0x03F8 начинается Dispersed String “Retail” или “OEM”, и должно соответствовать сгенерированному ранее приложением параметру.
Смещение 0x0478 содержит ту же строку, что и 0x03F8.

svcKBNumber

[KB2841134, KB4088835, KB4032782, KB4016446, KB3210694, KB3200006, KB3199375, KB3192665, KB4096040, KB4089187, KB4074736, KB4056568, KB4052978, KB4047206, KB4040685, KB4036586, KB4034733, KB4025252, KB4021558, KB4018271, KB4014661, KB4012204, KB3185319, KB3175443, KB3170106, KB3160005, KB3154070, KB3148198]

IE Installed Date

Бинарный массив из 8 байт, где байты с 0x1 до 0x4 - Unix time, остальные – случайные числа

Аппаратный профиль

Key	Value	Format
HKLM\SYSTEM\CurrentControlSet\Control\IDConfigDB\Hardware Profiles\0001	HwProfileGuid	{UUID}
HKLM\SOFTWARE\Microsoft\Cryptography	MachineGuid	UUID
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate	SusClientId	UUID
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate	SusClientIDValidation	See format

{UUID}

UUID в фигурных скобках:
{ffffffff-ffff-ffff-ffff-ffffffffffff}

UUID

Стандарный UUID в формате HEX:
ffffffff-ffff-ffff-ffff-ffffffffffff

SusClientIDValidation

Первые четыре байта [0x06, 0x02, 0x28, 0x01]
Следующие три (5-7) байта случайные
Восьмой байт нулевой

Со смещения 0x08 начинается Disperse String длиной 19 символов (38 байт), состоящая из случайных численных символов и букв в UPPERCASE
По смещению 0x2D находится массив [0x0, 0x06, 0x0]
По смещению 0x30 находится массив из 5 случайных байт
Со смещения 0x36 начинается Disperse String “None”
Посмещению 0x3D идентификатор заканчивается байтами [0x20, 0x0]

Параметры для добавления в следующих версиях

Key	Value	Format
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion	CSDVersion	From list
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion	CSDBuildNumber	REG_DWORD
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion	InstallationType	From list

CSDVersion

Версия последнего Service Pack, если установлен. Например "Service Pack 1: для Windows 7

CSDBuildNumber

Номер билда последнего Service Pack, должен соответствовать CSDVersion, например 1130 для Windows 7 Service Pack 1

InstallationType

Client или Server в зависимости от семейства ОС, значение “Server” актуально для любой версии Windows Server

Список версий

0.1	Начальный вариант, перечистены параметры, расположение в реестре и типы
0.2	Описаны возможные значения сетевых идентификаторов и системных идентификаторов, кроме DigitalProductId4
0.3	Добавлено описание DigitalProductId4 и SusClientIDValidation
0.4	Добавлены параметры для будущих версий приложения