ID: 635341
Sample Name:
activation.reg.exe
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 19:30:37
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

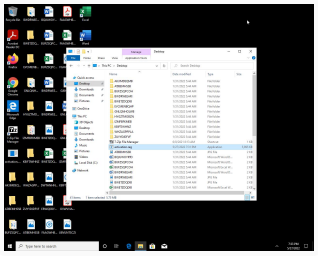
Windows Analysis Report

activation.reg.exe

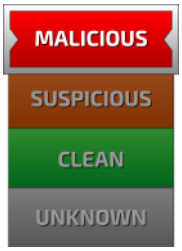
Overview

General Information

Sample Name:	activation.reg.exe (renamed file extension from exe to dll)
Analysis ID:	635341
MD5:	e49b92466821b1.
SHA1:	b2bbafa02be38b..
SHA256:	90a0e059cd3f4e..



Detection

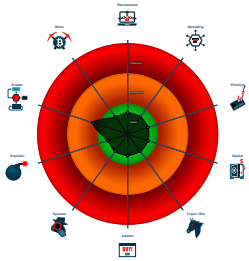


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Uses 32bit PE files
- Creates a process in suspended mo…
- Creates files inside the system direc…

Classification



Process Tree

- **System is start**
- loaddll32.exe (PID: 7648 cmdline: loaddll32.exe "C:\Users\alfredo\Desktop\activation.reg.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 6804 cmdline: cmd.exe /C rundll32.exe "C:\Users\alfredo\Desktop\activation.reg.dll",#1 MD5: 4943BA1A9B41D69643F69685E35B2943)
    - rundll32.exe (PID: 7120 cmdline: rundll32.exe "C:\Users\alfredo\Desktop\activation.reg.dll",#1 MD5: D0432468FA4B7F66166C430E1334DBDA)
  - rundll32.exe (PID: 4228 cmdline: rundll32.exe C:\Users\alfredo\Desktop\activation.reg.dll,dummy MD5: D0432468FA4B7F66166C430E1334DBDA)
  - rundll32.exe (PID: 7468 cmdline: rundll32.exe "C:\Users\alfredo\Desktop\activation.reg.dll",dummy MD5: D0432468FA4B7F66166C430E1334DBDA)
- rundll32.exe (PID: 6364 cmdline: C:\Windows\System32\rundll32.exe C:\Windows\System32\shell32.dll,SHCreateLocalServerRunDll {9aa46009-3ce0-458a-a354-715610a075e6} -Embedding MD5: F68AF942FD7CCC0E7BAB1A2335D2AD26)
- **cleanup**

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

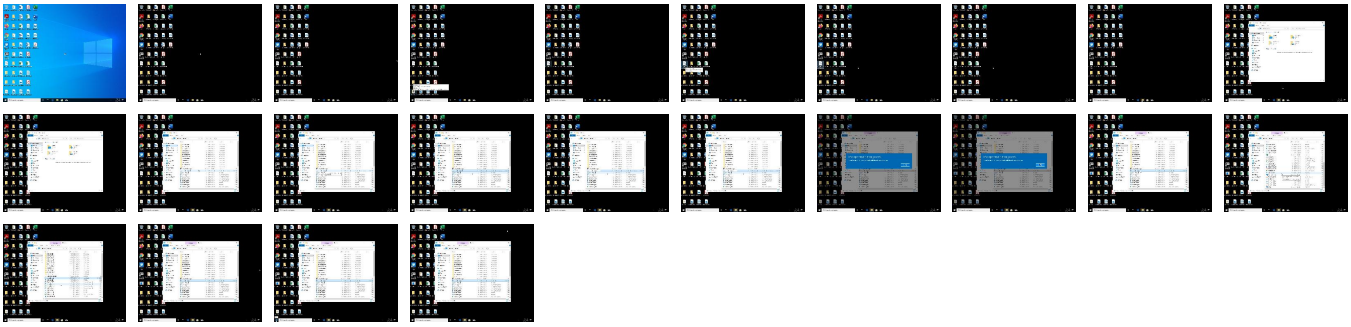
Mitre Att&ck Matrix

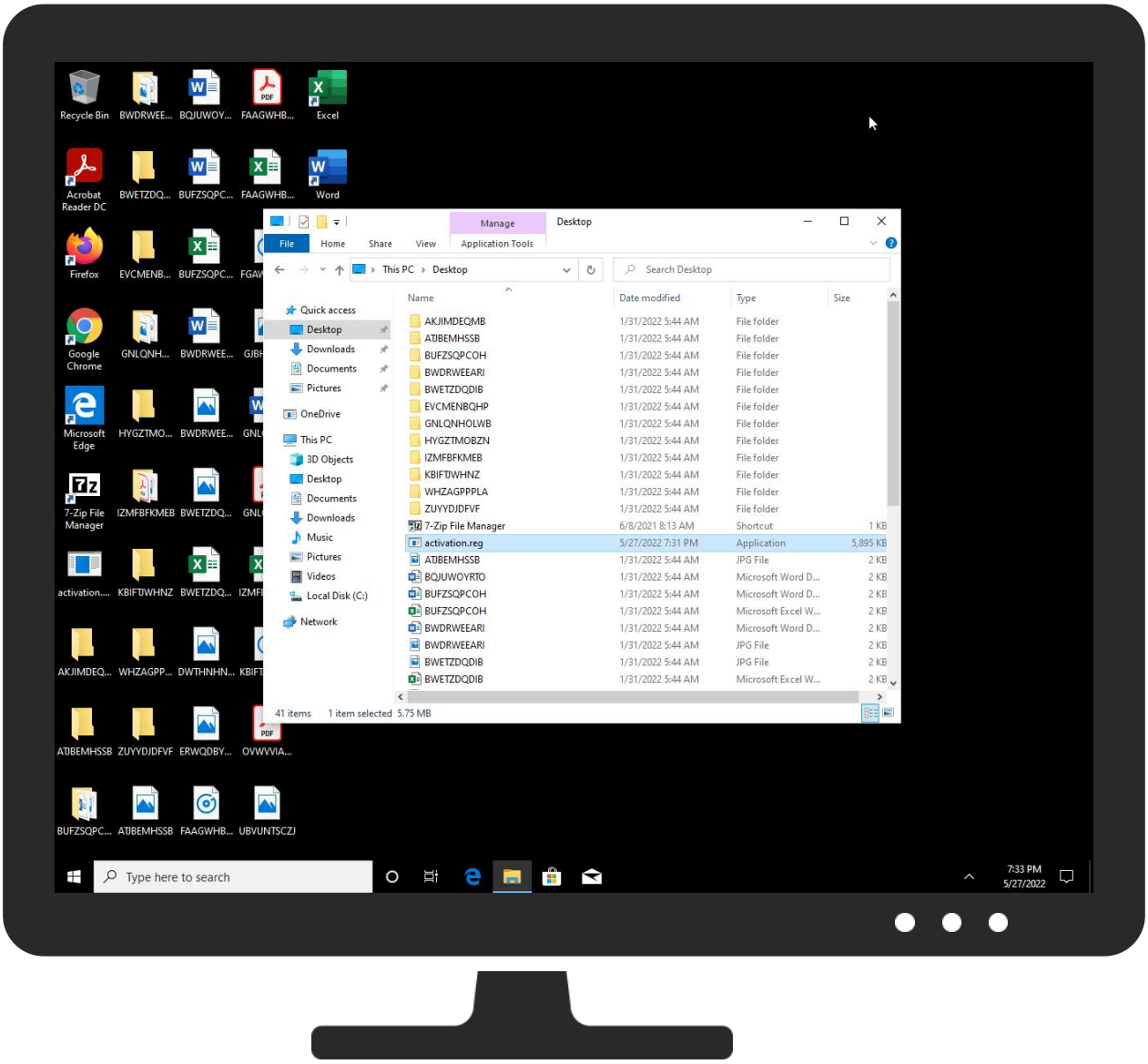
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 1 Process Injection	1 Masquerading	OS Credential Dumping	1 Virtualization/Sandbox Evasion	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Rundll32	LSASS Memory	1 System Information Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Virtualization/Sandbox Evasion	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
activation.reg.exe	9%	Virustotal		Browse
activation.reg.exe	0%	Metadefender		Browse
activation.reg.exe	9%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635341
Start date and time: 27/05/202219:30:37	2022-05-27 19:30:37 +02:00
Joe Sandbox Product:	CloudBasic
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	activation.reg.exe (renamed file extension from exe to dll)
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Number of analysed new started processes analysed:	17
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• EGA enabled
Analysis Mode:	stream
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal48.winEXE@10/1@0/0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): SIHClient.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com, login.live.com, slscr.update.microsoft.com, nexusrules.officeapps.live.com
- Not all processes where analyzed, report is missing behavior information

Created / dropped Files

C:\Windows\SysWOW64\SyncAppvPublishingServer.vbs

Process:	C:\Windows\SysWOW64\rundll32.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1504
Entropy (8bit):	4.593124153231039
Encrypted:	false
SSDEEP:	
MD5:	1036B168053FE25365402C8F4903335D
SHA1:	3439C5DDE557FC629B70009296DDC2B5821791DF
SHA-256:	7392CBE9B30701E83658892A9025F06FD1DFE2ECD1B6E5F670BD19F9034CD2F7
SHA-512:	23F14F1732462E5F166162049C530E97236131C181E91781402FC2E9F092B7B646E2C26EDF55E8BB5E3005AB9B78FD7FE9E0783A14BDA46A0000186196E85A95
Malicious:	false

Reputation:	low
Preview:	'----------..' Copyright: Microsoft Corp...'..' This script is designed to be used only for scheduled tasks(s)...' There no extensive error check, and will not dump the output from the Powershell CmdLet...'..' Usage: SyncAppvPublishingServer {cmdline-args(passthrough to cmdlet)}..'----------....Option Explicit.....Dim g_cmdArgs..g_cmdArgs = "".....' main entrance....' Enable error handling..On Error Resume Next....ParseCmdLine....if g_cmdArgs = "" Then...Wscript.echo "Command line arguments are required."...Wscript.quit 0..End If.....Dim syncCmd..syncCmd = g_cmdArgs....Dim psCmd..psCmd = "powershell.exe -Command &{" & syncCmd & "}".....Dim WshShell..Set WshShell = WScript.CreateObject("WScript.Shell")..Wsh Shell.Run psCmd, 0.....' Reset error handling..On Error Goto 0..WScript.Quit 0.....'----------

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.85636255256613
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	activation.reg.exe
File size:	6035976
MD5:	e49b92466821b19645b618b6a09a6880
SHA1:	b2bbafa02be38b07a4eb61049638ff86f0f8638b
SHA256:	90a0e059cd3f4ed0c9fac00a88ea262988b4cd6635aeb23bb7f5aab64d6aca0a
SHA512:	745af8a642385353e806eb675792f2591f0c414378709a797fcafde66894bad8fa11ffcdbb503853849646ad8b1f5bec4c2db87c42af9541da783b00498b5431
SSDEEP:	98304:mnjvqvbckqQludU/wVW3njOaInQR0yuVoQ9FQQNscWnjNOf28e24bUVO1EuMNs0:6vqvonQodSosqjQRQVnPQ+WnEfcsO1ET
TLSH:	0F5633A075D1CC7BE2BA5431606C972988EEAE300F20DADBE7545DB34D356C1BE3A853
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Dk4S%.gS%.gS%.gGN.f]%.gGN.f.%.g.P.f\%.g.P.fF%.g.P.f.%.gGN.fD%.gGN.fQ%.gGN.f^%.gS%.g.%.g.P.fQ%.g.P.fR%.g.P.gR%.gS%.gR%.g.P.fR%.

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x100098ce
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61FBE176 [Thu Feb 3 14:06:46 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	96d3c2641591e37caeb685212dac8a26

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h

Instruction
jne 00007F16DC4907E7h
call 00007F16DC490CFBh
push dword ptr [ebp+10h]
push dword ptr [ebp+0Ch]
push dword ptr [ebp+08h]
call 00007F16DC490693h
add esp, 0Ch
pop ebp
retn 000Ch
mov ecx, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], ecx
pop ecx
pop edi
pop edi
pop esi
pop ebx
mov esp, ebp
pop ebp
push ecx
ret
mov ecx, dword ptr [ebp-10h]
xor ecx, ebp
call 00007F16DC48FCF4h
jmp 00007F16DC4907C2h
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [10036054h]
xor eax, ebp
push eax
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax
ret
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [10036054h]
xor eax, ebp
push eax
mov dword ptr [ebp-10h], eax
push dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFFh
lea eax, dword ptr [ebp-0Ch]
mov dword ptr fs:[00000000h], eax
ret

Instruction
push eax
push dword ptr fs:[00000000h]
lea eax, dword ptr [esp+0Ch]
sub esp, dword ptr [esp+0Ch]
push ebx
push esi
push edi
mov dword ptr [eax], ebp
mov ebp, eax
mov eax, dword ptr [00000054h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x355c0	0x48	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x35608	0x78	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x38000	0x546210	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x57f000	0x1f00	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x33340	0x70	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x33480	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x333b0	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x27000	0x1b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x25746	0x25800	False	0.5687890625	data	6.66228685301	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x27000	0xef80	0xf000	False	0.523795572917	data	5.65398004769	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x36000	0x1fbc	0x1000	False	0.20849609375	DOS executable (block device driver)	3.17515181057	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0x546210	0x546400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x57f000	0x1f00	0x2000	False	0.756713867188	data	6.55565458928	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
BIN	0x38110	0x5453c0	data	English	United States
BIN	0x57d4d0	0x5d0	data	English	United States
BIN	0x57daa0	0x5f0	data	English	United States
RT_MANIFEST	0x57e090	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import

DLL	Import
KERNEL32.dll	GetModuleFileNameA, SizeofResource, TerminateProcess, ExpandEnvironmentStringsA, InitializeCriticalSectionEx, FindResourceA, MultiByteToWideChar, GetLastError, LockResource, CloseHandle, RaiseException, LoadResource, DecodePointer, DeleteCriticalSection, CreateProcessA, GetModuleFileNameW, CreateMutexA, ReleaseMutex, GetProcAddress, WideCharToMultiByte, CreateDirectoryA, SetEndOfFile, WriteConsoleW, CreateFileW, SetStdHandle, GetProcessHeap, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineW, GetCommandLineA, GetOEMCP, GetACP, IsValidCodePage, FindNextFileW, FindFirstFileExW, FindClose, HeapReAlloc, HeapSize, ReadConsoleW, IsDebuggerPresent, OutputDebugStringW, EnterCriticalSection, LeaveCriticalSection, EncodePointer, LocalFree, LCMapStringEx, GetStringTypeW, GetCPInfo, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetCurrentProcess, IsProcessorFeaturePresent, InitializeCriticalSectionAndSpinCount, SetEvent, ResetEvent, WaitForSingleObjectEx, CreateEventW, GetModuleHandleW, GetStartupInfoW, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, RtlUnwind, InterlockedFlushSList, SetLastError, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, FreeLibrary, LoadLibraryExW, VirtualQuery, ExitProcess, GetModuleHandleExW, LCMapStringW, GetLocaleInfoW, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, GetFileSizeEx, SetFilePointerEx, GetStdHandle, GetFileType, FlushFileBuffers, WriteFile, GetConsoleOutputCP, GetConsoleMode, HeapFree, HeapAlloc, ReadFile
USER32.dll	GetSystemMetrics
ole32.dll	CoUninitialize, CoInitializeSecurity, CoInitializeEx, CoCreateInstance
OLEAUT32.dll	VariantInit, SysFreeString, SysAllocString, VariantClear
SHLWAPI.dll	PathFileExistsA

Exports

Name	Ordinal	Address
dummy	1	0x10003a30

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States