Malware Analysis Report

VirusTotal Report:

Harmless: 0
Malicious: 63
Suspicious: 0
Undetected: 8
Timeout: 0

Strings Analysis Summary:

IP Addresses: 0
URLs: 1
Executable Keywords: 2
Hex Encoded: 0

PE Analysis:

Entry Point: 0x15cf
Image Base: 0x400000
Compilation Time: 2019-08-30 22:26:59
PE Header:
Machine: 0x14c
Number of Sections: 4
Subsystem: 0x2
DLL: False
File Size: 36864
Size of Image: 36864
Sections:

- {'Name': '.text', 'Entropy': 3.12, 'Size': 4096, 'Executable': True, 'Writable': False, 'Suspicious': False}
- {'Name': '.rdata', 'Entropy': 1.59, 'Size': 4096, 'Executable': False, 'Writable': False, 'Suspicious': False}
- {'Name': '.data', 'Entropy': 0.51, 'Size': 4096, 'Executable': False, 'Writable': True, 'Suspicious': False}
- {'Name': '.rsrc', 'Entropy': 0.71, 'Size': 20480, 'Executable': False, 'Writable': False, 'Suspicious': False}

Suspicious APIs:

- GetProcAddress
- WinExec
- CreateRemoteThread
- OpenProcess

Suspicious Sections:
Imports:

- {'KERNEL32.dll': ['GetProcAddress', 'LoadLibraryA', 'WinExec', 'WriteFile', 'CreateFileA', 'SizeofResource', 'CreateRemoteThread', 'FindResourceA', 'GetModuleHandleA', 'GetWindowsDirectoryA', 'MoveFileA', 'GetTempPathA', 'GetCurrentProcess', 'OpenProcess', 'CloseHandle', 'LoadResource']}
- {'ADVAPI32.dll': ['OpenProcessToken', 'LookupPrivilegeValueA', 'AdjustTokenPrivileges']}

- {'MSVCRT.dll': ['_snprintf', '_exit', '_XcptFilter', 'exit', '__p___initenv', '__getmainargs', '_initterm', '__setusermatherr', '_adjust_fdiv', '__p__commode', '__p__fmode', '__set_app_type', '_except_handler3', '_controlfp', '_stricmp']}

Exports:

Packer Indicators:

  detected: False
  reasons: []