

Malware Analysis Report

VirusTotal Report:

Harmless: 0

Malicious: 41

Suspicious: 0

Undetected: 31

Timeout: 0

File Metadata:

File Type: Win32 EXE

SHA256: 14c0c9bef6830d139c36c1cea8f0ef1010e49373aad52c55f167e677ce4c6bd5

MD5: 6bdc203bdfbb3fd263dadf1653d52039

SHA1: 1140fc0ed8900f8bb52e26958d1032d3f872d6ab

Reputation Score: 0

Popular Threat Label: trojan.agent5/r002c0pdm21

First Submission Date: 2012-08-02 21:03:09

Last Analysis Date: 2025-05-09 12:00:46

Total Votes: Harmless: 0, Malicious: 0

Signature Info:

Strings Analysis Summary:

IP Addresses: 0

URLs: 1

Executable Keywords: 5

Hex Encoded: 0

Base64 Strings: 8

Suspicious File Paths: 0

Registry Keys: 0

Email Addresses: 0

Embedded Powershell: 0

PE Analysis:

Entry Point: 0x1489

Image Base: 0x400000

Compilation Time: 2011-10-23 03:37:19

PE Header:

Machine: 0x14c

Number of Sections: 3

Subsystem: 0x3

DLL: False

File Size: 36864

Size of Image: 36864

Sections:

- {'Name': '.text', 'Entropy': 6.13, 'Size': 16384, 'Executable': True, 'Writable': False, 'Suspicious': False}

- {'Name': '.rdata', 'Entropy': 3.7, 'Size': 4096, 'Executable': False, 'Writable': False, 'Suspicious': False}
- {'Name': '.data', 'Entropy': 0.46, 'Size': 12288, 'Executable': False, 'Writable': True, 'Suspicious': False}

Suspicious APIs:

- TerminateProcess
- VirtualAlloc
- GetProcAddress

Suspicious Sections:

Imports:

- {'KERNEL32.dll': ['WaitForSingleObject', 'SetWaitableTimer', 'CreateWaitableTimerA', 'CreateThread', 'GetCurrentProcess', 'CreateMutexA', 'OpenMutexA', 'GetModuleFileNameA', 'SystemTimeToFileTime', 'GetShortPathNameA', 'GetStringTypeA', 'LCMapStringW', 'LCMapStringA', 'MultiByteToWideChar', 'LoadLibraryA', 'ExitProcess', 'TerminateProcess', 'GetCommandLineA', 'GetVersion', 'UnhandledExceptionFilter', 'FreeEnvironmentStringsA', 'FreeEnvironmentStringsW', 'WideCharToMultiByte', 'GetEnvironmentStrings', 'GetEnvironmentStringsW', 'SetHandleCount', 'GetStdHandle', 'GetFileType', 'GetStartupInfoA', 'GetModuleHandleA', 'GetEnvironmentVariableA', 'GetVersionExA', 'HeapDestroy', 'HeapCreate', 'VirtualFree', 'HeapFree', 'RtlUnwind', 'WriteFile', 'HeapAlloc', 'GetCPInfo', 'GetACP', 'GetOEMCP', 'VirtualAlloc', 'HeapReAlloc', 'GetProcAddress', 'GetStringTypeW']}
- {'ADVAPI32.dll': ['CreateServiceA', 'OpenSCManagerA']}
- {'SHELL32.dll': ['ShellExecuteA']}
- {'WININET.dll': ['InternetOpenUrlA', 'InternetOpenA']}

Exports:

Packer Indicators:

detected: False
reasons: []