CARBERP - Threat Encyclopedia | Trend Micro (US)

Archived: 2026-04-06 00:16:22 UTC

CARBERP is a Trojan family first seen in 2009. This banking Trojan is designed to steal user credentials through hooking network APIs in *WININET.DLL*, monitoingr user browsing activities. It has the capability to connect to its C&C server to download configuration files and receive arbitrary commands, thus compromising the security of the infected systems.

CARBERP logs keystrokes, spoofs websites, and drops copies of itself in locations that do not require administrator privileges. This malware family is characterized as a plugin-dependent malware since it relies on downloaded/embedded modules to complete its routines. Two of the known plugins it uses are the *miniav* and *stopav* modules. These modules enable CARBERP to eliminate other malware and antivirus applications running on the infected computer.

Installation

This Trojan drops the following files:

- %System Root%\{random folder name}\wndsksi.inf
- %System%\ieunitdrf.inf
- {All User's Profile\wjver.dat

(Note: *%System Root%* is the root folder, which is usually C:\. It is also where the operating system is located.. *%System%* is the Windows system folder, which is usually C:\Windows\System32.)

It drops the following copies of itself into the affected system:

- %User Startup%\igfxtray.exe
- %User Startup%\{random filename}.exe

(Note: *%User Startup%* is the current user's Startup folder, which is usually C:\Windows\Profiles\{user name}\Start Menu\Programs\Startup on Windows 98 and ME, C:\WINNT\Profiles\{user name}\Start Menu\Programs\Startup on Windows NT, and C:\Documents and Settings\{User name}\Start Menu\Programs\Startup.)

Other System Modifications

This Trojan adds the following registry entries:

HKEY_CURRENT_USER\Software\Microsoft\
Internet\Explorer\Main
TabProcGrowth = "0"

NOTES:

It drops the following folders:

- %System Root%\{random folder name}
- %User Profile%\Application Data\MicroST

It connects to any of the following C&C Servers:

- {BLOCKED}y.in
- {BLOCKED}banksystem.ru
- http://{BLOCKED}t-dbo.ru/s.dll
- {BLOCKED}aff.com
- {BLOCKED}affer.com
- {BLOCKED}affer321.com
- http://{BLOCKED}ystemdwersfssnk.com
- http://{BLOCKED}m-ibank2.com/s.dll
- http://{BLOCKED}ticgamers.com
- {BLOCKED}j894iofhweihj.com
- http://{BLOCKED}sdriverdbo.com/rt_jar
- {BLOCKED}e1.com
- {BLOCKED}it23.com
- {BLOCKED}bb.com

Source: https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/carberp