Spyware:Win32/Infoaxe

Article URL
malware.php?mal_id=269437874bf15c2c6e4b22.93293540

Author
SecurityHome.eu

Published: 17 May 2010

Aliases :

Spyware:Win32/Infoaxe

is also known as *Trojan.Win32.Pasta.knt (Kaspersky), DR/Pasta.knt (Avira), Gen:Trojan.StartPage.bmGfaOQf19lc (BitDefender), Adware.InfoAex (Dr.Web), NewHeur_PE virus (ESET), Generic.dx!rxv (McAfee), Trojan.Win32.Generic.52004DCC (Rising AV), Trojan.Win32.Generic!BT (Sunbelt Software)*

.

Explanation :

Spyware:Win32/Infoaxe is a Web Browser Help Object (BHO) that monitors a user's browsing history and stores this information, which it then uses to feed the company's search engine.
Top

Spyware:Win32/Infoaxe is a Web Browser Help Object (BHO) then monitors a user's browsing history and stores this information, which it then uses to feed the company's search engine.
InstallationSpyware:Win32/Infoaxe's installation method may vary according to the browser being used on the affected computer. Internet Explorer Spyware:Win32/Infoaxe can be installed as a Web Browser Help Object (BHO) in Internet Explorer. Spyware:Win32/Infoaxe may be present as the following files: %ProgramFiles%webhistorysearchietb.dll %ProgramFiles%webhistorysearchunins000.dat %ProgramFiles%webhistorysearchunins000.exe %ProgramFiles%webhistorysearchwebhistorysearch_update.exe Note - %ProgramFiles% refers to a variable location that is determined by the malware by querying the Operating System. The default installation location for the %ProgramFiles% folder is C:Program Files. When executed, the spyware makes the following registry modifications: Creates subkey: HKCUSoftwareInfoaxe Creates subkey: HKCUSoftwareInfoaxeInfoaxeToolbar Adds value: "HomePageChanged" With data: dword:00000001 Adds value: " SearchHookInstalled " With data: dword:00000001 To subkey: HKCUSoftwareInfoaxeInfoaxeToolbar Creates subkey: HKCUSoftwareLowRegistryInfoaxe Creates

subkey: HKCUSoftwareLowRegistryInfoaxeInfoaxeToolbar Adds value: "AutoEnabled " With data: dword:00000001 Adds value: "ExportAnswer " With data: dword:00000001 Adds value: "ExportAsked " With data: dword:00000001 Adds value: "Exported " With data: dword:00000001 Adds value: "History " Adds value: "LastUpdateTime " Adds value: "ShowedOnInstall " With data: dword:00000001 Adds value: "SplashShowed " With data: dword:00000001 Adds value: "Started " With data: dword:00000001 To subkey: HKCUSoftwareLowRegistryInfoaxeInfoaxeToolbar Creates subkey: HKCUSoftwareLowRegistryInfoaxeInfoaxeToolbarfiles Adds value: "ietb.dll" With data: dword:0000006f To subkey: HKCUSoftwareLowRegistryInfoaxeInfoaxeToolbarfiles Creates subkey: HKCUSoftwareMicrosoftInternet ExplorerSearchScopesinfoaxe_google Adds value: "DisplayName " With data: €œGoogle + Infoaxe€• Adds value: "FaviconURL " With data: http://www.infoaxe.com/favicon.ico Adds value: "URL" With data: "http://www.infoaxe.com/enhancedsearch.jsp?cx=partner-pub-6808396145675874:scfw9ganq4h&cof=FORID:10&ie=ISO-8859-1&q={searchTerms}&sa=Search&dummyRnd=29" To subkey: HKCUSoftwareMicrosoftInternet ExplorerSearchScopesinfoaxe_google Creates subkey: HKCUSoftwareMicrosoftInternet ExplorerURLSearchHooks Adds value: "{717EDDE0-444F-4ff0-B9C9-F60EC423E690}" To subkey: HKCUSoftwareMicrosoftInternet ExplorerURLSearchHooks Adds value: "InfoToolbarUpdate" With data: "<location of updater>" (for example, "C:Program Fileswebhistorysearchwebhistorysearch_update.exe") To subkey: HKCUSoftwareMicrosoftWindowsCurrentVersionRun Note: <location of updater> is defined as the full path of the file that updates the program on the user's machine. Creates subkey: HKLMSOFTWAREClassesCLSID{2F8D500E-4546-45b7-9236-D4FD9850CF1C} Adds value: "(Default)" With data: "infoaxe.com Toolbar" To subkey: HKLMSOFTWAREClassesCLSID{2F8D500E-4546-45b7-9236-D4FD9850CF1C} Creates subkey: HKLMSOFTWAREClassesCLSID{2F8D500E-4546-45b7-9236-D4FD9850CF1C}InProcServer32 Adds value: "(Default)" With data: <location of toolbar> For example, "C:Program Fileswebhistorysearchietb.dll" To subkey: HKLMSOFTWAREClassesCLSID{2F8D500E-4546-45b7-9236-D4FD9850CF1C}InProcServer32 Note: <location of toolbar> is defined as the full path of the file that is the toolbar on the user's machine. Creates subkey: HKLMSOFTWAREClassesCLSID{717EDDE0-444F-4ff0-B9C9-F60EC423E690} Adds value: "(Default)" With data: "infoaxe.com Toolbar" To subkey: HKLMSOFTWAREClassesCLSID{717EDDE0-444F-4ff0-B9C9-F60EC423E690} Creates subkey: HKLMSOFTWAREClassesCLSID{717EDDE0-444F-4ff0-B9C9-F60EC423E690}InProcServer32 Adds value: "(Default)" With data: <location of toolbar> For example, "C:Program Fileswebhistorysearchietb.dll" To subkey: HKLMSOFTWAREClassesCLSID{717EDDE0-444F-4ff0-B9C9-F60EC423E690}InProcServer32 Note: <location of toolbar> is defined as the full path of the file that is the toolbar on the user's machine. Creates subkey: HKLMSOFTWAREMicrosoftInternet ExplorerToolbar Adds value: "{717EDDE0-444F-4ff0-B9C9-F60EC423E690}" With data: "infoaxe.com Toolbar" To subkey: HKLMSOFTWAREMicrosoftInternet ExplorerToolbar Creates subkey: HKLMSOFTWAREMicrosoftWindowsCurrentVersionExplorerBrowser Helper Objects{2F8D500E-4546-45b7-9236-D4FD9850CF1C} Adds value: "(Default)" With data: "infoaxe.com Toolbar" To subkey: HKLMSOFTWAREMicrosoftWindowsCurrentVersionExplorerBrowser Helper Objects{2F8D500E-4546-45b7-9236-D4FD9850CF1C} Creates subkey: HKLMSOFTWAREMicrosoftWindowsCurrentVersionUninstallWeb History Search Toolbar_is1 Adds value: "DisplayName" With data: "Web History Search Toolbar" Adds value: "Inno Setup: App Path" With data: <directory of installation> (for example, "C:Program Fileswebhistorysearch") Adds value: "Inno Setup: Icon Group" With data: "Web History Search Toolbar" Adds value: "Inno Setup: Setup Version" With data: "5.2.3" Adds value: "Inno Setup: User" With data: "Administrator" Adds value: "InstallDate" With data:

"20100511" Adds value: "InstallLocation" With data: <directory of installation> (for example, "C:Program Fileswebhistorysearch") Adds value: "NoModify" With data: dword:00000001 Adds value: "NoRepair" With data: dword:00000001 Adds value: "Publisher" With data: "Infoaxe.com" Adds value: "QuietUninstallString" With data: ""C:Program Fileswebhistorysearchunins000.exe" /SILENT" Adds value: "UninstallString" With data: ""C:Program Fileswebhistorysearchunins000.exe"" To subkey: HKLMSOFTWAREMicrosoftWindowsCurrentVersionUninstallWeb History Search Toolbar_is1 Note: <directory of installation> is defined as the full path to the folder where the files are located. Adds value: €œStart Page€• With data: €œhttp://www.infoaxe.com/enhancedsearchform.jsp€• To subkey: HKCUSoftwareMicrosoftInternet ExplorerMain Once the spyware has been installed, it can been seen in the 'Add or Remove Programs' window that can be accessed from the Control Panel. The image below displays an 'Add or Remove Programs' window with the adware listed as the name "Web History Search Toolbar". Once installed in Internet Explorer, the spyware's presence can be seen in the 'Manage Add-ons' window that can be accessed from the Tools menu. The image below displays a 'Manage Add-ons' window with the spyware listed as a Toolbar and BHO. Once the spyware has been installed, it adds a toolbar to the Internet Explorer Web browser window. Once the spyware has been installed, it changes the user's homepage to a site that resembles Google in that it displays the Google brand; however the site is hosted by the spyware's company. Mozilla Firefox Spyware:Win32/Infoaxe can install itself as an extension in Mozilla Firefox. It may create the following directories: %AppData%MozillaFirefoxProfiles<mozilla profile>extensions{3EB3C1FE-4FED-4ef7-A78C-6616E2521FB5} %AppData%MozillaFirefoxProfiles<mozilla profile>searchplugins Note - %AppData% refers to a variable location that is determined by the malware by querying the Operating System. The default installation location for the %Appdata% folder for Windows XP is C:Documents and Settings<user>Application Data; and for Vista, and Windows 7 is C:Users<user>AppDataRoaming. Note - <mozilla profile> is defined as a value given to the user by Mozilla products and varies from user to user. A user may have more than one profile on a machine. Spyware:Win32/Infoaxe then creates the following files beneath the above listed directories: chrome.manifest install.rdf infoaxetb.jar infoaxe.gif infoaxe.ico infoaxe.png infoaxe.src infoaxe.xml Once installed in Mozilla Firefox, the adware's presence can be seen in the 'Manage Add-ons' window that can be accessed from the Tools menu. The image below displays a 'Manage Add-ons' window with the adware listed as 'Infoaxe Web History Search Engine'. Once the spyware has been installed, it adds a toolbar to the Mozilla Firefox Web browser window. Additional information Defaults to spyware's search engine / Hijacks search results Spyware:Win32/Infoaxe stores the user's browser history in an Online location, then uses this information to influence future search results. The images below displays search results from an affected user's Web browser. Displays pop-upsSpyware:Win32/Infoaxe displays pop-ups that do not give the affected user an option to cancel out.

Analysis by Michael Johnson

Last update 17 May 2010