Автор: Administrator
26.02.2019 18:55

{jcomments on}

Специалисты Quihoo 360 заметили первую вредоносную кампанию, использующую для внедрения вредоносного ПО на компьютеры пользователей.

Специалисты обнаружили электронную рассылку, распространяющую RAR архив, который при распаковке устанавливает на компьютер инструмент Cobalt Strike Beacon, применяемый злоумышленниками для получения удаленного доступа к компьютеру.

Как показал анализ, проведенный экспертами ресурса BleepingComputer, при распаковке вредоносный архив извлекает файлы в папку автозагрузки Windows. Если на устройстве включена функция контроля учетных записей пользователей (User Account Control, UAC), WinRAR отобразит сообщение об ошибке, однако в случае, если UAC отключен или архиватор работает с правами администратора, вредоносные файлы будут извлечены в C:ProgramDataMicrosoftWindowsStart MenuProgramsStartupCMSTray.exe и при следующей загрузке системы выполнится исполняемый файл CMSTray.exe.

При запуске CMSTray.exe копируется в папку %Temp%wbssrv.exe, а затем выполняется файл wbssrv.exe. Последний подключается к серверу и загружает различные файлы, в том числе инструмент Cobalt Strike Beacon. После загрузки вредоносной DLL атакующие получат возможность удаленно подключаться к компьютеру, выполнять команды и инфицировать другие компьютеры в сети.

Подробнее: https://www.securitylab.ru/news/498108.php

(function(w, d, n) { w[n] = w[n] || []; w[n].push({ section_id: 263974, place: "advertur_263974", width: 300, height: 250 }); })(window, document, "advertur_sections");