Автор: Administrator
24.06.2016 19:11

Специалистами компании "Доктор Вэб" обнаружен потенциально опасный вредонос **1С.Drop.1**
, который самостоятельно распространяется по электронной почте среди зарегистрированных в базе контрагентов, заражает компьютеры с установленными бухгалтерскими приложениями 1С и запускает на них опасного троянца-шифровальщика.

1С.Drop.1 распространяется в виде вложения в сообщения электронной почты с темой «
У нас сменился БИК банка
» и следующим текстом:

Здравствуйте!

У нас сменился БИК банка.

Просим обновить свой классификатор банков.

Это можно сделать в автоматическом режиме, если Вы используете 1С Предприятие 8.

Файл - Открыть обработку обновления классификаторов из вложения.

Нажать ДА. Классификатор обновится в автоматическом режиме.

При включенном интернете за 1-2 минуты.

К письму прикреплен файл внешней обработки для программы «1С:Предприятие» с

именем *ПроверкаАктуальностиКлассификатораБанков.epf*.

1C.Drop.1 поддерживает работу с базами следующих конфигураций 1С:

- "Управление торговлей, редакция 11.1"
- "Управление торговлей (базовая), редакция 11.1"
- "Управление торговлей, редакция 11.2"
- "Управление торговлей (базовая), редакция 11.2"
- "Бухгалтерия предприятия, редакция 3.0"
- "Бухгалтерия предприятия (базовая), редакция 3.0"
- "1С:Комплексная автоматизация 2.0"

При запуске вредоноса начинается массовая рассылка по e-mail копии троянца по адресам контрагентом. После этого, осуществляется шифрование данных на жестком диске зараженного компьютера.

Проявляйте особую бдительность и не открывайте полученные по электронной почте файлы в приложении «1С:Предприятие».

Источник: news.drweb.ua/

(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");