Автор: Administrator
25.05.2015 11:49

{jcomments on}

Злоумышленники используют SVG-файлы для распространения вымогательского ПО

Исследователи ИБ-компании AppRiver зафиксировали кампанию, в ходе которой злоумышленники пытались распространять вымогательское ПО при помощи файлов SVG.

Как пояснили специалисты, преступники рассылали электронные письма, к которым было прикреплено фальшивое резюме. Приложение к письму представляло собой ZIP-архив, содержавший файл с расширением SVG. Он включал небольшой код JavaScript, который злоумышленники использовали для перенаправления жертв на вредоносную страницу, распространявшую вымогательское ПО.

Код JavaScript, проанализированный специалистами, содержал IP-адрес, перенаправлявший пользователей на ресурс, содержащий CryptoWall – один из наиболее популярных представителей семейства вымогателей. Вредонос инфицирует компьютер жертвы и шифрует важные файлы, требуя затем выкуп за их дешифрование.

CryptoWall уже не раз доказывал свою эффективность тем, что пользователи в большинстве случаев действительно платят требуемую сумму, отмечают эксперты. Данная практика до сих пор существует и, скорее всего, продолжит развиваться дальше. Исследователи AppRiver рекомендуют пользователям делать резервные копии

важных файлов и сохранять там, где вредоносы не смогут до них добраться.

Источник: www.securitylab.ru