Автор: Administrator
27.03.2016 13:32

{jcomments on}

Исследователи G DATA обнаружили новое вымогательское ПО, получившее название Petya. В отличие от существующих в настоящее время троянов Locky, CryptoWall, TeslaCrypt и пр., шифрующих отдельные файлы, Petya полностью шифрует жесткий диск инфицированного компьютера.

По словам экспертов, вредоносное ПО разработано специально для атак на предприятия. Petya распространяется с помощью фишинговых электронных писем, адресованных кадровым отделам компаний. Письма приходят якобы от соискателей и содержат резюме и ссылку на Dropbox, откуда можно загрузить «портфолио».

После нажатия на ссылку загружается EXE-файл, а при попытке его запуска система аварийно завершает работу, появляется синий экран и перезагружается компьютер. До перезагрузки Petya изменяет главную загрузочную запись, тем самым получая контроль над процессом перезагрузки.

После возобновления работы системы открывается диалоговое окно, якобы отображающее проверку ее работы, однако на самом деле с этого момента ПК становится недоступным для пользователя. По мнению экспертов, Petya не шифрует сами файлы, а только блокирует к ним доступ.

Когда «проверка системы» завершается, на экране появляется изображение черепа и

требование нажать на любую клавишу. После нажатия открывается инструкция по покупке ключа для разблокировки компьютера.

Источник: h www.securitylab.ru