Название

Шифровальщик

Дата рождения

1989

Происхождение

США

Описание

Этот тип кибер-преступности шифрует файлы на компьютере и держит их заблокированными, пока жертва не заплатит выкуп, как правило, в биткоинах, чтобы нельзя было отследить платеж.

Не доверяйте шифровальщикам и никогда не платите выкуп, потому что нет никаких гарантий, что вы получите доступ к своим файлам.

Арест

Данная угроза уже арестована и нейтрализована Panda Security.

Но если Вы не используете антивирус Panda или Ваш уровень защиты требует улучшения, Вам необходимо обратить внимание на решения безопасности Panda для дома или офиса.

Решения безопасности Panda

Криминальное прошлое

Wannacry

12 мая 2017 года шифровальщик с функционалом сетевого червя поразил некоторые системы Microsoft Windows с помощью старой известной уязвимости. Таким образом, он сумел зашифровать все файлы на зараженных ПК и на ПК в тех же локальных сетях с имеющейся уязвимостью Windows.

Процесс закончился запросом выкупа за расшифровку файлов. Преступники требовали 300 долларов в биткоинах за каждый компьютер, где были зашифрованы файлы.

WannaCry был описан как беспрецедентная угроза с точки зрения своего масштаба, заразив свыше 230 000 компьютеров в более чем 150 странах. Общий ущерб составил более 5 миллиардов долларов США.

GoldenEye/Petya

27 июня 2017 года мир потрясла новая атака, парализовавшая крупные компании во многих странах. Эта крупномасштабная атака была выполнена с помощью нового варианта шифровальщика из семейства GoldenEye. Копия страшного WannaCry.

Petya запускался на компьютерах, шифровал определенные файлы и блокировал доступ к загрузочной области пораженного компьютера. Таким образом, он не позволял пользователю получить доступ к своему компьютеру, пока он не ввел ключ доступа, полученный после оплаты выкупа.

Новое по сравнению с WannaCry: кибер-атака могла выключать компьютер или создавать задачу на его выключение в определенное время.