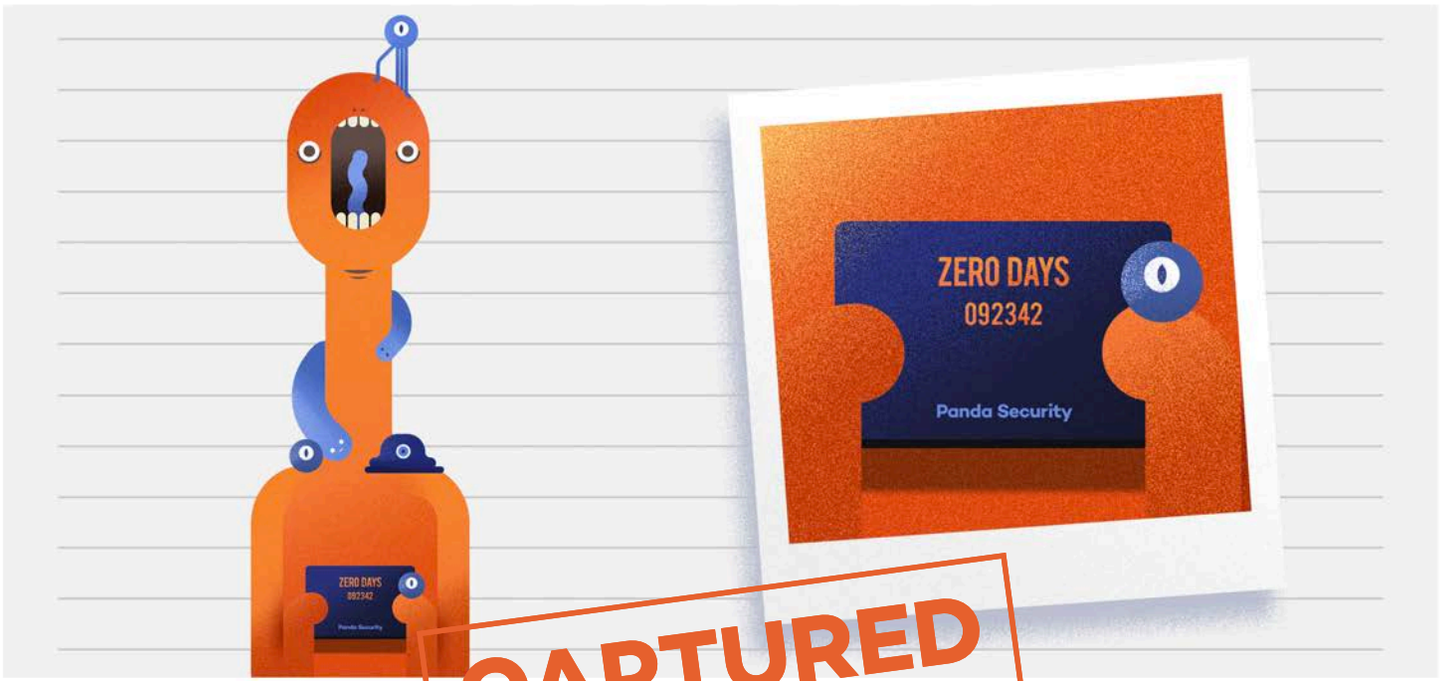

Название

Атака "нулевого дня" (Zero days)

Дата рождения

2010

Происхождение

Неизвестно

Описание

"Атака нулевого дня" дается любой атаке, которая запускается с использованием недавно обнаруженной уязвимости, которая пока не закрыта. Другими словами, это быстрая атака, которая запускается хакерами до того, как соответствующий производитель ПО еще не устранил уязвимость и не выпустил обновление (или даже пока не знает о данной уязвимости).

Такие атаки очень часто используются кибер-преступниками для подрыва работы критических систем других стран или компаний, которые их разработали.

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

Stuxnet

Червь, поразивший компьютеры с Windows. Обнаружен в июне 2010 года. Стал первым известным червем, который шпионил и перепрограммировал промышленные системы.

Цель червя - ядерная инфраструктура Ирана, где использовались системы контроля Siemens. Ряд СМИ приписывают атаку спецслужбам США и Израиля.

Атака на Sony Pictures

В 2014 году Sony Pictures пережила одну из самых ужасных атак в своей истории. Группа хакеров под названием "Стражи мира" (Guardians of Peace) использовала атаку "нулевого дня" для поражения корпоративной сети Sony, откуда в течение нескольких недель осуществляли кражу конфиденциальной информации.

Среди украденных данных оказались персональные данные сотрудников и членов их семей, конфиденциальные письма, информация о доходах руководителей компании, зарплаты сотрудников, копии не выпущенных фильмов. Большая часть украденной информации была опубликована в Интернете.

Демократический национальный комитет

Благодаря шести уязвимостям в Microsoft Windows 10, Adobe Flash и Java, в 2016 году якобы русские хакеры при поддержке спецслужб сумели проникнуть в систему Демократического национального комитета (орган управления Демократической партии США).

Чтобы использовать эти уязвимости, различным членам Комитета и ряду других политических фигур были отправлены фишинговые письма с целью кражи их паролей.

Полученные данные были преимущественно опубликованы в WikiLeaks.