Название

APT (Advanced Persistent Threats)

Дата рождения

1989

Происхождение

Москва (СССР, Россия)

Описание

Это набор скрытых, сложных и непрерывных процессов взлома компьютера под управлением организованных групп кибер-преступников. Как правило, ориентированы на гос. учреждения и крупные компании.

Они используют комплексные техники проникновения в ИТ-системы (включая уязвимости и бэкдоры в операционных системах).

APT характерны тем, что стараются оставаться незаметными как можно дольше. Ищут ценную информацию, которую потом можно будет быстро продать: конфиденциальные и персональные данные и т.д.

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

GhostNet

Крупномасштабная атака, обнаруженная в марте 2009 года. Проведена, скорее всего, из Китая.

GhostNet проник на компьютеры в более чем 100 странах мира.

Операция "Аврора"

Серия кибер-атак была запущена в 2009 году из Китая. Использовался эксплойт "нулевого дня" для установки трояна с целью кражи информации.

В 2010 году Google сообщил об этих атаках, заявив, что были атакованы и другие компании.

Среди них оказались ведущие банки, оборонные предприятия, поставщики услуг безопасности, нефтяные и газовые компании, другие ИТ-компании.

Stuxnet

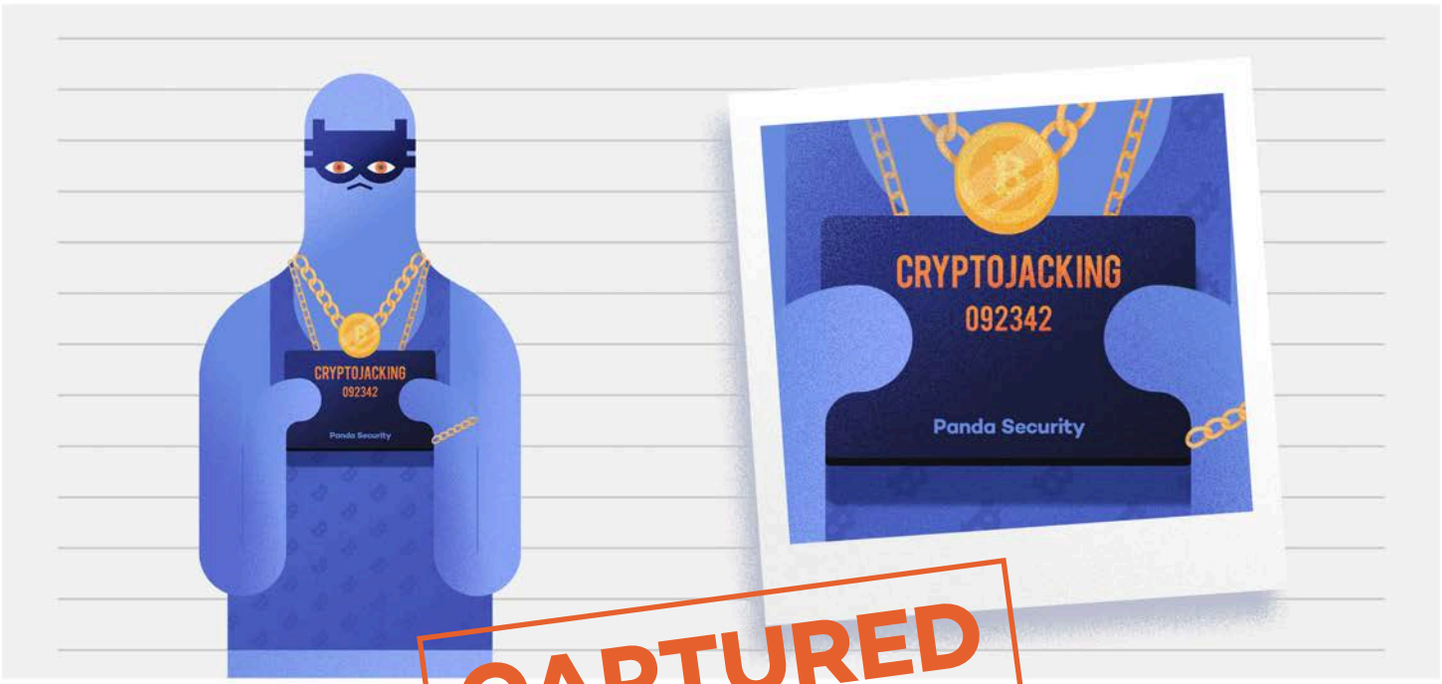
Червь, поразивший компьютеры с Windows. Обнаружен в июне 2010 года. Стал первым известным червем, который шпионил и перепрограммировал промышленные системы.

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

Красный октябрь

В октябре 2012 года была обнаружена вредоносная программа для кражи конфиденциальной информации из правительственных органов и исследовательских организаций.

Считается, что она действовала во всем мире минимум 5 лет до обнаружения, осуществляя кражу конфиденциальной информации из дипломатических, коммерческих, военных, авиационных и исследовательских организаций в России, США, Иране и еще не менее 36 стран.



Название

Криптоджекинг

Дата рождения

2011

Происхождение

Подсказки указывают на Россию

Описание

Криптоджекинг использует чужие устройства без разрешения для незаконной добычи криптовалюты.

Преступники используют вредоносные программы для захвата компьютеров, планшетов или смартфонов, и используют их мощности для тайной добычи (майнинга) криптовалют, потребляя электроэнергию жертв.

Большинство атак криптоджекинга используют код CoinHive для майнинга криптовалют.

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

Smominru

В начале 2018 года была обнаружен Smominru - зловред для майнинга Monero. Заразил более полумиллиона компьютеров с мая 2017 года, в основном, в России, Индии и Тайване. По оценкам, кибер-преступники сумели заработать до 3,6 млн. долларов США.

Adylkuzz и Wannamine

Одна из самых проблематичных уязвимостей в 2018 году, - это EternalBlue, которая также использовалась для WannaCry. С ее помощью на компьютеры проникал и Adylkuzz. Этот зловред использовался для майнинга Monero, заразив сотни тысяч компьютеров во всем мире. Считается, что он поразил даже больше ПК, чем известный WannaCry.

Атака на DoubleClick

К концу января 2018 г. YouTube узнал, что был заражен, когда было обнаружено, что внутри его рекламных объявлений был скрыт вредоносный код, подвергающий риску многих пользователей. В этом случае жертвой атаки стала рекламная платформа DoubleClick, где был спрятан код CoinHive для криптоджекинга через рекламу на YouTube.

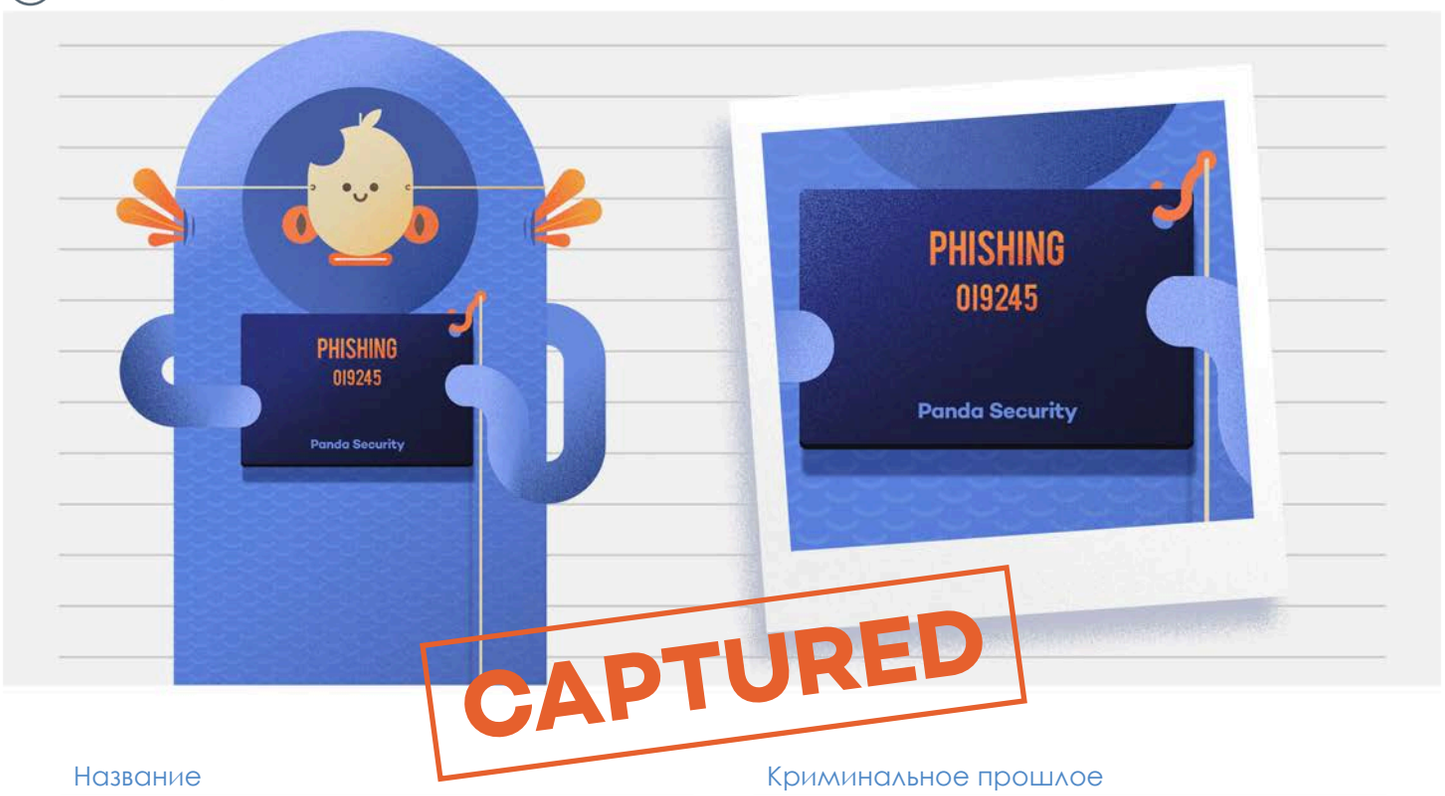
WinstarNssmMiner

В мае 2018 года другая очень опасная угроза под названием WinstarNssmMiner заразила полмиллиона ПК за три дня. Эта вредоносная программа использовала фишинговые письма и зараженные сайты. Попав в систему, использовала все ресурсы ПК для майнинга.

HiddenMiner

Обнаруженный в марте 2018 года, HiddenMiner сумел пробиться в мобильные устройства через приложения, загруженные со сторонних сайтов (не через официальные магазины приложений).

Он был еще опасен потому, что в старых версиях Android от него невозможно было избавиться. Оказавшись внутри, он использовал все ресурсы устройства, которое перегревалось и ломалось.



Название

Фишинг

Дата рождения

1995

Происхождение

Подсказки указывают на США

Описание

Одна из самых известных афер 90-х годов, и в наши дни остается одной из техник, которая часто используется кибер-преступниками. Свыше 90% вредоносных программ в мире передаются по электронной почте.

Фишинг заключается в отправке электронных писем, которые отправляются якобы из надежных источников (например, банк пользователя), чтобы пытаются обмануть пользователя и получить его конфиденциальные данные для дальнейших преступлений (мошенничества).

Проявление и тактика различны, но цель всегда одна: получить данные с помощью обманных сообщений, чтобы затем получить доступ к персональным или корпоративным счетам пользователя.

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

Операция Phish Phry

В 2009 году банки США подверглись фишинговой атаке Phish Phry, от которой пострадало свыше 500 человек, потерявшие свыше 1,5 млн. долларов. Более 100 человек в США и Египте были ответственны за эту операцию.

Среди банков пострадали Bank of America и Wells Fargo. На сегодняшний день это самая крупная международная фишинговая кампания.

Атака на RSA

В марте 2011 года RSA сообщила о том, что была атакована в рамках фишинговой кампании. Для атаки использовалась незакрытая уязвимость в Adobe Flash. Письмо сообщало, что отправитель якобы отправлял некий файл для ознакомления с просьбой открыть его и просмотреть. В письме был вложен файл "2011 Recruitment plan".

Фишинговая афера Dyre

В октябре 2014 года фишинговая кампания Dyre заразила свыше 20 000 пользователей и смогла украсть свыше миллиона долларов. В большинстве отправленных писем сообщалось, что оно отправлено от налогового инспектора. Цель письма - обмануть пользователя, чтобы он установил вредоносную программу.

Фишинг на Snapchat

В июле 2018 года фишинговая атака позволила заполучить регистрационные данные у 50 000 пользователей Snapchat. На фишинговом сайте klkviral.org был опубликован список с данными о 55 851 аккаунте Snapchat вместе с их логинами и паролями.

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.

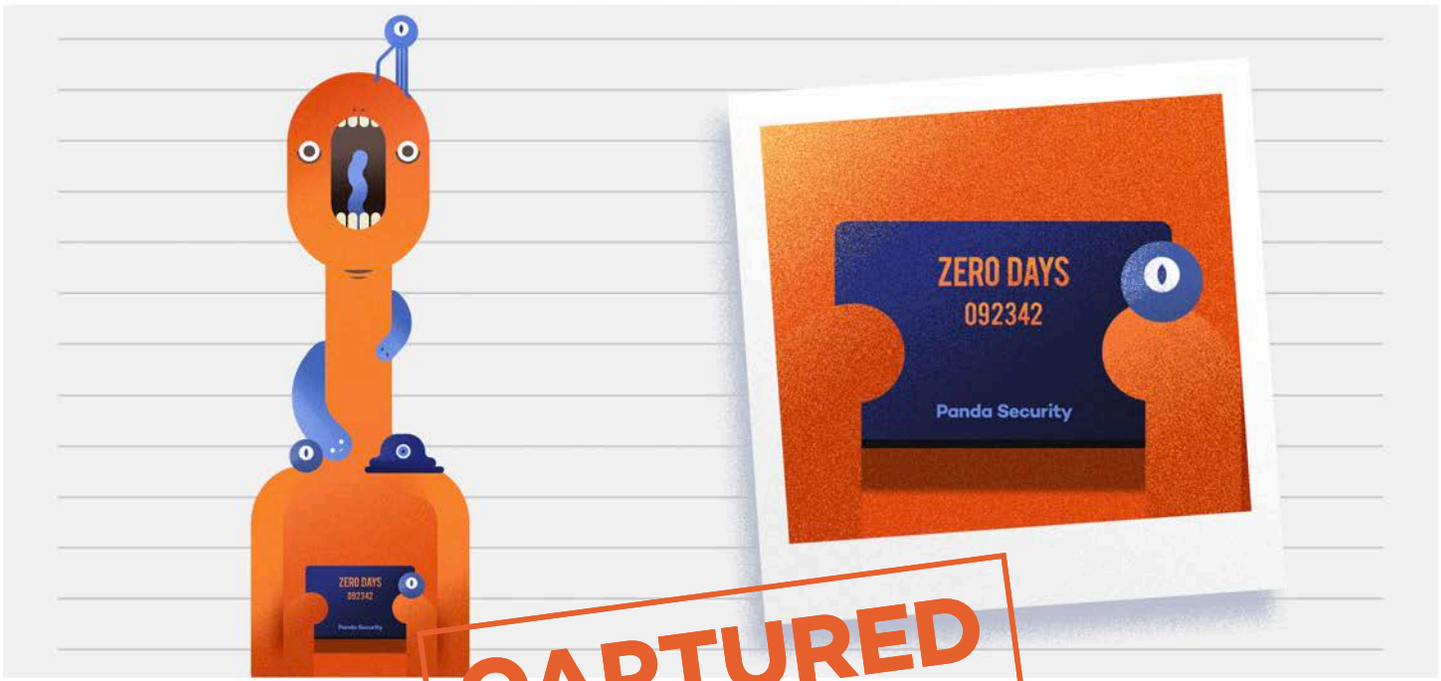
WannaCry был описан как беспрецедентная угроза с точки зрения своего масштаба, заразив свыше 230 000 компьютеров в более чем 150 странах. Общий ущерб составил более 5 миллиардов долларов США.

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.



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.