

Кибербезопасность

Уголовная ответственность за совершение киберпреступлений (преступлений в сфере компьютерной информации - Глава 28 Уголовного кодекса Российской Федерации)

Статья 272. Неправомерный доступ к компьютерной информации

(в ред. Федерального **закона** от 07.12.2011 N 420-ФЗ)

1. **Неправомерный доступ** к охраняемой законом компьютерной информации, если это деяние повлекло **уничтожение, блокирование, модификацию** либо **копировани**
е компьютерной информации, -

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, -

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.

(в ред. Федерального **закона** от 28.06.2014 N 195-ФЗ)

3. Деяния, предусмотренные **частями первой** или **второй** настоящей статьи, совершенные группой лиц по предварительному сговору или

организованной группой либо лицом с использованием своего **служебного положения**, -

наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные **частями первой, второй** или **третьей** настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, -

наказываются лишением свободы на срок до семи лет.

Примечания. 1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

2. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

Статья 273. Создание, использование и распространение вредоносных компьютерных программ

(в ред. Федерального **закона** от 07.12.2011 N 420-ФЗ)

1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, -

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением

свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Деяния, предусмотренные **частью первой** настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие **крупный ущерб** или совершенные из корыстной заинтересованности, -

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные **частями первой** или **второй** настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, -

наказываются лишением свободы на срок до семи лет.

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

(в ред. Федерального **закона** от 07.12.2011 N 420-ФЗ)

1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и окончного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение,

блокирование, модификацию либо копирование **компьютерной информации**, причинившее **крупный ущерб**, -

наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. Деяние, предусмотренное **частью первой** настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления, -

наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок.

Определение хакеров Черные шляпы

Хакеры Черные шляпы – это преступники, злонамеренно взламывающие компьютерные сети. Они также создают вредоносные программы, которые уничтожают файлы, блокируют компьютеры, крадут пароли, номера кредитных карт и другую личную информацию.

Черные шляпы мотивированы корыстными целями: финансовая выгода, месть или просто сеяние хаоса. Иногда

их мотивация может быть идеологической – их атаки нацелены на людей, с которыми они категорически не согласны.

Кто такие Черные шляпы?

Черные шляпы часто начинают как дилетанты, используя приобретенные хакерские инструменты для эксплуатации недостатков систем безопасности. Некоторых обучают взломам их начальники, стремящиеся быстро заработать деньги. Ведущие Черные шляпы – это, как правило, опытные хакеры, работающие на крупные преступные организации, которые иногда предоставляют своим сотрудникам инструменты для совместной работы, а также предлагают клиентам соглашения об обслуживании, как и законные предприятия. Наборы вредоносных программ, разработанных Черными шляпами, продаются в даркнете, и иногда даже включают гарантийное и клиентское обслуживание.

Хакеры Черные шляпы часто развиваются в определенных направлениях, таких как фишинг или управление инструментами удаленного доступа. Многие получают заказы на форумах или через связи в даркнете. Некоторые сами разрабатывают и продают вредоносные программы, другие предпочитают работать по франшизе или лизингу – все так же, как и в легальном деловом мире.

Хакерство стало неотъемлемым инструментом сбора разведданных для правительств, но Черные шляпы чаще работают в одиночку или с организованными преступными структурами за легкие деньги.

Как работают Черные шляпы

Хакерство может действовать как крупный бизнес, масштабы которого позволяют легко распространять вредоносные программы. У организаций есть партнеры, торговые посредники, поставщики и совладельцы, которые покупают и

продают лицензии на вредоносное ПО другим преступным организациям для использования в новых регионах и на новых рынках.

У некоторых хакерских организаций даже есть колл-центры, которые они используют для исходящих звонков, выдавая себя за сотрудников известных технологических компаний, например, Microsoft. При таком виде мошенничества потенциальных жертв пытаются убедить предоставить удаленный доступ к компьютерам или загрузить программное обеспечение. Предоставляя доступ или загружая рекомендованное программное обеспечение, жертва непреднамеренно позволяет преступникам получить пароли и банковскую информацию или захватить компьютер и использовать его для атак на других пользователей. Кроме того, за эту «помощь» с жертвы обычно взимают неоправданно высокую плату, что еще усугубляет ситуацию.

Другой тип взлома – быстрый и автоматизированными, не требующий контакта с людьми. В этих случаях атакующие боты выполняют поиск незащищенных компьютеров в интернете и проникают на них, часто с использованием фишинга, вредоносных вложений или ссылок на взломанные веб-сайты.

Взломы, осуществляемые Черными шляпами – это глобальная проблема, которую крайне сложно решить. Работа правоохранительных органов осложняется тем, что хакеры оставляют мало улик, используют компьютеры ничего не подозревающих жертв и действуют в нескольких юрисдикциях. Иногда властям удается закрыть хакерский сайт в одной стране, однако эти же действия могут выполняться в другом месте, что позволяет преступной группе продолжать работу.

Примеры хакеров Черные шляпы

Одним из самых известных хакеров Черная шляпа является Кевин Митник, который в свое время был самым разыскиваемым киберпреступником в мире. Он взломал более 40 крупных корпораций, включая IBM и Motorola, и даже систему предупреждения Министерства гражданской обороны США. Впоследствии он был арестован и отбывал срок в тюрьме. После освобождения он стал консультантом по кибербезопасности и использует свои знания как эксперт, помогающий улучшить защиту систем.

Другой известный пример – Цутому Шимомура, эксперт по кибербезопасности, которому приписывают отслеживание Кевина Митника. Шимомура, исследователь в области вычислительной физики, также работал в Агентстве национальной безопасности США. Он был одним из ведущих исследователей, первым поднявшим вопрос о незащищенности и отсутствии конфиденциальности сотовых телефонов. Основатель Neofocal Systems использовал свой опыт в области безопасности в этических целях и сыграл решающую роль в привлечении Кевина Митника к ответственности. Его книга «Взлом» (Takedown) позже была использована в качестве сценария к фильму *Взлом* (Track Down).

Определение хакеров Белые шляпы

Хакеры Белые шляпы, которых также называют этичными или хорошими хакерами – полная противоположность Черным шляпам. Они выявляют недостатки безопасности компьютерных систем и сетей и дают рекомендации по улучшению.

Кто такие Белые шляпы?

Белые шляпы используют свои знания и опыт для обнаружения недостатков в системе безопасности, чтобы защитить организации от опасных хакерских атак. Иногда они могут быть штатными сотрудниками или подрядчиками,

работающими в компании на должности специалистов по безопасности, задача которых – поиск недостатков систем безопасности.

Работа Белых шляп – одна из причин, почему в крупных организациях обычно меньше простоев и проблем с веб-сайтами. Большинство хакеров знают, что проникнуть в системы, управляемые крупными компаниями, труднее, чем в управляемые малыми предприятиями, у которых, вероятно, нет ресурсов для изучения возможных уязвимостей систем безопасности.

Группа этичных хакеров включает тестировщиков на проникновение, которые специализируются на обнаружении уязвимостей и оценке рисков в системах.

Как работают Белые шляпы

Белые шляпы используют те же методы взлома, что и Черные шляпы, но главное отличие состоит в том, что они сначала получают разрешение владельца системы, что делает процесс полностью законным. Вместо того чтобы использовать уязвимости для распространения кода, Белые шляпы работают с операторами сетей и пытаются решить проблему до того, как ее обнаружат злоумышленники.

Белые шляпы используют следующие приемы и навыки:

1. Социальная инженерия

Белые шляпы обычно используют социальную инженерию («взлом людей») для обнаружения слабых мест в человеческом аспекте защиты организации. Социальная инженерия – это обман и манипуляции, заставляющие жертв делать то, чего они не должны (совершать электронные переводы средств, раскрывать учетные данные и прочее).

2. Тестирование на проникновение

Тестирование на проникновение направлено на выявление уязвимостей и слабых мест в защите организации и ее конечных точек, с последующим устранением уязвимостей.

3. Разведка и исследования

На этом этапе выполняется исследование организации с целью обнаружения уязвимостей в физической и ИТ-инфраструктуре. Задача – получить достаточно информации для выявления способов законного обхода средств и механизмов безопасности без повреждения или взлома чего-либо.

4. Программирование

Белые шляпы создают приманки для привлечения киберпреступников, чтобы сбить их с толку или получить о них ценную информацию.

5. Использование разнообразных цифровых и физических инструментов

Такие инструменты включают оборудование и устройства, позволяющие тестировщикам на проникновение устанавливать боты и другие вредоносные программы и получать доступ к сети и серверам.

Для некоторых этот процесс превращается в игру Баг баунти – соревнования, в ходе которых хакеры награждаются денежными призами за сообщения об обнаруженных уязвимостях. Есть даже учебные курсы, мероприятия и сертификаты, посвященные этичному хакингу.

Черные шляпы против Белых шляп

Основное различие между ними – мотивация. В отличие от Черных шляп, которые получают доступ к системам незаконно, со злыми намерениями и часто с целью личного обогащения, Белые шляпы сотрудничают с компаниями и

помогают им выявлять слабые места в их системах и исправлять соответствующие уязвимости, чтобы гарантировать, что злоумышленники не смогут незаконно получить доступ к данным системы.



Примеры хакеров Белые шляпы

Вот некоторые из самых известных примеров хакеров Белые шляпы:

Тим Бернерс-Ли

Тим Бернерс-Ли, создатель Всемирной паутины, является членом лагеря хакеров Белые шляпы. Сегодня он является директором Консорциума World Wide Web (W3C), который курирует развитие Интернета.

Грег Хогланд

Грег Хогланд – эксперт в области компьютерной криминалистики, наиболее известный своим вкладом в работу и исследования в области обнаружения вредоносных

программ, руткитов и взлома онлайн-игр. Ранее он работал на правительство США и разведку.

Ричард М. Столлман

Ричард М. Столлман – основатель проекта GNU и проекта свободного программного обеспечения, продвигает свободу использования компьютеров. В середине 1980-х он основал движение свободного программного обеспечения, основная идея которого состоит в том, что компьютеры предназначены для облегчения, а не для препятствования сотрудничеству.

Чарли Миллер

Чарли Миллер, известный тем, что обнаружил уязвимости Apple и выиграл в 2008 году известный конкурс хакеров Rwn2Own, также работал «этичным хакером» в Агентстве национальной безопасности США.

Дэн Каминский

Дэн Каминский – главный научный сотрудник компании White Ops, занимающейся обнаружением активности вредоносных программ с помощью JavaScript. Он известен тем, что обнаружил фундаментальный недостаток в протоколе системы доменных имен (DNS), который позволял проводить широкомасштабные атаки с порчей кеша.

Джефф Мосс

Джефф Мосс работал в Консультативном совете США по национальной безопасности во время президентства Обамы и был сопредседателем Целевой группы совета по CyberSkills. Он также основал хакерские конференции Black Hat и DEFCON и является членом Глобальной комиссии по стабильности киберпространства.

Определение хакеров Серые шляпы

Между Белыми и Черными шляпами работают Серые шляпы. Действия Серых шляп представляют собой смесь действий Черных и Белых шляп. Серые шляпы часто ищут уязвимости в системе без разрешения или ведома владельца. При обнаружении уязвимостей они сообщают о них владельцу, иногда запрашивая небольшую плату за устранение проблем.

Некоторым хакерам из группы Серых шляп нравится думать, что они приносят компаниям пользу, взламывая их веб-сайты и вторгаясь в их сети без разрешения. Однако владельцы компаний редко ценят несанкционированные вторжения в инфраструктуру своих бизнес-данных.

Часто реальный мотив Серых шляп – продемонстрировать навыки и добиться известности, возможно, даже признательности за то, что они считают своим вкладом в кибербезопасность.

Кто такие Серые шляпы?

Серые шляпы иногда могут нарушать законы и стандарты этики, но без злого умысла, характерного для Черных шляп.

Если уязвимость обнаружена Белой шляпой, ее эксплуатация будет производиться только с разрешения; до момента устранения уязвимости об этом никому не будет сообщено. Черная шляпа будет незаконно эксплуатировать уязвимость или рассказывать, как это сделать. Серая шляпа не будет эксплуатировать уязвимость незаконно и не расскажет другим, как это сделать.

Многие Серые шляпы считают, что Интернет небезопасен для бизнеса, и что их миссия – сделать его более безопасным для частных лиц и организаций. Они делают это посредством взлома сайтов и сетей, создавая хаос, с целью доказать миру свою правоту. Серые шляпы часто говорят, что не хотят навредить своим вторжением. Иногда им просто интересно

взломать известную систему, не соблюдая конфиденциальность и другие законы.

В большинстве случаев Серые шляпы предоставляют компаниям ценную информацию. Тем не менее, сообщество Белых шляп и большая часть кибермира не считают их методы этичными. Взломы, осуществляемые Серыми шляпами, является незаконным, поскольку не было получено разрешение на попытку проникновения в систему организации.

Как работают Серые шляпы

После получения незаконного доступа к системе или сети, Серая шляпа может предложить системному администратору нанять его или одного из его друзей для решения проблемы за определенную плату. Однако эта практика сокращается из-за растущей готовности компаний к судебному преследованию хакеров.

Некоторые компании используют программы вознаграждения за найденные ошибки, чтобы побудить Серые шляпы сообщать о результатах взломов. В этих случаях организации назначают вознаграждение, чтобы избежать риска эксплуатации уязвимости хакером с целью личной выгоды. Но это не всегда так, поэтому получение разрешения от компании – это единственный способ гарантировать, что хакер будет действовать в рамках закона.

Однако, если организация не успела оперативно отреагировать или не подчинилась требованиям, Серые шляпы могут превратиться в Черные и разместить информацию об уязвимости в интернете или даже использовать эту уязвимость.

Серые шляпы против Белых шляп

Основное различие между Серыми и Белыми шляпами состоит в том, что Серые шляпы не связаны этическими правилами взлома или трудовым договором, и если организация не обращает внимания на их действия, они могут использовать обнаруженные уязвимости самостоятельно или рассказать о них в Интернете другим хакерам.

Примеры хакеров Серые шляпы

Самый известный пример Серой шляпы – Халил Шрайтех, безработный исследователь в области компьютерной безопасности, который в августе 2013 года взломал страницу Марка Цукерберга в Facebook. Его мотивация заключалась в том, чтобы заставить исправить обнаруженную им ошибку, которая позволяла публиковать сообщения на странице любого пользователя без его согласия. Он сообщил Facebook об этой ошибке, однако Facebook ответил, что это не является ошибкой. После этого инцидента Facebook исправил эту уязвимость, которая могла стать мощным оружием в руках профессиональных спамеров. Однако в рамках программы поощрения Белых шляп Шрайтеху не было выплачено вознаграждение, поскольку имело место нарушение политики Facebook.

Виды атак на сайт

В эпоху цифровых технологий, с ростом популярности Интернета увеличивается и киберпреступность, целью которой является кража данных в сети и использование их в незаконных целях. Один из наиболее распространенных видов хакерских атак – нарушение информационной безопасности веб-сайтов и серверов. За один месяц в мире происходит в

среднем 1,7 млн. киберпреступлений в виде утечки информации. Злоумышленники действуют по разным схемам кибератак. Ниже приведены наиболее частые атаки на сайты и способы защиты от них.

Что такое хакерская атака



Кибератака, хакерская атака – преднамеренное действие злоумышленника в сети, направленное на нарушение функциональности или взлома сетевого устройства для получения несанкционированного доступа к информационной системе с целью кражи личных данных, вымогательства денежных средств, отключения системы жертвы.

Классификация атак на сайт

Атаки на сайт классифицируют по разным параметрам: в зависимости от их цели, характера воздействия на сеть

(активные, пассивные), наличия обратной связи с атакуемой сетью, по уровню эталонной модели ISO/OSI и пр. Хотя существует множество различных способов проникновения злоумышленника в систему, большинство кибератак основываются на схожих моделях. Ниже приведены некоторые из наиболее распространенных типов кибератак и их схемы.

Виды кибератак

1. Атаки MitM

Атака типа «человек посередине» (MitM) также известна как атака с перехватом. Она происходит, когда злоумышленник пытается перехватить связь между двумя сторонами (веб-сервером и клиентским браузером), чтобы следить за жертвой, украсть личную информацию или учетные данные, передаваемые по сети. Для выполнения атаки хакер ищет незащищенные сетевые соединения в общедоступных сетях Wi-Fi. Для предотвращения атак MitM при доступе к сети из незащищенной общедоступной точки доступа Wi-Fi используют виртуальную частную сеть (VPN), обеспечивающую безопасное соединение с шифрованием данных.

Примечание. В наши дни MitM не широко распространены, так как в большинстве систем электронной почты, чатов используется сквозное шифрование, которое предотвращает вмешательство третьих лиц в данные, передаваемые по сети, независимо от того, является ли сеть безопасной или нет.

Распространенные виды атак типа MitM:

- **Захват сеанса.** Злоумышленник захватывает сеанс между клиентом и сетевым сервером. После соединения клиента с сервером, хакер отключает клиента от

трафика и заменяет IP-адрес клиентского компьютера своим собственным IP-адресом, подделывая номера клиента. Сервер продолжает сеанс, полагая, что обменивается данными с клиентом. Если IP-адрес злоумышленника вставлен в середине сеанса, сервер может не обнаружить этого, так как пользователь уже задействован в доверенном соединении, то есть прошел проверку подлинности.

- IP-спуфинг. Это подмена IP-адреса пользователя злоумышленником для того, чтобы убедить систему в том, что она взаимодействует с известным доверенным лицом, и предоставить злоумышленнику доступ к системе. Хакер отправляет пакет с IP-адресом источника известного доверенного хоста вместо своего собственного IP-адреса на целевой хост. Целевой хост может принять пакет и действовать в соответствии с ним.

Атаки типа «человек посередине» опасны для сайтов без шифрования данных при их передаче от клиента к серверам. Это веб-ресурсы, не использующие HTTPS (расширение протокола HTTP для поддержки шифрования). URL-адрес такого веб-сайта начинается с HTTP, а не HTTPS, как рекомендуется. Наличие сертификата безопасности HTTPS также определяют по значку слева в адресной строке. Сайты, использующие протокол HTTPS, имеют символ замкнутого замка, что свидетельствует о защищенном соединении с сайтом.

Простой способ предотвратить атаку MitM – установить на сайте сертификат Secure Sockets Layer (SSL), обеспечивающий шифрование всей информации, передаваемой между сторонами. Большинство современных провайдеров имеют встроенный сертификат SSL в своем хостинг-пакете. Таким образом, эффективную защиту от атак MitM обеспечивают шифрование и цифровые сертификаты, гарантируя конфиденциальность и надежность связи.

2. Отказ в обслуживании (DoS-, DDoS-атаки)

Атаки типа «отказ в обслуживании» (DoS, DDoS) перегружают системы, серверы, сайты трафиком для нарушения или прекращения их обслуживания, чтобы сделать его недоступным для посетителей. В результате перегруженного сервера система не может отвечать на запросы пользователей и прекращает свою работу.

Распределенная атака «отказ в обслуживании» DDoS – тот же метод, что и традиционный DoS, за исключением того, что хакер использует несколько взломанных устройств для запуска атаки трафиком на целевой веб-ресурс в более крупном масштабе. Эта атака сложнее и опаснее, так как выполняется одновременно с разных IP-адресов по всему миру, что затрудняет определение её источника для сетевых администраторов.

Существуют разные типы DoS- и DDoS-атак, наиболее распространенные из них – TCP SYN flood, smurf, ping-of-death, ботнеты. Злоумышленники часто используют Dos-, DDoS-атаки вместе с другими атаками, чтобы отвлечь автоматизированные системы защиты от реагирования на проблему.

Атаки DoS, DDoS используются спонсируемыми государством хакерами, цель которых – нарушить работу иностранных правительств и организаций. Согласно отчету Cisco, веб-сайты Олимпийских игр 2016 года в Рио пострадали от 223 крупномасштабных DDoS-атак. Токио для проведения Олимпийских игр создало совет по кибербезопасности. Атака «отказ от обслуживания» также может принести финансовую выгоду для бизнес-конкурентов, заинтересованных в устранении конкурента для охвата большей части рынка. Исследование рисков информационной безопасности, проведенное «Лабораторией Касперского», показало, что

одна DDoS-атака («распределенный отказ в обслуживании») обходится малому бизнесу в 123 тыс. \$, а крупным предприятиям в среднем 2,3 млн. \$.

Для предотвращения DoS- и DDoS-атак необходимо уменьшить трафик с помощью сети доставки контента (CDN), балансировщика нагрузки, масштабируемых ресурсов. Также следует использовать брандмауэр на случай, если DDoS-атака скрывает другой метод кибератаки, такой как SQL-инъекция или XSS.

3. Межсайтовый скриптинг (XSS)

Межсайтовый скриптинг (XSS), атака с использованием межсайтовых сценариев – атака, при которой злоумышленник загружает в базу данных веб-сайта вредоносный клиентский код (скрипт JavaScripts, реже HTML, VBScript, ActiveX, Flash). Атаки XSS разделяют на три категории: сохраненные (постоянные), отраженные (непостоянные), основанные на DOM.

Межсайтовый скриптинг происходит следующим образом. Когда пользователь входит на страницу веб-сайта, его браузер автоматически запускает скрипт хакера как часть кода HTML, который выполняет вредоносный сценарий. Вредоносный код может передать файлы cookie из браузера пользователя на сервер злоумышленника, который использует их для перехвата сеанса и дальнейшего извлечения учетных данных клиента, управления его устройством.

Атака является успешной для уязвимых веб-сайтов, использующих недостаточный уровень кодирования и проверки на наличие вредоносного содержимого веб-запроса. Браузер пользователя не может обнаружить, что вредоносный источник (чаще всего веб-запрос) ненадежный, и

предоставляет ему доступ к файлам cookie, токенам сеанса или другой конфиденциальной информации, связанной с сайтом, или позволяет вредоносному сценарию переписывать содержимое HTML.

Недавнее исследование Precise Security показало, что XSS-атака является наиболее распространенной кибератакой, составляющей примерно 40% всех атак. Основная защита от XSS-атак – правильное кодирование, включая кодирование HTML, атрибутов, кодирование JavaScript, CSS и т. д. Разработчики устанавливают брандмауэры, действующие как фильтр, который выявляет и блокирует любые вредоносные запросы к веб-сайту. Большинство современных веб-хостинговых платформ используют эти функции автоматически.

4. Атака с использованием SQL-инъекции

Атака с использованием SQL-инъекции – тип атаки, нацеленный на серверы, использующие язык программирования структурированных запросов SQL для управления информацией в базах данных. Базы данных SQL используют операторы SQL для запроса данных, и эти операторы обычно выполняются через HTML-форму на веб-странице. Если разрешения базы данных не были установлены должным образом, злоумышленник может использовать HTML-форму для выполнения вредоносных запросов.

Атака с использованием SQL-инъекции нацелена на получение доступа к базам данных, хранящихся на сервере. Хакеры загружают скрытые запросы, содержащие вредоносный код, в веб-формах (например, в форме данных пользователя при входе на сайт – логин, пароль). Когда пользователь вводит свои данные в веб-форму и нажимает кнопку «Войти», он отправляет запрос SQL в базу данных на

сервере для извлечения его данных и отражения их в пользовательском интерфейсе. В это же время и запускается вредоносный код, который дает злоумышленникам возможность полного контроля над сайтом: просматривать, изменять, удалять данные, отдавать операционные команды и полностью отключить работу системы. Это также может быть использовано для взлома корпоративной сети, что приведет к дальнейшим атакам внутри организации.

К этому типу атак кибербезопасности уязвимы сайты, использующие динамический SQL, приложениях PHP и ASP из-за преобладания более старых функциональных интерфейсов.

Защита веб-сайта от атак на основе SQL-инъекции зависит от надежности кодовой базы. Чтобы снизить риск атаки, используют параметризованные запросы, аутентификацию для защиты базы данных, проверяют входные данные по белому списку портов и хостов, используют подходящую библиотеку ORM (Hibernate, Entity Framework, ActiveRecord и др., в зависимости от платформы), ограничивают права доступа к базе данных сайта.

5. Парольные атаки

Парольная атака – тип кибератаки, при которой злоумышленник пытается взломать пароль пользователя. Существует множество различных способов взлома пароля, в том числе атака грубой силы, атака по словарю, атака по радужной таблице, заполнение учетных данных, распыление паролей, атака кейлоггера.

Для получения пароля пользователя преступники также используют методы фишинга (попытки обманом заставить жертву передать ценную информацию, такую как пароли, данные кредитной карты и др.), используют ботов для взлома

учетных данных, пытаются перехватить сеансы пользователей, не зашифрованные в сети.

Во избежание взлома паролей рекомендуется настроить функцию блокировки учетной записи при авторизации, которая автоматически блокирует доступ к устройству, веб-сайту или приложению после определенного количества попыток ввода неверного пароля. Владельцы сайта могут потребовать от своих посетителей устанавливать надежные пароли с помощью криптографического алгоритма «хеширования пароля», такого как Bcrypt, Scrypt или Argon2, настроить двухфакторную аутентификацию (2FA), использовать программы-генераторы кодов сеанса, чтобы снизить риск взлома их учетной записи.

6. Несанкционированный доступ

Веб-сайты устанавливают контроль доступа пользователей к ограниченным областям. Но механизмы управления, обеспечивающие соблюдение этих ограничений, часто имеют недостатки. Злоумышленники пытаются обойти эти элементы, чтобы получить несанкционированный доступ к функциям или данным (учетным записям пользователей, конфиденциальным файлам, выполнению административных действий и т. д).

Исправление и предотвращение недостатков контроля доступа требует системного подхода. В зависимости от функционала могут применяться различные модели управления доступом, наиболее распространенные из которых – системы контроля доступа RBAC, DAC, MAC.

7. Использование неизвестного или стороннего кода

Электронные коды для сайта, созданные третьим лицом, могут привести к серьезному нарушению безопасности. Разработчик фрагмента кода может включить в него вредоносную строку или по незнанию оставить бэкдор, что несет риск нарушения безопасности – от простой передачи данных до получения административного доступа к сайту злоумышленниками. Чтобы избежать этих рисков, разработчикам необходимо проверять достоверность кода, убедиться, что используемые плагины (особенно для WordPress), обновлены и регулярно получают исправления безопасности.

8. Вредоносное ПО

Вредоносное ПО – это виды вредоносного программного обеспечения, выполняющие вредоносные задачи на устройстве с целью получения злоумышленником учетных или других ценных данных, прерывания работы системы, вымогательства у жертвы денежных средств и пр.

Вредоносное ПО активируется и заражает компьютер после его загрузки. Это требует определенных действий со стороны пользователя, например, щелчка по ссылке, нажатия кнопки загрузки файла, открытия приложения электронной почты, под которыми скрывается вредоносное ПО.

Некоторые из наиболее известных типов вредоносных программ – это вирусы, черви, трояны, боты, программы-вымогатели, бэкдоры, шпионское и рекламное ПО. Проникнув в систему, они могут блокировать доступ к сетевым файлам, передавать информацию жертвы с жесткого диска, отслеживать сетевой трафик, нарушать работу системы и полностью отключать её для похищения хакером конфиденциальных данных.

Согласно отчету Verizon о расследовании утечек данных, основная мотивация киберпреступников – финансовая, поэтому они чаще всего похищают банковские реквизиты и другие данные, открывающие доступ к денежным средствам.

Для защиты устройства от вредоносного ПО устанавливают антивирусные программы, популярные из которых – Eset NOD32, Антивирус Касперского, Avast!, Symantec Norton Anti-Virus, McAfee VirusScan и др. Антивирусы обнаруживают вредоносные программы, предупреждают о потенциальных угрозах во всплывающем окне и удаляют их.

Некоторое вредоносное ПО имеет код, который обходит антивирусные программы. Поэтому пользователям важно сохранять бдительность в отношении того, какие сайты они посещают и по каким ссылкам переходят. Атаки потенциально опасных программ также можно предотвратить с помощью межсетевого экрана нового поколения (NGFW), обеспечивающего комплексную сетевую защиту и способного выполнять глубокую проверку пакетов данных с использованием искусственного интеллекта (AI).

9. Атака нулевого дня

«Атака нулевого дня» – атака, при которой киберпреступники обнаруживают сетевые уязвимости в безопасности широко используемого программного обеспечения (Microsoft Windows, Google Chrome), операционных системах, и атакуют эти ресурсы до того, как исправление станет доступным. Атака предшествует обновлению ПО, который рассматривается «первый день», поэтому называется «атакой нулевого дня».

Хакеры действуют по двум сценариям: ищут уязвимости в обновлениях или исправлениях системы безопасности ПО для сайта или сервера, который своевременно не обновил систему, и используют их целью атаки. В обоих случаях безопасность сайта оказывается под угрозой, и последующий ущерб зависит от навыков злоумышленников. Лучший способ защитить себя и свой сайт от атак нулевого дня – обновлять программное обеспечение сразу после того, как разработчики предложат новую версию.

Легендарный Anonymous

Считается, что этот децентрализованный онлайн-коллектив образовался в 2003 году. Участники не имеют какой-либо конкретной политической принадлежности и выступают против цензуры и государственного контроля, который мешает продвижению свободы слова. На протяжении всего времени своего существования Anonymous противостоит террористическим организациям, наркокартелям и тд. В разные годы, члены команды скрытые под маской известного героя романа - утопии Гая Фокса, выражали поддержку движениям Occupy Wall Street и WikiLeaks. Полная анонимность участников группы не уберегла их от проблем с законом. Они не раз становились героями криминальной хроники, обвинённые во взломе компьютеров и кибер-преследовании.



Тактикой Anonymous являются мощные DDoS-атаки и многочисленные оффлайн-пранки. Хактивисты могут искусно заменять целевые страницы любого веб-сайта своими сообщениями и графикой. Anonymous завоевали большую популярность из-за своей приверженности определенным жизненным принципам. В 2012 году группировка вошла в список из 100 важнейших явлений планеты, который был составлен авторитетным изданием Time. Это не удивительно, ведь Anonymous стоял за громкими кибератаками на Visa, MasterCard и PayPal в 2010 году, саботажем сети PlayStation и преследованием правительственных сайтов Египта и Туниса в 2011 году. В 2020 году, после смерти Джорджа Флойда, Anonymous обвинил полицию Миннеаполиса в ужасающей репутации насилия и коррупции. С тех пор сайты города, включая полицейские, часто оказываются вне доступа.

Вымогатели BlackMatter

Множество представителей бизнес сообщества страдают от так называемых программ вымогателей, которые не раз попадали в заголовки известных изданий. Многие слышали о таких хакерских группировках, как DarkSide или REvil, которым приписывают нападение на крупного поставщика нефтепродуктов Colonial Pipeline весной этого года, а также атаки на системы известного производителя мяса JBS. Но есть мнение, что они прекратили своё существование или находятся в глубокой спячке, и на их место претендует новая партнерская программа: "вымогатели как услуга" (RaaS), под названием BlackMatter. Группа образовалась совсем недавно. Хакеры специализируются на поиске людей, которые готовы за солидное вознаграждение предоставить доступ к корпоративным сетям, чтобы затем запустить туда свою вредоносную программу. У BlackMatter здоровый аппетит. В поле их интересов только компании с ежегодным доходом более \$100 млн. За информацию "брокерам начального доступа" предлагается от 3 до 100 тысяч долларов.

APT31 она же Hurricane Panda она же Zirconium

Хакерская группировка APT31 имеет несколько названий и известна многочисленными целенаправленными атаками на государственные структуры разных стран. Компания Microsoft обвинила группу в атаке на участников выборов президента США 2020 года. Тогда за предвыборные месяцы было зафиксировано около тысячи атак группы APT31 на американских избирателей. Помимо этого, хакеры атаковали аккаунты международных и политических организаций, а также образовательных учреждений. Некоторые эксперты считают что эта команда контролируется китайскими спецслужбами. Злоумышленники используют АРТ-атаки (Advanced Persistent Threat) начиная с 2010 года. За это время, злоумышленники осуществляли нападения на веб сайты госструктур, Норвегии, Финляндии и Германии. Начиная с этого года APT31 стала применять новые инструменты для заражения различных устройств, используя фишинговые письма со ссылкой на подставной домен.

Lizard Squad - молодость не помеха

От 15 до 17 лет было членам Lizard Squad, когда их арестовали благодаря предоставленной информации от другой команды хакеров. Нужно сказать, что Ящерицы сами виноваты в таком исходе, ведь они так любили хвастать своими проделками в соцсетях. А именно - DDoS атаками на игровые серверы League of Legends и Call of Duty, разглашением конфиденциальной информации Sony или открытой поддержкой северокорейского режима и ИГИЛ (запрещенной в России террористической организации). Некоторые пользователи считают, что Lizard Squad сознательно создавали ажиотаж вокруг своей персоны. Своими DDoS атаками на компанию Play Station Network и конкурента Xbox Live, они давали понять о необходимости в большей защите игровых сервисов. На тот момент Ящерицы

могли бы успешно атаковать мировые биржи, что привело бы к настоящему коллапсу в экономике, но они не преследовали подобных целей. Главное, чтобы к вопросу защиты игровых сервисов наконец-то отнеслись серьезно. В итоге Sony и Microsoft пришлось совершенствовать свою защиту.

Syrian Electronic Army

Эта хакерская группировка открыто демонстрирует свои взгляды на мировой порядок и ведёт кибервойну против врагов нынешнего правителя Сирии. Изначально хакеры нацелились на главных, по их мнению, организаторов "арабской весны", США, Катар и Саудовская Аравия. SEA старается атаковать авторитетные новостные сайты с солидной репутацией. Это делается для того, чтобы опубликовать фейковую информацию, просто выдав её за подлинную. Например, в 2013 году хакеры использовали твит, чтобы обрушить фондовые рынки. После сообщения с официального аккаунта Associated Press о взрывах в Белом доме и якобы ранении Барака Обамы, им это удалось. Кроме того, SEA продолжает организовывать фишинги и DoS атаки на сайты сирийских повстанцев и западные онлайн ресурсы, которые критикуют политику нынешнего правительства Сирии.

1. WannaCry — самый массовый вирус десятилетия

Когда: май 2017 года.

Кого или что атаковали: компьютеры на ОС Microsoft Windows.

Что произошло:

WannaCry — вредоносная программа-вымогатель, которая использовала уязвимость нулевого дня в различных версиях Windows. Проникая в компьютеры, вирус зашифровывал все содержимое, а затем начинал требовать деньги за разблокировку. Однако расшифровать файлы было невозможно.



Окошко с требованиями вымогателей WannaCry

Впервые его обнаружили в Испании, а затем и в других странах. Больше всего пострадали Россия, Украина и Индия. Из-за WannaCry остановилась работа банков, правительственных организаций, аэропортов. В ряде британских больниц не смогли провести срочные операции. Код вируса выглядел слишком примитивным и как будто недописанным. Поэтому появились версии, что разработчик случайно выпустил его раньше времени. В пользу этого говорит и то, что коды для расшифровки не работали. Предполагают, что изначально WannaCry должен был поразить все устройства на Windows.

Остановить вирус удалось исследователю Маркусу Хатчинсу под ником Malwaretechblog. Он обратил внимание, что перед тем, как зашифровать файлы, программа отправляет запрос на несуществующий домен. Хатчинс зарегистрировал этот домен, после чего WannaCry перестал причинять вред. В создании вируса подозревают Lazarus Group и другие группировки, связанные с Агентством национальной безопасности США: данные об уязвимости были известны только АНБ.

Ущерб: вирус успел заразить 500 тыс. компьютеров в 150 странах мира и нанести ущерб в \$1 млрд.

2. Petya/NotPetya/ExPetr — самый большой ущерб от кибератаки

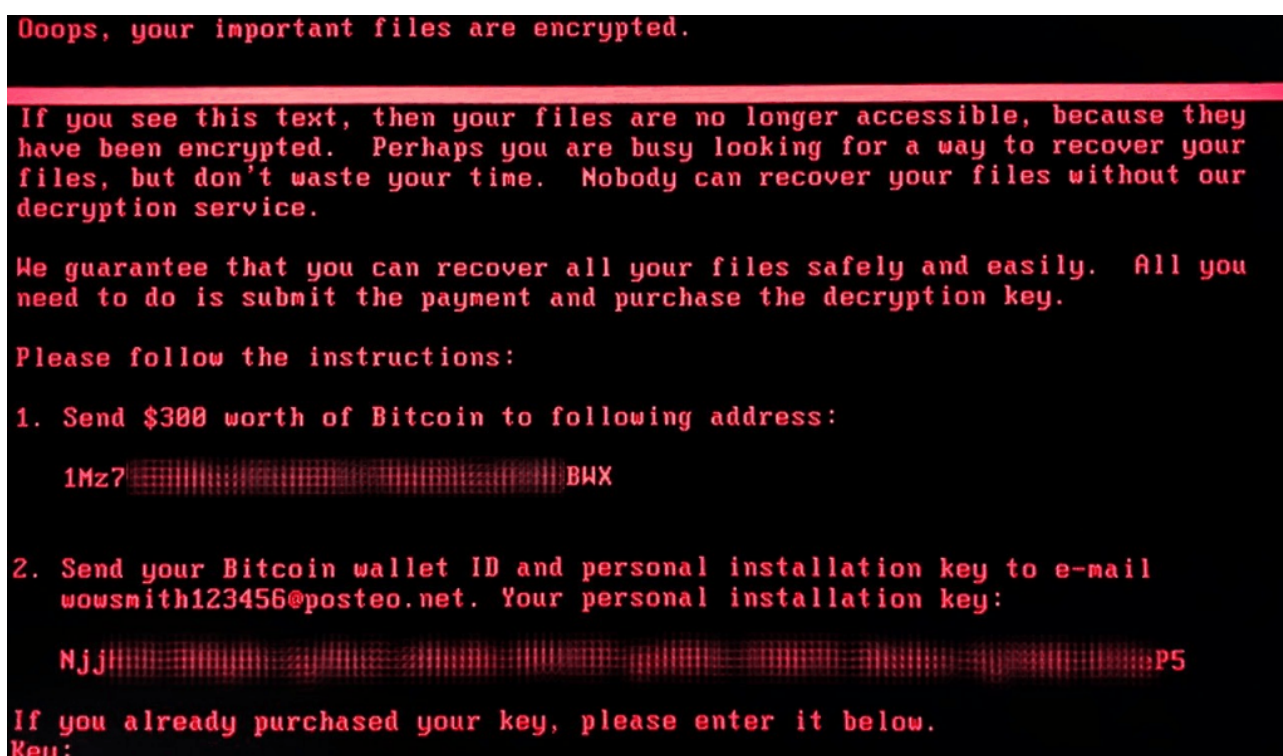
Когда: июнь 2017 года.

Кого или что атаковали: крупные корпоративные сети компаний и госслужб по всему миру

Что произошло:

Первая версия вируса появилась еще в марте 2016 года, но серьезные кибератаки начались в 2017-м. Не все согласны с тем, что в обоих случаях это был один и тот же вирус, но значительная часть кода действительно совпадала. По поводу названия тоже возникли споры: исследователи из «Лаборатории Касперского» предпочитают называть вирус New Petya, NotPetya или ExPetr.

Так же, как и WannaCry, Petya и его поздние версии поражали компьютеры на ОС Microsoft Windows. Они зашифровывали файлы — точнее, базу данных с информацией обо всех файлах на диске — и данные для загрузки ОС. Затем вирус требовал выкуп в биткоинах.

A screenshot of a ransomware message displayed on a black background with red text. The message is in English and Russian. It states that files are encrypted and offers a decryption service for \$300 in Bitcoin. It provides a Bitcoin address (1Mz7...BWx) and an email address (wowsmith123456@posteo.net) for sending wallet ID and installation key. It also mentions a personal installation key (Njji...P5). The message ends with a prompt to enter the key if already purchased.

Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:
1Mz7...BWx
2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:
Njji...P5

If you already purchased your key, please enter it below.
Key:

Экран пораженного вирусом NotPetya компьютера

Но коды для расшифровки не помогали, а, наоборот, уничтожали все данные на жестком диске. При этом вирус получал полный контроль над всей инфраструктурой компании, и защита от WannaCry против него уже не действовала.

Для создания NotPetya использовали коды хакерской группировки Equation, выложенные в открытый доступ. В октябре 2020 власти США обвинили хакерскую группировку Sandworm, состоящую из сотрудников российского ГУ ГШ, в причастности к вирусу NotPetya и другим кибератакам.

Больше всего от вируса пострадала Украина. Позднее пришли к выводу, что именно отсюда началось заражение. Причина — в автоматическом обновлении

бухгалтерской программы M.T.doc, которой пользуется большинство компаний и госорганов в стране.

Ущерб: Вирус затронул компании и госорганы Европы, США, Австралии, России, Украины, Индии, Китая. Среди пострадавших — российские компании «Роснефть» и «Башнефть», международные корпорации Merck, Maersk, TNT Express, Saint-Gobain, Mondelez, Reckitt Benckiser. На Украине пострадало более 300 компаний, включая «Запорожьеоблэнерго», «Днепроэнерго», Киевский метрополитен, украинские мобильные операторы «Киевстар», LifeCell и «Укртелеком», магазин «Ашан», Приватбанк, аэропорт Борисполь. 10% памяти всех компьютеров в стране оказалось стерто. Общая сумма ущерба от деятельности хакеров составила более \$10 млрд.

3. Выборы в США — главный политический скандал

Когда: июль 2016 года.

Кого или что атаковали: серверы Национального комитета Демократической партии США (DNC) и комитета Демократической партии по выборам в Конгресс (DCCC).

Что произошло:

Хакеры использовали вредоносное ПО для удаленного управления серверами и передачи файлов, а также слежки за всеми действиями пользователей в рамках сети. После кибератаки хакеры вычистили все следы своей активности.

Хакерам удалось получить доступ к электронной почте кандидата в президенты от демократов Хилари Клинтон и ее команды. В итоге 30 тыс. электронных писем были опубликованы на WikiLeaks, включая 7,5 тыс. документов, отправленных самой Клинтон. Многие документы были секретными и касались террористических атак на консульство США в Бенгази в 2012 году. Остальные содержали персональные данные членов и спонсоров демократической партии, включая номера их кредитных карт.

Американские эксперты по интернет-безопасности обвинили в этих атаках действующие из России хакерские группировки под названием Cozy Bear и Fancy Bear.

Ущерб: История с перепиской вызвала раскол внутри демократов и сильно пошатнула их позиции накануне выборов. Скандал негативно повлиял на рейтинги Клинтон и помешал ей победить Дональда Трампа на президентских выборах. Она же положила начало Пиццагейту — одной из самых масштабных теорий заговора в США.