Ужасные и не очень. Вирусы в телекоме

Сегодня вирусы регулярно обеспечивают массу популярных новостных поводов не только в специализированных СМИ, но и в тех, которые пишут обо всем подряд, ведь практически не осталось тех сфер или устройств, до которых хакеры не дотянулись своими мошенническими схемами.



И даже, как только появляются новые IoT-устройства, так сразу же на каждое из них находятся свои кибермошенники, которые готовы получить любую информацию о пользователе.

Массовый переход на удалённый режим работы задал определённые тенденции развития зловредов среди злоумышленников. На текущий момент средства антивирусной защиты способны обеспечить безопасность от уже известных вирусов, содержащих известный вредоносный код (сигнатуру), либо его модификацию, но учитывая рост целенаправленных атак и угроз "нулевого дня", для которых нет сформированных сигнатур и репутационной информации, использование "классических" антивирусных средств защиты будет недостаточно.

Проблема вирусов в телекоммуникациях всегда стояла достаточно остро. Современные вирусы имеют массу разновидностей: трояны, черви, всевозможные шпионы, вымогатели, майнинговые программы, ботнеты и даже просто рекламщики.

"На данный момент выделяется 3 наиболее распространённых и критичных типа угроз:

- Сбои в работе. По специфике работы операторов связи данный тип угроз является наиболее критичным в связи с недопущением отказа работоспособности активного сетевого оборудования и, как следствие, "простоя" предоставляемых сервисов и ухудшения качества предоставляемых услуг для абонентов.
- Утечка информации. В данном случае угроза связана с возможностью получения злоумышленником данных об абонентах. Прямых потерь оператор связи в случае реализации данной угрозы может не нести, но в случае публичного разглашения подобного инцидента оператор может потерять репутацию надёжного и доверенного Партнёра и провайдера.
- Мошенничество. В связи с последними событиями: переход на удалённую работу, использование облачных ресурсов, развитие различных сервисов и приложений, повышение объёма информации в СМИ в связи с пандемией и обсуждением мировой геополитической обстановки, данный тип угроз стал более актуальным и примечательным со стороны злоумышленников, например, перенаправление входящих/исходящих вызовов, манипуляции с переадресацией и перехват соединений, фишинговые атаки и манипуляции с переводами денежных средств", - рассказывает менеджер по продажам решений Департамента информационной безопасности ГК "Softline" Николай Спирихин.

"С помощью внедренного в IoT-устройства ВПО, осуществляется кража пользовательских данных (логины/пароли, номера банковских карт и др.) или перенаправление пользователей на поддельные (фишинговые) ресурсы вместо легитимных. Однако не правильно говорить о том, что данные угрозы являются новыми. Это устойчивая тенденция последних нескольких лет", - рассказывает директор департамента мониторинга и реагирования на киберугрозы ПАО "Ростелеком" Виктор Веренцов.

"Если говорить именно о специфике оператора связи (а "Ростелеком" уже давно не только оператор связи), то ключевая угроза – это нарушение доступности услуг связи, вследствие компьютерных атак, а также нарушение тайны связи в следствие несанкционированного доступа к системам мониторинга и управления сетями связи", - добавил директор департамента мониторинга и реагирования на киберугрозы ПАО "Ростелеком" Виктор Веренцов.

"Противодействие атаке начинается уже через 5-15 секунд после обнаружения. Самая мощная атака по стране, которую мы отразили в 2020 году, составила 1,35 Тбит/с, в 2021 году - 306 Гбит/с. На Урале такая платформа еженедельно отражает в среднем 25 атак на серверы компаний", - рассказывает директор по развитию корпоративного бизнеса ПАО "МегаФон" региона Центр-Урал Инна Смирнова.

Кибератаки набирают обороты. С чем это связано?

Не многие вспомнят, но десяток лет назад для того, чтобы быть хакером необходимо было иметь профессиональное образование. Сейчас же для того, чтобы написать простейший вирус достаточно воспользоваться инструкциями. Хакеры стали активно переходить на https, вследствие чего количество атак значительно увеличилось.

Раньше хакинг воспринимался как нечто очень сложное и был связан с элементами разработки, сейчас множество инструментов для проведения атак имеет удобный графический интерфейс, что значительно облегчает всевозможные атаки.

"Технологии не стоят на месте и все хотят денег", - комментирует ситуацию в целом, руководитель отдела проектного сетевого оборудования ООО "НАГ" Андрей Шепелев. "В 2021 году кибератак стало на порядок больше, чем в 2020 году в основном из-за массового перехода сотрудников крупнейших компаний на удаленку, многие перешли с рабочих защищенных устройств, на домашние, оказавшись наиболее уязвимыми".

Дело совершенно не в ранжировании типов атак, любая атака, в том числе с применением вредоносного ПО несёт риски для бизнес-процессов организации. При этом по общемировой практике, помимо вредоносного ПО (вирусов), злоумышленники в своих атаках зачастую применяют легальное ПО, либо диагностические утилиты, и в этом случае защититься от атаки становится куда сложнее. При использовании легального ПО на передний план выходят белые или черные списки приложений, сетевая настройка прав доступа и системы обнаружения и предотвращения вторжений.

"Хакеры также не стоят на месте, и средства проведения атак постоянно совершенствуются", - комментирует заместитель генерального директора по информационным технологиям, АО "Компания ТрансТелеКом" Алексей Берзин.

А кто же борется с вирусами?

"Многие "светлые" специалисты по безопасности - это бывшие хакеры, решившие завязать с темным прошлым - сами или с чьей-то помощью", - говорит руководитель отдела web-разработок ООО "НАГ" Алексей Газетдинов.

Разумеется, далеко не все спецы по борьбе с компьютерными угрозами – это бывшие хакеры. Подавляющее количество людей в отрасли всё-таки не занималось тёмными делишками и ежедневно защищают сети либо в составе специализированных отделов или даже компаний, либо, в качестве единственного специалиста, если организация невелика.

Тем не менее, нередки случаи, когда специалистами по кибербезопасности являются бывшие хакеры-самоучки, ставшие "матерыми" профессионалами в своей сфере не имея специализированного образования. Да, в университетах сегодня есть множество программ по кибербезопасности, ведь они набирают популярность у молодежи, но никто не знает от А до Я как устроены вирусы, как бывшие хакеры-самоучки, которые однажды раскаялись и перешли на "светлую сторону". Специалисты по кибербезопасности, пришедшие с "темной стороны" могут с легкостью решить задачу по восстановлению зараженного устройства с наименьшими потерями. Ведь изначально хакер - это не страшный злодей, желающий поработить весь мир - это программист, находящий уязвимости.

"Как и в любой крупной компании, у нас есть работники, кому по должностным обязанностям предоставляется доступ к использованию внешних носителей, разъездные, дистанционные, работники которым предоставляется расширенный доступ к веб-ресурсам", - рассказывает заместитель генерального директора по информационным технологиям, АО "Компания ТрансТелеКом" Алексей Берзин.

Что же делать?

"Риски атак и заражения зловредным ПО необходимо снижать путем организационных и технических мероприятий, в том числе: разработкой нормативной базы и доведением ее до работников, обучения персонала, назначением достаточных, а не избыточных прав доступа, установкой и настройкой средств антивирусной защиты, использованием белых и черных списков веб-ресурсов, списков программного обеспечения, использованием защищенных каналов связи (VPN), систем защиты почты, и систем обнаружения и предотвращения вторжений (IPS)", - добавил заместитель генерального директора по информационным технологиям, АО "Компания ТрансТелеКом" Алексей Берзин.

Необходимо помнить об этом и обеспечивать информирование работников в области ИБ, не надо стесняться напоминать работникам блокировать рабочие станции или запирать ящики с документами, не игнорировать обновление прикладного ПО и средств защиты, прорабатывать архитектуру информационных систем, в том числе систем управления операторским оборудованием, и архитектуру комплекса защитных мер, не бояться устанавливать и настраивать средства защиты в продуктивных информационных системах, а не только на рабочих станциях.

Главное, чтобы все участвующие в процессе понимали, что ИБ не является "злом, которое все запрещает", а обеспечивает снижение издержек в случае реализации рисков информационной безопасности.

Этот вопрос в организации защиты бизнес-процессов оператора. Всё зависит от того, сколько внимания оператор (организация) уделяет процессу защиты.

В этом случае вредоносное ПО (и не только оно) может нанести значительный ущерб, при этом значительная деградация сервиса будет намного дороже, чем модернизация и финансирование процесса ИБ.

Как можно препятствовать заражению компьютеров со стороны операторов

Основным активом и каналом распространения вредоносов является сетевая инфраструктура, поэтому необходимо использовать сетевые средства обеспечения безопасности, направленные на анализ происходящего, идентификацию зловредной, аномальной активности и, в случае возможности, предотвращение взаимодействия с источником угрозы, применение превентивных мер и оперативное реагирования на инциденты, так как заражение может происходить в считанные минуты и, в зависимости от типа вредоносного ПО, нанести соответствующий ущерб.

"В настоящий момент мы фиксируем рост заражения пользовательских устройств с целью объединения их в ботнеты, управляемые злоумышленниками. Такие ботнеты из зараженных IoT-устройств (в первую очередь из домашних роутеров) сейчас являются главным источником DDoS атак", - добавил директор департамента мониторинга и реагирования на киберугрозы ПАО "Ростелеком" Виктор Веренцов.

Что касается DDoS-атак, то здесь существует множество способов защиты: контроль межсетевого обмена информацией, регулирование зон покрытия, ограничение скорости, объёмов передаваемой информации, контроль использования ресурсов, использование специализированных средств, направленных на обнаружение и предотвращение DDoS-атак и т.д.

"Мы придерживаемся конкретизированного и комплексного подхода к проработке задач и оценке требований со стороны Партнёра для подбора наиболее эффективного и предпочтительного варианта решения в индивидуальном порядке", - рассказывает менеджер по продажам решений Департамента информационной безопасности ГК "Softline" Николай Спирихин.

"В случае обнаружения DDoS-атаки внутри сетевой инфраструктуры, во избежание распространения "заражения" и нарушения функционирования смежных устройств, работы пользователей и сервисов, мы рекомендуем в оперативном порядке заблокировать соединения и изолировать подверженный атаке ресурс, который потенциально становится источником распространения. Необходимо провести анализ данного инцидента ИБ и определить "узкие" места и уязвимости, которые способствовали и привели к реализации данной угрозы. Но данные меры являются реактивными, мы рекомендуем проактивный подход, включающий "тонкую" настройку имеющихся сетевых средств и использование специализированных средств защиты информации для активного реагирования, контроля доступа, минимизации рисков и предоставляющие расширенное журналирование для мониторинга уровня безопасности инфраструктуры", - добавил менеджер по продажам решений Департамента информационной безопасности ГК "Softline" Николай Спирихин.

Что может быть заражено

Поражаться вирусами могут любые современные устройства помимо компьютеров - телефоны,

телевизоры, приставки, а также чисто телеком-устройства - роутеры, точки доступа, коммутаторы, маршрутизаторы и.т.д.

> "Внедрение и использование новых технологий, способствует как повышению вариативности в интеграции систем, оптимизации рабочего процесса, так и перспективному развитию бизнеса с увеличением объёмов обрабатываемой информации и шириной предоставления и использования сервисов, но при этом привлекает внимание злоумышленников и создаёт дополнительные риски и векторы распространения угроз, в частности, если мы говорим о таком тренде, как Интернет вещей (Internet of Things, IoT)", - поделился менеджер по продажам решений Департамента информационной безопасности ГК "Softline" Николай Спирихин.

> "Проблема заражения абонентских устройств сейчас также актуальна, в подавляющем большинстве случаев заражаются терминалы с ОС Андроид. Это могут быть мобильные трояны с различным функционалом, например, нацеленные на хищения денежных средств или совершения различных несанкционированных действий. В данном случае страдают абоненты-владельцы зараженных смартфонов. Мы информируем абонента с зараженным устройством, рекомендуем проверить свое устройство антивирусным ПО, предупреждаем об опасности при переходе на выявленные ресурсы вредоносного ПО/фишинга, а также ограничиваем вредоносные сайты для недопущения заражения", - добавила директор по развитию корпоративного бизнеса ПАО "МегаФон" региона Центр-Урал Инна Смирнова.

Сможем ли мы избавиться от вирусов?

В основном, в появлении вирусов мы виноваты сами, потому что нас никто не заставляет переходить по вредоносным ссылкам или скачивать зараженные программы.

Но также, по слухам, мы находимся в "замкнутом круге". Говоря о "замкнутом круге" подразумеваются хитрые планы неких могущественных антивирусных компаний, которые, хорошо разбираясь в вирусах, пишут их сами, внедряют, после чего предлагают антивирусные программы для них. Именно антивирусы приносят компаниям хороший прирост достатка, что позволяет индустрии держаться на плаву и неплохо зарабатывать. Но это, без доказательств, все-таки не более, чем конспирология.

На безопасность компании готовы тратить огромные деньги, но всегда были и есть люди, которые выбирают "темную сторону силы". При наличии хороших знаний, один взлом системы может очень хорошо обогатить потенциального взломщика или создателя/распространителя вирусов.

Злоумышленники модернизируют и создают новые модификации уже используемых ранее типов вредоносного программного обеспечения, таких как: шифровальщики (программы-вымогатели), вирусы-майнеры, эксплойты, бесфайловые атаки и вредоносное программное обеспечение для получения удалённого доступа. Но несмотря на отсутствие "новых" типов киберугроз и неизменности основных каналов распространения угроз (веб и почта), основой развития деятельности и инструментария злоумышленника послужили во-первых, переход на удалённый формат работы, который способствовал обращению внимания к домашним сетям, личным и мобильным устройствам пользователей, как к дополнительному носителю конфиденциальной, корпоративной информации и вектору для проникновения в информационную систему, во-вторых – использование облачных сервисов и приложений, как к "неконтролируемому" варианту обработки данных ввиду расположения вне локальной инфраструктуры и в-третьих – цифровизация, способствующая возможности эксплуатации ранее необнаруженных уязвимостей в технологиях, вводимых в эксплуатацию, как системных, так и межсистемных интеграциях.

Кибермошенников иногда находят и наказывают

Да, бывает и такое, что удается найти тех, кто украл ваши данные и средства, несмотря на то, что это бывает крайне редко, но иногда у полиции получается выйти на хакеров или даже на целые группировки. Как в России, так и за рубежом лидерам и активным участникам хакерских групп, которых удается поймать, дают реальные уголовные сроки от 5 до 25 лет.

Вирусы становятся умнее, хитрее и злее, а значит, что их будет становится все больше и больше.

Хотим напомнить, что ваша безопасность это прежде всего ваша задача. Внимательное отношение к своему серфингу в интернете, здоровое недоверие и двухфакторная аутентификация помогут сохранить ваши данные и обезопасить ваших близких. Будьте бдительны.