ВИРУСОЛОГИЯ

Виталий Фёдоров: *Доходит до того, что вербуют человека*

Эксперт «Лаборатории Касперского» — о финансовых последствиях кибератак, группах риска и надёжных местах для хранения важных данных

Максим Анфалов

— В конце прошлого года компания «Лаборатория Касперского» предсказала, что в 2018 году число целенаправленных атак вырастет, а вредоносное программное обеспечение для кражи денег будет совершенствоваться. Оправдался ли ваш прогноз?

— С каждым годом количество всевозможных массовых инцидентов и атак на сетевую инфраструктуру растёт. Если говорить о наиболее заметных, то можно вспомнить 2010 год, когда компьютерный червь Stuxnet вмешался в работу иранской ядерной электростанции. В 2017 году случилась массовая атака, в которой был использован сетевой червь, программа-вымогатель WannaCry. И мы видим, что не просто выросло количество целенаправленных атак, а изменилось их качество. Теперь они могут развиваться очень витиевато, то есть если раньше они развивались линейно внутри атакуемой структуры, то сейчас одна группировка взламывает инфраструктуру, останавливается на достигнутом результате, продаёт взлом. Другая группировка покупает доступы к этим взломам, совершает какие-то действия (допустим, компрометирует ещё какие-то узлы внутри инфраструктуры), тоже останавливается на достигнутом, перепродаёт и так далее.

Конечная цель таких действий — получение денег. Злоумышленники стараются монетизировать всё, что находится внутри инфраструктуры. Допустим, они нашли учётные данные (связку логин/пароль). Дальше они начинают проверять их на каких-нибудь онлайн-ресурсах. Например, пытаются получить доступ к облачным почтовым сервисам с такой же парой. Если в результате у них получилось напрямую перевести деньги, «распылить» их по фиктивным счетам, то для них это, конечно, джек-пот. Но если не получилось, они начинают искать ту информацию, которую можно перепродать. Это могут быть и данные о пользователе, и персональные данные. Даже список пользователей в компании — это уже ценная информация, которая продаётся.

— На кого чаще всего нацелены целенаправленные атаки?

— Чаще всего угрозам подвержен банковский сектор либо компании, которые пользуются банковскими продуктами. То есть это та сфера, где можно получить деньги, а заметно или нет — каждые группировки делают это по-разному. Кто-то старается получить, что называется, «по копеечке», подменяя платёжные поручения и оставаясь какое-то время незамеченным. Кто-то находит лазейку и пытается умыкнуть сразу миллионы. И история знает случаи, когда у них это получалось. Так, например, в 2016 году задержали группировку Лурк, которая довольно долго промышляла таким способом.

С технической точки зрения эти атаки довольно сложные. Помимо технических методов могут также использоваться методы социальной инженерии: когда самый первый заражённый компьютер, назовём его условно «нулевой пациент», был заражён не техническим способом, а при помощи человека. Например, приходит на потенциально уязвимое предприятие якобы соискатель, говорит, что хочет устроиться на работу, просит распечатать со своей флешки резюме, а на ней вредоносная программа, которая проявит себя через какое-то время. Спектр инструментария, который используется злоумышленниками, растёт с каждым днём.

— А как совершенствуется вредоносное ПО для кражи денег? Что мы наблюдаем на сегодняшний день?

— Всё чаще злоумышленники используют так называемые программы-шифровальщики, используя опять же человеческий фактор либо уязвимость ПО. Эти программы шифруют данные таким образом, чтобы в результате к ним нельзя было получить доступ.

К примеру, для того чтобы заключить данные в некий зашифрованный контейнер, вам достаточно одного ключа шифрования, который есть только у вас, а чтобы открыть эти данные, требуется уже два ключа. И как раз второй ключ хранится у злоумышленника в единственном экземпляре. В этом вся сложность. Подобрать этот ключ невозможно, даже если все вычислительные центры в ближайшие десятки лет будут этим заниматься. Он очень длинный. То есть если мы представим себе обычный ключ от входной двери, то на нём будут сотни, а то и тысячи зубьев. Поэтому зашифрованные данные проще хранить в резервных копиях. Даже их расшифровка, как правило, занимает продолжительное время.

Защитой от таких вредоносных объектов, которые вымогают деньги за зашифрованные объекты, служат современные антивирусные продукты. На самом деле это уже не просто антивирус, а комплексные решения. По сути, это следующее поколение продуктов по уровню безопасности. Помимо антивирусной защиты, в защитных продуктах можно и нужно использовать резервное копирование данных, которые могут так или иначе пострадать от действий злоумышленников. При этом желательно сохранять их на отчуждаемых носителях (то есть не на том же компьютере). Ещё лучше — в «несгораемом сейфе». В этом случае, даже если вдруг вы подвергнетесь атаке, важную информацию можно будет легко восстановить.

— Раз уж мы говорим о деньгах, можете ли вы сказать, какие убытки ежегодно терпит бизнес от действий сетевых атак?

— К сожалению, мы не можем делиться данной информацией. Но приведу такой пример. В 2017 году компания Equifax (бюро кредитных историй), представительство которой есть в Москве, понесла колоссальные убытки в результате действий хакеров. Атака на компанию была совершена через уязвимый веб-сервер. Были украдены персональные данные пользователей: номера кредитных карт, паспортные данные. Причём пострадали как граждане США, так и российские граждане. В результате суммы одних только исковых требований к этой компании превысили её капитализацию, а это несколько сотен миллионов долларов.

— Ваша сфера ответственности — Уральский федеральный округ. Можно ли говорить о том, что для предприятий и компаний, которые находятся в УрФО, существует серьёзная угроза быть атакованными хакерами? И если существует, то для кого в первую очередь?

— Думаю, не секрет, что под угрозой как коммерческие, так и государственные структуры, оборонные предприятия. Они могут находиться где угодно. Но мы сегодня на форуме пообщались с несколькими нашими клиентами, в том числе потенциальными, и нам приятно осознавать, что многие наши заказчики применяют всё больше методов и средств в защите информации. Например, одно предприятие реализовало так называемый Whitelisting (белые списки приложений) по съёмным накопителям и запретило производить любой сетевой обмен, кроме того, который чётко определён и регламентирован руководством. Казалось бы, такие простые методы, но они в конечном счёте отсекают гигантский пласт «вредоносов». Вредоносные продукты не смогут проникнуть в инфраструктуру, в которой по умолчанию запрещены любые неизвестные приложения, флешки, где отключены уязвимые сетевые службы. Я вижу, что наши коллеги на уральской земле очень далеко продвинулись в этом вопросе, хотя буквально несколько лет назад была совершенно другая картина.

— Кто на сегодняшний день в этой схватке идёт на шаг впереди: тот, кто занимается предотвращением, защитой от сетевых угроз, или тот, кого можно назвать хакером?

— Быть может, это излишне оптимистично, но я считаю, что здесь соблюдается паритет. То есть когда мы выстраиваем защиту, которая по умолчанию всем известным и ненужным продуктам ставит заслон, это не оставляет злоумышленникам практически никаких шансов. Но возникает другая уязвимость — всё тот же пресловутый человеческий фактор. Доходит до того, что злоумышленники напрямую вербуют человека внутри компании, на которую нацелена атака.

— А если говорить о технических способах обеспечения информационной безопасности?

— Когда условно есть некая крупная компания и есть какая-то сетевая группировка, о которой никто ничего не знает, то эта компания на шаг позади, потому что её в любой момент могут атаковать, а она в любой момент не может атаковать, потому что она даже не знает о существовании этой группировки. Но в целом, если информационная безопасность выстроена грамотно, у злоумышленников мало шансов на то, чтобы проникнуть в информационную систему, что-то украсть.