ИНФОРМАЦИОННО-МЕТОДИЧЕСКИЙ ЖУРНАЛ

ЗАЩИТА ИНФОРМАЦИИ INSIDE®

«Почта России» 10770
«Вся пресса» 84592
«Роспечать» 84663

2 2013
март-апрель

ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Электронное государство и бюрократия

О квалификации мошенничества

Интеллект тонким слоем

Решения в динамике

Рай для фишинга

WWW.INSIDE-ZI.RU

Интеллект тонким слоем

Почему средства защиты информации не могут умнеть со временем?

Н. Н. Федотов, *главный аналитик компании InfoWatch*

Единственным носителем интеллекта на сегодня является человек. И то – далеко не всякий. Круг пользователей компьютерной техники ныне настолько широк, что IQ среднего пользователя упал ниже точки замерзания. Это объективный процесс.

Неумолимые законы экономики требуют постоянного расширения рынков. Как только рынок сбыта перестает расти, современное (особенно американское) предприятие норовит повести себя как банальная финансовая пирамида. Вот и с компьютерами так вышло: с начала 1980-х постоянно расширялся круг людей, способных управлять вычислительной техникой. Расширялся в значительной мере насильственно, не столько за счет обучения, сколько путем уверения потребителей, что им «это доступно». Изначально ограничиваясь лишь достаточно узким на тот момент сообществом инженеров-программистов, ныне он вобрал в себя бóльшую часть населения Земли вплоть до дошкольников и, наконец, уперся в естественный барьер: у человека только 2 глаза, 10 пальцев и 24 часа в сутках, поэтому он в состоянии управлять не более чем 4–5 компьютерами.

Итак, человеческого интеллекта остро не хватает на все существующие в мире машины, а искусственный интеллект пока не родился. Что делать? Оставлять технику неуправляемой? Брошенные без присмотра программы очень быстро дичают и становятся добычей киберхищников: вирусов, троянов, прочих вредоносов. А вместе с ними – обрабатываемые данные, управляемые объекты, а то и деньги пользователей. Если какой-либо объект, содержащий в себе компьютер, еще не начали взламывать, то исключительно потому, что трудно монетизировать результаты взлома. Спутники, автомобили, кофеварки, собачьи паспорта, телевизоры и фотоаппараты – все эти устройства хотя бы раз взломали. Более ликвидные устройства, такие как смартфоны, банкоматы и кассовые аппараты, ломают постоянно, отыскивая в них все новые уязвимости.

Средства защиты информации (СЗИ) нуждаются в человеческом интеллекте и ручном управлении в бóльшей степени, нежели другая компьютерная техника. Им требуется не просто живой человек, но специалист, профессионал в защите информации. Количество таких специалистов никак не поспевает за ростом парка информационных систем, не говоря уже о том, что стоимость рабочей силы растет, а цена компьютерных ресурсов падает. Где выход из складывающегося противоречия? Как подчинить человеку все компьютеры? Как распределить небольшое количество «живого» интеллекта на всю расширяющуюся кибервселенную?

Первый метод решения проблемы – полная автоматизация защиты. Такое СЗИ не должно требовать вмешательства оператора вообще. В этом случае его можно будет ставить на любое количество новых компьютеров, а интеллектуальные ресурсы тратить лишь на выпуск обновлений. Таким путем пошла индустрия антивирусов. Поставить себе антивирусную программу и периодически обновлять ее в состоянии даже человек с начальным уровнем компьютерной грамотности. Штат антивирусной лаборатории зависит от количества и сложности новых вирусов, но почти не зависит от числа инсталляций продукта. Поэтому один производитель может обслуживать хоть весь мир.

Однако за такую идеальную масштабируемость пришлось заплатить высокую цену. Все современные антивирусы работают на сигнатурном принципе. Антивирус ловит лишь ту заразу, сигнатура которой заранее внесена в базу. Ловит надежно, без пропусков (ошибок

первого рода) и ложных срабатываний (ошибок второго рода). Именно это позволяет сделать его необслуживаемым. Однако сигнатурный метод не в состоянии детектировать вредонос, который предварительно не был обнаружен вручную и препарирован вирусными аналитиками. Это делает нас беззащитными перед неизвестными вредоносными программами. Другими словами, даже самый лучший антивирус «с легким сердцем» пропустит только что появившийся вредонос, еще не успевший попасть на анализ к производителю либо предназначенный для узкой группы целей, а потому не являющийся массовым и поэтому обойденный вниманием антивирусников.

Последний пункт актуализировался совсем недавно, когда во многих государствах были созданы службы интернет-разведки и интернет-диверсий, принявшиеся выпускать средства кибершпионажа. Первые образцы кибершпионов уже выявлены, и выяснилось, что они беспрепятственно работали месяцами на сотнях узлов. Все антивирусы мира оказались бессильны – издержки сигнатурного метода.

Другие методы антивирусной защиты (эвристические, статистические, поведенческие) не обладают такой же надежностью, особенно в плане отсутствия ложных срабатываний, поэтому они не могут работать без присмотра квалифицированного оператора. Как следствие, они почти не применяются в массовых продуктах. Антивирусный продукт «для избранных», требующий постоянного присутствия квалифицированного оператора, в принципе, возможен, но на данный момент не создан по экономическим причинам: у него недостаточно потребителей, чтобы окупить разработку.

Сигнатурный метод хорош для массовой антивирусной защиты. Также он ограниченно годен для защиты от спама и очень ограниченно – для предотвращения утечек информации (DLP). Все прочие СЗИ на этом методе базироваться не могут. Следовательно, невозможно построить необслуживаемый межсетевой экран, систему обнаружения атак, DLP-систему, средство анализа логов и т. д.

Второй метод сопряжения немногочисленных специалистов с многочисленными компьютерами – это автоматизация управления. Редкого и дорогого работника можно сделать «многостаночником», дав ему инструменты для агрегации данных и единую консоль управления.

Когда разные СЗИ имеют универсальный интерфейс, для управления ими требуется меньше знаний. Когда многочисленные СЗИ выведены на единую консоль, команды можно отдавать быстрее, нескольким устройствам сразу. К сожалению, кроме экономии рабочего времени это ведет к появлению единой точки отказа. И еще – к зависимости от одного производителя. Да и возможности масштабирования при использовании этого метода ограничены: путем автоматизации команд производительность труда оператора поднимается в 2–3 раза, не более.

Третий метод – аутсорсинг. Вместо того чтобы держать специалиста по ЗИ в штате предприятия, можно передать обслуживание СЗИ в другую компанию. А еще лучше – передать не только обслуживание, но и размещение СЗИ.

Хороший пример – защита от DoS-атак. Оборудование для организации такой защиты дорогое, обучение специалиста – накладное. Атаки же случаются не слишком часто. Сам собой напрашивается выход из положения: защитное оборудование ставится у провайдера, там же сидит оператор, включающий защиту по требованию в зависимости от адреса атаки. Он реагирует на изменения тактики атакующего, переключает режим защиты при смене режима атаки.

Даже для тех угроз, где защита требуется не время от времени, а постоянно, этот метод несет экономию. Блокирование спама, цензура (блокирование вредного контента), организация шифрованных VPN-каналов, резервное копирование данных – все эти виды защиты выгоднее концентрировать у провайдера услуг, а не строить каждому самостоятельно. Представим себе 10 предприятий, на каждом из них работает один специалист по ИБ, который хорошо знаком со всеми пятью вышеперечисленными задачами. Объединяя таких специалистов в группу, провайдер услуг должен будет держать одного «спеца» по DoS-атакам, одного – по спаму, одного – по VPN и так далее – всего пятерых, каждый из которых в силу узкой специализации превосходит «местного» офицера безопасности. Пять работников вместо десяти – вот такое масштабирование.

Издержки аутсорсинга в том, что вместе с услугами приходится «отдавать» поставщику услуг и свои данные, повышая тем самым вероятность утечек, нарушения целостности и доступности. По этой причине пока не удается удешевить защиту от утечек. Эксплуатация DLP-системы требует затрат рабочего времени не только ИТ-специалистов, но также «безопасников», службы делопроизводства, отдела кадров и др. Состав конфиденциальных сведений у каждого предприятия свой. А главное – руководству не хочется передавать фильтрацию и архивирование трафика на аутсорсинг «чужому» предприятию. Поэтому DLP в виде услуги стороннего поставщика еще не работает. Хотя подвижки есть: бизнесмены уже почти согласились приобретать «как сервис» обработку бухгалтерской информации. Если они готовы доверять подрядчику бухгалтерию, то скоро доверят и защиту от утечек. А пока «местная» DLP-система по карману лишь крупным предприятиям и ведомствам. Средние и мелкие компании смогут себе позволить DLP только в виде сторонней услуги.

Итак, мы описали три метода, при помощи которых человеческий интеллект распределяется по многочисленным СЗИ.

А нельзя ли обойтись без такого размазывания? Без интеллекта вообще? Увы, нельзя. Потому что с другой стороны фронта действуют не стихийная сила и не алгоритм, а вполне себе интеллектуальные злоумышленники.

Человек всегда обманет программу, которая действует по алгоритму. Давайте вспомним «Обитаемый остров» Стругацких. Полоса обороны,

напичканная автоматическим оружием, зачищалась обычными людьми, даже не профессиональными солдатами, а каторжниками. Успешно зачищалась, с незначительными потерями. Потому что компьютер может выиграть у человеческого интеллекта только быстродействием или дешевизной. А когда есть время подумать и подготовиться, когда рабочая сила доступна, человек обыгрывает программу. Против человека должен играть человек, иначе шансов нет.

Кстати, перед злоумышленниками стоит та же проблема распределения одного человеческого интеллекта на много управляемых компьютеров. И методы ее решения – те же самые:

- автономизация программ (вирусы, черви);
- агрегация управления (ботнеты);
- передача на аутсорсинг (черный рынок услуг).

Однако деятели «темной стороны» не боятся отпускать «в мир» свои кибертворения на длинном поводке или вообще в автономном режиме, несмотря на многочисленные сбои и случаи некорректной работы. У них ограничение интеллектуального ресурса выражается в том, на сколько человек делить криминальный доход. Они готовы принимать риск выхода программы из-под контроля вследствие недостатка управления. Но зато чем меньше людей участвует в деле, тем больше денег достанется каждому и тем ниже вероятность предательства.

Многократно описанный в фантастической литературе «бунт машин» начался. Программы приступили к захвату власти над миром, только не насильственным путем, а при молчаливом согласии человека. Люди отдают власть машинам. Формально – по своей воле, но фактически – вынужденно. Во-первых, у людей не хватает интеллектуальных ресурсов, чтобы управлять расплодившимися программами. Во-вторых, там, где важна скорость реакции (в военном деле, в биржевой торговле, в скоростном транспорте, в энергетике, в управлении скоротечными производственными процессами), человек не в состоянии соревноваться с компьютером, поэтому вынужден передавать ему право принятия решений, иначе проиграет своему конкуренту.

Мы, человечество, должны найти способы распределять свой интеллектуальный потенциал все более тонким слоем на постоянно растущее число наших киберрабов. Иначе наши творения нас победят.