cezurity

5 причин, почему антивирус не защитит от целенаправленной атаки

Число атак, которые проводятся в каждый момент времени, неизвестно. Корпоративный шпионаж был всегда. Но сегодня специалисты по безопасности говорят о том, что мы вошли в новую эру киберпреступности – об этом свидетельствует характер обнаруженных в последнее время атак.

Сообщения о целенаправленных атаках, направленных на компании и правительственные организации, регулярно обсуждаются начиная с 2006 г. После нескольких громких инцидентов в индустрии защиты от киберугроз для обозначения целенаправленных атак стали использовать отдельный термин – *APT (Advanced Persistent Threats)*.

Можно провести различие между "массовыми" атаками и целенаправленными. Цели "массовых" атак – очень широкий круг пользователей. При этом жертвами становятся лишь наименее защищенные из них, которых все равно оказывается довольно много по той причине, что атакуется большое число целей. Если атакующие планируют обойти защиту, то их интересуют лишь распространенные решения – этого достаточно, чтобы атака оказалась успешной. То есть, принцип здесь можно сформулировать как "*миля вширь, дюйм вглубь*".

При этом надежность защиты может оказаться достаточной, если у других атакуемых она просто ниже. Например, на улице, где все двери открыты, от воров спасет даже самый простой замок.

Целенаправленные атаки строятся по другому принципу. Атакующего интересует конкретная информационная система компании. С помощью атаки решаются задачи, связанные с кибершпионажем или получением конкретной выгоды от компрометации информационных систем и данных. Атакуемый объект при этом всегда защищен – как минимум, с помощью антивирусного решения.

Для успеха атаки защиту нужно уметь обходить или отключать. В отличие от "массовых" атак, принцип здесь противоположен: "*дюйм вширь, миля вглубь*".

Целенаправленные атаки обычно хорошо спланированы, включают несколько этапов – от внедрения в информационную систему до уничтожения следов присутствия, и, как правило, растянуты во времени – от начала атаки до получения результатов могут пройти месяцы или годы. Иногда злоумышленники ставят цель закрепиться в атакуемых системах и как можно дольше оставаться незамеченными – это дает возможность, например, постоянно похищать конфиденциальную информацию.

Зачастую для осуществления целенаправленных атак совершаются точечные нападения на одного или нескольких пользователей. Задействуются самые разные методы сбора данных и внедрения в информационные системы. Это может быть социальная инженерия, эксплуатация известных и неизвестных (0day) уязвимостей, вредоносные программы и инструменты сокрытия их присутствия в системах. В таких атаках часто участвуют инсайдеры – помощники злоумышленников, работающие в атакуемых организациях.

Распространено заблуждение о том, что антивирусные решения способны обеспечить защиту от целенаправленных атак. Есть несколько веских причин усомниться в том, что антивирус способен защитить корпоративную IT-инфраструктуру от целенаправленной атаки.

1. Антивирусные решения изначально создавались для защиты от “массовых” атак

В основе антивирусных решений лежит сопоставление с сигнатурами уже известных атак или вредоносных программ. Такой подход к защите эффективен в том случае, когда одна вредоносная программа или уязвимость используется для атаки на большое число потенциальных жертв – то есть, атака является “массовой”.

После первого обнаружения атаки у антивирусной компании появляется сигнатура, на базе которой может быть создано правило или фильтр, который сможет защитить от подобных атак в будущем.

Но для целенаправленных атак могут применяться вредоносные программы, специально созданные для конкретного случая, то есть уникальные, а также еще не обнаруженные уязвимости.

Решение, основанное на сопоставлении с уже известными атаками или вредоносными программами, окажется бесполезным в случае уникальной атаки.

2. Злоумышленники всегда могут “обойти” антивирус

Идеология антивирусов не учитывает то обстоятельство, что неудачная атака не в состоянии остановить злоумышленников. Если отдельная попытка атаки будет обнаружена антивирусным решением, атакующие адаптируют используемые средства и методы атаки к защите.

Придумав более изощренный метод, они повторят попытку. Тесты антивирусов показывают, что все решения “пропускают” вирусы.

В серии тестовых испытаний “Real-World Protection Test”, которые проводились лабораторией AV-Comparatives в 2013 г.*, ни одному антивирусному решению не удалось обеспечить защиту от всех угроз. Хотя в тестах использовалась база вредоносных программ с несоизмеримо меньшим числом образцов, чем есть в реальном мире.

3. Антивирусные решения не учитывают контекст событий

Целенаправленные атаки поэтапны. На каждом шаге злоумышленники решают те или иные задачи – от внедрения в информационную систему до уничтожения следов присутствия.

* Источник: *www.av-comparatives.org*

Каждый из шагов сам по себе может не вызвать никаких подозрений – до тех пор, пока они не будут сопоставлены. Антивирусные решения не могут сравнивать между собой состояния систем в разные моменты времени. Антивирусы предназначены для защиты от таких вредоносных программ, которые решают задачи атакующих непосредственно – на первом же шаге.

4. Целенаправленная атака, от которой защитит антивирус, бессмысленна

Антивирусные решения сегодня – самое популярное средство для защиты от киберугроз. Если бы они обладали необходимой надежностью, такого явления, как целенаправленные атаки, не существовало бы вообще. Однако, сегодня их число быстро растет.

5. Вредоносные программы зачастую остаются неизвестны антивирусным лабораториям на протяжении многих лет

Использовавшийся в атаке на иранскую ядерную программу червь Stuxnet в течение нескольких лет не был замечен ни одной антивирусной лабораторией. Мировая общественность узнала о существовании этой вредоносной программы во многом случайно.

Успех всех известных целенаправленных атак, число которых сегодня – тысячи, стал возможен во многом благодаря тому, что то или иное антивирусное решение оказалось против них бессильно.

Обнаружение целенаправленных атак можно реализовать только с помощью специальных решений. Обратитесь за дополнительной информацией на www.cezurity.com

Россия, Санкт-Петербург
ул. Матроса Железняка, 57

+7 812 640 4143
www.cezurity.com