Илья ОСАДЧИЙ
директор по развитию бизнеса,
Тайгер Оптикс

Владимир СОЛОВЬЁВ
руководитель направления
внедрения средств защиты
АО «ДиалогНаука»

ХАНИПОТЫ И DECEPTION

КАК МЕНЯЮТСЯ ТЕХНОЛОГИИ АКТИВНОЙ ЗАЩИТЫ НА ОСНОВЕ КИБЕРОБМАНА

ВВЕДЕНИЕ В ТЕХНОЛОГИИ КИБЕРОБМАНА

Несмотря на существенные усилия, которые компании прилагают к предотвращению успешных взломов, реальность такова, что, если продвинутые киберпреступники нацеливаются на определённую организацию, они найдут способ проникновения во внутренний контур.

Обмануть злоумышленника и заставить его думать, что он получил доступ к ценным данным, — это совсем не новая идея в сфере ИБ. Первая сеть ханипотов была разработана ещё в 1999 году в рамках Honeynet Project. Тогда эта идея была инновационной и результативной, но за последние 20 лет ИТ-инфраструктура компаний стала гораздо сложнее, а злоумышленники набрались опыта.

У современных ханипотов, как и у Deception-технологий нового поколения (таких как, например, система Illusive), есть свои преимущества, и очень важно понимать разницу между этими двумя классами решений — это позволит выбрать оптимальный способ защиты компании от злоумышленников, которые смогли обойти первый эшелон средств защиты и незаметно проникнуть внутрь сети.

ТРАДИЦИОННЫЕ СРЕДСТВА ЗАЩИТЫ ПАСУЮТ ПЕРЕД СОВРЕМЕННЫМИ ХАКЕРАМИ

Злоумышленники всё чаще обходят такие классы решений, как NGFW, песочницы, антивирусы, EDR и XDR — независимо от того, насколько высоко эти решения находятся в квадрантах аналитических компаний и насколько хорошо они настроены. Эксперты рекомендуют считать, что вы уже взломаны, и ваша задача — как можно скорее найти и остановить злоумышленника в своей сети до того, как он нанесёт реальный ущерб.

Поэтому своевременное выявление и грамотное реагирование на активную атаку являются залогом успеха. Ханипоты и Deception-технологии нового поколения заметно отличаются от традиционных средств и подходов к киберзащите. Там, где традиционные продукты стремятся отреагировать на кибератаку и как можно скорее изолировать её, ханипоты и Deception-системы нового поколения занимают более активную позицию, детектируя не атаку, а самих киберпреступников в процессе их работы.

ВЫЧИСЛЯТЬ ХАНИПОТЫ — ПРИВЫЧНОЕ ДЕЛО ДЛЯ ЗЛОУМЫШЛЕННИКОВ

Понимание способностей злоумышленников важно для построения системы защиты, которая сможет их выявить. Вот несколько способов, которыми злоумышленники определяют наличие ханипотов:

- если доступ к системе кажется слишком простым, вероятно, это подделка;
- обычно системы, подключённые к Интернету, не имеют ненужных портов и служб; любое отклонение от этой конфигурации может указывать на ловушку;
- если в системе всё ещё есть настройки по умолчанию, это увеличивает вероятность использования ханипота;
- если на жёстком диске много свободного места или установлено очень мало программного обеспечения, это может быть ханипот;
- если названия папок тривиальны (например, «Зарплаты», «Данные клиентов», «Пароли»), очевидно, что системы нацелены на заманивание злоумышленников.

Все эти сигналы говорят злоумышленникам, что система может быть ненастоящей.

DECEPTION-ТЕХНОЛОГИИ СРЫВАЮТ ПЛАНЫ ЗЛОУМЫШЛЕННИКОВ ПО ВСЕЙ СЕТИ

Атаки с использованием социальной инженерии и нацеленного фишинга служат примером того, как можно обойти любые классы решений, в том числе ханипоты. Многие современные атаки начинаются с того, что пользователю доставляют «приманку», например фишинговое письмо, которое он открывает на компьютере, что позволяет вредоносному ПО проникнуть во внутреннюю сеть, а злоумышленнику — перейти к планированию и выполнению следующего этапа атаки.

Ханипоты не способны взаимодействовать с целенаправленной фишинговой атакой так, как это делают пользователи. Следовательно, ханипоты не смогут спровоцировать и выявить атаку, использующую такой вектор. В отличие от ханипотов, обманные технологии нового поколения могут автоматически изменять обманную среду, не оставляя её статичной, как и подобает настоящей сети, в которой пользовательские и сетевые данные естественным образом меняются. При этом Deception-технологии выявляют злоумышленника всего за три или четыре его шага по сети, даже если обманные элементы развёрнуты не на каждом узле.

Практический опыт внедрений авторов статьи показывает, что даже непосредственные администраторы систем киберобмана не всегда могут определить, какие артефакты реальны, а какие являются результатом работы Deception-систем

Практический опыт внедрений авторов статьи показывает, что даже непосредственные администраторы систем киберобмана не всегда могут определить, какие артефакты реальны, а какие являются результатом работы Deception-систем.

Технологии обмана нового поколения дают пользователям мощную функциональность обнаружения атак и сбора форензики в реальном времени, практически без ложных срабатываний, а атакующие никогда не узнают, что они находятся под наблюдением. Ханипоты тоже эффективны при поимке злоумышленников, но они обладают гораздо меньшей степенью обнаружения реальных угроз, генерируют гораздо больше ложных срабатываний и не предоставляют форензику с реальных узлов, используемых злоумышленниками для атаки.

RED TEAM ПОДТВЕРЖДАЮТ: ТЕХНОЛОГИИ КИБЕРОБМАНА ПРЕУСПЕВАЮТ ТАМ, ГДЕ ХАНИПОТЫ НЕ СПРАВЛЯЮТСЯ

В недавних параллельных тестах Red Team ханипоты продемонстрировали сравнительно низкие показатели обнаружения, но высокие издержки на обслуживание и управление. Ханипоты не предоставляют контекста, они одномерны, и их сложно масштабировать в динамической среде.

Обманные технологии нового поколения были разработаны с учётом современного ландшафта угроз. В тестах Red Team эти технологии получили высокие оценки по всем показателям:

- участники Red Team сообщают, что обойти современные технологии киберобмана крайне сложно. Попытки горизонтального продвижения Red Team по сети генерировали тысячи алертов. Технологии киберобмана позволили легко отследить траекторию атаки и не дали Red Team достигнуть конечной цели;
- киберпреступники компрометируют системы, горизонтально перемещаясь от одного узла к другому. Защитные обманные технологии обнаруживают горизонтальное движение на ранних этапах, собирают данные форензики в реальном времени и составляют «портрет» атакующего;
- большое внимание уделяется векторам атаки злоумышленника, благодаря которым их можно застать врасплох: приманки появляются там, где они не могли бы появиться при использовании ханипотов, поэтому у атакующих практически нет возможности узнать, что они действуют по фальшивому сценарию.

БОЛЬШЕ МЁДА, МЕНЬШЕ ДЁГТЯ: ЛЁГКИЕ И УДОБНЫЕ ТЕХНОЛОГИИ КИБЕРОБМАНА

Подходы ханипотов и Deception-технологий значительно различаются как с точки зрения злоумышленника, так и с точки зрения специалиста по ИБ. Ханипоты — это статические системы, которые устанавливаются в выбранной подсети. Они действуют как своего рода песочницы, пытаясь заманить злоумышленников наличием конфиденциальных данных, а затем отслеживая их действия.

С другой стороны, Deception-технологии представляют собой «королевство кривых зеркал». Ложная информация оказывается повсюду на пути злоумышленников, которые используют её на стадии горизонтального продвижения. Злоумышленники методичны — они собирают данные, анализируют их и рассчитывают свой следующий шаг, неустанно продвигаясь по сети.

Обманные технологии Illusive учитывают такую методичность злоумышленников и извлекают из неё пользу, органично вплетая искусно подобранные «приманки» в реальную инфраструктуру компании, привлекая хакеров, уведомляя специалистов по ИБ и блокируя атаку. При этом компании могут не только останавливать атаки до того, как нанесён реальный ущерб, но и получать критически важную информацию о них в виде форензики, которая может пригодиться в расследованиях.

ЗАКЛЮЧЕНИЕ

Архитектура с применением ханипотов была передовой технологией для своего времени. Она заложила основу для более проактивного подхода к киберзащите и позволила держать злоумышленников на безопасном расстоянии. Однако современные киберпреступники уверенно обходят традиционные СЗИ, при этом избегая ханипотов. Очевидно, что компании, которые хотят защищаться от продвинутых и нацеленных атак, больше не могут фокусировать все свои ресурсы только на этих системах защиты.

* * *

Организациям нужно внедрять и продукты, направленные на внутреннюю поверхность атаки, например, такие как Deception-технологии Illusive. Такая превентивная технология позволяет выслеживать и блокировать злоумышленников, обошедших первую линию обороны, что является важным шагом на пути к современной системе кибербезопасности.