Обман и сбой

Как специалист по IT-безопасности, вы потратите много времени на то, чтобы не дать злоумышленникам получить доступ к вашим системам. Но и свои знания и приемы безопасности вы сможете использовать для создания обмана и срыва тех самых злоумышленников.

Один из способов обеспечить этот обман - использовать приманку. Приманка - это способ привлечь злоумышленников в вашу систему и уметь держать их в этих системах, чтобы вы могли видеть, какие методы безопасности они пытаются использовать против вас. В большинстве этих случаев, конечно, злоумышленник на самом деле является автоматизированным процессом. И вы пытаетесь увидеть, какой тип автоматизации используется и какие системы они пытаются атаковать.

Эти приманки - это виртуальный мир, который эффективно привлекает эти автоматизированные системы или злоумышленников. И они проводят все свое время, пытаясь идентифицировать или атаковать системы, которые на самом деле не являются частью ваших производственных процессов. Если вы хотите построить свой собственный приманку и виртуальный мир, вы можете сделать это, используя ряд коммерческих пакетов программного обеспечения с открытым исходным кодом.

Это также создает некоторую гонку между созданием виртуальных миров, которые в большинстве случаев не являются производственными системами, и злоумышленниками, которые пытаются определить, являются ли эти системы реальными системами или они заперты внутри приманки. По мере того, как злоумышленникам становится лучше идентифицировать приманку, мы увеличиваем сложность и интеллект наших приманок, чтобы сделать их гораздо более реалистичными.

Очень принято, собственно, объединять ряд таких виртуализированных приманок в гораздо более крупные инфраструктуры, которые мы называем сотами. Эти соты могут состоять из рабочих станций, серверов, маршрутизаторов, межсетевых экранов и всего остального, чтобы вся инфраструктура выглядела для злоумышленника немного более реальной. Как только вы объедините всех этих меньших приманок в одну гораздо большую сотовую сеть, вы теперь создали гораздо более правдоподобную среду и, надеюсь, такую, которая будет держать нападающих очень занятыми. Если вы хотите узнать больше о техниках и технологиях, которые мы используем сегодня для создания этих приманок и сот, вы можете посетить projecthoneypot.org.

Мы можем даже спуститься на уровень файлов и создать файлы меда. Это файлы, которые имеют поддельную информацию, или это могут быть файлы, которые кажутся очень важными или содержат конфиденциальную информацию. Например, у вас может быть файл меда под названием passwords.txt, который, конечно, на самом деле не содержит паролей к вашим системам. Но злоумышленник этого не знает. И они могут счесть этот файл очень привлекательным и потратить много времени на просмотр информации, содержащейся в этом медовом файле.

В вашей обычной производственной сети никто не должен получать доступ к этим файлам меда. Таким образом, если кто-то получает доступ к файлу и открывает или просматривает информацию, вы можете отправить оповещения или сигналы тревоги обратно на станцию управления, чтобы вы знали, что в медовых файлах ковыряется кто-то, кого, вероятно, не должно там быть.

И еще одним видом данных, который мог бы помочь выявить проблемы с данными, которые выходят в открытый доступ, был бы медовый знак. Honeytokens - это немного отслеживаемых данных,

которые вы бы добавили в свою сотовую сеть. Итак, если эта информация скопирована и распространена, вы точно знаете, откуда она взялась.

Например, вы можете разместить учетные данные API в общедоступном облаке, чтобы узнать, кто может прийти и получить эти учетные данные. Конечно, эти учетные данные API не являются реальными полезными учетными данными API. Вы их просто выдумали и поместили в файл, к которому потом обращается злоумышленник.

Или у вас может быть файл, содержащий несколько поддельных адресов электронной почты. Поскольку эти адреса электронной почты никем не используются, вы можете постоянно отслеживать появление этих адресов где-либо еще в Интернете. И если они это сделают, вы сможете точно увидеть, кто это опубликовал, что может дать вам информацию о том, кто может атаковать вашу сеть.

И, конечно же, эти медовые токены могут представлять собой данные любого типа, которые вы можете фальсифицировать и поместить в область, которую злоумышленник сможет найти. Это могут быть записи базы данных, файлы cookie браузера, пиксели на веб-странице или что-то еще, что вы можете отслеживать, если они будут размещены где-то еще в Интернете.