УДК 004.05

Р. В. Стрельников

SOC. НАЧИНАЕТ И ПРОИГРЫВАЕТ

Проанализированы основные недостатки и проблемы противостояния ситуационного центра мониторинга информационной безопасности (Security Operation Center) методам социальной инженерии.

The paper analyzes the main shortcomings and problems of opposition to the methods of social engineering a situational center for monitoring information security (Security Operation Center).

Ключевые слова: SOC, центр мониторинга информационной безопасности, информационная безопасность, социальная инженерия

Keywords: SOC, information security monitoring center, information security, social engineering

Введение

Продолжая тему, затронутую в изданной ранее статье [1], рассмотрим типичную ситуацию. Есть центр мониторинга некой финансовой организации. Произошел случай вывода средств клиента. Заявление от клиента поступило в службу безопасности. Начинается расследование.

Шаг первый — звонок клиенту:

— Сообщите пожалуйста код, который вам пришел через СМС.

Клиент, знающий основы информационной безопасности (ИБ) в финансовой сфере:

— Я вам сообщать пароль (код) не буду.

Шаг второй — убеждение:

— И правильно делаете, мы просто проверили вашу осведомленность в области защиты. Перевожу вас на автоматического помощника, чтобы закончить процесс.

Клиент не сообщал код собеседнику по телефону, как его информировали в брошюре, выданной в кредитной организации.

Шаг третий — техническая подготовка злоумышленника. Разговор переводится на автоответчик. Металлический голос бота подсказывает:

— Наберите в тоновом режиме 6 цифр кода, полученного посредством СМС.

Так на практике срабатывают методы социальной инженерии (СИ).

SOC и СИ

Как происходит типичная эволюция информационной системы? Есть некая инфраструктура, которая развивается, зреет, повышает уровень своей информационной безопасности. В результате возникает центр мониторинга, который защищает от киберугроз. Все прекрасно работает. Однако…

Вестник Балтийского федерального университета им. И. Канта.
Сер.: Физико-математические и технические науки. 2021. № 1. С. 26 – 30.

Большинство команд ИБ приоритетно фокусируется на таргетированных угрозах, наиболее актуальных для финансового сектора. Такие атаки реализуются с использованием технических методов, а их доля в общем числе атак составляет не более 5 %. Иными словами, сотрудники SOC фокусируются лишь на малой части кибератак.

Это связано с тем, что технические векторы много проще отследить, проще настроить сценарии реагирования. К тому же высокой квалификации специалистов для выявления такого рода атак не требуется.

Однако в реальности большинство таргетированных атак сочетают в себе векторы нетехнические (социальной инженерии в том числе) и технические.

По факту СИ:

— всегда действует в зависимости от уровня зрелости ИБ;

— представляет собой огромное количество нетехнических и технических векторов атак и стратегий;

— может являться составной частью стратегии кибератаки;

— всегда таргетирована и предполагает цель (ориентирована на организацию, конкретного сотрудника и т. д.);

— может использовать непредсказуемые сценарии.

Угроза ИБ может быть реализована без вектора кибератаки. За последний год много данных утекло не по техническим каналам. Таким образом, непредсказуемость действий социальных инженеров предполагает невозможность построения вектора атаки. То есть кибератаки с применением методов СИ в большинстве своем являются успешными и невидимыми для SOC. Коммерческим организациям это наиболее очевидно, именно поэтому в последнее время происходит такое сокращение количества SOC. Технические средства не поспевают за талантами социальных инженеров, и финансовые вложения в создание и развитие SOC становятся менее оправданными.

Однако в методах кибератак с использованием СИ можно выявить закономерность и цикличность, как и в любой атаке ИБ, которая зависит от подготовки атакующего: разведка — сбор информации — извлечение информации — предлог — манипуляция и обман — убеждение — определение цели.

Техники социальной инженерии

Основные (некоторые) техники СИ:

— первичная обработка (загрузка информации, фоновая обработка);

— манипуляция и обман (жесты и мимика, сомнение, наказание, шантаж, комплименты, противоречия, колебания, повышение предсказуемости, отвлечение, контроль окружающей обстановки, слабость, работа по типу мышления, работа с микроэкспрессиями, фиксация изменения поведения, невербалика);

— нейролингвистическое программирование (воздействие на восприятие, воздействие на убеждения, воздействие интонацией, метамоделирование, воздействие звуками, воздействие вербальными образами, «загрузка»);

— предлоги (махинации с телефонами, использование личностных интересов, применение диалектов);

— извлечение информации (волонтерство, техника «хорошего» слушателя, подтасовка данных, апеллирование к эго, искренность и заинтересованность, лесть, игнорирование, алкоголь, техника управляемых вопросов);

— влияние (последовательный переход, уступки, искусственный дефицит, симпатия, услуга за услугу, социальное, юридическое и организационное влияние, подарки, влияние авторитетом, подмена реальности).

Со многими из перечисленных техник можно бороться превентивными мерами. Однако есть целый пласт атак, которые действуют на уровне подсознания. Среди экспертов ИБ существует дискуссия на эту тему, поэтому приведу факты:

— в подсознании сосредоточено от 95 до 99 % вычислительной мощности мозга;

— в подсознании сосредоточено приблизительно 95 % когнитивной деятельности;

— сознание ограниченно;

— скорость распространения импульса в сознании почти в 1000 раз меньше, чем в подсознании;

— количество бит информации в секунду в подсознании больше на 400 млрд;

— глубина памяти в сознании составляет до 20 секунд и бесконечна в подсознании;

— подсознание оперирует настоящим временем;

— 99 % решений мы принимаем подсознательно.

Исходя из изложенных фактов и учитывая скорость роста возможностей искусственного интеллекта, использование машинного обучения в системах слежения за человеком, изучение карты быта человека, поведенческих характеристик и карты человеческого сознания в итоге, высока вероятность того, что в скором будущем станет возможным «подобрать ключ» к любому человеку. Если при воздействии на сознание оно может сопротивляться осознаваемому воздействию (постсознательные процессы), то подсознание без сопротивления запускает целезависимые (предсознательные) процессы. В результате «уязвимости» мозга на порядки превышают уязвимости программного обеспечения.

Техническое оснащение социальных инженеров также прогрессирует, делая возможными, например, подделку интонаций и синтезирование тембра голоса начальника при звонке подчиненному с помощью программных средств.

Очевидно, что количество угроз с использованием методов СИ в будущем только возрастет.

Почему SOC проигрывает?

Почему финансовые средства, вложенные в центры мониторинга, пропадают?

Используя модель SANS Institute, можно увидеть, что каким бы технически оснащенным ни был центр мониторинга, какая бы киберза-

щита ни была построена, при реальном мотиве Red Team может сделать с защищенной информацией что угодно (первый и второй уровни) [2].

Но даже с учетом роста технической подготовки SOC не представляется возможным фиксировать намерения злоумышленников. Поэтому создать матрицу по атомарным техникам технических векторов предатаки касательно СИ невозможно [3].

Хорошо подготовленный социальный инженер, предполагая наличие грамотных специалистов центров мониторинга, будет максимально обходить «опасные места» для своей атаки, нивелировать этап сбора информации (делая, например, фотографию информации с экрана).

Для SOC борьба с пользователями защищаемой информационной структуры меняет модель. Причем остается всего два-три этапа до фиксации действий злоумышленника. А с учетом того, что политики безопасности по умолчанию настроены более щадящее по отношению к внутренним сотрудникам (пользователям), атака с использованием СИ становится успешной.

При низкой зрелости системы информационной безопасности, когда предполагается, что атакующий будет реализовывать атаку при помощи технических векторов, методы СИ могут не требоваться в принципе. Успешные работы команд пентестеров доказывает этот факт.

В более зрелых системах ИБ злоумышленнику будет сложнее выстраивать стратегию атаки, то есть происходит удорожание реализации атаки, использующей технические векторы. В данном случае применение методов СИ существенно упростит реализацию. Стоит отметить, что в случае применения СИ происходит деанонимизация и риск раскрытия физической личности злоумышленника возрастает. В зависимости от цели (финансовая, шпионаж, дестабилизация работы, промышленная авария) меняется и риск злоумышленника.

Как же действовать при нетехнических векторах атак?

Первичный вектор (выявление атакующего) предполагает информированность сотрудников. Вторичный (выявление атакуемого) предполагает анализ различных событий технических систем (UAM, DLP, UBA, TBA, EDR, MDM, Threat hunting).

Борьба с СИ

В 2017 г. в России произошло знаковое событие, на которое мало кто обратил внимание: Банк России совместно с Министерством образования утвердил «дорожную карту» повышения финансовой грамотности населения страны в области информационной безопасности. Как показывает практика утечек информации, краж финансовых средств, самым слабым звеном в цепи защиты информации является человек. И обучать методикам детектирования использования злоумышленниками СИ необходимо со школьной скамьи.

Однако наряду с повышением грамотности в вопросах ИБ скачкообразно растет количество атак на кредитные организации с использо-

ванием СИ. Не стоит полагать, что параллельно создаются и развивается аналогичные школы злоумышленников, но методы и сценарии реализации атак становятся все изощреннее.

Многие кредитные организации, имея собственный SOC, разрабатывают программы повышения квалификации сотрудников, направленные в том числе на борьбу с социальными инженерами команд злоумышленников. В некоторых организациях проводятся тренировки по целевому антифишингу. Но даже в условиях осведомленности сотрудников, по статистике, от 10 % фишинговых атак являются успешными при грамотном предоставлении информации.

Концепцию Zero Trust в отношении сотрудников защищаемой SOC информационной инфраструктуры трудно реализовать на практике. А такой способ защиты, как непрерывная верификация-аутентификация пользователей, слишком дорог в реализации. Остальные методы защиты SOC будут, к сожалению, давать сбой при столкновении с методами социальной инженерии.

Список литературы

1. *Стрельников Р. В.* SOC. Неэффективность внедрения // Вестник Балтийского федерального университета им. И. Канта. Сер.: Физико-математические и технические науки. 2019. № 4. С. 81—85.

2. *Muniz J., McIntyre G., Al Fardan N.* Security Operations Center: Building, Operating, and Maintaining your SOC // Cisco Press. Nov 2, 2015. URL: http://www.ciscopress.com/store/security-operations-center-building-operating-and-main taining-9780134052076 (дата обращения: 15.09.2020).

3. *SANS* Institute. URL: https://www.sans.org (дата обращения: 15.09.2020).

Об авторе

Роман Владимирович Стрельников — техн. директор, компания «Информационная безопасность», Россия.

E-mail: strelnikov.roman@gmail.com

The author

Roman V. Strelnikov, Technical Director, «Infobez39.ru», Russia.

E-mail: strelnikov.roman@gmail.com