1) Часто ли злоумышленники закрепляются через редактирование DACL объектов AD? Например, AdminSDHolder. Точнее, часто ли используют такие техники? Пусть даже не для закрепления.

Злоумышленники используют эту технику, например, для обхода средств защиты в инфраструктуре на базе Windows — File and Directory Permissions Modification: Windows File and Directory Permissions Modification, а для Linux или macOs — File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification, но в рамках пентестов ее не применяли. К примеру, операторы программы-вымогателя BlackCat используют в своих атаках технику File and Directory Permissions Modification: Windows File and Directory Permissions Modification (T1222.001).

2) Можете ли подсказать действенный способ защиты от почтовых MITM-атак?

Злоумышленники могут провести атаку типа man in the middle, нацеленную на почтовый сервис, если у почтового клиента неправильно выполняется проверка подлинности SMTP-сервера в режиме SSL/TLS, то есть письма отправляются по незашифрованному SMTP. Для того чтобы защититься от такой атаки, следует включить TLS на почтовом сервере. Протокол SMTP при этом шифруется на транспортном уровне, заключая SMTP в соединение TLS, и преобразуется в SMTPS.

Клиенты, использующие SMTPS для отправки сообщений, защищены от MITM-атаки, но не защищены от спуфинга домена, фишинга и других популярных атак на корпоративные почтовые сервисы. Для того чтобы выстроить систему защиты от таких атак, следует настроить:

- Sender Policy Framework (SPF) — информирует, от какого сервера происходит отправка сообщения по электронной почте.
- Domain Keys Identified Mail (DKIM) — добавляет к сообщениям цифровую подпись.
- Domain-based Message Authentication Reporting and Conformance (DMARC) — аутентифицирует сообщения, согласовывает возможности SPF и DKIM.
- Brand Indicators for Message Identification (BIMI) — отображает логотип бренда в почтовых сообщениях.

3) Часто ли при пентесте вы попадаетесь на ханипоты? Если факты попадания на ханипоты были, то почему их не заметили?

Да, иногда попадаемся. Ведь суть ханипотов в том, чтобы выглядеть как легитимные узлы. Наличие ханипотов в инфраструктуре вынуждает злоумышленника предпринимать дополнительные действия в системе и удлиняет цепочку атаки; таким образом, у специалиста по информационной безопасности появляется дополнительное время на обнаружение атаки.

4) Какие фишинговые атаки, по вашему мнению, самые эффективные (если можно, с примерами и техниками)?

Сейчас наиболее эффективны атаки, в которых используется техника HTML Smuggling. Злоумышленник скрывает вредоносный скрипт внутри специально сформированной HTML-страницы и отправляет пользователю эту страницу или ссылку на нее. Когда пользователь открывает HTML-страницу, его браузер локально обрабатывает скрипт и

компилирует вредоносное ПО прямо на устройстве пользователя. Такая техника позволяет обойти стандартные средства защиты периметра, например, веб-прокси, почтовые шлюзы, потому что зачастую они проверяют только подозрительные вложения или трафик на основе подписей и шаблонов.

Для защиты от таких атак мы рекомендуем использовать песочницы, анализирующие почтовые вложения на предмет вредоносных скриптов для HTML Smuggling, а также средства защиты конечных узлов — EDR (или расширенную версию, XDR).

Узнать больше об актуальных атаках с использованием социальной инженерии можно посмотрев выступление Константина Полишина на Standoff Talks.

Также рекомендуем обратить внимание на наш топ-10 тем, используемых в фишинговых рассылках.

5) **Какие бывают основные ошибки в защите сети Wi-Fi?**
   Основными ошибками можно назвать:
   - Использование простого пароля для подключения к беспроводной сети.
   - Использование ненадежных механизмов шифрования.
   - Использование стандарта WPS, так как методом перебора можно получить ПИН-код и таким образом подключиться к внутренней сети.
   - Отсутствие разделения сети на гостевую и корпоративную. Это может привести к тому, что сотрудники компании станут использовать общедоступную сеть для передачи конфиденциальной информации, а злоумышленники смогут эти данные перехватить.
   - Отсутствие изоляции пользователей в гостевой сети позволит злоумышленнику атаковать сотрудников компании, прослушивать трафик и перехватывать конфиденциальную информацию.
   - Использование протокола PEAPv0/EAP-MSCHAPv2 без проверки сертификата точки доступа со стороны клиента. В таком случае злоумышленник может проводить атаки с поддельной точки доступа, направленные на перехват данных, которые используются в запросах на аутентификацию. На основе этих данных можно методом перебора получить хеш пароля.
   - Отсутствие wireless intrusion prevention system (WIPS).

Еще одна ошибка, которую могут допустить специалисты по информационной безопасности, — отказ от проведения проверок защищенности сети Wi-Fi. В качестве таких проверок могут выступать как внутренние аудиты, так и анализ защищенности силами сторонней компании.