Атака ближайшего соседа нарушила привычные меры защиты.

В 2022 году была обнаружена новая сложная кибератака, которая стала одной из самых нестандартных за последнее время. Злоумышленники использовали уникальную технику, получившую название «Атака ближайшего соседа». Эта методика позволяла атакующим с помощью сетей Wi-Fi проникать в корпоративные сети компаний, находящихся в физической близости друг к другу, оставаясь при этом на значительном расстоянии от своих целей.

Для реализации атаки использовались ранее скомпрометированные учетные данные, которые добывались через атаки на сервисы с общедоступным доступом. Основная цель — подключение к корпоративной Wi-Fi сети, не защищенной многофакторной аутентификацией (MFA (многофакторная аутентификация) — это метод защиты аккаунта, который требует предоставления нескольких способов аутентификации для получения доступа к учетной записи. Вместо использования только логина и пароля, пользователь должен предоставить дополнительные подтверждения, такие как код, отправленный на телефон или использование биометрических данных, таких как отпечаток пальца или сканирование лица. Это делает процесс взлома аккаунта сложнее и повышает уровень безопасности.

 2FA (двухфакторная аутентификация) также относится к MFA. Только термин MFA не ставит ограничений на количестве вспомогательных методов аутентификации, а в 2FA таких методов ровно два.» data-html=»true» data-original-title=»MFA» >MFA). Несмотря на защиту интернет-ресурсов целевой компании, корпоративная Wi-Fi сеть оказалась уязвимой, требуя лишь корректного логина и пароля для подключения.

Злоумышленники действовали поэтапно . Сначала компрометировались системы одной из компаний, находящихся поблизости от цели, после чего искались устройства с доступом к Wi-Fi. Такие устройства, называемые двухсредными, подключались одновременно как к проводным, так и беспроводным сетям. Через них злоумышленники входили в Wi-Fi сети соседних организаций. Используя метод цепной компрометации, атакующие добирались до своих целей, обходя системы безопасности.

Ключевым элементом атаки стали стандартные инструменты Windows, такие как PowerShell и утилита Cipher.exe, которая позволяла надежно удалять файлы без следов. В процессе атак фиксировались попытки извлечения активной базы данных доменов и других критически важных данных.

Расследование показало, что атакующие также использовали уязвимость нулевого дня в Windows для эскалации привилегий. Уязвимость, ранее не известная, позволяла

злоумышленникам углублять свои позиции в сети жертвы.

Этот инцидент подчеркнул необходимость пересмотра подходов к безопасности корпоративных Wi-Fi сетей. В условиях растущих угроз такие сети требуют защиты на уровне других критически важных сервисов, включая многофакторную аутентификацию или сертификаты. Эксперты также рекомендуют разделение проводных и беспроводных сетей, мониторинг аномального поведения сетевых устройств и внедрение строгих правил для сетевого трафика.

Пример данной атаки показал, что злоумышленники готовы использовать сложные и многослойные подходы, чтобы обойти традиционные меры безопасности. Такие случаи подтверждают необходимость усиления контроля за всеми компонентами корпоративной инфраструктуры.