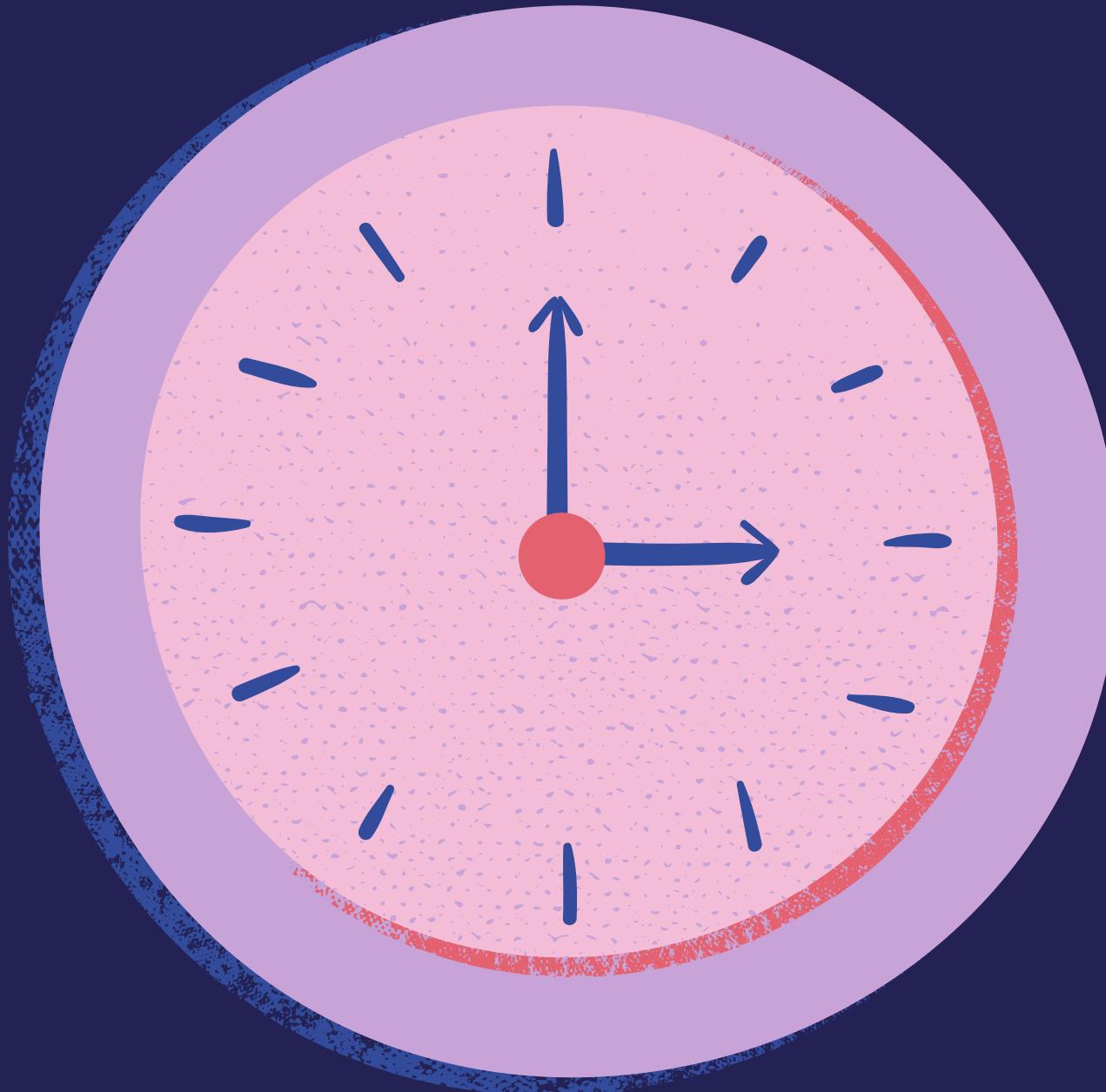


Взломы крупных компаний

Uber (2022)

- Был взломан внутренний доступ сотрудников
- Хакер получил доступ к Slack, GitHub и внутренним системам
- Использовалась атака MFA Fatigue (спам подтверждениями входа)

КАК ВЗЛОМАЛИ?



- Точка входа: аккаунт подрядчика/сотрудника
- Uber официально писал, что был скомпрометирован аккаунт внешнего подрядчика (EXT).
- Украденный пароль + попытки входа
- Злоумышленник, по версии Uber, получил пароль (вероятно, из-за заражения личного устройства вредоносным ПО и/или утечки учётных данных) и начал пытаться войти.
- MFA сначала остановила вход, но “сломали человека”, а не систему
- Когда включена двухфакторная защита, при входе на телефон приходят запросы подтверждения. Атака MFA Fatigue (она же push-bombing) – это когда человеку отправляют много запросов, чтобы он в какой-то момент “устал” и нажал “Approve”, либо поверил “лжесаппорту”.
- Дальше – “разрастание доступа” по внутренним сервисам
- После входа в корпоративную среду часто открывается доступ к внутренним инструментам (в их числе могут быть Slack, репозитории кода, панели админов и т.д.). В новостных разборках отмечалось, что злоумышленник публиковал сообщения в Slack и заявлял о широком доступе к внутренним системам.



Capital One

Взломан банковский сервис

Утекли данные более 100 миллионов клиентов

Причина: ошибка в настройках сервера и облака



КАК ВЗЛОМАЛИ?

- Не “взлом банка”, а ошибка в облачной конфигурации + уязвимость веб-компонентта
- Суть: данные лежали в облачной инфраструктуре, и был путь, который позволил получить доступ к ним из-за ошибки настройки и уязвимости на стороне веб-защиты/приложения.
- SSRF: сервер “сам” делает запросы туда, куда не должен
- В публичных разборах фигурирует техника SSRF (Server-Side Request Forgery): злоумышленник заставляет сервер выполнить внутренний запрос и тем самым получить доступ к служебным данным/учётным данным внутри облака.
- Добыли временные “ключи” доступа и скопировали данные
- После получения внутренних облачных полномочий (credentials) стало возможно копирование данных из хранилищ.
- Масштаб утечки
- Публично сообщалось о примерно 106 млн затронутых заявителях/клиентах (США и Канада).

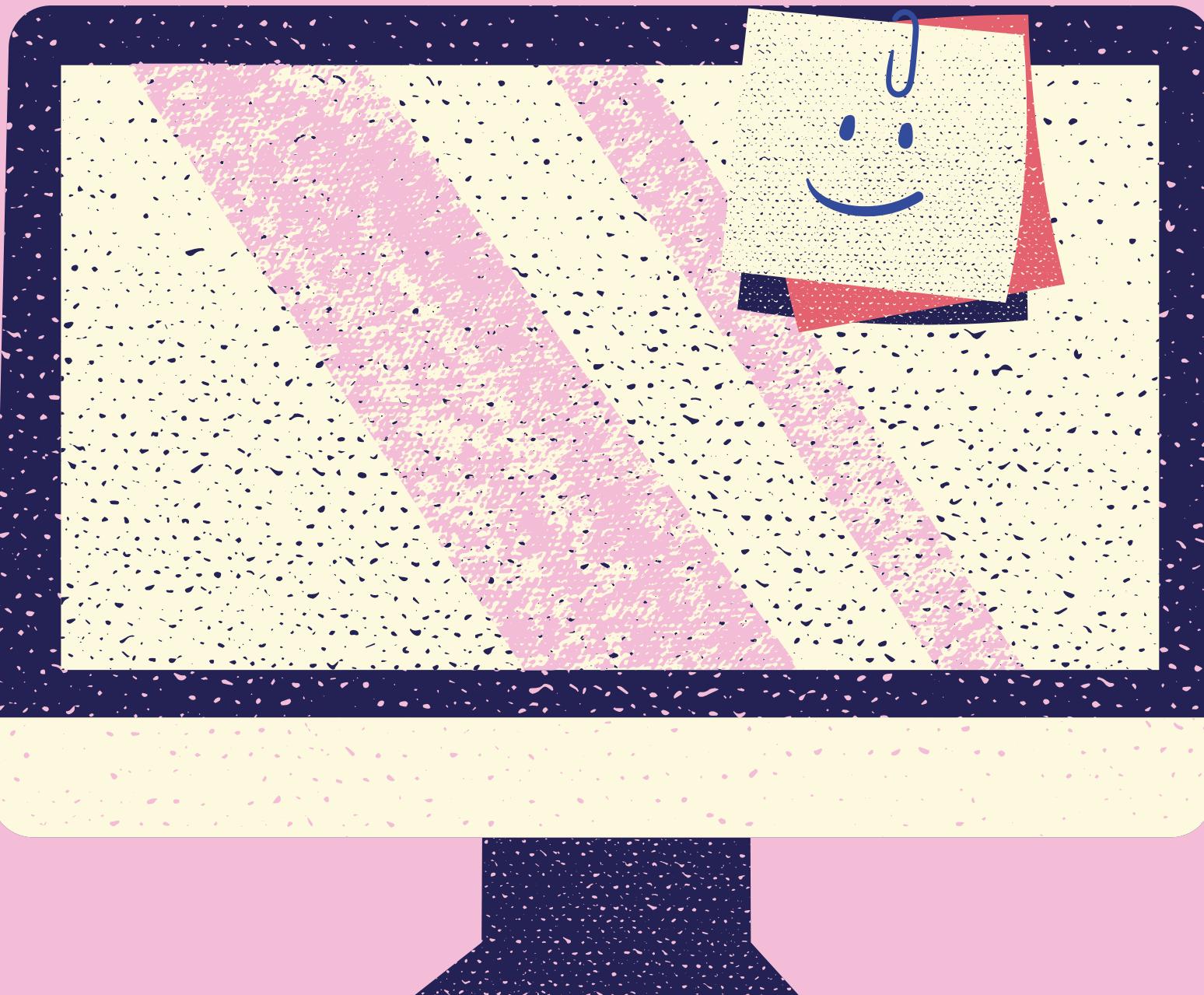
Epic Games/Fortnite

Что случалось:

- Массовые взломы аккаунтов игроков
- Продажа аккаунтов, скинов

Причина:

- Слабые пароли
- Отсутствие 2FA у пользователей



EpicGames/Fortnite

- Самый популярный проект — Fortnite, вышедший в 2017 году и собравший миллионы игроков по всему миру.
- В 2017–2019 годах часто происходили взломы аккаунтов игроков Fortnite, а не серверов Epic Games.
- Аккаунты были целью из-за редких скинов, V-Bucks и привязанных платёжных данных.
- Основные причины взломов: слабые пароли, использование одного пароля на разных сайтах, отсутствие двухфакторной защиты (2FA).
- Распространённым способом был фишинг — поддельные сайты с обещанием «бесплатных V-Bucks».
- После этого Epic Games усилила безопасность, ввела 2FA и систему уведомлений о входах.

Спасибо за внимание!

Защищайте свои аккаунты и пароли!