**Рекомендации клиентам о необходимых действиях в период повышенного уровня угрозы проведения компьютерных атак.**

Компьютерная атака – целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств.

**Основные виды компьютерных атак:**

Заражение вредоносным кодом (компьютерные вирусы): устанавливаются на компьютеры и распространяются на другие файлы в системе. Распространяются через внешние жесткие диски, или посредством определенных интернет-сайтов или как вложения по электронной почте. Цель заразить множество файлов и других систем.

Перехват управлением компьютером: злоумышленники получают доступ в систему с использованием различного набора программ управления и полностью завладевают управлением компьютера. Относятся к числу наиболее опасных компьютерных атак. Злоумышленник может получить больше контроля над системой, чем владелец системы.

Парольные атаки: злоумышленники получают доступ к компьютеру и ресурсам сети путем получения пароля управления. В результате злоумышленники меняют конфигурацию сети и в некоторых случаях даже могут удалить данные. Кроме того, данные могут передаваться в разные сети.

Отказ в обслуживании DoS (Denial of Service) – это перегрузка сети паразитным трафиком (т.н. флуд), когда на атакуемый ресурс отправляется большое количество злонамеренных запросов, из-за чего полностью «забиваются» все каналы сервера или вся полоса пропускания входного маршрутизатора. При этом передать легитимный трафик на сервер становится невозможно. Запросов может быть так много, что сервер не успевает их обрабатывать и переходит в режим «отказа в обслуживании». На жаргоне специалистов это называется «положить сервер».

Основной и наиболее активной угрозой для клиентов Банка, юридических лиц и индивидуальных предпринимателей, является воздействие на персональные компьютеры, используемые для доступа к системам дистанционного банковского обслуживания (ДБО).

**Что делать, если атака состоялась**

Есть действия, которые необходимо совершить вне зависимости от того, с каким конкретным видом атаки вы столкнулись. Действовать надо быстро, чтобы избежать заражения по цепочке внутри корпоративной сети.

1. Выявите и изолируйте зараженные компьютеры от корпоративной сети. Используйте ваши средства защиты от вредоносного кода (антивирусные программы). Проверьте файлы с записями о событиях, в которые заносится вся информация о работе сервера или компьютера, о действиях программы или пользователя, сведения об ошибках. Отключите зараженные компьютеры от сети. Также обратите внимание на расширения ваших персональных файлов: если они изменились или вместо них появилось множество других с неизвестными именами, то компьютер заражен.
2. Постарайтесь определить первоисточник заражения и уязвимость, которую использовали злоумышленники. Чаще всего источником заражения становятся письма со спамом, зараженные съемные носители, установка вместе с другим программным обеспечением и взломанные или скомпрометированные веб-страницы. Разобраться, что именно послужило отправной точкой, поможет аудит изменения зашифрованных файлов, чтобы понять, с какого компьютера они шифровались. Этот способ работает при условии, что аудит был заблаговременно включен системным администратором. Выявить причины помогут и специальные организации, которые проводят расследования подобных инцидентов, или — в минимальном объеме — специалисты технической поддержки антивируса, который использовался в компании.
3. Обратитесь за помощью в организацию, специализирующуюся на информационной безопасности: компетенции IT-департамента может не хватить, а время будет упущено.

4. Примите все возможные меры по устранению уязвимости и усилению защитных мер, проведите аудит безопасности и выявите другие возможные бреши в защите.

- создайте резервную копию данных и регулярно ее обновляйте;
- регулярно устанавливайте патчи и обновления вашего ПО;
- уделяйте внимание повышению грамотности сотрудников в вопросах информационной безопасности;
- настройте отображение расширений файлов;
- настройте фильтр EXE-файлов в почте;
- отключите возможность запуска файлов из папок AppData или LocalAppData;
- отключите возможности удаленного управления рабочим столом (RDP) или ограничьте его использование;
- используйте программы для защиты, которым можно доверять;
- используйте восстановление системы, чтобы откатить систему до «чистого» состояния;
- используйте стандартную учетную запись вместо учетной записи администратора.

**Как защититься**

1. Не экономьте на безопасности:

- используйте только лицензионное ПО;
- используйте эффективные средства антивирусной защиты на всех устройствах;
- своевременно обновляйте используемое ПО.

2. Защищайте ваши данные:

- наиболее важные файлы храните не только на жестком диске компьютера, но и на съемных носителях, внешних жестких дисках или в облачном хранилище;
- для повседневной работы в ОС используйте учетную запись без привилегий администратора;
- используйте двухфакторную аутентификацию там, где это возможно, например, для защиты электронной почты.
- 3. Не используйте простые пароли:
- используйте сложные пароли, состоящие из незначащих комбинаций букв, цифр и знаков, длиной не менее 8 символов. Для создания и хранения паролей можно воспользоваться менеджером паролей (защищенным хранилищем с функциями генерации новых паролей);
- не используйте один и тот же пароль для разных систем (для сайтов, электронной почты и др.);
- меняйте все пароли хотя бы раз в полгода, а лучше — каждые два-три месяца.

4. Будьте бдительны:

- проверяйте все вложения, полученные по электронной почте, с помощью антивирусного ПО;
- с осторожностью относитесь к сайтам с некорректными сертификатами и учитывайте, что введенные на них данные могут быть перехвачены злоумышленниками;
- будьте предельно внимательны при вводе учетных данных на сайтах и во время работы с онлайн-платежами;
- не переходите по ссылкам на незнакомые подозрительные ресурсы, особенно когда браузер предупреждает об опасности;
- не переходите по ссылкам из всплывающих окон, даже если рекламируемые компания или продукт вам знакомы;
- не загружайте файлы с подозрительных веб-ресурсов или из других неизвестных источников.