Вопросы и ответы по атакам на систему доменных имен

(См.: Объявление ICANN от 22 февраля 2019 года)

Вопрос: Почему ICANN публикует заявления сейчас?
Ответ: После того как ICANN узнала об атаках (из отчетов масс-медиа и специалистов по безопасности), было важно принять меры, чтобы уведомить об этой ситуации сообщество ICANN и широкую общественность. Это соответствует нашей миссии по обеспечению безопасности и стабильности системы доменных имен (DNS).

Вопрос: О какой атаке идет речь?
Ответ: В общедоступных отчетах говорится о повторяющемся сценарии разноплановых атак, использующих различные методы. Некоторые атаки нацелены на DNS. Они задействуют несанкционированные изменения в структуре делегирования доменных имен, заменяя адреса определенных серверов адресами компьютеров, находящихся под контролем злоумышленников. Этот конкретный вид атаки, нацеленный на DNS, работает, только если не использовать
расширения безопасности системы доменных имен (DNSSEC).

Вопрос: Кто стоит за этими атаками?
Ответ: Имеются противоречивые сведения о том, кто стоит за этими атаками, и зачастую сложно определить, кто конкретно их организует.

Вопрос: Правоохранительные органы расследуют эти атаки?
Ответ: В общедоступных отчетах говорится о том, что правоохранительные органы и органы национальной безопасности во многих странах расследуют эти атаки. Гражданское общество (технические специалисты по обслуживанию DNS, специалисты в сфере кибербезопасности и другие) также активно работает над определением видов использованных атак. Кроме того, оно помогает пострадавшим организациям повысить уровень защищенности их систем.

Вопрос: ICANN пострадала?
Ответ: У нас нет оснований полагать, что системы ICANN были взломаны. В целях обеспечения дополнительной безопасности мы провели проверку систем.

Вопрос: Какие-либо корневые серверы были взломаны?
Ответ: Нет оснований полагать, что хотя бы один из корневых серверов DNS был взломан. ICANN связалась с Консультативным комитетом системы корневых серверов (RSSAC) и обратилась к нему с просьбой провести консультацию с операторами корневых серверов, чтобы подтвердить отсутствие оснований для предположения взлома. На сегодняшний день ни один оператор корневого сервера не уведомил нас об обнаружении взлома.

Вопрос: Насколько распространен этот риск? Сколько доменных имен не защищены?
Ответ: Некоторые атаки задействовали взломанные пароли. Невозможно знать, сколько других паролей могло быть взломано. Поэтому мы призываем всех участников экосистемы DNS использовать надежные пароли, часто их

чередовать, не использовать одни и те же пароли на разных сайтах и при любой возможности пользоваться многофакторной аутентификацией.

Вопрос: Атаки продолжаются? Когда они начались? Когда они закончились?
Ответ: Хотя нам неизвестно о текущих атаках, мы полагаем, что такой риск существует. Мы призываем все организации усовершенствовать свою онлайн-защиту, в том числе реализовать расширения безопасности системы доменных имен (DNSSEC), если они этого еще не сделали. Им также следует убедиться в надежности учетных данных для управления доменным именем и проверить свои системы на признаки взлома, искажения и т. д. Согласно опубликованным отчетам, этот набор атак начался еще в 2017 году.

Вопрос: ICANN рекомендует какие-либо конкретные меры?
Ответ: Да, 15 февраля 2019 года ICANN предложила указанный ниже контрольный список, хотя он не включает все меры, которые можно реализовать для обеспечения полной защиты:

- обязательно проверьте и примените все патчи для устранения ошибок защиты системы;
- проверьте журнал событий на наличие несанкционированного доступа к системам, особенно это касается доступа администратора;
- проверьте системы внутреннего контроля над доступом администратора («корневой доступ»);
- проверьте целостность каждой записи DNS и историю изменений этих записей;
- используйте достаточно сложные пароли, особенно, что касается их длины;
- не сообщайте свои пароли другим пользователям;
- не храните и не передавайте свои пароли в виде незашифрованного текста;
- регулярно и периодически меняйте пароли;
- обеспечьте исполнение политики блокировки паролей;
- убедитесь, что записи зоны DNS подписаны при помощи DNSSEC, а ваши резолверы DNS проводят валидацию DNSSEC;
- по возможности активируйте многофакторную аутентификацию для всех систем, особенно это касается доступа администратора;
- по возможности настройте для своего домена электронной почты политику DMARC с SPF и/или DKIM и обеспечьте выполнение таких политик другими доменами в системе вашей электронной почты.

Вопрос: Реализация DNSSEC защищает конечных пользователей?
Ответ: Да. Реализация DNSSEC защитит конечных пользователей от конкретных видов атак. Некоторые системы, которые были задействованы для организации атак, использовали доменные имена, защищенные DNSSEC, и владельцы этих зон подтвердили, что DNSSEC помогли им смягчить последствия этих атак.