Postmortem сбоя в ДВУ .RU 30.01.24 (18:28 – 21:00 МСК)

Общие сведения:

Сбой произошел в период с 18:28 по 21:00 МСК 30.01.2024 и затронул работоспособность домена верхнего уровня (ДВУ) .RU, вызвав некорректное сопоставление доменных имен в домене .RU с IP-адресами для части аудитории российского сегмента интернета.

Анализ и установленные факты:

Процедура ротации ключа подписи зоны (ZSK) для ДВУ .RU проводится четыре раза в год. При этом используется метод Pre-Publish Zone Signing Key Rollover, который предусматривает наличие двух ключей в системе – старого и нового, но для валидации используется только один.

24 января 2024 была начата плановая смена ZSK.

26 января 2024 новый ZSK был опубликован для распространения его открытой части в рамках глобальной DNS инфраструктуры.

30 января 2024 произошло отключение старого ZSK и активация нового. Однако в результате сбоя конфигурации в системе оказались две пары ключей с одинаковым keytag. Вследствие чего с помощью старого ключа были сгенерированы RRSIG записи, а новый ключ был занесен в зону. В результате RRSIG записи не могли быть валидированы новым ключом.

Хронология развития:

30.01 18:28 – В системе мониторинга обнаружены проблемы после публикации файла зоны, подписанного новым ZSK.

30.01 19:29 – Запуск временного отключения валидации DNSSEC для ДВУ .RU на резолверах Национальной системы доменных имен (НСДИ) для восстановления доступности зоны.

30.01 21:00 – Выполнен возврат к использованию предыдущей версии файла зоны и ключей и возобновление нормального функционирования ДВУ .RU.

31.01 01:07 – Валидация DNSSEC для ДВУ .RU вновь активирована на резолверах НСДИ.

Корневая причина:

Коллизия ZSK с одинаковыми keytag в системе вследствие сбоя программного обеспечения.

Хронология устранения корневой причины сбоя:

31.01 17:21 – Запущено распространение обновлённого файла зоны .RU по DNS серверам.

31.01 17:58 – Публикация файла зоны переведена в штатный режим работы.

Меры по недопущению события в дальнейшем:

В хранилище ключевой информации проведен комплекс мер, направленный на устранение возникших проблем и нормализацию данных, обеспечивающих работу с новым ключом ZSK.

Заключение:

Сбой коснулся публикации файла зоны ДВУ .RU в системе DNS, при этом не была остановлена генерация обновленного файла зоны .RU. Данное событие также привело к временной деградации производительности серверов, которые обслуживают ДВУ .ДЕТИ и .TATAR.

Последствия сбоя были успешно ликвидированы в течение 2,5 часов, а его корневая причина была устранена в течение суток.

С целью предотвращения повторения подобных сбоев предпринимаются шаги по доработке процессов проверки и публикации файлов зон, а также модернизации используемого программного обеспечения.