



ОТЧЕТ ПО РЕЗУЛЬТАТАМ ДЕЯТЕЛЬНОСТИ КОМПЕТЕНТНЫХ ОРГАНИЗАЦИЙ

В РАМКАХ СОГЛАШЕНИЯ С КООРДИНАЦИОННЫМ ЦЕНТРОМ ПО ПРОТИВОДЕЙСТВИЮ НЕСАНКЦИОНИРОВАННОМУ ИСПОЛЬЗОВАНИЮ ДОМЕНОВ .RU И .RF

Январь 2021 года

В 2012 году Координационный центр национального домена сети Интернет внедрил практику взаимодействия с организациями, компетентными в определении нарушений в сети Интернет. Это компании, которые предоставляют Координационному центру и аккредитованным регистраторам доменных имен информацию о ресурсах с противоправным контентом, о случаях фишинга, несанкционированного доступа к информационным системам и распространения вредоносных программ с использованием доменных имен в зонах .RF и .RU. Регистраторы вправе прекратить делегирование доменных имен для подобных ресурсов. Сегодня с Координационным центром сотрудничают десять компетентных организаций – Лига безопасного интернета, Group-IB, Лаборатория Касперского, RU-CERT, РОЦИТ, Роскомнадзор, ООО «БИЗон», Банк России, Доктор Веб и Национальный координационный центр по компьютерным инцидентам.



НАЦИОНАЛЬНЫЙ
КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ



Любой пользователь сети может сообщить об обнаруженном им случае неподобающего использования доменного имени на горячую линию одной из этих организаций, и меры будут приняты незамедлительно.

За отчетный период (январь 2021 года) компетентными организациями в адрес регистраторов было направлено в общей сложности 560 обращений о ресурсах с противоправной информацией с использованием доменных имен в зонах .RU и .РФ.

Анализ доменов-нарушителей по типу выявленной вредоносной активности в отчетном периоде показал, что лидирующее место принадлежит доменным именам, связанным с фишингом (481 обращение). Далее следуют ресурсы с порнографическим материалом с участием несовершеннолетних (22 обращения), ресурсы используемые для распространения вредоносного программного обеспечения (7 обращений) и контроллеры бот-сетей (1 обращение). Также, 49 обращений были направлены компетентными организациями, с просьбой инициировать проверку идентификационных сведений администратора.

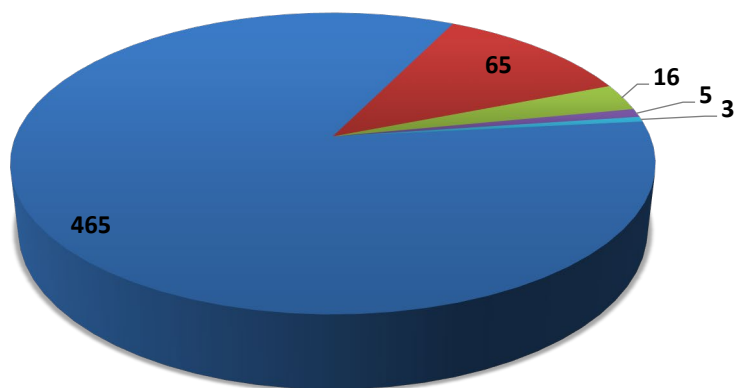


Рис.1 Распределение доменов по видам вредоносной активности (январь 2021)

За отчетный период по обращениям компетентных организаций были сняты с делегирования 470 доменных имен. Для 3 доменных имен снятие делегирования не потребовалось вследствие оперативного устранения причин блокировки администратором домена или своевременного подтверждения администратором домена идентификационных данных. В 16 случаях, снятия делегирования не потребовалось, так как ресурс был заблокирован хостинг-провайдером. В 65 случаях,



регистратором не усмотрено достаточно оснований для снятия делегирования или инициирования проверки администратора. На момент подготовки отчета, 6 обращения находились в статусе обработки.



- Делегирование снято
- Регистратором не усмотрено достаточно оснований для снятия делегирования
- Ресурс был заблокирован хостинг-провайдером
- Восстановлено делегирование после устранения причин блокировки
- Снятие делегирования не производилось вследствие оперативного устранения причины блокировки или подтверждения данных

Рис.2 Итоги обработки обращений о снятии делегирования (январь 2021)

В настоящее время остаются заблокированными 465 доменных имени (в 5 случаях делегирование было восстановлено по ходатайству соответствующей компетентной организации после устранения причины блокировки).