



ОТЧЕТ ПО РЕЗУЛЬТАТАМ ДЕЯТЕЛЬНОСТИ КОМПЕТЕНТНЫХ ОРГАНИЗАЦИЙ

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

Ноябрь 2019 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.





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 (ноябрь 2019 года) компетентными организациями в адрес регистраторов было направлено в общей сложности 576 обращений.

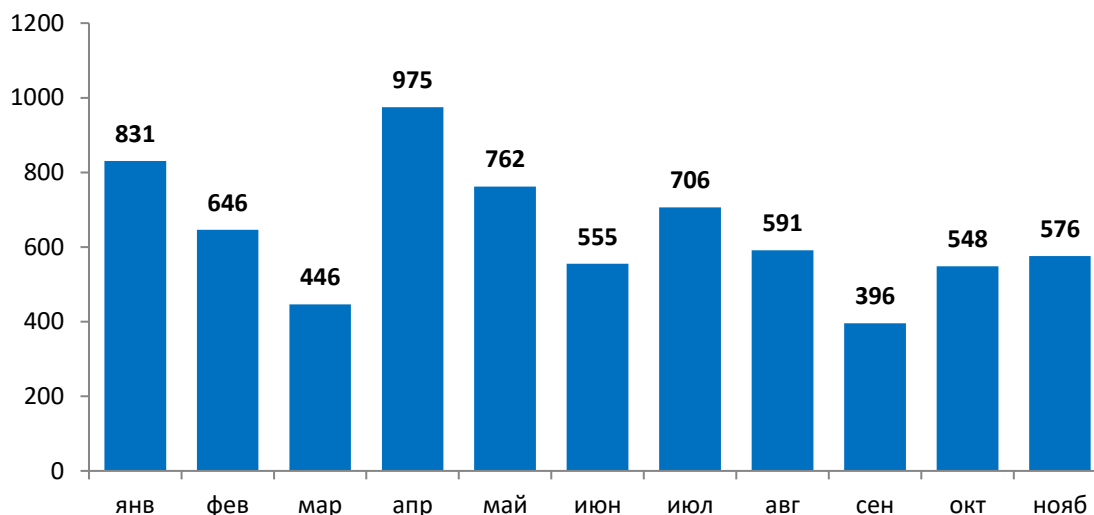


Рис.1 Число обращений к регистраторам

Анализ доменов-нарушителей по типу выявленной вредоносной активности в отчетном периоде показал, что лидирующее место принадлежит доменным именам, связанным с фишингом (508 обращений). Далее следуют контроллеры бот-сетей (18 обращений), ресурсы используемые для распространения вредоносного программного обеспечения (3 обращения) и ресурсы для распространения материалов с порнографическими изображениями несовершеннолетних (2 обращения). Также, 45 обращений были направлены компетентными организациями, с просьбой инициировать проверку идентификационных сведений администратора.

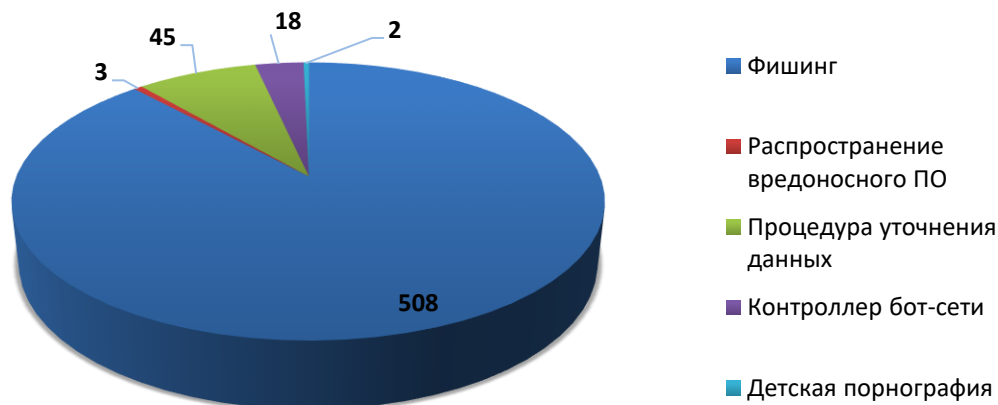


Рис.2 Распределение доменов по видам вредоносной активности (ноябрь 2019)



За отчетный период по обращениям компетентных организаций были сняты с делегирования 434 доменных имени. Для 21 доменного имени снятие делегирования не потребовалось вследствие оперативного устранения причин блокировки администратором домена или своевременного подтверждения администратором домена идентификационных данных. В 52 случаях, снятия делегирования не потребовалось, так как ресурс был заблокирован хостинг-провайдером. В 11 случаях, регистратором не усмотрено достаточно оснований для снятия делегирования или инициирования проверки администратора. На момент подготовки отчета, 58 обращений находились в статусе обработки.



Рис.3 Итоги обработки обращений о снятии делегирования (ноябрь 2019)

В настоящее время остаются заблокированными 422 доменных имени (в 12 случаях делегирование было восстановлено по ходатайству соответствующей компетентной организации после устранения причины блокировки).