# BI.ZONE: мошенники угоняют домены с истекшим сроком регистрации

*Эксперты выявили более 370 потенциально мошеннических адресов в доменной зоне .рф. В прошлом они принадлежали легальным компаниям, а теперь рекламируют казино.*

Злоумышленники отслеживают домены, срок регистрации которых подходит к концу, а затем выкупают их для своих целей. Их может заинтересовать любой сайт: страница жилого комплекса или онлайн-визитка мастера. На этих ресурсах мошенники размещают запрещенный контент, пользуясь тем, что у сайта уже есть аудитория и репутация.

***Дмитрий Кирюшкин, руководитель BI.ZONE Brand Protection:***

|  |
| --- |
| Домены с истекшим сроком регистрации можно приобрести на специальных аукционах. Перекупщик ничего не нарушает до тех пор, пока не размещает на угнанном домене нелегальный контент.В некоторых случаях владелец может потерять ресурс из-за ошибки в настройке DNS-записей. В результате преступники получают возможность опубликовать свой контент на чужом сайте. Чтобы минимизировать риск ошибки при регистрации сайта, следует обратиться к хостинг-провайдерам для комплексной настройки домена. Также необходимо отслеживать его срок действия — это позволит защитить ресурс от перекупки и предотвратить репутационные риски для прежнего владельца сайта.  |

Чтобы попасть в личный кабинет на сайте регистратора, мошенники также могут использовать авторизационные данные, добытые при помощи стилеров. По данным исследования теневых ресурсов «Threat Zone 2025: обратная сторона», стилеры являются самым популярным коммерческим ВПО. С ними связаны 33% всех объявлений о продаже вредоносных программ на теневых ресурсах.

В более редких случаях злоумышленники создают фишинговые домены, маскируют их под официальные домены регистратора или хостинг-провайдера, а затем получают данные для входа в аккаунт жертвы.

***Евгений Панков, аналитик данных Координационного центра доменов .RU/.РФ:***

|  |
| --- |
| Координационный центр неоднократно сталкивался с обращениями пользователей, которые пострадали из-за того, что мошенники регистрировали освободившиеся домены. Причины их освобождения бывают разными: от закрытия юридического лица до банальной ошибки с продлением. Кроме утраты домена, эта схема опасна еще и тем, что она открывает мошенникам широкие возможности: email-рассылки от имени бывшего администратора или с вложениями вредоносного ПО, размещение на этом домене вводящего в заблуждение контента и другие злоупотребления.Доменное имя – важный цифровой актив, и компаниям нужно относиться к нему максимально ответственно. Необходимо следить за сроками регистрации и своевременно продлевать домен, а также следить  за актуальностью указанных в реестре данных и в случае прекращения деятельности юридического лица оперативно переоформлять его на нового администратора. Проверить сроки регистрации домена всегда можно с помощью бесплатного сервиса WHOIS на сайте Координационного центра — <https://cctld.ru/service/whois/>. |

Чтобы противодействовать нелегитимному использованию бренда на мошеннических сайтах, компании применяют специализированные решения, например BI.ZONE Brand Protection. Эта платформа класса digital risk protection позволяет выявлять, а затем блокировать фишинговые кампании и мошеннические домены, находить утечки данных в даркнете, а также искать случаи нелегитимного использования бренда и дезинформации в медиа.

|  |
| --- |
| BI.ZONE — компания по управлению цифровыми рисками, которая помогает организациям безопасно развивать бизнес в киберпространстве. BI.ZONE разрабатывает собственные продукты для обеспечения устойчивости IT‑инфраструктур любого размера и оказывает широкий спектр услуг по киберзащите: от расследования инцидентов и мониторинга угроз до создания стратегий по кибербезопасности и комплексного аутсорсинга профильных функций. С 2016 года компания реализовала более 1600 проектов в сферах финансов, телекоммуникаций, энергетики, авиации и многих других, защитив свыше 800 клиентов. Сайт: <https://bi.zone>. |