Отчет по мониторингу фишинг-страниц в 2016 году

Данный отчет – результат анализа связанной с фишингом информации, поступившей в RU-CERT за 2016 год.

RU-CERT ежедневно получает жалобы на фишинг-сайты, а также сам активно ведет сбор информации о новых фишинг-атаках как в российском сегменте сети Интернет, так и вне его.

RU-CERT

Центр Реагирования на Компьютерные Инциденты

RUSSIAN COMPUTER SECURITY INCIDENT RESPONSE TEAM

RU-CERT

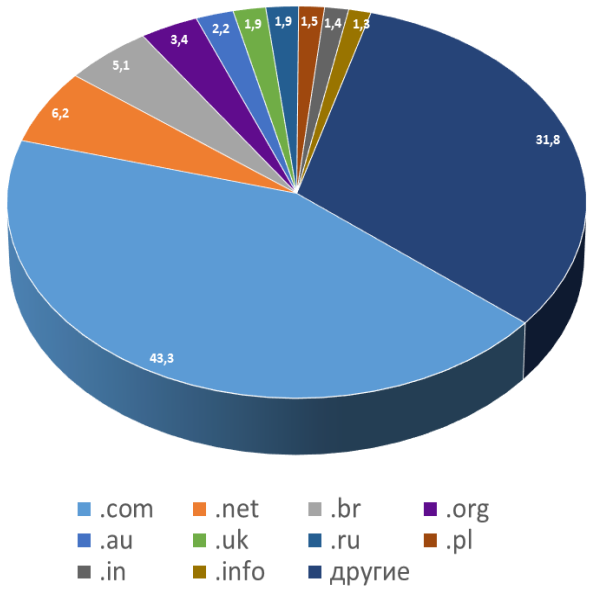
Источники данных

Все получаемые сообщения о фишинге фиксируются в базе данных RU-CERT. Кроме жалоб через веб-форму сайта www.cert.ru, а также жалоб, полученных по электронной почте на адрес info@cert.ru, RU-CERT самостоятельно анализирует ряд источников, которые предоставляют доступ к своим базам данных фишинга.

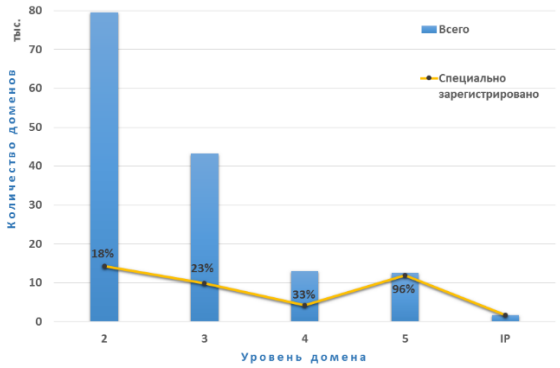
За 2016 год RU-CERT по разным каналам получил данные о 607378 фишинг-страницах, размещенных на 150051 доменах, т.е. в среднем на одном домене размещено 4,05 страницы.

Используемые домены

В ходе исследования было замечено использование 207 различных доменных зон (включая gTLD) для размещения фишинг-страниц.



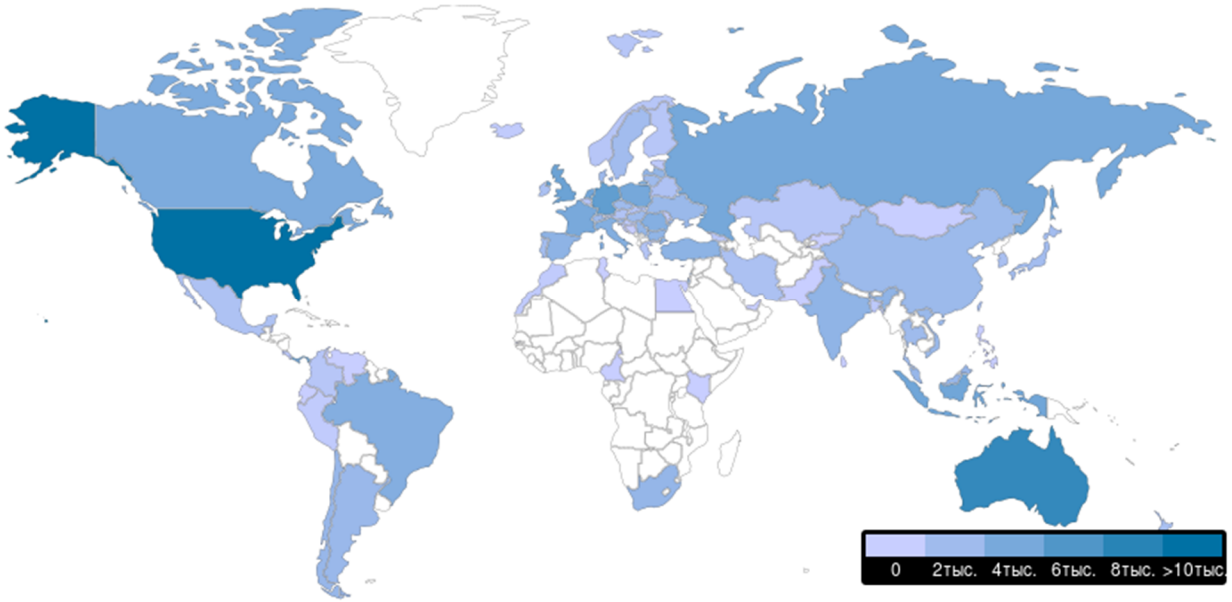
В основном фишинг размещался на доменах второго уровня. В ходе исследования было зарегистрировано 19 доменов с уровнем больше 20, наибольший зарегистрированный уровень домена: 32. С ростом уровня домена растет количество специально зарегистрированных для распространения фишинга доменов. Объясняется подобный рост разной политикой регистрации доменов в зависимости от уровня. Домены третьего и выше уровней зачастую выдаются различными сервисами и бесплатными хостингами без строгих проверок.



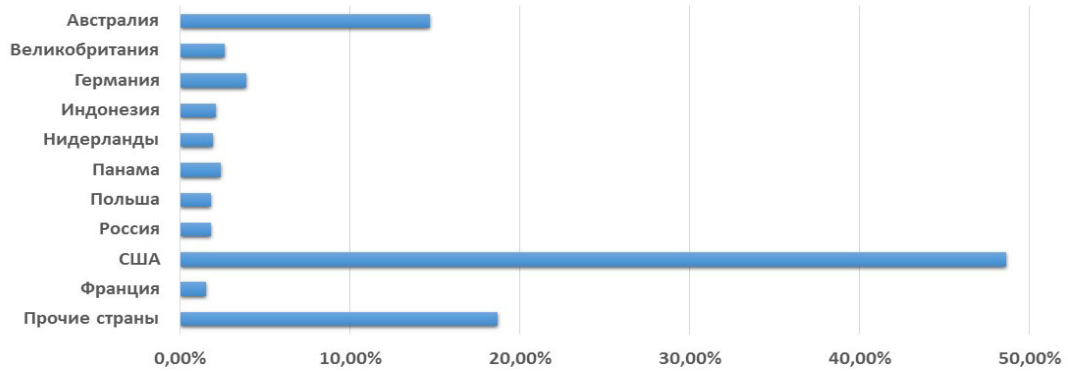
Таким образом 96% доменов 5-го уровня на которых были найдены фишинг-страницы, зарегистрированы были исключительно для целей фишинга. В то время как с доменами 2-го уровня картина иная: фишинг-страниц было найдено почти 80 тысяч, из них только 18% размещалось на доменах зарегистрированных специально под эти цели, остальные были взломаны.

Карта распределение фишинга по странам

RU-CERT за 2016 год зафиксировал факты размещения фишинг-страниц в 125 странах мира.

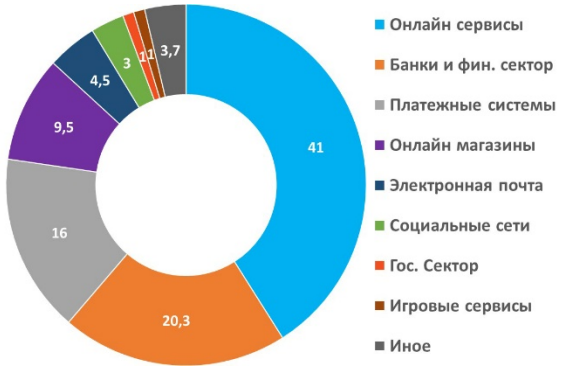


Страны лидеры по размещению фишинга

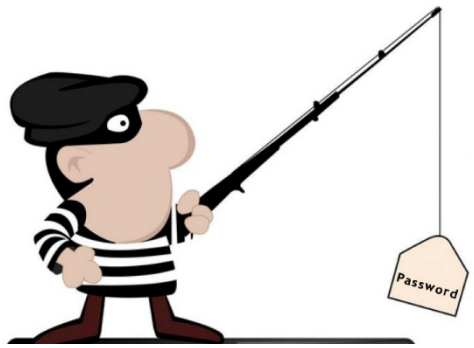


Скомпрометированные компании

Как правило злоумышленники выбирают в качестве своей целевой аудитории пользователей и клиентов известных банков, платежных сервисов, социальных сетей и других компаний, предоставляющих свои услуги через интернет.

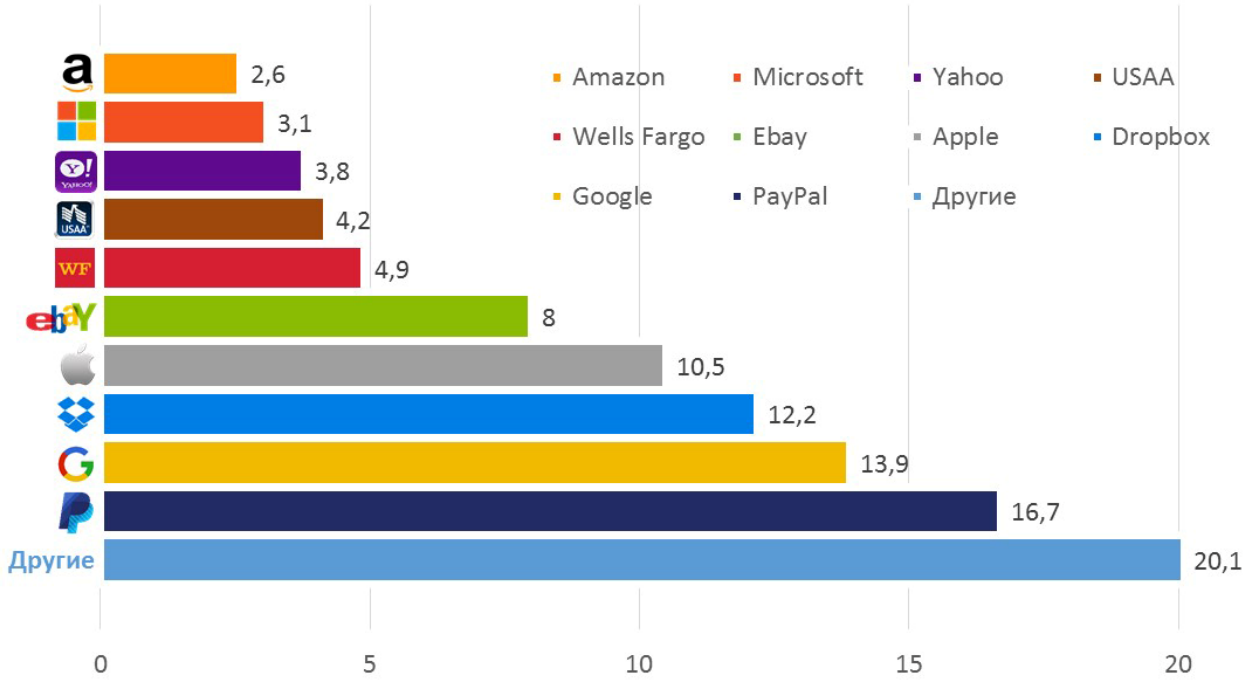


За 2016 год большего всего фишинг-атак было зарегистрировано на онлайн сервисы, банки и финансовый сектор в целом, а также на различные платежные системы и онлайн магазины.



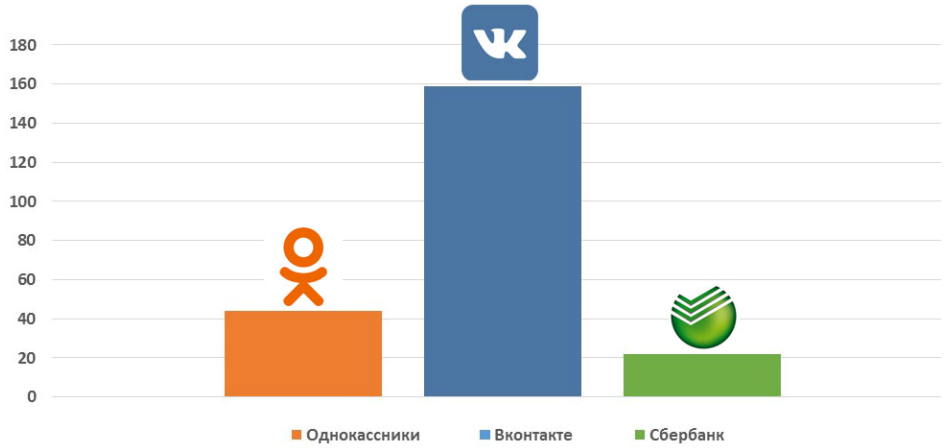
Мировые бренды

Реестр крупнейших компаний и сервисов, сайты которых были мишенью для фишинг-атак в минувшем году, возглавляет платежный сервис PayPal. Вместе с ним на верхних строчках расположились сервисы Google и Apple, а также файловый хостинг Dropbox.



Наши бренды

За 2016 год был выявлен 261 поддельный сайт отечественных компаний (0.2% от общего числа выявленных фишинг-сайтов). Больше всего фишинг-атак зарегистрировано на сайты социальных сетей "Вконтакте" и "Одноклассники". Также неоднократно подвергался атакам сайт Сбербанка России.



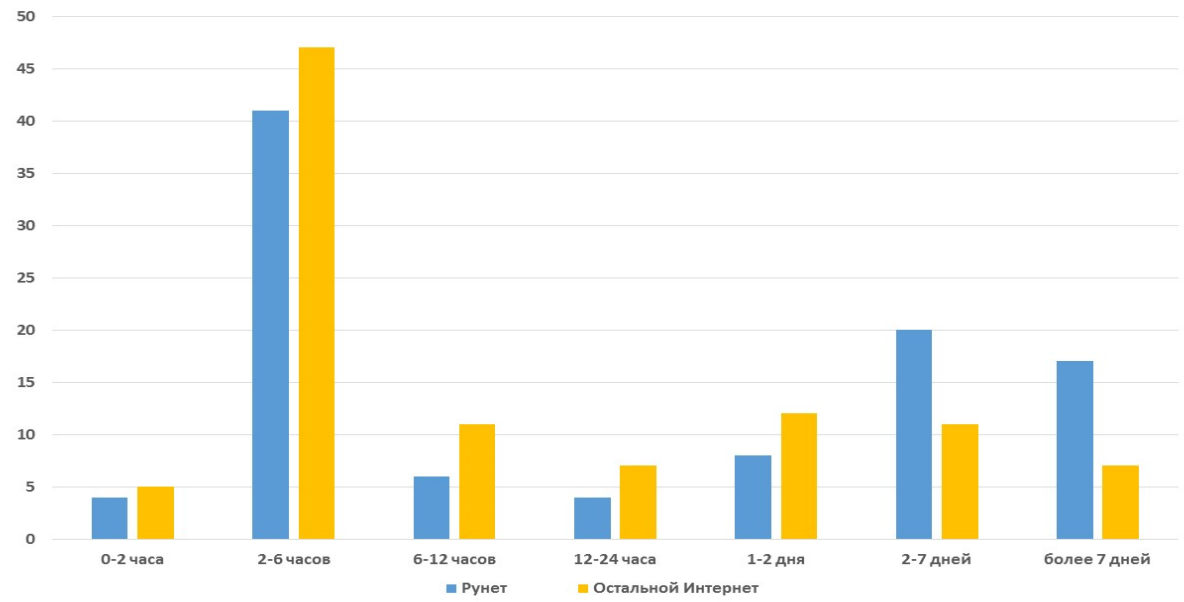
Взлом систем управления контентом

Для размещения фишинг-страниц злоумышленники часто используют взломанные сайты. Взлом обычно осуществляется через уязвимости различных CMS (систем управления контентом). Статистика за 2016 год показывает, что лидируют по числу зарегистрированных случаев взлома такие CMS как Wordpress и Joomla. В основном это старые версии систем, без актуальных обновлений в области безопасности.

21%

2%

Время жизни фишинг-страниц



Среднее время жизни фишинг-страницы в 2016 году по данным RU-CERT составляет 35 часов, медиана — 6 часов, т.е. половина фишинг-страниц остаются доступными для посещения в течении 6 и более часов с момента их появления. В российском сегменте сети Интернет среднее время жизни фишинг-страницы составляет 59 часов, медиана — 10 часов 30 минут.

Время жизни также зависит от особенностей размещения фишинга. Фишинг, размещенный на взломанных сайтах в среднем закрывается на 7 часов раньше чем фишинг, размещенный с использованием злонамеренно зарегистрированных доменов.