Babr24.com

Автор: Виктория Федосеенко НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 2233
29.08.2015, 22:20 21

Мошенники попытались взломать тысячи российских сайтов

27 августа злоумышленники под видом сотрудников Роскомнадзора разослали администраторам доменных имен вредоносные сообщения. Фишинговое письмо пришло и редактору сайта «Бабр в Тайшете» Андрею Лаховскому. Если бы он выполнил указанные в письме требования, мошенники получили доступ ко всей файловой системе интернет-ресурса.

За «Бабр в Тайшете» можно не беспокоиться, чего нельзя сказать о сотнях других российских сайтов. Масштабы фишинговой атаки неизвестны, однако география — обширна.

Сообщения о письмах якобы от Роскомнадзора приходили из разных городов России. Тревогу забили в Москве, нам удалось найти жалобы из Казани, Салехарда, Нижнего Новгорода, Красноярска и Хабаровска. Есть мнение, что «удочки» были заброшены на все сайты с посещаемостью более 3000 в сутки.

Администраторам сайтов приходили письма одного содержания и с одного адреса — zapret-info@roskomnadzor.org (реальный домен Роскомнадзора — rkn.gov.ru). С целью внесения в реестр организаторов распространения информации мошенники требовали создать в корневом каталоге сайта исполняемый файл.

Код, который требовалось вписать в файл, позволяет удаленно выполнить на сайте любое предусмотренное PHP действие. Получив такой доступ, можно украсть все данные с ресурса и даже сам сайт, а также использовать его для противоправных действий. За неисполнение требования мошенники грозили расправой в духе Роскомнадзора (орфография и пунктуация сохранены):

> «Если в течении 72 часов с момента получения данного письма Вы не идентифицируете себя, как администратор доменного имени, следую инструкции указанной выше, то Ваш сайт будет внесен в чёрные списки интернет-провайдеров и заблокирован на территории Российской Федерации»

Как удалось распознать мошенников? Рассказывает редактор Бабра Дмитрий Таевский:

1. Я программист, и сразу посмотрел на код.

Он достаточно хитрый, но по сути позволяет выполнить на сайте любую операцию. Например, сосканировать содержание базы данных с паролями или добраться до конфигурационного файла тоже с паролями. По сути получить полный админский доступ к сайту.

Проблема в том, что некоторые системы, например, Яндекс-Каталог, тоже используют такой метод для идентификации принадлежности сайта определенной фирме или человеку. Но они просят прописать в файле символы, а не исполняемый код.

2. Я посмотрел на домен, с которого было отправлено письмо. Это не домен Роскомнадзора. Мошенники сделали хитро — они зарегистрировали этот домен и сделали с него редирект на настоящий сайт Роскомнадзора.

3. Запросы Роскомнадзора выглядят не так. Но, если с ними никогда не сталкиваться, то и не поймешь.

> В целом мошенничество сделано очень профессионально. Я думаю, не менее четверти всех, кто получил письмо, на него повелись. Виной всему, конечно, определенная неадекватность недавно принятых законов, которые позволяют Роскомнадзору без суда и следствия закрывать сайты. Этого все боятся, на этом страхе и построена разводка.

18 августа уведомление о внесении в реестр запрещённых сайтов получили администраторы русскоязычной «Википедии», подробности здесь.

По поводу фишинговой атаки Роскомнадзор отправил официальные обращения в МВД и ФСБ России.

Автор: Виктория Федосеенко © SmartBabr НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 2233
29.08.2015, 22:20 21
URL: https://babr24.com/?ADE=269753 Bytes: 3403 / 3171 Версия для печати Скачать PDF

Автор текста: **Виктория Федосеенко**, журналист.

эл.почта: bratska.net.net@gmail.com

КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь
Телеграм: @bur24_link_bot
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта