Babr24.com

Автор: Виктория Федосеенко НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 2884
27.12.2016, 16:42 11

«Я не вор». Кто и зачем взломал сайт Российского визового центра в США

«Исследователь безопасности» Kapustkiy нашел уязвимость на сайте Российского визового центра в США и с ее помощью получил доступ к данным тысяч клиентов центра. О находке Kapustkiy рассказал всему миру через BuzzFeed. Таким образом он хотел обратить внимание на уязвимость и не собирается использовать ее в корыстных целях, рассказал исследователь SmartBabr.

Что случилось?

Сайт Российского визового центра в США был взломан на прошлых выходных, сообщило 27 декабря издание BuzzFeed News. О получении данных людей, подавших заявление на получение российской визы, изданию сообщил исследователь безопасности Kapustkiy. Он представил скриншот украденной информации. Речь идет, в частности, об именах, электронных адресах, телефонных номерах дюжины людей.

По словам Kapustkiy, который назвал себя членом группы New World Hackers и сообщил, что ему 17 лет, у него есть данные, связанные с «тысячами людей». В то же время он подчеркнул, что не будет их публиковать, поскольку является «этичным хакером, который находит уязвимости сайтов».

BuzzFeed News отметило, что связалось с людьми, которые значились в присланном хакером скриншоте. Пять человек подтвердили, что подавали заявление на получение визы. Юрист визового центра Джон Шорман также подтвердил, что некоторые люди из списка в скриншоте являются клиентами организации. В то же время по словам Шормана, эксперты безопасности проверили сайт и не обнаружили следов взлома. В центре предполагают, что скорее всего взломан календарь, в котором содержатся данные о назначенных встречах получателей виз с представителями консульства.

Шомар подчеркнул, что в ближайшее 48 часов центр свяжется со всеми клиентами и сообщит им о взломе.

> Как отметил BuzzFeed News, Российский визовый центр запущен американской компанией Invista Travel Logistics (ILS) и работает в Вашингтоне, Нью-Йорке, Сан-Франциско, Сиэтле и Хьюстоне. Организация помогает гражданам США получить необходимые документы для поездки в Россию, а также организовать встречу с представителями российского консульства.

Что известно об «исследователе безопасности» Kapustkiy?

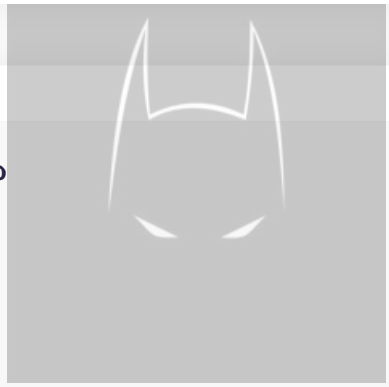
Ранее Kapustkiy уже находил уязвимости на сайтах посольств по всему миру. На своей странице вTwitter Kapustkiy указал, что живет в Ростове-на-Дону.

На своей странице вTwitter Kapustkiy указал, что живет в Ростове-на-Дону. При этом размещенные на этой странице ранее англоязычные твиты удалены, но некоторые из них сохранились в кэше Google. В частности, сохранился твит от 19 ноября 2016 года, в котором Kapustkiy утверждает, что он не хакер. *«Самое смешное, что я не хакер, но медиа продолжают настаивать, что я хакер»,* – сказано в удаленном твите (англ.).

Последние упоминания о Kapustkiy датированы как раз ноябрем 2016 года.Как пишет SecurityLab, тогда он атаковал сайты Виргинского и Висконсинского университета и скомпрометировал сайт посольства Индии в Нью-Йорке, опубликовав похищенную информацию в открытом доступе. О более ранних похождениях исследователя безопасности известно, что он взламывал сайты посольства Индии в Швейцарии, Мали, Италии, Румынии, Малави и Ливии, а так же атаковал посольство Парагвая в Тайване.

SmartBabr связался с Kapustkiy по электронной почте.

Kapustkiy
ищет уязвимости на сайтах связанных с правительством организаций



Правда ли, что вы нашли уязвимость на сайте российского визового центра в США?

Да, это правда. Я нашел SQL-уязвимость на их вебсайте. Я нигде не публиковал полученную базу данных или сведения об уязвимости.

Почему вы говорите, что вы не хакер? Вам больше по душе, когда вас называют исследователем безопасности?

Потому что многие неверно понимают значение слова «хакер». Я украл базу данных, но я не публиковал содержащиеся в ней сведения и не продавал ее. Я украл ее, чтобы доказать, что сайт очень плохо защищен. Я желаю, чтобы этот сайт стал более защищенным, как и сайты других «российских визовых центров». Это может сделать каждый. Ничего особенного. Хакер – это тот, кто много знает. Я не тот человек.

Какие цели вы преследовали, исследуя сайт российского визового центра в США. Почему именно этого учреждения?

Я анализировал сайты российских визовых центров по всему миру и обнаружил, что этот был единственным недостаточно защищенным. Я сообщил об уязвимости в CERT и администраторам сайта. Но никакого ответа не последовало. Тогда мне пришлось сделать утечку для доказательства. Я не публиковал базу данных и не продавал ее.

Ищите ли вы уязвимости на других сайтах, и по какому принципу отбираете объекты для анализа?

Ищу только для сайтов, которые связаны с правительством и имеют самый простой эксплойт, как SQL /LFI/XSS. Если я могу найти уязвимость в течение пяти секунд, это доказывает, что администраторы сайта не заботятся о его безопасности. Здесь есть нарушение какого-либо права?

Используете ли полученную информацию в корыстных целях?

Нет, я уже удалил ее с моего компьютера. Как я уже сказал, я не вор, и я никогда не сделал бы такого рода действий. Я просто парень, который хочет, чтобы владельцы веб-сайтов осознали последствия недостаточной безопасности и поняли, что может случиться, если хакеры «черной шляпы» (BLACK HAT Hacker) решат взломать их сайт.

Правда ли, что вы живете в Ростове-на-Дону?

Может быть, я не могу сказать больше.

Правда ли, что вам 17 лет?

Да.

Автор: Виктория Федосеенко © SmartBabr НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 2884
27.12.2016, 16:42 11
URL: https://babr24.com/?ADE=271264 Bytes: 6140 / 5283 Версия для печати Скачать PDF

- *ВКонтакте*

Связаться с редакцией Бабра:
newsbabr@gmail.com

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

На сайте опубликовано **1274** текстов этого автора.

НАПИСАТЬ ГЛАВРЕДУ:

Телеграм: @babr24_link_bot
Эл.почта: newsbabr@gmail.com

ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:

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