Официальное опровержение Group-IB относительно использования технологий компании для защиты инфраструктуры Руформа (владелец видеохостинга Rutube)

Москва, 11.05.2022 — Компания Group-IB, один из лидеров в сфере кибербезопасности, официально публикует опровержение относительно недостоверной информации: связанной с применением ее технологий для защиты инфраструктуры Руформа (владелец видеохостинга Rutube).

9 мая в 16:10 в одном из аккаунтов в социальной сети Twitter был опубликован пост пользователя под ником sudormRF-6, создавший почву для домыслов и появления множества источников недостоверной информации относительно участия Group-IB в проекте по защите российского видеохостера Rutube, подвергшегося кибератаке 9 мая 2022 года, согласно официальному сообщению пострадавшей компании.

Пост sudormRF-6 содержал скриншот письма, активно распространяемого сейчас в интернете. В связи с этим заявляем, что Group-IB полностью опровергает информацию о том, что продукты компании используются или когда-либо использовались для защиты от кибератак офисной или серверной инфраструктур или отдельных приложений видео-хостера Rutube.

Group-IB подчеркивает, что во время атаки 9 мая 2022 года, равно как и до нее, продукты Group-IB не использовались для защиты Rutube.

«Нам неизвестно о происхождении опубликованного в посте письма, его подлинности и реальном авторстве. Однако мы можем утверждать, что оно содержит ряд технических, логических, юридических, математических и даже грамматических ошибок, — комментирует **Дмитрий Волков, CEO Group-IB.** — Часть указанных сумм контрактов не соответствует действительности, подписанты со стороны Group-IB также указаны неверно. Документ содержит ряд домыслов относительно процедур выбора комплекса ПО, а также согласования сделок».

Отметим, что продукты Group-IB могли быть использованы для защиты ООО “Руформ” в рамках комплексного проекта, соглашения по которому были подписаны в марте 2021 года, однако работы по проекту, которые должны были начаться в апреле 2021 года, были остановлены по инициативе ООО “Руформ”. Большая часть контрактов между компаниями была аннулирована. Никаких претензий у сторон друг к другу нет. Group-IB неизвестно средства защиты какого вендора в итоге были выбраны заказчиком и используются сейчас в его инфраструктуре.

Также мы считаем необходимым указать, что никаких нарушений по контрактным обязательствам со стороны Group-IB допущено не было, равно как и никаких претензий к нам со стороны правоохранительных органов ни на одно юрлицо Group-IB по взаимодействию с ООО “Руформ”не поступало.

Стоит выделить и тот факт, что Group-IB проводила ряд тестирований на проникновение для ООО “Руформ” до 2021 года. По результатам тестирования клиент получил отчет (был сдан в феврале 2021 года) с рекомендациями по усилению мер защиты. Выполнение рекомендаций всегда остается на стороне клиента. Нам доподлинно неизвестно, были ли они выполнены. Повторных аудитов мы не проводили.

Относительно кибератаки 9 мая на Rutube, достоверно можем сообщить следующее:

- средств защиты от кибератак производства Group-IB на платформе Rutube не использовалось
- к реагированию на инцидент, имевший место 9 мая, Group-IB не привлекалась. Соответственно нам нечего сказать об атаке и атакующих, кроме того, что доступ в инфраструктуру был получен.

О Group-IB

Group-IB — один из ведущих разработчиков решений для детектирования и предотвращения кибератак, выявления мошенничества, исследования высокотехнологичных преступлений и защиты интеллектуальной собственности в сети. Штаб-квартира расположена в Сингапуре. Центры исследования киберугроз компании находятся на Ближнем Востоке (Дубай), в Азиатско-Тихоокеанском регионе (Сингапур), в Европе (Амстердам) и в России (Москва).

Group-IB Threat Intelligence & Attribution – это система исследования и атрибуции кибератак, содержащая структурированные данные о тактиках, инструментах и активности злоумышленников с возможностью персонализации под конкретную отрасль или компанию. Group-IB TI&A позволяет выстроить проактивную систему ИБ, ориентированную на защиту активов компании с низким количеством ложных инцидентов.
Это результат объединения 18-летнего опыта Group-IB по расследованиям, сбору и анализу информации об инцидентах ИБ, атаках, злоумышленниках и их инфраструктуре. TI&A от Group-IB признана лучшей в своём классе аналитическими агентствами IDC, Forrester, Gartner.
Решение Group-IB Threat Hunting Framework для проактивного поиска и защиты от сложных и неизвестных киберугроз получило признание ведущего европейского аналитического агентства KuppingerCole Analysts AG, а компания Group-IB вошла в число лидеров рынка в категориях «Product Leader» и «Innovation Leader».
Технологии Group-IB по защите от онлайн-мошенничества в интернет-банкинге и сервисах электронной коммерции получили признание Gartner, агентство присвоило Group-IB статус надежного поставщика в категории «Решения по выявлению онлайн-мошенничества». Решение Digital Risk Protection для выявления и устранения цифровых рисков, а также противодействия атакам с неправомерным использованием бренда получило престижную премию Innovation Excellence от глобального консалтингового агентство Frost & Sullivan.

В основе технологического лидерства компании и возможностей в сфере научных исследований и разработки — 18-летний практический опыт исследований киберпреступлений по всему миру и более 70 000 часов реагирования на инциденты информационной безопасности, аккумулированные в одной из крупнейших лабораторий компьютерной криминалистики и круглосуточном центре оперативного реагирования CERT-GIB.
Компания является резидентом «Сколково», Иннополиса и партнером Europol.

Для получения дополнительной информации:

Комарова Ника
Head of Corporate Communications
+7 910 472 24 06 | +7 495 984 3364 ext. 910
komarova@group-ib.com

Павел Седаков
Press officer
+7 909 979 87 77
sedakov@group-ib.com
Подробнее:
https://www.group-ib.ru
https://www.group-ib.ru/blog/
telegram | facebook | twitter | linkedin