История ликвидации поддельной антивирусной компании хакером NanoBaiter.

В апреле прошлого года хакер под псевдонимом NanoBaiter проник в центр телефонных мошенников, похитил исходный код их инструментов и отправил письма всем жертвам, оповестив их о мошенничестве. Согласно предоставленным хакером скриншотам и файлам, его целью стала компания Waredot, которая занимается так называемым «антивирусным мошенничеством».

Хакерские атаки на мошеннические центры становятся всё более частыми в последнее время. Самый популярный на YouTube хакер-линчеватель под псевдонимом «Scambaiter», например, открыто издевается над подобными центрами, регулярно взламывая их инфраструктуру и демонстрируя весь процесс на видео, попутно привлекая миллионы зрителей. Герой сегодняшней истории также поучаствовал в подобной хактивистской кампании.

«Здравствуйте! Если вы получили это письмо, значит, вы стали жертвой фальшивой антивирусной компании под названием Waredot» — написал NanoBaiter в своём письме клиентам Waredot. Хакер порекомендовал жертвам оформить возврат средств, так как программное обеспечение компании, мягко говоря, не стоит заявленных $300-$400 в месяц.

Центры телефонных мошенников часто нацелены на пожилых людей или тех, кто плохо разбирается в технологиях. Они убеждают свою целевую аудиторию в том, что на компьютере последней обнаружен вирус, а затем предлагают дорогостоящее антивирусное ПО, которое на самом деле является пустышкой и не работает ровным счётом никак.

Стоит отметить, что подобное явление достаточно распространено в США. В марте этого года Федеральная торговая комиссия США (Федеральная торговая комиссия (Federal Trade Commission, FTC) – независимое агентство правительства США, которая была создана в 1941 году. Главной задачей комиссии является защита прав потребителей и устранение всех тех факторов, которые угрожают конкурентной деловой практике, к примеру, принудительных монополий.

 Во главе Федеральной торговой комиссии находятся пять уполномоченных лиц, которые назначаются президентом и утверждаются Сенатом США.

 FTC расследует жалобы, которые исходят от потребителей и представителей бизнес-индустрии. В частности, это касается ложной рекламы и других форм мошенничества. Если в результате расследования были обнаружены противоправные действия, то FTC может добиваться добровольного устранения нарушений со стороны компании, либо же

подать административную жалобу и инициировать федеральный процесс." data-html="true" data-original-title="FTC" >FTC) даже провела отдельную операцию против таких мошенников.

На своём сайте Waredot утверждает, что помогает людям «жить в цифровом мире безопасно». Однако NanoBaiter, который помимо Хактивизм — привлечение внимания общественности к социальным, политическим и другим вопросам при помощи кибератак. В отличие от «черных шляп» хактивисты, как правило, не ищут финансовой или иной выгоды. Мишенью хактивистов обычно становятся крупные организации, государственные структуры или публичные лица, чьи действия противоречат идеологии хактивистов." data-html="true" data-original-title="Хактивизм" >хактивизма ещё и ведёт свой блог на YouTube, посчитал, что Waredot — это чистой воды мошенничество.

«Исходный код антивируса крайне примитивен и вызовет гнев у любого разумного человека, который увидит его и сопоставит с ценником в $400», — заявил хакер в своём письме.

В своём видео NanoBaiter в подробностях показал, как он получил доступ к камерам видеонаблюдения Waredot и почти год наблюдал за работой сотрудников в режиме реального времени, попутно собирая доказательную базу для обвинения мошенников.

Едва ли такой подход можно назвать правильным или законным, однако хакер предпочёл действовать основательно и жёстко. В ролике также продемонстрировано, как на компанию совершается полицейский рейд.

Примерно через месяц после публикации видео хакер связался с изданием 404 Media — это онлайн-издание, которое занимается журналистикой в области технологий и интернета. Оно было основано в 2023 бывшими сотрудниками Vice Media, Motherboard и прочих известных изданий." data-html="true" data-original-title="404 Media" >404 Media и предоставил доказательства своего взлома Waredot. «Мы решили опубликовать исходный код, чтобы окончательно покончить с Waredot», — написал хакер.

Он также добавил, что компания Waredot продолжала продавать свою продукцию и рекламироваться даже после полицейского рейда, что и вынудило хакера NanoBaiter пойти дальше, обратившись в крупное интернет СМИ. В свою очередь, издание придало данный случай большей огласке, чем этого мог бы добиться блоггер самостоятельно.