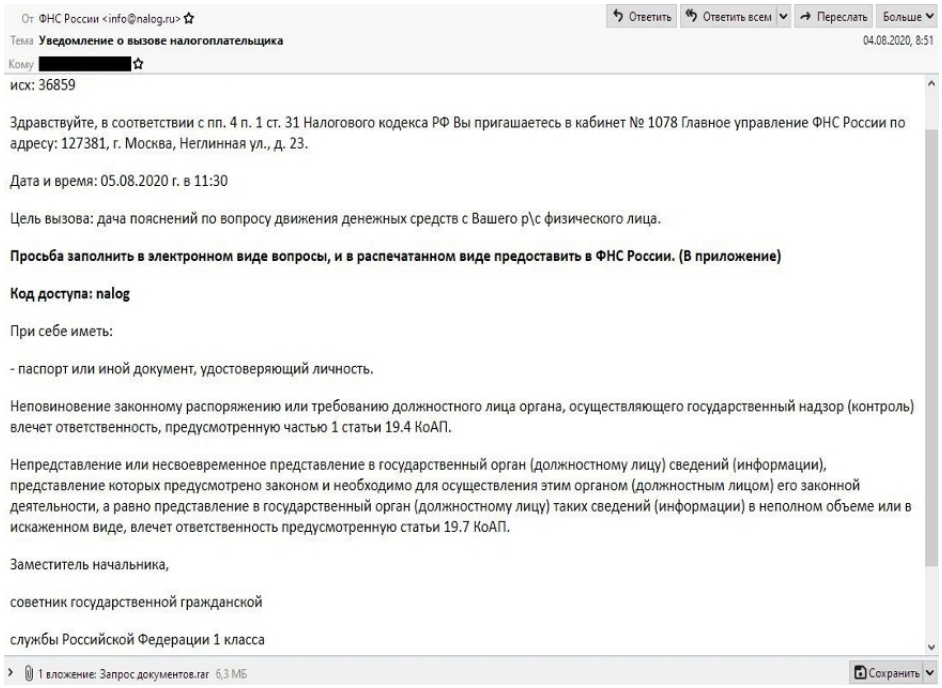
Обнаружена вредоносная рассылка от имени ФНС

Автор: Administrator
18.08.2020 08:44

{jcomments on}

Group-ib зафиксировали вредоносную кампанию якобы от имени ФНС: в поддельных письмах под видом вызова в налоговую киберпреступники распространяют ПО для удаленного управления компьютером. Рекомендуется проявить максимальную бдительность и с осторожностью относиться к требованиям открыть файлы во вложении.

Рассылка началась 27 июля. Всем атакуемым приходило одинаковое письмо, в адресе отправителя которого была указана почта info@nalog.ru, которая полностью имитировала легитимный домен ФНС. На самом деле письма рассылались с публичных почтовых сервисов, технические заголовки были подделаны. Автор письма просил явиться в «Главное Управление ФНС России» для «дачи показаний по движению денежных средств», а также распечатать и заполнить документы, находящиеся во вложении к письму. В случае неповиновения, отправитель «обещал» санкции, предусмотренные УК РФ. Как подчеркивают в ФНС, ни организации, фигурирующей в подписи к письму, ни сотрудников, от имени которых были отправлены эти сообщения, не существует.



От ФНС России <info@nalog.ru>
Ответить | Ответить всем | Переслать | Больше
Тема **Уведомление о вызове налогоплательщика**
04.08.2020, 8:51
Кому [redacted]

исх: 36859

Здравствуйте, в соответствии с пп. 4 п. 1 ст. 31 Налогового кодекса РФ Вы пригашаетесь в кабинет № 1078 Главное управление ФНС России по адресу: 127381, г. Москва, Неглинная ул., д. 23.

Дата и время: 05.08.2020 г. в 11:30

Цель вызова: дача пояснений по вопросу движения денежных средств с Вашего р\с физического лица.

Просьба заполнить в электронном виде вопросы, и в распечатанном виде предоставить в ФНС России. (В приложение)

Код доступа: nalog

При себе иметь:

- паспорт или иной документ, удостоверяющий личность.

Неповиновение законному распоряжению или требованию должностного лица органа, осуществляющего государственный надзор (контроль) влечет ответственность, предусмотренную частью 1 статьи 19.4 КоАП.

Непредставление или несвоевременное представление в государственный орган (должностному лицу) сведений (информации), представление которых предусмотрено законом и необходимо для осуществления этим органом (должностным лицом) его законной деятельности, а равно представление в государственный орган (должностному лицу) таких сведений (информации) в неполном объеме или в искаженном виде, влечет ответственность предусмотренную статьи 19.7 КоАП.

Заместитель начальника,

советник государственной гражданской

службы Российской Федерации 1 класса

1 вложение: Запрос документов.rar 6,3 МБ
Сохранить

«Данные сообщения являются поддельными и не имеют к Федеральной налоговой службе никакого отношения, — пояснили в ФНС. — ФНС России не направляет налогоплательщикам письма о наличии задолженности и с предложениями оплатить долг в режиме онлайн. Вся необходимая информация о неуплаченных налогах и способах их оплаты размещена в группе сервисов «Личный кабинет налогоплательщика». Будьте бдительны и не открывайте подобные письма».

В ходе анализа было установлено, что во вложении к поддельному письму находился архив «zapros-dokumentov.rar», в котором был другой запароленный архив и текстовый файл с паролем от него. При открытии аттача на компьютер жертвы загружалась легитимная программа для удалённого администрирования и управления компьютером, RMS (Remote Manipulator System). Именно поэтому для большинства антивирусных средств подобное письмо не выглядело вредоносным.

Однако в данном случае ПО RMS было модифицировано злоумышленниками таким образом, что при запуске исполняемого файла они получали полный удаленный контроль над атакованной рабочей станцией. Как правило, такое ПО используется на первом этапе целевой атаки для закрепления в сети, дальнейшего продвижения по ней или для эксфильтрации данных с зараженной машины.

В связи с тем, что в настоящее время рассылка вредоносных писем продолжается, рекомендуется проявить бдительность. Любые просьбы загрузить или установить файлы должны расцениваться как подозрительные. При получении подобного письма необходимо оперативно сообщить внутренней службе безопасности и работать с документами только после их проверки. В ФНС также напоминают, что официальная рассылка направляется только тем, кто указал и подтвердил адрес своей электронной почты в Личном кабинете налогоплательщика. В таких письмах обычно указана информация об изменениях в Личном кабинете налогоплательщика, о регистрации обращения в Службу и получении ответа на него. Причем формат ответа на обращение (.pdf, .xml) пользователь выбирает самостоятельно при обращении через сайт.

Источник: https://www.securitylab.ru

(function(w, d, n) { w[n] = w[n] || []; w[n].push({ section_id: 263974, place: "advertur_263974", width: 300, height: 250 }); })(window, document, "advertur_sections");