Электронная рыбалка: какие «приманки» используют злоумышленники в фишинговых спам-письмах

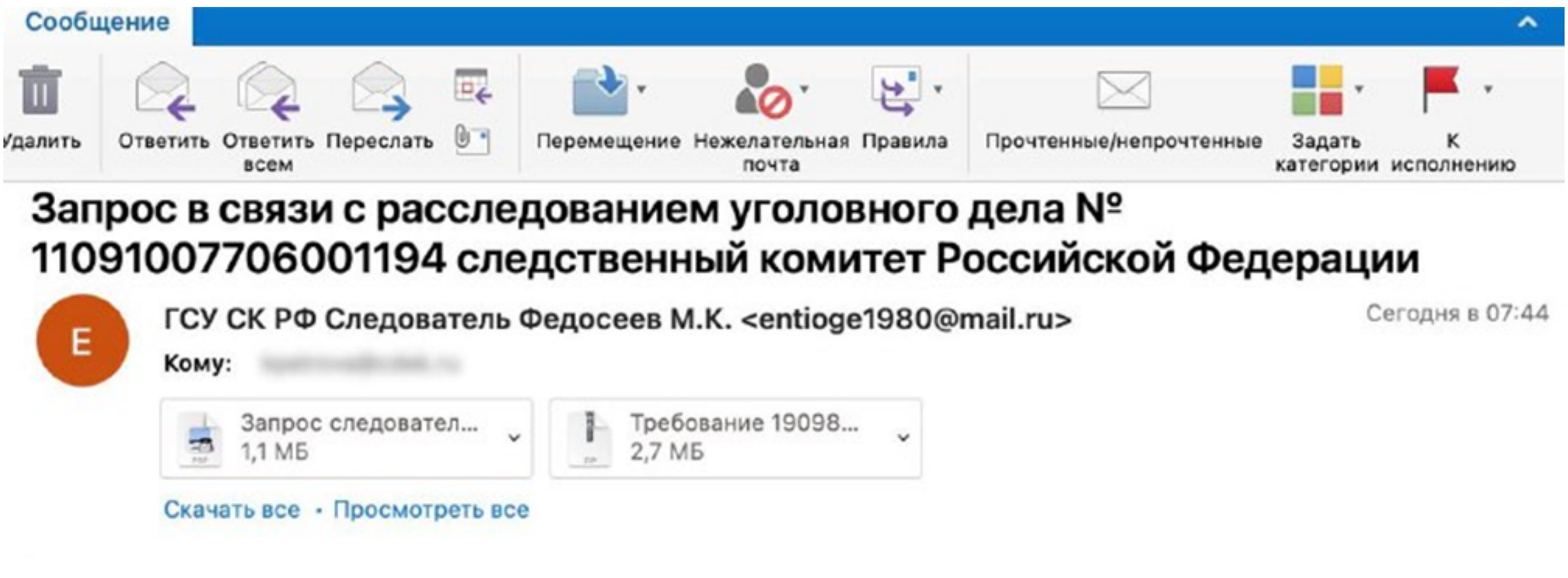
Хакерская группировка Scaly Wolf, используя социальную инженерию, рассылает фишинговые письма от лица крупных российских компаний и российский государственных служб. Их цель — получить доступ к ресурсам госорганизаций Российской Федерации.

В фишинговом арсенале преступников: требования Роскомнадзора, Следственного комитета РФ и Военной прокуратуры РФ. Иногда письма маскируют под коммерческое предложение.

Тексты всегда юридически грамотно составлены. Это делает рассылку убедительной, вызывает доверие и побуждает запустить вредоносный файл.

Примеры спам-писем

1 Вариант атаки



1. Отправитель — якобы Следственный комитет РФ.
   Тема — расследование уголовного дела.
   Пример: «Запрос в связис расследованием уголовного дела № 11091007706001194 следственный комитетРФ» или «Требование в рамках расследования уголовного дела № 11091007706011194 следственныйкомитет РФ».

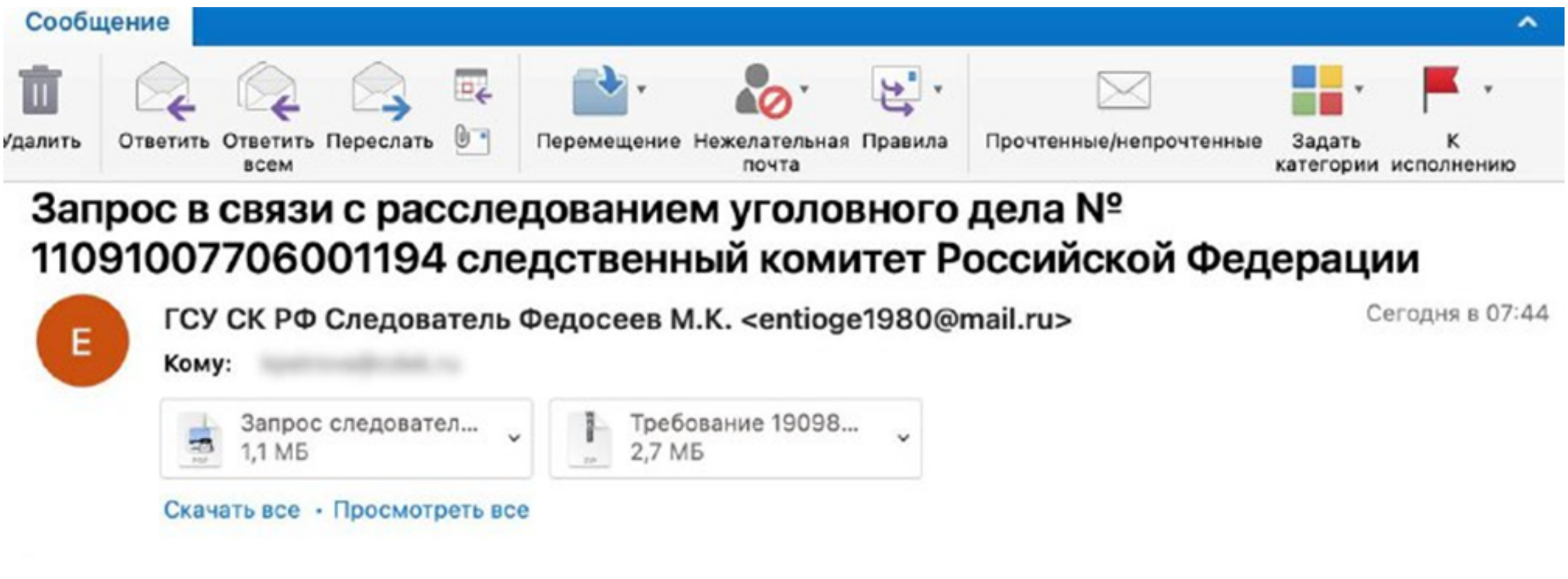
2. ПрикрепленPDF-файл с предписанием явиться в СКР, а также запароленный архив.
   Парольнаходился в имени файла: «Требование 19098 СК РФ от 07.09.23 ПАРОЛЬ — 123123123.zip».

3. Архивсодержит документы и вредоносный файл, замаскированный под приложение к ним — «Переченьюридических лиц и предприятий, уклонение от уплаты налогов, требования идополнительные. exe».

4. Файлпредставляет собой стиллер White Snake — вирус, который крадет логины и пароли жертвы.

Примеры спам-писем

2 Вариант атаки



1. Фишинговое письмо с прикрепленным архивом с документами:
   - Требование РОСКОМНАДЗОР № 02 12143.odt
   - Приложение к требованию РОСКОМНАДЗОРА о предоставлении пояснений, по факту выявления данных в ходе мониторинга и анализа списков запрещенных интернет ресурсов, IT адресов. exe
   - РОСКОМНАДЗОР. png
2. Первый файл — фишинговый документ, который отвлекает внимание жертвы от второго файла-стиллера White Snake.
3. В случае успешной атаки злоумышленники получают доступ сразу к нескольким корпоративным ресурсам: к электронной почте, корпорталу и информационным системам. Вредоносное ПО собирает пароли, копирует файлы, записывает нажатие клавиш и получает удалённый доступ к устройству.

Как распознать фишинговое письмо?

Просят сообщить информацию

Безопасные сервисы не рассылают письма с просьбой сообщить какую-либо информацию.

Сиюминутные действия

Тема письма и/или его текст содержат призыв к действию: перейти по ссылке, нажать на кнопку, открыть файл, срочно ответить на сообщение.

Письма с общих почтовых доменов

Киберпреступники выступают от лица известных компаний (в том числе и Ваших коллег), но пишут с общих почтовых доменов: gmail. com, mail. ru и т. п. Безопасные сообщения приходят с корпоративных адресов. Например, «tularegion.ru».

Вложения разного характера

- с двойным расширением;
- с неизвестным расширением;
- «.app», «.exe», «.bat», «.js», «.scr».

Необходимо убедиться, что у Вас в почтовом клиенте отображается расширение файлов. Иначе, вероятно, файл имеет скрытое расширение.

Нет сертификата подлинности сайта

У ресурсадля перехода отсутствуют логотип на вкладке в браузере, сертификатподлинности, защищённое соединение между пользователем и сайтом (используется «http://» вместо «https://»).

Что делать, если Вы обнаружили спам-письмо на почте?

1. **Не нажимайте** на гиперссылки
2. **Не копируйте** адрес ссылки
3. **Не открывайте** и не скачивайте вложения
4. **Не пересылайте** письма коллегам
5. **Перешлите письмо** с пометкой «Прошу проверить приложенное письмо на наличие вредоносной активности» **на адрес spam@tularegion.ru** (только для пользователей домена tularegion.org и tularegion.ru).

Что делать, если Вы попались на обман?

1. **Незамедлительно отключите** автоматизированное рабочее место от локальной сети, принудительно выключите его и обесточите.

2. **Сообщите** о данном факте своему администратору безопасности и оставить заявку в службу поддержки пользователей.

3. **Эксплуатация** автоматизированного рабочего места до его полной проверки на наличие/отсутствие вредоносного программного обеспечения строго **запрещена**.