

Ф.А.С.С.Т. обнаружил новые атаки проукраинских кибершпионов Sticky Werewolf

 habr.com/ru/companies/f_a_c_c_t/news/873762/

F6

EditorF6 15 янв в 11:46

3 мин

3К



После новогодних праздников АРТ-группировка **Sticky Werewolf** пыталась атаковать российские научно-производственные предприятия. На этот раз кибершпионы отправляли фейковые фишинговые письма от имени Минпромторга России. Одно из таких фишинговых писем вечером 13 января перехватило и заблокировало решение по выявлению сложных киберугроз F.A.C.C.T. Managed XDR. Специалисты Центра кибербезопасности F.A.C.C.T. провели анализ рассылки.

Sticky Werewolf — проукраинская кибершпионская группа, атакующая преимущественно госучреждения, НИИ и промышленные предприятия из сферы военно-промышленного комплекса России. Отмечались также атаки в Беларуси и Польше. В качестве первоначального вектора атак группа использует фишинговые рассылки по электронной почте с вредоносными вложениями, в которых часто встречаются такие инструменты, как трояны удаленного доступа Darktrack RAT и Ozone RAT, стилеры Glory Stealer и MetaStealer (вариация RedLine Stealer).

Как действовали Sticky Werewolf

Злоумышленники отправляли вредоносные письма, в которых содержалось "поручение" проработать вопрос о необходимости размещения заказов предприятий оборонно-промышленного комплекса в учреждениях уголовно-исправительной системы с привлечением осужденных.

В качестве приманки Sticky Werewolf использовали поддельное письмо от Минпромторга. На то, что документ "липовый", указывает, среди прочего, несоответствие должности Дениса Мантурова (с мая 2024 года он уже не глава Минпромторга) и разные даты принятия "решения", о которых говорится в январской и декабрьской рассылках.

Письмо содержит два вложения:

- 1) Сопроводительное письмо-приманку на бланке Минпромторга
- 2) Форма заполнения.rar — вредоносный архив, защищенный паролем: 2025.

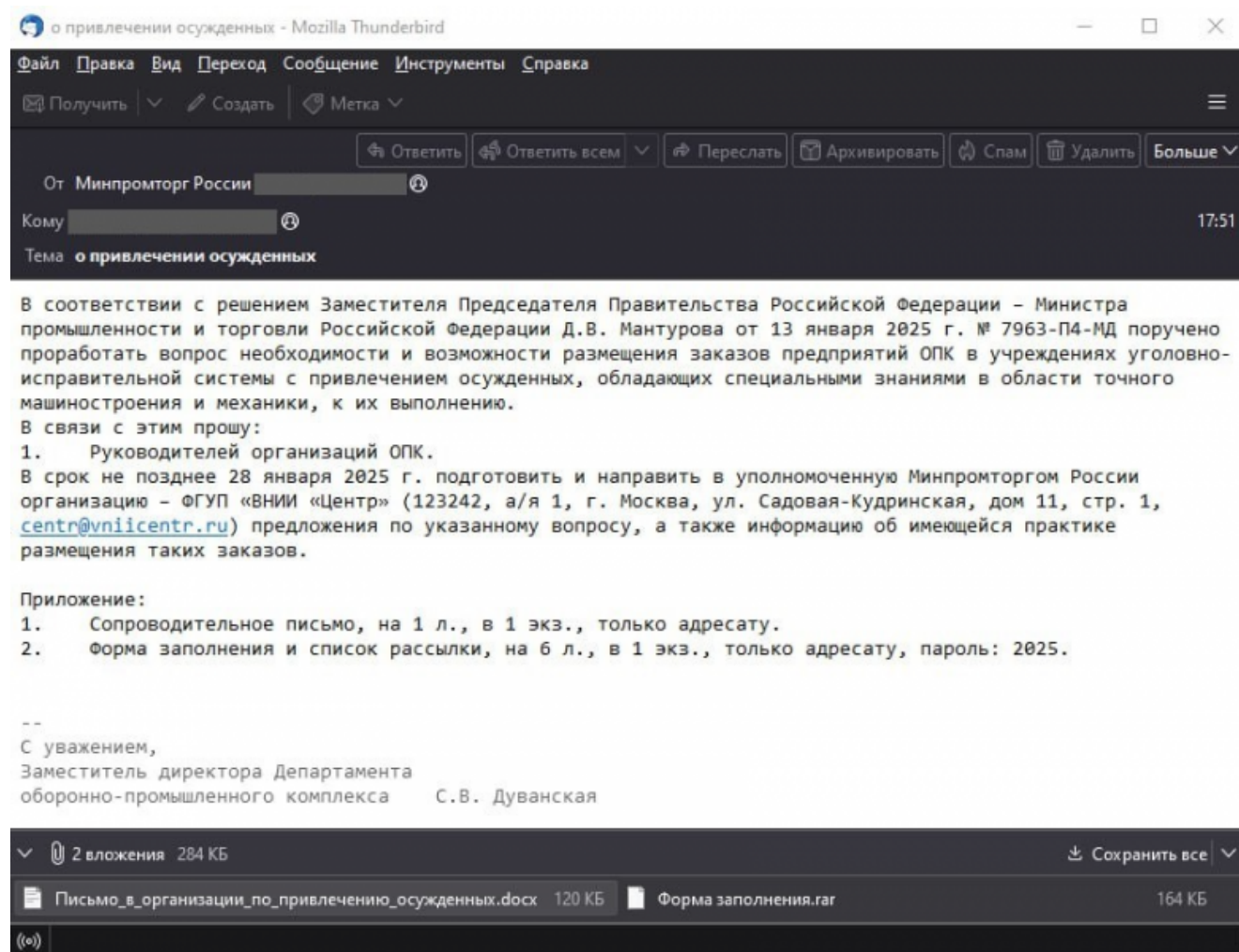


Рисунок 1. Образец фишингового письма.

Содержимое вложений

Первое вложение содержало фальшивый документ-приманку
«Письмо_в_организации_по_привлечению_осужденных.docx».

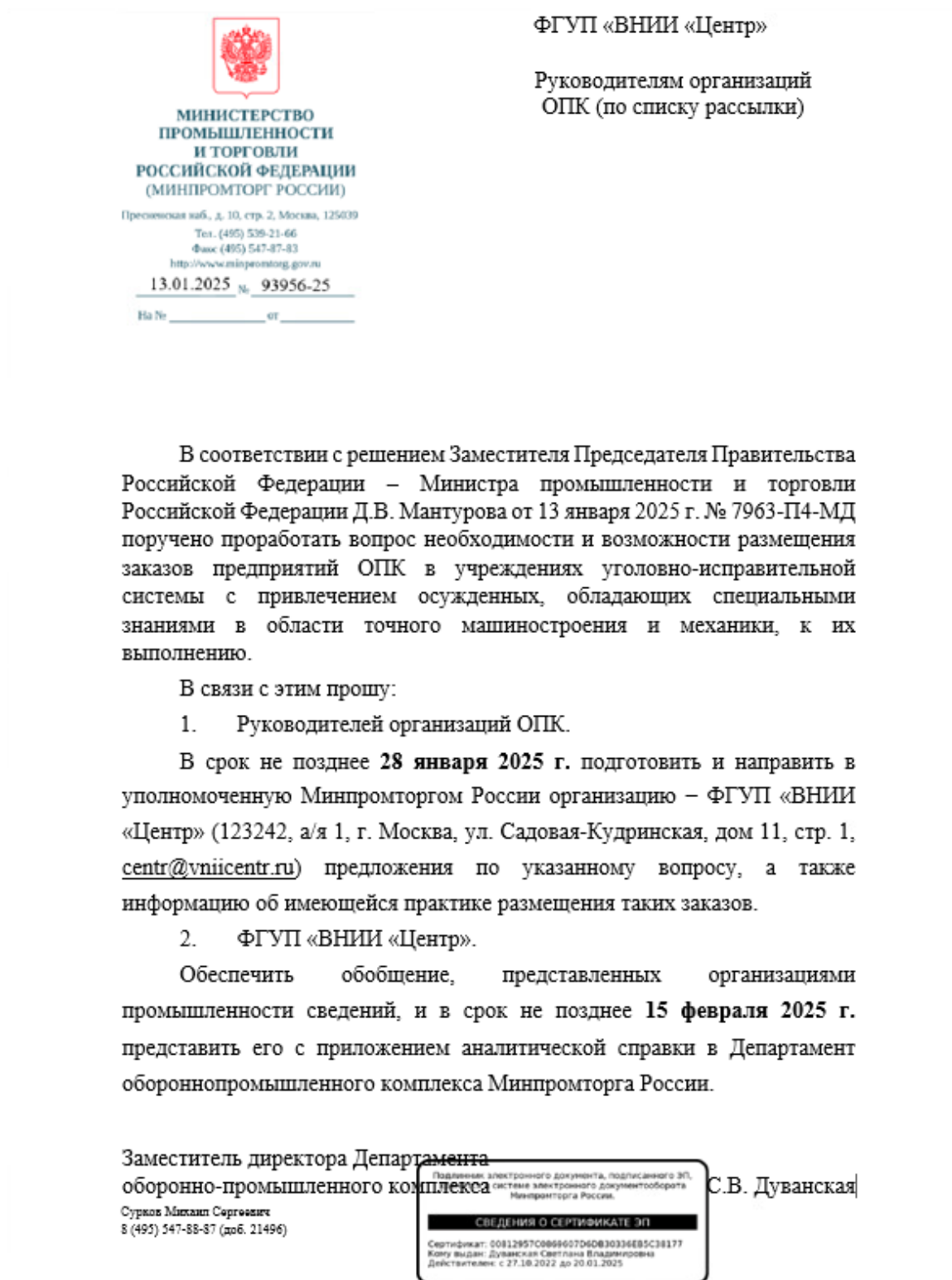


Рисунок 2. Документ-приманка из фишингового письма.

Второе вложение содержало запароленный архив. Внутри архива находился документ «список рассылки.docx» и вредоносный исполняемый файл «Форма заполнения.pdf.exe».

При запуске в конечном итоге происходит доставка трояна удаленного доступа **Ozone RAT**, предназначенного для предоставления скрытого удаленного доступа к скомпрометированному устройству.

Форма заполнения.rar - RAR архив, размер исходных файлов 183 667 байт					
Имя	Размер	Сжат	Тип	Изменён	CRC32
..			Папка с файлами		
список рассылки.docx *	12 033	11 088	Документ Micros...	13.01.2025 18:31	4636B821
Форма заполнения.pdf.exe *	171 634	156 000	Приложение	13.01.2025 17:32	22B4D7A9

Рисунок 3. Содержимое вредоносного архива.

Основная информация

SHA1: 0919987e12e51e55824959323ed23a9d3387fbad

Информация Видео Configs

Файл **Форма заполнения.rar** проанализирован в MDP с вердиктом **вредоносный с вероятностью 98.4%**

Впервые замечен 13 Jan 2025 · Последний раз замечен 14 Jan 2025

Ozone RAT

Windows 10/x64/ru Интернет: **Доступен** Таймаут: 9.6 мин - 575 сек

Рисунок 4. Сведения об атрибуции Ozone RAT, полученные после анализа в F.A.C.C.T. Malware Detonation Platform.

Примеры автоматизированных отчетов F.A.C.C.T. Malware Detonation Platform можно посмотреть [здесь](#). **Поиск похожих рассылок**

В ходе дополнительного исследования было обнаружено фишинговое письмо от 23 декабря 2024 года с аналогичной темой, в котором содержалось два фейковых документа «Письмо_в_организации_по_привлечению_осужденных.docx» и «список рассылки.docx». Злоумышленники также атаковали научно-производственное предприятие, однако в письме отсутствовал архив с полезной нагрузкой внутри.

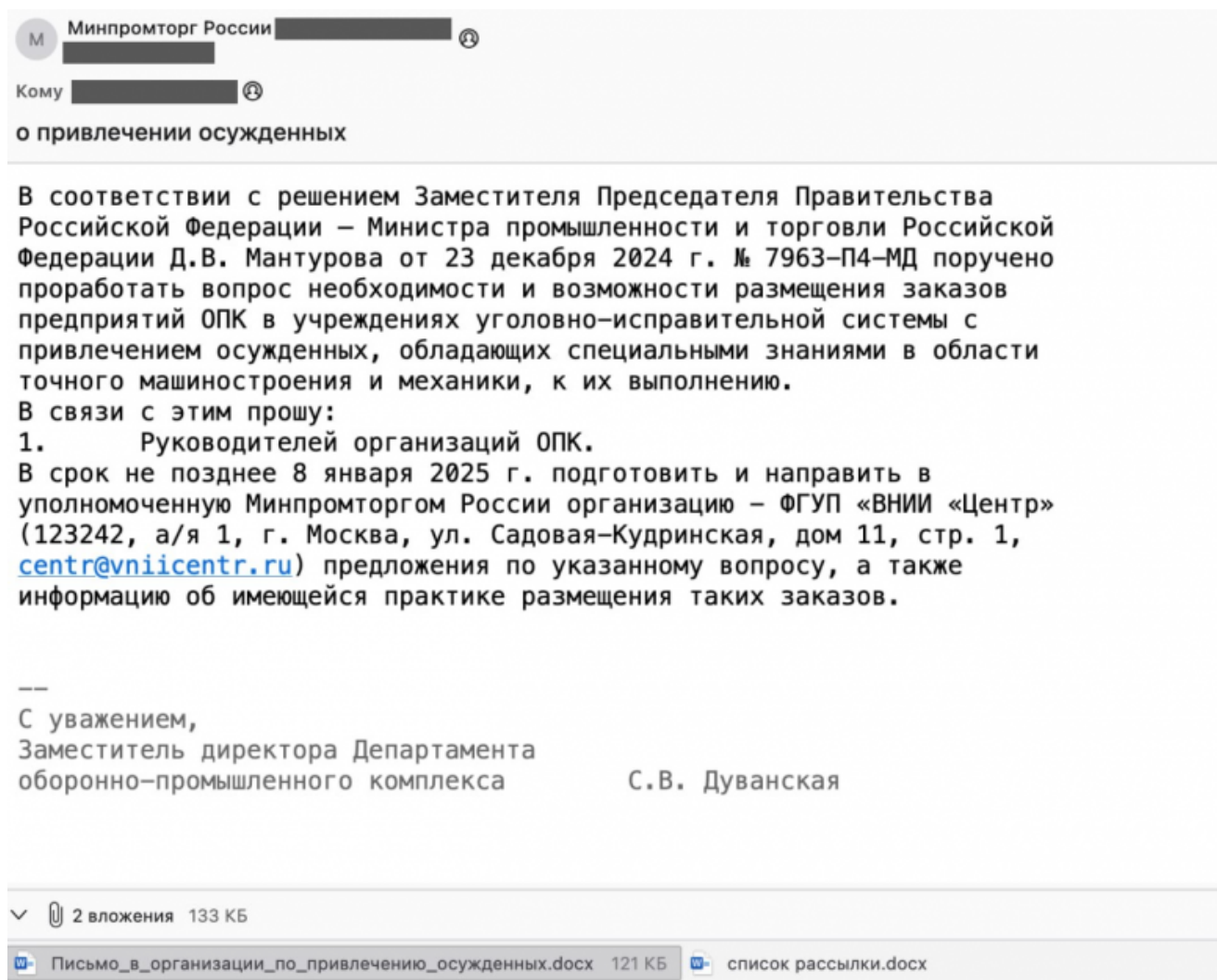


Рисунок 5. Фишинговое письмо, найденное в открытых источниках.

Напомним, что в декабре 2023 года Sticky Werewolf дважды атаковали российскую фарму, прикрываясь МЧС и Минстроем, а в январе 2024 года отправляли фейковые письма якобы от ФСБ.

Индикаторы компрометации

Файловые индикаторы

Письмо_в_организации_по_привлечению_осужденных.docx

SHA1: 969977a682bac07eb1f9196041077d3c332b2b37

Форма заполнения.rar

SHA1: 0919987e12e51e55824959323ed23a9d3387fbad

Форма заполнения.pdf.exe

SHA1: 74f6f78bd8f1cc30e911350b60fe9b4eaf69e21c

rebrand.exe

SHA1: 4c92e612f006838f10b50a9aa102c4430f9b8495

ser.vbs

SHA1: d558d8501286b0b322a06a2e2f21fc6c03d45316

список рассылки.docx

SHA1: 861118c8a32157349c1d3dc76e774c027c05433c

Сетевые индикаторы

- 45[.]155[.]249[.]126
- 84[.]22[.]195[.]72
- bitbucket[.]org/5w457/ed512/downloads/emnfpac[.]txt
- hXXps://bitbucket[.]org/ghjkkkkkkkk/tdrdreest/downloads/img[.]jpg?537612
- hXXps://raw[.]githubusercontent[.]com/gmedusa135/nano/refs/heads/main/new_img123[.]jpg