F.A.C.C.T. обнаружил новые атаки проукраинских кибершпионов Sticky Werewolf

By EditorF6

Published: 2025-01-15 · Archived: 2026-04-05 18:58:59 UTC

3 мин

6.4K

После новогодних праздников APT-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.

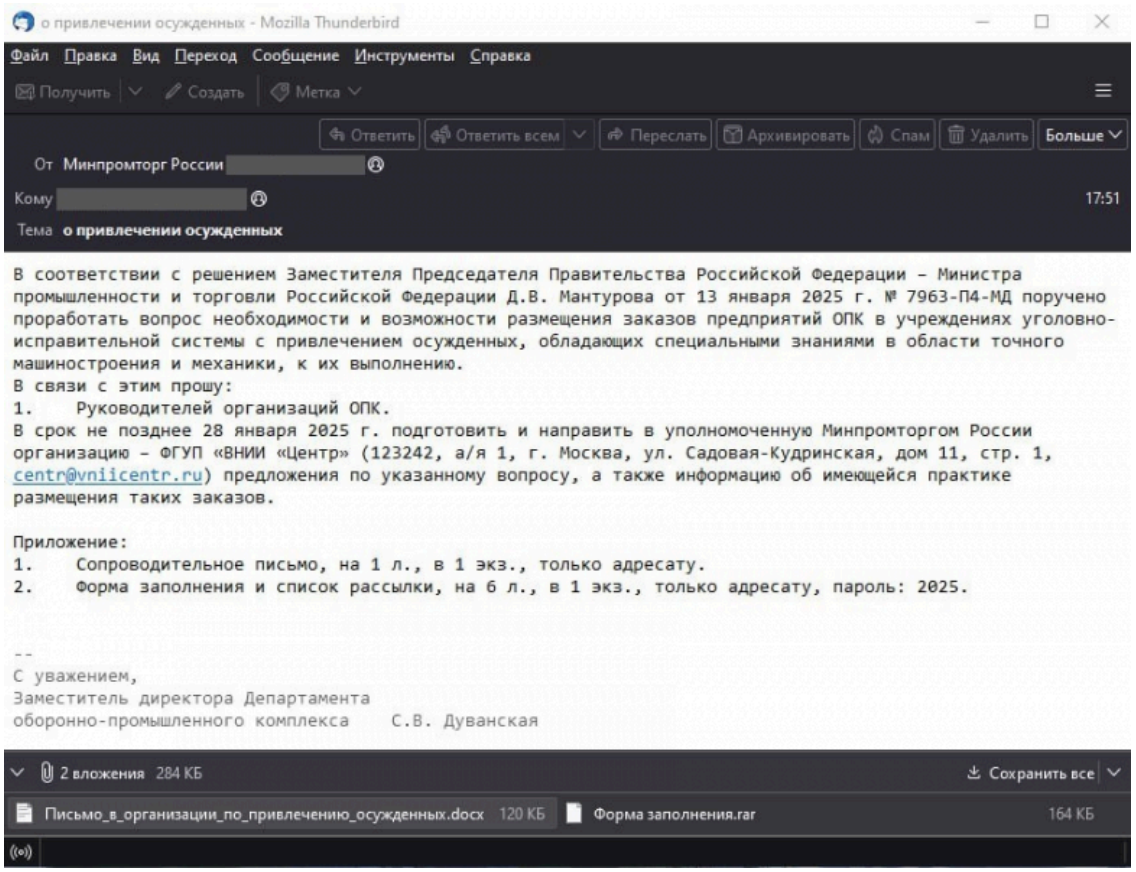
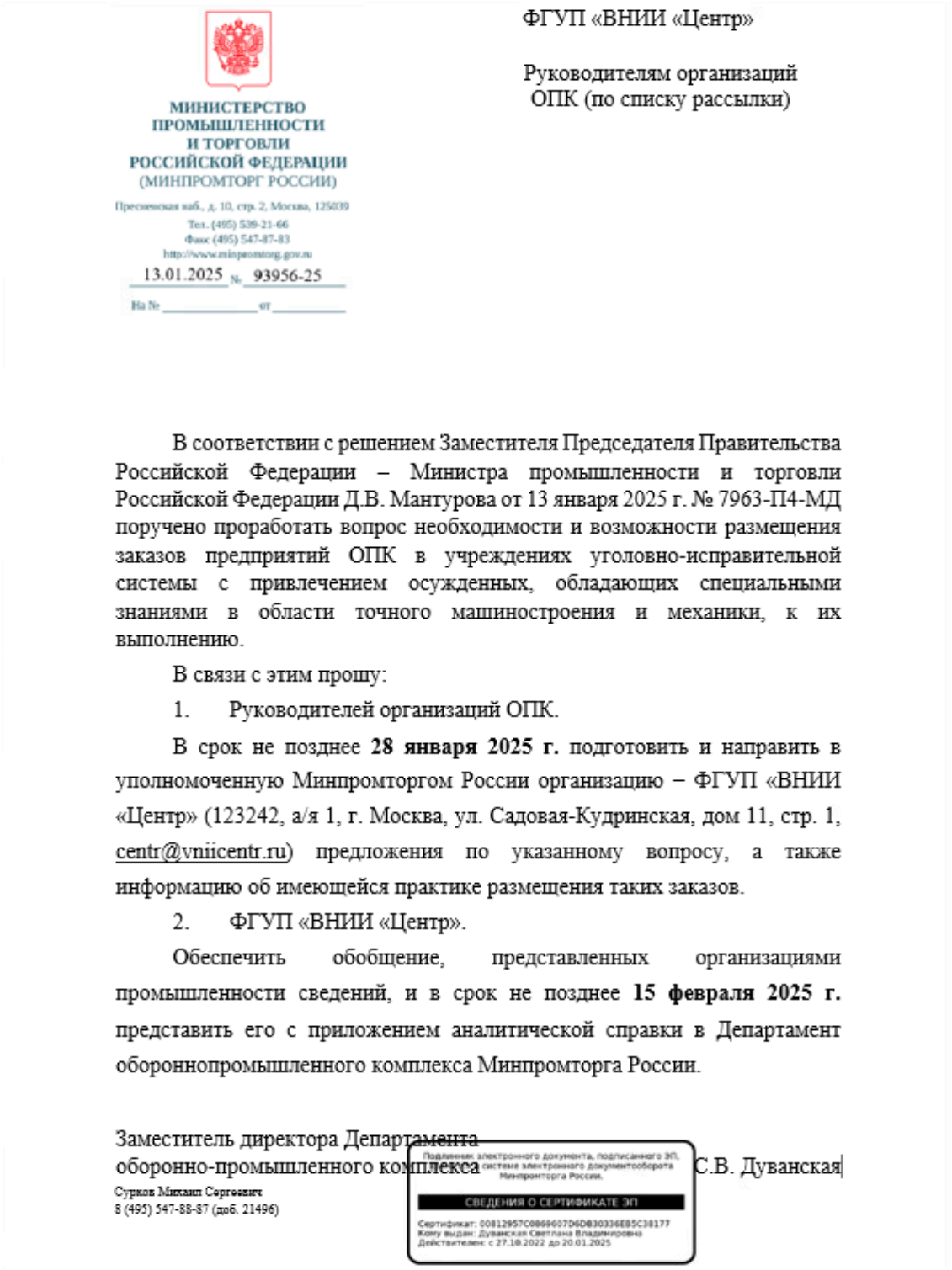


Рисунок 1. Образец фишингового письма.

Содержимое вложений

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



МИНИСТЕРСТВО ПРОМЫШЛЕННОСТИ И ТОРГОВЛИ РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНПРОМТОРГ РОССИИ)

Пресненская наб., д. 10, стр. 2, Москва, 125039
Тел.: (495) 539-21-66
Факс: (495) 547-87-83
http://www.minpromtorg.gov.ru

13.01.2025 № 93956-25

На № _____ от _____

ФГУП «ВНИИ «Центр»

Руководителям организаций
ОПК (по списку рассылки)

В соответствии с решением Заместителя Председателя Правительства Российской Федерации – Министра промышленности и торговли Российской Федерации Д.В. Мантурова от 13 января 2025 г. № 7963-П4-МД поручено проработать вопрос необходимости и возможности размещения заказов предприятий ОПК в учреждениях уголовно-исправительной системы с привлечением осужденных, обладающих специальными знаниями в области точного машиностроения и механики, к их выполнению.

В связи с этим прошу:

1. Руководителей организаций ОПК.

В срок не позднее **28 января 2025 г.** подготовить и направить в уполномоченную Минпромторгом России организацию – ФГУП «ВНИИ «Центр» (123242, а/я 1, г. Москва, ул. Садовая-Кудринская, дом 11, стр. 1, centr@vniicentr.ru) предложения по указанному вопросу, а также информацию об имеющейся практике размещения таких заказов.

2. ФГУП «ВНИИ «Центр».

Обеспечить обобщение, представленных организациями промышленности сведений, и в срок не позднее **15 февраля 2025 г.** представить его с приложением аналитической справки в Департамент оборонно-промышленного комплекса Минпромторга России.

Заместитель директора Департамента
оборонно-промышленного комплекса С.В. Дуванская

Подлинник электронного документа, подписанного ЭП, в системе электронного документооборота Минпромторга России.
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат: 00812957C0869607D6DB30336EB5C38177
Кому выдан: Дуванская Светлана Владимировна
Действителен: с 27.10.2022 до 20.01.2025

Сурков Михаил Сергеевич
8 (495) 547-88-87 (доб. 21496)

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.

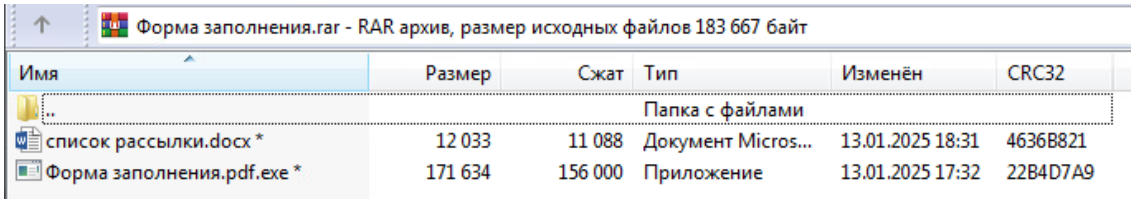


Рисунок 3. Содержимое вредоносного архива.

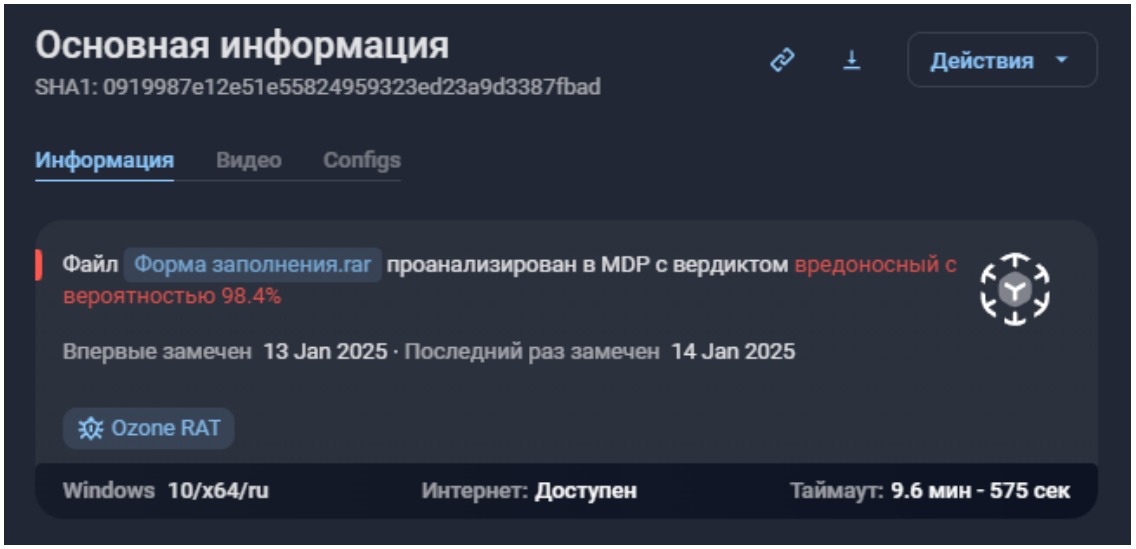


Рисунок 4. Сведения об атрибуции Ozone RAT, полученные после анализа в F.A.C.C.T. Malware Detonation Platform.

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.

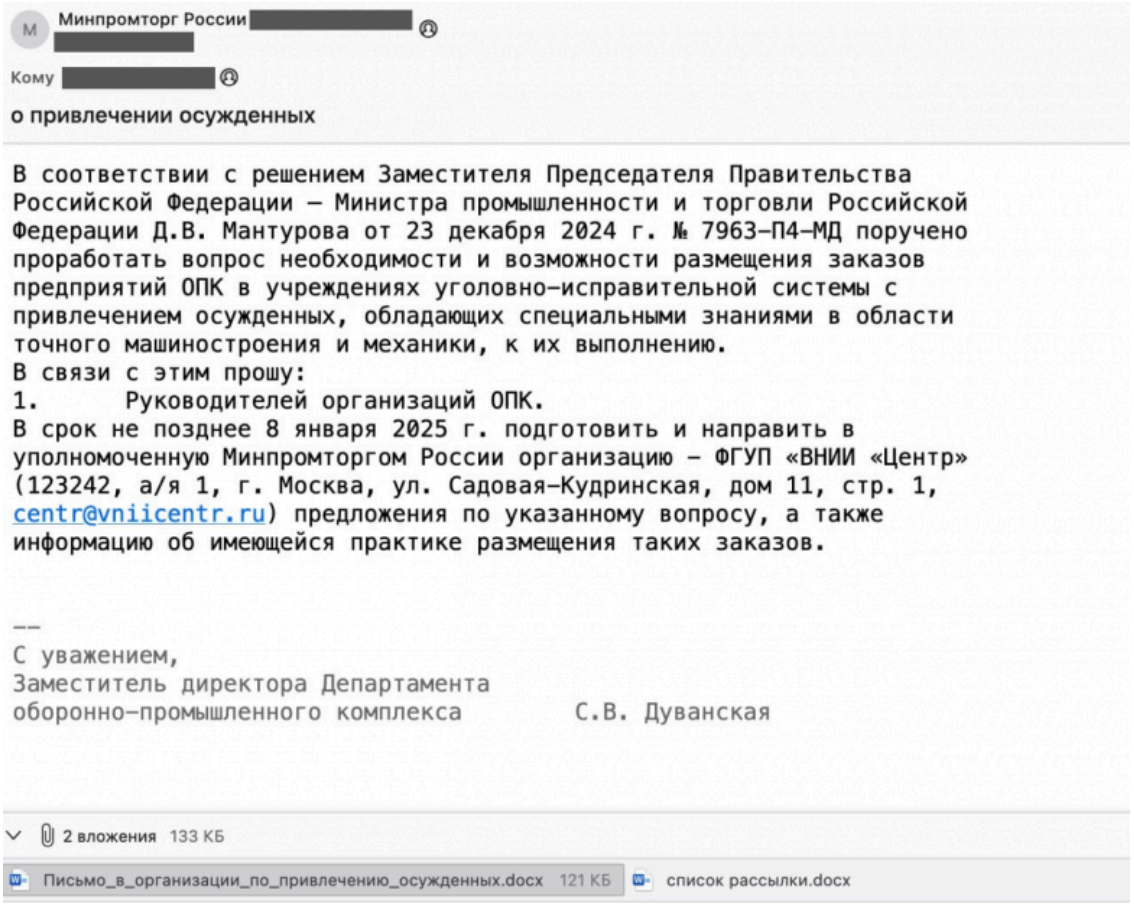


Рисунок 5. Фишинговое письмо, найденное в открытых источниках.

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

---